Ali Nesin

Okura Not: Henüz bitmemiş ve gözden geçirilmemiş kitap notlarıdır. İçinde yanlışlar, eksiklikler, dikkatsizlikler, yanlış ifadeler, kötü anlatımlar olabilir.
anesin@nesinvakfi.org adresine yollanan her türlü düzeltme ve yorum şükranla karşılanacaktır.

Eksikler:
Composition factors
Inverse limit and Hom
BN'den alıştırmalar
Daha fazla Sylow alıştırmaları
Minimal normal subgroups of finite groups
Serbest gruplar ve groups and relations
quaternion group, generalized quaternions
wreath products
HNN?

Nesin Yayıncılık Ltd. Şti.
künye. . .

Ali Nesin

Cebir I

Temel Grup Teorisi

İçindekiler

Önsöz 1
Cebire Başlarken 5

1 Grup Kavramı **9**
1.1 Üç Grup Örneği 9
1.2 Grup Tanımı 12

2 $\mathbb{Z}$ Grubu ve Tamsayılar **23**
2.1 $\mathbb{Z}$'nin Altgrupları 23
2.2 $\mathbb{Z}$'de Bölünebilirlik 24
2.3 $\mathbb{Z}$'de Asallık, İndirgenemezlik vs. 25
2.4 Aritmetiğin Temel Teoremi 27
2.5 En Küçük Ortak Kat 29

3 Simetrik Grup Sym n **33**
3.1 Sym n'nin Elemanlarının Yazılımı 33
3.2 Sym n'de Bileşke 38
3.3 Sym n'de Elemanların Tersleri ve Dereceleri 41
3.4 Sym n'nin Üreteçleri 43
3.5 Alt n Grubu 45
3.6 Sym n'de Eşleniklik 47
3.7 Sym n'de Hangi Tipten Kaç Eleman Var? 50
3.8 Sym n'de Eşlenik Sınıfı Sayısı 54

4 Elemanların Kuvvetleri ve Dereceleri **57**
4.1 Elemanların Kuvvetleri 57
4.2 Elemanların Dereceleri 62

5 Altgruplar **69**

6 Geometri ve Gruplar **79**

7 Üreteçler **95**

8 Altgrup Ötelemeleri **105**
8.1 Altgrupların Ötelemeleri 105
8.2 Bölüm Kümesi 112

9 Normal Altgrup ve Bölüm Grubu **121**
9.1 Normal Altgrup 121
9.2 Bölüm Grubuna Hazırlık 129
9.3 Bölüm Grubu 132
9.4 $\mathbb{Z}$'nin Bölüm Grupları 139

10 Homomorfiler **143**
10.1 Homomorfi 143
10.2 Otomorfi Grubu 152
10.3 İzomorfik Gruplar 157
10.4 Çekirdek 162
10.5 $\mathbb{Z}$, Yeniden 170

11 Bölüm Grubu Üzerine Daha Fazla **177**
11.1 Bölüm Gruplarının Altgrupları 177
11.2 Bölüm Gruplarının Bölüm Grupları 182

12 Direkt ve Yarıdirekt Çarpımlar **185**
12.1 İki Grubun Kartezyen Çarpımı 185
12.2 Çok Sayıda Grubun Direkt Toplamı 188
12.3 Yarıdirekt Çarpım 197

13 Abel Grupları **205**
13.1 Serbest Abel Grupları 205
13.1.1 $\mathbb{Z}$'nin Direkt Toplamları 205
13.1.2 Taban 208
13.1.3 Serbest Abel Grupları 209
13.1.4 Boyut 211
13.1.5 Sonuçlar 212
13.1.6 Evrensel Özellik 217
13.2 Sonlu Sayıda Üreteçli Abel Grupları (1) 220
13.3 Burulmalı Abel Grupları 221
13.4 Sonlu Sayıda Üreteçli Abel Grupları (2) 225
13.5 Bölünür Abel Grupları 226
13.5.1 Prüfer p-Grupları 228
13.5.2 Bölünür Abel Gruplarının Sınıflandırılması 233
13.6 Abel Gruplarının Saf Altgrupları 240

14 Grup Etkisi **245**
14.1 Tanım ve Örnekler 245
14.2 Kavramlar ve Temel Teoremler 249

15 Sıfırkuvvetli ve Çözülür Gruplar **259**
15.1 Komütatör Altgrupları 259
15.2 Azalan Merkezî Seriler, Türev Serileri 263
15.3 Çözülür Gruplar 266
15.4 Artan Merkezî Seri 269
15.5 Sıfırkuvvetli Gruplar 271

16 Sylow Teoremleri **281**
16.1 Sylow Teoremleri 281
16.2 Sylow Teoremlerinin Sonuçları ve Uygulamaları 285

Seminer Konuları ve Ekler **293**

A Öklid Düzleminin Simetrileri **293**
A.1 İzometriler 293
A.1.1 $\mathbb{R}$'nin İzometrileri 294
A.1.2 $\mathbb{R}^2$'nin İzometrileri 297
A.2 Doğruları Doğrulara Götüren Dönüşümler 299

B Kartezyen Çarpım Serbest Abel Grubu Olmayabilir **309**

C Hemen Hemen Her Sonlu Çizge Asimetriktir **313**

D Direkt ve Ters Limit **321**
D.1 Özdeşleştirme 321
D.2 Direkt Limit 327
D.3 Direkt Limitin Evrensel Özelliği 331
D.4 Cebirsel Yapılarda Direkt Limit 338
D.5 Ters Limit 342
D.6 Aralarındaki İlişki 342

E Serbest Gruplar Üzerine **343**
E.1 Altgrupların Üreteçleri 343
E.2 Serbest Grupların Altgrupları 345
E.3 Serbest Tümleyen 349
E.4 Birkaç Sonuç 353

F Zorn Önsavı **357**
F.1 Problemler 357
F.1.1 İmkânsız Bir Problem 357
F.1.2 Çok Kolay Bir Problem 359
F.1.3 Benzer Bir Problem 361
F.1.4 Orta Zorlukta Bir Problem 362
F.1.5 Çetin Bir Problem 365
F.2 Zorn Önsavı ve Birkaç Sonucu 366
F.2.1 Hazırlık 366
F.2.2 Zorn Önsavı 368

Kaynakça ve Okuma Listesi **373**

Önsöz

Soyut cebir bir öğrenci için matematiğin hiç kuşkusuz en zor konusudur. Satır satır okuyarak anlamak o kadar zor değildir (eğer buna anlamak denirse), ne de olsa mantığın sınırları içinde dolanıyoruz, ama soyut cebirin özümsenmesi zordur. Bu zorluğu yenmenin yegâne yolu zamana ve aklına güvenip yılmadan çalışmaktır. Zamanla kavramlar oturacaktır.

Çalışmaktan kastım: Bol örnek ve alıştırma, harcanan kâğıda ve zamana acımadan yazıp silmek, teoremleri kendi başına kanıtlamaya çalışmak ve bunu "tabii ki böyle olmalı, başka türlü nasıl mümkün ki" diyene kadar tekrar tekrar yapmak, kendi örneklerini yaratmak, soyut kavramların somut resimlerini çizmek, harcanan zamana acımadan geriye dönüp kitabı tekrar tekrar okumak. Bir iki ay çalışmaya ara verip tekrar geri dönmek de işe yarar; bezdiğinizde, umutsuzluğa kapıldığınızda böyle yapın, zaman ve bilinçaltı devreye girer ve iki ay sonra kitaba geri döndüğünüzde her şeyi çok daha rahat anlayabilirsiniz. Özellikle en basit örneklere özellikle önem verin. Zor örnekler sanılanın aksine kafa karıştırır.

Eğer kitabın amaçladığı seviyede bir öğrenciyseniz, muhtemelen satır satır okuyarak, sayfaları teker teker çevirerek anlamayacağınız anlar olacaktır. Bölümü bitirdiğinizde, hatta bazen bir iki bölüm daha sonra, önce okuduklarınızı çok daha iyi anlayacaksınız, o kadar ki ilk okuyuşta neden anlamadığınıza bile şaşıracaksınız.

İkinci bir önerim de, anlamadığınız bir şeyle karşılaştığınızda, ondan daha zor şeyleri anlamaya çalışmanız. Böylece daha zor şeylerianlamasanız da daha kolaylarını anlayacaksınız. Grup teorisi zaten yeterince soyut, dolayısıyla zor olduğundan, akademisyenler aşağıdan (öğrencilerden) ve yukarıdan (idareden) gelen baskılara direnemeyerek, dersleri ve kitapları giderek daha fazla kolaylaştırıyorlar. Böyle yaparak öğrencilerin sınavı başarmalarına yardımcı oluyorlar belki ama konuyu anlamalarını imkânsız hale getiriyorlar. Ben şahsen, grup teoriyi faso fiso kitapları bir yana atıp en zor konuları anlamaya çalışarak anladım.

En az dört ciltten oluşacak olan bu soyut cebir serisi grup teoriyle başlıyor. İkinci cilt halkalara ve cisimlere ayrılacak. Üçüncü ciltte lineer cebir yapacağız, yani modüller ve vektör uzaylarıyla ilgileneceğiz. Dördüncü ve beşinci ciltlerde

ilk üç cilde sığmayan konuları ele alırız.

Bölüm ve altbölüm başlıklarına bakıldığında teoremlere değil, kavramlara önem verdiğim gözlenecektir. Örneğin çok yararlı olan ve grup teorisinin vazgeçilmezi olan meşhur Cauchy teoremini örnek ve alıştırmalarda, dolayısıyla küçük puntoyla bulacaksınız. Buna tek istisna, özel bir bölüm ayrılmış olan ve kitabın son bölümünde yer alan Sylow teoremleridir.

Her ne kadar kitabı birinci sayfasından sonuncu sayfasına kadar satır satır okunması niyetiyle yazmışsam da, bunun çoğu zaman mümkün olmadığını biliyorum. Zaten bu kitapta da bezdirici sayıda örnek ve alıştırma olduğundan, kitabı satır satır okumak pek akıl kârı değildir. Bir matematik kitabı bir Dostoyevski romanı okur gibi satır satır okunmaz. Sık sık geçmişe referans koyarak, bazen de kendimi tekrarlayarak, kitabı atlaya zıplaya okumaya karar veren okura kolaylık sağlamak istedim. Umarım tekrar eden bu referanslar akıcılığı bozmaz ve referanslara ihtiyacı olmayan okuru fazla rahatsız etmez.

Örnekleri, alıştırmaları ve ilk okunuşta şöyle bir bakılması gereken bölümleri küçük puntolarla yazdım. Ama gerektiğinde buralara geri dönüp daha dikkatli bir okuma yapmak gerekecektir. Örnek ve alıştırmaların her biri önemlidir; örnek olsun çuval dolsun diye konmamışlardır. Bazı örnek ve alıştırmalar ilk okunuşta zor bulunabilir; geri dönüldüğünde zorluğun kaybolacağını umuyorum. İlk okuyuşta zamansızlıktan ya da başka nedenden atladığınız bölümlere daha sonra geri dönün, daha iyi anlayacaksınız ve iyi anlayacağınız birkaç kavram, kanıt ve teorem, daha başka birçok şeyi çok daha rahatlıkla anlamınızı sağlayarak soyut cebirin kapısını aralayacaktır. (Ne kadar söylesem azdır!)

Dediğim gibi örnekler ve alıştırmalar metnin bir parçasıdır. İçinde teorem geçen örnekleri okumanızı tavsiye ederim, en azından bir göz atın ve beş on dakika zaman geçirip neyin kanıtlandığını anlayın. Örnek ve alıştırmalar arasından bazılarına daha fazla zaman ayırın, özellikle ilk örnek ve alıştırmalara, bunlar neredeyse hemen her zaman diğerlerinden daha temel ve önemlidir; doğal olarak.

Bazen daha sonra kanıtlayacağım teoremleri önceki bölümlerde örnek olarak verdiğim ya da alıştırma olarak okura sorduğum oldu. Aynı teoremin birkaç farklı kanıtını verdiğim de oldu.

Kitabı yazarken aklımda olan okur tipi, matematik lisans 2'nci ya da 3'üncü sınıf öğrencileriydi. Bir de lisansüstü öğrencileri düşündüm. (Dördüncü sınıf lisans öğrencileri için bu kitap ya çok geç ya da çok erkendir!) Bir dönemlik bir ders kitabı olarak düşündüm. (Ama bu, kitap bir dönemde özümsenecektir anlamına gelmez!) Atlanacak bölüm olmamalı, ancak atlanacak ve gerektiğinde geri dönülecek örnek ve alıştırma bol bol olmalı. Bölüm 13'teki Altbölüm 13.5 ve sonrası ilk iki üç (!) okumada atlanabilir. Lisansüstü öğrencileri ise, ekler dahil, kitabı başından sonuna satır satır okumalı.

Ama her durumda yetişmekte olan genç matematikçi kitabı iki üç kez baştan aşağı, bazı bölümleri daha fazla kez okumalı.

Kitabın sonuna, öğrencilerin birbirlerine seminer olarak sunabilecekleri, böylece grup teoriyi daha iyi öğrenebilecekleri bazıları kolay, bazıları daha zor birkaç ek bölüm koydum. Ek bölümler illa kolaydan zora doğru sıralanmamışlardır. Bunlardan biri dışında hiçbiri ana metinde kullanılmayacaktır. Ama mutlaka hepsinin metinde bir önemi olacaktır. Ekleri bilen bir öğrenci hiç kuşkusuz konuyu daha iyi kavrayacaktır. Metinde kullanılacak olan ek, Zorn Önsavı'yla ilgili olan ektir. Zorn Önsavı'na da sadece Bölüm 13'ün sonlarına doğru, Altbölüm 13.3'ten sonra esaslı biçimde ihtiyaç duyulacaktır ve kitabın sonuna kadar da Zorn Önsavı kullanılarak kanıtlanmış sonuçlar kullanılmayacaktır. Öte yandan, sonlu eleman tarafından üretilmiş gruplarla ilgilenen, dolayısıyla Zorn Önsavı'na ihtiyacı olmayan öğrencinin bu bölümleri Zorn Önsavı'na takılmadan kolaylıkla okuyabilmesi için gereken uyarıları yaptım.

Son olarak şunu söyleyeyim ki sınıfta öğrencilerin karşısında ders vermekle kitap yazmak arasında dağlar kadar fark var. Hiçbir dersimde hiçbir kitabı takip edemem. Önceden öğrencilere söz vermiş olsam bile. Kendi yazdığım kitaplar da dahil buna. Ders vermek başka türlü bir özgürlük tanıyor insana. Vereceğim soyut cebir derslerinde halkalara ve modüllere daha hızlı bir giriş yapardım. En azından bu olgun yaşlarımda. Kitapta bu mümkün olmuyor ne yazık ki.

Teşekkür. Birçok yazıyı LaTeX'e dönüştüren Çiğdem Şahin'e, bana her türlü çalışma imkânı yaratan ve teknik konularda yardımcı olan asistanım Aslı Can Korkmaz'a, ortak yazdığımız bazı yazıları kitaba ek olarak aldığım öğrencilerim Halime Ömrüuzun ve Seyfi Türkelli'ye, düzeltmeler yapan öğrencilerim Ergin ve Ersin Süer kardeşlere, Betül Tolgay'a teşekkürü borç bilirim ama yeterli bulmam.

Ali Nesin / NMK, xx xxx 2013

Cebire Başlarken

Matematiğin, en azından tarihin ilk dönemindeki ve belki de nihai amacı, içinde yaşadığımız evreni anlamaktır. Gözle görülen evren de büyük ölçüde geometriyle anlaşılır. Öklid geometrisi önemlidir, olmazsa olmaz, ama tüm geometriyi anlamaya yeterli değildir. Öklid geometrisinden ötesini anlamak için analiz gerekir.

Analiz ise mesafelerle, yani sayılarla yapılır. Sayılarda da toplama, çıkarma, çarpma, bölme gibi işlemler vardır. İşte cebirin başlangıcı bu işlemlerdir. Cebir sayılarla başlar, ama sayılarla bitmez.

Cebirin varoluş nedeni geometriye yardımcı olmaktır. Geometri problemlerini fazla düşünmeden, otomatiğe bağlanarak, yani bir algoritma kullanarak çözmeyi amaçlar cebir. Gerçekten de sayılarla yapılan işlemlerin çoğu zaman pek anlamlı oldukları söylenemez. Örneğin iki sayıyı çarparken ya da bir sayıyı bir başka sayıya bölerken kendimizi alışkanlıklarımıza bırakırız, yaptığımızın bir anlamı olup olmadığını, yazdıklarımızın hangi gerçekle örtüştüğünü pek düşünmeyiz. Tümevarımla kanıt yapıldığında da çoğu zaman otomatiğe bağlanıp kanıt yaparız. Zaten tümevarımla kanıta başlamadan önce neyi kanıtlamak istediğimizi, yani doğru önermeyi önceden bilmemiz gerekir, ki bu da ancak cebirin matematiğin özünü teşkil etmediğine dair bir delil olabilir. Cebirin nesneleri olan polinomlar ve matrislerle çalışırken de anlam peşinden koşmayız. Geometri daha anlamlıdır, geometri sezgilerimize seslenir çünkü; oysa cebir anlamsızdır, algoritmiktir, hesap kitap, kalem kâğıt işidir. Bu yüzden geometrik kavramları resmetmek cebirsel kavramları resmetmekten daha kolaydır. Geometri kitaplarında bol bol şekil, şema, resim vardır, ama cebir kitaplarında bunlardan pek eser yoktur.

Cebiri bu algoritmik özünden kurtarmak tamamen imkânsız değildir, bunu yapmak için cebirle geometriyi yanyana görmek lazım. Cebirle geometri arasında bir seçim yaparken geometriyi yeğlemek lazım. Bu kitapta elimizden geldiğince işte bunu yapmaya çalışacağız. Ama bu hemen olmayacak, biraz zaman gerekecek.

Aşina olduğumuz sayı yapıları dışında birçok cebirsel yapı vardır. Örnek verelim: $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ gibi "halka" adı verilen yapılar matematikte büyük ölçüde sıfat görevini görürler. Okurun muhtemelen daha önce

gördüğü $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ modüler sayı yapıları da halkadırlar.

$(\mathbb{Q}, +, \times)$ ve $(\mathbb{R}, +, \times)$ halkalarına özel bir ad verilir, bunlara "cisim" denir, çünkü bu halkalarda 0 dışında her elemanın çarpımsal bir tersi vardır; ama mesela $(\mathbb{Z}, +, \times)$ halkası cisim değildir. Eğer p bir asalsa, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ yapısı da bir cisimdir. Cisimler özel halkalardır.

$\mathbb{R}^2$, $\mathbb{R}^3$ gibi birkaç boyutlu uzaylar geometrinin temel nesneleridir. Bunlara "vektör uzayı" denir.

$\mathbb{Z}^2$ ve $\mathbb{Z}^3$ yapıları vektör uzayı değildirler ama matematikte önemlidirler. Bunlara "modül" adı verilir. Modülleri matematiğin nesneleri olarak algılayabiliriz.

Modüller ve vektör uzayları nesnedirler, halkalar ve cisimler ise sıfat.

Bazı yapılar hem modül hem de halkadırlar. Bunlara "cebir" adı verilir. Örneğin matrisler bir cebir oluştururlar. Yani aynı anda hem nesne hem de sıfat olabilirler.

Modüller, vektör uzayları, halkalar, cisimler ve cebirler dışında cebirde çok önemli bir yapı daha vardır: Gruplar.

Gruplar soyut cebirin, ele avuca sığan, hesaba kitaba gelen, insanı karşısında çaresiz bırakmayan olabilecek en yalın ve en doğal yapılardır. Bu söylediklerime anlam kazandırmak için şöyle bir örnek vereyim: Diyelim elimizde bir X kümesi var. Bu küme hakkında ne söyleyebiliriz? Ne söyleyebiliriz ki? Sadece bir küme hakkında ne söylenebilir ki? Söylenecek fazla bir şey yok, en azından cebirsel anlamda. Bu küme üzerine bir de

$$f : X \times X \longrightarrow X$$

fonksiyonu verilmiş olsun. Şimdi bu küme ve fonksiyon üzerine ne söyleyebiliriz? Gene söylenecek fazla bir şey bulamayız. Ama diyelim bu fonksiyon, her x, y, $z \in X$ için

$$f(x, f(y, z)) = f(f(z, x), y)$$

gibi bir eşitliği sağlıyor. Konu biraz daha ilginçleşti. Bir de ayrıca mesela

$$f(f(x, y), f(y, z)) = f(x, z)$$

gibi bir eşitlik sağlanıyorsa, söyleyecek çok daha fazla şeyimiz olabilir.

Yukardaki örnek yapaydı ve sanırım pek ilginç değildi. Gruplar ise çok daha doğal, uygulamada yararlı ve ilginç yapılardır. Matematiğin en temel kavramlarından biridir. Her yerde karşımıza çıkarlar.

Her ne kadar grupların ele avuca sığan, hesaba kitaba gelen, insanı karşısında çaresiz bırakmayan olabilecek en yalın ve en doğal yapılar olduğunu söylediysek de, bundan grupların anlaşılması çok kolay yapılar olduğu sanılmasın. Tam tersine, grup teori oldukça zor bir konudur. Cebirin diğer önemli kavramları olan halka, cisim, modül, vektör uzayı, cebir gibi yapılardan daha soyut ve daha zordur.

Modülleri ve vektör uzaylarını yer yüzündeki toz parçacıkları kümesine, halka ve cisimleri de bu toz parçacıklarını niteleyen sıfat kümelerine (örneğin sayı kümelerine) benzetirsek, grupları da bu tozları hareket ettiren rüzgar filan gibi kuvvet kümelerine benzetmek lazım.

Kuvveti gözle görmek daha zor olduğu için, grup teori daha soyuttur. Örneğin bir kürenin resmi çizilebilir, fotoğrafı çekilebilir ama bir grup için aynı şeyi yapamayız.

Bu toz ve kuvvet benzetmesini ciddiye alırsak, pedagojik olarak cebir çalışmaya modüllerden ve vektör uzaylarından, o da olmadı sıfat görevini gören halkalardan başlamak lazım. Cebir yazarları tarafından pek rağbet görmese de ve teknik olarak mümkün olmasa da bunun çok yanlış bir bakış açısı olduğunu sanmıyorum. Kısa bir grup teoriye girişten sonra halkalara ve cisimlere, ardından modüllere ve vektör uzaylarına yöneleceğiz. Grup teoriyi de – olabildiğince – etkilediği nesnelerle birlikte göreceğiz.

Okuyacağınız cebir notları herhangi bir cebir altyapısı gerektirmeyecek biçimde yazılmaya çalışılmıştır. Ama bu demek değildir ki matematiğe yeni başlayanlar için yazılmışlardır; sanırım notlardan maksimum yarar için belli bir matematiksel olgunluk gerektiriyor. Öte yandan yazılanı hemen anlamayan okur paniğe kapılmadan devam etsin, çok büyük bir olasılıkla daha sonra birkaç sayfa önce söyleneni çok daha iyi anlayacaktır ve hatta neden daha önce anlamadığına şaşıracaktır. En azından böyle olacağını umuyorum.

İçimden başarı ve kolaylıklar dilemek geçiyor ama ne yazık ki her ikisi birden aynı anda mümkün olmuyor.

1. Grup Kavramı

1.1 Üç Grup Örneği

Üç örnekle grup kavramına giriş yapalım. Matematiksel tanımı daha sonra vereceğiz.

Notlar ve Örnekler

1.1. Tamsayılar kümesi $\mathbb{Z}$'yi ve $\mathbb{Z}$ üzerine tanımlanan toplama işlemini ele alalım, yani $(\mathbb{Z}, +)$ yapısını ele alalım. Her şeyden önce toplama $\mathbb{Z}$ kümesi üzerine (ikili) bir işlemdir, yani **iki** tamsayının toplamı gene bir tamsayıdır. $\mathbb{Z}$ kümesi üzerine tanımlanmış bu toplama işleminin şu özellikleri vardır.

Toplama işlemi "birleşme özelliği"ni sağlar, yani her x, y, $z \in \mathbb{Z}$ için

$$x + (y + z) = (x + y) + z$$

olur. Bunun dışında, $\mathbb{Z}$'de toplama işlemi için bir "etkisiz eleman" vardır: 0; yani her $x \in X$ için

$$x + 0 = 0 + x = x$$

olur. Bir üçüncü özellik daha vardır: Her $x \in \mathbb{Z}$ için öyle bir $y \in \mathbb{Z}$ vardır ki

$$x + y = y + x = 0$$

olur. Bu y'nin $-x$ olduğunu bilmeyen yoktur. İşte grup denen şey, bir küme (örnekte $\mathbb{Z}$) ve bu küme üzerinde yukardaki üç özelliği sağlayan (ikili) bir işlemdir (örnekte toplama). Tam matematiksel tanım örneklerden sonra gelecek.

Bu örnekte, işlemi değiştirmeden $\mathbb{Z}$ kümesi yerine $\mathbb{Q}$ ya da $\mathbb{R}$ kümesini de alabilirdik, üç özellik gene sağlanırdı. Hatta çift sayılar kümesi $2\mathbb{Z}$'yi ya da daha genel olarak bir n sayısının katlarından oluşan $n\mathbb{Z}$ kümesini de alabilirdik. Burada n, 0 dahil, herhangi bir gerçel sayı olabilir, mesela $\frac{1}{2}\mathbb{Z}$ kümesi ve toplama işlemi yukardaki üç özelliği sağlar. Ama $\mathbb{Z}$ yerine $\mathbb{N}$'yi alsaydık üçüncü özellik doğru olmazdı.

$\mathbb{Z}$ yerine $\mathbb{Z}\setminus\{3, -3\}$ alsaydık toplama altında bir grup elde etmezdik, çünkü her ne kadar üç özellik doğruysa da, bu küme üzerinde toplama her zaman tanımlı değildir, örneğin 1 ile 2 bu kümededir ama toplamları olan 3 bu kümede değildir. 9 ve -6'nın toplamı da bu kümede değildir. Yani toplama $\mathbb{Z}\setminus\{3, -3\}$ kümesi üzerinde bir işlem değildir. $\mathbb{Z}\setminus\{0\}$ kümesi de toplama altında kapalı değildir.

1.2. Bu sefer $\mathbb{R}^*$ olarak göstereceğimiz 0'dan farklı gerçel sayılar kümesini alacağız: $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$. Ama işlemimiz çarpma olacak. Yani $(\mathbb{R}^*, \cdot\,)$ yapısını ele alacağız. Birleşme özelliği gene geçerli:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

Etkisiz eleman gene var: 1; yani her $x \in \mathbb{R}^*$ için

$$x \cdot 1 = 1 \cdot x = x$$

olur. Ayrıca her $x \in \mathbb{R}^*$ için öyle bir $y \in \mathbb{R}^*$ vardır ki

$$x \cdot y = y \cdot x = 1$$

olur. Bu y elbette $1/x$ sayısıdır.
Bu örnekte $\mathbb{R}^*$ yerine $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^{>0} = (0, \infty)$ ya da $\mathbb{Q}^{>0} = \mathbb{R}^{>0} \cap \mathbb{Q}$ kümelerinden birini de alabilirdik, üç özellik gene sağlanırdı. Ama $\mathbb{R}^*$ yerine $\mathbb{Z} \setminus \{0\}$ kümesini alsaydık üçüncü özellik doğru olmazdı, mesela 2 sayısının çarpımsal tersi olan $1/2$ bu kümede değildir. Öte yandan $\{1, -1\}$ kümesi çarpma işlemi için yukardaki üç özelliği de sağlar. Tek elemanlı $\{1\}$ kümesi de çarpma altında kapalıdır ve üç özelliği sağlar. Şu örnek de ilginç: Eğer $a \in \mathbb{R}^*$ ve $A = \{a^n : n \in \mathbb{Z}\}$ ise, $(A, \cdot)$ yapısının yukardaki üç özelliği vardır. Eğer $a, b \in \mathbb{R}^*$ ve $A = \{a^n b^m : n, m \in \mathbb{Z}\}$ ise, $(A, \cdot)$ yapısının da yukardaki üç özelliği vardır. Bir de şu örneğe bakalım:

$$B = \{\pi^n q : n \in \mathbb{Z},\, q \in \mathbb{Q}^*\}.$$

Bu son küme de çarpma işlemi altında kapalıdır ve yukardaki üç özelliği de sağlar.

1.3. Yukardaki örnekler ***değişmeli*** grup örnekleridir, yani her x, y için, birinci örnekte $x + y = y + x$, ikinci örnekte $x \cdot y = y \cdot x$ olur. Değişmeli gruba daha ziyade ***abel*** grubu denir. Bu örnekteki grup abel grubu olmayacak.
Dikkat ederseniz yukardaki iki örnekte bir küme ve bu küme üzerine bir işlem (birinci örnekte toplama, ikinci örnekte çarpma) aldık. Nitekim bir grup olması için bir küme ve bu küme üzerine tanımlı (ikili) bir işlem olmalıdır. Bu son örneğimizde herhangi bir X kümesi alacağız ve üzerine işlem tanımlayacağımız küme X'in eşleşmeleri (ya da bijeksiyonları), yani X'ten X'e giden birebir ve örten fonksiyonlar kümesi olacak. Grup teoride eşleşme ya da bijeksiyon yerine ***permütasyon*** sözcüğü kullanılır, biz de öyle yapacağız. X'in permütasyonları kümesi $\operatorname{Sym} X$ olarak yazılır:

$$\operatorname{Sym} X = \{f : X \longrightarrow X : f \text{ birebir ve örten}\}.$$

İşlem olarak fonksiyonların bileşkesini alacağız. Bileşke kavramını anımsatalım. Eğer $f : X \longrightarrow Y$ ve $g : Y \longrightarrow Z$ birer fonksiyonsa, kısaca "gof" diye okunan $g \circ f : X \longrightarrow Z$ fonksiyonu, her $x \in X$ için

$$(g \circ f)(x) = g(f(x))$$

olarak tanımlanır. Birebir ve örten fonksiyonların bileşkesi de birebir ve örtendir, dolayısıyla eğer $f, g \in \operatorname{Sym} X$ ise $g \circ f$ ve $f \circ g$ fonksiyonları da $\operatorname{Sym} X$ kümesindedir.
İlk iki örnekte altını çizdiğimiz üç özelliği teker teker kontrol edelim. Birleşme özelliği sadece permütasyonlar için değil, bileşkesi alınabilen tüm fonksiyonlar için geçerlidir: Eğer $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$, $h : Z \longrightarrow T$ ise,

$$h \circ (g \circ f) = (h \circ g) \circ f$$

olur. Bu önemli eşitliği kanıtlayalım. Her iki fonksiyonun da tanım kümesi X, değer kümesi T. Bakalım iki fonksiyon da aynı elemanda aynı değeri alıyor mu? $x \in X$, rastgele bir eleman olsun. Bileşkenin tanımını kullanarak hesaplayalım:

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$$

ve

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$$

olur. Böylece birinci özelliğin (birleşme özelliğinin) sağlandığını göstermiş olduk. İkinci özellik, etkisiz elemanın varlığını söylüyor. Sym X'te etkisiz eleman var mı? Özdeşlik fonksiyonu ya da ***birim fonksiyon*** $\mathrm{Id}_X : X \longrightarrow X$, sadece eşleşmelerin değil, tüm uygun fonksiyonlar için bileşke işleminin etkisiz elemanıdır ve elbette Sym X'in bir elemanıdır. Unutanlar için anımsatalım, Id_X fonksiyonu, her $x \in X$ için

$$\mathrm{Id}_X(x) = x$$

olarak tanımlanmıştır. Elbette her $f : X \longrightarrow Y$ fonksiyonu için

$$f \circ \mathrm{Id}_X = f \text{ ve } \mathrm{Id}_Y \circ f = f$$

olur. Bu özellik de sağlandı. Sonuncu özelliğe gelelim. $f \in \mathrm{Sym}\, X$ olsun. Acaba

$$f \circ g = g \circ f = \mathrm{Id}_X$$

eşitliğini sağlayan bir $g \in \mathrm{Sym}\, X$ var mı? Var, çünkü f birebir ve örten olduğundan, f'nin bir "ters fonksiyonu" vardır. Bunu da unutanlar için anımsatalım: Eğer $f : X \longrightarrow Y$ bir eşlemeyse, o zaman $f^{-1} : Y \longrightarrow X$ fonksiyonu, her $y \in Y$ için

$$f^{-1}(y) = x \Leftrightarrow f(x) = y$$

önermesi doğru olacak biçimde tanımlanmıştır, yani f fonksiyonu a'yı b'ye götürüyorsa, f^{-1} fonksiyonu f'nin yaptığını bozarak b'yi tekrar a'ya geri getirir. f^{-1} fonksiyonu da bir eşlemedir ve

$$f \circ f^{-1} = \mathrm{Id}_Y \text{ ve } f^{-1} \circ f = \mathrm{Id}_X$$

olur. Demek ki eğer $f \in \mathrm{Sym}\, X$ ise f^{-1} fonksiyonu da Sym X'tedir ve

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}_X$$

olur. Önemsediğimiz üçüncü özellik de sağlandı.
Eğer $|X| > 2$ ise bileşke işlemi Sym X üzerine değişmeli değildir. Örneğin $X = \{1, 2, 3\}$ olsun ve f, $g \in \mathrm{Sym}\, X$ permütasyonları şöyle tanımlansınlar:

$$f(1) = 2,\ f(2) = 1,\ f(3) = 3$$

ve

$$g(1) = 1,\ g(2) = 3,\ g(3) = 2.$$

O zaman

$$(g \circ f)(1) = g(f(1)) = g(2) = 1$$

ve

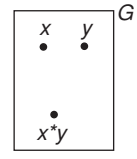
$$(f \circ g)(1) = f(g(1)) = f(1) = 2$$

olur. $g \circ f$ ve $f \circ g$ permütasyonları 1'de farklı değer aldıklarından birbirine eşit değildirler. Sonuç olarak Sym X kümesi bileşke işlemiyle birlikte bir grup olur. Çok çok önemli bir gruptur. Hakkında çok daha fazla konuşacağız.
Eğer $X = \{1, 2, \ldots, n\}$ ise Sym X yerine Sym n yazılır. Bölüm 3'te sadece bunları konu edeceğiz.

Örnekleri daha sonra çoğaltmak üzere, grubun tanımına gelelim.

1.2 Grup Tanımı

Küme ve İşlem. Bir grubun oluşması için her şeyden önce bir küme gerekir. Kümeye G diyelim, grubun G'si. Bir grup sadece bir küme değildir – yoksa grup yerine küme derdik. Bir grup bir G kümesinden ve $G \times G$ kartezyen çarpımından G'ye giden bir fonksiyondan oluşur. Bu fonksiyona "fonksiyon"dan ziyade ***işlem***, bazen de ***ikili işlem*** denir. Ayrıca eğer $(x, y) \in G \times G$ ise, fonksiyonun bu ikiliyi gönderdiği G'nin elemanını $\star(x, y)$ olarak değil, $x \star y$ olarak yazalım. Yukarıdaki örneklerde $x \star y$ işlemi sırasıyla $x + y$, $x \cdot y$ ve $x \circ y$ idi. İşlemde unutulmaması gereken nokta, işlemin sonucunun gene G kümesinde olma zorunluluğudur. Örneğin $(x, y) \mapsto x - y$ kuralı $\mathbb{N}$ üzerine bir işlem tanımlamaz, çünkü x ve y birer doğal sayıysa $x - y$ her zaman bir doğal sayı değildir; öte yandan aynı kural bize $\mathbb{Z}$ kümesi üzerine bir işlem tanımlar. Bir başka örnek: $(x, y) \mapsto x/y$ kuralı $\mathbb{R}$ üzerine bir işlem tanımlamaz, çünkü $y = 0$ ise x/y anlamsızdır; öte yandan aynı kural bize $\mathbb{R} \setminus \{0\}$ kümesi üzerine bir işlem tanımlar.



Bir grubun oluşması için bir küme ve bu küme üzerine tanımlanmış bir işlem gerekir dedik, ama bir grubun oluşması için bunlar yeterli değildir, ayrıca kümenin ve işlemin aşağıda G1, G2, G3 olarak listeleyeceğimiz üç özelliği sağlaması gerekir.

G1. Birleşme Özelliği. Bir grubun oluşması için sağlanması gereken birinci özellik, birleşme özelliğidir. Yani her x, y, $z \in G$ için

$$x \star (y \star z) = (x \star y) \star z$$

olmalı. Bu çok önemli bir özelliktir. Bir işlemde bu ya da en azından buna benzer bir özellik yoksa durum umutsuz demektir, işlemi erişmesi uzak bir kenara kaldırabilirsiniz! En azından

$$x \star (x \star x) = (x \star x) \star x$$

eşitliği doğru olmalı ki, hangi sırayla çarpacağımıza (yani işlem yapacağımıza) dair kuşkuya düşmeden x'i kendisiyle üç defa çarpabilelim ve x^3 diye bir elemandan sözedebilelim.

Birleşme özelliği sayesinde elli tane elemanı, belirlenmiş sırayı bozmamak kaydıyla istediğimiz gibi çarpabiliriz; örneğin,

$$((x \star y) \star z) \star t,\ (x \star (y \star z)) \star t,\ (x \star y) \star (z \star t),\ x \star ((y \star z) \star t),\ x \star (y \star (z \star t))$$

çarpımlarının hepsi eşittir; dolayısıyla bu çarpımları

$$x \star y \star z \star t$$

olarak parantezsiz yazabiliriz. Üç ve dört eleman için doğru olan bu özellik her sayıda elemanın çarpımı için de doğrudur. (Bunun kanıtlanması gerekir, ama Bourbaki dışında herhangi bir kitapta bu bariz ve sıkıcı önermenin kanıtlandığını görmedim; güzelim geleneklere uyarak biz de kanıtlamayacağız.)

Ama elemanların çarpım sırasını her zaman değiştiremeyebiliriz, çünkü $x \star y$ her zaman $y \star x$ olmak zorunda değildir. Bu özelliğin sağlandığı gruplara değişmeli grup ya da abel grubu denir. Abel grupları, en basit gruplar olduklarından, bunların grup teorisinde özel bir yeri vardır.

Sonlu sayıda elemanın çarpımının tanımlandığını da gözlemleyelim. Sonsuz sayıda elemanı çarpmak (ya da toplamak) için yakınsaklık gibi analize özgü kavramlar gerekir.

G2. Etkisiz Elemanın Varlığı. Bir grubun oluşması için $\star$ işleminin birleşme özelliği dışında bir de ayrıca ***etkisiz elemanı*** olmalıdır, yani G'nin öyle bir e elemanı olmalıdır ki, her $x \in G$ için

$$e \star x = x \star e = x$$

eşitliği sağlansın. (Dikkat: "her x için öyle bir e vardır ki..." demedik, "öyle bir e var ki her x için..." dedik.) Bu özelliği sağlayan bir elemana ***etkisiz eleman*** denir. Aslında her $x \in G$ için $e \star x = x$ eşitliğini sağlayan elemana ***soldan etkisiz eleman***, her $x \in G$ için $x \star e = x$ eşitliğini sağlayan elemana ***sağdan etkisiz eleman*** denir. Ama soldan ve sağdan etkisiz elemanlar - eğer varlarsa - eşittirler:

Önsav 1.1. *$\star$, G üzerine ikili bir işlemse ve bu işlemin sağdan ve soldan etkisiz elemanları varsa, bu elemanlar eşittirler.*

Kanıt: e soldan, f de sağdan etkisiz eleman olsun. Her $x \in G$ için $e \star x = x$ olduğundan (bunu $x = f$ özeline uygulayarak)

$$e \star f = f$$

eşitliğini elde ederiz. Her $x \in G$ için $x \star f = x$ olduğundan (bunu $x = e$ özeline uygulayarak)

$$e \star f = e$$

eşitliğini elde ederiz. Demek ki

$$f = e \star f = e.$$

İstediğimiz kanıtlanmıştır. □

Demek ki bir grupta tek bir etkisiz eleman vardır.

G3. Elemanların Tersi. Bir grupta, grubun her x elemanı için

$$x \star y = y \star x = e$$

eşitliğini sağlayan bir y elemanı olmalıdır. Buradaki e, G2'de varlığı söylenen grubun yegâne etkisiz elemanıdır. Verilmiş bir x için bu özelliği sağlayan bir y vardır ama her x için başka bir y olabilir (ve nitekim öyle de olur.) Önce verilmiş bir x için bu özelliği sağlayan y'nin biricik olduğunu kanıtlayalım.

Önsav 1.2. *Birleşme özelliğini sağlayan ve etkisiz elemanı e olan bir $(G, \star)$ yapısında (e'nin biricik olduğunu bir önceki önsavdan biliyoruz) eğer $z \star x = x \star y = e$ ise $z = y$ olur.*

Kanıt: Kanıtımız tek bir satırdan oluşacak:

$$y = e \star y = (z \star x) \star y = z \star (x \star y) = z \star e = z.$$

Kanıtımız bitmiştir. □

Madem ki bir grupta, verilmiş bir x için, $x \star y = y \star x = e$ eşitliğini sağlayan bir ve bir tane y var, bu y elemanına özel bir ad verelim: y'ye x'in ($\star$ işlemine göre) ***tersi*** adı verilir ve bu eleman

$$x^{-1}$$

olarak yazılır. Yukardaki önsava göre bir grupta her x elemanı için

$$y = x^{-1} \Leftrightarrow x \star y = e \Leftrightarrow y \star x = e$$

olur. Bunun sonucu olarak, eğer y, x'in tersiyse, x'in de y'nin tersi olduğu anlaşılır; nitekim yukardaki eşdeğer koşullardan son ikisi x ve y'ye göre birbirinin simetriğidir. Yani x'in tersinin tersi x'tir:

$$(x^{-1})^{-1} = x.$$

$e \star e = e$ olduğundan, $e^{-1} = e$ olur. Ama e kendi kendisinin tersi olan yegâne eleman olmayabilir; örneğin $\mathbb{R}^\star$ grubunda -1 elemanı da kendisinin tersidir, ya da $\operatorname{Sym} X$ grubunda X'in iki elemanını değiştiren ama diğer hiçbir elemanı değiştirmeyen eşleme kendi kendisinin tersidir.

Kolayca gösterilebileceği üzere bir grupta $x \star y$ elemanının tersi $y^{-1} \star x^{-1}$ elemanıdır ve ($x \star y = y \star x$ olmadıkça) $x^{-1} \star y^{-1}$ değildir.

Bir grupta sadeleştirme yapılabilir, yani $x \star a = x \star b$ ise $y = z$ olur. Nitekim, eşitliğin her iki tarafını da x^{-1} ile çarparsak $a = b$ eşitliğini buluruz. Bu kanıtı daha formel olarak yazalım:

$$a = e \star a = (x^{-1} \star x) \star a = x^{-1} \star (x \star a) = x^{-1} \star (x \star b) = (x^{-1} \star x) \star b = e \star b = b.$$

Ve elbette $a \star x = b \star x$ ise $a = b$ olur, kanıt aynıdır. Ama dikkat $x \star a = b \star x$ ise a ve b eşit olmak zorunda değildirler.

Bir grupta $a \star x \star b = c$ denkleminin bir ve bir tane çözümü vardır: $x = a^{-1} \star c \star b^{-1}$. Ama $x \star a \star x = b$ eşitliğinin çözümü olmayabilir.

Grubun tanımını biçimsel olarak yazalım.

Tanım. *Bir grup, bir G kümesi ve bu G kümesi üzerine aşağıdaki* G1, G2, G3 *özelliklerini sağlayan bir $\star : G \times G \longrightarrow G$ ikili işleminden oluşur.*
G1. *Her x, y, $z \in G$ için $x \star (y \star z) = (x \star y) \star z$.*
G2. *Öyle bir $e \in G$ vardır ki, her $x \in G$ için $x \star e = e \star x = x$ olur. (Bu özelliği olan e elemanı zorunlu olarak biriciktir.)*
G3. *e, bir önceki özelliği sağlayan yegâne eleman olsun. Her $x \in G$ için öyle bir $y \in G$ vardır ki $x \star y = y \star x = e$ eşitlikleri sağlanır. (Verilmiş her $x \in G$ için, bu özelliği sağlayan y elemanı zorunlu olarak biriciktir ve x^{-1} olarak yazılır.)*

Demek ki bir grup, yukarıdaki G1, G2, G3 özelliklerini sağlayan bir G kümesinden ve bu küme üzerine tanımlanmış bir $\star$ işleminden oluşur; yani bir grup bir $(G, \star)$ ikilisidir. Ama çoğu zaman işlemin ne olduğu ya çok barizdir ya da işelem önemli değildir ve bu durumda $(G, \star)$ grubundan değil G grubundan sözedilir. Örneğin $\mathbb{R}$, $\mathbb{Q}$ ya da $\mathbb{Z}$ grubundan sözedildiğinde işlemin toplama olduğu söylenmeden varsayılır. $\mathbb{R}^\star$, $\mathbb{Q}^\star$, $\mathbb{R}^{>0}$, $\mathbb{Q}^{>0}$ grupları aksi söylenmedikçe çarpma altında bir gruptur. $\operatorname{Sym} X$ ise şaşmaz bir biçimde bileşke altında bir gruptur.

$x \star y$ elemanına "x ve y'nin ***çarpımı***" denir (ama işlem toplama bile olabilir!)

Notlar ve Örnekler

1.4. İlk 3 örneğimiz sayı ve fonksiyon kümelerinden oluşuyordu. Bu örnekte bir X kümesinin altkümelerini eleman olarak kabul eden $\wp(X)$ kümesine bakacağız. Bu kümeyi bir gruba dönüştüreceğiz. Önce işlemi tanımlayalım, bir gruba ulaşmanın başka yolu yok. İşlemimiz ***simetrik fark*** işlemi olarak adlandırılan Δ işlemi olacak. Bu işlemi tanımlayalım: A, $B \in \wp(X)$ için, $A \Delta B$ şöyle tanımlanmıştır:

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

Simetrik farkı şöyle de tanımlayabilirdik:

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

İki tanımın eşdeğer olduğunun kanıtını okura bırakıyorum. Şu özellikler doğrudur:
G1. Her A, B, $C \in \wp(X)$ için $A \Delta (B \Delta C) = (A \Delta B) \Delta C$. Bu, hemen bakınca doğruluğu anlaşılacak eşitliklerden değil, biraz uğraşmak gerekiyor. Ama bundan sonraki eşitlikler bariz.
G2. Her $A \in \wp(X)$ için $A \Delta \emptyset = \emptyset \Delta A = A$ olur. Demek ki $\emptyset$, simetrik fark işleminin etkisiz elemanı.
G3. Her $A \in \wp(X)$ için $A \Delta A = \emptyset$ olur. Demek ki her elemanın tersi var ve bu ters elemanın kendisi. Bir başka deyişle her A için $A^{-1} = A$.

Demek ki $(\wp(X), \Delta)$ bir gruptur. Ayrıca bir abel grubudur, yani her A, $B \in \wp(X)$ için $A\Delta B = B\Delta A$ olur.

1.5. X tercihan sonsuz bir küme olsun ve X'in sonlu altkümelerinden oluşan $\wp^{<\omega}(X)$ kümesine bakalım. Eğer A ve B bu kümedelerse, $A\Delta B$ de elbette bu kümededir. Demek ki Δ, $\wp^{<\omega}(X)$ kümesi üzerine bir işlemdir. G1 elbette sağlanıyor. Boşküme sonlu bir küme olduğundan $\wp^{<\omega}(X)$ kümesinin bir elemanıdır, dolayısıyla G2 de sağlanıyor. Yukardaki örnekte de gördüğümüz üzere bir $A \in \wp^{<\omega}(X)$ elemanının Δ işlemi için tersi gene kendisi olduğundan, G3 özelliği de sağlanıyor. Demek ki $(\wp^{<\omega}(X), \Delta)$ bir gruptur. Bu tür durumlarda $\wp^{<\omega}(X)$ grubunun (bir önceki örnekte tanımlanan) $\wp(X)$ grubunun bir altgrubu olduğu söylenir. Ama altgruplar çok önemli bir kavram olduğu için bu kavramı apayrı ve upuzun bir yazıda ele alacağız.

1.6. $G = \{x^2 + y^2 : x,\, y \in \mathbb{Q}\} \setminus \{0\}$ olsun.

$$(x^2 + y^2)(z^2 + t^2) = (xz + yt)^2 + (xt - yz)^2$$

eşitliğinden G'nin çarpma altında kapalı olduğu belli.

$$\frac{1}{x^2 + y^2} = \left(\frac{x}{x^2 + y^2}\right)^2 + \left(\frac{y}{x^2 + y^2}\right)^2$$

eşitliğinden, eğer $q \in G$ ise $1/q \in G$ olduğu belli. Tabii ki $1 \in G$. Dolayısıyla G çarpma işlemi altında bir gruptur.

Vwerdiğimiz bu üç örneğin oldukça egzotik olduğunu söyleyebiliriz. Grupların en olmadık yerlerde karşımıza çıkabileceklerini göstermek için verilmişlerdir. Aşağıda ve (genel olarak) bu kitapta çok daha klasik grup örnekleri vereceğiz.

1.7. **(Kartezyen Çarpım 1.)** G ve H iki grup olsun. G ve H farklı kümeler ve işlemleri de farklı olabilir ama biz gene de G'nin ve H'nin işlemlerini aynı simgeyle, $\star$ ile gösterelim. $G \times H$ kartezyen çarpımı kümesi,

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \star g_2, h_1 \star h_2)$$

formülüyle tanımlanan işlemle "doğal olarak" bir grup olur. G1'in basit kanıtı:

$$\begin{aligned}((g_1, h_1) \star (g_2, h_2)) \star (g_3, h_3) &= (g_1 \star g_2, h_1 \star h_2) \star (g_3, h_3)\\ &= ((g_1 \star g_2) \star g_3, (h_1 \star h_2) \star h_3)\\ &= (g_1 \star (g_2 \star g_3), h_1 \star (h_2 \star h_3))\\ &= (g_1, h_1) \star (g_2 \star g_3, h_2 \star h_3)\\ &= (g_1, h_1) \star ((g_2, h_2) \star (g_3, h_3)).\end{aligned}$$

Diğer iki özelliğin de kanıtı kolay: Eğer e_G ve e_H sırasıyla G ve H gruplarının etkisiz elemanıysa,

$$(e_G, e_H)$$

elemanı $G \times H$ grubunun etkisiz elemanıdır. Ayrıca, eğer $(g, h) \in G \times H$ ise, kolayca kontrol edilebileceği üzere

$$(g, h)^{-1} = (g^{-1}, h^{-1})$$

olur.

$G \times H$ grubuna G ve H gruplarının ***kartezyen çarpımı*** adı verilir. Eğer G ve H abel gruplarıysa, $G \times H$ grubu da bir abel grubudur.

İki grubun kartezyen çarpımı gibi, sonlu sayıda grubun da kartezyen çarpımı alınabilir. Sonraki örneklerde sonsuz sayıda grubun kartezyen çarpımını almayı göreceğiz.

Bu kitapta sık sık karşılaşacağız,

$$\pi_1(g, h) = g \text{ ve } \pi_2(g, h) = h$$

formülleriyle tanımlanmış

$$\pi_1 : G \times H \longrightarrow G \text{ ve } \pi_2 : G \times H \longrightarrow H$$

fonksiyonlarına ***doğal izdüşüm fonksiyonları*** adı verilir. Kolayca kontrol edilebileceği üzere,

$$\pi_i((g,h)(g_1,h_1)) = \pi_i(g,h)\pi_i(g_1,h_1)$$

olur.

1.8. **(Kartezyen Çarpım 2.)** I herhangi bir küme ve G bir grup olsun. Fonk(I,G), I'dan G'ye giden foksiyonlar kümesi olsun. G'yi grup yapan işlemi $\star$ olarak yazalım. G'nin etkisiz elemanı da e olsun. Şimdi Fonk(I,G) üzerinde bir işlem tanımlayalım. Bu işlem de genellikle $\star$ olarak yazılır. Eğer f, $g \in$ Fonk(I,G) ise $f \star g : I \longrightarrow G$ fonksiyonu şöyle tanımlanır: Her $i \in I$ için,

$$(f \star g)(i) = f(i) \star g(i).$$

$f \star g$ fonksiyonuna f ve g fonksiyonlarının ***noktasal çarpımı*** adı verilir. Fonk(I,G) bu işlem altında bir grup olur. G1 özelliğinin kanıtını okura bırakıyoruz; nitekim G bu özelliği sağladığından Fonk(I,G) de sağlar. I'nın her noktasında e değerini alan sabit e fonksiyonu Fonk(I,G) grubunun etkisiz elemandır. Ve son olarak eğer $f \in$ Fonk(I,G) ise, her $i \in I$ için

$$f^{-1}(i) = f(i)^{-1}$$

kuralıyla tanımlanan fonksiyon f'nin tersidir; nitekim, her $i \in I$ için,

$$(f \star f^{-1})(i) = f(i) \star f^{-1}(i) = f(i) \star f(i)^{-1} = e$$

olur, yani $f \star f^{-1}$ fonksiyonu sabit e değerini alan fonksiyondur; benzer şekilde $f^{-1} \star f$ fonksiyonunun sabit e fonksiyonu olduğu gösterilebilir.

Bu grup genelde Fonk(I,G) olarak değil de $\prod_I G$ ya da G^I ya da ${}^I G$ olarak yazılır ve G grubunun kendisiyle I defa ***kartezyen çarpımı*** olarak adlandırılır. Ve bir fonksiyon aldığı değerler tarafından belirlendiğinden, $f \in$ Fonk$(I,G) = G^I$ fonksiyonu

$$f = (f(i))_i$$

olarak yazabilir ve bu yazılım tercih edilir. Hatta çoğu zaman $f(i)$ yerine f_i yazılır:

$$f = (f_i)_i.$$

Bu yazılımla fonksiyonların çarpımı,

$$(f_i)_i \star (g_i)_i = (f_i \star g_i)_i$$

şeklini alır.

Eğer I sonluysa, diyelim 3 elemanı varsa, $G \times G \times G$ yazılımı tercih edilebilir ve elemanları (g_1, g_2, g_3) olarak yazılabilir. Eğer I'nın n tane elemanı varsa G^n ya da $G \times G \times \cdots \times G$ yazılır. $n = 2$ olduğunda bir önceki örneğin $G = H$ durumuna çok benzer bir örnek elde ettiğimize dikkat edin[1].

G^I grubunun abel olması için G'nin abel olması yeter ve gerek koşuldur. Ayrıca, bir X kümesinin kardinalitesini $|X|$ olarak gösterirsek, $\left|G^I\right| = |G|^{|I|}$ eşitliği geçerlidir.

1.9. **(Kartezyen Çarpım 3.)** I bir küme ve $(G_i)_{i \in I}$ bir grup ailesi olsun. Her G_i grubunun işlemini aynı simgeyle, $\star$ ile gösterelim.

$$\prod_I G_i = \left\{ f : I \longrightarrow \bigcup_{i \in I} G_i : \text{her } i \in I \text{ için } f(i) \in G_i \right\}$$

[1] İleride bu benzerliği izomorfi olarak adlandıracağız ve grupların izomorfik olduklarını söyleyeceğiz.

olsun. $f \in \prod_I G_i$ için $f(i)$ yerine f_i yazalım ve f elemanını (ya da fonksiyonunu) $(f_i)_i$ olarak gösterelim. Şimdi $\prod_I G_i$ kümesinde

$$(f_i)_i \star (g_i)_i = (f_i \star g_i)_i$$

tanımını yapalım. Bu işlemle $\prod_I G_i$ kümesi bir grup olur. Bunun kanıtı kolaydır ve okura bırakılmıştır. $\prod_I G_i$ grubuna $(G_i)_i$ grup ailesinin ***kartezyen çarpımı*** adı verilir. Kartezyen çarpımın abel olması için yeter ve gerek koşul her G_i grubunun abel olmasıdır. Eğer her G_i grubu G grubuna eşitse, bir önceki örneği buluruz.
Eğer I sonluysa, mesela $I = \{1, 2, \ldots, n\}$ ise $\prod_I G_i$ yerine şu yazılımlar da kullanılır:

$$G_1 \times \ldots \times G_n = \prod_{i=1}^{n} G_i.$$

Bu kitapta sık sık karşılaşacağız,

$$\pi_i((g_i)_i) = g_i$$

formülüyle tanımlanmış

$$\pi_i : \prod_I G_i \longrightarrow G_i$$

fonksiyonlarına ***doğal izdüşüm fonksiyonları*** adı verilir. Bu fonksiyonlar elbette örtendir ve kolayca kontrol edilebileceği üzere,

$$\pi_i((g_i)_i(h_i)_i) = \pi_i((g_i)_i)\pi_i((h_i)_i)$$

olur.

1.10. **(Direkt Toplam, Yan Çarpım ya da Kısıtlanmış Çarpım.)** Yukarıda, bir $(G_i)_{i\in I}$ grup ailesi için $\prod_I G_i$ kümesini bir fonksiyon kümesi olarak tanımladık: $(G_i)_{i\in I}$ kümesinin bir g elemanı I'dan $\bigcup_{i\in I} G_i$ kümesine giden ve her $i \in I$ için $g_i = g(i) \in G_i$ özelliğini sağlayan bir fonksiyondu.

$$\operatorname{Supp} g = \{i \in I : \text{ her } i \in I \text{ için } g_i \neq e_i\}$$

olsun. (Küme parantezi içindeki e_i, G_i grubunun etkisiz elemanıdır.) $\operatorname{Supp} g$ kümesine g'nin ***kaidesi*** adı verilir. Şimdi şu kümeye bakalım:

$$\bigoplus_{i\in I} G_i = \left\{ f \in \prod_I G_i : \operatorname{Supp} f \text{ sonlu} \right\}.$$

Bu kümenin çarpma altında kapalı olduğunu, $\prod_I G_i$ grubunun etkisiz elemanını içerdiğini ve içerdiği her elemanın tersini de içerdiğini kanıtlamak zor değil. Dolayısıyla $\bigoplus_{i\in I} G_i$ kümesi $\prod_I G_i$ grubunda tanımlanan işlemle birlikte bir grup olur. Bu gruba ***kısıtlanmış çarpım***, ***yan çarpım*** ya da ***direkt toplam*** adı verilir. Biz, birinci ya da sonuncu terimi tercih edeceğiz. Direkt toplam bazen $\coprod_{i\in I} G_i$ olarak yazılır.
Eğer I sonluysa, $\bigoplus_{i\in I} G_i$ ile $\prod_{i\in I} G_i$ arasında bir fark yoktur. Eğer $I = \{1, 2, \ldots, n\}$ ise $\bigoplus_I G_i$ yerine

$$G_1 \oplus \ldots \oplus G_n$$

yazılımı da kullanılır.

1.11. Eğer bir önceki örnekte her $i \in I$ için $G_i = G$ alırsak, o zaman direkt toplam $\oplus_I G$ ya da $\coprod_I G$ ya da $G^{(I)}$ olarak gösterilir. Biz daha sade olduğundan sonuncu yazılımı tercih edeceğiz.

1.12. Her grup matematiksel bir yapı örneğidir. Bu kitaplarda ileride çok daha başka matematiksel yapı örnekleri göreceğiz. M herhangi bir matematiksel yapı olsun. M bir çizge, bir topolojik uzay, bir metrik uzay, bir grup, bir halka, bir cisim, bir modül, bir vektör uzayı, bir cebir ya da yazarın ya da okurun adını duymadığı, varlığını bilmediği matematiksel bir yapı olabilir. Her matematiksel yapının otomorfileri bir biçimde tanımlanır. Otomorfisi tanımlanmamış matematiksel yapı nerdeyse düşünülemez. Otomorfiler, M'den M'ye giden ve bazı özellikleri olan fonksiyonlardır. Otomorfi kavramı yapıya göre değişir ama otomorfi kavramı istisnasız her zaman, otomorfiler kümesi $\operatorname{Aut} M$ bileşke altında grup olacak biçimde tanımlanır. Dolayısıyla otomorfiler her zaman eşleşmedirler ve

a. İki otomorfinin bileşkesi otomorfi,
b. Özdeşlik fonksiyonu Id_M otomorfi,
c. Bir otomorfinin tersi de otomorfi

olacak biçimde tanımlanırlar.

1.13. Analizden biraz grup örneği verelim. $\mathbb{R}$'den $\mathbb{R}$'ye giden fonksiyonlar (toplama altında) bir grup oluştururlar. $\mathbb{R}$'den $\mathbb{R}$'ye giden sürekli fonksiyonlar (gene toplama altında) bir grup oluştururlar. $\mathbb{R}$'den $\mathbb{R}$'ye giden türevlenebilir ya da integrallenebilir fonksiyonlar bir grup oluştururlar. Aşağıdaki fonksiyon kümeleri de toplama işlemi altında bir grup oluştururlar:

$$\{f:\mathbb{R}\longrightarrow\mathbb{R} : \lim_{x\to 5} f(x)=0\},\quad \{f:\mathbb{R}\longrightarrow\mathbb{R} : \lim_{x\to 3^-} f(x)=0\},$$
$$\{f:\mathbb{R}\longrightarrow\mathbb{R} : \lim_{x\to \infty} f(x)=0\},\quad \{f:\mathbb{R}\longrightarrow\mathbb{R} : f'(5)=0\},$$
$$\{f:\mathbb{R}\longrightarrow\mathbb{R} : \textstyle\int_0^1 f(x)\,dx=0\},\quad \{f:\mathbb{R}\longrightarrow\mathbb{R} : \textstyle\int_0^1 f(x)\,dx\in\mathbb{Z}\}.$$

1.14. Biraz da geometriden grup örneği verelim. Bir $(a,b)\in\mathbb{R}^2$ elemanı için

$$(x,y)\mapsto(x+a,y+b)$$

kuralıyla tanımlanmış $\mathbb{R}^2$'nin dönüşümlerine bakalım. (Bunlara ***öteleme*** adı verilir.) Bu dönüşümü $\tau_{(a,b)}$ olarak gösterelim.

$$T=\{\tau_{(a,b)} : (a,b)\in\mathbb{R}^2\}$$

olsun. T, bileşke işlemi altında bir gruptur. Nitekim,

$$\tau_{(a,b)}\circ\tau_{(c,d)}=\tau_{(a+c,b+d)} \tag{1}$$

olur, $\tau_{(0,0)}$ etkisiz elemandır ve

$$\tau_{(a,b)}^{-1}=\tau_{(-a,-b)}$$

olur. (1)'den dolayı bu grupla $\mathbb{R}^2$ grubu arasında pek bir fark yoktur.
Bir $r\in\mathbb{R}^*$ elemanı için $\mathbb{R}^2$'nin

$$(a,b)\mapsto(ra,rb)$$

kuralıyla tanımlanmış μ_r dönüşümlerine bakalım. Bu tür dönüşümlerin kümesi M olsun. (Bu tür dönüşümlere ***homoteti*** denir.) M, fonksiyonların bileşkesi altında bir gruptur. Nitekim,

$$\mu_r\circ\mu_s=\mu_{rs} \tag{2}$$

olur, μ_1 etkisiz elemandır ve

$$\mu_r^{-1}=\mu_{r^{-1}}$$

olur. (2)'den dolayı bu grupla $\mathbb{R}^*$ grubu arasında pek bir fark yoktur.
Bir α açısı için, $\mathbb{R}^2$ düzlemini $O(0,0)$ noktası etrafında α derece döndürelim. Bu döndürüyü ρ_α olarak gösterelim. Bu tür dönüşümlerin kümesi R olsun. R, fonksiyonların bileşkesi altında bir gruptur. Nitekim,

$$\rho_\alpha\circ\rho_\beta=\rho_{\alpha+\beta} \tag{3}$$

olur, ρ_0 etkisiz elemandır ve

$$\rho_\alpha^{-1} = \rho_{-\alpha} = \rho_{2\pi-\alpha}$$

olur. Bu arada $\rho_{2\pi} = \rho_0 = \mathrm{Id}$ eşitliğini farkedelim.

1.15. Daha sonra matematiksel olarak tanımlayacağımız ama okurun lise yıllarından bilmesi gereken "modülo n" sayılar kümesi toplama altında bir grup oluşturur.

Bundan böyle, $(\mathbb{Z}, +)$ ve $(\mathrm{Sym}\, X, \circ)$ örneklerinde olduğu gibi somut bir gruptan sözedilmiyorsa, sözkonusu olan rastgele bir grupsa, dolayısıyla $\star$ işlemi belirtilmemişse, $\star$ yerine $\cdot$ ve $x \star y$ yerine $x \cdot y$, hatta hiç noktasız xy yazacağız. Ayrıca e yerine 1 yazacağız. Tabii bu 1, 1 doğal sayısı olmayabilir. Bu yazıda kanıtladığımız

$$y = x^{-1} \Leftrightarrow x \star y = e \Leftrightarrow y \star x = e$$

eşdeğerlikleri bir defa daha bu dilde yazalım, önemliler çünkü:

$$y = x^{-1} \Leftrightarrow xy = 1 \Leftrightarrow yx = 1.$$

Bundan böyle bütün kitap boyunca, aksi söylenmedikçe G bir grup olacak.

Alıştırmalar

1.16. $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ olsun. $\mathbb{Q}[\sqrt{2}]$ kümesinin toplama işlemi altında, $\mathbb{Q}[\sqrt{2}]\setminus\{0\}$ kümesinin çarpma işlemi altında birer grup olduğunu gösterin. (İkincisi birincisi kadar kolay olmayabilir.)

1.17. G bir grup, X bir küme olsun. $f : G \longrightarrow X$ herhangi bir eşleme olsun. $x, y \in X$ için $x \star y = f(f^{-1}(x)f^{-1}(y))$ tanımını yapalım. $(X, \star)$ ikilisinin bir grup olduğunu kanıtlayın. Her $a, b \in G$ için $f(ab) = f(a) \star f(b)$ eşitliği kanıtlayın.

1.18. G ve H iki grup olsun. $f : G \longrightarrow H$ fonksiyonu her $x, y \in G$ için $f(xy) = f(x)f(y)$ eşitliğini sağlasın. $f(e_G) = e_H$ eşitliğini ve her $x \in G$ için $f(x^{-1}) = f(x)^{-1}$ eşitliğini kanıtlayın. (Buradaki e_G ve e_H, sırasıyla G ve H gruplarının etkisiz elemanlarıdır.)

1.19. G ve H iki grup olsun. $f : G \longrightarrow H$ fonksiyonu her $x, y \in G$ için $f(xy) = f(x)f(y)$ eşitliğini sağlasın. Ayrıca f birebir ve örten olsun. $f^{-1} : H \longrightarrow G$ fonksiyonunun her $u, v \in H$ için $f^{-1}(uv) = f^{-1}(u)f^{-1}(v)$ eşitliğini sağladığını kanıtlayın.

1.20. G sonlu bir abel grubu olsun. G'nin derecesi 2 olmayan elemanlarının çarpımının 1 olduğunu gösterin. G'nin elemanlarının karelerinin çarpımının 1 olduğunu gösterin.

1.21. $c \in G$ olsun. Eğer $x \in G$ için $xc = cx$ eşitliği doğruysa x'in c'yi ***merkezlediği*** ya da c ile x'in ***birbiriyle değiştiği*** söylenir.

$$C_G(c) = \{x \in G : xc = cx\}$$

olsun. Şunları kanıtlayın:

a. G'nin etkisiz elemanı $C_G(c)$'dedir.

b. Eğer $x, y \in C_G(c)$ ise $xy \in C_G(c)$ olur.

c. Eğer $x \in C_G(c)$ ise $x^{-1} \in C_G(c)$ olur.

$C_G(c)$ kümesine c'nin (G'de) ***merkezleyicisi*** adı verilir.

1.22. $C \subseteq G$ olsun. Eğer $x \in G$ elemanı her $c \in C$ için $xc = cx$ eşitliğini sağlıyorsa x'in C'yi ***merkezlediği*** ya da x ile C'nin elemanlarının ***birbiriyle değiştiği*** söylenir.

$$C_G(C) = \{x \in G : \text{ her } c \in C \text{ için } xc = cx\}$$

olsun.

$$C_G(C) = \bigcap_{c \in C} C_G(c)$$

eşitliğine dikkat edelim. Şunları kanıtlayın:
a. G'nin etkisiz elemanı $C_G(C)$'dedir.
b. Eğer x, $y \in C_G(C)$ ise $xy \in C_G(C)$ olur.
c. Eğer $x \in C_G(c)$ ise $x^{-1} \in C_G(c)$ olur.
d. $C \subseteq C_G(C_G(C))$.
e. $C \subseteq D$ ise $C_G(D) \subseteq C_G(C)$.
f. $C_G(C_G(C_G(C))) = C_G(C)$.
$C_G(C)$ kümesine C'nin (G'de) ***merkezleyicisi*** adı verilir.

1.23. Her a, $b \in G$ için

$$[a,b] = a^{-1}b^{-1}ab \text{ ve } a^b = b^{-1}ab$$

tanımlarını yapalım. Her a, b, $c \in G$ için,

$$\begin{aligned}(ab)^c &= a^c b^c,\\ [a,b]^c &= [a^c, b^c],\\ (a^b)^c &= a^{bc}\end{aligned}$$

(bunlar çok bilinen temel eşitliklerdir) ve daha az bilinen ama önemli

$$\begin{aligned}[a,b]^{-1} &= [b,a],\\ [a,b^{-1}] &= [b,a]^{b^{-1}},\\ [a^{-1},b] &= [b,a]^{a^{-1}},\\ [a,bc] &= [a,c][a,b]^c,\\ [ab,c] &= [a,c]^b[b,c]\end{aligned}$$

eşitliklerini kanıtlayın. $[a,b]$ türünden yazılan elemanlara ***komütatör*** adı verilir. $[a,b] = 1$ ve $ab = ba$ eşdeğer eşitliklerdir. Eğer $a^b = c$ ise a ve b elemanlarının ***eşlenik*** oldukları söylenir. Philip Hall eşitliği olarak adlandırılması gereken

$$[[a,b^{-1}],c]^b[[b,c^{-1}],a]^c[[c,a^{-1}],b]^a = 1$$

eşitliğini kanıtlayın. Her n doğal sayısı için,

$$(ab)^n = a^n b^n [b,a^{n-1}]^{b^{n-1}}[b,a^{n-2}]^{b^{n-2}} \cdots [b,a]^b$$

eşitliğini kanıtlayın.

1.24. Her x, $y \in G$ ve her n doğal sayısı için

$$[x,y^n] = [x,y][x,y]^y \cdots [x,y]^{y^{n-1}}$$

olduğunu kanıtlayın. İpucu: (1) ve tümevarım. Ayrıca ($n = 0$ için) "hiç tane" komütatörün çarpımı tanım gereği 1'dir.

1.25. Her x, $y \in G$ ve her n doğal sayısı için $[x^m, y^n]$ elemanının $[x,y]^{x^i y^j}$ türünden elemanların çarpımı olduğunu kanıtlayın.

1.26. $a \in G$ için $a^G = \{a^g : g \in G\}$ olsun. a^G kümesine a'nın ***eşleniklik sınıfı*** adı verilir. Her a, $b \in G$ için ya $a^G = b^G$ ya da $a^G \cap b^G = \emptyset$ olduğunu kanıtlayın. Bir başka deyişle

$$a \equiv b \Leftrightarrow \text{ bir } g \in G \text{ için } a = b^g$$

olarak tanımlananan $\equiv$ ilişkisinin bir denklik ilişkisi olduğunu kanıtlayın.

1.27. $a \in G$ için $\lambda_a : G \longrightarrow G$ fonksiyonu her $x \in G$ için $\lambda_a(x) = ax$ formülüyle tanımlanmış olsun. λ_a fonksiyonunun birebir ve örten olduğunu, yani $\lambda_a \in \operatorname{Sym} G$ olduğunu kanıtlayın. $\lambda_a \circ \lambda_b = \lambda_{ab}$, $\lambda_1 = \mathrm{Id}_G$ (buradaki 1, grubun etkisiz elemanıdır) ve $\lambda_a^{-1} = \lambda_{a^{-1}}$ eşitliklerini kanıtlayın. $a \mapsto \lambda_a$ kuralıyla tanımlanmış $\lambda : G \longrightarrow \operatorname{Sym} G$ fonksiyonunun birebir olduğunu kanıtlayın.

1.28. $a \in G$ için $\rho_a : G \longrightarrow G$ fonksiyonu her $x \in G$ için $\rho_a(x) = xa^{-1}$ formülüyle tanımlanmış olsun. ρ_a'nın birebir ve örten olduğunu, yani $\rho_a \in \operatorname{Sym} G$ olduğunu kanıtlayın. $\rho_a \circ \rho_b = \rho_{ab}$, $\rho_1 = \mathrm{Id}_G$ (buradaki 1, grubun etkisiz elemanıdır) ve $\rho_a^{-1} = \rho_{a^{-1}}$ eşitliklerini kanıtlayın. $a \mapsto \rho_a$ kuralıyla tanımlanmış $\rho : G \longrightarrow \operatorname{Sym} G$ fonksiyonunun birebir olduğunu kanıtlayın.

1.29. G bir grup ve $\lambda : G \longrightarrow \operatorname{Sym} G$ ve $\rho : G \longrightarrow \operatorname{Sym} G$ yukardaki alıştırmalarda verilen fonksiyonlar olsun. Her $a, b \in G$ için $\rho_a \circ \lambda_b = \lambda_b \circ \rho_a$ olduğunu kanıtlayın. $\rho(G)$, ρ fonksiyonunun $\operatorname{Sym} G$'deki imgesi olsun, yani

$$\rho(G) = \{\rho_g : g \in G\}$$

olsun.

$$\rho(G) = \{f \in \operatorname{Sym} G : \text{ her } a \in G \text{ için } f \circ \lambda_a = \lambda_a \circ f\}$$

eşitliğini kanıtlayın. Aynı şeyi ρ ve λ'nın yerlerini değiştirerek yapın.

1.30. G bir grup olsun. $a \in G$ için $\phi_a : G \longrightarrow G$ fonksiyonu her $x \in G$ için $\phi_a(x) = axa^{-1}$ formülüyle tanımlanmış olsun.

a. $\phi_a \in \operatorname{Sym} G$ olduğunu gösterin.

b. Her $x, y \in G$ için $\phi_a(xy) = \phi_a(x) \circ \phi_a(y)$ eşitliğini kanıtlayın.

c. $\phi_a \circ \phi_b = \phi_{ab}$, $\phi_1 = \mathrm{Id}_G$ ve $\phi_a^{-1} = \phi_{a^{-1}}$ eşitliklerini kanıtlayın.

1.31. $X \subseteq G$ ve $a \in G$ olsun. Yukardaki alıştırmalardan yararlanarak aX, Xa ve $a^{-1}Xa$ kümelerinin eleman sayılarının (X sonsuzsa kardinalitelerinin) eşit olduğunu kanıtlayın.

1.32. $\emptyset \neq A \subseteq G$ olsun. Eğer $AA^{-1} \subseteq A$ ise, A'nın G grubunun işlemi altında kapalı olduğunu ve A'nın bu işlemle birlikte bir grup olduğunu kanıtlayın. (AA^{-1} kümesi, $a, b \in A$ için ab^{-1} olarak yazılan elemanlardan oluşan kümedir.)

1.33. $A \subseteq G$ olsun. Eğer her $x \in G$ için $x^{-1}Ax \subseteq A$ ise her $x \in G$ için $x^{-1}Ax = A$ eşitliğini kanıtlayın.

1.34. Eğer her $x \in G$ için $x^2 = 1$ ise her $x, y \in G$ için $xy = yx$ eşitliğini kanıtlayın. (Öte yandan her $x \in G$ için $x^3 = 1$ eşitliğini sağlayan ama değişmeli olmayan gruplar vardır. En küçüğünün 27 elemanı vardır.)

2. $\mathbb{Z}$ Grubu ve Tamsayılar

Tamsayılar kümesi $\mathbb{Z}$, toplama işlemiyle birlikte, bir önceki bölümde gördüğümüz üzere bir gruptur. Gruplar arasında herhalde okurun en âşina olduğu gruptur. Oldukça basit bir gruptur ama yapacağımız her şeyin temelidir. Bu yazıda $\mathbb{Z}$ grubunu inceleyeceğiz. Ama sadece toplamayla değil, çarpmayla da ilgileneceğiz. Tam sayılarda toplamayla çarpma arasında oldukça yakın bir ilişki olduğundan, bu pek zor olmayacak.

2.1 $\mathbb{Z}$'nin Altgrupları

Bir n tamsayısı için

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

olarak tanımlanan $n\mathbb{Z}$ kümesi de toplama altında bir gruptur. Nitekim grup olmanın tüm özelliklerini sağlar. Bu yüzden $n\mathbb{Z}$ grubuna $\mathbb{Z}$'nin ***altgrubu*** adı verilir. Daha genel tanım şöyle: Eğer $\mathbb{Z}$'nin bir A altkümesi toplama işlemiyle birlikte bir grup oluyorsa, o zaman A'ya $\mathbb{Z}$'nin ***altgrubu*** adı verilir ve bu durumda $A \leq \mathbb{Z}$ yazılır. Eğer A altgrubu $\mathbb{Z}$'den farklıysa, A'ya $\mathbb{Z}$'nin ***öz altgrubu*** adı verilir.

Aşağıdaki teorem bu yazının ana teoremidir. Kanıtının özünde şu basit olgu yatar: Eğer $n > 0$ ise, n sayısı, $n\mathbb{Z}$ kümesinin en küçük pozitif doğal sayısıdır, yani $n = \min(\mathbb{N} \cap n\mathbb{Z} \setminus \{0\})$ olur.

Teorem 2.1. *$\mathbb{Z}$'nin her altgrubu, bir ve bir tek $n \in \mathbb{N}$ için $n\mathbb{Z}$ biçimindedir.*

Kanıt: $A \leq \mathbb{Z}$ olsun.

A'nın etkisiz elemanına bu paragraflık x adını verelim. Tabii ki $x + x = x$ eşitliği sağlanır. Demek ki $x = 0$ olur. Böylece 0 sayısının A'da olduğunu kanıtladık. Demek ki A'nın etkisiz elemanı 0 imiş.

Eğer $x \in A$ ise, x'in A'da bir tersi vardır, diyelim $y \in A$. Bir önceki paragrafa göre $x + y = 0$ olur. Demek ki $-x = y \in A$. Böylece A'nın her elemanının eksilisinin de A'da olduğunu, yani $-A \subseteq A$ içindeliğini kanıtlamış olduk.

Eğer $A = \{0\}$ ise, $n = 0$ alalım; teorem sağlanır. Bundan böyle A'nın 0 sayısından ibaret olmadığını varsayalım. Eğer $0 \neq x \in A$ ise, bir önceki paragrafa göre $-x$ de A'da olduğundan, A'da en azından pozitif bir doğal sayının olduğunu görürüz. Yani $\mathbb{N} \cap A \setminus \{0\} \neq \emptyset$ olur.

$$n = \min(\mathbb{N} \cap A \setminus \{0\})$$

olsun. $n\mathbb{Z} = A$ eşitliğini kanıtlayacağız.

Önce $n\mathbb{Z} \subseteq A$ içindeliğini kanıtlayalım. Eğer $nk \in A$ ise, n sayısı da A'nın bir elemanı olduğundan,

$$n(k+1) = nk + n \in A$$

olur. Ayrıca $n0 = 0 \in A$. Bu iki olgudan, tümevarımla $n\mathbb{N} \subseteq A$ çıkar. Şimdi istediğimize içindeliği kanıtlayabiliriz:

$$n\mathbb{Z} = n(\mathbb{N} \cup -\mathbb{N}) = n\mathbb{N} \cup n(-\mathbb{N}) = n\mathbb{N} \cup -(n\mathbb{N}) \subseteq A \cup -A = A.$$

Şimdi $A \subseteq n\mathbb{Z}$ içindeliğini kanıtlayalım. Önce $A \cap \mathbb{N}$ kümesinden rastgele bir m elemanı alalım. Tümevarımla m'nin $n\mathbb{Z}$ kümesinde olduğunu kanıtlayacağız. $A \cap \mathbb{N}$ kümesinin m'den küçük sayılarının $n\mathbb{Z}$ kümesinde olduklarını varsayalım. Eğer $m < n$ ise, n sayısının seçiminden dolayı $m = 0 \in n\mathbb{Z}$ olmak zorundadır. Eğer $m \geq n$ ise, $0 \leq m - n \in A$ olur. $m - n < m$ olduğundan, tümevarım varsayımına göre $m - n \in n\mathbb{Z}$ olur. Buradan da $m \in n\mathbb{Z}$ çıkar.

Eğer $m \in A$ negatif bir sayıysa, o zaman $-m \in A \cap \mathbb{N}$ olur ve bir önceki paragrafa göre $-m \in n\mathbb{Z}$ olur. Buradan $m \in n\mathbb{Z}$ bulunur. □

Benzer bir sınıflandırmayı, Örnek 5.23'de $\mathbb{Z} \times \mathbb{Z}$ için yapacağız.

2.2 $\mathbb{Z}$'de Bölünebilirlik

$n\mathbb{Z}$ altgruplarının bazı basit ama önemli özellikleri vardır. Bu özellikleri sıralayalım. Ama önce bir tanım. $a, b \in \mathbb{Z}$ olsun. Eğer bir $k \in \mathbb{Z}$ için $a = bk$ eşitliği sağlanıyorsa, b'nin a'yı ***böldüğü*** söylenir ve bu $b|a$ olarak gösterilir. Tanıma göre ± 1 her sayıyı böler ve 0 sayısı, 0 dahil, her sayıya bölünür. Ama 0 sadece 0'ı böler, nitekim $a = 0k$ eşitliğinin ancak $a = 0$ ise bir çözümü vardır ve bu durumda her k bir çözümdür. Eğer $b|a$ ve $b \neq 0$ ise tanımdaki k sayısı biriciktir; bu durumda k'ya "a bölü b" adı verilir ve $k = a/b$ olarak yazılır. Eğer $b = a = 0$ ise her k sayısı $a = bk$ eşitliğini sağladığından bu durumda "0 bölü 0" diye bir sayıdan sözedilmez, yani "0 bölü 0" tanımlanmamıştır.

Eğer $d \neq 0$ sayısı $a - b$'yi bölüyorsa, bu olgu $a \equiv b \bmod d$ yazısıyla gösterilir. Bunu "a, modülo d, b sayısına denk" olarak okuruz.

Bölme hakkında en basit olguları okurun bildiğini varsayacağız.

Önsav 2.2. *Her $n, m \in \mathbb{Z}$ için şu önermeler doğrudur:*

i. *$n\mathbb{Z} \subseteq m\mathbb{Z}$ içindeliği ancak ve ancak $n \in m\mathbb{Z}$ ise, yani ancak ve ancak $m|n$ ise doğrudur.*

ii. *$n\mathbb{Z} = m\mathbb{Z}$ eşitliği ancak ve ancak $n = \pm m$ ise doğrudur. Demek ki $n\mathbb{Z}$'nin bir özaltgrup olmasıyla $n \neq \pm 1$ eşdeğer koşullardır.*

iii. *$n\mathbb{Z}$ altgrubunun maksimal bir özaltgrup olması için $n \neq \pm 1$ ve n'nin ± 1 ve $\pm n$'den başka bir tamsayıya bölünmemesi gerek ve yeter koşuldur.*

Kanıt: (i) okura bırakılmıştır. (ii), (i)'den hemen çıkar. (iii) de (i) ve (ii)'den çıkar. □

2.3 $\mathbb{Z}$'de Asallık, İndirgenemezlik vs.

Önsavın iii'üncü maddesindeki gibi bir n tamsayısına ***indirgenemez*** adı verilir. 2, 3, 5 gibi sayılar indirgenemezdir. -2, -3, -5 sayıları da indirgenemezdir. 0, 1, -1, 4, 6 sayıları indirgenemez değildirler.

A ve B, $\mathbb{Z}$'nin iki altgrubu olsun. O zaman,

$$A + B = \{a + b : a \in A,\, b \in B\}$$

kümesi de bir gruptur. Nitekim, $a, a_1 \in A$ ve $b, b_1 \in B$ rastgele elemanlar olsun.

$$(a + b) + (a_1 + b_1) = (a + a_1) + (b + b_1)$$

olduğundan, $A + B$ kümesi toplama altında kapalıdır. Ayrıca, $0 \in A \cap B$ olduğundan, $0 = 0 + 0 \in A + B$ olur. Son olarak, $-(a + b) = (-a) + (-b) \in A + B$ olur. Demek ki $A + B$ kümesi gerçekten toplama işlemiyle birlikte bir grupmuş, yani $\mathbb{Z}$'nin bir altgrubuymuş. Bu söylediklerimizden ve Teorem 2.1'den şu önemli sonuç çıkar:

Teorem 2.3. *Her $n, m \in \mathbb{Z}$ için öyle bir ve bir tane $d \in \mathbb{N}$ vardır ki $n\mathbb{Z}+m\mathbb{Z} = d\mathbb{Z}$ olur.* □

Yazımızın bundan sonraki bölümü grup teoriden ziyade basit aritmetikle ve çarpmayla ilgili olacak. Okur muhtemelen ve umarız kanıtlayacaklarımızın özünü biliyordur. Yöntemin ve tanımların ilgi çekeceğini umuyoruz.

Teorem 2.3'teki d sayısına n ve m'nin ***en büyük ortak böleni*** adı verilir. Nitekim gerçekten öyledir, adına layıktır yani: $n = n\cdot 1+m\cdot 0 \in n\mathbb{Z}+m\mathbb{Z} = d\mathbb{Z}$ olduğundan, n sayısı d'ye bölünür. Benzer şekilde m sayısı da d'ye bölünür. Demek ki d sayısı hem n'yi hem de m'yi bölüyor. Ayrıca, eğer e doğal sayısı hem n'yi hem de m'yi bölüyorsa, o zaman e sayısı $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ kümesinin tüm elemanlarını ve özellikle de d'yi böler. Yani n ve m sayılarının ortak bölenleri aynen d sayısının bölenleridir.

Verilmiş $n, m \in \mathbb{Z}$ için teoremde varlığı ve biricikliği kanıtlanan d sayısı $d = \text{ebob}(n, m)$ olarak yazılır. Bazıları ebob yerine Türkçe ses uyumuna daha uyduğu için obeb'i tercih eder.

Aşağıdaki sonuç ebob'un tanımının doğrudan bir sonucu.

Sonuç 2.4 (Bézout Teoremi)**.** *Her $n, m \in \mathbb{Z}$ için öyle $u, v \in \mathbb{N}$ vardır ki $nu + mv = \text{ebob}(n, m)$ olur.* □

Eğer $\text{ebob}(n, m) = 1$ ise n, m tamsayılarının ***aralarında asal*** olduğu söylenir. Örneğin 6 ve 35 aralarında asal sayılardır. Bazen de n, m'ye ***asal*** deriz.

Teorem 2.5. *n ve m tamsayılarının aralarında asal olması için yeter ve gerek koşul $nu + mv = 1$ eşitliğini sağlayan $u, v \in \mathbb{Z}$ tamsayılarının olmasıdır.*

Kanıt: Gereklilik (yani soldan sağa) tanımdan hemen anlaşılıyor. Tersine $nu + mv = 1$ eşitliğini sağlayan $u, v \in \mathbb{Z}$ tamsayıların olduğunu varsayalım. O zaman $\text{ebob}(n, m)$ sayısı hem n'yi hem de m'yi böldüğünden, 1'i de bölmek zorundadır. Demek ki $\text{ebob}(n, m) = 1$. □

Ama yukarıdaki teoremde 1 yerine d alamayız; örneğin $3 \cdot 4 + 2 \cdot (-5) = 2$ olur ama $\text{ebob}(3, 2) = 2$ olmaz.

Eğer ± 1'den farklı bir $p \in \mathbb{Z}$ tamsayısı, her $n, m \in \mathbb{Z}$ için, nm'yi böldüğünde, ya n'yi ya da m'yi bölmek zorunda kalıyorsa, o zaman p'ye ***asal sayı*** adı verilir. Elbette eğer p bir asal sayıysa ve $n_1 n_2 \cdots n_k$ çarpımını bölüyorsa, o zaman (k üzerine tümevarımla) p sayısı $n_1, \ldots, n_k$ sayılarından birini böler.

Şimdi indirgenemezlikle asallık arasında bir ayrım olmadığını göreceğiz.

Teorem 2.6. *Bir tamsayının asal olması için yeter ve gerek koşul indirgenemez olmasıdır.*

Kanıt: Önce p'nin asal olduğunu varsayalım. d doğal sayısı p'yi bölsün.

$$d = \pm 1, \pm p$$

eşitliklerinden birinin doğru olduğunu kanıtlayacağız. Demek ki bir $e \in \mathbb{Z}$ için $p = de$ olur. O zaman p sayısı de'yi böler. Bundan da, p asal olduğundan, p'nin ya d'yi ya da e'yi böldüğü çıkar. Önce $p|d$ varsayımını yapalım. O zaman bir f tamsayısı için $d = pf$ olur. Buradan da

$$p = de = (pf)e = p(fe)$$

ve dolayısıyla $fe = 1$, $e = \pm 1$ ve $p = de = \pm d$ ve $d = \pm p$ çıkar. Şimdi $p|e$ varsayımını yapalım. O zaman bir f tamsayısı için $e = pf$ olur. Buradan da

$$p = de = d(pf) = p(df)$$

ve dolayısıyla $df = 1$, $d = \pm 1$ çıkar.

Şimdi de p'nin bir indirgenemez olduğunu varsayalım. $n, m \in \mathbb{Z}$ için $p = nm$ olsun. p'nin ya n'yi ya da m'yi böldüğünü kanıtlamalıyız. Diyelim p sayısı n'yi bölmüyor. O zaman p'nin m'yi böldüğünü kanıtlamalıyız. p bir asal olduğundan, hem p'yi hem de n'yi sadece ± 1 ve $\pm p$ sayıları böler. Ama $\pm p$, n'yi (varsayımımızdan dolayı) bölmediğinden, p ve n'nin ortak bölenleri sadece ± 1 sayılarıdır, yani p ve n aralarında asaldır. Bézout teoremine göre $nu + pv = 1$ eşitliğini sağlayan u ve v sayıları vardır. Bu eşitliği m ile çarpalım: $nmu + pvm = m$ elde ederiz. Ama $nm = p$. Demek ki $pu + pvm = m$. Bu eşitliğin sağ tarafını p böler. Demek ki sol tarafını da böler. Yani p, m'yi böler. □

Alıştırmalar

2.1. obeb$(n, m) = d$ ise, $n\mathbb{Z}$ ve $m\mathbb{Z}$'in içeren en küçük altgrubun $d\mathbb{Z}$ olduğunu kanıtlayın.

2.2. $n_1, \ldots, n_k \in \mathbb{Z}$ olsun. d, bu sayıların en büyük böleni olsun.

$$n_1 u_1 + \cdots + n_k u_k = d$$

eşitliğini sağlayan $u_1, \ldots, u_k \in \mathbb{Z}$ sayılarının varlığını kanıtlayın.

2.3. $n_1, \ldots, n_k \in \mathbb{Z}$ sayılarının ortak böleni olmaması için

$$n_1 u_1 + \cdots + n_k u_k = 1$$

eşitliğini sağlayan $u_1, \ldots, u_k \in \mathbb{Z}$ sayılarının varlığının gerek ve yeter koşul olduğunu kanıtlayın.

2.4 Aritmetiğin Temel Teoremi

Buraya kadar gelmişken aritmetiğin temel teoremini kanıtlamamak olmaz. Önce bir iki yardımcı sonuç kanıtlayalım.

Önsav 2.7. *1'den büyük her doğal sayı bir indirgenemeze (yani bir asala) bölünür.*

Kanıt: Doğal sayımıza n diyelim. $A = \{m \in \mathbb{N} \setminus \{1\} : m|n\}$ olsun. $n \in A$ olduğundan, A boşküme değildir. A, $\mathbb{N}$'nin bir altkümesi olduğundan en küçük bir elemanı vardır. Bu elemana p diyelim. Demek ki p, n'yi bölüyor ve p, n'yi bölen en küçük 1'den büyük doğal sayı. p'yi bölen her doğal sayı n'yi de bölmek zorunda olduğundan, p bir indirgenemez olmalı. □

Sonuç 2.8. *Eğer a sayısı bc çarpımını bölüyorsa ve a ve b aralarında asalsa, a sayısı c'yi böler.*

Kanıt: Eğer $a = 0, \pm 1$ ise sorun yok, ayrıntıları okura bırakıyoruz. Bundan böyle $|a| > 1$ olsun. p, a'yı bölen pozitif bir asal sayı olsun. O zaman p, bc'yi de böler. Demek ki p ya b'yi ya da c'yi böler. Ama a ile b aralarında asal olduğundan, p, b'yi bölemez. Demek ki p, c'yi böler. Şimdi $a = pa_1$ ve

$c = pc_1$ yazalım. $a = pa_1$ sayısı $bc = bpc_1$ sayısını böldüğünden, a_1 sayısı bc_1 sayısını böler. Ve a_1 ve b sayıları (aynen a ve b gibi) aralarında asaldır. $|a_1| < |a|$ olduğundan, tümevarımla a_1'in c_1'i böldüğünü söyleyebiliriz. Demek ki $a = pa_1$ sayısı $c = pc_1$ sayısını böler. □

Teorem 2.9 (Aritmetiğin Temel Teoremi)**.** *0'dan farklı her doğal sayı sonlu sayıda pozitif asalın çarpımı olarak yazılır. Ayrıca eğer $p_1, \ldots, p_n$ ve $q_1, \ldots, q_m$ asalları için*

$$p_1 \cdots p_n = q_1 \cdots q_m$$

ise $n = m$ olur ve bir $\sigma \in \operatorname{Sym} n$ için $p_i = \pm q_{\sigma(i)}$ olur. (Yani sağda ve solda aynı sayıda asal vardır ve soldaki çarpımla sağdaki çarpım arasında, belki asalların çarpım sırası dışında, hiçbir fark yoktur.)

Kanıt: $0 \neq n \in \mathbb{Z}$ olsun. Kanıtımızda asallarla indirgenemezler arasında ayrım olmadığı olgusunu kullanacağız, ama iki ayrı kavramdan sözettiğimiz açıkça belli olsun diye "asal" ve "indirgenemez" terimlerini tanımlarına uygun biçimde kullanacağız. n'yi (asalların değil!) indirgenemezlerin çarpımı olarak yazacağız. Bunu n üzerine tümevarımla yapacağız.

Eğer $n = 1$ ise, n, hiç tane indirgenemezin çarpımıdır! Çünkü matematikte boşkümenin elemanlarının çarpımı 1 olarak tanımlanır. (Boşkümenin elemanlarının toplamı da 0 olarak tanımlanır.) Bundan böyle $n > 1$ olsun ve n'den küçük her sayının sonlu sayıda indirgenemezin çarpımı olarak yazıldığını varsayalım. Önsav 2.7'ye göre bir p indirgenemezi n'yi böler. Diyelim $n = pm$. Ama $m < n$ olduğundan, tümevarım varsayımına göre m sonlu sayıda indirgenemezin çarpımıdır. Demek ki $n = pm$ sayısı da sonlu sayıda asalın çarpımıdır.

Bunu tümevarımla kanıtlamak yerine (aslında aynı kapıya çıkan) "sonsuza iniş" yöntemiyle de kanıtlayabilirdik: Diyelim teoremin ilk önermesi yanlış, yani 0'dan farklı her doğal sayı indirgenemezlerin çarpımı olarak yazılamıyor. O zaman indirgenemezlerin çarpımı olarak yazılan en küçük pozitif doğal sayı vardır. Bu doğal sayıya n diyelim ve yukardaki paragaraftaki gibi p ve m sayılarını bulalım. $n < m$ olduğundan, m indirgenemezlerin çarpımı olarak yazılabilir; demek ki $n = pm$ sayısı da indirgenemezlerin çarpımı olarak yazılabilir.

Şimdi ikinci önermeyi kanıtlayalım. $p_1, \ldots, p_n$ ve $q_1, \ldots, q_m$ asalları için

$$p_1 \cdots p_n = q_1 \cdots q_m$$

olsun. Kanıtımızı n üzerinden tümevarımla yapacağız. Eğer $n = 0$ ise, yani sol tarafta çarpılan hiç asal yoksa, o zaman soldaki çarpım 1'e eşittir. Dolayısıyla sağdaki çarpım da 1'e eşittir. Buradan da sağda da çarpılan asal olmadığı çıkar. Demek ki $m = 0$ olur. Bundan böyle $n > 1$ olsun. p_1 asalı soldaki çarpımı böldüğü için sağdaki çarpımı da böler, demek ki sağdaki q_i asallarından birini

böler. p_1'in böldüğü bu asala q_i diyelim. Ama $q_i > 1$ bir asal, dolayısıyla bir indirgenemez olduğundan, bundan $p_1 = q_i$ çıkar. Sadeleştirmeyi yaparsak,

$$p_2 \cdots p_n = q_1 \cdots q_{i-1} q_{i+1} \cdots q_m$$

çıkar. Sol tarafta $n-1$ tane, sağ tarafta $m-1$ tane asal sayı çarpıldığından, tümevarım varsayımına göre, $n-1 = m-1$ olur ve soldaki $p_2, \ldots, p_n$ asalının her biri sağdaki $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_m$ asallarından birine eşit olur. Bu da kanıtımızı tamamlar. □

2.5 En Küçük Ortak Kat

$\mathbb{Z}$'nin iki altgrubunun kesişimi de bir altgruptur. Nitekim eğer A, $B \leq \mathbb{Z}$ ise, $0 \in A \cap B$ olur; eğer x, $y \in A \cap B$ ise, hem $x+y$, $-x \in A$ hem de $x+y$, $-x \in B$ olduğundan, $x+y$, $-x \in A \cap B$ olur.

Şimdi n, $m \in \mathbb{Z}$ olsun. Bir önceki paragrafa göre $n\mathbb{Z} \cap m\mathbb{Z} \leq \mathbb{Z}$ olur. Teorem 2.1'e göre, bir ve bir tane $e \in \mathbb{N}$ için $n\mathbb{Z} \cap m\mathbb{Z} \leq e\mathbb{Z}$ olur. Bu e sayısına n ve m sayılarının ***en küçük ortak katı*** adı verilir ve bu sayı

$$e = \text{ekok}(n, m)$$

olarak yazılır. Tanıma göre, n'ye **ve** m'ye bölünen sayılar aynen ekok(n, m)'ye bölünen sayılardır. Yani e, gerçekten de adının ifade ettiği gibi hem n'ye hem de m'ye bölünen en küçük doğal sayıdır.

Bazıları ekok yerine Türkçe ses uyumuna daha uyduğu için okek'i tercih eder.

ebob ile ekok arasında basit bir ilişki vardır:

Teorem 2.10. *Her n, $m \in \mathbb{Z}$ için $nm = \pm \text{ebob}(n, m)\,\text{ekok}(n, m)$ olur.*

Kanıt: Teoremi pozitif n ve m doğal sayıları için kanıtlamak yeterli. Bundan böyle n, $m \in \mathbb{N}$ olsun. Amacımız $nm = \text{ebob}(n, m)\,\text{ekok}(n, m)$ eşitliğini kanıtlamak.

ebob$(n, m) = d$, $n = dn_1$, $m = dm_1$ olsun. Elbette n_1 ve m_1 sayıları aralarında asaldır. Ve d sayısı elbette nm sayısını böler. $nm/d = n_1 m = nm_1 = dn_1 m_1$ sayısının ekok(n, m) sayısına eşit olduğunu kanıtlayacağız.

$nm/d = n_1 m = nm_1$ eşitliklerinden dolayı nm/d sayısı hem n'ye hem de m'ye bölünür.

Diğer yandan; diyelim k sayısı hem n'ye hem de m'ye bölünüyor. k'nın $nm/d = n_1 m = nm_1 = dn_1 m_1$ sayısına bölündüğünü kanıtlayacağız ve böylece $nm/d = \text{ekok}(n, m)$ eşitliği kanıtlanmış olacak. Bir $u \in \mathbb{Z}$ için $k = nu = dn_1 u$ yazalım. $m = dm_1$ sayısı $k = dn_1 u$ sayısını böldüğüne göre, m_1 sayısı $n_1 u$

sayısını böler. Ama m_1 ile n_1 aralarında asal olduğundan, buradan m_1'in u'yu böldüğü çıkar. Demek ki $nm/d = nm_1$ sayısı $k = nu$ sayısını böler. □

Notlar ve Örnekler

2.4. Bu örnekte $n\mathbb{Z}+a$ gibi kümelerin kesişimlerini bulacağız. Herhangi bir karışıklığa mahal vermemek için tanımı açık açık yazalım:

$$n\mathbb{Z} + a = \{nx + a : x \in \mathbb{Z}\}.$$

Örneğin $2\mathbb{Z} + 1$ tek sayılar kümesidir. $5\mathbb{Z} + 2$, 5'e bölündüğünde kalanın 2 olduğu tamsayılar kümesidir, yani

$$5\mathbb{Z} + 2 = \{\ldots, -13, -8, -3, 2, 7, 12, \ldots\}.$$

Bu arada,

$$5\mathbb{Z} + 2 = 5\mathbb{Z} + 7 = 5\mathbb{Z} + 12 = 5\mathbb{Z} - 3 = -5\mathbb{Z} + 2$$

gibi eşitliklere dikkat edelim. Genel olarak $n\mathbb{Z} + a$ kümesini betimlemede kullanılan n yerine $-n$ ve a yerine $n\mathbb{Z} + a$ kümesinden herhangi bir sayı koyabiliriz, küme değişmez; yani

$$n\mathbb{Z} + a = m\mathbb{Z} + b \Leftrightarrow m = \pm n \text{ ve } n|a - b$$

eşdeğerliği geçerlidir. Bunun kanıtını okura bırakıyoruz. Dolayısıyla n'yi her zaman ≥ 0 ve a'yı $0, 1, \ldots, n-1$ sayıları arasından seçebiliriz (a yerine, a'yı n'ye böldüğümüzde elde edilen kalanı alabiliriz).
Birkaç örnekle başlayalım:

$$(2\mathbb{Z} + 1) \cap (6\mathbb{Z} + 4) = \emptyset$$

olur çünkü $2\mathbb{Z}+1$ kümesi tek sayılardan oluşur, oysa $6\mathbb{Z}+4$ kümesinin elemanları çifttir. Şu örnek de kolay:

$$(2\mathbb{Z} + 1) \cap (6\mathbb{Z} + 1) = 6\mathbb{Z} + 1.$$

ya da

$$3\mathbb{Z} \cap (9\mathbb{Z} + 6) = 9\mathbb{Z} + 6.$$

Daha zor örnekler var. Örneğin,

$$(18\mathbb{Z} + 7) \cap (21\mathbb{Z} + 4).$$

Bu kesişimi bulmak yukarıdaki örneklerdeki kesişimleri bulmaktan daha zor. Birazdan doğruluğunu göreceğimiz yanıtı verelim:

$$(18\mathbb{Z} + 7) \cap (21\mathbb{Z} + 4) = 126\mathbb{Z} + 25.$$

Bu örnekte soracağımız soru şu: $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b)$ kesişimi ne zaman boşküme olur? Ve boşküme olmadığında hangi kümeye eşit olur?
Diyelim $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) \neq \emptyset$. Kesişimden bir s elemanı alalım. Demek ki $x, y \in \mathbb{Z}$ için

$$s = nx + a = my + b$$

olur. n, m, a, b sayılarının verildiğini ve yukarıdaki eşitliği sağlayan x ve y sayılarını bulmaya çalıştığımızı unutmayalım. Yukarıdaki eşitlikten, eğer $d = \text{ebob}(n, m)$ ise

$$b - a = nx - my \in n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$$

olur. Demek ki $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) \neq \emptyset$ ise $a \equiv b \bmod d$ olur.

Şimdi $a \equiv b \bmod d$ varsayımını yapalım. Diyelim $b - a = dw$. Bézout teoremine göre $nu + mv = d$ eşitliğini sağlayan u ve v tamsayıları vardır. Bu eşitliği w ile çarparsak, $nuw + mvw = dw = b - a$ yani,

$$nuw + a = -mvw + b$$

buluruz. Ama bu sayıya s dersek, soldaki ifadeden $s \in n\mathbb{Z} + a$ olduğu, sağdaki ifadeden $s \in m\mathbb{Z} + b$ olduğu çıkar. Demek ki $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) \neq \emptyset$. Böylece, $d = \text{ebob}(n, m)$ tanımıyla,

$$(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) \neq \emptyset \Leftrightarrow a \equiv b \bmod d$$

önermesini kanıtlamış olduk.
Şimdi $a \equiv b \bmod d$ önermesini varsayıp, boşküme olmadığını bildiğimiz $(n\mathbb{Z}+a)\cap(m\mathbb{Z}+b)$ kümesinin hangi küme olduğunu bulalım. d tabii ki hâlâ $\text{ebob}(n, m)$ sayısına eşit. w sayısı $b - a = dw$ olacak biçimde seçilsin. Şimdi,

$$(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) = (n\mathbb{Z} + a) \cap (m\mathbb{Z} + a + dw) = (n\mathbb{Z} \cap (m\mathbb{Z} + dw)) + a$$

olur. Ama d hem n'yi hem de m'yi böldüğünden, xxxx dergiden tamamla xxx MD-2013-II sayısı
xxxxxxxxxxxxxxxx

3. Simetrik Grup Sym n

Eğer X bir kümeyse, X'in eşleşmelerinden (ya da permütasyonlarından, yani X'ten X'e giden birebir ve örten fonksiyonlardan) oluşan $\operatorname{Sym} X$ kümesi bileşke işlemi altında bir gruptur. Bunu bir önceki bölümde görmüştük. ***Simetrik grup*** adı verilen bu gruplar matematikte çok önemlidir ve elbette X'in sonlu olduğu durumlar daha da önemlidir.

Eğer X ve Y arasında bir eşleme varsa, kümeler kuramı açısından X ile Y arasında fazla bir fark yoktur; dolayısıyla, fonksiyonlar da kümeler kuramının nesneleri olduğundan, bu durumda $\operatorname{Sym} X$ ile $\operatorname{Sym} Y$ arasında da fazla bir fark yoktur; birini anlamak demek diğerini de anlamak demektir[1]. Demek ki $|X| = n$ ise, $\operatorname{Sym} X$ grubunu anlamakla $\operatorname{Sym}\{1, 2, \ldots, n\}$ grubunu anlamak aynı şeydir. $\operatorname{Sym}\{1, 2, \ldots, n\}$ yerine $\operatorname{Sym} n$ bazen de S_n yazılır.

Bu yazıda $\operatorname{Sym} n$ grubuyla haşır neşir olacağız.

$\operatorname{Sym} n$ Grubunun Eleman Sayısı. n kadın ve n erkek kaç farklı biçimde (her kadına bir erkek ve her erkeğe bir kadın düşecek biçimde) eşleştirilebilir? Sorunun (kolay olan) yanıtını bulmak için kadınları numaralandıralım. Birinci kadını n erkekten birini eşleştireceğiz. İkinci kadını geri kalan $n - 1$ erkekten birini, üçüncü kadını geri kalan $n - 2$ erkekten birini eşleştireceğiz ve bunu böylece devam ettireceğiz. Anlaşılacağı gibi, toplam $n!$ farklı kadın-erkek eşlemesi vardır. Bu $n!$ sayısı, elbette, aynı zamanda, n elemanlı herhangi bir kümeden n elemanlı herhangi bir kümeye giden eşleme sayısıdır.

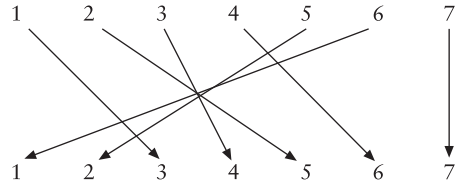
Sonuç olarak, $\operatorname{Sym} n$'nin tam $n!$ tane elemanı vardır.

3.1 $\operatorname{Sym} n$'nin Elemanlarının Yazılımı

Önce $\operatorname{Sym} n$ kümesinin elemanlarını inceleyelim, sonra modern matematik gereği, kümeye bir bütün olarak bakarız. Bir örnekle başlayalım.

$\operatorname{Sym} 7$'nin aşağıdaki permütasyonunu ele alalım.

[1] İleride iki grup arasında pek bir fark olmadığını belirtmek için, matematiksel olarak tanımlayacağımız "izomorfik" sıfatını kullanacağız.



Tanım kümesini üst sırada, değer kümesini alt sırada gösterdik. Permütasyon aslında şunu yapıyor:

$$\begin{aligned} 1 &\mapsto 3 \\ 2 &\mapsto 5 \\ 3 &\mapsto 4 \\ 4 &\mapsto 6 \\ 5 &\mapsto 2 \\ 6 &\mapsto 1 \\ 7 &\mapsto 7 \end{aligned}$$

Bu permütasyonu daha sade olarak şöyle yazabiliriz:

$$\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 3\,5\,4\,6\,2\,1\,7 \end{pmatrix}.$$

Üst sıra tanım kümesinin elemanlarını, alt sıra da değer kümesinin elemanlarını simgeler. 5'in hemen altında 2 olması, bu permütasyonun 5'teki değerinin 2 olduğunu söyler, yani,

$$f = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 3\,5\,4\,6\,2\,1\,7 \end{pmatrix}$$

ise, $f(1) = 3$, $f(2) = 5$, $f(3) = 4$, $f(4) = 6$, $f(5) = 2$, $f(6) = 1$, $f(7) = 7$ olur.

Yukardakinden daha kolay bir yazılım vardır. Örneğimizdeki permütasyona bakalım.

- Bu permütasyonu 1'i 3'e, 3'ü 4'e, 4'ü 6'ya, 6'yı da 1'e (başladığımız sayıya) göndermiş. Yani

$$1 \mapsto 3 \mapsto 4 \mapsto 6 \mapsto 1$$

diye bir ***döngü*** olmuş.

- Aynı permütasyon 2'yi 5'e ve 5'i 2'ye (başladığımız sayıya) yollamış. Demek ki bir de

$$2 \mapsto 5 \mapsto 2$$

diye bir döngü sözkonusu.

- Son olarak, bu permütasyon 7'yi 7'ye göndermiş.

Yukardaki üç nedenden dolayı bu permütasyon

$$(1\,3\,4\,6)(2\,5)(7)$$

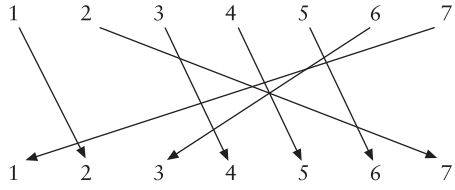
olarak gösterilir. Buradaki her sayının imgesi hemen sağındaki sayıdır, ama eğer sayı parantezin sonundaysa, o zaman o sayının imgesi bulunduğu parantezin ilk sayısıdır.

Her bir paranteze ***döngü*** adı verilir. (1 3 4 6)(2 5)(7) permütasyonunda 3 döngü vardır.

(1 3 4 6) ve (2 5) döngüleri ***ayrıktır***. Ama (1 3 4 6) ve (2 5 6) döngüleri ayrık değildirler, ortak bir elemanları (6) vardır.

Sym n'nin her elemanı, yukarıdaki yöntemle, ayrık döngülerin çarpımı olarak yazılabilir.

Örneğin Sym 7'nin (1 2 7)(3 4 5 6) permütasyonunun resmi aşağıdadır. Görüldüğü gibi, (1 2 7) döngüsü nedeniyle 1 sağındaki 2'ye, 2 sağındaki 7'ye, 7 de ta en baştaki 1'e gidiyor.



Döngüyle gösterilen permütasyonlarda her sayı hemen sağındaki sayıya gider. Sağında sayı olmayan sayılar, bulundukları döngünün (parantezin) en başına giderler. Sym 7'nin her elemanı (ki 7! = 5040 tane elemanı vardır) böyle ayrık döngüler biçiminde yazılabilir.

Yalnız dikkat edilmesi gereken bir nokta var: Bu yazılımla,

$$(1\ 2\ 7)(3\ 4\ 5\ 6) \text{ ile } (3\ 4\ 5\ 6)(1\ 2\ 7)$$

permütasyonları da birbirine eşittir. Aynı biçimde,

$$\begin{aligned}(1\ 2\ 7)(3\ 4\ 5\ 6) &= (2\ 7\ 1)(3\ 4\ 5\ 6) = (3\ 4\ 5\ 6)(2\ 7\ 1)\\ &= (4\ 5\ 6\ 3)(2\ 7\ 1) = (5\ 6\ 3\ 4)(7\ 1\ 2)\end{aligned}$$

gibi eşitlikler geçerlidir. Genel olarak (1 5 9 3 6) gibi bir döngüyü yazmaya döngüdeki herhangi bir elemandan başlayabiliriz:

$$(1\ 5\ 9\ 3\ 6) = (5\ 9\ 3\ 6\ 1) = (9\ 3\ 6\ 1\ 5) = (3\ 6\ 1\ 5\ 9) = (6\ 1\ 5\ 9\ 3).$$

Ama döngünün en küçük sayısından başlamak bir gelenektir.

Sym 4'ün 4! yani 24 elemanını bu yazılımla yazabiliriz:

(1)(2)(3)(4)
(1 2)(3)(4), (1 3)(2)(4), (1 4)(2)(3), (1)(2 3)(4), (1)(2 4)(3), (1)(2)(3 4)
(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)
(1 2 3)(4), (1 2 4)(3), (1 3 4)(2), (1)(2 3 4)
(1 3 2)(4), (1 4 2)(3), (1 4 3)(2), (1)(2 4 3)
(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)

Yazılımı biraz daha sadeleştirebiliriz. Eğer n'nin kaç olduğunu önceden biliyorsak tek elemanlı döngüleri yazmasak da olur. Örneğin (1 3 4 6)(2 5)(7) yerine daha basit olarak (1 3 4 6)(2 5) yazabiliriz. Bunun gibi (1 2 3)(4 5)(6)(7) yerine (1 2 3)(4 5) yazalım. Ama o zaman (1)(2)(3)(4)(5)(6)(7) yerine ne yazacağız? Onun yerine de Id_7 yazalım. Eğer 7 umurumuzda değilse, Id_7 yerine sadece Id yazalım. Bu daha basit yazılımla, Sym 4'ün 24 elemanı aşağıdaki gibi yazılır.

Id_4
(1 2), (1 3), (1 4), (2 3), (2 4), (3 4)
(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)
(1 2 3), (1 2 4), (1 3 4), (2 3 4)
(1 3 2), (1 4 2), (1 4 3), (2 4 3)
(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)

Bu yazılımın bir tehlikesi var. O da şu: Bu yazılımla

$$(1\ 3\ 4\ 6)(2\ 5)$$

elemanı Sym 6'nın da, Sym 7'nin de, Sym 8'in de elemanı olabilir. Hatta hatta Sym $\mathbb{N}$'nin de bir elemanı olabilir. Nasıl anlayacağız hangisinin elemanı olduğunu? Konunun gelişinden... Biraz dikkat etmek gerekir sadece o kadar.

Bu yazılımın tehlikesi yanında bir avantajı vardır: Bu yazılım sayesinde, örneğin, Sym 6'yı rahatlıkla Sym 9'un altkümesi olarak görebiliriz. Nitekim Sym 6'nın her elemanı, Sym 9'un 7, 8 ve 9'u sabitleyen bir elemanı olarak görülebilir.

Notlar ve Örnekler

3.1. İskambil kâğıtlarını 1'den 52'ye kadar numaralandıralım ve 1 en üstte, 52 en altta olmak üzere sıraya dizelim. Bu numaralar aslında kâğıtların üstten başlayarak sıraları. Desteyi tam ortadan 26'şar kâğıtlık iki küçük desteye bölelim. Destelerden birinde 1'den 26'ya kadar olan kâğıtlar (sol deste), diğerinde 27'den 52'ye kadar olan kâğıtlar (sağ deste) var. Şimdi iki desteyi o bilinen fiyakalı biçimde karalım.



Sağ destenin son kâğıdı olan 52 numara gene en alta gelsin. Sol destenin sonuncu kâğıdı olan 26 numara sondan bir önceki kâğıt olsun. Kâğıtları bu yöntemle bir sağdan bir soldan kararsak, birinci destenin ilk kâğıdı (1 yani) en üste gelir, ikinci destenin ilk

kâğıdı (27 yani) ikinci kâğıt olur. Sonra 2 numaralı kâğıt, sonra 28 numaralı kâğıt, sonra 3 numaralı kâğıt gelir ve bu böyle devam eder. Karmadan önceki destenin kâğıtları nasıl değişmiştir? 1 numaralı kâğıt gene en baştadır, gene 1 numaradır diyelim. Dolayısıyla (1) döngüsü oluşmuştur. Ama 2 numaralı kâğıt karmadan sonra 3'üncü sıraya gelmiştir, yani 3 numaralı kâğıt olmuştur. 3 numara ise 5 numara olmuştur. Genel olarak, ilk destedeki 1 ile 26 arasındaki n numaralı kâğıt yeni destede $2n-1$ numaralı kâğıt olmuşlardır. Öte yandan 27 numaralı kâğıt 2 numaralı kâğıt, 28 numaralı kâğıt 4 numaralı kâğıt olmuştur. Genel olarak ikinci destedeki 27 ile 52 arasında olan n numaralı kâğıt yeni destede $2(n-26)$ numaralı kâğıt olmuştur. Dönüşümü şöyle gösterebiliriz:

$$f(n) = \begin{cases} 2n-1 & \text{eğer } 1 \le n \le 26 \text{ ise} \\ 2(n-26) & \text{eğer } 27 \le n \le 52 \text{ ise} \end{cases}$$

Bu dönüşümü (permütasyonu) öğrendiğimiz biçimde yazarsak (tek satıra sığmayan),

(1)(2 3 5 9 17 33 14 27)(4 7 13 25 49 46 40 28)(6 11 21 41 30 8 15 29)
(10 19 37 22 43 34 16 31)(12 23 45 38 24 47 42 32)(18 35)(20 39 26 51 50 48 44 36)(52)

permütasyonunu elde ederiz.

3.2. $\operatorname{Sym}\mathbb{N}$ grubunun elemanlarını da bu yöntemle yazabiliriz, en azından formülü olan permütasyonlarını. Örneğin

$$(0\ 1)(2\ 3)(4\ 5)\dots$$

permütasyonu çift sayılara 1 ekler, tek sayılardan 1 çıkarır.

$$(0\ 1)(2\ 3\ 4)(5\ 6\ 7\ 8)\dots$$

bir başka örnek. Ama dikkat

$$(0\ 1\ 2\ 3\ \dots)$$

bir permütasyonun gösterimi değildir çünkü 0'a giden eleman yok, yani fonksiyon örten değil.

$\mathbb{Z}$'den $\mathbb{Z}$'ye giden ve $f(n) = n+1$ formülüyle tanımlanan eşleşmeyi ele alalım. Kümeler kuramı açısından $\mathbb{Z}$ ile $\mathbb{N}$ arasında bir fark yoktur, çünkü her ikisi de sayılabilir sonsuzluktadır. $\mathbb{Z}$'den $\mathbb{N}$'ye giden bir g eşlemesi bulalım. O zaman $g \circ f \circ g^{-1} \in \operatorname{Sym}\mathbb{N}$ olur. g olarak mesela,

$$g(n) = \begin{cases} 2n & \text{eğer } n \ge 0 \text{ ise} \\ -2n-1 & \text{eğer } n < 0 \text{ ise} \end{cases}$$

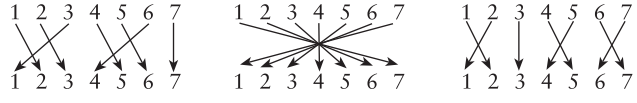
olabilir. Bu durumda kolayca kontrol edilebileceği üzere

$$g \circ f \circ g^{-1} = (\ \dots\ 5\ 3\ 1\ 0\ 2\ 4\ 6\ \dots\ )$$

olur.

Alıştırmalar

3.3. Aşağıda gösterilen permütasyonların en kısa yazılımını bulun.



3.4. f ve g aşağıda (bu sırayla) gösterilen permütasyonlar olsun. $f \circ g$ ve $g \circ f$ permütasyonlarını bulun.

$$\begin{array}{ll} 1 \mapsto 3 & 1 \mapsto 5 \\ 2 \mapsto 5 & 2 \mapsto 6 \\ 3 \mapsto 4 & 3 \mapsto 3 \\ 4 \mapsto 6 & 4 \mapsto 7 \\ 5 \mapsto 2 & 5 \mapsto 4 \\ 6 \mapsto 1 & 6 \mapsto 2 \\ 7 \mapsto 7 & 7 \mapsto 1 \end{array}$$

3.5. Aşağıda gösterilen permütasyonların en kısa yazılımını bulun.

$$\begin{array}{lll} 1 \mapsto 3 & 1 \mapsto 5 & 1 \mapsto 2 \\ 2 \mapsto 5 & 2 \mapsto 6 & 2 \mapsto 3 \\ 3 \mapsto 4 & 3 \mapsto 3 & 3 \mapsto 4 \\ 4 \mapsto 6 & 4 \mapsto 7 & 4 \mapsto 5 \\ 5 \mapsto 2 & 5 \mapsto 4 & 5 \mapsto 6 \\ 6 \mapsto 1 & 6 \mapsto 2 & 6 \mapsto 7 \\ 7 \mapsto 7 & 7 \mapsto 1 & 7 \mapsto 1 \end{array}$$

3.6. Aşağıdaki f ve g permütasyonları için $f \circ g$ permütasyonunu bulun ve bu permütasyonu en kısa gösterimiyle yazın.

$$\begin{array}{ll} f = (1\ 2\ 3)(4\ 5\ 6\ 7), & g = (1\ 4\ 3)(2\ 5\ 6\ 7) \\ f = (1\ 2\ 3)(4\ 5\ 6\ 7), & g = (1\ 3\ 2)(4\ 5\ 7\ 6) \\ f = (1\ 2\ 3)(4\ 5\ 6\ 7), & g = (1\ 3\ 2) \\ f = (1\ 2\ 3)(4\ 5\ 6\ 7), & g = (1\ 3\ 2)(4\ 7\ 6\ 5) \\ f = (1\ 2\ 3), & g = (4\ 5\ 6\ 7) \\ f = (1\ 2\ 3)(4\ 5), & g = f = (1\ 2\ 3)(4\ 5) \end{array}$$

Hangi durumlarda $f \circ g = g \circ f$ olur?

3.7. Örnek 3.1'de karmaya sağ destenin son kâğıdı en alta gelecek biçimde değil de, sol destenin en son kâğıdı en alta gelecek biçimde başlasaydık hangi permütasyonu elde ederdik?

3.2 Sym n'de Bileşke

Sym X'ten iki elemanın bileşkesinin yine Sym X'tedir elbette. Sym n gruplarında ve hatta Sym $\mathbb{N}$ grubunda, elemanların bileşkesini almanın kolay bir yöntemi vardır.

Notlar ve Örnekler

3.8. Sym 7'den iki eleman alıp bunların bileşkesini bulalım. Diyelim,

$$(1\ 2\ 3)(4\ 5) \text{ ile } (1\ 4\ 7\ 2)(3\ 6\ 5)$$

elemanlarını aldık. Bu iki elemanın

$$(1\ 2\ 3)(4\ 5) \circ (1\ 4\ 7\ 2)(3\ 6\ 5)$$

bileşkesini bulalım:

$$\begin{aligned}
1 &\mapsto 4 \mapsto 5\\
2 &\mapsto 1 \mapsto 2\\
3 &\mapsto 6 \mapsto 6\\
4 &\mapsto 7 \mapsto 7\\
5 &\mapsto 3 \mapsto 1\\
6 &\mapsto 5 \mapsto 4\\
7 &\mapsto 2 \mapsto 3
\end{aligned}$$

En soldan başlayıp okları takip edersek (yani ortadaki kademeyi resimden atarsak),

$$\begin{aligned}
1 &\mapsto 5\\
2 &\mapsto 2\\
3 &\mapsto 6\\
4 &\mapsto 7\\
5 &\mapsto 1\\
6 &\mapsto 4\\
7 &\mapsto 3
\end{aligned}$$

buluruz. Bu permütasyon da

$$(1\ 5)(3\ 6\ 4\ 7)$$

olarak yazılır. Demek ki

$$(1\ 2\ 3)(4\ 5) \circ (1\ 4\ 7\ 2)(3\ 6\ 5) = (1\ 5)(3\ 6\ 4\ 7)$$

olur. Bu eşitliği yukardaki zahmetli şekilleri çizmeden de bulabiliriz. Şöyle yaparız: Bileşkeyi bulmak için önce 1'in imgesini bulalım.

$$(1$$

yazarak hesaplara başlayalım. (1 4 7 2)(3 6 5) permütasyonu 1'i 4'e götürüyor. Bir sonraki (1 2 3)(4 5) permütasyonu da 4'ü 5'e götürüyor. Demek ki bulmak istediğimiz bileşke 1'i 5'e götürüyor. Bu yüzden 1'in yanına 5 yazalım:

$$(1\ 5$$

Şimdi 5'in bileşke altında akıbetini bulmalıyız. (1 4 7 2)(3 6 5) permütasyonu 5'i 3'e götürüyor. Bir sonraki (1 2 3)(4 5) permütasyon da 3'ü 1'e götürüyor. Demek ki bulmak istediğimiz bileşke 5'i 1'e götürüyor. Hesaplara başladığımız 1 sayısına geri döndük. Açtığımız parantezi kapatalım:

$$(1\ 5)$$

Şimdi nereye gittiğini bilmediğimiz ilk sayı olan 2'nin akıbetini öğrenelim. Yeni bir parantez açıp sağına 2 yazalım:

$$(1\ 5)(2$$

(1 4 7 2)(3 6 5) permütasyonu 2'yi 1'e götürüyor. Bir sonraki (1 2 3)(4 5) permütasyonu da 1'i 2'ye götürüyor. Demek ki bulmak istediğimiz bileşke 2'yi 2'ye götürüyor. Paranteze başladığımız 2 sayısına çabuk geri döndük. Parantezi hemen kapatalım:

$$(1\ 5)(2)$$

Akıbetini bilmediğimiz bir sonraki sayı 3. Önce

$$(1\ 5)(2)(3$$

yazalım. (1 4 7 2)(3 6 5) permütasyonu 3'ü 6'ya götürüyor. Bir sonraki (1 2 3)(4 5) permütasyon da 6'yı 6'ya götürüyor. Demek ki bulmak istediğimiz bileşke 3'ü 6'ya götürüyor. Bu yüzden 3'in yanına 5 yazalım:

$$(1\ 5)(2)(3\ 6$$

Şimdi 6'nın nereye gittiğini bulmalıyız. (1 4 7 2)(3 6 5) permütasyonu 6'yı 5'e götürüyor. Bir sonraki (1 2 3)(4 5) permütasyonu da 5'i 4'e götürüyor. Demek ki bulmak istediğimiz bileşke 6'yı 4'e götürüyor. Bu yüzden 6'nın yanına 4 yazalım:

$$(1\ 5)(2)(3\ 6\ 4$$

Bakalım 4 nereye gidiyor? Diğer tüm sayıları kullandığımız için 4'ün ya 3'e ya da 7'ye gitmesi gerektiğini biliyoruz. Bulalım: (1 4 7 2)(3 6 5) permütasyonu 4'ü 7'ye götürüyor. Bir sonraki (1 2 3)(4 5) permütasyonu da 7'yi 7'ye götürüyor. Demek ki bulmak istediğimiz bileşke 4'ü 7'ye götürüyor. Bu yüzden 4'ün yanına 7 yazalım:

$$(1\ 5)(2)(3\ 6\ 4\ 7$$

Şimdi 7'nin bileşke altında nereye gittiğini bulmalıyız. 7'nin 3'ten başka gidecek yeri kalmadı ama biz gene de yukarıdaki yöntemi uygulayalım: (1 4 7 2)(3 6 5) permütasyonu 7'yi 2'ye götürüyor. Bir sonraki (1 2 3)(4 5) permütasyonu da 2'yi 3'e götürüyor. Demek ki bulmak istediğimiz bileşke 7'yi gerçekten 3'e götürüyor. Paranteze başladığımız 3 sayısına geri döndük. Açtığımız parantezi kapatalım:

$$(1\ 5)(2)(3\ 6\ 4\ 7).$$

Kontrol edilmemiş başka sayı kalmadığından,

$$(1\ 2\ 3)(4\ 5) \circ (1\ 4\ 7\ 2)(3\ 6\ 5) = (1\ 5)(2)(3\ 6\ 4\ 7)$$

eşitliğine ulaşırız. (2) parantezini yazmadığımızdan, aynen yukardaki gibi

$$(1\ 2\ 3)(4\ 5) \circ (1\ 4\ 7\ 2)(3\ 6\ 5) = (1\ 5)(3\ 6\ 4\ 7)$$

buluruz.

3.9. Tabii ikiden fazla permütasyonun da bileşkesini alabiliriz. Örneğin,

$$(1\ 3\ 5) \circ (2\ 3\ 6) \circ (1\ 2\ 6) = (1\ 5)(2)(3\ 6).$$

Alıştırmalar

3.10. Eğer $f \in \operatorname{Sym}\mathbb{N}$ ise

$$\operatorname{Soc} f = \{n \in \mathbb{N} : f(n) \neq n\}$$

olsun. $\operatorname{Soc} f$'ye f'nin ***kaidesi*** (İngilizcesi *socle*) adı verilir.

$$\operatorname{Sym}^{<\omega}\mathbb{N} = \{f \in \operatorname{Sym}\mathbb{N} : \operatorname{Soc} f \text{ sonlu}\}$$

olsun. $\operatorname{Sym}^{<\omega}\mathbb{N}$ kümesinin bileşke altında kapalı olduğunu ve bileşke işlemiyle birlikte bir grup olduğunu gösterin.

Son olarak (1 2 3)(4 5) permütasyonunun (1 2 3) ile (4 5) permütasyonunun bileşkesi olduğuna dikkat edelim, yani

$$(1\ 2\ 3) \circ (4\ 5) = (1\ 2\ 3)(4\ 5).$$

Bu iki permütasyon birbiriyle yer değiştirir: (1 2 3)(4 5) = (4 5)(1 2 3); çünkü (1 2 3) ile (4 5) permütasyonlarının değiştirdiği elemanlar kümesi (yani bu permütasyonların kaideleri) sırasıyla $\{1, 2, 3\}$ ve $\{4, 5\}$ kümeleridir ve bu kümeler ayrık kümelerdir.

3.3 Sym n'de Elemanların Tersleri ve Dereceleri

Her permütasyonun bir tersi vardır: Eğer bir permütasyon x'i y'ye götürüyorsa, bu permütasyonun tersi y'yi x'e götürür. Örneğin $f = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8\ 9)$ permütasyonun tersi $g = (1\ 4\ 3\ 2)(5\ 9\ 8\ 7\ 6)$ permüstasyonudur. Örneğin f permütasyonu 1'i 2'ye götürdüğünden, g permütasyonu 2'yi 1'e götürür; f permütasyonu 4'ü 1'e götürdüğünden, g permütasyonu 1'i 4'e götürür. f ne yapıyorsa, g tam tersini yapar.

f'nin tersi f^{-1} olarak yazılır.

Ayrık döngüler halinde yazılmış bir permütasyonun tersini gene ayrık döngüler halinde yazmak çok kolaydır: her döngünün ilk elemanını sabitleyip geri kalan elemanları tersten sıralayarak yazmak yeter. Yukarda olduğu gibi. Bir örnek daha:

$$[(1\ 4\ 7\ 3)(2\ 5\ 8)(6\ 9)]^{-1} = (1\ 3\ 7\ 4)(2\ 8\ 5)(6\ 9).$$

Bazı elemanlar kendi kendilerinin tersidir. Örneğin, $(1\ 2)$, $(1\ 3)(2\ 5)$ gibi elemanların tersleri kendileridir.

Eğer f bir permütasyonsa (hatta bir kümeden kendisine giden herhangi bir fonksiyonsa), f'nin kendisiyle bileşkesini alabiliriz, yani $\circ f$ bileşkesini bulabiliriz. Bu bileşke f^2 olarak yazılır. (Ama f'nin değerlerinin karelerini alma fonksiyonuyla karıştırılmasın.) f'nin kendisiyle 3 defa da bileşkesini alabiliriz. Bu yeni permütasyon f^3 olarak gösterilir. Bunu böyle devam ederek f^n bileşkesini alabiliriz. $f^0 = \mathrm{Id}$ ve $f^1 = f$ anlamına gelirler. Bunlara f'nin kuvvetleri adı verilir. Birkaç örnek verelim:

Notlar ve Örnekler

3.11. $f = (1\ 2\ 3\ 4)(5\ 6\ 7)$ olsun. f'nin kuvvetlerini teker teker yazalım:

$$\begin{aligned}
f^0 &= \mathrm{Id}\\
f^1 &= (1\ 2\ 3\ 4)(5\ 6\ 7) = f\\
f^2 &= (1\ 3)(2\ 4)(5\ 7\ 6)\\
f^3 &= (1\ 4\ 3\ 2)\\
f^4 &= (5\ 6\ 7)\\
f^5 &= (1\ 2\ 3\ 4)(5\ 7\ 6)\\
f^6 &= (1\ 3)(2\ 4)\\
f^7 &= (1\ 4\ 3\ 2)(5\ 6\ 7)\\
f^8 &= (5\ 7\ 6)\\
f^9 &= (1\ 2\ 3\ 4)\\
f^{10} &= (1\ 3)(2\ 4)(5\ 6\ 7)\\
f^{11} &= (1\ 4\ 3\ 2)(5\ 7\ 6)\\
f^{12} &= \mathrm{Id}
\end{aligned}$$

Görüldüğü üzere tam 12'inci kuvvette Id buluyoruz. daha önce değil. Bu durumda f'nin ***derecesinin*** 12 olduğu söylenir. Bu listeyi devam ettirirsek, pek farklı bir şey bulmayız:

$$f^{13} = f,\ f^{14} = f^2,\ f^{15} = f^3,$$

yukarıdaki liste kendini yeniler. Örneğin,

$$f^{132} = f^{10} = (1\ 3)(2\ 4)(5\ 6\ 7)$$

olur.

3.12. Yukardaki örnekte iki döngü vardı: (1 2 3 4) döngüsü ve (5 6 7) döngüsü. Kolayca görüleceği üzere birinci döngünün derecesi 4, ikincisinin ise 3. Çarpımın derecesi ise $4 \times 3 = 12$ ama her zaman böyle olmaz. Örneğin,

$$f = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10)(11\ 12)$$

ise f'nin derecesi $10 \times 2 = 20$ değil 10 olur. Aynı şekilde

$$f = (1\ 2\ 3\ 4\ 5\ 6)(\ 7\ 8\ 9\ 10)$$

permütasyonunun derecesi $6 \times 4 = 24$ değil 12 olur.

3.13. k uzunluğunda bir döngünün derecesi tam k'dır.

3.14. Genel olarak $k_1, \ldots, k_r$ uzunluğunda ayrık r döngüden oluşan bir permüstasyonun derecesi ekok$(k_1, \ldots, k_r)$ olur.

3.15. Id derecesi 1 olan yegâne elemandır.

3.16. Sym 5'in derecesi 2 olan elemanlarını yazalım:

$$\begin{array}{l}(1\ 2),\ (1\ 3),\ (1\ 4),\ (1\ 5),\ (2\ 3)\ (2\ 4)\ (2\ 5)\ (3\ 4)\ (3\ 5)\ (4\ 5),\\ (1\ 2)(3\ 4),\ (1\ 2)(3\ 5),\ (1\ 2)(4\ 5),\ (1\ 3)(2\ 4),\ (1\ 3)(2\ 5),\ (1\ 3)(4\ 5),\\ (1\ 4)(2\ 3),\ (1\ 4)(2\ 5),\ (1\ 4)(3\ 5),\ (1\ 5)(2\ 3),\ (1\ 5)(2\ 4),\ (1\ 4)(3\ 5).\end{array}$$

Sym n'nin bir f elemanının ***derecesi***, f^d kuvvetinin özdeşlik fonksiyonu olduğu en küçük pozitif d doğal sayısıdır. Bu durumda $f \circ f^{d-1} = f^d = \mathrm{Id}$ eşitliğinden dolayı $f^{-1} = f^{d-1}$ olur. Genel olarak eğer $f^n = \mathrm{Id}$ ise $f^{-1} = f^{n-1}$ olur.

(1 2), (1 3)(2 5) gibi elemanların dereceleri 2'dir. Derecesi 2 olan her elemanın döngüleri 2 uzunluğundadır. Nitekim eğer $f^2 = \mathrm{Id}$ ise ve $f(a) \neq a$ ise,

$$(a, f(a))$$

döngüsü mutlaka f'de yer almalıdır. Elbette derecesi 2 olan elemanlar kendi kendilerinin tersidir ve kendi kendisinin tersi olan her elemanın derecesi 2'dir.

Alıştırmalar

3.17. Sym 6'nın kaç tane derecesi 2 olan elemanı vardır?

3.18. Sym 7'nin kaç tane derecesi 3 olan elemanı vardır?

3.19. Sym 8'in kaç tane derecesi 4 olan elemanı vardır?

3.20. Sym 9'un kaç tane derecesi 6 olan elemanı vardır?

3.21. Eğer p bir asalsa, Sym n'nin $(p-1)! \times \binom{n}{p}$ tane derecesi p olan döngüsü olduğunu kanıtlayın.

3.22. $n = 1, \ldots 20$ için Sym n'nin elemanlarının maksimum derecelerini bulun.

3.23. Örnek 3.1'deki karmayı kaç defa yaparsak kartlar eski haline gelir?

3.24. Aynı soru Alıştırma 3.7'teki karma için.

3.25. Yukardaki iki soruda destedeki kâğıt sayısı (çift kalmak üzere) değişse yanıt ne olur?

3.26. $f^n = f^m = \mathrm{Id}$ ise $d = \mathrm{ebob}(n, m)$ için $f^d = \mathrm{Id}$ olduğunu kanıtlayın.

3.27. f'nin derecesi d olsun. Eğer bir $n \in \mathbb{N}$ için $f^n = \mathrm{Id}$ ise d'nin n'yi böldüğünü kanıtlayın.
3.28. $g \in \operatorname{Sym} n$ ise $g^{n!} = \mathrm{Id}_n$ eşitliğini kanıtlayın.

3.4 Sym n'nin Üreteçleri

(1 2), (3 5) gibi sadece iki elemanın yerlerini değiştiren (diğerlerini sabitleyen) permütasyonlara ***transpozisyon*** adı verilir. Türkçe karşılığı olarak ***makas*** terimini öneriyoruz. Makasların derecesi 2'dir elbette ve $\operatorname{Sym} n$ grubunda tam

$$\binom{n}{2} = \frac{n(n+1)}{2}$$

tane makas vardır. Ama derecesi 2 olan her eleman bir makas değildir, örneğin (1 2)(3 5) permütasyonunun derecesi 2 olmasına rağmen bir makas değildir. Öte yandan, (1 2)(3 5)(4 7) gibi, $\operatorname{Sym} n$'nin derecesi 2 olan her eleman **ayrık** makasların çarpımı olarak yazılabilir. (Neden?)

Öte yandan $\operatorname{Sym} \mathbb{N}$'de

$$(0\ 1)(2\ 3)(4\ 5)(6\ 7)\cdots$$

elemanı sonlu sayıda makasın çarpımı değildir[2].

Makasların önemi şuradan gelmektedir: $\operatorname{Sym} n$'nin her elemanı (ayrık ya da değil) makasların bileşkesi olarak yazılabilir. Örneğin

$$\begin{aligned}
&(1\ 2) \circ (2\ 3) = (1\ 2\ 3),\\
&(1\ 2) \circ (2\ 3) \circ (3\ 4) = (1\ 2\ 3\ 4),\\
&(1\ 2) \circ (2\ 3) \circ (3\ 4) \circ (4\ 5) = (1\ 2\ 3\ 4\ 5).
\end{aligned}$$

Bir başka örnek:

$$(1\ 2\ 5\ 6)(3\ 8\ 4) = (1\ 2) \circ (2\ 5) \circ (5\ 6) \circ (3\ 8) \circ (8\ 4).$$

$(1\ a)$ türünden makaslara ***temel makas*** diyelim. $\operatorname{Sym} n$'de tam $n-1$ tane temel makas vardır: $(1\ 2), \ldots, (1\ n)$.

$$(1\ a) \circ (1\ b) \circ (1\ a) = (a\ b)$$

olduğundan, bir önceki paragrafa göre, $\operatorname{Sym} n$'nin her elemanı temel makasların bileşkesi olarak yazılabilir. Örneğin,

$$\begin{aligned}
(1\ 2\ 3\ 4) &= (1\ 2) \circ (2\ 3) \circ (3\ 4)\\
&= (1\ 2) \circ (1\ 2) \circ (1\ 3) \circ (1\ 2) \circ (1\ 3) \circ (1\ 4) \circ (1\ 3)\\
&= (1\ 3) \circ (1\ 2) \circ (1\ 3) \circ (1\ 4) \circ (1\ 3)
\end{aligned}$$

[2]Bir grupta sadece sonlu sayıda eleman çarpılabilir; sonsuz sayıda elemanın çarpımını tanımlamak için özel koşullar gerekir.

olur. Daha teknik bir deyişle, temel makaslar Sym n grubunun ***üreteçleridir***.

(1 2), (2, 3), (3 4) gibi ardışık sayılardan oluşan makaslara ***ardışık makaslar*** adı verelim.

$$(1\ 3) = (2\ 3) \circ (1\ 2) \circ (2\ 3)$$
$$(1\ 4) = (3\ 4) \circ (2\ 3) \circ (1\ 2) \circ (2\ 3) \circ (3\ 4)$$
$$(1\ 5) = (4\ 5) \circ (3\ 4) \circ (2\ 3) \circ (1\ 2) \circ (2\ 3) \circ (3\ 4) \circ (4\ 5)$$

gibi eşitlikler sayesinde, bir önceki paragraftan dolayı, Sym n'nin her elemanının ardışık makasların bileşkesi olarak yazılabileceği görülür. Yani ardışık makaslar da (aynen temel makaslar gibi) Sym n grubunun ***üreteçleridir***.

Ayrıca, doğruluğu kolayca kontrol edilebilen

$$(1\ 2\ \ldots\ n) \circ (1\ 2) \circ (1\ 2\ \ldots\ n)^{-1} = (2\ 3)$$
$$(1\ 2\ \ldots\ n) \circ (2\ 3) \circ (1\ 2\ \ldots\ n)^{-1} = (3\ 4)$$
$$\ldots$$

gibi eşitlikler sayesinde, bir önceki paragraftan dolayı Sym n'nin her elemanının

$$(1\ 2\ \ldots\ n),\ (1\ 2),\ \text{ve}\ (1\ 2\ \ldots\ n)^{-1}$$

permütasyonlarının çarpımı olarak yazıldığı görülür.

Kanıtladıklarımızı yazalım:

Teorem 3.1. Sym n*'nin her elemanı makaslar/temel makaslar/ardışık makaslar cinsinden yazılabilir.* Sym n*'nin her elemanı* $(1\ 2\ \ldots\ n)$ *ve* $(1\ 2)$ *permütasyonları cinsinden de yazılır.*

Kanıt: $(1\ 2\ \ldots\ n)^{-1} = (1\ 2\ \ldots\ n)^{n-1}$ olduğundan, sonuç bir önceki paragraftan çıkar. □

Bundan böyle bileşke için $\circ$ işaretini kullanamayacağız. Örneğin $(1\ 2) \circ (2\ 3)$ yerine $(1\ 2)(2\ 3)$ yazacağız. $(1\ 2) \circ (3\ 4) = (1\ 2)(3\ 4)$ eşitliğinden dolayı bu yeni yazılım herhangi bir karışıklığa neden olmayacak. Sık sık bileşke yerine çarpım dediğimiz de olacak.

Alıştırmalar

3.29. Sym 3 ve Sym 4 gruplarının elemanlarını temel makasların çarpımı olarak en kısa biçimde yazın.

3.30. Sym 3 ve Sym 4 gruplarının elemanlarını ardışık makasların çarpımı olarak en kısa biçimde yazın.

3.31. Sym 3 ve Sym 4 gruplarının elemanlarını $(1\ 2)$ ve $(1\ 2\ \ldots\ n)$ elemanlarının çarpımı olarak yazın.

3.32. Çift sayıda makasın çarpımının tek sayıda makasın çarpımına eşit olamayacağını gösterin. (Bunun kanıtı zordur; ileride, biraz daha grup teorisi öğrendiğimizde bunun çok daha kolay bir kanıtını göreceğiz.)

3.5 Alt n Grubu

Önceki altbölümde Sym n'nin her elemanının makasların çarpımı olarak yazıldığını gördük. Sym n'nin çift sayıda makasın çarpımı olarak yazılan elemanlarından oluşan kümeye Alt n diyelim. Alt n kümesinin bileşke işlemi altında kapalı olduğu belli, ne de olsa $2k$ makasın çarpımıyla, 2ℓ makasın çarpımını çarparsak, $2(k+\ell)$ makasın çarpımını elde ederiz. Alt n'nin elemanlarının tersi de Alt n'dedir, çünkü bir makasın tersi yine bir makastır. Id_n de Alt n kümesindedir, çünkü Id_n'yi 0 tane makasın çarpımı olarak görebiliriz, ya da eğer $n \geq 2$ ise, Id_n'yi (1 2)(1 2) olarak yazabiliriz. Demek ki Sym n'nin Alt n altkümesi (bileşke işlemiyle birlikte) kendi başına bir gruptur.

Mesela Alt 4 grubu aşağıdaki elemanlardan oluşur:

$$\begin{array}{l} \mathrm{Id}_4,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3), \\ (1,\ 2\ 3),\ (1\ 2\ 4),\ (1\ 3\ 4),\ (2\ 3\ 4), \\ (1\ 3\ 2),\ (1\ 4\ 2),\ (1\ 4\ 3),\ (2\ 4\ 3). \end{array}$$

Bundan böyle $n \geq 2$ olsun. Eğer Alt n'yi soldan ya da sağdan (1 2) ile (ya da herhangi bir makasla) çarparsak tek sayıda makasın çarpımı olarak yazılan elemanlar kümesini buluruz. Bunun tersi de doğrudur: Tek sayıda makasın çarpımı olarak yazılan bir elemanı solda ya da sağdan (1 2) ile çarparsak çift sayıda makasın çarpımı olarak yazılan elemanlar kümesini, yani Alt n'yi buluruz. Demek ki,

$$\mathrm{Sym}\, n = \mathrm{Alt}\, n \cup (1\ 2)\, \mathrm{Alt}\, n$$

olur. Birazdan Alt n ve $(1\ \ 2)\,\mathrm{Alt}\, n$ altkümelerinin ayrık olduklarını göstereceğiz. Yani çift sayıda makasın çarpımı olarak yazılan bir eleman tek sayıda makasın çarpımı olarak yazılamaz. Makasların çarpımından oluşan olası bir

$$\alpha_1 \cdots \alpha_{2k} = \beta_1 \cdots \beta_{2\ell+1}$$

eşitliğinde, tüm makasları eşitliğin bir tarafında toplayarak, tek sayıda makasın çarpımının Id_n'ye eşit olduğunu görürüz. Bunun mümkün olmadığını göstermemiz lazım. Diyelim, $(a_i\ b_i)$ makasları için

$$(a_1\ b_1)(a_2\ b_2)\cdots(a_k\ b_k) = \mathrm{Id}_n\,. \tag{1}$$

Burada $a_i \neq b_i$ varsayımını yapıyoruz elbette.

$$(a_2\ b_2)\cdots(a_k\ b_k)$$

çarpımında a_1 mutlaka belirmeli, aksi halde (1)'in solundaki çarpımda a_1, a_1'e değil b_1'e giderdi. a_1'in soldan ikinci makastan itibaren belirdiği ilk makası ele alalım. Diyelim a_1 ilk defa i'inci makasta beliriyor. $i \geq 2$ elbette. $(a_i\ b_i)$ makası yerine buna eşit olan $(b_i\ a_i)$ makasını alırsak, $a_i = a_1$ varsayımını yapabiliriz.

Şimdi bu i'inci makası soldan ikinci makas olarak yazabileceğimizi göreceğiz. İlk makastan sonra ve i'inci makastan önce a_1 belirmediğini aklımızda tutup şu gözlemi yapalım: a, b, c, d birbirinden farklı sayılar ise,

$$(c\ d)(a\ b) = (a\ b)(c\ d) \text{ ve } (b\ c)(a\ b) = (a\ c)(b\ c) = (a\ c\ b)$$

eşitlikleri geçerlidir. Bu eşitlikleri kullanarak i'inci makasta beliren a_1 sayısını, teker teker sola geçirerek ikinci makas haline getirebiliriz ve bunu yaparken araya daha fazla a_1 koymuş olmayız. Yani çarpımdaki a_1 sayısı aynı kalır, ama i'inci makasta beliren i artık ikinci makasta belirir. Ayrıca yeni çarpımda makas sayısı değişmez. Böylece (1) çarpımı

$$(a_1\ b_1)(a_1\ b_2)(a_3\ c_3)\cdots(a_k\ b_k) = \mathrm{Id}_n \tag{2}$$

biçiminde bir eşitliğe dönüşür. Eğer $b_2 = b_1$ ise, en soldaki iki makası sadeleştirip $k-2$ tane makasın çarpımının Id_n olduğunu görürüz ve tümevarımla $k-2$'nin, dolayısıyla k'nın da çift olduğuna hükmederiz. Bundan böyle $b_2 \neq b_1$ varsayımını yapalım. Ama

$$(a_1\ b_1)(a_1\ b_2) = (a_1\ b_2)(b_1\ b_2) = (a_1\ b_2\ b_1)$$

eşitlikleri geçerli olduğundan, (2) eşitliğini

$$(a_1\ b_2)(b_1\ b_2)(a_3\ c_3)\cdots(a_k\ b_k) = \mathrm{Id}_n \tag{3}$$

olarak yazabiliriz. Sadece ilk iki terim değişti. Ama çarpımdaki a_1 sayısı 1 azaldı, ikinci makasta beliren a_1 kayboldu. Bu işlemi tekrar tekrar yaparak, ya k'yı 2 eksiltip $k-2$ yaparız (ve tümevarımla sonuca varırız), ya da en baştaki a_1 dışında çarpımlardaki tüm a_1'leri yok ederiz. İşlemler bittiğinde çarpımda tek bir a_1 kalamayacağından, bir zaman sonra sadeleştirme olmalı ve uzunluk 2 eksilmeli. Böylece istediğimiz kanıtlanmış olur. Bulduğumuzu yazalım:

Teorem 3.2. *$n \geq 2$ olsun.* Sym n*'nin çift sayıda makasın çarpımı olarak yazılan elemanlar $n!/2$ tane elemanı olan bir gruptur.* □

Alt n grubu ***alterne grup*** olarak bilinir. Grup teorisinde çok önemlidir.

Yukarıdaki kanıt [Sp]'tan alınmıştır. İleride Teorem 3.2'nin daha kavramsal ve daha az zahmetli bir kanıtını vereceğiz. (Bkz. Teorem 14.3.)

Sym n'nin bir elemanı farklı biçimlerde ve farklı sayılarda makasların çarpımı olarak yazılabilir, yani eğer $\sigma \in \mathrm{Sym}\, n$ elemanı k tane makasın çarpımı olarak yazılıyorsa, k sayısı σ'nın bir değişmezi değildir; öte yandan $(-1)^k$ sayısı σ'nın bir değişmezidir, çünkü k tane makasın çarpımı ℓ tane makasın çarpımına eşitse, artık $k-\ell$ sayısının çift olduğunu biliyoruz. Bu $(-1)^k$ sayısına σ'nın ***işareti*** adı verilir ve ± 1'e eşit olan bu sayı $\mathrm{sg}\,\sigma$ olarak gösterilir.

Alıştırmalar

3.33. Sym n'in 3'e bölünen sayıda makasların çarpımı da bir grup olur elbette. Ama bu grup Sym n'ye eşittir!

3.34. Alt 5'in elemanlarının tiplerini ve her bir tipten kaç tane olduğunu bulun.

3.35. Bir önceki alıştırmayı $n = 6, \ldots, 10$ için yapın.

3.36. Her α, $\beta \in \operatorname{Sym} n$ için $\operatorname{sg}(\alpha\beta) = \operatorname{sg}(\alpha)\operatorname{sg}(\beta)$ olduğunu gösterin.

3.6 Sym n'de Eşleniklik

Sym 9'da, örneğin

$$(1\ 2)(3\ 4\ 5)(6\ 7\ 8) \text{ ile } (2\ 9)(3\ 7\ 6)(4\ 5\ 8)$$

elemanları aynı tiptendirler, çünkü her ikisinde de her k için uzunluğu k olan her ayrık döngüden aynı sayıda vardır. Sym 9'un elemanlarının tiplerini sıralayalım:

Id_0 tipi
(1 2) tipi
(1 2 3) tipi
(1 2)(3 4) tipi
(1 2 3 4) tipi
(1 2)(3 4 5) tipi
(1 2 3 4 5) tipi
(1 2)(3 4)(5 6) tipi
(1 2)(3 4 5 6) tipi
(1 2 3)(4 5 6) tipi
(1 2 3 4 5 6) tipi
(1 2)(3 4)(5 6 7) tipi
(1 2)(3 4 5 6 7) tipi
(1 2 3)(4 5 6 7) tipi
(1 2 3 4 5 6 7) tipi
(1 2)(3 4)(5 6)(7 8) tipi
(1 2)(3 4)(5 6 7 8) tipi
(1 2)(3 4 5)(6 7 8) tipi
(1 2)(3 4 5 6 7 8) tipi
(1 2 3)(4 5 6 7 8) tipi
(1 2 3 4)(5 6 7 8) tipi
(1 2)(3 4)(5 6)(7 8 9) tipi
(1 2)(3 4)(5 6 7 8 9) tipi
(1 2)(3 4 5)(6 7 8 9) tipi
(1 2 3)(4 5 6)(7 8 9) tipi
(1 2 3)(4 5 6 7 8 9) tipi
(1 2 3 4)(5 6 7 8 9) tipi
(1 2 3 4 5 6 7 8 9) tipi

Her birinden kaç tane olduğunu ileride bulacağız. Bu paragrafta amacımız aynı tipten iki eleman arasında grup teorisi açısından nasıl bir ilişki olduğunu irdelemek. Örnek olarak aynı tipten olan

$$f = (1\ 2)(3\ 4)(5\ 6\ 7\ 8\ 9)$$

permütasyonuyla

$$g = (1\ 5)(2\ 8)(3\ 7\ 9\ 6\ 4)$$

permütasyonuna bakalım. Birincisinde sayıların adlarını değiştirirsek (Sayıları Türkçeden Macarcaya çevirelim), mesela

1 yerine 1
2 yerine 5
3 yerine 2
4 yerine 8
5 yerine 3
6 yerine 7
7 yerine 9
8 yerine 6
9 yerine 4

yazarsak (Macarca 2 yerine 5 deniyormuş) ikincisini buluruz.

$$g = (1\ 5)(2\ 8)(3\ 7\ 9\ 6\ 4) = (8\ 2)(1\ 5)(7\ 9\ 6\ 4\ 3)$$

olduğundan, şöyle de yapabilirdik:

1 yerine 8
2 yerine 2
3 yerine 1
4 yerine 5
5 yerine 7
6 yerine 9
7 yerine 6
8 yerine 4
9 yerine 3

de yazabilirdik. Bu "yerine yazmanın" ne demek olduğunu görelim. İkinci yer değişikliğini ele alarak,

$$h = (1\ 8\ 4\ 5\ 7\ 6\ 9\ 3)$$

yazalım ve

$$h \circ f \circ h^{-1}$$

elemanına bakalım. (Eğer h, Türkçeden Macarcaya sözlükse, h^{-1} Macarcadan Türkçeye sözlük olsun; böylece Türkçe bir dönüşüm olan f'yi Macarcaya çevirmişoluruz. Tahmin edileceği üzere f'nin tipi değişmemeli. Aşağıda bileşke için artık $\circ$ yazmayacağız.)

$$\begin{aligned} hfh^{-1} &= (1\ 8\ 4\ 5\ 7\ 6\ 9\ 3)(1\ 2)(3\ 4)(5\ 6\ 7\ 8\ 9)(1\ 3\ 8\ 6\ 7\ 5\ 4\ 8) \\ &= (1\ 5)(2\ 8)(3\ 7\ 9\ 6\ 4) = g \end{aligned}$$

buluruz. Yani

$$hfh^{-1} = g$$

olur. Ve elbette soldaki h'leri sağ tarafa atarak ve $k = f^{-1}$ tanımını yaparsak,

$$kgk^{-1} = f$$

buluruz. Eğer $\operatorname{Sym} n$'nin f ve g elemanlarının tipleri aynıysa, bir $h \in \operatorname{Sym} n$ için,

$$hfh^{-1} = g$$

olur. Bu eşitliği sağlayan birden çok $h \in \operatorname{Sym} n$ vardır ama en az bir tane vardır.

Teorem 3.3. *Eğer* $\operatorname{Sym} n$*'nin* f *ve* g *elemanlarının tipi aynıysa, o zaman bir* $h \in \operatorname{Sym} n$ *için* $hfh^{-1} = g$ *olur. Bunun tersi de doğrudur: Eğer bir* $h \in \operatorname{Sym} n$ *için* $hfh^{-1} = g$ *oluyorsa o zaman* f *ve* g*'nin tipleri aynıdır.*

Kanıt: Birinci kısmın kanıtının nasıl olması gerektiği teoremden önce yazılanlardan belli. İkinci önermeyi kanıtlayalım. Diyelim f'nin içinde uzunluğu k ile başlayan bir döngü var. Bu döngünün $(1\ 2\ \ldots\ k)$ döngüsü olduğunu varsaymak bize bir şey kaybettirmez. Öyle yapalım. Şimdi

$$g(h(1)) = (hfh^{-1})(h(1)) = h(f(1)) = h(2)$$

olur. Ayrıca

$$g(h(2)) = (hfh^{-1})(h(2)) = h(f(2)) = h(3)$$

olur. Bunu $h(k)$'ya kadar devam ettiririz, her $i = 1, 2, \ldots, k-1$ için

$$g(h(i)) = h(i+1)$$

buluruz. k için ise,

$$g(h(k)) = (hfh^{-1})(h(k)) = h(f(k)) = h(1)$$

bulunur. Yani f'nin $(1\ 2\ \ldots\ k)$ döngüsü, g'de $(h(1)\ h(2)\ \ldots\ h(k))$ döngüsüne dönüşmüştür. Her döngü için aynı şey olduğundan kanıtımız tamamlanmıştır. □

Sonuç 3.4. *Eğer $n \geq 5$ ise $(a\ b\ c) \in \operatorname{Alt} n$ gibi üçlü döngüler $\operatorname{Alt} n$'de eşleniktirler, yani α ve β bu tür iki eleman ise, bir $\gamma \in \operatorname{Alt} n$ için $\gamma\alpha\gamma^{-1} = \beta$ olur.*

Kanıt: Bu eşitliği sağlayan bir $\gamma \in \operatorname{Sym} n$ olduğunu biliyoruz. Eğer $\gamma \in \operatorname{Alt} n$ ise sorun yok. Aksi halde, $n \geq 5$ olduğundan α'nın yerinden oynatmadığı iki farklı $i, j \in \{1, 2, \ldots, n\}$ vardır; şimdi $\delta = \gamma\,(i\ j) \in \operatorname{Alt} n$ olur ve elbette $\delta\alpha\delta^{-1} = \gamma\alpha\gamma^{-1} = \beta$ olur. □

3.7 Sym n'de Hangi Tipten Kaç Eleman Var?

$\operatorname{Sym} n$ ile biraz daha haşır neşir olmak için biraz hesap yapalım. Bu ve bundan sonraki bölüm, $\operatorname{Sym} n$'nin anlaşılması için ya da grup teorisi için illa okunması gereken bölümler değildir. Konuyla daha âşina olmak isteyenlere önerilir ama.

$\operatorname{Sym} n$'de "tipi" aynı olan elemanların sayısını hesaplayalım.

Örneğin (1 2) gibi ikili döngü biçiminde yazılabilen kaç eleman vardır? Eğer $n = 4$ ise 6 tane vardır:

$$(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4).$$

Eğer $n = 5$ ise, 10 tane vardır:

$$(1\ 2),\ (1\ 3),\ (1\ 4),\ (1\ 5),\ (2\ 3),\ (2\ 4),\ (2\ 5),\ (3\ 4),\ (3\ 5),\ (4\ 5).$$

Genel olarak bu tip elemanlardan n'nin ikilisi kadar, yani

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

tane vardır.

Ya (1 2 3) gibi yazılabilen kaç eleman vardır?

$$\binom{n}{3}$$

tane değil. Çünkü seçtiğimiz her üçlü için iki ayrı seçeneğimiz var. Örneğin, 1, 2, 3 seçilmişse, bu sayılarla elde edeceğimiz (1 2 3) ve (1 3 2) gibi iki ayrı permütasyon var. Bu tipten toplam

$$\binom{n}{3} \times 2$$

tane eleman vardır. $n = 5$ olsun ve bu 20 elemanın her birini yazalım:

$$\begin{array}{l}(1\ 2\ 3),\ (1\ 2\ 4),\ (1\ 2\ 5),\ (1\ 3\ 4),\ (1\ 3\ 5),\ (1\ 4\ 5),\\ (2\ 3\ 4),\ (2\ 3\ 5),\ (2\ 4\ 5),\ (3\ 4\ 5),\\ (1\ 3\ 2),\ (1\ 4\ 2),\ (1\ 5\ 2),\ (1\ 4\ 3),\ (1\ 5\ 3),\ (1\ 5\ 4),\\ (2\ 4\ 3),\ (2\ 5\ 3),\ (2\ 5\ 4),\ (3\ 5\ 4).\end{array}$$

Ya (12)(34) tipinden? Birinci çift için

$$\binom{n}{2}$$

seçenek var. İkinci çift için

$$\binom{n-2}{2}$$

tane seçenek vardır. Ancak bu iki sayıyı çarparsak yanlış sonuç buluruz. Çünkü böyle yaparsak (12)(34) ve (34)(12)'yi sanki iki ayrı elemanmış gibi iki kez sayarız. Çarpımı ikiye bölmek gerekir. Sonuç olarak, (12)(34) tipinden

$$\frac{\binom{n}{2}\binom{n-2}{2}}{2}$$

tane eleman vardır. Gene $n = 5$ için bu 15 elemanın hepsini teker teker yazalım:

$$\begin{array}{c}(1\ 2)(3\ 4),\ (1\ 2)(3\ 5),\ (1\ 2)(4\ 5),\\ (1\ 3)(2\ 4),\ (1\ 3)(2\ 5),\ (1\ 3)(4\ 5),\\ (1\ 4)(2\ 3),\ (1\ 4)(2\ 5),\ (1\ 4)(3\ 5),\\ (1\ 5)(2\ 3),\ (1\ 5)(2\ 4),\ (1\ 5)(3\ 4),\\ (2\ 3)(4\ 5),\ (2\ 4)(3\ 5),\ (2\ 5)(3\ 4).\end{array}$$

Aynı tipten olan elemanlara ***eşlenik*** denir. Eşlenik elemanlardan oluşan kümeye de ***eşleniklik sınıfı*** denir.

Aşağıdaki tabloda $n = 2, \ldots, 8$ için, S_n'de her eşlenik sınıfında kaç eleman olduğunu hesapladık. Her sütunun altında bulduğumuz sayıları toplayarak, toplamın $n!$ olup olmadığını kontrol ettik. Böylece yaptığımız hesapların sağlamasını yapmış olduk. (Gene de hata olabilir! Yanlışa tahammülü olmayan okur kendi başına hesaplamalıdır bu sayıları.)

Eşlenik Sınıfları Sayısı							
	Sym 2	Sym 3	Sym 4	Sym 5	Sym 6	Sym 7	Sym 8
Id	1	1	1	1	1	1	1
(12)	1	**3**	6	10	15	21	28
(123)		2	**8**	20	40	70	112
(12)(34)			3	15	45	105	210
(1234)			6	**30**	90	210	420
(12)(345)				20	120	420	1120
(12345)				24	**144**	504	1344
(12)(34)(56)					15	105	420
(12)(3456)					90	630	2520
(123)(456)					40	280	1120
(123456)					120	**840**	3360
(12)(34)(567)						210	1680
(12)(34567)						504	4032
(123)(4567)						420	3360
(1234567)						720	**5760**
(12)(34)(56)(78)							105
(12)(34)(5678)							1260
(12)(345)(678)							1120
(12)(345678)							3360
(123)(45678)							2688
(1234)(5678)							1260
(12345678)							5040
Toplam	2	6	24	120	720	5040	40320

Örneğin tipi, (1 2)(3 4)(5 6) elemanının tipiyle aynı olan eleman sayısını bulmak için,

$$\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}$$

sayısını 3!'e bölmek zorundayız, aksi halde, örneğin, hepsi birbirine eşit olan

$$(1\ 2)(3\ 4)(5\ 6),\ (1\ 2)(5\ 6)(3\ 4),\ (3\ 4)(1\ 2)(5\ 6),$$
$$(3\ 4)(5\ 6)(1\ 2),\ (5\ 6)(1\ 2)(3\ 4),\ (5\ 6)(3\ 4)(1\ 2)$$

permütasyonların hepsini ayrı ayrı saymış olurduk.

Bunun gibi, $n \geq 22$ için, Sym n'de, tipi

$$(1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)(11\ 12\ 13)(14\ 15\ 16)(17\ 18\ 19)(20\ 21\ 22)$$

olan elemanlardan tam,

$$\frac{\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}\binom{n-6}{2}\binom{n-8}{2}\binom{n-10}{3}\binom{n-13}{3}\binom{n-16}{3}\binom{n-19}{3}2^4}{5!\times 4!}$$

tane vardır; paydaki ilk beş ve son dört terim sadeleşir ve geriye,

$$\frac{n!}{(n-22)! \times (5!2^5) \times (4!3^4)}$$

kalır. Bir sonraki teoremi okuduğunuzda bu sayının anlamını daha iyi anlaşılacak.

Teorem 3.5. *$f \in S_n$ olsun. k_i, f'de i uzunluğundaki döngülerin sayısı olsun. (Demek ki $\sum i \cdot k_i = n$.) O zaman, f'nin eşleniklik sınıfının eleman sayısı,*

$$\frac{n!}{(k_1!1^{k_1})\,(k_2!2^{k_2}) \cdots (k_n!n^{k_n})}$$

olur[3]*.*

Kanıt: Önce döngülerimizin parantezlerini hazırlayalım.

$$(_)(_)\ldots(_)(_\ _)(_\ _)\ldots(_\ _)(_\ _\ _)(_\ _\ _)\ldots(_\ _\ _)\ldots$$

Burada k_1 tane 1 sayılık parantez, k_2 tane 2 sayılık parantez, ..., k_n tane n sayılık parantez var. (En uzun döngünün uzunluğu ancak n olabilir.) Sayı konulabilecek toplam n tane yuva var. Önce n tane sayıyı her biçimde bu parantezlere (her parantezin kabul ettiği kadar) yerleştirelim. Bunu elbette $n!$ değişik biçimde yapabiliriz. Ama bu $n!$ yerleştirmenin bazıları S_n'nin aynı elemanını verir. Kaç tanesinin aynı elemanı verdiğini bulup bu sayıya bölelim. İçinde i tane sayı yerleştirilebilen bir parantezi alalım. Bu parantezin içindeki sayıları i değişik biçimde yerleştirirsek S_n'nin aynı elemanını elde ederiz. Örneğin,

$$(1\ 2\ 3\ 4\ 5), (2\ 3\ 4\ 5\ 1), (3\ 4\ 5\ 1\ 2), (4\ 5\ 1\ 2\ 3), (5\ 1\ 2\ 3\ 4)$$

yerleştirmeleri aynı permütasyonu verir. Bu parantezlerden tam k_i tane olduğundan, sayıları bulundukları parantezlerden çıkarmadan

$$i^{k_i}$$

tane farklı yerleştirmenin aynı permütasyonu verdiğini buluruz. Öte yandan bu parantezlerin de yerlerini değiştirebiliriz. Örneğin,

$$(1\ 2)(3\ 4)(5\ 6),\ (1\ 2)(5\ 6)(3\ 4),\ (3\ 4)(1\ 2)(5\ 6),$$
$$(3\ 4)(5\ 6)(1\ 2),\ (5\ 6)(1\ 2)(3\ 4),\ (5\ 6)(3\ 4)(1\ 2)$$

yerleştirmelerinin hepsi aynı permütasyonu verir. i uzunluğundaki k_i parantezi $k_i!$ farklı biçimde yerleştirebiliriz. Demek ki sadece i uzunluğundaki parantezlere yapılan

$$i^{k_i} \cdot k_i!$$

[3]Bu sayının bir tamsayı olması bile şaşırtıcı olmalı!

tane farklı yerleştirme aynı permütasyonu verir. Bunları $i = 1, 2, \ldots, n$ için çarparsak, toplam

$$(1^{k_1} \cdot k_1!)(2^{k_2} \cdot k_2!) \cdots (i^{k_i} \cdot k_i!) \cdots (n^{k_n} \cdot k_r!)$$

farklı yerleştirmenin aynı permütasyonu vereceğini buluruz. Demek ki bu tipteki eleman sayısını bulmak için, toplam yerleştirme sayısı olan $n!$ sayısını bu sayıya bölmeliyiz. □

Önceki sayfadaki listede Sym n'de en fazla eleman olan eşleniklik sınıflarını koyu harflerle, Id permütasyonu dışında, en az eleman olan sınıfları da altı çizili olarak gösterdik.

Belli ki, eğer $n \geq 5$ ise en az (12) tipinde eleman var.

Ve gene belli ki S_n'de en kalabalık sınıf

$$(1\ 2\ \ldots\ n-1)$$

sınıfı. Bu sınıfın $n(n-2)!$ tane, yani

$$\frac{n!}{(n-1)}$$

tane elemanı var. Bir başka deyişle, her $n-1$ elemandan biri bu tipten (yani bu eşleniklik sınıfında). En az elemanlı eşlenik sınıfının (1 2)'nin eşleniklik sınıfı olduğunu birazdan kanıtlayacağız.

$$(1\ 2\ \ldots\ n-1)$$

elemanının sınıfının en kalabalık olduğu da doğru ama bu olgunun bu kitaba alacak kadar kolay bir kanıtını bilmiyorum. Meraklı okur Matematik Dünyası dergisinin 2003-II sayısının 103'üncü sayfasındaki Özer Çözer'in kanıtını okuyabilir. Zaten o kadar da ilginç bir soru değil!

3.8 Sym n'de Eşlenik Sınıfı Sayısı

Her eşleniklik sınıfının sayısını bulduk. Peki Sym n kümesinde kaç tane eşleniklik sınıfı var? Birkaç sayfa önce eşleniklik sınıflarını ve dolayısıyla kaç tane olduklarını $n = 8$'e kadar teker teker bulduk. Biraz daha ileri gidelim:

S_n'deki eşleniklik sınıfı sayısı aslında n sayısının ***parçalanış sayısına*** eşittir. Örneğin, eğer $n = 6$ ise, n'nin parçalanışlarıyla eşleniklik sınıfları

arasında şöyle bir permütasyon vardır:

$$\begin{array}{lcll} 6 & = & 1+1+1+1+1+1 & \text{Id sınıfı} \\ 6 & = & 2+1+1+1+1 & (1\ 2) \text{ sınıfı} \\ 6 & = & 3+1+1+1 & (1\ 2\ 3) \text{ sınıfı} \\ 6 & = & 2+2+1+1 & (1\ 2)(3\ 4) \text{ sınıfı} \\ 6 & = & 4+1+1 & (1\ 2\ 3\ 4) \text{ sınıfı} \\ 6 & = & 3+2+1 & (1\ 2\ 3)(4\ 5) \text{ sınıfı} \\ 6 & = & 5+1 & (1\ 2\ 3\ 4\ 5) \text{ sınıfı} \\ 6 & = & 2+2+2 & (1\ 2)(3\ 4)(5\ 6) \text{ sınıfı} \\ 6 & = & 4+2 & (1\ 2\ 3\ 4)(5\ 6) \text{ sınıfı} \\ 6 & = & 3+3 & (1\ 2\ 3)(4\ 5\ 6) \text{ sınıfı} \\ 6 & = & 6 & (1\ 2\ 3\ 4\ 5\ 6) \text{ sınıfı} \end{array}$$

Bir doğal sayının parçalanış sayısı, o sayıyı (sıra gözetmeden) doğal sayıların toplamı olarak kaç türlü yazılabileceğidir. Dolayısıyla 6'nın parçalanış sayısı yukarda görüldüğü gibi 11'dir, Sym 6'nın eşleniklik sınıfı sayısına eşittir. Genel olarak, Sym n'nin eşleniklik sınıfı sayısı n'nin parçalanış sayısına eşittir. İlk birkaç sayı için liste aşağıda:

n :	1	2	3	4	5	6	7	8	9	10	11	12	13	15
sınıf sayısı :	1	2	3	5	7	11	15	22	30	42	56	77	101	135

Üzerine pek çok araştırmalar yapılan parçalanış sayısı matematiğin başka bir dalının konusudur ve bu konuya daha fazla girmeyeceğiz.

Teorem 3.6. *Eğer $n \geq 4$ ise,* $(1\ 2)$*'nin eşleniklik sınıfı,* Id*'in sınıfı dışında,* Sym n*'nin en az elemanlı eşleniklik sınıfıdır.*

Kanıt: $\mathrm{Id} \neq f \in \mathrm{Sym}\, n$ olsun. f'nin eşleniklik sınıfının eleman sayısını $[f]$ olarak gösterelim. f'yi ayrık döngülerine ayırıp, uzunluğu r olan döngülerini, adına f_r diyeceğimiz bir elemanda toparlayalım. Örneğin

$$f = (1\ 2)(3\ 4)(5\ 6\ 7\ 8)$$

ise

$$f_2 = (1\ 2)(3\ 4), f_3 = \mathrm{Id}, f_4 = (5\ 6\ 7\ 8).$$

Demek ki her f_r uzunluğu r olan ayrık döngülerin çarpımı ve f, bu f_r'lerin çarpımı. Eğer f ve g permütasyonları aynı tiptelerse, yani aynı eşleniklik sınıfındalarsa, elbette f_r ve g_r de aynı eşleniklik sınıfındadırlar. Ve f_r ile aynı eşleniklik sınıfında olan her eleman mutlaka f ile aynı eşleniklik sınıfında olan bir elemanda belirir, hatta muhtemelen 1'den fazla kez belirir. Örneğin yukardaki örnekteki f_2 ile aynı eşleniklik sınıfında olan $(1\ 3)(2\ 5)$ elemanı, f'ye eşlenik olan $(1\ 3)(2\ 5)(4\,6\,7\ 8)$ elemanında belirir. Eğer $f_r \neq \mathrm{Id}$ ise, $[f_r] \leq [f]$

eşitsizliği bu yüzden bariz. Demek ki $[(1\ 2)] \leq [f_r]$ eşitsizliğini kanıtlamak yeterli.

Bundan böyle, f, herbirinin uzunluğu r olan k ayrık döngünün çarpımı olsun. Demek ki $kr \leq n$. Ayrıca $2 \leq r$. Bu bilgiler daha sonra gerekecek. Şimdi $g = (1\ 2 \dots r)$ olsun. Önce $[g] \leq [f]$ eşitsizliğini kanıtlayacağız. Her iki sayıyı da açık açık bulabiliriz:

$$[g] = \binom{n}{r}(r-1)!$$
$$[f] = \binom{n}{r}\binom{n-r}{r}\cdots\binom{n-kr+r}{r}\frac{((r-1)!)^k}{k!}$$

(Teorem 3.5'i de kullanabilirdik.) Bundan sonra $[g] \leq [f]$ eşitsizliğini k ve n üzerine tümevarımla kanıtlamak, biraz meşakkatli olsa da çok zor değil; okura bırakıyoruz. Demek ki $[(12)] \leq [g]$ eşitsizliğini, yani

$$\binom{n}{2} \leq \binom{n}{r}(r-1)!$$

eşitsizliğini kanıtlamamız gerekiyor. Bu da meşakkatli belki ama kolay. Ufak tefek ayrıntıları saymazsak teorem böylece kanıtlanmıştır. □

Alıştırmalar

3.37. (Bu soru IMO 1987 yarışmasında sorulmuştur).

$$P_n(k) = |\{f \in \mathrm{Sym}_n : f \text{ tam } k \text{ eleman sabitliyor}\}|$$

olsun.

$$\sum_{k=0}^{n} kP_n(k) = n!$$

eşitliğini kanıtlayın.

3.38. Her $i = 1, \dots, n-1$ için $\sigma_i = (i, i+1) \in S_n$ olsun. S_n'nin her elemanının sonlu tane σ_i'nin çarpımı olduğunu kanıtlayın. Her i ve $j = 1, \dots, n-1$ için ya $(\sigma_i \circ \sigma_j)^1 = \mathrm{Id}$, ya $(\sigma_i \circ \sigma_j)^2 = \mathrm{Id}$, ya da $(\sigma_i \circ \sigma_j)^3 = \mathrm{Id}$ olmalı. Kanıtlayın.

3.39. Her $i = 2, \dots, n$ için $\tau_i = (1, i) \in S_n$ olsun. S_n'nin her elemanının sonlu tane τ_i'nin çarpımı olduğunu kanıtlayın.

3.40. Sym $\mathbb{N}$'nin her elemanının $f^2 = g^2$ eşitliklerini sağlayan iki f ve g permütasyonu için $f \circ g$ olarak yazıldığını kanıtlayın.

4. Elemanların Kuvvetleri ve Dereceleri

4.1 Elemanların Kuvvetleri

Bundan böyle, $(\mathbb{Z}, +)$ ve $(\mathrm{Sym}\, X, \circ)$ örneklerinde olduğu gibi somut bir gruptan sözedilmiyorsa, yani sözkonusu olan özellikle belirtilmemiş rastgele bir grupsa, yani ne grubun elemanları ne de $\star$ işlemi belirtilmişse, $\star$ yerine $\cdot$ ve $x \star y$ yerine $x \cdot y$, hatta hiç noktasız xy yazacağız. Ayrıca e yerine 1 yazacağız. Tabii bu 1, 1 doğal sayısı olmayabilir. Önceki yazıda kanıtladığımız

$$y = x^{-1} \Leftrightarrow x \star y = e \Leftrightarrow y \star x = e$$

eşdeğerlikleri bir defa daha bu dilde yazalım, önemliler çünkü:

$$y = x^{-1} \Leftrightarrow xy = 1 \Leftrightarrow yx = 1.$$

Bir grubun bir x elemanı kendisiyle n defa çarpıldığında elde edilen eleman x^n olarak gösterilir ve bu elemana x'in n'inci ***kuvveti*** adı verilir. Burada n pozitif bir doğal sayıdır. x^0 elemanı 1 olarak tanımlanır. Tanım gereği $x^1 = x$ olur. Diğer kuvvetlerin ne demek oldukları bariz: $x^2 = xx$, $x^3 = xxx = x^2x = xx^2$. Bir grubun bir x elemanının kuvvetinin formel tanımı şöyle: $x^0 = 1$ ve her $n \in \mathbb{N}$ için $x^{n+1} = x^n x$.

Eğer bir grupta, $n > 0$ tamsayısı için $x^n = 1$ olursa, o zaman, $xx^{n-1} = x^n = 1$ olduğundan, yukardaki eşdeğerliklere göre $x^{-1} = x^{n-1}$ olur. Bu önemli gözlemi sık sık kullanacağız. Bunun özel bir durumu olarak, $x^2 = 1$ ise $x^{-1} = x$ olduğu bulunur.

Önsav 4.1. *Bir grupta her x elemanı ve her n, $m \in \mathbb{N}$ için $x^n x^m = x^{n+m}$ ve $(x^n)^m = x^{nm}$ olur. Demek ki $x^n x^m = x^m x^n$ olur.*

Kanıt: Birinci eşitlikten başlayalım. m üzerine tümevarımla kanıtlayacağız. Eğer $m = 0$ ise

$$x^n x^m = x^n x^0 = x^n 1 = x^n = x^{n+0} = x^{n+m}.$$

Şimdi eşitliğin m için doğru olduğunu varsayıp eşitliği $m+1$ için kanıtlayalım:

$$x^n x^{m+1} = x^n(x^m x) = (x^n x^m)x = x^{n+m}x = x^{(n+m)+1} = x^{n+(m+1)}.$$

Sıra ikinci eşitlikte. Eğer $m = 0$ ise hem $(x^n)^m$ hem de x^{nm} elemanı 1'e eşittir. Şimdi eşitliğin m için doğru olduğunu varsayalım. Kanıtlanan bir önceki eşitliği kullanarak,

$$(x^n)^{m+1} = (x^n)^m x^n = x^{nm}x^n = x^{nm+n} = x^{n(m+1)}$$

elde ederiz. Kanıtımız tamamlanmıştır. □

Eğer $n > 0$ bir tamsayıysa, x^{-n}'yi $(x^n)^{-1}$ olarak (yani x^n'nin tersi olarak) tanımlıyoruz:

$$x^{-n} = (x^n)^{-1}.$$

Ama burada bir şeyi kontrol etmek gerekir: Daha önce x^{-1} elemanını x'in tersi olarak tanımlamıştık. Oysa burada x^{-1}'in farklı bir tanımını yaptık: Burada x^{-1} (eğer tanımda $n = 1$ alınırsa), x^1'in, yani x'in tersi olarak tanımlanmıştır. Her iki tanımın da aynı elemanı işaret ettiği belli, yani daha önceki tanımla bu tanım $n = 1$ ise örtüşüyor; bir sorun yok. Hatta tanımda $n = 0$ bile alabiliriz, gene bir sorun olmaz: Eski tanıma göre $x^{-0} = x^0 = 1$ diğer yandan yeni tanıma göre de $x^{-0} = (x^0)^{-1} = 1^{-1} = 1$ çıkar.

Pozitif n tamsayıları için (tanım gereği) doğru olan bu eşitliğin taraflarının tersini alırsak $x^n = (x^{-n})^{-1}$ elde ederiz. Demek ki $m = -n$ için $(x^m)^{-1} = x^{-m}$ olur. aynı eşitliğin negatif sayılar için de doğru olduğunu görürüz. Demek ki her $n \in \mathbb{Z}$ için

$$x^{-n} = (x^n)^{-1}$$

olur.

Önsav 4.2. *Bir grubun her x elemanı ve her $n, m \in \mathbb{Z}$ için $x^n x^m = x^{n+m}$ ve $(x^n)^m = x^{nm}$ olur. Demek ki $(x^{-1})^n = x^{-n}$ ve $x^n x^m = x^m x^n$ olur.*

Kanıt: Birinci eşitlikten başlayalım. Gerekirse kanıtlamak istediğimiz eşitliğin tersini alarak (o zaman $x^{-(n+m)} = x^{-m}x^{-n}$ elde ederiz), $n+m \geq 0$ varsayımını yapabiliriz. Demek ki ya $n \geq 0$ ya da $m \geq 0$. Önsav 4.1'den dolayı n ya da m'nin negatif olduğunu varsayabiliriz.

Birinci Şık: $m < 0$. Bu durumda Önsav 4.1'e göre,

$$x^{n+m}(x^m)^{-1} = x^{n+m}x^{-m} = x^{(n+m)+(-m)} = x^n$$

olur. Sol taraftaki x^m'yi sağ tarafa atarak istediğimiz $x^{n+m} = x^n x^m$ eşitliğini elde ederiz.

İkinci Şık: $n < 0$. Bu durumda Önsav 4.1'e göre,

$$(x^n)^{-1}x^{n+m} = x^{-n}x^{n+m} = x^{(-n)+(n+m)} = x^m$$

olur. Soldaki x^n'yi sağ tarafa atarak istediğimiz $x^{n+m} = x^n x^m$ eşitliğini elde ederiz.

Gelelim $(x^n)^m = x^{nm}$ eşitliğine. Gerekirse tarafların tersini alarak $m \geq 0$ varsayımını yapabiliriz. Eğer $m = 0$ ise eşitlik 0'ıncı kuvvetin tanımından çıkıyor. Eşitliğin m için doğru olduğunu varsayıp eşitliği $m+1$ için kanıtlayalım. Kanıtlanan bir önceki eşitlikten ve tanımdan,

$$(x^n)^{m+1} = (x^n)^m x^n = x^{nm} x^n = x^{nm+n} = x^{n(m+1)}$$

elde ederiz.

$(x^{-1})^n = x^{-n}$ eşitliği bir öncekinden elde edilir. Nitekim bir önceki $(x^n)^m = x^{nm}$ eşitliğinde $n = -1$ alırsak, her $m \in \mathbb{Z}$ için $(x^{-1})^m = x^{-m}$ buluruz.

Son eşitliğin kanıtı: $x^n x^m = x^{n+m} = x^{m+n} = x^m x^n$. □

Sonuç 4.3. *Her grubun her x elemanı için, $\{x^n : n \in \mathbb{Z}\}$ kümesi çarpma ve tersini alma işlemleri altında kapalıdır ve grubun etkisiz elemanını içerir. Bir başka deyişle bu küme grubun işlemi altında kendi başına bir grup olur.*

Kanıt: Doğrudan bir önceki önsavın sonucudur. □

Ama dikkat, $\{x^n : n \in \mathbb{Z}\}$ kümesi sonsuz olmak zorunda değildir. Bu konuya bir sonraki bölümde değineceğiz.

Sonuç 4.4. *Eğer bir grubun bir x elemanı için $x^n = 1$ oluyorsa ve eğer n sayısı $k - \ell$ sayısını bölüyorsa (yani $k \equiv \ell \bmod n$ oluyorsa), o zaman $x^k = x^\ell$ olur.*

Kanıt: $k - \ell = nu$ olsun. O zaman $x^k = x^{\ell+nu} = x^\ell x^{nu} = x^\ell (x^n)^u = x^\ell 1^u = x^\ell 1 = x^\ell$ olur. □

Önemli bir şeye dikkat etmek lazım: $(xy)^n$ elemanı $x^n y^n$ elemanına eşit olmayabilir. Öte yandan eğer $xy = yx$ ise $(xy)^n = x^n y^n$ olur. Şimdi bunu kanıtlayalım.

Önsav 4.5. *Eğer bir grubun x ve y elemanları birbirleriyle değişiyorlarsa, yani $xy = yx$ ise o zaman her n ve m tamsayısı için $x^n y^m = y^m x^n$ ve $(xy)^n = x^n y^n$ olur.*

Kanıt: Önce $xy^m = y^m x$ eşitliğini kanıtlayalım. İlk olarak $m \geq 0$ varsayımını yapalım. Eğer $m = 0$ ya da $m = 1$ ise kanıtlayacak bir şey yok. Eşitliğin m için geçerli olduğunu varsayalım. O zaman eşitlik $m + 1$ için de geçerli olur:

$$\begin{aligned} xy^{m+1} &= x(yb^y b) = (xy^m)y = (y^m x)y = y^m(xy) \\ &= y^m(yx) = (y^m y)x = y^{m+1}x. \end{aligned}$$

Demek ki her $m \geq 0$ için $xy^m = y^m x$. Eğer $m < 0$ ise, $-m > 0$ olduğundan, biraz önce yaptığımızdan

$$xy^{-m} = y^{-m}x$$

olur. y^{-m} terimlerini diğer tarafa atarak

$$xy^m = y^m x$$

buluruz.

Şimdi de $x^n y^m = y^m x^n$ eşitliğini kanıtlayalım. Eğer $n = 0$ ise eşitlik bariz. Eğer eşitlik n için doğruysa, biraz önce kanıtlanan $y^n x = xy^n$ eşitliğini kullanarak,

$$\begin{aligned}(xy)^{n+1} &= (xy)^n(xy) = (x^n y^n)(xy) = x^n(y^n x)y \\ &= x^n(xy^n)y = (x^n x)(y^n y) = x^{n+1}y^{n+1}\end{aligned}$$

elde ederiz. Demek ki (tümevarımla) eşitlik $n \geq 0$ için doğru. Şimdi $n < 0$ olsun. $m = -n > 0$ tanımını yapalım. Biraz önce kanıtladığımız $(xy)^m = x^m y^m$ eşitliğini ters çevirirsek, $y^{-m}x^{-m} = (xy)^{-m}$, yani $y^n x^n = (xy)^n$ buluruz. Bu ve bir önceki eşitlik $x^n y^n = (xy)^n$ verir. □

İlerde bu önsavları referans vermeden özgürce kullanacağız.

Notlar ve Örnekler

4.1. Eğer $g = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8\ 9) \in \operatorname{Sym} 9$ ise

$$\begin{aligned}g^2 &= (1\ 3)(2\ 4)(5\ 7\ 9\ 6\ 8) \\ g^3 &= (1\ 4\ 3\ 2)(5\ 8\ 6\ 9\ 7) \\ g^4 &= (5\ 9\ 8\ 7\ 6) \\ g^5 &= (1\ 2\ 3\ 4) \\ g^6 &= (1\ 3)(2\ 4)(5\ 6\ 7\ 8\ 9) \\ g^7 &= (1\ 4\ 3\ 2)(5\ 7\ 9\ 6\ 8) \\ g^8 &= (5\ 8\ 6\ 9\ 7) \\ g^9 &= (1\ 2\ 3\ 4)(5\ 9\ 8\ 7\ 6) \\ g^{10} &= (1\ 3)(2\ 4)\end{aligned}$$

olur. Dolayısıyla

$$g^{20} = g^{10\cdot 2} = \left(g^{10}\right)^2 = [(1\ 3)(2\ 4)]^2 = \mathrm{Id}_9$$

ve $g^{-1} = g^{19}$ olur. Ayrıca,

$$g^{143} = g^{20\cdot 7+3} = \left(g^{20}\right)^7 g^3 = g^3 = (1\ 4\ 3\ 2)(5\ 8\ 6\ 9\ 7)$$

olur.

4.2. $g = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)(10\ 11\ 12\ 13\ 14)$ ise g^{143} permütasyonunu bulalım. $g^{60} = \mathrm{Id}$ olduğu belli. Demek ki $g^{143} = g^{23}$. Şimdi g^{23} permütasyonunu bulalım. Kareler alarak,

$$\begin{aligned}g^2 &= (3\ 5\ 4)(6\ 8)(7\ 9)(10\ 12\ 14\ 11\ 13) \\ g^4 &= (3\ 4\ 5)(10\ 14\ 13\ 12\ 11) \\ g^8 &= (3\ 5\ 4)(10\ 13\ 11\ 14\ 12) \\ g^{16} &= (3\ 4\ 5)(10\ 11\ 12\ 13\ 14)\end{aligned}$$

buluruz. Buradan

$$\begin{aligned}g^{143} &= g^{23} = g^{16+8-1} = g^{16}g^8 g^{-1} \\ &= [(3\ 4\ 5)(10\ 11\ 12\ 13\ 14)][(3\ 5\ 4)(10\ 13\ 11\ 14\ 12)] \\ &\quad [(1\ 2)(3\ 5\ 4)(6\ 9\ 8\ 7)(10\ 14\ 13\ 12\ 11)] \\ &= (1\ 2)(3\ 5\ 4)(6\ 9\ 8\ 7)(10\ 13\ 11\ 14\ 12)\end{aligned}$$

Şöyle de yapabilirdik: $a = (1\ 2)$, $b = (3\ 4\ 5)$, $c = (6\ 7\ 8\ 9)$, $d = (10\ 11\ 12\ 13\ 14)$ olsun. Bu dört eleman birbirleriyle değişirler, yani mesela $ab = ba$ olur.

$$a^2 = \mathrm{Id}_9,\ b^3 = \mathrm{Id}_9,\ c^4 = \mathrm{Id}_9,\ d^5 = \mathrm{Id}_9$$

olduğundan,

$$g^{143} = g^{23} = (abcd)^{23} = a^1b^2c^3d^3 = (1\ 2)(3\ 5\ 4)(6\ 9\ 8\ 7)(10\ 13\ 11\ 14\ 12)$$

olur.

4.3. Eğer G ve H birer grupsa ve $g \in G$ ve $h \in H$ ise, $G \times H$ kartezyen çarpımında, her $n \in \mathbb{Z}$ için $(g,h)^n = (g^n, h^n)$ olur. Benzer şey $\prod_I G_i$ ve $\bigoplus_I G_i$ gruplarında da geçerlidir.

4.4. Eğer grubun işlemi $+$ ise, ki bu durumda matematikçiler arasında yapılan bir anlaşmaya göre grup değişmeli olmak zorundadır, o zaman g^n yerine ng yazıldığını söylemiştik. İşlemi toplamayla yazılan bir grup olan $\mathbb{Z} \times \mathbb{Z}$'den örnek verelim. $k \in \mathbb{Z}$ ve $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ için $k(x,y) = (kx, ky)$ olur.

Eğer grubun işlemi toplama $(+)$ işaretiyle simgeleniyorsa (ki bu durumda grubun abel olduğu varsayılır), o zaman G'nin etkisiz elemanı 0 olarak ve bir g elemanının tersi $-g$ olarak yazılır. Ayrıca $n \in \mathbb{Z}$ için g^n yerine ng yazılır. Elbette $1g = g$, $0g = 0$ ve $-1g = -g$ olur. Yukarıda kanıtladığımız eşitlikler bu yeni yazılımla şu hali alırlar: Her n, $m \in \mathbb{Z}$ ve her x, $y \in G$ için,

$$\begin{aligned}(n+m)x &= nx + mx\\ n(mx) &= (nm)x\\ n(x+y) &= nx + ny.\end{aligned}$$

Ayrıca bu durumda

$$\begin{aligned}x + (-y) &\text{ yerine } x - y,\\ (-x) + y &\text{ yerine } -x + y,\\ (-x) + (-y) &\text{ yerine } -x - y\end{aligned}$$

yazılır. İşlemi toplama olarak yazılan bir gruba ***toplamsal grup*** denir. Bu durumda işlemin her zaman değişmeli olduğu varsayıldığını bir kez daha anımsatalım.

Alıştırmalar

4.5. Eğer bir grubun a ve b elemanları için $ab = ba$ ve $a^n = b^m = 1$ oluyorsa, $e = \mathrm{ekok}(n,m)$ için $(ab)^e = 1$ eşitliğini kanıtlayın.

4.6. Eğer bir grubun bir a elemanı için $a^n = a^m = 1$ oluyorsa, $d = \mathrm{ebob}(n,m)$ için $a^d = 1$ eşitliğini kanıtlayın.

4.7. X bir küme, $x \in X$ ve $f \in \mathrm{Sym}\, X$ olsun. Eğer $f^n(x) = x$ ve $f^m(x) = x$ oluyorsa, $d = \mathrm{ebob}(n,m)$ için $f^d(x) = x$ eşitliğini kanıtlayın.

4.8. G bir grup ve c, $x \in G$ olsun. Eğer x^n, $x^m \in C_G(c)$ ise, $d = \mathrm{ebob}(n,m)$ için $x^d \in C_G(c)$ olduğunu kanıtlayın.

4.2 Elemanların Dereceleri

G bir grup ve $g \in G$ olsun. Bazen bir $n \neq 0$ tamsayısı için $g^n = 1$ olur. $g^{-n} = (g^n)^{-1} = 1$ olduğundan, eğer $g^n = 1$ eşitliğini sağlayan bir $n \neq 0$ tamsayısı varsa, o zaman $g^n = 1$ eşitliğini sağlayan pozitif bir n doğal sayısı vardır. Bu durumda, $g^n = 1$ eşitliğini sağlayan en küçük $n > 0$ doğal sayısına g'nin ***derecesi*** (ya da mertebesi) adı verilir ve bu $\deg g = n$ olarak gösterilir. Bazen de böyle bir $n > 0$ sayısı yoktur; bu durumda derecenin ***sonsuz*** olduğu söylenir ve $\deg g = \infty$ yazılır. Derecesi 1 olan yegâne eleman 1'dir. Bir grubun derecesi sonlu olan elemanlarına ***burulmalı*** eleman adı verilir. Diğer elemanlar ***burulmasız*** eleman olarak anılır. Her elemanı burulmalı olan bir gruba ***burulmalı grup*** denir. Eğer bir grupta bir $n > 0$ doğal sayısı için, her g elemanı $g^n = 1$ eşitliğini sağlıyorsa, gruba ***sonlu eksponentli*** grup denir; eğer n bu eşitlikleri sağlayan en küçük doğal sayıysa, grubun ***eksponentinin*** n olduğu söylenir.

Eğer G değişmeli bir grupsa ve işlemi $+$ ile ifade edilmişse, g^n yerine ng yazıldığını unutmayın. Konuya yeni başlayan biri için, çarpımsal ifadeden toplamsal ifadeye geçmek biraz zahmet ve dikkat gerektirebilir.

Notlar ve Örnekler

4.9. Bir grupta bir elemanın ve tersinin dereceleri eşittir: $\deg g = \deg g^{-1}$ çünkü

$$g^n = 1 \Leftrightarrow g^{-n} = 1$$

önermesi doğrudur.

4.10. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ gruplarında etkisiz eleman 0 dışında elemanların dereceleri sonlu olamazlar çünkü bu gruplarda $n \in \mathbb{Z}$ için $nx = 0$ oluyorsa, $n = 0$ olmak zorundadır.

4.11. $g = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8\ 9\ )$ elemanının derecesi 20'dir.

4.12. $\operatorname{Sym}\mathbb{N}$ grubunun şu iki elemanını alalım:

$$g = (0\ 1)(2\ 3)(4\ 5)\ldots \text{ ve } h = (1\ 2)(3\ 4)(5\ 6)\ldots$$

Her iki elemanın da derecesi 2'dir. Çarpım (bileşke yani) yapılırsa,

$$gh = (\ \ldots\ 6\ 4\ 2\ 0\ 1\ 3\ 5\ \ldots\ ) \text{ ve } hg = (\ \ldots\ 5\ 3\ 1\ 0\ 2\ 4\ 6\ \ldots\ )$$

bulunur. $\deg g = \deg h = 2$'dir ama $\deg gh = \deg hg = \infty$ olur.

4.13. G, eleman sayısı çift olan sonlu bir grup olsun. G'nin derecesi 2 olan elemanı olduğunu göstereceğiz. Eğer $g^2 \neq 1$ ise, $g \neq g^{-1}$ olur. Ayrıca her g elemanı için $\deg g = \deg g^{-1}$ olur. $\{g \in G : g^2 = 1\}$ kümesi $\{g, g^{-1}\}$ olarak ikişer ikişer gruplanırlar, dolayısıyla eleman sayısı çifttir. Dolayısıyla geriye kalan $\{g \in G : g^2 \neq 1\}$ kümesinin eleman sayısı da çift olmak zorundadır. Bu kümede derecesi 1 olan 1 elemanı da var. O elemanı çıkarırsak geriye tek sayıda derecesi 2 olan eleman kalır.

İleride, eğer p bir asalsa ve p, G grubunun eleman sayısını bölüyorsa, o zaman G'nin derecesi p olan bir elemanı olduğunu göstereceğiz (bkz. Teoprem 4.11 ve Teorem 10.15).

Alıştırmalar

4.14. G_1 ve G_2 iki grup, $g_1 \in G_1$ ve $g_2 \in G_2$ olsun. Eğer g_1 ve g_2 elemanlarından birinin derecesi sonsuzsa, $G_1 \times G_2$ kartezyen çarpımının (g_1, g_2) elemanının da derecesinin sonsuz olduğunu kanıtlayın. Eğer $\deg g_1$ ve $\deg g_2$ birer doğal sayıysa, $\deg(g_1, g_2) = \text{ekok}(\deg g_1, \deg g_2)$ eşitliğini kanıtlayın. Buradan, eğer $\deg(g_1, g_2) = \infty$ ise ya $\deg g_1$'in ya da $\deg g_2$'nin sonsuz olması gerektiği çıkar.

4.15. Bir grupta derecesi sonlu olan iki elemanın çarpımının derecesi sonlu olmak zorunda mıdır?

4.16. ab ve ba'nın derecelerinin aynı olduğunu kanıtlayın. abc ve bca'nın derecelerinin aynı olduğunu kanıtlayın. Öyle bir grup ve a, b, c elemanları bulun ki abc ve acb'nin dereceleri farklı olsun.

4.17. $a^{-1}ba = b^2$ ise $a^{-n}ba^n = b^{2^n}$ eşitliğini kanıtlayın. $a^4 = 1$ ise b'nin derecesi hakkında ne söyleyebilirsiniz?

4.18. $b^{-1}ab = a^2$ ve $c^{-1}ac = a^3$ ise ve b ve c elemanlarının dereceleri sırasıyla 4 ve 3 ise a'nın derecesi hakkında ne söyleyebilirsiniz?

4.19. $(G_i)_i$ bir grup ailesi olsun. Her G_i grubunun her elemanın burulmalıysa, $\bigoplus_{i\in I} G_i$ grubunun her elemanının burulmalı olduğunu kanıtlayın.

Sonlu bir grupta tüm elemanların derecesi sonludur. Çünkü sonlu bir grupta

$$g,\ g^2,\ g^3,\ \ldots$$

elemanlarının hepsi birbirinden farklı olamaz, demek ki $0 < m < n$ için $g^n = g^m$ ve dolayısıyla $g^{n-m} = 1$ olmak zorundadır. Bundan da $\deg g < \infty$ çıkar.

Önsav 4.6. *G bir grup, $g \in G$ ve $\deg g = d < \infty$ olsun. O zaman $g^n = 1$ eşitliğinin doğru olması için d'nin n'yi bölmesi gerek ve yeter koşuldur. Bunun sonucu olarak, $g^k = g^\ell$ eşitliğinin doğru olması için yeter ve gerek koşul d'nin $k - \ell$ sayısını bölmesidir.*

Kanıt: Eğer d, n'yi bölüyorsa, $n = dq$ eşitliğini sağlayan bir $q \in \mathbb{Z}$ seçelim. O zaman,

$$g^n = g^{dq} = (g^d)^q = 1^q = 1$$

olur.

Şimdi $g^n = 1$ varsayımını yapalım. n'yi d'ye bölelim: Bir $q \in \mathbb{Z}$ ve $r = 0, 1 \ldots, d-1$ için $n = qd + r$ olur ve o zaman da

$$1 = g^n = g^{qd+r} = g^{qd}g^r = (g^d)^q g^r = 1^1 g^r = g^r,$$

yani

$$g^r = 1$$

olur. Ama $0 \le r < d$ olduğundan, derecenin tanımından dolayı $r = 0$ bulunur. Demek ki $n = qd + r = qd + 0 = qd$ ve d, n'yi böler.

$g^k = g^\ell$ eşitliği ancak $g^{k-\ell} = 1$ ise geçerlidir. Son önerme bundan ve bir önceki önermeden çıkar. □

Sonuç 4.7. *G bir grup, $g \in G$ ve p bir asal olsun. Eğer $g^p = 1$ ise ya $g = 1$ ya da $\deg g = p$ olur.* □

Eğer p bir asalsa ve bir n tamsayısı için $g^{p^n} = 1$ oluyorsa g'ye ***p-eleman*** adı verilir. 1'den farklı bir eleman ancak tek bir p asalı için bir p-eleman olabilir (bkz. Alıştırma 4.6).

Sonuç 4.8. *G bir grup ve $g \in G$ bir p-elemansa g'nin derecesi p'nin bir kuvvetidir.* □

Sonuç 4.9. *G bir grup ve $g \in G$ olsun. Eğer $\deg g = n < \infty$ ve m sayısı n'ye asalsa, bir $h \in G$ için $h^m = g$ olur. Dilenirse h, g'nin bir kuvveti olarak alınabilir.*

Kanıt: $A = \{1, g, g^2, \ldots, g^{n-1}\}$ olsun. $f(x) = x^m$ formülüyle verilmiş A'dan A'ya giden fonksiyonu ele alalım. Eğer $f(x) = f(y)$ ise, $(xy^{-1})^m = 1$ olur. Önsav 4.6'ya göre $\deg(xy^{-1})|m$, aynı önsava göre $\deg(xy^{-1})|n$. Alıştırma 4.6'e göre $\deg(xy^{-1}) = 1$, yani $x = y$. Demek ki f fonksiyonu birebirdir; dolayısıyla örtendir. Demek ki g'nin bir kuvvetinin m'inci kuvveti g'ye eşit olur.

Aynı sonucu daha basit olarak şöyle de kanıtlayabilirdik: Bir $u, v \in \mathbb{Z}$ için $un + mv = 1$ olur. Demek ki

$$g = g^1 = g^{un+mv} = (g^n)^u (g^v)^m = (g^v)^m$$

olur. □

Notlar ve Örnekler

4.20. Bu örnekte şu sonucu kanıtlayacağız.

Teorem 4.10. *G bir grup, $g \in G$, $\deg g = n < \infty$ olsun. $n = p_1^{j_1} \cdots p_k^{j_k}$, n'nin farklı asal çarpanlarıma ayrımı olsun. O zaman öyle $g_1, \ldots, g_k \in G$ vardır ki,*

1. *$g = g_1 \cdots g_k$ olur.*
2. *Her i, j için $g_i g_j = g_j g_i$ olur. (Dolayısıyla $g g_i = g_i g$ olur.)*
3. *Her g_i bir p_i-elemandır.*

Hatta g_i'leri g'nin bir kuvveti olarak seçebiliriz.

Kanıt: $m_i = n/p_i^{j_i}$ olsun. O zaman $m_1, \ldots, m_k$ sayıları aralarında asaldır. Dolayısıyla

$$m_1 u_1 + \cdots + m_k u_k = 1$$

eşitliğini sağlayan $u_1, \ldots, u_k$ sayıları vardır (bkz. Alıştırma 2.3). Şimdi kolay bir hesap yapalım:

$$g = g^1 = g^{m_1 u_1 + \cdots + m_k u_k = 1} = g^{m_1 u_1} \cdots g^{m_k u_k}$$

Şimdi $g_i = g^{m_i u_i}$ tanımını yaparsak istediğimiz her şey doğru olur. □

İleride bu sonucu bir kez daha Sonuç 10.23 olarak kanıtlayacağız.

4.21. p bir asal ve G, eleman sayısı p'ye bölünen bir grup olsun. Bu paragrafta G'nin derecesi p olan bir elemanı olduğunu göreceğiz.

$$X = \{(g_1, \ldots, g_p) : g_1 \cdots g_p = 1\}$$

olsun. Her $g_1, \ldots, g_{p-1}$ için

$$(g_1, \ldots, g_{p-1}, g) \in X$$

önermesini sağlayan bir ve bir tane $g \in G$ olduğu için

$$|X| = |G|^{p-1}$$

olur; ama bizim için önemli olan X'in eleman sayısının p'ye bölündüğü olgusu olacak. Bu arada $(1, \ldots, 1) \in X$ ve

$$(x, \ldots, x) \in X \Leftrightarrow x^p = 1$$

olduğunu gözden kaçırmayalım. Demek ki Sonuç 4.7'ye göre

$$(x, \ldots, x) \in X \Leftrightarrow (x = 1 \text{ ya da } \deg x = p)$$

olur.

$$D = \{(x, \ldots, x) \in X\}$$

tanımını yapalım. D'nin 1'den fazla elemanı olduğunu göstermek istiyoruz.
$(g_1, \ldots, g_p) \in X$ için

$$t(g_1, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_{p-1})$$

olsun. Yani t, X'in elemanlarının koordinatlarını bir sağa kaydırsın, en sağdaki koordinatı da en başa alsın. t elbette X'ten X'e giden birebir ve örten bir fonksiyondur (yani $t \in \operatorname{Sym} X$ olur); ayrıca $t^p = \mathrm{Id}_X$ olur.

$$T = \{\mathrm{Id}_X, t, t^2, \ldots, t^{p-1}\}$$

olsun. Elbette t, D'nin elemanlarını sabitler, yani $x \in D$ ise $t(x) = x$ olur, ama t, D dışında bir eleman sabitleyemez. Bunun da ötesinde, T'nin Id_X dışında hiçbir elemanı X'in herhangi bir elemanını sabitleyemez (bkz. Örnek 4.7) çünkü p bir asal. Demek ki her $x \in X \setminus D$ için

$$Tx = \{x, t(x), t^2(x), \ldots, t^{p-1}(x)\}$$

kümesinin tam p elemanı var. Ayrıca eğer $x \neq y$ ise,

$$Tx \cap Ty = \emptyset$$

olur (neden?) Bundan $X \setminus D$ kümesinin her biri ayrık ve her birinde p elemanı olan Tx parçalarına ayrıldığı çıkar. Demek $X \setminus D$ kümesinin eleman sayısı p'ye bölünür. Dolayısıyla D'nin eleman sayısı p'ye bölünür. Şunu kanıtladık:

Teorem 4.11 (Cauchy Teoremi)**.** *Eleman sayısı p asalına bölünen sonlu bir grubun, derecesi p olan bir elemanı vardır.* □

İleride bu teoremin daha standart bir başka kanıtını vereceğiz (Teorem 10.15).

Demek ki Önsav 4.6'ya göre, bir grupta $\deg g = 6$ ise, $g^{124} = g^4$ olur ve g'nin (negatif ya da pozitif) tüm kuvvetleri

$$1,\ g,\ g^2,\ g^3,\ g^4,\ g^5$$

elemanlarından birine eşittir. Ayrıca yukarıda sıralanan elemanlar birbirine eşit olamazlar. Bunu bir önsav olarak yazalım:

Teorem 4.12. *Eğer bir grubun bir g elemanının derecesi $d < \infty$ ise*

$$\{g^n : n \in \mathbb{Z}\} = \{1,\ g,\ g^2,\ \ldots,\ g^{d-1}\}$$

olur ve bu kümenin tam d tane elemanı vardır. Tersine, eğer bu kümenin d tane elemanı varsa, o zaman g'nin derecesi d'dir.

Kanıt: $n \in \mathbb{Z}$ olsun. n'yi d'ye bölelim: Bir $q \in \mathbb{Z}$ ve $r = 0, 1 \ldots, d-1$ için $n = qd + r$ olur ve o zaman da

$$g^n = g^{qd+r} = g^{qd} g^r = (g^d)^q g^r = 1^1 g^r = g^r$$

olur. Bu birinci önerme. Eşitliğin sağındaki kümede d tane eleman olduğunu kanıtlayalım: Eğer $k, \ell \in \{0, 1 \ldots, d-1\}$ için $g^k = g^\ell$ ise o zaman $g^{k-\ell} = 1$ olur. Demek ki bir Önsav 4.6'ya göre d sayısı $k - \ell$ sayısını bölmeli. $-d < k - \ell < d$ olduğundan, bu da ancak $k - \ell = 0$ ise, yani $k = \ell$ ise mümkündür.

Şimdi $\{g^n : n \in \mathbb{Z}\}$ kümesinin tam d tane elemanı olduğunu varsayalım. Eğer $0 \leq k < \ell < d$ için $g^k = g^\ell$ olsaydı, o zaman $g^{\ell-k} = 1$ olurdu. Ama o zaman da g'nin derecesi $\ell - k$'dan, dolayısıyla d'den küçük olurdu. Ama birinci önermeye göre bu durumda $\{g^n : n \in \mathbb{Z}\}$ kümesinin d'den az elemanı olurdu, çelişki. Demek ki

$$1 = g^0, g = g^1, g^2, \ldots, g^{d-1}$$

elemanları birbirinden farklı ve

$$\{g^n : n \in \mathbb{Z}\} = \{1, g, g^2, \ldots, g^{d-1}\}.$$

Demek ki g^d elemanı sağ kümede beliren d elemandan birine eşit olmalı, yani $0 \leq k \leq d-1$ için $g^d = g^k$ olmalı. Buradan $g^{d-k} = 1 = g^0$ çıkar. Bir iki satır önce bu eşitliğin ancak $k = 0$ ise doğru olabileceğini gördük. Demek ki $g^d = g^k = g^0 = 1$. Öte yandan g'nin daha küçük bir pozitif kuvveti 1 olamayacağından, g'nin derecesi d olmalıdır. □

Eğer grubun işlemi + ise, teoremdeki

$$\{g^n : n \in \mathbb{Z}\} = \{1, g, g^2, \ldots, g^{d-1}\}$$

eşitliği

$$\{ng : n \in \mathbb{Z}\} = \{0, g, 2g, \ldots, (d-1)g\}$$

biçimini alır. Bu durumda (elemanın derecesi sonlu da olsa sonsuz da olsa) $\{ng : n \in \mathbb{Z}\}$ kümesi $\mathbb{Z}g$ ya da $g\mathbb{Z}$ olarak yazılır.

Teoremden, sonlu bir grubunun eksponentinin sonlu olduğu anlaşılır.

Bu önemli teoremden sonra yazıyı dereceler üzerine çok yararlı birkaç sonuçla bitiriyoruz.

Önsav 4.13. $\deg g = d < \infty$ *ve* $n \in \mathbb{Z}$ *ise*

$$\deg g^n = \frac{d}{\text{ebob}(d, n)}$$

olur. Demek ki $\text{ebob}(d, n) = 1$ *ise* $\deg g = \deg g^n$ *olur.*

Kanıt: Önsav 4.12'ye göre, $0 \leq n < d$ varsayımını yapabiliriz. $\deg g^n = k$ olsun. Kanıtı iki parçaya ayıracağız.
a. Eğer $\text{ebob}(d, n) = 1$ **ise.** Bu durumda $\deg g^n = d$ eşitliğini kanıtlamalıyız. Elbette $(g^n)^d = (g^d)^n = 1^n = 1$ olur. Önsav 4.6'ya göre $k|d$. Ayrıca $1 = (g^n)^k = g^{nk}$ olduğundan, $d|nk$. Demek ki varsayımımıza göre $d|k$. Buradan $k = d$ çıkar.
b. Eğer $n|d$ **ise.** Bu durumda $\deg g^n = d/n$ eşitliğini kanıtlamalıyız. Elbette $(g^n)^{d/n} = g^d = 1$ olur. Önsav 4.6'ya göre $k|d/n$ ve $k \leq d/n$. Eğer $k < d/n$ olsaydı, $kn < d$ ve $g^{kn} = (g^n)^k = 1$ olurdu, çelişki. Demek ki $k = d/n$.
c. Genel durum. d'yi bölen bir a ve d'ye asal bir b için $n = ab$ olsun. Elbette $a = \text{ebob}(d, n)$'dir. O zaman yukarda yapılanlardan dolayı, $\deg g^n = \deg(g^a)^b = \deg g^a = d/a$ olur. □

Önsav 4.14. *G bir grup ve $a, b \in G$ dereceleri sonlu olan ve $ab = ba$ eşitliğini sağlayan iki eleman olsun. Bu durumda* $\deg ab | \text{ekok}(\deg a, \deg b)$ *olur. Ayrıca eğer* $\text{ebob}(\deg a, \deg b) = 1$ *ise* $\deg ab = \deg a \deg b$ *olur.*

Kanıt: Birinci kısım Önsav 4.5 ve 4.6'dan çıkar. İkinci kısmı kanıtlayalım. $k = \deg ab$ olsun. Demek ki $(ab)^k = 1$, yani $a^k = b^{-k}$.

Birinci kısma göre $k | \deg a \deg b$. Madem öyle, $d | \deg a$ ve $e | \deg b$ için $k = de$ yazalım. Önsav 4.13'a göre

$$\deg a^k = \frac{\deg a}{\text{ebob}(\deg a, k)} = \frac{\deg a}{d} \text{ ve } \deg b^{-k} = \frac{\deg b}{\text{ebob}(\deg b, k)} = \frac{\deg b}{e}$$

olur. Dolayısıyla

$$\frac{\deg a}{d} = \frac{\deg b}{e}$$

olmalı. Ama $\deg a$ ve $\deg b$ aralarında asal olduğundan, bundan, $\deg a = d$ ve $\deg b = e$ çıkar. Demek ki $k = de = \deg a \deg b$ olur. □

Alıştırmalar

4.22. G değişmeli bir grup olsun. Eğer $a \in G$ burulmasız, $1 \neq b \in G$ burulmalıysa, ab elemanının burulmasız olduğunu kanıtlayın.

4.23. Sym 12 grubunun derecesi en büyük elemanlarının tipini bulun.

4.24. Eğer $\deg g = n$ ve m sayısı n'yi bölüyorsa, grupta derecesi m olan bir elemanın varlığını kanıtlayın.

5. Altgruplar

Bazen bir grubun bir altkümesi, grubun işlemiyle birlikte kendi başına bir grup olur;

$$n\mathbb{Z} \subseteq \mathbb{Z} \subseteq \frac{1}{2}\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \text{ ve } \mathbb{Q}^\star \subseteq \mathbb{R}^\star$$

örneklerinde olduğu gibi. G'nin işlemiyle birlikte bir grup olan altkümelerine G'nin ***altgrubu*** adı verilir. Eğer H, G'nin altgrubuysa, bu, $H \leq G$ olarak gösterilir. Genelde bir alkümenin altgrup olması için işlem altında kapalı olması yetmez, örneğin $\mathbb{N}$ toplama altında kapalı olmasına rağmen $\mathbb{Z}$'nin bir altgrubu değildir. (Öte yandan birazdan kanıtlayacağımız Teorem 5.1'e göre altküme sonluysa çarpma altında kapalı olmak altgrup olmak için yeterlidir.)

G, G'nin bir altgrubudur elbette. G'nin G'den farklı altgruplarına ***özaltgrup*** adı verilir ve eğer H, G'nin bir özaltgrubuysa, bu $<$ olarak gösterilir. Eğer G'nin etkisiz elemanı e ise, $\{e\} \leq G$ olur. Bu altgruba ***trişkadan altgrup*** adı verilir. Bunlar pek o kadar ilginç altgruplar değiller.

Alıştırmalar

5.1. Eğer G bir grupsa ve $g \in G$ ise

$$\{g^n : n \in \mathbb{Z}\}$$

kümesinin bir altgrup olduğunu gösterin. Eğer g'nin derecesi $d < \infty$ ise bu altgrubun tam d tane elemanı olduğunu ve

$$\{1, g, g^2, \ldots, g^{d-1}\}$$

kümesine eşit olduğunu Teorem 4.12'de görmüştük. Eğer $d = 12$ ise $\{1, g^3, g^6, g^9\}$ kümesi, hem G'nin hem de $\{1, g, g^2, \ldots, g^{11}\}$ grubunun bir altgrubudur.

5.2. G bir grup olsun. i ve j iki doğal sayı olsun. $\{g^{in} : n \in \mathbb{Z}\}$ ve $\{g^{jn} : n \in \mathbb{Z}\}$, G'nin iki altgrubudur. Bu altgrupların kesişimini bulun. (Eğer $\deg g = \infty$ ise, sonuç pek zor değil. Eğer $\deg g = d < \infty$ ise biraz uğraşmak gerekebilir.)

5.3. p bir doğal sayıysa $A(p) = \{a/p^n : a \in \mathbb{Z},\ n \in \mathbb{N}\}$ kümesinin $\mathbb{Q}$ grubunun bir altgrubu olduğunu gösterin. Birbirine asal p ve q doğal sayıları için $A(p) \cap A(q) = \mathbb{Z}$ olduğunu kanıtlayın. Eğer p ve q aralarında asal değilse kesişim ne olur?

Birazdan çok daha fazla örnek vereceğiz. Önce altgrupların temel özelliklerini ortaya çıkaralım.

G'nin bir H altgrubunun, H kendi başına bir grup olduğundan, etkisiz elemanı vardır. Eğer G'nin etkisiz elemanına e ve H'ninkine de f diyelim.

Elbette $ff = f$ olur; ayrıca $f \in G$ olduğundan, G'de hesap yaparak $fe = f$ bulunur; demek ki $ff = f = fe$ ve buradan da (G grubunda sadeleştirme yaparak) $e = f$ buluruz. Demek ki H ile G'nin etkisiz elemanı aynıdır. Benzer şekilde H'deki bir elemanın H'de ve G'de terslerinin aynı olduğu kanıtlanır.

Eğer G bir grup ve A, $B \subseteq G$ ise,

$$AB = \{ab : a \in A,\, b \in B\} \text{ ve } A^{-1} = \{a^{-1} : a \in A\}$$

tanımlarını yapalım. Demek A'nın çarpma altında kapalı olması demek, aynen $AA \subseteq A$ demektir. $(AB)C = A(BC)$ ve $(AB)^{-1} = B^{-1}A^{-1}$ gibi eşitlikler bariz olmalı. Dolayısıyla $(AB)C$ yerine parantezsiz olarak ABC yazabiliriz.

Demek ki bir $H \subseteq G$ altkümesinin G'nin bir altgrubu olması için,

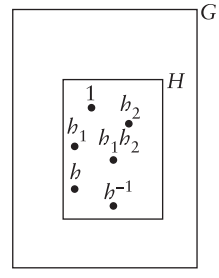
$$HH \subseteq H,\, e \in H,\, H^{-1} \subseteq H$$

koşulları gerek ve yeterdir. Birinci koşul, H'nin işlem altında kapalı olduğunu, ikincisi H'nin G'nin etkisiz elemanını içerdiğini ve üçüncüsü H'deki bir elemanın G grubundaki tersinin gene H'de olduğunu söylüyor. Eğer G toplama altında bir grupsa, yukardaki koşullar,

$$H + H \subseteq H,\, 0 \in H,\, -H \subseteq H$$

koşullarına dönüşür.

Bir grup ve altgrubunun ve eşantiyon olarak altgrubun birkaç elemanının resmi aşağıda:



Aşağıda böyle bir durum irdeleniyor.

Teorem 5.1. *Bir grubun, çarpma işlemi altında kapalı olan, ama boşküme olmayan sonlu bir altkümesi grubun işlemiyle birlikte bir grup olur.*

Kanıt: Gruba G, grubun sonlu altkümesine de H diyelim. Varsayıma göre H'nin elemanlarıyla H'nin elemanlarını çarptığımızda sonuç gene H'de çıkar. Grup tanımının üç özelliğinin H için sağlandığını kanıtlamalıyız. İşlem olarak, tabii ki G'yi grup yapan işlemi alıyoruz. Birleşme özelliği G'nin elemanları için

doğru olduğundan, H'nin elemanları için de doğrudur. Şimdi H'de etkisiz elemanın varlığını kanıtlayalım. Aslında G'nin etkisiz elemanının zorunlu olarak H'de olduğunu kanıtlayacağız. H'nin boşküme olmadığını biliyoruz. H'den bir h elemanı seçelim ve h'yi kendisiyle çarpıp

$$h,\ h^2,\ h^3,\ h^4,\ \ldots$$

elemanlarını elde edelim. Varsayıma göre bunların hepsi H'nin elemanlarıdır. Ama H sonlu bir küme olduğundan, iki farklı n ve m pozitif doğal sayısı için

$$h^n = h^m$$

olmalı. Diyelim $n > m$. O zaman $h^m = h^n = h^{n-m}h^m$ eşitliğinden, G grubunda sadeleştirme yaparak, $h^{n-m} = 1$ elde ederiz. Varsayıma göre $h^{n-m} \in H$. Demek ki $1 \in H$. Ayrıca $h^{n-m} = 1$ eşitliğinden, $hh^{n-m-1} = h^{n-m} = 1$ çıkar. Demek ki

$$h^{-1} = h^{n-m-1}$$

olur. Eğer $n - m = 1$ ise $h^{-1} = h^0 = 1 \in H$, eğer $n - m > 1$ ise $h^{-1} = h^{n-m-1} \in H$ olur. Demek ki her iki durumda da h'nin (G grubundaki) tersi H'dedir. Böylece H'nin kendi başına bir grup olduğu kanıtlanmış oldu. □

Teoreme göre, eğer X sonlu bir kümeyse, $\operatorname{Sym} X$'in bileşke işlemi altında kapalı olan ama boşküme olmayan her altkümesi bileşke işlemiyle birlikte bir grup olur. İleride bu olguyu sık sık kullanacağız.

Aşağıdaki sonuç da çok yararlıdır.

Önsav 5.2. *G bir grup olsun. Eğer $A, B \subseteq G$ altkümeleri çarpma altında kapalıysa ve $BA \subseteq AB$ ise, AB kümesi de çarpma altında kapalıdır. Eğer ayrıca A ve B sonluysa, $AB \leq G$ olur.*

Kanıt: Kanıt bir satırdan ibarettir: $(AB)(AB) = A(BA)B \subseteq A(AB)B = (AA)(BB) \subseteq AB$. İkinci önerme bundan ve bir önceki teoremden çıkar. □

Önsav 5.3. *G bir grup olsun. Eğer $A, B \leq G$ ve $BA \subseteq AB$ ise, $AB \leq G$ olur.*

Kanıt: AB'nin çarpma altında kapalı olduğu önceki önsavdan anlaşılıyor. AB'nin elemanlarının da terseleri AB'dedir: $(AB)^{-1} \subseteq B^{-1}A^{-1} \subseteq BA \subseteq AB$. □

Bundan böyle G'nin etkisiz elemanını e yerine 1 ile göstereceğiz. G, elbette G'nin bir altgrubudur. Ayrıca sadece 1 elemanından oluşan altküme bir altgruptur: $\{1\} \leq G$. Belki okur tasvip etmeyebilir ama $\{1\}$ altgrubu yerine sık sık 1 yazılır ve bu yazılım çok kullanışlıdır. Ama hiçbir zaman $1 = \{1\}$

yazılmaz çünkü böyle bir tanım kümeler kuramının temellendirme aksiyomuyla çelişirdi. $\{1\}$ yerine 1 yazılması (yanlış olan!) $1 = \{1\}$ eşitliğinden değil, matematikçilerin yaptığı bir anlaşmadan kaynaklanır. 1 simgesinin ne zaman etkisiz eleman 1 olarak ne zaman $\{1\}$ altgrubu olarak kullanıldığı her zaman anlaşılacağından, bu tuhaf anlaşma herhangi karışıklığa yol açmayacaktır. (Öyle bir olasılık varsa 1 altgrubu yerine yazılması gerektiği gibi $\{1\}$ yazın.)

Aşağıdaki sonuç da çok yararlı olacak.

Önsav 5.4. *G bir grup ve A, $B \leq G$ olsun. Eğer $A \cap B = \{1\}$ ise $(a, b) \mapsto ab$ kuralı $A \times B$'den AB'ye giden bir eşleme verir. Dolayısıyla $|AB| = |A||B|$ olur.*

Kanıt: Fonksiyonun örten olduğu belli. Diyelim, a, $a_1 \in A$ ve b, $b_1 \in B$ için $ab = a_1b_1$ o zaman $a_1^{-1}a = b_1b^{-1} \in A \cap B = \{1\}$ olur, yani $a_1^{-1}a = b_1b^{-1} = 1$, yani $a = a_1$ ve $b = b_1$ olur. Demek ki fonksiyon birebirmiş. □

Notlar ve Örnekler

5.4. Önce basit örneklerden başlayalım: $2\mathbb{Z} \leq \mathbb{Z} \leq \frac{3}{2}\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$, $\{1, -1\} \leq \mathbb{Q}^\star \leq \mathbb{R}^\star$, $\mathbb{Q}^{>0} \leq \mathbb{R}^{>0}$. Ayrıca

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a,\, b \in \mathbb{Z}\} \text{ ve } \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a,\, b \in \mathbb{Q}\}$$

gibi kümeler de $\mathbb{R}$'nin altgruplarıdır.

Biraz daha az bariz bir örnek: $\mathbb{Q}[\sqrt{2}] \setminus \{0\} \leq \mathbb{R}^\star$ olur. (Okura alıştırma.)

5.5. $\mathbb{Z}$ grubunun tüm altgruplarını Teorem 2.1'de sınıflandırmıştık: $\mathbb{Z}$'nin her altgrubu bir ve bir tek $n \in \mathbb{Z}$ için $n\mathbb{Z}$ biçimindedir. Birazdan $\mathbb{Z} \times \mathbb{Z}$ grubunun tüm altgruplarını da sınıflandıracağız.

5.6. G bir abel grubu olsun.

Eğer $n \in \mathbb{Z}$ ise, $G_n = \{g \in G : g^n = 1\}$ kümesi G'nin bir altgrubudur. (Bkz. Sonuç 4.3.)

π, bir asal sayılar kümesi olsun. Asal bölenleri π kümesinde olan sayılara ***π-sayı*** adı verilir. $\{g \in G : \deg g \text{ bir } \pi\text{-sayı}\}$ bir altgruptur.

Eğer π, tüm asallar kümesiyse, yukardaki örnek, derecesi sonlu olan (yani burulmalı) elemanlardan oluşan bir kümenin bir altküme olduğunu gösterir.

Ama 1 dışında burulmalı elemanları olan değişmeli bir grupta, burulmasız elemanlar kümesi hiçbir zaman bir altgrup olamaz. (Neden?)

5.7. G değişmeli bir grup ve $n \in \mathbb{Z}$ olsun. $G_n = \{g^n : g \in G\}$, G'nin bir altgrubudur. Bu tür altgrupların çeşitli n sayıları için kesişimleri de alınabilir elbet. Eğer $G_n = G$ ise G'ye ***n-bölünür*** denir. $\mathbb{Q}$ grubu her $n \neq 0$ için n-bölünürdür çünkü $\mathbb{Q}$ grubunda her $a \in \mathbb{Q}$ ve $n \neq 0$ için $nx = a$ denklemi çözülebilir. Bu tür gruplara ***bölünür grup*** denir. $\mathbb{R}^{>0}$ grubu da bölünürdür. Ama $\mathbb{R}^\star$ grubu sadece tek n sayıları için n-bölünürdür. Örneğin $x^2 = -1$ denkleminin $\mathbb{R}$'de çözümü olmadığından $\mathbb{R}^\star$ grubu 2-bölünür değildir. Eğer $p_1, \ldots, p_k$ asalları n'yi bölen tüm asallarsa, grubun n-bölünür olması demek, grubun her i için p_i-bölünür olması demektir (neden?)

Bölünür bir grubun ya 1 elemanlı ya da sonsuz olduğunu gösterin. Bölünür grupların kartezyen çarpımlarının ve kısıtlanmış çarpımlarının bölünür olduğunu kanıtlayın. Bir kartezyen çarpım ya da kısıtlanmış çarpım bölünürse, çarpımı alınan grupların da bölünür olduğunu kanıtlayın.

5.8. $(G_i)_{i \in I}$ bir grup ailesi olsun. O zaman $\bigoplus_I G_i \leq \prod_I G_i$ olur.

5.9. $A \leq G$ ve $B \leq H$ olsun. O zaman $A \times B \leq G \times H$ olur. Ama dikkat: $G \times H$'nin tüm altgrupları bu türden değildir. Örneğin, eğer $G = H$ ise,

$$\{(g, g) : g \in G\} \leq G \times G$$

olur ve $G = 1$ olmadıkça (yani $G = \{1\}$ olmadıkça!) $A \times B$ türünden yazılan bir altgrup değildir.

Birazdan, Alıştırma 5.23'te $\mathbb{Z} \times \mathbb{Z}$ grubunun altgruplarını sınıflandıracağız.

Ne tür G grupları için $\{(g, g^{-1}) : g \in G\} \leq G \times G$ olur?

5.10. Bir önceki örneği sonsuz sayıda grubun kartezyen çarpımına genelleştirmek işten bile değildir: $(G_i)_{i \in I}$ bir grup ailesi olsun. Her $i \in I$ için $H_i \leq G_i$ olsun. O zaman $\bigoplus_I H_i \leq \bigoplus_I G_i$ ve $\prod_I H_i \leq \prod_I G_i$ olur.

5.11. $H \leq \prod_I G_i$ olsun. $i_0 \in I$ sabit bir göstergeç olsun. $\pi_{i_0} : \prod_I G_i \longrightarrow G_{i_0}$ fonksiyonu $\pi_{i_0}((g_i)_i) = g_{i_0}$ formülüyle tanımlanmış olsun. π_{i_0} fonksiyonuna i_0'ıncı ***doğal izdüşüm fonksiyonu*** denir. $\pi_{i_0}(H) \leq G_{i_0}$ olur.

5.12. **[Merkezleyici]** G bir grup ve $X \subseteq G$ olsun. O zaman

$$C_G(X) = \{g \in G : \text{ her } x \in X \text{ için } gx = xg\}$$

olarak tanımlanan $C_G(X)$ kümesi G'nin bir altgrubudur. (Bkz. Alıştırma 1.22.) Bu altgruba X'in ***merkezleyicisi*** adı verilir.

5.13. **[Merkezleyici]** G bir grup, $H \leq G$ ve $X \subseteq G$ olsun. O zaman

$$C_H(X) = \{g \in G : \text{ her } x \in X \text{ için } gx = xg\}$$

olarak tanımlanan $C_H(X)$ kümesi G'nin bir altgrubudur. (Bkz. Alıştırma 1.22.) Bu altgruba X'in H'deki ***merkezleyicisi*** adı verilir.

5.14. **[Merkez]** G bir grup ve $H \leq G$ olsun. O zaman H'nin ***merkezi***

$$Z(H) = \{z \in H : \text{ her } x \in H \text{ için } zx = xz\}$$

olarak tanımlanır. Elbette bir altgruptur ve bir önceki alıştırmanın yazılımıyla $Z(H) = C_H(H)$ olur. $Z(G)$'nin altgruplarına G'nin ***merkezî altgruplar***, elemanlarına da ***merkezî elemanlar*** denir.

5.15. Her şey yukarıdaki alıştırmalarda olduğu gibiyse, $Z(C_H(X))$ gibi altgruplar da tanımlanabilir. Eğer $g \in G$ için $g^n \in H$ oluyorsa, $g^n \in Z(C_H(g))$ olduğunu kanıtlayın.

5.16. **[Normalleyici]** Eğer G bir grup ve $X \subseteq G$ ise,

$$X^g = \{x^g : x \in X\} = \{g^{-1}xg : x \in X\}$$

olarak tanımlansın. O zaman,

$$N_G(X) = \{g \in G : X^g = X\}$$

kümesi G'nin bir altgrubu olur. Bu altgruba X'in ***normalleyicisi*** adı verilir. (Uygulamada genellikle X bir altgrup olur.)

5.17. X bir küme ve $Y \subseteq X$ olsun.

$$\{g \in \operatorname{Sym} X : g(Y) = Y\} \text{ ve } \{g \in \operatorname{Sym} X : \text{ her } y \in Y \text{ için } g(y) = y\}$$

kümeleri $\operatorname{Sym} X$'in altgruplarıdır. İkinci birincisinin de altgrubudur. Eğer $Z \subseteq X$ ise,

$$\{g \in \operatorname{Sym} X : \text{ ya } g(Y) = Y \text{ ve } g(Z) = Z \text{ ya da } g(Y) = Z \text{ ve } g(Z) = Y\}$$

kümesi de $\operatorname{Sym} X$'in bir altgrubudur.

5.18. Eğer $g \in \operatorname{Sym} X$ ise, g, X'in altkümeler kümesi olan $\wp(X)$ kümesi üzerine de bir etkisi vardır: $A \subseteq X$ için

$$\tilde{g}(A) = \{g(a) : a \in A\}.$$

$\tilde{g} \in \operatorname{Sym} \wp(X)$ olur ve $g \mapsto \tilde{g}$ fonksiyon her $g, h \in \operatorname{Sym} X$ için $\widetilde{gh} = \tilde{g}\tilde{h}$ eşitliğini sağlayan $\operatorname{Sym} X$'ten $\operatorname{Sym} \wp(X)$'e giden birebir bir fonksiyondur. Böylece g elemanını $\operatorname{Sym} \wp(X)$ grubunun bir elemanı olarak da görebiliriz.

5.19. G bir grup ve $a, b \in G$ olsun. H kümesi, a, b, a^{-1}, b^{-1} elemanlarının **her türlü** çarpımlarından oluşan küme olsun. Örneğin, $a^4b^2a^{-3}b^5a$, $b^3a^2b^{-4}a^7b^8a^{-7} \in H$. (Tabii bu elemanlar eşit olabilirler, örneğin grup değişmeliyse eşittirler.) H kümesi bir altgruptur. Bu yaptığımızı a, b, c elemanlarıyla ya da sonsuz sayıda elemanla da yapabiliriz.

5.20. Bir grupta her altgrup kümesinin kesişimi bir altgruptur.

5.21. Bir altgrubun da altgrupları vardır. Bir grubun bir altgrubunun altgrupları grubun altgruplarıdır elbette. Yani $C \leq B$ ve $B \leq A$ ise $C \leq A$ olur.

5.22. $\mathbb{Z}$'nin altgruplarının bir ve bir tek $n \in \mathbb{N}$ için $n\mathbb{Z}$ biçiminde olduklarını biliyoruz (Teorem 2.1). Elbette $n\mathbb{Z} \leq m\mathbb{Z}$ içindeliği ancak ve ancak m, n'yi bölüyorsa doğrudur. Dolayısıyla $\mathbb{Z}$'nin maksimal altgrupları[1] bir p asalı için $p\mathbb{Z}$ biçimindedir. Öte yandan $\mathbb{Z}$'nin minimal altgrubu yoktur. İleride $\mathbb{Q}$'nun maksimal altgrubu olmadığı göstereceğiz. Ancak $\mathbb{Q}$'nun 1'i içermeyen maksimal altgrubu vardır. Yani öyle bir $A \leq \mathbb{Q}$ vardır ki, $1 \notin A$ olur ve eğer $A < B \leq \mathbb{Q}$ ise $1 \in B$ olur. Okur böyle bir A altgrubu bulmaya çalışabilir. Çok kolay değildir ama imkânsız da değildir. (Bkz. Teorem F.3.) $\mathbb{R}$ grubunun da böyle bir altgrubu vardır ancak bu algrubun varlığını kanıtlamak için Seçim Aksiyomu'na ihtiyaç vardır, yani varlığı bilinen altgrubun ne olduğunu kimse bilemez!

5.23. **[$\mathbb{Z} \times \mathbb{Z}$'nin Altgrupları]** $\mathbb{Z}$'nin altgruplarının bir ve bir tek $n \in \mathbb{N}$ için $n\mathbb{Z}$ biçiminde olduklarını biliyoruz (Teorem 2.1). Bu örnekte $\mathbb{Z} \times \mathbb{Z}$ grubunun altgruplarını sınıflandıracağız[2]. $H \leq \mathbb{Z} \times \mathbb{Z}$ olsun.

$$A = \{x \in \mathbb{Z} : \text{ bir } y \in \mathbb{Z} \text{ için } (x, y) \in H\}$$

tanımını yapalım. (A, H'nin birinci izdüşümüdür.) A'nın $\mathbb{Z}$'nin bir altgrubu olduğunu kanıtlamak zor değil. Demek ki Teorem 5.1'e göre bir ve bir tek $n \in \mathbb{N}$ için $A = n\mathbb{Z}$ olur. Tanıma göre

$$H \leq A \times \mathbb{Z} = n\mathbb{Z} \times \mathbb{Z}$$

olmalı. Ayrıca

$$B = \{y \in \mathbb{Z} : (0, y) \in H\}$$

tanımını yapalım. $B \leq \mathbb{Z}$ olduğundan (kanıtı kolay), bir ve bir tek $k \in \mathbb{N}$ için $B = k\mathbb{Z}$ olur. Demek ki

$$H \cap (\{0\} \times \mathbb{Z}) = \{0\} \times B = \{0\} \times k\mathbb{Z}.$$

Eğer $n = 0$ ise $H \leq \{0\} \times \mathbb{Z}$ ve $H = \{0\} \times B = \{0\} \times k\mathbb{Z}$ olur. Bundan böyle $n > 0$ olsun.

---

[1] Bir grubun ***maksimal altgrubu*** terimi, en büyük özaltgrubu anlamına kullanılır, aksi halde grubun kendisi tabii ki grubun maksimal altgrubu olurdu. Benzer şekilde 1 altgrubu bir grubun en küçük altgrubudur. Bu yüzden ***minimal altgrup*** deyimi en küçük ve 1'den farklı altgrup anlamına kullanılır.

[2] Matematikte bir kümeyi ***sınıflandırmak***, kümeyle çok daha aşina olduğumuz bir küme arasında bir eşleme bulmak anlamına gelir. Bir başka deyişle sınıflandırılmak istenen kümenin elemanları, daha aşina olduğumuz bir kümenin elemanlarıyla kodlanır. Örneğin $\mathbb{Z}$'nin altgrupları $\mathbb{N}$'nin elemanları tarafından kodlanmışlardır. $\mathbb{Z}$'nin her altgrubu $\mathbb{N}$'nin birelemanına ve $\mathbb{N}$'nin her elemanı $\mathbb{Z}$'nin bir altgrubuna tekabül eder. $\mathbb{N}$'nin elemanlarıyla daha aşina olduğumuzdan (ne de olsa doğal sayılar), böylece $\mathbb{Z}$'nin altgruplarını sınıflandırmış oluruz.

$n \in A$ olduğundan, öyle bir $m \in \mathbb{Z}$ vardır ki $(n, m) \in H$ olur. Böyle bir $m \in \mathbb{Z}$ sabitleyelim. Şimdi H'den herhangi bir (x, y) elemanı seçelim. x'i n'ye bölelim: Öyle q, $r \in \mathbb{Z}$ bulunur ki,

$$x = nq + r \text{ ve } 0 \leq r < n$$

olur. $(x, y) - q(n, m) \in H$ ve

$$(x, y) - q(n, m) = (x - qn, y - qm) = (r, y - qm) \in H \leq n\mathbb{Z} \times \mathbb{Z}$$

olduğundan $r = 0$ olmak zorunda. Demek ki,

$$(x, y) - q(n, m) = (0, y - qm) \in H \cap (\{0\} \times \mathbb{Z}) = \{0\} \times k\mathbb{Z}.$$

Dolayısıyla bir $z \in \mathbb{Z}$ için

$$(x, y) - q(n, m) = (0, kz) = z(0, k)$$

olur. Buradan da

$$(x, y) = q(n, m) + z(0, k)$$

çıkar. Demek ki

$$H \leq \mathbb{Z}(n, m) + \mathbb{Z}(0, k).$$

Diğer yandan, (n, m), $(0, k) \in H$ olduğundan, $\mathbb{Z}(n, m) + \mathbb{Z}(0, k) \leq H$ içindeliği bariz. Böylece $n \in \mathbb{N} \setminus \{0\}$, $k \in \mathbb{N}$ ve $m \in \mathbb{Z}$ için

$$H = \mathbb{Z}(n, m) + \mathbb{Z}(0, k)$$

eşitliğini kanıtlamış olduk. Ancak bulunan n, m, k sayıları biricik olmayabilir. Aslında n ve k sayıları biricik de, k değişik değerler alabilir. k üzerindeki koşulları daha da kısıtlamak amacıyla devam edelim. Eğer $k = 0$ ise $H = \mathbb{Z}(n, m)$ olur ve biriciklik konusunda bir sorun yaşanmaz. Ama eğer $k > 0$ ise, m'yi k'ya bölelim ve

$$m = kq_1 + r_1 \text{ ve } 0 \leq r_1 < k$$

önermelerini sağlayan q_1, $r_1 \in \mathbb{Z}$ bulalım.

$$(n, m) = (n, r_1) + q_1(0, k) \in \mathbb{Z}(n, r_1) + \mathbb{Z}(0, k)$$

olduğundan

$$H = \mathbb{Z}(n, m) + \mathbb{Z}(0, k) \leq \mathbb{Z}(n, r_1) + \mathbb{Z}(0, k)$$

olur. Ama $(n, r_1) = (n, m) - q_1(0, k) \in H$, dolayısıyla $\mathbb{Z}(n, r_1) \leq H$ ve

$$H = \mathbb{Z}(n, r_1) + \mathbb{Z}(0, k).$$

Aşağıdaki teoremin yarısını kanıtladık:

Teorem 5.5. *$H \leq \mathbb{Z} \times \mathbb{Z}$ olsun. Aşağıdakilerden biri ve sadece biri geçerldiir:*
i. *Bir ve bir tek $k \in \mathbb{N}$ için $H = \mathbb{Z}(0, k)$ olur.*
ii. *Bir ve bir tek $0 \neq n \in \mathbb{N}$ ve $m \in \mathbb{Z}$ çifti için $H = \mathbb{Z}(n, m)$ olur.*
iii. *Bir ve bir tek n, $k \in \mathbb{N}\setminus\{0\}$ ve $m \in \{0, 1, \ldots, k-1\}$ üçlüsü için $H = \mathbb{Z}(n, m)+\mathbb{Z}(0, k)$ olur.*

Kanıt: Varlık kısmını biraz önce kanıtladık. İlk iki şıkkın biriciklik kısmı kolay ve okura bırakılmıştır. Üçüncüsününki de çok zor değil. Eğer koşulları sağlayan (n, m, k) ve (n_1, m_1, k_1) üçlüleri için

$$\mathbb{Z}(n, m) + \mathbb{Z}(0, k) = \mathbb{Z}(n_1, m_1) + \mathbb{Z}(0, k_1)$$

olursa, o zaman kolayca görüleceği üzere $(0, k)$ ve $(0, k_1)$ birbirinin katı olmak zorunda. Buradan da $k = k_1$ çıkar. Aynı şey n ve n_1 için de geçerli. Demek ki $n = n_1$. Son olarak $m = m_1$ eşitliğini kanıtlayalım. Bir x, $y \in \mathbb{Z}$ için $(n, m) = x(n_1, m_1) + y(0, k_1) = x(n, m_1) + y(0, k) = (xn, xm_1 + yk)$ olduğundan, $x = 1$ ve $m = m_1 + yk$ olmalı. Ama $m \in \{0, 1, \ldots, k - 1\}$ içindeliği $y = 0$ verir. Demek ki $m = m_1$. □

Alıştırmalar

5.24. G bir grup ve H ve K iki altgrup olsun. Eğer $K \subseteq H$ ise $K \leq H$ olduğunu kanıtlayın.

5.25. G bir grup ve $A, B \leq G$ olsun. $A \cup B$ kümesinin bir altgrup olması için ya A'nın B'yi ya da B'nin A'yı içermesi gerektiğini kanıtlayın. Üç altgrup için bu doğru değildir. Karşıörnek bulun.

5.26. G bir grup olsun. Eğer $Z(G) \leq H \leq G$ ise $Z(G) \leq Z(H)$ olduğunu kanıtlayın. Eğer $H \leq G$ ise, $Z(G) \cap H \leq Z(H)$ olduğunu kanıtlayın.

5.27. G bir grup olsun ve her n doğal sayısı için $H_n \leq G$ olsun. Eğer her n için $H_n \leq H_{n+1}$ ise, $\bigcup_n H_n \leq G$ olduğunu kanıtlayın.

5.28. G bir grup olsun. G'nin bir $(H_i)_{i\in I}$ altgrup ailesi verilmiş olsun. Her $i, j \in I$ için, $H_i \leq H_j$ ve $H_j \leq H_i$ içindeliklerinden birinin geçerli olduğunu varsayalım. O zaman $\bigcup_I H_i \leq G$ olduğunu kanıtlayın.

5.29. G bir grup ve p bir asal olsun. Eğer bir $H \leq G$ altgrubunun her elemanının derecesi p'nin bir kuvvetiyse, H'ye ***p*-altgrup** denir. Bir önceki alıştırmadaki H_i altgrupları p-gruplarsa, $\bigcup_I H_i$ altgrubunun da bir p-grup olduğu belli. Bu olgudan hareket ederek ve Zorn Önsavı'nı kullanarak, G'nin maksimal p-altgruplarının olduğunu kanıtlayın.

5.30. Alıştırma 5.28'yı genelleştirebiliriz. G bir grup ve $(H_i)_{i\in I}$, G'nin bir altgrup ailesi olsun. Eğer her $i, j \in I$ ve her $h_i \in H_i$ ve $h_j \in H_j$ için $h_i h_j \in H_k$ içindeliğini sağlayan bir $k \in K$ varsa, $\bigcup_{i\in I} H_i$ kümesinin bir altgrup olduğunu kanıtlayın.

5.31. G bir grup, $H \leq G$ ve $x \in G$ olsun. Eğer x^n, $x^m \in H$ ise, $d = \text{ebob}(n, m)$ için $x^d \in H$ olduğunu kanıtlayın.

5.32. Eğer $n \geq 3$ ise $Z(\operatorname{Sym} n) = \{\mathrm{Id}_n\}$ eşitliğini kanıtlayın.

5.33. $\operatorname{Sym} 3$ grubunun tüm altgruplarını bulun.

5.34. $\operatorname{Sym} 4$ grubunun tüm altgruplarını bulun.

5.35. $K \leq G$ ve $N_G(K) \leq H \leq G$ olsun. $N_G(K) = N_H(K)$ eşitliğini gösterin.

5.36. $f(T_1, \ldots, T_n)$ bir polinom olsun. (Katsayıların nereden alındığı önemli değil, örneğin $\mathbb{Z}$'den alınabilir.) $\sigma \in \operatorname{Sym} n$ için

$$(\sigma f)(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

olsun.

$$G(f) = \{\sigma \in \operatorname{Sym} n : \sigma f = f\}$$

kümesinin $\operatorname{Sym} n$'nin bir altgrubu olduğunu kanıtlayın.

$$f(X_1, X_2, X_3) = X_1X_2X_3 + X_1 + X_2 + X_3$$

için $G(f)$ grubunu bulun.

$$f(X_1, X_2, X_3) = X_1X_2 + X_1X_3 + X_2X_3$$

için $G(f)$ grubunu bulun.

$$f(X_1, X_2, X_3) = X_1X_2X_3 + X_1 + X_2$$

için $G(f)$ grubunu bulun.

$$f(X_1, X_2, X_3) = X_1X_2 + X_3$$

için $G(f)$ grubunu bulun.

$$f(X_1, X_2, X_3) = X_1X_2 + X_3 + X_1$$

için $G(f)$ grubunu bulun.

5.37. $\mathbb{Q}$ grubunun maksimal bir altgrubunun olmadığını kanıtlayın. (Not: Maksimal altgrup, maksimal özaltgrup anlamına gelir. Bu alıştırma kolay olmayabilir; Bkz. Örnek 11.10.)

5.38. Öyle bir G grubu ve bu grubun öyle $H_1 > H_2 > \ldots$ altgruplarını bulun ki $\bigcap_n H_n = 1$ olsun. (Buradaki 1, $\{1\}$ anlamındadır.)

5.39. $H \leq G$ ve $x \in G$ olsun. $x^{-1}Hx$ kümesinin bir altgrup olduğunu kanıtlayın. Bu tür altgruplara H'nin ***eşleniği*** adı verilir. $x^{-1}Hx$ yerine H^x yazmak adettendir (ve çok yararlıdır!) $(H^x)^y = H^{xy}$ eşitliğini kanıtlayın. Eğer her $x \in G$ için $H^x \leq H$ oluyorsa, her $x \in G$ için $H^x = H$ olduğunu kanıtlayın. $C_G(H^x) = C_G(H)^x$ ve $N_G(H^x) = N_G(H)^x$ eşitliklerini kanıtlayın.

5.40. $H \leq G$ ve $x \in G$ olsun. xH kümesinin bir altgrup olması için x'in H'de olmasının yeter ve gerek koşul olduğunu kanıtlayın. (Bu durumda $xH = H$ olur, yani yeni bir altgrup elde edilmez.)

5.41. $\mathbb{Z}\times\mathbb{Z}$ grubunun altgruplarını Örnek 5.23'de sınıflandırmıştık. $\mathbb{Z}\times\mathbb{Z}$ grubunun maksimal altgruplarını bulun.

5.42. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ grubunun altgruplarını Örnek 5.23'deki (ya da Teorem 5.5'teki) gibi tamsayılarla sınıflandırın.

5.43. Eğer $p_1, \ldots, p_k$ asalları n'yi bölen tüm asallarsa, bir grubun n-bölünür olması demek, grubun her i için p_i-bölünür olması demek olduğunu kanıtlayın.

5.44. Küme olarak $G = \mathbb{R} \times \mathbb{R}^\star$ olsun[3]. G üstüne şu ikili işlemi tanımlayalım:

$$(x, y)(z, t) = (yz + x, yt).$$

a. G'nin bu işlemle birlikte bir grup olduğunu kanıtlayın. G'nin değişmeli bir grup olmadığını gösterin.
b. $H = \{(x, 1) \in G : x \in \mathbb{Z}\}$ olsun. $H \leq G$ olduğunu kanıtlayın.
c. $t = (0, 2)$ olsun. $Ht \subseteq tH$ olduğunu ama eşitliğin doğru olmadığını kanıtlayın.
d. $C_G(t) = \{g \in G : gt = tg\}$ altgrubunu bulun. (Bkz. Örnek 5.12.) Bu altgrubun değişmeli bir grup olduğunu kanıtlayın.
e. $u = (1, 1)$ olsun. $C_G(u)$ altgrubunu bulun. Bu altgrubun değişmeli bir grup olduğunu kanıtlayın.
f. $G = C_G(u)C_G(t)$ eşitliğini kanıtlayın. G'nin her elemanının, bir ve bir tek $a \in C_G(u)$ ve $b \in C_G(t)$ için ab biçiminde yazıldığını kanıtlayın.

5.45. 1 ve G'den başka altgrubu olmayan (yani en fazla iki altgrubu olan) bir grubun sonlu olduğunu ve eleman sayısının 1 ya da bir asal sayı olduğunu kanıtlayın.

5.46. G bir grup ve $X \subseteq G$ olsun.

$$\{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} : n \in \mathbb{N},\, x_i \in X,\, \epsilon_i = \pm 1\}$$

kümesinin bir altgrup olduğunu gösterin. Bu algrubun

$$\{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} : n \in \mathbb{N},\, x_i \in X,\, \epsilon_i \in \mathbb{Z}\}$$

kümesine eşit olduğunu gözlemleyin. Sabit her $k > 0$ doğal sayısı için

$$\left\{ x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} : n \in \mathbb{N},\, x_i \in X,\, \epsilon_i = \pm 1,\, \sum_i \epsilon_i \equiv 0 \bmod k \right\}$$

kümesinin bir altgrup olduğunu kanıtlayın.

[3]Bilenlere: $\mathbb{R}$ yerine, $\mathbb{Q}$, $\mathbb{C}$ ya da asal bir $p > 2$ için $\mathbb{Z}/p\mathbb{Z}$ gibi, karakteristiği 2 olmayan herhangi bir K cismi alınabilir. Alıştırmadaki her şey gene geçerlidir.

5.47. G bir grup ve $H \leq G$ olsun. Her a, $b \in G$ için, ya $aH \cap bH = \emptyset$ ya da $aH = bH$ olduğunu kanıtlayın. Ayrıca her a, $b \in G$ için aşağıdaki önermelerin eşdeğer olduğunu kanıtlayın:
i. $aH = bH$.
ii. $aH \cap bH \neq \emptyset$.
iii. $b^{-1}a \in H$.
iv. $a^{-1}b \in H$.
v. $a \in bH$.
vi. $b \in aH$.

5.48. G bir grup ve $a \in G$ olsun. Hangi koşullarda $\{x \in G : x^2 \neq a\}$ bir grup olur. (Bu alıştırma kolay olmayabilir. $x^2 \neq a$ yerine $x^2ax^3 \neq b$ gibi koşullar alınırsa çok çok daha zor olabilir.)

5.49. Bölünür bir grubun ya 1 elemanlı ya da sonsuz olduğunu gösterin. Bölünür grupların kartezyen çarpımlarının ve kısıtlanmış çarpımlarının bölünür olduğunu kanıtlayın. Bir kartezyen çarpım ya da kısıtlanmış çarpım bölünürse, çarpımı alınan grupların da bölünür olduğunu kanıtlayın.

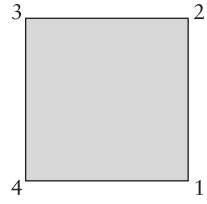
5.50. G bir grup ve A, $B \leq G$ olsun. $|AB| \leq |A||B|$ eşitsizliği bariz olmalı. $|AB||A \cap B| = |A||B|$ eşitliğini kanıtlayın. (İpucu: $f(a, b) = ab$ formülüyle tanımlanan $f : A \times B \longrightarrow AB$ fonksiyonundan hareket edebilirsiniz.) Eğer A ve B sonlu altgruplarsa, ekok$(|A|, |B|)$ sayısının $|AB|$ sayısını böldüğünü kanıtlayın.

6. Geometri ve Gruplar

Bu uzun bölümde çeşitli geometrik nesnelerin "simetri"lerini bulacağız. Her seferinde, ele aldığımız geometrik nesnenin simetriler kümesi bileşke işlemiyle birlikte bir grup olacak. Yani bu bölümde birçok grup örneği göreceğiz. İlk örneklerden sonra, okuma daha hızlı yapılabilir, her okur her örneği ilk okumada anlamak zorunda değildir, ama ilk birkaç örneğin iyi anlaşılması gerekir.

Notlar ve Örnekler

6.1. **Karenin Simetrileri.** Bir kareyle başlayalım. Karenin köşelerini 1, 2, 3 ve 4 olarak numaralandıralım. Henüz simetrinin matematiksel anlamını bilmesek de karenin simetrilerini bulacağız. Karenin simetrileri bileşke işlemi altında bir grup oluşturacak biçimde tanımlanacak. (Tanım birazdan.) Karenin simetrilerinden oluşan gruba G adını verelim.



Merkezini sabit tutarak kareyi saatin (mesela) ters yönüne doğru 90 derece döndürebiliriz. Şekil aşağıda. Bu dönüşüme r adını verelim. O zaman, sadece karenin köşelerine odaklanırsak, bu dönüşüm

$$r = (1\ 2\ 3\ 4)$$

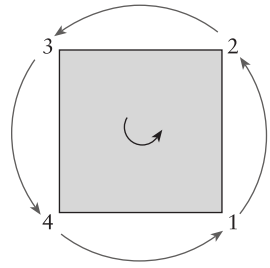
olarak yazılır. r'yi iki defa da uygulayıp kareyi 180 derece döndürebiliriz. Üç defa da uygulayabiliriz. Dört defa uyguladığımızda kare 360 derece dönüp eski yerine gelir; yani

$$r^4 = \mathrm{Id}_4$$

olur. Demek ki r'nin derecesi 4'tür. r'nin kendisiyle bileşkesini alarak

$$\begin{aligned} &\mathrm{Id}_4 \\ &r = (1\ 2\ 3\ 4) \\ &r^2 = (1\ 3)(2\ 4) \\ &r^3 = (1\ 4\ 3\ 2) \end{aligned}$$

dönüşümlerini elde ederiz. (r^0, tanım gereği Id_4 olur; dolayısıyla $r^4 = r^0 = \mathrm{Id}_4$ ve $r^5 = r$, $r^6 = r^2$, $r^{103} = r^3$ olur.)



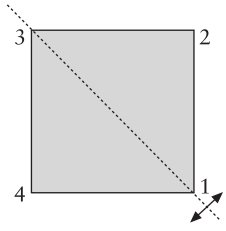
Bunlara ***döndürü*** denir. Döndürüler kümesine R diyelim:

$$R = \{\mathrm{Id}_4, r, r^2, r^3\}.$$

R'nin bileşke altında kapalı olduğuna dikkat edelim. Mesela $r^3 r = r^4 = \mathrm{Id}_4$ ve $r^2 r^3 = r^5 = r$ olur. Ayrıca r'deki her elemanın bir tersi vardır ve bu ters de R'dedir:

$$r^{-1} = r^3,\ (r^2)^{-1} = r^2,\ (r^3)^{-1} = r.$$

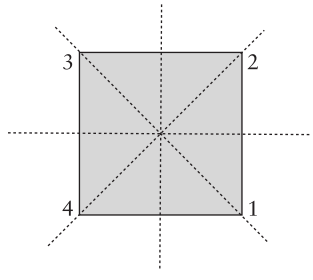
Yani R bir gruptur. (Bunu Teorem 5.1'ten de biliyoruz.) Bir başka deyişle $R \leq G$ olur.
Bu dört dönüşümü gerçekleştirmek için düzlemden çıkmaya gerek yok, kareyi düzlemde kalarak döndürebiliriz.
Bu dört dönüşüm dışında karenin dört simetrisi daha vardır. Bunlardan biri aşağıdaki noktalı eksene göre ayna görüntüsüdür.



Köşelere odaklanırsak, bu dönüşümü

$$s = (2\ 4)$$

permütasyonu olarak yazabiliriz. Bu tür simetrilere ***yansıma*** adı verilir.
Yansımaları kareyi eğip bükmeden ve düzlemin dışına çıkarmadan fiziksel olarak gerçekleştiremeyiz. Yansımaları fiziksel olarak gerçekleştirmek için üçüncü boyutu kullanarak kareyi kaldırıp ters çevirip tekrar düzleme yatırmak gerekir.
Karenin yukardaki eksen gibi üç simetri ekseni daha vardır (toplamda dört tane yani).



Örneğin karenin ortasından dikey inen doğru da bir simetri eksenidir; karenin bu eksene göre simetrisini alırsak (1 2)(3 4) yansımasını buluruz. Karenin tüm yansımaları şöyle:

$$(2\ 4) = s,$$
$$(1\ 2)(3\ 4),$$
$$(1\ 4)(2\ 3),$$
$$(1\ 3).$$

Bir yansımayı kareye iki defa peşpeşe uygularsak özdeşlik fonksiyonu Id_4'ü buluruz; yani yansımaların derecesi 2'dir. Dolayısıyla yansımaların her biri Id_4 ile birlikte bir grup oluşturur. (Bu kadar basit bir şey için Teorem 5.1'i uygulamaya gerek yok) Örneğin

$$S = \{\mathrm{Id}_4, s\}$$

bir gruptur, yani $S \leq G$ olur. Ama iki yansımanın bileşkesi yansıma değildir. Kontrol edildiği zaman görüleceği ve aşağıda da göreceğimiz üzere iki yansımanın bileşkesi yukarıdaki dört döndürüden biridir.
s'yi teker teker R'nin dört elemanıyla (soldan ya da sağdan) çarparsak aynen yukarıda sıraladığımız 4 simetriyi elde ederiz:

$$s\,\mathrm{Id}_4 = s = (2\ 4) = \mathrm{Id}_4\, s$$
$$sr = (2\ 4)(1\ 2\ 3\ 4) = (1\ 4)(2\ 3) = r^3 s$$
$$sr^2 = (2\ 4)(1\ 3)(2\ 4) = (1\ 3) = r^2 s$$
$$sr^3 = (2\ 4)(1\ 4\ 3\ 2) = (1\ 2)(3\ 4) = rs.$$

Böylece toplam 8 tane simetri bulduk. Bu simetrilerin kümesi D_8 olarak gösterilir.

$$D_8 = SR = RS = R \sqcup Rs = \{\mathrm{Id}_4, r, r^2, r^3, s, rs, r^2 s, r^3 s\}.$$

Nitekim $R \cap S = \{1\}$ olduğundan, Önsav 5.4'e göre RS'nin $|R||S| = 4 \times 2 = 8$ tane elemanı vardır. Ayrıca Önsav 5.2'ye göre D_8 kümesi bileşke işlemi altında kapalıdır, dolayısıyla Teorem 5.1'e göre bir gruptur, yani $D_8 \leq G$ olur. (Hâlâ daha G'nin tanımını bilmiyoruz! Ama tanımı her ne olursa olsun, bileşke altında bir grup olacak.) D_8 grubunun çarpım tablosunu çizelim. i'inci satırdaki elemanı soldan j'inci satırdaki elemanla çarparsak,

	Id_4	2	r^2	r^3	s	rs	$r^2 s$	$r^3 s$
Id_4	Id_4	r	r^2	r^3	s	rs	$r^2 s$	$r^3 s$
r	r	r^2	r^3	Id_4	rs	$r^2 s$	$r^3 s$	s
r^2	r^2	r^3	Id_4	r	$r^2 s$	$r^3 s$	s	rs
r^3	r^3	Id_4	r	r^2	$r^3 s$	s	rs	$r^2 s$
s	s	$r^3 s$	$r^2 s$	rs	Id_4	r^3	r^2	r
rs	rs	s	$r^3 s$	$r^2 s$	r	Id_4	r^3	r^2
$r^2 s$	$r^2 s$	rs	s	$r^3 s$	r^2	r	Id_4	r^3
$r^3 s$	$r^3 s$	s	rs	$r^2 s$	r^3	r^2	r	Id_4

çarpım tablosunu elde ederiz. Çarpım tablosu aslında şu üç kuralla belirlenmiştir:

$$r^4 = \mathrm{Id}_4,\ s^2 = \mathrm{Id}_4,\ sr = r^3 s.$$

Nitekim bu kuralları bilirsek, grupların birleşme özelliğini kullanarak, istediğimiz elemanla istediğimiz elemanı çarpabiliriz. Örneğin

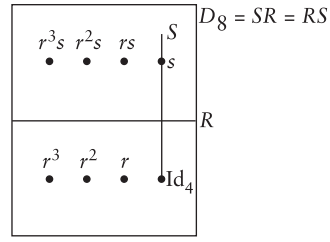
$$(r^2 s)(rs) = r^2(sr)s = r^2(r^3 s)s = r^5 s^2 = r^5 = r^4 r = r$$

ya da

$$rs(r^3) = r(sr)r^2 = r(r^3 s)r^2 = r^4(sr)r = r^4(r^3 s)r = r^7(sr) = r^7(r^3 s) = r^{10}s = r^2 s.$$

Bu grup 8 elemanlı ***dihedral grup*** olarak adlandırılır ve biraz önce de dediğimiz gibi D_8 olarak gösterilir.

Bir kareyi, bir eğriyi ya da genel olarak fiziksel bir nesneyi resmetmek kolaydır, fotoğrafı bile çekilebilir ama bir grubu resmetmek kolay değildir. Daha çok hareketi temsil ettiğinden, bir grubun her elemanının ancak filmi çekilebilir, bir grup da o zaman bir film arşivi olur! Bir kitapta bu mümkün olmadığından biz gene de grupların resmini çizmeye çalışacağız. D_8'i şöyle çizeceğiz:



Karenin başka simetrisi yoktur. Bunu kanıtlamak için simetrinin tanımını bilmemiz lazım. Çeşitli tanımlar verilebilir. Biz şu tanımı tercih edeceğiz: Karenin ***simetrisi*** köşelerin bir permütasyonudur, ama herhangi bir permütasyonu değil, bağlantılı köşeleri bağlantılı köşelere götüren bir permütasyonudur. Örneğin yukardaki notasyonla, karenin bir simetrisi, 1 köşesini 3 köşesine götürüyorsa, 2 köşesini ya kendisine ya da 4 köşesine götürmek zorundadır, çünkü 2 köşesi 1 köşesine bağlantılıdır; dolayısıyla 2'nin gittiği köşe, 1'in gittiği köşeye (örneğimizde 3 köşesine) bağlantılı olmak zorundadır.

Bu tanımla karenin yukarıdaki 8 simetriden başka simetrisi olmadığını kanıtlayalım.

G, karenin simetrilerinden oluşan küme olsun. G elbette $\mathrm{Sym}\,4$'ün bir altkümesidir ve D_8'i içerir. G'nin bileşke altında kapalı olduğu simetrinin tanımından belli. Sayfa xx'teki Teorem 5.1'e göre G bileşke işlemiyle birlikte bir gruptur.

Rastgele bir $g \in G$ alalım. Bu g elemanının D_8'in yukarıda sıraladığımız 8 permütasyonundan biri olduğunu kanıtlayacağız. Önce şu saptamayı yapalım: R'nin

$$r^0 = \mathrm{Id}_4,\ r,\ r^2,\ r^3$$

elemanları 1 köşesini sırasıyla 1, 2, 3 ve 4 köşesine götürür. Demek ki bir ve bir tek $i \in \{0, 1, 2, 3\}$ için

$$g(1) = r^i(1)$$

olur. (Aslında $i = g(1) - 1$ olur ama bunun bir önemi yok.) Şimdi $r^{-i}g$ permütasyonuna bakalım. Bu permütasyon da G'dedir, yani karenin bir simetrisidir, çünkü ne de olsa karenin simetrilerinin bileşkesidir. Ama en başta aldığımız g simetrisi 1'i rastgele bir köşeye götürürken, bu simetri 1'i 1'e götürür:

$$(r^{-i}g)(1) = 1.$$

Eğer tabiri caizse $r^{-i}g$ simetrisi g permütasyonundan daha evcildir. Şimdi $(r^{-i}g)(2)$ köşesine bakalım. 1 ile 2 köşeleri karede bağlantılı olduklarından, $(r^{-i}g)(1) = 1$ ile $(r^{-i}g)(2)$ köşeleri de bağlantılı olmalılar. Ama 1'e bağlantılı olan sadece 2 ve 4 köşeleri var. Demek ki

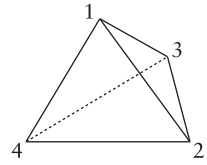
$$\text{ya } (r^{-i}g)(2) = 2 \text{ ya da } (r^{-i}g)(2) = 4.$$

Şimdi s'nin 1 köşesini sabitlediğini ve 2 ve 4 köşelerinin yerlerini değiştirdiğini gözlemleyelim. Eğer $(r^{-i}g)(2) = 2$ ise $r^{-i}g$ simetrisi 1 ve 2 noktalarını sabitler. Eğer $(r^{-i}g)(2) = 4$ ise, bu sefer $sr^{-i}g$ simetrisi 1 ve 2 noktalarını sabitler. Demek ki birinci durumda $s^0r^{-i}g$ simetrisi, ikinci durumda $s^1r^{-i}g$ simetrisi 1 ve 2 noktalarını sabitler. Bir ve bir tek $j \in \{0, 1\}$ için $s^jr^{-i}g$ simetrisinin 1 ve 2 noktalarını sabitlediğini gösterdik. Ve $s^jr^{-i}g$

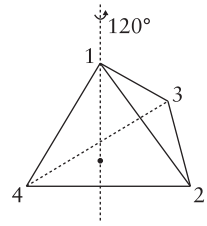
hâlâ daha karenin bir simetrisidir, yani hâlâ G'dedir. Son olarak 1 ve 2 noktalarını sabitleyen karenin bir simetrisinin özdeşlik fonksiyonu olması gerektiğini kanıtlayalım. Bunu kanıtlarsak, $s^j r^{-i} g = \mathrm{Id}_4$ ve dolayısıyla $g = r^i (s^j)^{-1} = r^i s^j \in D_8$ olur ve istediğimiz kanıtlanmış olur.

$t \in G$ simetrisi 1 ve 2 noktalarını sabitlesin. 2 ve 3 noktaları bağlantılı olduklarından, $t(3)$ noktası $t(2) = 2$ noktasına bağlantılı olmalıdır. Demek ki ya $t(3) = 1$ ya da $t(3) = 3$. Ama zaten $t(1) = 1$. Demek ki $t(3) = 1$ olamaz ve $t(3) = 3$ olmalı. Şimdi t simetrisi 1, 2 ve 3 noktalarını sabitliyor. Geriye kalan son noktanın kendisinden başka gidecek yeri kalmamıştır. Böylece $t = \mathrm{Id}_4$ ve $G = D_8$ eşitlikleri kanıtlanmış oldu. □

6.2. **Üçgen Tabanlı Piramidin Simetrileri.** Bu sefer üç boyutlu bir nesne alalım: Üçgen tabanlı düzgün piramit.



Köşelerden birinden, diyelim 1 noktasından, bu noktanın karşısındaki yüzeye dik bir doğru geçirelim. Bu doğruyu eksen kabul eden 120 derecelik bir döndürü vardır ve bu döndürü elbette piramitin bir simetrisidir. Bu döndürüyü r_1 olarak gösterelim.



Şekilden de görüleceği üzere, köşelere odaklanırsak, $r_1 = (2\ 3\ 4)$ olur. r_1'in kendisiyle bileşkesini alabiliriz:

$$r_1 = (2\ 3\ 4),\ r_1^2 = (2\ 4\ 3),\ r_1^3 = \mathrm{Id}_4\,.$$

Aynen bu r_1 gibi, r_2, r_3, r_4 simetrilerini de bulabiliriz:

$$r_2 = (1\ 4\ 3),\ r_3 = (1\ 2\ 4),\ r_4 = (1\ 3\ 2).$$

Böylece toplam 9 tane simetri bulduk: Id_4 ve

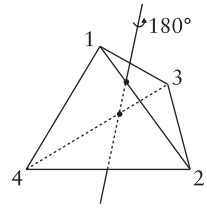
$$\begin{array}{ll} r_1 = (2\ 3\ 4), & r_1^2 = (2\ 4\ 3), \\ r_2 = (1\ 4\ 3), & r_2^2 = (1\ 3\ 4), \\ r_3 = (1\ 2\ 4), & r_3^2 = (1\ 4\ 2), \\ r_4 = (1\ 3\ 2), & r_4^2 = (1\ 2\ 3). \end{array}$$

Çok daha fazlasını bulacağız. Şimdilik, $i = 1, 2, 3, 4$ için

$$R_i = \{\mathrm{Id}_4,\ r_i,\ r_i^2\}$$

tanımını yapalım. R_i, bileşke işlemi altında bir gruptur.

Başka simetriler bulmaya çalışalım. Kesişmeyen iki kenarın orta noktalarını birleştiren doğruyu alalım. Piramiti bu doğru etrafında 180 derece döndürebiliriz.



Şekildeki döndürüyü yaparsak

$$a_2 = (1\ 2)(3\ 4)$$

permütasyonunu buluruz. Bunun gibi iki tane daha vardır. Her birini yazalım:

$$\begin{aligned} a_2 &= (1\ 2)(3\ 4),\\ a_3 &= (1\ 3)(2\ 4),\\ a_4 &= (1\ 4)(2\ 3). \end{aligned}$$

Şimdi çok tuhaf bir şey söyleyeceğim:

$$A = \{\mathrm{Id}_4,\ a_2,\ a_3,\ a_4\}$$

kümesi bileşke işlemiyle birlikte bir grup olur. (Bu tuhaf olgu sadece 4 sayısına özgüdür.) Hatta abelyen bir grup olur. Okur bunu kolaylıkla kontrol edebilir ama biz de kontrol edelim:

$$a_2a_3 = [(1\ 2)(3\ 4)][(1\ 3)(2\ 4)] = (1\ 4)(2\ 3) = a_4.$$

Benzer eşitlik diğerleri için de geçerlidir:

$$\begin{aligned} a_2a_3 &= a_3a_2 = a_4,\\ a_2a_4 &= a_4a_2 = a_3,\\ a_3a_4 &= a_4a_3 = a_2. \end{aligned}$$

Ayrıca A kümesinin her elemanı kendisinin tersidir. Ve

$$A \cap R_1 = \{\mathrm{Id}_4\}$$

olur. Nitekim Önsav 5.4'e göre $|AR_1| = |A||R_1| = 4 \times 3 = 12$ olmalıdır. AR_1 kümesinin elemanları şimdiye kadar bulduğumuz

$$\mathrm{Id}_4,\ r_1,\ r_1^2,\ r_2,\ r_2^2,\ r_3,\ r_3^2,\ r_4,\ r_4^2,\ a_2, a_3, a_4.$$

elemanlarıdır. Gerçekten de,

$$\begin{aligned} a_2r_1 &= (1\ 2)(3\ 4)(2\ 3\ 4) = (1\ 2\ 4) = r_3, & a_2r_1^2 &= (1\ 2)(3\ 4)(2\ 4\ 3) = (1\ 2\ 3) = r_4^2,\\ a_3r_1 &= (1\ 3)(2\ 4)(2\ 3\ 4) = (1\ 3\ 2) = r_4, & a_3r_1^2 &= (1\ 3)(2\ 4)(2\ 4\ 3) = (1\ 3\ 4) = r_2^2,\\ a_4r_1 &= (1\ 4)(2\ 3)(2\ 3\ 4) = (1\ 4\ 3) = r_2, & a_4r_1^2 &= (1\ 4)(2\ 3)(2\ 4\ 3) = (1\ 4\ 2) = r_3^2 \end{aligned}$$

eşitliklerinden

$$AR_1 = A \sqcup Ar_1 \sqcup Ar_1^2 = \{\mathrm{Id}_4,\ r_1,\ r_1^2,\ r_2,\ r_2^2,\ r_3,\ r_3^2,\ r_4,\ r_4^2,\ a_2,\ a_3,\ a_4\}$$

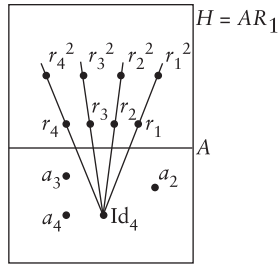
eşitliğini buluruz. Bu kümeye H adını verelim:

$$H = AR_1 = \{\mathrm{Id}_4,\ r_1,\ r_1^2,\ r_2,\ r_2^2,\ r_3,\ r_3^2,\ r_4,\ r_4^2,\ a_2,\ a_3,\ a_4\}.$$

Benzer şekilde $R_1A = H$ eşitliğini kanıtlayabiliriz:

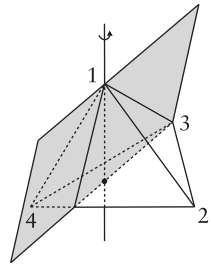
$$\begin{aligned} r_1a_2 &= (2\ 3\ 4)(1\ 2)(3\ 4) = (1\ 3\ 2) = r_4, & r_1^2a_2 &= (2\ 4\ 3)(1\ 2)(3\ 4) = (1\ 4\ 2) = r_3^2,\\ r_1a_3 &= (2\ 3\ 4)(1\ 3)(2\ 4) = (1\ 4\ 3) = r_2, & r_1^2a_3 &= (2\ 4\ 3)(1\ 3)(2\ 4) = (1\ 2\ 3) = r_4^2,\\ r_1a_4 &= (2\ 3\ 4)(1\ 4)(2\ 3) = (1\ 2\ 4) = r_3, & r_1^2a_4 &= (2\ 4\ 3)(1\ 4)(2\ 3) = (1\ 3\ 4) = r_2^2. \end{aligned}$$

Demek ki Önsav 5.2'ye göre H bileşke altında kapalıdır ve Teorem 5.1'e göre bir gruptur. Şekli aşağıda



H'nin her elemanının piramitin bir simetrisi olduğunu biliyoruz. (Simetriyi bir önceki örnekteki gibi tanımlıyoruz.) Yani eğer G piramitin simetrilerinden oluşan grupsa, $H \leq G$ olur.

Piramitin daha fazla simetrisi vardır, ama diğerleri piramidi eğip bükmeden üç boyutlu uzayda fiziksel olarak gerçekleştirilemezler. Nitekim piramitin karşılıklı iki kenarından birini içeren, diğerinin orta noktasından geçen düzleme göre simetrisini (ayna görüntüsünü) alabiliriz.



Yukarıdaki şekildeki örnekte

$$t = (1\ 4)$$

simetrisini elde ederiz. $t^2 = \mathrm{Id}_4$ olur elbette. Her ne kadar t dönüşümü üç boyutlu uzayda gerçekleştirilemiyorsa da, t piramitin bir simetrisidir, ama H'de değildir (çünkü t dönüşümü sağı sol, solu sağ yapar, oysa uzayda istediğiniz kadar dolaşın sağınız solunuza, solunuz sağınıza gelmez).

$T = \{\mathrm{Id}_4, t\}$ olsun. T bir gruptur ve $H \cap T = \{\mathrm{Id}_4\}$ olur. Demek ki Önsav 5.4'e göre

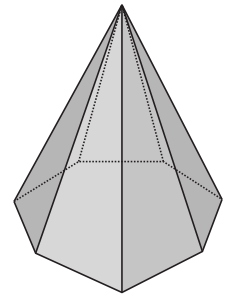
$$|HT| = |H| \times |T| = 12 \times 2 = 24$$

olur. Ama $HT \subseteq \mathrm{Sym}\,4$ ve her ikisinin de 24 elemanı var. Demek ki

$$G = HT = \mathrm{Sym}\,4.$$

H'nin elemanları sağı solu koruduğundan, t ise sağı sol yaptığından, Ht kümesinin elemanları sağı sol yaparlar, dolayısıyla üç boyutlu uzayda çekip çekiştirmeden gerçekleştirilemezler. H'nin elemanları (12 tane) uzayda gerçekleştirilebilirler. İleride H'nin $\mathrm{Alt}\,4$ olarak adlandırıldığını göreceğiz.

6.3. **Piramitin Simetrileri.** Bu sefer tabanı düzgün n-gen olan bir dik piramit alalım. $n = 3$ durumunu yukarda görmüştük. Şimdi $n > 3$ durumuna bakalım.



Tabandaki noktaların üç bağlantısı vardır; yani ***dereceleri*** 3'tür. Oysa tepe noktasının derecesi n'dir. Tepe noktası derecesi n olan yegâne nokta olduğundan, her simetri tepe noktasını tepe noktasına götürmek zorundadır. Dolayısıyla eğer istersek tepe noktasını unutup düzgün bir n-gen olan tabanın simetrilerine odaklanabiliriz. (Tabanın her simetrisi piramitin bir simetrisine genişletebilir ve piramitin her simetrisi tabanın bir simetrisini verir.)

Bildiğimiz simetrileri yazalım. Öncelikle tepe noktasını sabitleyen döndürüler var. Eğer r en küçük pozitif açılı döndürüyse, toplam n tane döndürü elde ederiz:

$$R = \{1, r, r^2, \ldots, r^{n-1}\}.$$

Bunların dışında bir de tabanın farklı eksenlere göre ayna simetrileri vardır. Bunlardan da tam n tane vardır, ama eğer s bunlarsan biriyse, Rs kümesi tüm ayna simetriler kümesidir. Piramitin simetriler grubu

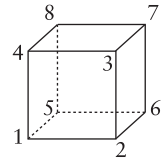
$$D_{2n} = R \sqcup Rs$$

dir ve bu simetrilerin sadece yarısı (R'deki döndürüler) üç boyutlu uzayda gerçekleştirilebilir. Bunun böyle olduğunun kanıtını okura bırakıyoruz. Çarpım tablosu da

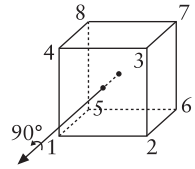
$$r^n = \mathrm{Id},\ s^2 = \mathrm{Id} \ \text{ ve } sr = r^{n-1}s$$

eşitlikleri tarafından belirlenir. D_{2n} grubuna, $2n$ elemanlı ***dihedral grup*** adı verilir.

6.4. **Küpün Simetrileri.** Köşelerini aşağıdaki şekildeki gibi 1'den 8'e kadar adlandırdığımız küpün simetrilerini bulacağız.



Küpü bize doğru gelen eksen üzerinde saatin ters yönünde 90 derece döndürebiliriz.



Bu dönüşüme r diyelim. Köşeler r altında şöyle dönüşür:

$$r = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8).$$

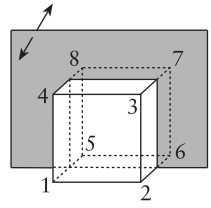
Tabii r'nin kuvvetlerini alırsak,

$$\begin{aligned} r^0 &= \mathrm{Id}_8 \\ r^1 &= r = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) \\ r^2 &= (1\ 3)(2\ 4)(5\ 7)(6\ 8) \\ r^3 &= (1\ 4\ 3\ 2)(5\ 8\ 7\ 6) \end{aligned}$$

buluruz. $r^4 = \mathrm{Id}_8$ olur.

$$R = \{\mathrm{Id}_8,\ r,\ r^2,\ r^3\}$$

olsun. R bileşke işlemi altında bir gruptur.
Bir de ön yüzle arka yüzü ayna görüntüsü sayesinde değiştirebiliriz.



Bu dönüşümü s olarak gösterelim:

$$s = (1\ 5)(2\ 6)(3\ 7)(4\ 8).$$

Tabii $s^2 = \mathrm{Id}_8$ olur.

$$S = \{\mathrm{Id}_8,\ s\}$$

olsun. S de bileşke işlemi altında bir gruptur. Ama RS de bir gruptur. Nitekim,

$$srs = (1\ 5)(2\ 6)(3\ 7)(4\ 8)(1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(1\ 5)(2\ 6)(3\ 7)(4\ 8) = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) = r$$

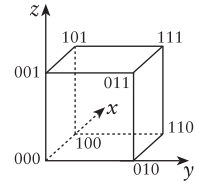
olduğundan,

$$sr = rs$$

olur ve Teorem 5.2'e göre RS bir gruptur, hatta değişmeli bir gruptur. RS grubunun tam 8 elemanı vardır:

$$\begin{aligned} &\mathrm{Id}_8 \\ &r = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) \\ &r^2 = (1\ 3)(2\ 4)(5\ 7)(6\ 8) \\ &r^3 = (1\ 4\ 3\ 2)(5\ 8\ 7\ 6) \\ &s = (1\ 5)(2\ 6)(3\ 7)(4\ 8) \\ &rs = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(1\ 5)(2\ 6)(3\ 7)(4\ 8) = (1\ 6\ 3\ 8)(2\ 7\ 4\ 5) \\ &r^2s = (1\ 3)(2\ 4)(5\ 7)(6\ 8)(1\ 5)(2\ 6)(3\ 7)(4\ 8) = (1\ 7)(2\ 8)(3\ 5)(4\ 6) \\ &r^3s = (rs)^{-1} = (1\ 8\ 3\ 6)(2\ 5\ 4\ 7) \end{aligned}$$

RS'nin 8 tane elemanı olduğu sayfa xx'teki Önsav 5.4'ten de belli.
Dikkat ederseniz $i = 1, \ldots 8$ verilmişse, 1 köşesini i köşesine götüren bir ve bir tane $g \in RS$ var. Mesela 1'i 6'ya sadece $rs \in RS$ götürüyor, 1'i 1'e sadece $\mathrm{Id}_8 \in RS$ götürüyor.
Yukarıda yaptıklarımızı aklımızın bir kçşesinde tutup küpün başka simetrilerini bulmak amacıyla yola koyulalım. Bunu yapmak için küpün köşelerini 1, 2 gibi sayılarla değil, aşağıdaki gibi 0 ve 1 üçlüleriyle gösterelim.



Dikkat ederseniz iki köşenin birbiriyle bağlantılı olması için yeter ve gerek koşul iki köşenin sadece tek bir teriminin farklı olmasıdır. Örneğin 010 ile 011 bağlantılıdır, çünkü sadece son terimleri farlıdır. Bunun gibi 110 ile 100 bağlantılıdır ama 010 ile 001 bağlantılı değildir. Hatta iki noktanın farklı terim sayısı iki nokta arasındaki "***mesafedir***: 100 noktasından 011 noktasına gitmek için 3 kenardan geçmek gerekir, daha az kenardan geçerek gidemeyiz.

Bir önceki paragraftaki açıklamalardan dolayı, koordinatların yerlerini değiştirmek küpün bağlantılılık ilişkisini bozmaz. Örneğin, birinci ve ikinci koordinatların yerlerini değiştirirsek, küpün

$$\begin{array}{lcl} 000 & \mapsto & 000 \\ 001 & \mapsto & 001 \\ 010 & \mapsto & 100 \\ 011 & \mapsto & 101 \\ 100 & \mapsto & 010 \\ 101 & \mapsto & 011 \\ 110 & \mapsto & 110 \\ 111 & \mapsto & 111 \end{array}$$

dönüşümünü elde ederiz, ki bu dönüşüm bağlantılı noktaları bağlantılı noktalara, bağlantısız noktaları bağlantısız noktalara götürür Ya da birinci koordinatı ikinci koordinata, ikinci koordinatı üçüncü koordinata, üçüncü koordinatı birinci koordinata yollayabiliriz. O zaman,

$$\begin{array}{lcl} 000 & \mapsto & 000 \\ 001 & \mapsto & 100 \\ 010 & \mapsto & 001 \\ 011 & \mapsto & 101 \\ 100 & \mapsto & 010 \\ 101 & \mapsto & 110 \\ 110 & \mapsto & 011 \\ 111 & \mapsto & 111 \end{array}$$

dönüşümünü elde ederiz. Böylece, koordinatların her dönüşümü bize küpün bir simetrisini verir ve bunlardan da $3! = 6$ tane vardır, Sym 3'ün eleman sayısı kadar. Bu dönüşümlerin kümesine T adını verelim. T elbette bir gruptur. (Sym 3'e çok benzer.)

T'nin elemanlarının her biri 000 köşesini (yani yukarıdaki yazılımla 1 köşesini) sabitler. Daha önce bulduğumuz RS grubunun sadece Id_8 elemanı 1 köşesini sabitlediğinden $T \cap RS = \{\mathrm{Id}_8\}$ olur. Buradan da, Önsav 5.4'e göre, RST kümesinin $|RS| \times |T| = 8 \times 6 = 48$ elemanı olduğu çıkar.

Küpün RST'nin elemanlarından başka bir simetrisinin olmadığını kanıtlayalım. g, küpün herhangi bir simetrisi olsun. RS grubunun her elemanının 1 köşesini bir başka köşeye götürdüğünü anımsayalım. RS'de 1 köşesini $g(1)$ köşesine götüren bir ve bir tane a elemanı vardır. O zaman $a^{-1}g$ simetrisi 1 köşesini 1 köşesine götürür. Ama 1 köşesini 1 köşesine götüren her simetri T'de olmak zorundadır. (Neden?) Demek ki bir ve bir tane $t \in T$ için $a^{-11}g = t$, yani $g = at$ olur. Böylece küpün tüm simetrileri RST kümesindedir. Böylece küpün toplam 48 tane simetrisi olduğunu gördük.

Soru: Küpün köşelerini 01-üçlüleri olarak gösterelim. Her 0 koordinatını 1'e, her 1 koordinatını da 0'a dönüştüren simetri $G = RST$ grubunda nasıl yazılır?

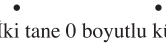
6.5. **[Dört Boyutlu Küpün Simetrileri.]** Önce dört boyutlu küpü tanımlayalım. Ama daha önce 0, 1, 2 ve 3 boyutlu küpün tanımlarına bir başka gözle bakalım.

0 boyutlu küp bir noktadan ibarettir. Çizmeyi gerek görmüyoruz.

1 boyutlu küpü $[0, 1]$ aralığı olarak görebiliriz. Köşe noktaları 0 ve 1'dir.



1 boyutlu küpü şöyle de gösterebiliriz: İki tane 0 boyutlu (yani iki nokta) alıp noktaları bir doğruyla birleştirmek.

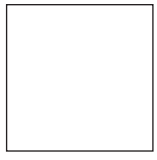


İki tane 0 boyutlu küp

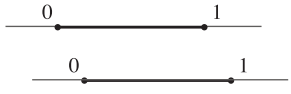


0 boyutlu küpler birleştirilerek
1 boyutlu küp elde ediliyor.

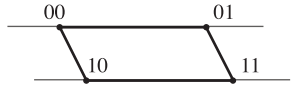
2 boyutlu küpü, köşeleri $(0, 0)$, $(1, 0)$, $(0, 1)$, $(1, 1)$ noktalarına gelecek biçimde yerleştirelim.



Bunu şöyle de gösterebiliriz. İki tane 1 boyutlu küple (yani iki tane $[0, 1]$ doğru parçasıyla) başlayalım. (Bkz. aşağıdaki soldaki şekil.) Sonra 1 boyutlu küplerden birinin koordinatlarının başına 0, diğerinin başına 1 getirelim ve birbirine tekabül eden noktalarını bir doğruyla birleştirelim. (Bkz. aşağıdaki sağdaki şekil. Elde edilen şeklin bir kare olmaması sizi rahatsız etmesin, kare de yapabilirdik.)

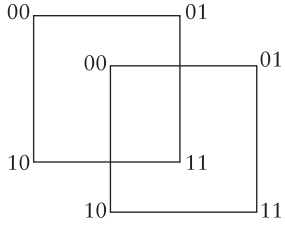


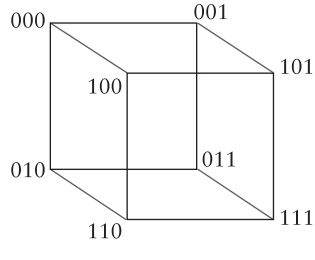
İki tane 1 boyutlu küp



1 boyutlu küpler birleştirilerek
2 boyutlu küp elde ediliyor.

3 boyutlu küpü, $\mathbb{R}^3$ uzayına yukardakine benzer şekilde, köşeler i, j, $k = 0, 1$ için (i, j, k) ya da daha basit olarak ijk noktalarına gelecek şekilde yerleştirelim. (Aşağıdaki sağdaki şekil.) Eğer iki noktanın üç koordinatından sadece biri değişikse, köşeler arasına bir kenar çiziyoruz.

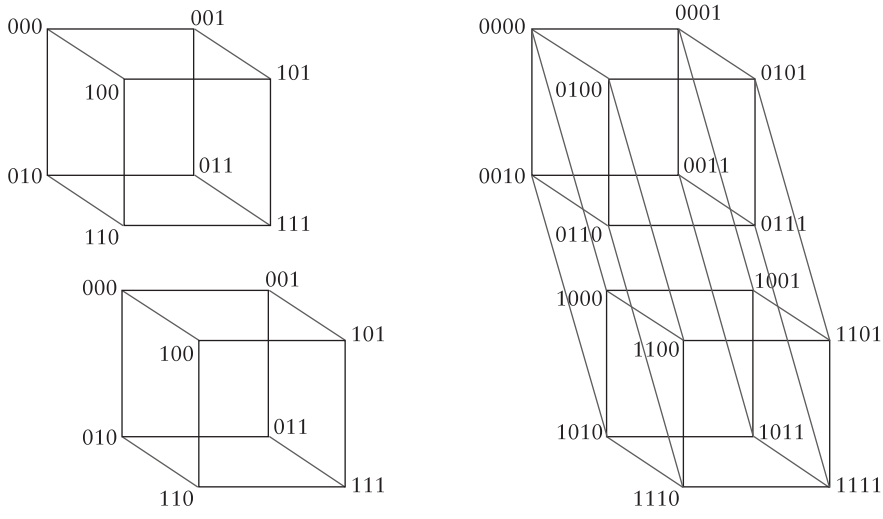




Bunu şöyle de gösterebiliriz. İki tane 2 boyutlu küple (yani iki tane kareyle) başlayalım. (Bkz. yukarıdaki soldaki şekil.) Sonra 2 boyutlu küplerden birinin koordinatlarının

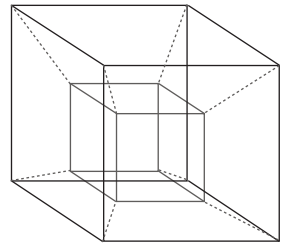
başına 0, diğerinin başına 1 getirelim ve birbirine tekabül eden noktalarını bir doğruyla birleştirelim. (Bkz. yukarıdaki sağdaki şekil.)

Şimdi 4 boyutlu küpü betimleyebiliriz. İki tane üç boyutlu küp alalım. Bunlardan birinin koordinatlarının başına 0, diğerinin başına 1 getirelim ve küplerin birbirine tekabül eden köşelerini bir kenarla birleştirelim.



İki tane 3 boyutlu küpten bir tane 4 boyutlu küp elde edilir.

Dikkat ederseniz, iki nokta sadece tek bir koordinatta ayrışıyorsa birbiriyle bağlantılıdır. Böylece geometriyi cebirselleştirmiş olduk.



Daha estetik bir 4 boyutlu küp

Dört boyutlu küpe K adını verelim. K'nın simetrilerini bulalım. K'nın simetrilerinden oluşan gruba G adını verelim.

K'nın başında 0 olan noktaları üç boyutlu bir küp oluştururlar. Bu küpe K_0 diyelim. Başında 1 olanlara da K_1 diyelim.

Bir önceki örnekte bulduğumuz üç boyutlu küpün RS simetrilerini ele alalım. Anımsarsanız RS, 8 elemanlı bir gruptu ve üç boyutlu küpün herhangi bir noktasını RS'nin elemanlarıyla üç boyutlu küpün herhangi bir noktasına götürebiliyorduk. Eğer RS'deki simetrileri **aynı anda** K_0 ve K_1 küplerine uygularsak (birinci koordinata dokunmadan), K'nın simetrilerini buluruz. K'nın bu simetri grubuna da üç boyutlu küpte olduğu gibi RS adını verelim.

Bir de K_0 ile K_1 değiştokuş eden bir t ayna simetrisi bulalım. Mesela t, noktaların birinci koordinatını değiştirsin, 0 ise 1, 1 ise 0 yapsın. $t^2 = \mathrm{Id}_{16}$ olduğundan, $T = \{\mathrm{Id}_{16}, t\}$

kümesi bir gruptur. $RS \cap T = \{Id_{16}\}$ olduğundan, $|RST| = |RS| \times |T| = 8 \times 2 = 16$ olur. Ayrıca RST kümesinin, K'nın herhangi bir noktasını istediğimiz herhangi bir noktasına götürecek bir ve bir tane elemanı vardır. Aslında kolay bir hesapla görüleceği üzere RST değişmeli bir gruptur.

Yukarıdaki paragrafta bulunan RST simetrileri dışında, K'nin dört koordinatını karan ve bu yüzden Sym 4'e çok çok benzeyen bir simetri grubu vardır. Bu simetri grubuna U adını verelim: mesela $\sigma = (1\ 2\ 3)$ permütasyonuysa, $\sigma(i,j,k,\ell) = (k,i,j,\ell)$ olur, ya da $\sigma = (1\ 2)(3\ 4)$ permütasyonuysa, $\sigma(i,j,k,\ell) = (j,i,\ell,k)$ olur.

U'nun her elemanı $(0,0,0,0)$ noktasını sabitlediğinden, ama RST'nin sadece Id_{16} elemanı bu noktayı sabitlediğinden, $RST \cap U = \{\mathrm{Id}_{16}\}$ olur. Buradan da $|RSTU| = |RST| \times |U| = 16 \times 4! = 2^4 \times 4!$ çıkar.

Ayrıca U'nun elemanları $A_1 = (1,0,0,0)$, $A_2 = (0,1,0,0)$, $A_3 = (0,0,1,0)$, $A_4 = (0,0,0,1)$ elemanlarını birbirine götürür, hatta U'nun elemanları bu noktalara olan etkileriyle betimlenirler.

Böylece, $RSTU \subseteq G$ olduğundan, G'nin $16 \times 4!$ tane elemanını bulduk. Şimdi $G = RSTU$ eşitliğini kanıtlayalım. $g \in G$ rastgele bir eleman olsun. RST grubunda,

$$g(0,0,0,0) = a(0,0,0,0)$$

eşitliğini sağlayan bir ve bir tane a elemanı vardır. Şimdi $a^{-1}g$ elemanı $(0,0,0,0)$ noktasını sabitler. Ve bu yüzden de K'nın dört eksenini birbirine dönüştürür. U grubunda, eksenleri ya da (aynı şey) A_1, A_2, A_3, A_4 noktalarını aynen $a^{-1}g$ elemanı gibi dönüştüren bir σ elemanı vardır. Demek ki, G'nin $\sigma^{-1}a^{-1}g$ elemanı $(0,0,0,0)$ ve A_1, A_2, A_3, A_4 noktalarını sabitler. Böyle bir eleman tüm noktaları sabitlemek, yani Id_{16}'ya eşit olmak zorundadır. Nitekim bu eleman A_1 ve A_2 noktalarını sabitlediğinden, bu noktalara komşu olan

$$(0,0,0,0) \text{ ve } (1,1,0,0)$$

noktalarını birbirine götürmek zorundadır. Ama $(0,0,0,0)$ noktasını zaten kendine götürüyor, demek ki $(1,1,0,0)$ noktasını da kendine götürmek zorundadır. Bu fikri devam ettirirsek, $\sigma^{-1}a^{-1}g$ elemanının K'nın tüm noktalarını sabitlediği, yani Id_{16} olduğu anlaşılır. Demek ki $\sigma^{-1}a^{-1}g = \mathrm{Id}_{16}$ ve $g = a\sigma \in RSTU$.

Soru: Küpün köşelerini 01-üçlüleri olarak gösterelim. 0 koordinatını 1'e, 1 koordinatını da 0'a dönüştüren simetri $G = RST$ grubunda nasıl yazılır?

6.6. n boyutlu küpü

$$K_n = \{(\delta_1, \ldots, \delta_n) : \text{her } i \text{ için } \delta_i = 0,\ 1\}$$

olarak tanımlayabiliriz. Eğer küpü, küpün içini de içerecek biçimde tanımlamak istersek,

$$K_n = \{(\delta_1, \ldots, \delta_n) : \text{her } i \text{ için } \delta_i \in [0,\ 1]\}$$

tanımını yapabiliriz. Bizim için hangi tanımın kabul edildiği farketmeyecek. Fikirleri sabitemek amacıyla birincisini kabul edelim. Eğer iki noktanın sadece bir koordinatı değişikse, bu noktalar arasında bir bağlantı olsun. (Bağlantılar küpün kenarlarıdır.) K_n'nin $2^n \times n!$ tane simetrisi vardır. Bu, aynen yukarıdaki iki örnekteki yöntemle gösterilebilir. Ama bunların hepsi n boyutlu uzayı eğip bükmeden gerçekleşmez, bazıları ayna simetrileridir. Sadece yarısı n-boyutlu uzaydan çıkmadan gerçekleştirilebilir.

6.7. $\prod_\omega \{0,1\}$ ve $\bigoplus_\omega \{0,1\}$ kümelerinden de bir nevi sonsuz boyutlu küp elde edilebilir. İki köşenin (noktanın yani) bağlantılı olması demek, tek bir koordinatın farklı olması demektir. Bu küplerin de simetri grupları vardır. Ama bu sefer simetriyi biraz farklı tanımlamak gerekebilir. Daha önce simetriyi

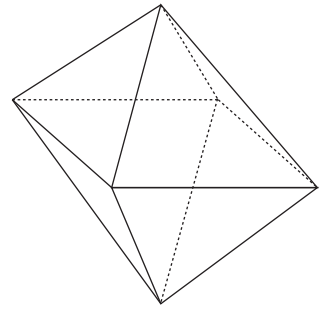
$$A \text{ ile } B \text{ köşeleri bağlantılıysa, } f(A) \text{ ile } f(B) \text{ köşeleri de bağlantılıdır}$$

koşulunu sağlayan köşelerin bir f permütasyonu olarak tanımlanmıştık. Bu sefer,

$$A \text{ ile } B \text{ köşelerinin bağlantılı olması için,}$$
$$f(A) \text{ ile } f(B) \text{ köşelerinin bağlantılı olmaları yeter ve gerektir}$$

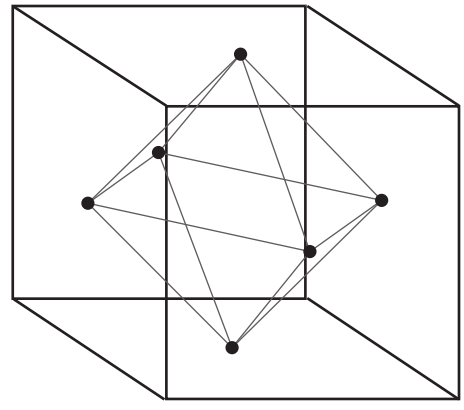
koşulunu sağlayan köşelerin bir f permütasyonu olarak tanımlamak gerekir, ki eğer f bir simetriyse, f^{-1} de bir simetri olsun. (Ama bu özelliğin sağlanması için eski tanım da yeterli olabilir. Bu cümleden de anlaşılacağı üzere sonsuz boyutlu küplerin simetri grubu hakkında bu yazarın bir bilgisi bulunmamaktadır.)

6.8. **[Oktahedronun Simetrileri.]** Oktahedron, aşağıdaki 6 köşeli, 12 kenarlı, 8 yüzeyli düzgün cisimdir.



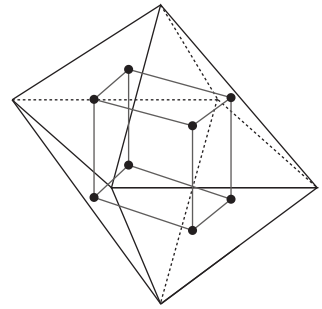
Küpün örneğinde olduğu gibi köşeleri değil de, yüzeyleri birbirine dönüştüren 8 elemanlı bir simetri grubu bulmak zor değildir. Mesela dikey eksen etrafında döndürülerle, yatay düzleme göre ayna simetrisi böyle bir grup verir. Bu grup sayesinde oktahedronun tam $8 \times 3! = 48$ tane simetrisi olduğunu göstermek zor değildir. Okur alıştırma olarak bunu göstermelidir. Biz burada bir başka yöntem kullanacağız.

Üç boyutlu küpün her yüzeyinin ağırlık noktasını alıp, komşu yüzeylerin ağırlık merkezlerini birleştirirsek bir oktahedron elde ederiz.



Bu sayede küpün her simetrisinin oktahedronun bir simetrisine yol açtığını gözlemleyebiliriz. Nitekim küpün bir σ simetrisini ve bir $ABCD$ yüzeyini alalım. σ mesafesi 2 olan A ve C köşelerini mesafesi 2 olan $\sigma(A)$ ve $\sigma(C)$ köşelerine götürür. Dolayısıyla A ve C köşelerinin ortak komşuları olan B ve C köşelerini $\sigma(A)$ ve $\sigma(B)$ köşelerinin ortak komşularına götürür. Demek ki σ simetrisi küpün $ABCD$ yüzeyini gene küpün bir başka yüzeyine, $\sigma(A)\sigma(B)\sigma(C)\sigma(D)$ yüzeyine götürür. Dolayısıyla σ simetrisi küpün $ABCD$ yüzeyinin orta noktasını $\sigma(A)\sigma(B)\sigma(C)\sigma(D)$ yüzeyinin orta noktasına götürür, yani küpün içine çizilen oktahedronu gene oktahedrona götürür.

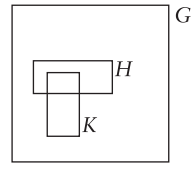
Nasıl küpten oktahedron elde etmişsek, oktahedrondan da benzer şekilde bir küp elde ederiz.



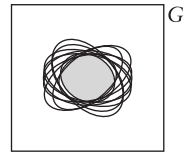
Aynen yukarıdaki yaptığımız gibi oktahedronun her simetrisinin küpün bir simetrisini verdiği kanıtlanabilir. Dolayısıyla oktahedronun simetri grubuyla 3 boyutlu küpün simetri grubu aynıdır.

7. Üreteçler

Bir grupta iki altgrubun kesişimi gene bir gruptur. Bunun kanıtı çok basittir: H ve K iki altgrup olsun. 1 elemanı her iki altgrupta da olduğundan kesişimdedir de. Eğer xK kesişimdeyse, x elemanı hem H'de hem de K'da olduğundan, x'in tersi, yani x^{-1} elemanı hem H'de hem de K'dadır; demek ki $x^{-1} \in H \cap K$ olur. Şimdi kesişimden iki eleman alalım: x ve y. Bu elemanlar hem H'de hem de K'da olduklarından çarpımı olan xy de hem H'de hem de K'dadır. Demek ki xy kesişimdedir. Böylece $H \cap K$ kesişimin bir altgrup olduğu kanıtlanmış oldu.



Dikkat ederseniz yukarıdaki akıl yürütme sadece iki altgrubun değil, kaç tane olursa olsun, isterse sonsuz sayıda olsun, altgrupların kesişiminin de bir altgrup olduğunu gösteriyor. Yani bir grupta, herhangi bir altgruplar kümesinin kesişimi bir altgruptur.



Şimdi X, bir G grubunun herhangi bir altkümesi olsun. X'i içeren en az bir altgrup vardır: G. Bu altkümeyi içeren **tüm** altgrupları kesiştirelim. Bu kesişimin bir altgrup olduğunu biliyoruz. Ayrıca kesişim X'i de içerir tabii ki. Demek ki X'i içeren tüm algrupların kesişimi gene X'i içeren bir altgruptur. Dolayısıyla bu kesişim X'i içeren en küçük altgrup olmak zorundadır. Şu sonucu kanıtladık:

Teorem 7.1. *G bir grup ve $X \subseteq G$ olsun. X'i içeren tüm altgrupların kesişimi X'i içeren en küçük altgruptur.* □

X'i içeren en küçük altgrubu $\langle X\rangle$ olarak gösterelim. Eğer $X = \{x_1, \ldots, x_n\}$ sonluysa, $\langle\{x_1, \ldots, x_n\}\rangle$ yerine $\langle x_1, \ldots, x_n\rangle$ yazılır. Ve eğer $X, Y \subseteq G$ ise, $\langle X \cup Y\rangle$ yerine $\langle X, Y\rangle$ yazılır. Benzer kısaltmaları yapmakta kendimizi kısıtlamayacağız.

$$\langle X\rangle = \bigcap_{X\subseteq H\leq G} H$$

eşitliğini biliyoruz. Ayrıca eğer $X \subseteq H \leq G$ ise $\langle X\rangle \leq H$ içindeliğini de biliyoruz.

Eğer $X = \emptyset$ ya da $X = \{1\}$ ise $\langle X\rangle = 1$ olur[1]. $\langle G\rangle = G$ eşitliği de kolay. $\langle G \setminus \{1\}\rangle = G$ eşitliğinin kanıtını da okura bırakıyoruz.

Yukarıdaki teorem uygulamada pek yararlı olmayabilir, çünkü teorem bize X'i içeren en küçük altgrubun olduğunu söylüyor ama altgrubun neye benzediğini söylemiyor. Şimdi $\langle X\rangle$ altgrubunun neye benzediğini biraz daha somut olarak görelim.

$x, y \in X$ ise, $xy \in \langle X\rangle$ olduğunu biliyoruz. Bunun gibi

$$xy^{-1},\ x^2,\ y^{-3},\ xyx,\ yx^{-1}y^{-2} \in \langle X\rangle$$

içindelikleri de biliyoruz. Daha da genel olarak, $x_1, \ldots, x_n \in X$ ve $\epsilon_1, \ldots, x_n = \pm 1$ ise,

$$x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \in \langle X\rangle$$

olur. Demek ki,

$$\{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} : n \in \mathbb{N},\ x_i \in X,\ \epsilon_i = \pm 1\} \subseteq \langle X\rangle$$

olur[2]. Ama sol taraftaki küme X'i içeriyor (tanımda $n = 1$ ve $\epsilon_1 = 1$ alın) ve ayrıca bir altgrup (çünkü çarpma altında kapalı, elemanlarının tersi de kümenin içinde ve elbette 1'i içeriyor[3]). Bundan ve $\langle X\rangle$ altgrubunun X'i içeren en küçük altgrup olmasından eşitlik çıkar:

$$\langle X\rangle = \{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} : n \in \mathbb{N},\ x_i \in X,\ \epsilon_i = \pm 1\}.$$

Bu yüzden $\langle X\rangle$ altgrubuna X ***tarafından üretilen altgrup*** adı verilir ve X'e de ***üreteç kümesi*** denir.

$$\langle X\rangle = \{x_1^{k_1} \cdots x_n^{k_n} : n \in \mathbb{N},\ x_i \in X,\ k_i \in \mathbb{Z}\}$$

eşitliğini okur gözden kaçırmamalıdır. Bu tür bir yazılımla x_i ile x_{i+1} elemanlarının birbirinden farklı olduklarını varsayabiliriz.

[1] Buradaki 1, {1} altgrubu anlamına geliyor.

[2] Dikkat: Tanımdaki $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ ifadesinde X'in aynı elemanı tekrar edebilir.

[3] Eğer $X \neq \emptyset$ ise, X'ten bir x seçelim ve tanımda $n = 2$, $x_1 = x_2 = x$ ve $\epsilon_1 = 1$, $\epsilon_2 = -1$ alalım; $1 = xx^{-1}$ olur. Eğer $X = \emptyset$ ise, tanımda $n = 0$ olsun, G'nin hiç tane elemanının çarpımı 1 olarak tanımlanmıştır. Demek ki 1 gerçekten soldaki kümededir.

Eğer $X = \{x_1, \ldots, x_n\}$ ise $\langle X \rangle$ yerine $\langle x_1, \ldots, x_n \rangle$ yazılır.

Özel bir durum olarak $X = \{x\}$ durumunu ele alalım. Bu durumda bütün x_i'ler x'e eşit olmak zorundadır ve

$$\langle x \rangle = \{x^n : n \in \mathbb{N}\}$$

bulunur. Eğer $\deg x = n < \infty$ ise,

$$\langle x \rangle = \{1, x, x^2, \ldots, x^{n-1}\}$$

eşitliğini daha önce görmüştük. Tek bir eleman tarafından üretilen gruplara ***döngüsel*** ya da ***devirli grup*** denir. Devirli gruplar abel gruplarıdırlar ve en basit gruplardır. İleride bu konuya özel bir bölüm ayıracağız.

Eğer $X = \{x, y\}$ ise durum hemen karmaşıklaşır:

$$\langle x, y \rangle = \{x^{k_1} y^{\ell_1} \cdots x^{k_n} y^{\ell_n} : n \in \mathbb{N},\ k_i,\ \ell_i \in \mathbb{Z}\}.$$

Ama $xy = yx$ ise bu karmaşık durum kendini toparlar:

$$\langle x, y \rangle = \{x^k y^\ell : k,\ \ell \in \mathbb{Z}\}.$$

Eğer bir de ayrıca $\deg x = n < \infty$ ve $\deg y = m < \infty$ ise, o zaman,i

$$\langle x, y \rangle = \{x^k y^\ell : k = 0, 1, \ldots, n-1,\ \ell = 0, 1, \ldots, m-1\}$$

olur. (Ama sağda görülen bütün elemanlar farklı olmak zorunda değildir.)

Daha genel olarak, eğer X'in elemanları aralarında değişiyorlarsa, yani her $x, y \in X$ için $xy = yx$ oluyorsa, o zaman,

$$\langle X \rangle = \{x_1^{k_1} \cdots x_n^{k_n} : n \in \mathbb{N},\ x_i \in X,\ k_i \in \mathbb{Z}\}$$

olur ve bu ifadede eğer istersek $i \neq j$ için $x_i \neq x_j$ alabiliriz.

Bazen $xy = yx$ yerine x ile y arasında başka ilişkiler olabilir; bu durumda da $\langle x, y \rangle$ altgrubunun oldukça basit gösterimi olabilir. En standart örnek $\deg x = \deg y = 2$ ve $\deg xy = n$ olduğu durumdur. Bu durumda $z = xy$ tanımıyla, $xz = z^{n-1}x$ olur ve

$$\langle x, y \rangle = \langle z, x \rangle = \{x^i z^j : i \in \{0, 1\},\ j \in \{0, 1, \ldots, n-1\}\}$$

elde edilir. Ayrıntıları okura alıştırma olarak bırakıyoruz.

Tabii eğer grubun işlemi + ile ifade ediliyorsa (dolayısıyla değişmeli bir grup sözkonusuysa) o zaman,

$$\langle X \rangle = \{k_1 x_1 + \cdots + k_n x_n : n \in \mathbb{N},\ x_i \in X,\ \epsilon_i = \pm 1\}$$

olur ve istersek $i \neq j$ için $x_i \neq x_j$ alabiliriz.

Notlar ve Örnekler

7.1. Eğer $n \in \mathbb{Z}$ ise $\langle n \rangle = n\mathbb{Z}$ olur.

7.2. Eğer $n,\ m \in \mathbb{Z}$ ise, $d = \text{ebob}(n, m)$ için $\langle n,\ m \rangle = n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ olur.

7.3. Eğer $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ ise, $\langle (n, m) \rangle = (n, m)\mathbb{Z}$ olur.

7.4. $\langle (n, 0),\ (0, m) \rangle = n\mathbb{Z} \times m\mathbb{Z}$ olur. n ya da m sayılarından en az biri 0'a eşit olmadıkça bu iki altgrup birbirine eşit değildir. (Neden?)

7.5. $\mathbb{Z} \times \mathbb{Z}$ grubu $e_1 = (1, 0)$ ve $e_2 = (0, 1)$ elemanları tarafından üretilir. $\mathbb{Z}^n$ grubu da

$$e_1 = (1, 0, 0, \ldots, 0, 0),\ e_2 = (0, 1, 0, \ldots, 0, 0),\ \ldots,\ e_n = (0, 0, 0, \ldots, 0, 1)$$

elemanları tarafından üretilir. Bu grubun başka üreteçleri de vardır elbette. Ancak yukarıda verilen üreteçlere ***doğal üreteçler*** diyebiliriz. Teorem 5.5'te $\mathbb{Z} \times \mathbb{Z}$ grubunun her elemanının en fazla iki eleman tarafından üretildiğini göstermiştik. Birazdan $\mathbb{Z}^n$ grubunun her elemanının en fazla n eleman tarafından üretildiğini göstereceğiz.

7.6. $\text{Sym}\, n$ grubu $\{(1\ k) : k = 2, \ldots, n\}$ kümesi tarafından üretilir ve daha küçük bir altküme tarafından üretilmez. (Neden? Bkz. sayfa 43.)

7.7. $\text{Sym}\, n$ grubu $\{(k\ k+1) : k = 1, \ldots, n-1\}$ kümesi tarafından üretilir ve daha küçük bir altküme tarafından üretilmez. (Neden? Bkz. sayfa 44.)

7.8. $\text{Sym}\, n$ grubu $(1\ 2\ \ldots\ n)$ ve $(1\ 2)$ tarafından üretilir ve daha küçük bir altküme tarafından üretilmez. (Teorem 3.1.)

7.9. Eğer $n \geq 2$ ise, $\text{Sym}\, n$'nin $(a\ b)(c\ d)$ türünden elemanlar tarafından üretilen altgrubu $\text{Sym}\, n$'nin $\text{Alt}\, n$ olarak gösterilen bir özaltgrubudur, tam $n!/2$ tane elemanı vardır. (Bkz. Teorem 3.2 ve Teorem 14.3.)

$n \geq 3$ için $\text{Alt}\, n$ grubu $(i\ j\ k)$ biçiminde yazılan elemanlar tarafından üretilir. Nitekim $(a\ b)(b\ c) = (a\ b\ c)$ ve $(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d)$ olduğundan, çift sayıda makasın çarpımını bu sayede $(a\ b\ c)$ türünden döngülerin çarpımı olarak yazabiliriz.

$n \geq 5$ için $\text{Alt}\, n$ grubu iki ayrık makasın çarpımı olarak yazılan $(a\ b)(c\ d)$ elemanları tarafından üretilir. Nitekim bir önceki paragrafta $\text{Alt}\, n$'nin $(a\ b\ c)$ türünden döngüler tarafından üretildiğini gördük. Eğer e ve d, bu a, b, c sayılarından farklıysa, $(a\ b\ c) = (a\ b)(b\ c) = (a\ b)(d\ e)(d\ e)(b\ c)$ olduğundan, her $(a\ b\ c)$ döngüsünü $(a\ b)(c\ d)$ tipinden iki elemanın çarpımı olarak yazabiliriz.

7.10. G bir grup ve $X \subseteq G$ olsun. $C_G(X) = C_G(\langle X \rangle)$ eşitliğini gösterin.

Eğer $H = \langle X \rangle$ ise H'in X kümesi tarafından üretildiği söylenir. Eğer ayrıca $|X| = n < \infty$ ise, H'nin n eleman tarafından üretildiği söylenir.

$X \subseteq \langle X \rangle$ olduğundan elbette $|X| \leq |\langle X \rangle|$ olur. Eğer X sonluysa ya da sayılabilir sonsuzluktaysa $|\langle X \rangle| \leq \omega$ olur, aksi halde, $|\langle X \rangle| = |X|$ olur. Kümeler kuramından kardinaliteleri anımsayan biri için bunlar çok kolay alıştırmalardır.

Notlar ve Örnekler

7.11. Eğer $\mathbb{Z} = \langle a \rangle$ ise, a tamsayısı ya 1 ya da -1 olmak zorundadır.

7.12. $G = \mathbb{R}$ olsun. O zaman her $a \in \mathbb{R}$ için $\langle a \rangle = a\mathbb{Z}$ olur.

7.13. $G = \mathbb{R}^\star$ olsun. O zaman her $a \in \mathbb{R}^\star$ için $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ olur (tabii ki!) Eğer $a = -1$ ise $\langle a \rangle = \{1, -1\}$ olur.

7.14. Eğer $G = \langle Z(G), x \rangle$ ise G bir abel grubudur. (Burada $Z(G)$, G'nin tüm elemanlarıyla değişen elemanlar kümesi, yani G'nin merkezidir.) Nitekim koşuldan dolayı,

$$G = \{zx^n : z \in Z(G),\ n \in \mathbb{Z}\}$$

olur ve bu grubun bir abel grubu olduğu

$$(zx^n)(z_1x^m) = zz_1x^nx^m = zz_1x^{n+m} \text{ ve } (z_1x^m)(zx^n) = zz_1x^mx^n = zz_1x^{m+n}$$

eşitliklerinden belli.

7.15. Eğer A, $B \subseteq G$ ise (genellikle uygulamada A ve B altgrup olurlar), $\langle [a,b] : a \in A,\ b \in B\rangle$ altgrubu $[A,B]$ olarak gösterilir. Burada $[a,b]$ yazılımının $a^{-1}b^{-1}ab$ anlamına geldiğini anımsatırız.
Eğer $B \leq N_G(A)$ ise, $a \in A$, $b \in B$ için $[a,b] = a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) \in AA \subseteq A$ olduğundan, $[A,B] \leq A$ olur.
Eğer $B \leq N_G(A)$ ve $A \leq N_G(B)$ ise, kolayca görüleceği üzere $[A,B] \leq A \cap B$ olur.
Bir önceki satırdan, eğer $B \leq N_G(A)$, $A \leq N_G(B)$ ve $A \cap B = \{1\}$ ise, $[A,B] \leq A \cap B = \{1\}$ olduğu anlaşılır; yani her $a \in A$, $b \in B$ için $ab = ba$ olur.

7.16. G bir grup ve A, $B \leq G$ olsun. $B \leq N_G(A)$ olsun, yani her $b \in B$ için $A^b = A$ olsun. O zaman $\langle A,B\rangle = AB$ olur (bkz. Önsav 5.3).

7.17. G bir grup ve $x \in G$ olsun. Eğer $n_1,\ldots,n_k \in \mathbb{Z}$ ise $d = \text{ebob}(n_1,\ldots,n_k)$ için

$$\langle x^{n_1},\ldots,x^{n_k}\rangle = \langle x^d\rangle$$

olur. Nitekim bir m_i için $dm_i = n_i$ olduğu için

$$x^{n_i} = x^{dm_i} = (x^d)^{m_i} \in \langle x^d\rangle$$

olur. Demek ki $\langle x^{n_1},\ldots,x^{n_k}\rangle \leq \langle x^d\rangle$.
Diğer yöndeki içindeliği kanıtlayalım. $d = \text{ebob}(n_1,\ldots,n_k)$ olduğundan, Alıştırma 2.2'ye göre, öyle $u_1,\ldots,u_k \in \mathbb{Z}$ vardır ki,

$$d = n_1u_1 + \cdots + n_ku_k$$

olur; dolayısıyla

$$x^d = x^{n_1u_1+\cdots+n_ku_k} = (x^{n_1})^{u_1}\cdots(x^{n_k})^{u_k} \in \langle x^{n_1},\ldots,x^{n_k}\rangle,$$

yani $\langle x^d\rangle \leq \langle x^{n_1},\ldots,x^{n_k}\rangle$ olur. Bundan şu çıkar

Teorem 7.2. *Döngüsel bir grubun altgrupları da döngüseldir.*

7.18. $G = \prod_I \mathbb{Z}$ olsun. $e_i \in G$ elemanı, i dışında her koordinatı 0 olan ve i'inci koordinatı 1 olan eleman olsun. Yani eğer

$$\delta_{i,j} = \begin{cases} 1 & \text{eğer } i = j \text{ ise} \\ 0 & \text{eğer } i \neq j \text{ ise} \end{cases}$$

ise[4],

$$e_i = (\delta_{i,j})_{j\in I}$$

olsun. Eğer $X = \{e_i : i \in I\}$ ise

$$\langle X\rangle = \oplus_I\mathbb{Z}$$

olur. Benzer durum başka grupların kartezyen çarpımında da yaşanır.

7.19. Teorem 2.1'de $\mathbb{Z}$'nin altgruplarının en fazla bir eleman tarafından üretildiğini göstermiştik[5]. Teorem 5.5'te de $\mathbb{Z}\times\mathbb{Z}$ grubunun her altgrubunun en fazla iki eleman tarafından üretildiğini göstermiştik. Şimdi $\mathbb{Z}^n$ grubunun her altgrubu en fazla n eleman tarafından üretildiğini göstereceğiz.

---

[4] $\delta_{i,j}$ ***Kronecker*** δ ***sembolü*** olarak bilinir.

[5] 0 eleman tarafından üretilen altgrup $\{0\}$ altgrubudur.

Teorem 7.3. *$\mathbb{Z}^n$ grubunun her altgrubu en fazla n eleman tarafından üretilir.*

Kanıt: $n = 1$ ve $n = 2$ için, ve hatta $n = 0$ için teoremin doğru olduğunu biliyoruz. Bundan böyle $n \geq 2$ olsun ve teoremin $n-1$ için doğru olduğunu varsayalım. $A \leq \mathbb{Z}^n$ olsun. Kanıtımızda $\mathbb{Z}^n = \mathbb{Z}^{n-1} \times \mathbb{Z}$ eşitliğini kullanacağız. Şu kümeye bakalım

$$B = \{y \in \mathbb{Z} : \text{bir } x \in \mathbb{Z}^{n-1} \text{ için } (x, y) \in A\}.$$

Bir başka deyişle B, A altgrubunun son koordinata izdüşümüdür. $B \leq \mathbb{Z}$ olduğunu göstermek kolay. Demek ki bir ve bir tek $m \geq 0$ için

$$B = m\mathbb{Z}$$

olur. Yani A'nın elemanlarının son koordinatları m'nin bir katı olmak zorunda. $m \in B$ olduğundan, bir $x_0 \in \mathbb{Z}^{n-1}$ için

$$(x_0, m) \in A$$

olur.
A'dan rastgele bir eleman alalım. Bu elemanı, $x \in \mathbb{Z}^{n-1}$ ve $y \in \mathbb{Z}$ için, (x, y) olarak yazalım. $y \in B$ olduğundan, bir $u \in \mathbb{Z}$ için $y = um$ olur. Buradan,

$$(x, y) - u(x_0, m) = (x, y) - (ux_0, um) = (x - ux_0, y - um) = (x - ux_0, 0) \in \mathbb{Z}^{n-1} \times \{0\}$$

olur. Ama bu eleman ayrıca A altgrubunda da, çünkü hem (x, y), hem de (x_0, m) elemanı A'da. Böylece bir $u \in \mathbb{Z}$ için,

$$(x, y) - u(x_0, m) \in A \cap (\mathbb{Z}^{n-1} \times \{0\})$$

eldeederiz.
Şimdi hesaplara bir paragraflık ara verip $A \cap (\mathbb{Z}^{n-1} \times \{0\})$ kümesine (aslında altgrubuna) daha yakından bakalım.

$$C = \{x \in \mathbb{Z}^{n-1} : (x, 0) \in A\}$$

olsun.

$$A \cap (\mathbb{Z}^{n-1} \times \{0\}) = C \times \{0\}$$

olur. Elbette $C \leq \mathbb{Z}^{n-1}$. Tümevarım varsayımına göre C en fazla $n-1$ elemanla üretilir, diyelim $c_1, \ldots, c_{n-1} \in C \leq \mathbb{Z}^{n-1}$ ile üretiliyor, yani

$$C = \mathbb{Z}c_1 + \ldots + \mathbb{Z}c_{n-1}$$

olur.

$$a_i = (c_i, 0)$$

tanımını yaparsak

$$A \cap (\mathbb{Z}^{n-1} \times \{0\}) = C \times \{0\} = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_{n-1}$$

buluruz.
Kaldığımız yerden devam edelim. Rastgele bir $(x, y) \in A$ almış ve bir $u \in \mathbb{Z}$ için,

$$(x, y) - u(x_0, m) \in A \cap (\mathbb{Z}^{n-1} \times \{0\}) = C \times \{0\}$$

olduğunu kanıtlamıştık. Bir önceki paragrafa göre,

$$(x, y) - u(x_0, m) \in \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_{n-1}$$

olur. Eğer

$$a_n = (x_0, m)$$

tanımını yaparsak, bundan,

$$(x, y) \in \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_{n-1} + \mathbb{Z}a_n$$

çıkar. Demek ki,

$$A \leq \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_{n-1} + \mathbb{Z}a_n.$$

Diğer yöndeki içindelik kolay, çünkü $a_1, \ldots, a_{n-1}, a_n \in A$. □

7.20. Burada daha sonra çeşitli vesilelerle kullanacağımız şu teoremi kanıtlayacağız:

Teorem 7.4. *$(g_i)_{i\in I}$, G grubunun bir üreteç altkümesi olsun. Ayrıca I'nın sonsuz olduğunu ve $\{g_i : i \in I\}$ kümesinin daha küçük kardinalitede bir altkümesinin G'nin üreteç kümesi olamayacağını varsayalım. O zaman G'nin her üreteç kümesinin en az $|I|$ kadar elemanı vardır.*

Kanıt: $(h_j)_{j\in J}$, G'nin bir üreteç kümesi olsun. Her h_j, g_i'ler cinsinden yazılır; bu yazılımda kullanılan I'nın altkümesine I_j diyelim. Her I_j sonlu bir kümedir. Elbette I'nın $\bigcup_{j\in J} I_j$ altkümesi G'nin bir üreteç kümesidir. Buradan ve varsayımdan dolayı

$$|I| = \left|\bigcup_{j\in J} I_j\right|$$

çıkar. Buradan da J'nin sonlu olamayacağı çıkar. J sonsuz olduğundan, kardinal aritmetiğinden,

$$\left|\bigcup_{j\in J} I_j\right| \leq |J|$$

çıkar. Yani $|I| \leq |J|$. □

7.21. Aşağıdaki sonuç direkt toplamda üretilen bir altgrubun ne kadar büyük olabileceğine dair bir şey söylüyor.

Teorem 7.5. *$G = \bigoplus_I G_i$, $\pi_i : G \longrightarrow G_i$ doğal izdüşüm fonksiyonları, $\varphi_i : G_i \longrightarrow G$ doğal gömme fonksiyonları, $X \subseteq G$ ve $H_i = \langle \varphi_i(\pi_i(X))\rangle \leq G_i$ olsun. O zaman $\langle X\rangle \leq \bigoplus_I H_i$ olur.*

Kanıt: X'in her elemanının $\bigoplus_I H_i$ altgrubunda olduğunu kanıtlamak yeterli. Ama elbette her x elemanı $x = \prod_I \varphi_i(\pi_i(x))$ olarak yazılır. Eğer $\varphi_{i_1}(\pi_{i_1}(x)), \ldots, \varphi_{i_n}(\pi_{i_n}(x)) \neq 1$ ama diğerleri 1 ise,

$$x = \prod_{j=1}^{n} x = \prod_{j=1}^{n} \varphi_{i_j}(\pi_{i_j}(x)) \in \prod_{j=1}^{n} H_j \leq \bigoplus_I H_i$$

olur. □

Alıştırmalar

7.22. $G = \mathbb{Z}$ ve $x = 3$, $y = 2$ olsun. $\langle x, y\rangle = \mathbb{Z}$ eşitliğini kanıtlayın.

7.23. $G = \mathbb{Z}$ ve $x = 84$, $y = 30$, $z = 231$ olsun. $\langle x, y, z\rangle$ altgrubunun neye eşit olduğunu bulun.

7.24. $G = \mathbb{R}^\star$, $x = \sqrt{2}$, $y = \sqrt{3}$ olsun. $\langle x, y\rangle$ altgrubunun $x^n y^m$ elemanlarının farklı n ve m tamsayıları için farklı değerler verdiğini kanıtlayın.

7.25. G bir grup ve $x, y \in G$ olsun. Bir $n \in \mathbb{Z}$ için $x^n = y$ varsayımını yapalım. $\langle y\rangle = \langle x\rangle$ olduğunu kanıtlayın.

7.26. G bir grup ve $x, y \in G$ olsun. Bir $n \in \mathbb{Z}$ için $x^n = y$ varsayımını yapalım. $\langle x, y\rangle = \langle x\rangle$ olduğunu kanıtlayın.

7.27. G bir grup ve $x, y \in G$ için

$$x \equiv y \Leftrightarrow \langle x \rangle = \langle y \rangle$$

tanımını yapalım. Bu ilişkinin bir denklik ilişkisi olduğunu ve her denklik sınıfının sonlu olduğunu kanıtlayın.

7.28. Ne zaman $X = \langle X \rangle$ olur?

7.29. G bir grup ve $Y \subseteq X \subseteq G$ olsun. $\langle Y \rangle \leq \langle X \rangle$ olduğunu kanıtlayın.

7.30. G bir grup, Y, $X \subseteq G$ ve $Y \subseteq \langle X \rangle$ olsun. $\langle Y \rangle \leq \langle X \rangle$ olduğunu kanıtlayın.

7.31. $\mathbb{Z}^2$ grubunun $(2,3)$ ve $(1,2)$ elemanları tarafından üretildiğini gösterin.

7.32. $\mathbb{Z}^2$ grubunun $(2,3)$ ve $(3,2)$ elemanları tarafından üretilen altgrubunun elemanlarını bulun.

7.33. $\mathbb{Z}^2$ grubunun $(2,3)$ ve $(5,1)$ elemanları tarafından üretilen altgrubunun elemanlarını bulun.

7.34. $\mathbb{Q}$ grubunun $2/7$ ve $1/5$ elemanları tarafından üretilen altgrubunu bulun. (Bkz. Teorem 10.24 ve kanıtı.)

7.35. $\mathbb{Q}$ grubunun $2/5$, $4/7$ ve $6/13$ elemanları tarafından üretilen altgrubunu bulun. (Bkz. Teorem 10.24 ve kanıtı.)

7.36. G bir grup ve $X \subseteq G$ olsun. $\langle X \rangle = \langle X^{-1} \rangle = \langle X \cup X^{-1} \rangle$ olduğunu kanıtlayın.

7.37. $X \subseteq G$ olsun. Her $x, y \in X$ için $xy = yx$ varsayımını ayaplım. Bu durumda $\langle X \rangle$ altgrubunun bir abel grubu olduğunu kanıtlayın.

7.38. G bir grup ve $x, y \in G$ olsun. $\deg x = \deg y = 2$ ve $\deg xy = n < \infty$ varsayımını yapalım. $|\langle x, y \rangle| = 2n$ eşitliğini kanıtlayın.

7.39. $H \leq G$ ve $x \in G$ olsun. Eğer H altgrubu en fazla n eleman tarafından üretiliyorsa, $\langle H, x \rangle$ altgrubunun en fazla $n+1$ eleman tarafından üretildiğini kanıtlayın.

7.40. $n > 0$ bir tamsayı olsun. r, düzlemi $(0,0)$ noktası etrafında $2\pi/n$ radyan (ya da $360/n$ derece) döndüren dönüşüm olsun. $r \in \operatorname{Sym} \mathbb{R}$ ve $\deg r = n$ olur. $k \in \mathbb{Z}$ olsun. $\langle r^k \rangle = \langle r \rangle$ eşitliğinin geçerli olması için $\operatorname{obeb}(n,k) = 1$ olması gerektiğini kanıtlayın.

7.41. Bir grubun minimal bir altgrubunun (olduğunda) döngüsel olmak zorunda olduğunu kanıtlayın.

7.42. Farklı n doğal sayıları için $\operatorname{Sym} n$'nin en fazla elemanlı döngüsel altgruplarını bulun.

7.43. G bir grup, $X \subseteq G$ ve $H = \langle X \rangle$ olsun. Eğer $g \in G$ için $g^{-1}Xg \subseteq X$ oluyorsa $g^{-1}Hg \subseteq H$ olduğunu kanıtlayın. Eğer **her** $g \in G$ için $g^{-1}Xg \subseteq X$ oluyorsa, her $g \in G$ için $g^{-1}Hg = H$ olduğunu kanıtlayın.

7.44. H, $K \leq G$ olsun. Eğer H altgrubu en fazla n, H altgrubu en fazla m eleman tarafından üretiliyorsa, $\langle H, K \rangle$ altgrubunun en fazla $n+m$ eleman tarafından üretildiğini kanıtlayın.

7.45. $H \leq G$ ve $x \in G$ olsun. Eğer H altgrubu en fazla n eleman tarafından üretiliyorsa, $x^{-1}Hx$ altgrubunun da en fazla n eleman tarafından üretildiğini kanıtlayın

7.46. G bir grup ve $x, y \in G$ olsun. $\deg x = \deg y = 2$ ve $\deg xy = \infty$ varsayımını yapalım.

$$\langle x, y \rangle = \{(xy)^n : n \in \mathbb{Z}\} \sqcup \{x(xy)^n : n \in \mathbb{Z}\}$$

eşitliğini ve sağ tarafta gösterilen elemanların herbirinin diğerinden farklı olduğunu kanıtlayın.

7.47. G bir grup ve $x, y \in G$ olsun. $xy = yx$ varsayımını yapalım. $\langle x, y \rangle$ altgrubunun $x^n y^m$ elemanlarının farklı n ve m tamsayıları için farklı değerler vermemesiyle, her ikisi birden 0 olmayan n ve m tamsayıları için $x^n = y^m$ eşitliğinin doğru olmasının yeter ve gerek olduğunu kanıtlayın.

7.48. $\mathbb{Z}^n$'nin her altgrubunun en fazla n eleman tarafından üretilebileceğini kanıtlayın. (n üzerine tümevarımla ama bu alıştırma bu aşamada zor olabilir, bkz. Teorem 13.6.)

7.49. $\mathbb{Q}$ grubunun sonlu sayıda eleman tarafından üretilmediğini kanıtlayın.

7.50. Eğer X kümesi $\mathbb{Q}$ grubu üretiyorsa ve $x \in X$ ise $X \setminus \{x\}$ kümesinin de $\mathbb{Q}$ kümesini ürettiğini kanıtlayın. (Çok kolay olmayabilir.)

7.51. $\mathbb{R}$'nin (ya da $\mathbb{Q}$'nün) her altgrubunun ya 1 eleman tarafından üretildiğini ya da $\mathbb{R}$'de (ya da $\mathbb{Q}$'de) yoğun olduğunu kanıtlayın.

7.52. G bir grup olsun. Bir α kardinali için $(G_\beta)_{\beta<\alpha}$ bir altgrup ailesi olsun. Her $\gamma \leq \beta < \alpha$ için $G_\gamma \leq G_\beta$ varsayımını yapalım. $X_\beta \subseteq G_\beta$ bir üreteç kümesi olsun. $\bigcup_{\beta<\alpha} X_\beta$ kümesinin $\bigcup_{\beta<\alpha} G_\beta$ altgrubunu ürettiğini kanıtlayın.

8. Altgrup Ötelemeleri

Sanırım soyut cebirin en önemli konusuna geldik. Bu ve bundan sonraki birkaç bölüm ne kadar çok okunur, üzerinde ne kadar çok durulursa o kadar yararlıdır.

8.1 Altgrupların Ötelemeleri

G bir grup, H de G'nin bir altgrubu olsun. Eğer $a \in G$ ise, aH'yi tahmin edildiği gibi tanımlayalım:

$$aH = \{ah : h \in H\}.$$

aH kümesini H'nin ötelemesi olarak yorumlayabiliriz, çünkü gerçekten aH kümesinin elemanları, H'nin elemanlarının a ile soldan bir tür ötelenmesidir. aH kümesine H'nin a tarafından ***soldan ötelemesi*** (bazen de sol eşküme, sol yanküme ya da sol sınıf) adı verilir. Biz daha çok öteleme terimini kullanacağız ve çok gerekmedikçe "sol" ibaresini kullanmaktan kaçınacağız. Ama okur sol öteleme olduğu gibi sağ ötelemenin de olduğunu ve bu iki ötelemenin farklı olabileceğini aklından çıkarmamalıdır.

Eğer $a \in H$ ise elbette $aH \subseteq H$, hatta $aH = H$ olur. (Neden?) Bunun tersi de doğrudur: $aH = H$ ise, $a \in H$ olmak zorundadır. Demek ki H'nin kendisi de H'nin bir ötelemesidir. Bu arada $a = a \cdot 1 \in aH$ içindeliğini de gözlemleyelim.

Elbette $h \mapsto ah$ kuralı bize H ile aH arasında bir eşleme tanımlar[1]. Dolayısıyla H ile aH kümesinin eleman sayısı aynıdır. Bir başka deyişle tüm sol ötelemelerin kardinalitesi (eleman sayısı) eşittir; bu dediğimiz H altgrubu sonsuz olsa da geçerlidir. Benzer şekilde sağ ötelemeler de tanımlanır ve aynı sonuç sağ ötelemeler için de geçerlidir. Dolayısıyla sol ötelemelerle sağ ötelemelerin eleman sayısı eşittir.

Birazdan bir altgrubun herhangi iki sol ötelemesinin ya eşit ya da ayrık olduğunu kanıtlayacağız; yani kesişimde en az bir eleman olan iki sol öteleme eşit olmak zorundadırlar. Bunun böyle olduğunu aşağıdaki örneklerde de tespit edeceksiniz.

[1] Bu eşlemenin tersi $x \mapsto a^{-1}x$ kuralıyla verilmiştir.

Notlar ve Örnekler

8.1. $G = \operatorname{Sym} 5$ ve $H = \operatorname{Sym} 4$ olsun. H grubunu G'nin içine gömebiliriz, yani H'yi G'nin bir altgrubu olarak görebiliriz[2].

H'nin kendisi H'nin bir ötelemesidir. Hatta biraz önce gördüğümüz gibi

$$\sigma H = H \Leftrightarrow \sigma \in H$$

önermesi doğrudur. Şimdi H dışından bir σ alalım. σ'nın H dışında olması $\sigma(5) \neq 5$ demektir. Mesela $\sigma = (1\ 5)$ olsun. σH ötelemesinin elemanlarını bulalım. H'nin elemanları 5'i 5'e götürdüğünden, σ da 5'i 1'e götürdüğünden, σH'nin elemanları 5'i 1'e götürürler. Demek ki,

$$\sigma H \subseteq \{\alpha \in \operatorname{Sym} 5 : \alpha(5) = 1\}.$$

Öte yandan $\operatorname{Sym} 5$'in 5'i 1'e götüren tam 4! tane elemanı vardır (neden?), yani $|\sigma H| = |H| = 4!$ kadar. Demek ki yukarıdaki içindelik aslında bir eşitliktir:

$$\sigma H = \{\alpha \in \operatorname{Sym} 5 : \alpha(5) = 1\}.$$

Örneğin

$$(1\ 3\ 5),\ (1\ 3\ 2\ 5),\ (1\ 3\ 5)(2\ 4) \in \sigma H$$

olur.

H'nin başka ötelemesi var mı? Evet var. Örneğin,

$$(2\ 5)H = \{\alpha \in \operatorname{Sym} 5 : \alpha(5) = 2\}$$

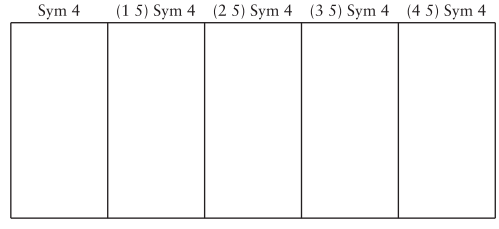
kümesi H'nin bir başka ötelemesidir. Böylece $\operatorname{Sym} 4$'ün $\operatorname{Sym} 5$ içinde tam 5 farklı ötelemesi olduğu görülür: Her $i = 1, 2, 3, 4, 5$ için $\sigma_i = (i\ 5)$ ise[3]

$$\sigma_i H = \{\alpha \in \operatorname{Sym} 5 : \alpha(5) = i\}$$

kümeleri H'nin birbirinden farklı sol ötelemeleri olur ve H'nin başka da ötelemesi yoktur. Toplamda, her birinin eleman sayısı 4! olan 5 tane sol öteleme bulduk. Bu ötelemelerin ayrık olduklarını ve $\operatorname{Sym} 5$'i kapladıklarını gözlemleyin. Yani

$$\operatorname{Sym} 5 = \bigsqcup_{i=1}^{5} (i\ 5) \operatorname{Sym} 4$$

olur. Şekil aşağıda.



$\operatorname{Sym} 4$'ün $\operatorname{Sym} 5$ içindeki ötelemeleri

[2]Aslında, $\operatorname{Sym} 4$'ün elemanları $\{1, 2, 3, 4\}$ kümesinin permütasyonları, $\operatorname{Sym} 5$'in elemanları $\{1, 2, 3, 4, 5\}$ kümesinin permütasyonları olduklarından, illa formel olmak gerekiyorsa, $\operatorname{Sym} 4$ grubuyla $\operatorname{Sym} 5$ grubu kesişmezler, ayrıktırlar. Ancak $\operatorname{Sym} 4$'ün her elemanı $\operatorname{Sym} 5$'in bir elemanına gayet doğal bir biçimde genişletilebilir; bunun için bir $\sigma \in \operatorname{Sym} 4$ için $\sigma(5) = 5$ tanımını yapmak yeterlidir. Demek ki $\operatorname{Sym} 4$ grubunu (doğal olarak) $\operatorname{Sym} 5$'in bir altgrubu olarak görebiliriz. Daha genel olarak eğer $Y \subseteq X$ ise, $\operatorname{Sym} Y$ grubu $\operatorname{Sym} X$'in bir altgrubu olarak görülebilir. Bunun için $\operatorname{Sym} Y$'nin elemanlarını X üzerine $X \setminus Y$ üstünde özdeşlik olacak biçimde genişletmek yeterlidir.

[3]Eğer $i = 5$ ise $(5\ 5)$ permütasyonunu Id_5 olarak algılayın.

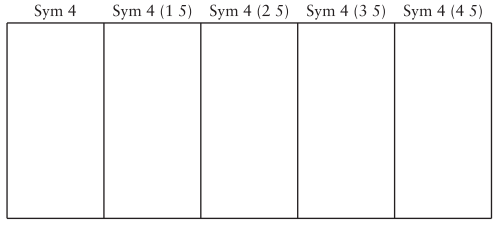
$(2\ 4\ 5)(1\ 3)H = (2\ 5)H$ ve benzer eşitlikleri okur görebilmelidir. H'nin G'deki her ötelemesi yukarıdaki 5 kümeden biridir.

Bu arada $X = \{(1\ 5), (2\ 5), (3\ 5), (4\ 5), \mathrm{Id}_5\}$ kümesinin her sol ötelemeden bir ve bir tek eleman içerdiğini gözlemleyelim. Bu özelliği olan kümelere H'nin ***sol temsilci kümesi*** denir.

H'nin sağ ötelemeleri de vardır. Rastlantı bu ya, yukarıdaki X kümesi H'nin sağ temsilcileri kümesidir aynı zamanda. Nitekim, $i = 1, 2, 3, 4, 5$ için

$$H\sigma_i = \{\alpha \in \mathrm{Sym}\,5 : \alpha(i) = 5\}$$

kümeleri H'nin tüm sağ ötelemeleridir ve her biri diğerlerinden farklıdır. Bu örnekte H dışında hiçbir sol öteleme bir sağ öteleme değildir. Bazı özel durumlarda, örneğin G değişmeli grup olduğunda, ama bazı başka durumlarda da sol ötelemelerle sağ ötelemeler arasında fark yoktur.



Sym 4'ün Sym 5 içindeki ötelemeleri

8.2. Derecesi n olan bir g elemanı için $G = \langle g\rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ olsun. k, n'yi bölen bir doğal sayı olsun, diyelim $n = km$. Şimdi $H = \langle g^k\rangle = \{1, g^k, g^{2k}, \ldots, g^{(k-1)m}\}$ olsun. $H \leq G$ olur. H'nin her ötelemesi bir $i = 0, 1, \ldots, k-1$ için g^iH olarak yazılır (neden?) ve bu tür ötelemeler birbirinden farklıdır. Yani

$$G = \bigsqcup_{i=0}^{k-1} g^iH$$

olur. Demek ki $X = \{1, x, x^2, \ldots, x^{k-1}\}$ kümesi H'nin her (sağ ya da sol farketmez, çünkü G bir abel grubu) ötelemesinden bir ve bir tek eleman içerir. Bu tür kümelere temsilci kümesi dendiğini bir önceki örnekte söylemiştik.

8.3. Eğer grubun işlemi toplamayla yazılıyorsa[4], xH ötelemesi yerine $x + H$ olarak yazılır elbette. Alışkanlık daha çok $H + x$ olarak yazmaktır. Bu örnekte $G = \mathbb{Z}$ ve $H = 5\mathbb{Z}$ olsun. O zaman H'nin G içinde tam 5 ötelemesi vardır:

$$5\mathbb{Z},\ 5\mathbb{Z}+1,\ 5\mathbb{Z}+2,\ 5\mathbb{Z}+3,\ 5\mathbb{Z}+4.$$

Bu ötelemeler bir önceki örnekte olduğu gibi birbirinden ayrıktırlar. Ötelemeler şöyledir:

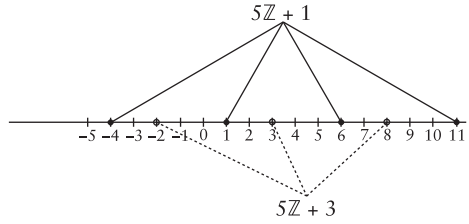
$$\begin{aligned}
5\mathbb{Z} &= \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}\\
5\mathbb{Z}+1 &= \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\}\\
5\mathbb{Z}+2 &= \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}\\
5\mathbb{Z}+3 &= \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}\\
5\mathbb{Z}+4 &= \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}
\end{aligned}$$

Sonuç olarak,

$$\mathbb{Z} = \bigsqcup_{i=0}^{4} (5\mathbb{Z} + i)$$

olur. Bu beş ötelemeden ikisini aşağıdaki resimde görüyorsunuz.

[4]Bu durumda işlemin değişmeli olduğunu unutmayalım.



Ama bu örnekte $\mathbb{Z}$'nin sıralaması pek önemli olmadığından, $\mathbb{Z}$'yi bir doğru üzerinde göstermenin yararı yoktur. Bu yüzden 5 ötelemenin 5'inin de kolaylıkla göründüğü aşağıdaki gösterimi tercih edeceğiz.

$5\mathbb{Z}$	$5\mathbb{Z}+1$	$5\mathbb{Z}+2$	$5\mathbb{Z}+3$	$5\mathbb{Z}+4$
• 0	• 1	• 2	• 3	• 4
• 5	• 6	• 7	• 8	• 9
• –5	• –4	• –3	• –2	• –1
⋮	⋮	⋮	⋮	⋮

Bu arada $\{0, 1, 2, 3, 4\}$ kümesinin her ötelemeden bir ve bir tek eleman içerdiğini gözlemleyelim[5].

8.4. Yukarıdaki iki örnekte öteleme sayısı sonluydu. Öteleme sayısının sonsuz olduğu bir örnek verelim. $G = \mathbb{R}$ ve $H = \mathbb{Z}$ olsun. Her $n \in \mathbb{Z}$ için $\mathbb{Z} + n = \mathbb{Z}$ olduğundan, her $r \in \mathbb{R}$ için

$$\mathbb{Z} + r = \mathbb{Z} + r - 1 = \mathbb{Z} + r - 2 = \mathbb{Z} + r - 3 = \mathbb{Z} + r + 1 = \mathbb{Z} + r + 2$$

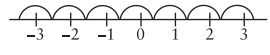
olur. Bu nedenle,

$$z + r = \mathbb{Z} + r - [r]$$

olur[6]. Demek ki her öteleme, bir $r \in [0, 1)$ elemanı için $\mathbb{Z} + r$ biçimindedir. Peki r, $s \in [0, 1)$ için ne zaman $\mathbb{Z}+r = \mathbb{Z}+s$ eşitliği geçerli olur? Ancak ve ancak $r - s \in \mathbb{Z}$ ise, yani $r = s$ ise geçerli olur. Böylece her ötelemenin bir ve bir tek $r \in [0, 1)$ elemanı için $\mathbb{Z} + r$ biçiminde olduğunu göstermiş olduk. $\mathbb{Z}$'nin her ötelemesinde de bir ve bir tek $r \in [0, 1)$ sayısı olduğunu gözlemleyin. Sonuç olarak,

$$\mathbb{R} = \bigsqcup_{r \in [0,1)} (\mathbb{Z} + r)$$

olur. Demek ki $[0, 1)$ kümesi $\mathbb{Z}$'nin $\mathbb{R}$'deki ötelemelerinin temsilciler kümesidir, yani $\mathbb{Z}$'nin her ötelemesinde $[0, 1)$ kümesinden bir ve bir tek eleman vardır. $[2, 3)$ ya da $(0, 1]$ başka temsilciler kümeleridir ama $[0, 1)$ en doğal seçimdir.



[5]Genel kanının aksine bunlar modüler sayılar değildirler, ilkokuldan beri bildiğimiz sayılardır!

[6]Burada $[r]$, r sayısının tamkısmıdır, yani r'den küçükeşit en büyük tamsayıdır.

8.5. Eğer $G = \mathbb{R}$ ve $H = \mathbb{Q}$ ise, H'nin gene sonsuz sayıda ötelemesi vardır, ancak bu sefer yukarıdaki gibi bir temsilciler kümesi bulamayız[7].

8.6. $G = \mathbb{R}^\star = \mathbb{R} \setminus \{0\}$ ve $H = \{1, -1\}$ olsun. G, çarpma altında bir gruptur, H de G'nin bir altgrubudur. H'nin her ötelemesi $xH = \{x, -x\}$ biçimindedir. $x = 0$ durumu dışında her öteleme biri pozitif biri negatif olmak üzere iki sayı içerir. Her ötelemede bir ve bir tek negatif olmayan bir sayı vardır. Yani

$$\mathbb{R}^\star = \bigsqcup_{x \geq 0} xH$$

olur.

Dikkat ettiyseniz yukarıdaki örneklerde ötelemeler ayrık kümelerdi. Bu, genel bir olgudur ve çok önemlidir. İleride çok daha fazla örnek vermek üzere, ötelemelerle ilgili bu önemli olguyu kanıtlayalım hemen.

Teorem 8.1. *G bir grup ve $H \leq G$ olsun. Her $a, b \in G$ için, ya $aH \cap bH = \emptyset$ olur ya da $aH = bH$. Yani eğer bir altgrubun iki ötelemesinin ortak tek bir elemanı dahi varsa bu ötelemeler eşittirler. Ayrıca her $a, b \in G$ için aşağıdaki önermeler eşdeğerdir:*

i. $aH = bH$.
ii. $aH \cap bH \neq \emptyset$.
iii. $b^{-1}a \in H$.
iv. $a^{-1}b \in H$.
v. $a \in bH$.
vi. $b \in aH$.

Kanıt: Diyelim $aH \cap bH \neq \emptyset$. Bu varsayımla $aH = bH$ eşitliğini kanıtlamalıyız. Varsayım a ve b'ye göre simetrik olduğundan (mesela) $aH \subseteq bH$ içindeliğini kanıtlamak yeterli.

$aH \cap bH \neq \emptyset$ önermesini doğrulayan bir eleman alalım: Diyelim h_1, $h_2 \in H$ için $ah_1 = bh_2 \in aH \cap bH$. Bu durumda her $h \in H$ için,

$$ah = (ah_1)(h_1^{-1}h) = (bh_2)(h_1^{-1}h) = b(h_2h_1^{-1}h) \in bH$$

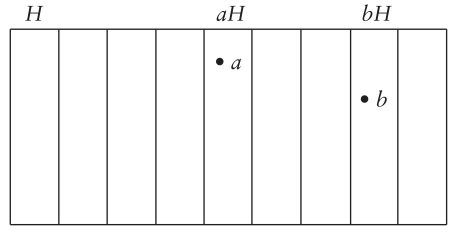
olur çünkü H bir altgrup olduğundan $h_2h_1^{-1}h \in H$ içindeliği doğrudur.

(ii) doğruysa (i)'in doğru olduğunu yukarıda kanıtladık.

Diğerleri çok bariz. □

Bu teoreme göre, H altgrubunun ötelemeleri G'yi kesişmeyen parçalara ayırır. İşte şekil:

[7]Bir temsilciler kümesi elle bulunamaz, ancak Seçim Aksiyomu kullanılarak temsilciler kümesinin varlığı kanıtlanabilir.



Bunun birkaç örneğini verelim.

Notlar ve Örnekler

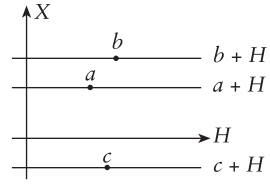
8.7. $G = \mathbb{R} \times \mathbb{R}$ olsun[8]. $H = \mathbb{R} \times \{0\}$ olsun. Elbette $H \leq G$ olur.

$$(x, y) = (x, 0) + (0, y) \in H + (0, y)$$

olduğundan, H'nin her ötelemesi bir $y \in \mathbb{R}$ için $H + (0, y)$ biçiminde yazılır. Ayrıca bu y biriciktir, çünkü

$$\begin{aligned} H + (0, y) = H + (0, z) \quad &\Leftrightarrow \quad (0, y) - (0, z) \in H \\ &\Leftrightarrow \quad (0, y - z) \in H \\ &\Leftrightarrow \quad (0, y - z) \in \mathbb{R} \times \{0\} \\ &\Leftrightarrow \quad y = z \end{aligned}$$

eşdeğerliği geçerlidir. Demek ki $X = \{0\} \times \mathbb{R}$ kümesi bir temsilciler kümesidir: H'nin her ötelemesinde X kümesinden bir ve bir tek eleman bulunur. Dikkat ederseniz X bir altgruptur. Bir temsilciler kümesinin altgrup olarak seçilebilmesi istisnaidir, her zaman olmaz.



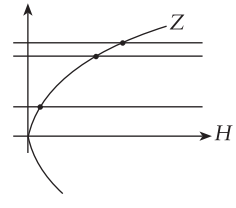
Başka temsilciler kümesi de vardır mesela

$$Y = \{(x, x) : x \in \mathbb{R}\}$$

kümesi de bir temsilciler kümesidir. Y de bir altgruptur. Ama

$$Z = \{(x^2, x) : x \in \mathbb{R}\}$$

kümesi bir temsilciler kümesidir ama bir altgrup değildir.



[8]Grup işlemi toplama elbette: $(x, y) + (z, t) = (x + z, y + t)$.

8.8. G gene yukarıdaki gibi olsun. $H = \{(x,x) : x \in \mathbb{R}\}$ olsun. Kolayca görüleceği üzere $H \leq G$ olur.

$$(x,y) = (x,x) + (0,y-x)$$

eşitliğinden, $X = \{0\} \times \mathbb{R}$ kümesinin (aslında altgrubunun) bir temsilciler kümesi olduğu anlaşılır. Aynı biçimde $Y = \mathbb{R} \times \{0\}$ ve $Z = \{(x,-x) : x \in \mathbb{R}\}$ kümeleri de (altgrupları de) temsilciler kümesidir.

8.9. (Karmaşık sayıları bilenlere.) $G = \mathbb{C}^\star$ kümesi çarpma altında bir gruptur.

$$H = S^1 = \{\zeta \in \mathbb{C} : |\zeta| = 1\} = \{\cos\theta + i\sin\theta : \theta \in \mathbb{R}\} = \{e^{i\theta} : \theta \in \mathbb{R}\}$$

kümesi $\mathbb{C}^\star$'ın bir altgrubudur. Her $\alpha \in \mathbb{C}$, tek bir $\theta \in [0, 2\pi)$ için

$$\alpha = |\alpha| e^{i\theta}$$

biçiminde yazıldığından ve $e^{i\theta} \in S^1$ olduğundan,

$$\alpha S^1 = |\alpha| e^{i\theta} S^1 = |\alpha| S^1$$

olur ve ayrıca αS^1'in her elemanının modülüsü (normu) $|\alpha|$'ya eşittir; yani S^1'in her ötelemesinde bir ve bir tane pozitif gerçel sayı vardır. Bir başka deyişle $\mathbb{R}^{>0}$ kümesi S^1'in ötelemelerinin bir temsilciler kümesi vardır. Daha başka temsilciler kümesi de vardır elbette.

Bir altgrup ötelemesi içindeki herhangi bir eleman tarafından belirlenir: Eğer α, bir H altgrubunun yankümesiyse ve $a \in \alpha$ ise, o zaman $\alpha = aH$ olur.

Bir kümeyi birbiriyle kesişmeyen parçalara ayırmak, o küme üzerinde bir denklik ilişkisi tanımlamak demektir. (Kesişmeyen parçalar verildiğinde, denklik ilişkisini tanımlamak için, aynı parçada olan iki elemanın birbirine denk olduğunu söylemek yeterlidir.) Demek ki her altgrup grupta bir denklik ilişkisi tanımlar ve altgrubun her ötelemesi bu denklik ilişkisinin bir denklik sınıfıdır; bir başka deyişle şu sonuç doğrudur:

Sonuç 8.2. *G bir grup ve H bir altgrup olsun.*

$$a \equiv b \Leftrightarrow aH = bH$$

olarak tanımlanan $\equiv$ ikili ilişkisi G üzerine bir denklik ilişkisi tanımlar. Aşağıdaki koşullardan her biri bu denklik ilişkisinin bu tanıma eşdeğer koşulları şöyledir:

a. $a \equiv b$.
b. $b \in aH$.
c. $a^{-1}b \in H$.
d. $aH \cap bH \neq \emptyset$.
e. $aH \subseteq bH$.

Eğer yukarıdaki satırda a ile b'nin yerlerini değiştirirsek, gene eşdeğer koşullar elde ederiz. Ayrıca her $a \in H$ için

$$\{x \in G : a \equiv x\} = aH$$

olur; yani aH yankümesi bu denklik ilişkisine göre a'nın sınıfıdır. □

Yukarıdaki örneklerde bulduğumuz temsilciler kümesi, her denklik sınıfından bir eleman seçmekten başka bir şey değildi; ama seçilen bu elemanların bir küme oluşturması gerekmektedir, ki bu da her zaman çok kolay değildir, Örnek 8.5'te örneğin böyle bir zorluk vardır.

Notlar ve Örnekler

8.10. **Farklı Altgrupların Ötelemelerinin Kesişimi.** Yukarıdaki sonuçta aynı altgrubun iki ötelemesinin kesişimi hakkında bir olgu kanıtladık. Burada bunu genelleştireceğiz:

Teorem 8.3. *$H, K \leq G$ ve $a, b \in G$ olsun. O zaman ya $aH \cap bK = \emptyset$ olur, ya da herhangi bir $c \in aH \cap bK$ için $aH \cap bK = c(H \cap K)$ olur.*

Kanıt: Diyelim $aH \cap bK \neq \emptyset$. Rastgele bir $c \in aH \cap bK$ alalım. O zaman, $c \in aH$ olduğundan, $cH = aH$ olur. Benzer şekilde $cK = bK$ olur. Demek ki $aH \cap bK = cH \cap cK = c(H \cap K)$ olur. □

Okur Örnek 2.4'ü buradaki sonuç ışığında da okumalıdır.

8.11. Yukarıdaki teoreme somut örnekler verelim. $G = \mathbb{Z}$, $H = 14\mathbb{Z}$, $K = 21\mathbb{Z}$, $a = 10$, $b = 9$ olsun. Yani $(14\mathbb{Z}+10)\cap(21\mathbb{Z}+9)$ kesişimini bulalım. $14\mathbb{Z}+10 \subseteq 7\mathbb{Z}+3$ ve $21\mathbb{Z}+9 \subseteq 7\mathbb{Z}+2$ olduğundan, kesişim boşküme olmak zorundadır. Öte yandan $(14\mathbb{Z} + 10) \cap (21\mathbb{Z} + 3)$ boşküme olmaz, çünkü mesela 24 her iki kümededir. Okur kesişimin bu durumda $42\mathbb{Z}+24$ olduğunu kanıtlamak isteyebilir. Daha genel olarak $(a\mathbb{Z} + b) \cap (b\mathbb{Z} + d)$ kesişiminin ne zaman boşküme olduğunu, ne zaman olmadığını ve olmadığında da hangi kümeye eşit olduğunu kanıtlamaya çalışabilir.

8.12. **Çifte Ötelemeler.** $H, K \leq G$ olsun. $g \in G$ için HgK kümesine H-K ***çifte ötelemesi*** denir. Kolayca gösterilebileceği üzere, $HxK \cap HyK \neq \emptyset$ ise $xK = HyK$ olur. Demek ki çifte ötelemeler bir grubu ayrık parçalara böler. Ama bu sefer her iki çifte ötelemenin eleman sayısı aynı değildir. HxK kümesinin eleman sayısını bulalım. Bunun için $f(h, k) = hxk$ eşitliğiyle tanımlanan $f : H \times K \longrightarrow HxK$ fonksiyonuna bakalım. Bu fonksiyon örtendir ama birebir olmak zorunda değildir. Bakalım kaç tane $(h_1, k_1) \in H \times K$ elemanı için $h_1xk_1 = hxk$ oluyor. Eşitliğin doğru olduğunu varsayıp h_1 ve k_1 hakkında bilgi toplayalım. $k_1k^{-1} = x^{-1}(h^{-1}h_1)x \in K \cap H^x$ olmalı. $L = K \cap H^x$ olsun. Demek ki $k_1k^{-1} \in L$ ve $k_1 \in Lk$ olmalı. Bundan da k_1 için en fazla $|L|$ tane seçeneğimiz olduğu çıkar. Ama her k_1 için en fazla bir tane $h_1 \in H$ bulunur, çünkü incelediğimiz eşitliğin sağlanması için $h_1 = hxkk_1^{-1}x^{-1}$ olmak zorundadır. Demek ki en fazla $|L|$ tane $(h_1, k_1) \in H \times K$ çifti için $h_1xk_1 = hxk$ olabilir. Şimdi diğer taraftan gidelim. $k_1 \in Lk$ rastgele bir eleman olsun. Diyelim $\ell \in L$ için $k_1 = \ell k$ eşitliği geçerli. L'nin tanımından dolayı $\ell \in K$ ve bir $h_2 \in H$ için $\ell = h_2^x = x^{-1}h_2x$ olmalı. Şimdi $h_1 = hxkk_1^{-1}x^{-1}$ tanımını yapalım. h_1'in tanımından dolayı elbette $h_1xk_1 = hxk$ olmalı. Önemli olan h_1'in H'de olup olmadığı. Bakalım: $h_1 = hxkk_1^{-1}x^{-1} = hxk(k^{-1}\ell^{-1})x^{-1} = hx\ell^{-1}x^{-1} = hx(x^{-1}h_2x)^{-1}x^{-1} = hx(x^{-1}h_2^{-1}x)x^{-1} = hh_2^{-1} \in H$. Böylece analizin sonuna geldik. $H \times K$ kümesinin tam $|L|$ tane elemanının imgesi aynı, ne daha az ne daha fazla. Demek ki

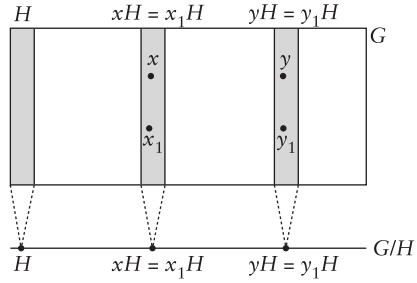
$$|H||K| = |HxK||K \cap H^x|.$$

8.2 Bölüm Kümesi

Şimdi önemli bir tanım yapalım. G bir grup ve $H \leq G$ olsun. ***Sol ötelemeler kümesi*** G/H şöyle tanımlanır:

$$G/H = \{xH : x \in G\}.$$

Bu küme aynen yukarıda tanımladığımız $\equiv$ denklik ilişkisinin sınıflarından oluşan kümedir. Bu yüzden G/H kümesine daha ziyade ***bölüm kümesi*** adı verilir. Resim aşağıda:



Sonuç 8.4 (Lagrange Teoremi)**.** *Eğer G bir grupsa ve $H \leq G$ ise, $|G| = |G/H|\,|H|$ olur. Dolayısıyla eğer G sonluysa*

$$|G/H| = \frac{|G|}{|H|}$$

olur. □

Bu sonuç elbette G sonlu bir grup iken geçerlidir, ama kardinaliteleri bilen biri aynı sonucun sonsuz gruplar için de geçerli olduğunu zorluk çekmeden anlayacaktır.

G/H kümesini sol ötelemeler için tanımladık. Aynı şeyi sağ ötelemeler için de tanımlayabilirdik. Aynı kümeyi bulmayız genellikle. Yani aslında yukarıda ayrı ayrı

$$(G/H)_{\text{sol}} \text{ ve } (G/H)_{\text{sağ}}$$

tanımlarını yapmalıydık. Notasyonu ağırlaştırmamak için bunu tercih etmeyeceğiz. Yeri geldiğinde G/H'yi sol bölüm kümesi için, yeri geldiğinde sağ bölüm kümesi anlamında kullanacağız. Ne zaman hangi anlamda kullandığımız kapsamdan anlaşılacak ve bir karışıklık olmayacak. Ama yukarıdaki sonuç elbette sağ ötelemeler kümesi için de geçerli olduğundan,

$$|(G/H)_{\text{sol}}| = \left|(G/H)_{\text{sağ}}\right|$$

olur. Bu eşitlik şöyle de görülebilir: $xH \mapsto Hx^{-1}$ kuralıyla tanımlanan fonksiyon, sol bölüm kümesiyle sağ bölüm kümesi arasında bir eşleme verir. (Ama $xH \mapsto Hx$ olmazdı! Çünkü $xH = yH$ ise, illa $Hx = Hy$ eşitliği doğru olmak zorunda değildir.)

Yukarıdaki sonuçlar konuya yeni başlayan biri için belki sıkıcı bulunabilir ama had safhada önemli oldukları aşağıdaki önemli ve ilginç sonuçlardan belli.

Sonuç 8.5. *Eğer G sonlu bir grupsa ve $H \leq G$ ise, H'nin (ve G/H'nin) eleman sayısı G'nin eleman sayısını böler.* □

Sonuç 8.6. *Eğer G sonlu bir grupsa ve $x \in G$ ise $\deg x$, G'nin eleman sayısını böler; bir başka deyişle her $g \in G$ için $g^{|G|} = 1$ olur.*

Kanıt: $|\langle x \rangle| = \deg x$ eşitliğini Teorem 4.12'den biliyoruz. Sonuç, bundan ve bir önceki sonuçtan çıkar. □

Örneğin 28 elemanlı bir grubun elemanlarının dereceleri ve altgruplarının eleman sayıları ancak 1, 2, 4, 7, 14 ve 28 olabilir, ama mesela 3 olamaz. Önceki sayıdaki tüm örneklerde bunun böyle olduğunu okur dilerse kontrol edebilir. Mesela $\operatorname{Sym} 3$ grubunun eleman sayısı $3! = 6$'dır ve derecesi 1, 2 ve 3 olan elemanları vardır, sırasıyla Id_3, $(1\ 2)$ ve $(1\ 2\ 3)$ mesela. Ama $\operatorname{Sym} 3$'ün derecesi 6 olan bir elemanı yoktur.

Sonuç 8.7. *Eleman sayısı asal olan bir grup döngüseldir ve 1'den farklı her elemanı tarafından üretilir.*

Kanıt: Gruba G diyelim. $|G| = p$ olsun. $g \in G \setminus \{1\}$ olsun. O zaman

$$1 < \langle g \rangle \leq G$$

olur. Demek ki $1 < |\langle g \rangle|$ olur ve bu sayı p asalını böler. Yani $|\langle g \rangle| = p = |G|$ olur. Bundan hemen $\langle g \rangle \leq G$ çıkar. □

Sonuç 8.8. *Sonlu bir grubun eksponenti sonludur. Hatta eksponent elemanların derecelerinin en küçük ortak katıdır ve grubun eleman sayısını böler.*

Gruba G diyelim. Eğer m, G'nin elemanlarının derecelerinin en küçük ortak katıysa, elbette her $g \in G$ için $g^m = 1$ olur. Demek ki eksponent sonludur ve $\exp G \leq m$ olur. Ayrıca her $g \in G$ için $g^{\exp G} = 1$ olduğundan, $\deg g$, $\exp G$'yi böler, dolayısıyla m, $\exp G$'yi böler ve $m \leq \exp G$ olur. □

Sonuç 8.9. *Eğer p bir asal ve $|G| = p^n$ ise, G'nin elemanlarının dereceleri ancak p'nin bir kuvveti olur.*

Notlar ve Örnekler

8.13. $\operatorname{Sym} 4$'ün altgruplarının olası eleman sayısını bulalım. $\operatorname{Sym} 4$'ün $4! = 24$ elemanı olduğundan, altgruplarının eleman sayısı ancak 1, 2, 3, 4, 6, 8, 12 ve 24 olabilir. 1 elemanlı sadece bir altgrup vardır: $\{\mathrm{Id}_4\}$.
$\langle (1\ 2) \rangle$, $\langle (1\ 2\ 3) \rangle$ ve $\langle (1\ 2\ 3\ 4) \rangle$ altgruplarının eleman sayısı sırasıyla 2, 3 ve 4'tür.
$\operatorname{Sym} 3$'ü doğal olarak $\operatorname{Sym} 4$'ün içine gömebileceğimizi biliyoruz: $\operatorname{Sym} 4$'ün 4'ü sabitleyen permütasyonlarından oluşan altgrup, yani $\langle (1\ 2), (1\ 2\ 3) \rangle$ altgrubu $\operatorname{Sym} 3$'e çok benzer ve eleman sayısı $3! = 6$'dır.
$\operatorname{Sym} 4$'ün 8 elemanlı altgrubu da vardır (bkz. sayfa 81): $\langle (1\ 2\ 3\ 4), (2\ 4) \rangle$.

Sym 4'ün 12 elemanlı altgrubu da vardır (bkz. sayfa 84): $\langle (1\ 2\ 3),\ (1\ 2\ 4),\ (1\ 3\ 4),\ (2\ 3\ 4)\rangle$. Nitekim bu grup şu 12 elemandan oluşur:

$$\begin{aligned}\operatorname{Alt} 4 \quad = \quad & \{\mathrm{Id}_4,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\\ & (1\ 2\ 3),\ (1\ 2\ 4),\ (1\ 3\ 4),\ (2\ 3\ 4),\ (1\ 3\ 2),\ (1\ 4\ 2),\ (1\ 4\ 3),\ (2\ 4\ 3)\}.\end{aligned}$$

Bu kümenin gerçekten bir altgrup oluşturduğunu göstermeyi okura bırakıyoruz. İleride bunun çok daha kolay bir yolunu bulacağız.

24 elemanlı bir altgrubu bulmak kolay, çünkü sadece bir tane var: Sym 4.

Demek ki 24'ü bölen her doğal sayı için, o kadar elemanı olan bir altgrup bulduk. Ama bu 4 sayısına özgüdür, aynı şey Sym 5'te geçerli değildir.

8.14. Sym 5'in altgruplarının olası eleman sayılarını bulabildiğimiz kadarıyla bulalım.

Sym 5'in $5! = 120$ elemanı olduğundan, altgruplarının eleman sayısı ancak 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 60, 120 olabilir. Bir önceki alıştırmanın yardımıyla eleman sayısı 1, 2, 3, 4, 6, 12, 24 olan altgruplar bulabiliriz, ne de olsa 5'i sabitleyen permütasyonlardan oluşan altgrup Sym 4'e çok benzer. $\langle (1\ 2\ 3\ 4\ 5)\rangle$ altgrubunun 5 elemanı vardır. 10 elemanlı bir altgrup bulmak da çok zor değil: $\langle (1\ 2\ 3\ 4\ 5),\ (2\ 5)(3\ 4)\rangle$ altgrubunun 10 elemanı vardır. (Bu altgrup, Örnek 6.3'te tanımlanan D_{10} grubuna benzer.) Sym 5 kendisinin 120 elemanlı bir altgrubudur. Geriye 15, 20, 30 ve 60 elemanlı altgruplar bulmak kaldı. 60 elemanlı bir altgrup vardır:

$$\operatorname{Alt} 5 = \langle (a\ b)(c\ d) : a,\ b,\ c,\ d \in \{1,\ 2,\ 3,\ 4,\ 5\}\rangle$$

altgrubunun tam 60 tane elemanı vardır (Teorem 3.2).

$$\langle (1\ 2\ 3\ 4\ 5),\ (2\ 3\ 5\ 4)\rangle$$

altgrubunun ise tam 20 elemanı vardır. (Okura alıştırma.) İleride Sym 5'in 15 ya da 30 elemanlı altgrubunun olmadığını gösterebilecek bilgiye sahip olacağız (bkz. Alıştırma 16.26).

8.15. $H,\ K \leq G$ olsun. $|H|$ bir asal olsun. O zaman ya $H \leq K$ ya da $H \cap K = \{1\}$ olur, çünkü $H \cap K$ kesişimi H'nin bir altgrubu olduğundan, eleman sayısı $|H|$'yi böler. Dolayısıyla ya $H \cap K = 1$ ya da $H \cap K = H$, yani $H \leq K$ olur.

Eğer $|H|$ ile $|K|$ aralarında asalsa da $H \cap K = \{1\}$ olmak zorundadır.

8.16. $n > 0$ bir doğal sayı olsun. $0 < m \leq n$ olsun.

$$A = \{\sigma \in \operatorname{Sym} n : \text{eğer } i > m \text{ ise } \sigma(i) = i\}$$

ve

$$B = \{\sigma \in \operatorname{Sym} n : \text{eğer } i \leq m \text{ ise } \sigma(i) = i\}$$

olsun. A'nın elemanları, sadece $\{1, \ldots, m\}$ sayıları üzerinde bir etkisi bulunan, m'den büyük sayıların yerini değiştirmeyen permütasyonlardır. B'nin elemanları da, sadece $\{m+1, \ldots, n\}$ sayıları üzerinde bir etkisi bulunan, $m+1$'den küçük sayıların yerini değiştirmeyen permütasyonlardır. A ve B, elbette $\operatorname{Sym} n$'nin altgruplarıdır ve $A \cap B = \{\mathrm{Id}_n\}$ olur. Ayrıca her $\alpha \in A$ ve $\beta \in B$ için $\alpha\beta = \beta\alpha$ olur. A'nın $m!$, B'nin ise $(n-m)!$ tane elemanı vardır. Dolayısıyla AB altgrubunun $n!(m-n)!$ tane elemanı vardır. $\operatorname{Sym} n$'nin $n!$ tane elemanı olduğundan, bundan $n!(m-n)!$ sayısının $n!$ sayısını böldüğü çıkar. Ama biz bunu zaten biliyorduk, ne de olsa

$$\binom{n}{m} = \frac{n!}{m!(n-m)!} \in \mathbb{N}$$

olduğunu biliyoruz. Ama aynı yöntemle şu kanıtlanabilir: $m_1, \ldots, m_k$ doğal sayılarsa, $m_1! \cdots m_k!$ sayısı $(m_1 + \cdots + m_k)!$ sayısını böler.

8.17. 3!, 4! ve 5! sayılarını bölen 3'ün en büyük kuvveti $3^1 = 3$'tür. Dolayısıyla Sym 3, Sym 4 ve Sym 5'in maksimum 3-altgruplarının eleman sayısı ancak 3 olabilir. $\langle(1\ 2\ 3)\rangle$ böyle bir altgruptur.
Öte yandan Sym 6, Sym 7 ve Sym 8 gruplarının eleman sayısı $3^2 = 9$ sayısına bölünür ama $3^3 = 27$'ye bölünmez. Dolayısıyla bu grupların 27 elemanlı bir altgrubu olamaz ama 9 elemanlı altgrupları olabilir. Nitekim, $\langle(1\ 2\ 3), (4\ 5\ 6)\rangle$ böyle bir altgruptur.
Sym 9, Sym 10 ve Sym 11'e gelince. Bu gruplar 3^4 sayısına bölünürler ama 3^5 sayısına bölünmezler. Acaba 3^4 elemanlı bir altgrupları var mı? Evet var:

$$\langle(1\ 2\ 3), (4\ 5\ 6), (7\ 8\ 9), (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)\rangle$$

böyle bir altgruptur. Bu altgrup diğerleri gibi abel grubu değildir.

$$\langle(1\ 2\ 3), (4\ 5\ 6), (7\ 8\ 9)\rangle$$

altgrubu 27 elemanlıdır ve abeldir ama sonuncu üreteç abelliği bozar.

Yukarıdaki örneklerden de anlaşılacağı üzere, sonlu bile olsa, bir grubun altgruplarını bulmak hiç de kolay bir uğraş değildir.

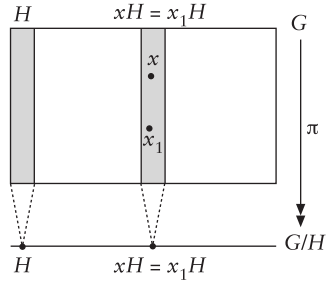
G'den G/H kümesine giden ve her $x \in G$ için,

$$\pi(x) = xH$$

olarak tanımlanan doğal bir $\pi : G \longrightarrow G/H$ fonksiyonu vardır. Bu fonksiyon örtendir ve

$$x \equiv y \Leftrightarrow \pi(x) = \pi(y)$$

olur. ***İzdüşüm fonksiyonu*** adı verilen bu örten fonksiyonun resmi aşağıda.



İleride bu izdüşüm fonksiyonunu sık sık kullanacağız. Bu arada (daha çok sonlu olduğunda) $|G|/|H|$ kardinalitesine H'nin G'deki ***indeksi*** dendiğini de söyleyelim. İndeks genellikle $[G : H]$ olarak yazılır. Sol indeks ile sağ indeksin ayrımının gereksiz olduğunu sayfa 113'da söylemiştik. Eğer $[G : H] = n$ ise bunu bazen kısaca

$$H \overset{n}{\leq} G$$

olarak göstereceğiz. Eğer index sonlu değilse, indeksin ***sonsuz*** olduğunu söyleyeceğiz ve bunu yazıyla $[G : H] = \infty$ olarak göstereceğiz.

Notlar ve Örnekler

8.18. Eğer $m \leq n$ ise $\operatorname{Sym} m$'yi $\operatorname{Sym} n$'nin bir altgrubu olarak görebiliriz. Bu durumda index $n!/m!$ olur elbette. Bunun özel bir durumu olarak $[\operatorname{Sym}(n+1) : \operatorname{Sym} n] = n+1$ olur. Örnek 8.1'i anlayan okur $\operatorname{Sym} n$'nin $\operatorname{Sym}(n+1)$'deki (sol ya da sağ) temsilciler kümesini bulmakta zorlanmayacaktır.

8.19. Teorem 3.2'a göre $n \geq 2$ için $[\operatorname{Sym} n : \operatorname{Alt} n] = 2$ olur.

8.20. *G bir grup ve $K \leq H \leq G$ ise $[G : K] = [G : H][H : K]$ olur.*
Kanıt: Eğer $[G : K] < \infty$ ise sonuç

$$[G : K] = |G/K| = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = [G : H][H : K]$$

eşitliğinden bariz, ki bu da en ilginç durumdur. En genel haliyle kanıtlayalım. K'nın H içinde bir sol temsilciler kümesi seçelim ve bu kümeye Y diyelim. Demek ki

$$H = \bigsqcup_{y \in Y} yH.$$

Ayrıca, H'nin G içinde bir sol temsilciler kümesi seçelim ve bu kümeye Z diyelim. Demek ki

$$G = \bigsqcup_{z \in Z} zH.$$

Bu ikisinden

$$G = \bigsqcup_{z \in Z} zH = \bigsqcup_{z \in Z,\, y \in Y} zyK$$

çıkar. Buradan da ZY'nin K'nın G'de temsilcileri kümesi olduğu anlaşılır ve bu da istenileni kanıtlar. □

8.21. H ve K, G'nin sonlu indeksli iki altgrubu olsun. $[H : H \cap K]$ indeksiyle ilgili bir şeyler söylemeye çalışalım. Tanım gereği,

$$H/(H \cap K) = \{x(H \cap K) : x \in H\}.$$

Ama $x \in H$ için,

$$x(H \cap K) = xH \cap xK = H \cap xK.$$

Demek ki,

$$H/(H \cap K) = \{H \cap xK : x \in H\} \subseteq \{H \cap xK : x \in G\}.$$

Dolayısıyla $H \cap K$'nın H'deki ötelemeleri K'nın G'deki ötelemelerinden daha fazla olamaz:

$$[H : H \cap K] \leq [G : K].$$

Buradan,

$$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K]$$

çıkar. Demek ki *sonlu indeksli iki altgrubun kesişiminin indeksi de sonludur.* Dolayısıyla *sonlu indeksli sonlu sayıda altgrubun kesişiminin indeksi de sonludur.* Hatta bu durumda

$$[G : H_1 \cap \ldots \cap H_n] \leq [G : H_1] \cdots [G : H_n]$$

olur.

Alıştırmalar

8.22. $H \leq G$ ve $x \in G$ olsun. Eğer bir $y \in G$ için $xH = Hy$ oluyorsa, $xH = Hx$ ve $yH = Hy$ olması gerektiğini gösterin.

8.23. Öyle $H \leq G$ ve $x, y \in G$ örneği bulun ki, $xH = yH$ olsun ama $Hx = Hy$ olmasın.

8.24. Eğer p ve q birbirine asal iki sayıysa, $1/p+\mathbb{Z}$ ve $1/q+\mathbb{Z}$ ötelemelerinin ayrık odluğunu gösterin. Buradan $[\mathbb{Q}:\mathbb{Z}]=\infty$ eşitliğini kanıtlayın.

8.25. $n \geq 3$ ve H, $\operatorname{Sym} n$'de, $\{1, 2, 3\}$ kümesini kendisine götüren permütasyonlar kümesi olsun. Elbette $H \leq \operatorname{Sym} n$ olur. $[\operatorname{Sym} n : H]$ sayısını bulun.

8.26. $\mathbb{Z}^2$ grubunda, $H = \langle (2,3), (3,2) \rangle$ altgrubunun indeksinin sonsuz olduğunu gösterin.

8.27. $\mathbb{Z}^2$ grubunda, $H = \langle (2,3), (5,1) \rangle$ altgrubunun indeksinin sonlu olduğunu gösterin.

8.28. G bir grup ve $H \leq G$ olsun. g, $x \in G$ için

$$\tilde{g}(xH) = gxH$$

tanımını yapalım. Böylece $g \mapsto \tilde{g}$ kuralıyla tanımlanmış bir $G \longrightarrow \operatorname{Sym}(G/H)$ fonksiyonu verildiğini kanıtlayın. $\tilde{g} \circ \tilde{h} = \widetilde{gh}$, $\tilde{1} = \mathrm{Id}_{G/H}$ ve $\widetilde{g^{-1}} = \tilde{g}^{-1}$ eşitliklerini kanıtlayın.

8.29. $G = \mathbb{R}^\star \times \mathbb{R}$ olsun. G üstüne şu ikili işlemi tanımlayalım:

$$(x,y)(z,t) = (yz + x, yt).$$

a. G'nin bu işlemle birlikte bir grup olduğunu kanıtlayın.
b. $H = \{(x,0) \in G : x \in \mathbb{Z}\}$ olsun. $H \leq G$ olduğunu kanıtlayın.
c. $t = (1,2)$ olsun. $Ht \subseteq tH$ olduğunu ama eşitliğin doğru olmadığını kanıtlayın.
d. $C_G(t) = \{g \in G : gt = tg\}$ altgrubunu bulun.
e. $u = (1,1)$ olsun. $C_G(u)$ altgrubunu bulun.
f. $G = C_G(u)C_G(t)$ eşitliğini kanıtlayın. G'nin her elemanının, bir ve bir tek $a \in C_G(u)$ ve $b \in C_G(t)$ için ab biçiminde yazıldığını kanıtlayın.

8.30. G bir grup olsun. $Z(G) = \{z \in G :$ her $g \in G$ için$zg = gz\}$ olsun. $Z(G)$'nin her sol ötelemesinin aynı zamanda bir sağ öteleme olduğunu kanıtlayın.

8.31. G bir grup ve H ve K iki altgrup olsun. $x \in G$ için HxK biçiminde yazılan bir kümeye H-K-***ötelemesi*** adı verilir. Herhangi iki H-K ötelemenin ya eşit ya da ayrık olduğunu kanıtlayın.

8.32. G bir grup ve H, $K \leq G$ olsun.

$$HK/K = \{hK : h \in H\}$$

ve

$$H/(H \cap K) = \{h(H \cap K) : h \in H\}$$

olsun. $hK \mapsto h(H \cap K)$ kuralının HK/K kümesinden $H/(H \cap K)$ kümesine giden bir fonksiyon olduğunu kanıtlayın. Bu fonksiyonun bir eşleme olduğunu kanıtlayın.

8.33. G bir grup ve $x \in G$ olsun. $C_G(x) = \{c \in G : cx = xc\}$ olsun. $C_G(x) \leq G$ olur. (x'in G'deki ***merkezleyicisi*** denir bu altgruba.) $g \in G$ için $x^g = g^{-1}xg$ tanımını yapalım. Bu elemana x'in bir ***eşleniği*** denir. $x^G = \{x^g : g \in G\}$ kümesine ise x'in ***eşleniklik sınıfı*** denir. $G/C_G(x) = \{C_G(x)g : g \in G\}$ olsun (sağ ötelemeler kümesi). $C_G(x)g \mapsto x^g$ kuralıyla belirlenen fonksiyonun $G/C_G(x)$ kümesinden x^G kümesine giden iyi tanımlı bir fonksiyon olduğunu kanıtlayın. Bu fonksiyonun bir eşleme olduğunu kanıtlayın. Dolayısıyla sonlu bir grupta eşleniklik sınıfının eleman sayısı grubun eleman sayısını böler.

8.34. $[G : Z(G)] = n$ ise G'deki her eşleniklik sınıfının eleman sayısının n'yi böldüğünü kanıtlayın.

8.35. G bir grup, $H \leq G$ ve $x \in G$ olsun. $C_H(x) = \{c \in H : cx = xc\}$ olsun. $C_H(x) \leq G$ olur. (x'in H'deki ***merkezleyicisi*** denir bu altgruba.) $x^H = \{x^h : h \in H\}$ olsun. $H/C_H(x) = \{C_H(x)g : g \in H\}$ olsun. $C_H(x)h \mapsto x^h$ kuralıyla belirlenen fonksiyonun $H/C_H(x)$ kümesinden x^H kümesine giden iyi tanımlı bir fonksiyon olduğunu kanıtlatın. Bu fonksiyonun bir eşleme olduğunu kanıtlayın.

8.36. G bir grup ve $H \leq G$ olsun. $g \in G$ için $H^g = g^{-1}Hg$ tanımını yapalım. $H^g \leq G$ olduğunu kanıtlayın. $N_G(H) = \{g \in G : H^g = H\}$ olsun. $H \leq N_G(H) \leq G$ olduğunu kanıtlayın. (H'nin G'deki ***normalleyicisi*** denir bu $N_G(H)$ altgrubuna.)

$$H^G = \{H^g : g \in G\} \text{ ve } G/N_G(H) = \{N_G(H)g : g \in G\}$$

olsun. $N_G(H)g \mapsto H^g$ kuralıyla belirlenen fonksiyonun $G/N_G(H)$ sağ ötelemeler kümesinden H^G kümesine giden iyi tanımlı bir fonksiyon olduğunu kanıtlayın. (Bir başka deyişle $N_G(H)g = N_G(H)g_1$ ise $H^g = H^{g_1}$ eşitliğini kanıtlamalısınız.) Bu fonksiyonun bir eşleme olduğunu kanıtlayın.

8.37. G bir grup ve H, $K \leq G$ olsun. $N_K(H) = \{g \in K : H^g = H\}$ olsun.

$$K \cap H \leq N_K(H) \leq K$$

olduğunu kanıtlayın. (H'nin K'daki ***normalleyicisi*** denir bu $N_K(H)$ altgrubuna.)

$$H^K = \{H^g : g \in K\} \text{ ve } K/N_K(H) = \{N_K(H)g : g \in K\}$$

olsun. $N_K(H)g \mapsto H^g$ kuralıyla belirlenen fonksiyonun $K/N_K(H)$ sağ ötelemeler kümesinden H^K kümesine giden iyi tanımlı bir fonksiyon olduğunu kanıtlayın.

8.38. $X \subseteq G$ altkümesi G'yi üretsin ve $0 < n \in \mathbb{N}$ olsun.

$$G_n = \left\{ x_1^{k_1} \cdots x_r^{k_r} : r \in \mathbb{N},\, x_i \in X,\, k_i \in \mathbb{Z},\, \sum_i k_i \equiv 0 \bmod n \right\}$$

altgrubunun G'deki indeksinin en fazla n olduğunu kanıtlayın.

8.39. Bir önceki alıştırmada $G = \operatorname{Sym} m$ ve $n = 2$ olsun. X makaslardan oluşan küme olsun. X'in G'yi ürettiğini Altbölüm 3.4'ten biliyoruz. $m = 2, 3, 4$ için bir önce alıştırmada tanımlanan G_2 altgrubunun indeksinin tam 2 olduğunu gösterin. Eğer n bir tek sayıysa indeksin 1 olduğunu gösterin.

8.40. Bu bölümü önemli bir sonuçla bitirelim:

Teorem 8.10. *p bir asal, $n > 0$ bir doğal sayı ve G, p^n elemanlı bir grup ise, $Z(G) \neq 1$ olur.* □

Kanıt: p bir asal, $n > 0$ bir doğal sayı ve G, p^n elemanlı bir grup olsun. Örnek 8.33'den dolayı her $g \in G$ için $|g^G| = |G|/|C_G(g)|$ olur, yani p'nin bir kuvveti olur.

$$g \in Z(G) \Leftrightarrow g^G = \{g\} \Leftrightarrow C_G(g) = G$$

eşdeğerliğinden dolayı, eğer $g \notin Z(G)$ ise, g^G eşleniklik sınıfının eleman sayısı p'nin pozitif bir kuvvetidir, dolayısıyla p'ye bölünür. Ayrıca G'nin eleman sayısı da p'ye bölünür. Eşleniklik sınıfları ayrık olduklarından (Alıştırma 1.26) G kümesini eşleniklik sınıflarının ayrık bileşimi olarak yazabiliriz:

$$G = Z(G) \sqcup \bigsqcup_{\text{bazı } g \notin Z(G) \text{ için}} g^G$$

olur. En sağdaki bileşimdeki her eşleniklik sınıfı p'ye bölündüğünden, $Z(G)$'nin eleman sayısı da p'ye bölünür, yani $Z(G) \neq 1$ olur. □

8.41. Aşağıdaki sonuca göre 169 elemanlı gruplar çok karmaşık olamazlar:

Sonuç 8.11. *p bir asal olsun. p^2 elemanlı her grup bir abel grubudur.*

Kanıt: G, p^2 elemanlı bir grup olsun. Bir önceki teoreme göre $Z(G) > 1$. Eğer $Z(G)$'nin p^2 elemanı varsa $Z(G) = G$ olur ve sorun kalmaz. Eğer $Z(G)$'nin p elemanı varsa, o

zaman $G/Z(G)$ grubunun p elemanı vardır, dolayısıyla döngüseldir. $\overline{g} \in G/Z(G)$ elemanı bir üreteç olsun. O zaman $G = \langle Z(G), g\rangle$ olur, dolayısıyla abeldir. □

Bunun sonucu olarak ileride p^2 elemanlı bir grubun ya $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ ya da $\mathbb{Z}/p^2\mathbb{Z}$ grubuna çok benzediğini (cebirin jargonunda izomorf olduğunu) göreceğiz.

Alıştırmalar

8.42. Sadece iki eşleniklik sınıfı olan bir grubun sadece 2 elemanı olduğunu kanıtlayın. (Teorem 8.10'u kullanabilirsiniz.)

9. Normal Altgrup ve Bölüm Grubu

Bu sefer soyut cebirin en önemli konusuna gerçekten geldik.

9.1 Normal Altgrup

G bir grup ve $H \leq G$ olsun. Bir önceki yazıdan G/H sol bölüm kümesinin tanımını anımsayalım:

$$G/H = \{xH : x \in G\}.$$

Bu küme üzerinde olabilecek en doğal ve aklımıza gelebilecek ilk yolla bir çarpma işlemi tanımlamaya kalkışalım: Her x, $y \in G$ için

$$(xH)(yH) = xyH$$

olsun. Görüldüğü gibi G/H kümesi üzerine tanımladığımızı iddia ettiğimiz bu işlem G'nin işlemini yansıtıyor; G/H'nin elemanlarını çarpmak için G'nin üzerine var olan çarpmayı kullanıyoruz.

Birazdan bu işlemin tanımda bir sorun olduğunu göreceğiz, ama bir an için bu tanımda bir sorun olmadığını kabul edip özelliklerini görelim.

Her şeyden önce G/H kümesinden alınan iki elemanın çarpımı gene bu kümede. Bunun dışında şu özellikler doğru:

1. *Bu işlemin birleşme özelliği vardır, yani her x, y, $z \in G$ için*

$$(xH)((yH)(zH)) = ((xH)(yH))(zH)$$

olur.

Bunun kanıtı çok basit:

$$\begin{aligned}(xH)((yH)(zH)) &= (xH)(yzH) = x(yz)H = (xy)zH \\ &= (xyH)(zH) = ((xH)(yH))(zH).\end{aligned}$$

2. *Bu işlemin bir etkisiz elemanı vardır.*

Nitekim $H \in G/H$ işlemin etkisiz elemanıdır çünkü her $x \in G$ için,

$$(xH)H = (xH)(1H) = x1H = xH$$

ve

$$H(xH) = (1H)(xH) = (1x)H = xH$$

olur.

3. *G/H kümesinin her elemanının bu işlem için bir tersi vardır.*

Nitekim xH elemanının tersi $x^{-1}H$ elemanıdır. (Etkisiz elemanın H olduğunu unutmayalım.) Bunu kontrol edelim:

$$(xH)(x^{-1}H) = xx^{-1}H = 1H = H \text{ ve } (x^{-1}H)(xH) = x^{-1}xH = 1H = H.$$

Böylece G/H kümesinin bu işlem altında bir grup olduğunu gördük... Yalnız tanımda bir hata var, o da şu: $(xH)(yH) = xyH$ kuralının gerçekten bir işlem tanımladığını göstermedik. Yani $xH = x_1H$ ise ve ayrıca $yH = y_1H$ ise, elbette

$$(xH)(yH) = (x_1H)(y_1H)$$

olmalı; aksi halde eşit elemanları çarparak farklı sonuçlar buluruz ki bu da işlem iyi tanımlanmamış demektir. Sorun şu ki xH ötelemesi x'i belirlemiyor; nitekim xH ötelemesinin her x_1 elemanı için $xH = x_1H$ olur ve çarpmada x yerine x_1 kullanırsak bir başka sonuç bulabiliriz.

Bu tanım sorununun biraz üstüne gidelim, önemlidir çünkü. Eğer

$$\pi : G \longrightarrow G/H$$

fonksiyonu,

$$\pi(x) = xH$$

kuralıyla tanımlanmışsa, G/H'nin α ve β elemanlarını çarpmak için, verilen tanıma göre, α ve β'nın π-önimgelerinden sırasıyla birer x ve y elemanı seçilir ve sonra $\alpha\beta$ çarpımı $\pi(xy)$ olarak tanımlanır. Aşağıdaki şekildeki görsellikle ifade edecek olursak, α ve β'yı çarpmak için "yukarı çık, çarp, aşağı in". Yani α, $\beta \in G/H$ elemanlarını çarpmak için,

1. $\pi^{-1}(\alpha)$ ve $\pi^{-1}(\beta)$ kümelerinden birer $x \in G$ ve $y \in G$ elemanı seç,
2. G grubunda xy çarpımını yap,
3. Şimdi $\alpha\beta$ çarpımını $\pi(xy)$ olarak tanımla.

Şekil gelecek, pi'li fila. alfa ve beta çarpılıyor... Yukarı çık aşağı in.

Sorun birinci adımdaki x ve y seçimlerinde. Farklı x ve y seçimleri için farklı $\pi(xy)$ sonuçları bulunabilir; nitekim aşağıdaki örnek de bazen gerçekten farklı sonuç bulacağımızı gösteriyor.

Notlar ve Örnekler

9.1. $G = \operatorname{Sym} 5$ ve $H = \operatorname{Sym} 4$ olsun. H'yi G'nin bir altgrubu olarak görebileceğimizi biliyoruz. $\alpha = (1\ 5)H \in G/H$ ve $\beta = (2\ 5)H \in G/H$ olsun.

$$\alpha = (1\ 5)H = (1\ 2\ 5)H = \{\sigma \in \operatorname{Sym} 5 : \sigma(5) = 1\}$$

eşitliğini Örnek 8.1'de gösterdik. Şimdi yukarıda metinde önerdiğimiz gibi $\alpha\beta$ çarpımını hesaplayalım. Bir yandan,

$$\alpha\beta = (1\ 5)H(2\ 5)H = (1\ 5)(2\ 5)H = (1\ 5\ 2)H = \{\sigma \in \operatorname{Sym} 5 : \sigma(5) = 2\}$$

olur, diğer yandan,

$$\alpha\beta = (1\ 2\ 5)H(2\ 5)H = (1\ 2\ 5)(2\ 5)H = (1\ 2)H = H = \{\sigma \in \operatorname{Sym} 5 : \sigma(5) = 5\}$$

olur; iki farklı yanıt!

9.2. $G = \operatorname{Sym} 4$ ve $H = \{\mathrm{Id}_4, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ olsun. $H \leq G$ olur. Bu sefer G/H kümesinde yukarıda metinde önerilen işlem herhangi bir sorun arzetmez, yani her x, x_1, y, $y_1 \in \operatorname{Sym} 4$ için, eğer $xH = x_1H$ ve $yH = y_1H$ ise,

$$(xH)(yH) = (x_1H)(y_1H)$$

olur.

Tanımın sorunsuz olması için şu özellik doğru olmalı elbette:

Her x, x_1, y, $y_1 \in G$ için, eğer $xH = x_1H$ ve $yH = y_1H$ ise $xyH = x_1y_1H$.

Bu özelliği sağlayan G'nin H altgruplarına ***normal*** adı verilir. Ama bu tanım, her ne kadar doğal olsa da, çok kullanışlı olmadığından, buna eşdeğer bir koşul bulmak yararlı olacaktır. Şimdi bunu yapıyoruz:

Teorem 9.1. *H'nin G'nin normal bir altgrubu olması için yeter ve gerek koşul her $x \in G$ için $xH = Hx$ eşitliğinin doğru olmasıdır.*

Kanıt: Önce H'nin G'nin normal bir altgrubu olduğunu varsayalım. Her $x \in G$ ve $h \in H$ için, $hH = 1H$ ve $xH = xH$ olduğundan, varsayıma göre, $hxH = 1xH = xH$, yani $hx \in xH$ olmalıdır. Demek ki $Hx \subseteq xH$. Eğer bu eşitlikte x yerine x^{-1} alırsak, $Hx^{-1} \subseteq x^{-1}H$ elde ederiz; kümelerin elemanlarının tersini alırsak da $xH \subseteq Hx$ elde ederiz. Demek ki $Hx = xH$.

Şimdi her $x \in G$ için $xH = Hx$ eşitliğinin doğru olduğunu varsayalım. x, x_1, y, $y_1 \in G$ elemanları $xH = x_1H$ ve $yH = y_1H$ eşitliklerini sağlasınlar. Hesap yapalım:

$$xyH = xy_1H = xHy_1 = x_1Hy_1 = Hx_1y_1 = x_1y_1H.$$

İstediğimizi kanıtladık. □

Tanım Üzerine. Teoremdeki koşul akılda tutulması çok daha kolay olduğundan, normal altgrubun tanımı kitaplarda bizim yaptığımız gibi yapılmaz; şöyle yapılır: Eğer $H \leq G$ altgrubu

$$\text{Her } x \in G \text{ için } xH = Hx$$

özelliğini sağlıyorsa[1], yani altgrubun sağ ötelemeleriyle sol ötelemeleri arasında bir fark yoksa H'ye G'nin ***normal altgrubu*** olduğu söylenir ve bu durum yazılı olarak

$$H \lhd G$$

biçiminde gösterilir. Bazen "H'ye, G'de normal" ya da G-***normal*** denir çünkü eğer $H \lhd G \leq G_1$ ise "$H \lhd G_1$" önermesi doğru olmayabilir. Hatta $H \lhd G \lhd G_1$ ise de $H \lhd G_1$ doğru olmayabilir. Bu yüzden H'nin G-normal ya da G_1-normal olduğunu özellikle belirtmekte yarar vardır (bkz. Örnek 9.7). Eğer H, G'de normal ise, bazen H'nin G-***normal*** olduğu söylenir.

Elbette $xH = Hx$ eşitliği ile $x^{-1}Hx = H$ eşitliği eşdeğerdir. $H^x = x^{-1}Hx$ tanımını anımsatırız. Bu eşitliği sağlayan bir x elemanının H'yi normalize ettiği söylenir. Demek ki bir $H \leq G$ altgrubunun G-normal olması için yeter ve gerek koşul,

$$\text{her } x \in G \text{ için } H^x = H$$

koşuludur. Şimdi bir $H \leq G$ altgrubu için şu tanımı yapalım:

$$N_G(H) = \{x \in G : H^x = H\}.$$

Elbette $H \leq N_G(H) \leq G$ olur. Ve gene elbette $H \lhd N_G(H)$ olur. Hatta $N_G(H)$, H'nin içinde normal olduğu G'nin en büyük altgrubudur. $N_G(H)$ altgrubuna G'nin ***normalleyicisi*** adı verilir.

Demek ki H'nin G-normal olması için yeter ve gerek koşul $N_G(H) = G$ eşitliğidir. Normalliğin bir başka eşdeğer koşulu

$$\text{her } x \in G \text{ için } H^x \subseteq H$$

koşuludur (bkz. Alıştırma 5.39). Ama dikkat, özel bir x elemanı için $H^x \subseteq H$ içindeliği $H^x = H$ eşitliği anlamına gelmeyebilir; eşitliğin olması için içindeliğin her x için olması gerekmektedir.

Eğer bir $K \leq G$ altgrubu için $K \leq N_G(H)$ oluyorsa, o zaman K'nın H'yi ***normallediği*** söylenir. Bu durumda $\langle H, K\rangle = HK$ eşitliğinin doğru olduğunu geçmişte, Önsav 5.3'te üstü kapalı bir biçimde söylemiştik. Okur bu önemli olguyu bir defa daha kontrol etmek isteyebilir (bkz. Alıştırma 9.8.)

Bu altbölümde kanıtladıklarımızı özetleyelim.

Teorem 9.2. *$H \lhd G$ olduğunda, G/H bölüm kümesi üzerine G'nin grup yapısını yansıtan bir grup yapısı vardır. Bu grup yapısı*

$$(xH)(yH) = xyH$$

çarpım kuralıyla tanımlanır. G/H grup yapısının etkisiz elemanı H'dir. ayrıca $xH \in G/H$ elemanının tersi $x^{-1}H$ elemanıdır. □

[1]Eğer her $h \in H$ için $xh = hx$ ise, elbette $xH = Hx$ eşitliği sağlanır, ama $xH = Hx$ eşitliğinin sağlanması için illa bu değişme özelliği gerekli değildir; her $h \in H$ için, $xh = h_1x$ ve $hx = xh_2$ eşitliklerinin sağlandığı h_1, $h_2 \in H$ olması eşitliğin sağlanması için yeter.

G/H grubuna ***bölüm grubu*** adı verilir. Eğer $H \lhd G$ ve $[G : H] = n < \infty$ ise, bu durum kısaca

$$H \overset{n}{\lhd} G$$

olarak gösterilir.

xyH olarak tanımlanan $(xH)(yH)$ çarpımının gerçekten xH kümesinin elemanlarıyla yH kümesinin elemanlarını (bu sırayla) çarpmak demek olduğunu görelim: Her $h, h_1 \in H$ için, $y^{-1}hy \in H^y = Y$ olduğundan, $(xh)(yh_1) = (xy)(y^{-1}hyh_1) \in xyH$ olur. Demek ki xH ile yH'nin elemanlarını bu sırayla çarptığımızda sonuç $xyH = (xH)(yH)$ kümesinde çıkıyor. Ters istikamet bariz: $xyh = (x1)(yh)$. Demek ki,

$$\{(xh)(yh_1) : h, h_1 \in H\} = xyH.$$

Ancak G/H grubunun çarpımını altkümelerin çarpımı olarak görmek yanlıştır. Hiçbir cebirci G/H üzerindeki çarpımı böyle görmez. Bu konudan sonraki altbölümlerde daha etraflıca sözedeceğiz.

Notlar ve Örnekler

9.3. Eğer G bir abel grubuysa, elbette her $H \leq G$ ve her $x \in G$ için $xH = Hx$ olur. Demek ki bu durumda G'nin her altgrubu normaldir.

9.4. G'nin merkezinin

$$Z(G) = \{z \in G : \text{ her } g \in G \text{ için } zg = gz\}$$

olarak tanımlandığını anımsayalım. $Z(G)$ bir altgruptur. $Z(G) \lhd G$ olduğunu göstermek kolaydır.

9.5. Eğer $H \leq G$ altgrubunun indeksi 2 ise, o zaman $H \lhd G$ olur. Nitekim bu durumda G'nin sadece iki sol ötelemesi ve iki sağ ötelemesi vardır. Bu ötelemelerden biri H'dir. Eğer $x \in G \setminus H$ ise, xH diğer sol ve Hx diğer sağ ötelemedir. Demek ki $G = H \sqcup xH = H \sqcup Hx$. Buradan da $Hx = xH$ çıkar. Eşitlik $x \in H$ iken bariz olduğundan, istediğimiz kanıtlanmıştır. Buradan da $\operatorname{Alt} n \lhd \operatorname{Sym} n$ çıkar.

9.6. $\operatorname{Sym} n$'nin $\operatorname{Sym}(n+1)$'deki indeksi $n+1$'dir ama eğer $n \geq 2$ ise normallik sözkonusu olamaz. Demek ki bir önceki örnekteki olgu, 2 yerine (mesela) 3 için yanlıştır. Ama daha sonra şunu kanıtlayacağız: Eğer p, $|G|$'yi bölen en küçük asal sayıysa, G'deki indeksi p olan altgruplar normaldirler (bkz. Sonuç 10.17).

9.7. $H = \{\mathrm{Id}_4, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ kümesinin $\operatorname{Sym} 4$'ün bir altgrubu olduğunu biliyoruz. $H \lhd G$ olur. (Bu, elle de gösterilebilir ama ayrıca Alıştırma 9.19 da kullanılabilir.) H ayrıca bir abel grubudur. Demek ki $K = \{\mathrm{Id}_4, (1\ 2)\} \lhd H$ olur. Ama K'nın G'de normal olmadığını göstermek kolay. (Teorem 3.3 de zaten öyle söylüyor.) Böylece $K \lhd H$ ve $H \lhd G$ olduğu ama $K \lhd G$ olmadığı bir örnek bulmuş olduk. Normallik ilişkisi geçişken bir ilişki değildir.

9.8. $H \lhd G$ ve $K \leq G$ olsun. O zaman $\langle H, K\rangle = HK = KH$ olur. Bu dediğimiz Önsav 5.3'ten hemen çıkar. Nitekim $H \lhd G$ olduğundan, $HK \subseteq KH$ olur. Demek ki $HK \leq G$; dolayısıyla $\langle H, K\rangle \subseteq HK$. Olur. $HK \subseteq \langle H, K\rangle$ içindeliği bariz.

Bir önceki paragrafta söylediğimizin doğru olması için illa H'nin normal bir altgrup olması gerekmez, $K \leq N_G(H)$ ise de aynı olgu aynı kanıtla doğrudur: $K \leq N_G(H)$ ise $\langle H, K\rangle = HK$ olur.

Bu alıştırmayı metinde defalarca kullanacağız; dolayısıyla özümsenmesinde yarar vardır.

9.9. $A \lhd G$ olsun. O zaman her $b \in G$ ve $a \in A$ için $[a,b] = a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) \in AA \subseteq A$ olur. Dolayısıyla A, $B \lhd G$ ise, her $a \in A$ ve $b \in B$ için $[a,b] \in A \cap B$ olur, daha profesyonel bir deyişle $[A,B] \leq A \cap B$ olur. Bunun sonucu olarak, eğer ayrıca $A \cap B = \{1\}$ ise $[A,B] = \{1\}$ olur, yani A'nın her elemanı B'nin her elemanıyla değişir.

9.10. 1 ve kendisinden başka normal altgrubu olmayan gruplara ***basit grup*** denir. Örneğin, asal p'ler $\mathbb{Z}/p\mathbb{Z}$ grupları basit gruplardır. Ama bunlar en basit basit gruplardır, basit gruplar genelde bu gruplar kadar basit olmazlar. $n \geq 5$için $\operatorname{Alt} n$ gruplarının basit gruplar olduklarını birazdan kanıtlayacağız. G herhangi bir grup olsun. H basit ama abel olmayan grup olsun. $G \times H$ grubunun normal altgruplarının, bir $G_1 \lhd G$ için $G_1 \times 1$ ya da $G_1 \times H$ biçiminde olduğunu göstereceğiz. Buradaki G_1 tabii ki normal altgrubun ilk izdüşümü olmak zorundadır. $N \lhd G \times H$ olsun. Eğer N'nin elemanlarının ikinci koordinatı hep 1 ise, $N = pr_1(N) \times 1$ olur elbette. Şimdi diyelim N'de ikinci koordinatı 1 olmayan bir eleman var, diyelim (g,h). Eğer $c \in H$ ise, $(g,h)^{(1,c)}(g,h)^{-1} \in N$ olur elbette. Ama,

$$(g,h)^{(1,c)}(g,h)^{-1} = (1,c)^{-1}(g,h)(1,c)(g,h)^{-1} = (1,[c,h]).$$

Bu her $c \in H$ için doğru olduğundan,

$$1 \times [H,h] \leq N$$

olur. h yerine h'nin kuvvetlerini de alırsak,

$$1 \times [H,\langle h\rangle] \leq N$$

buluruz. Ama Alıştırma 9.32.a'ya göre $[H,\langle h\rangle] \lhd H$ olur. $h \neq 1$ ve $Z(H) = 1$ olduğundan, $[H,\langle h\rangle] \neq 1$ olur. H basit bir grup olduğundan $[H,\langle h\rangle] = H$ olur. Demek ki

$$1 \times H \leq N$$

olur. Buradan kolaylıkla istenen sonuç çıkar. Aşağıdaki teorem de bu yaptığımızın bir sonucudur.

Teorem 9.3. *$H_1, \ldots, H_n$ basit ama abel olmayan gruplar olsun. O zaman $H_1 \times \ldots \times H_n$ grubunun tam 2^n tane normal altgrubu vardır ve bu altgruplar bazı koordinatları hep 1 olan, bazı koordinatlarda tüm değerleri alan altgruplardır, yani H_i'lerin bazılarının direkt çarpımıdır.*

9.11. İleride $n \geq 5$ için $\operatorname{Alt} n$ gruplarının basit olduklarını kanıtlayacağız. Şimdilik $n \geq 5$ için $\operatorname{Sym} n$'nin 1, $\operatorname{Alt} n$ ve kendisi olmak üzere sadece 3 tane normal altgrubu olduğunu, yani neredeyse basit olduğunu kanıtlayalım.

Teorem 9.4. *$n \geq 5$ için $\operatorname{Sym} n$'nin 1'den farklı normal bir özaltgrubu $\operatorname{Alt} n$ olmak zorundadır ve $\operatorname{Alt} n$ basit bir gruptur.*

Kanıt: $1 < H \lhd \operatorname{Sym} n$ olsun. H'nin $\operatorname{Alt} n$'yi içerdiğini kanıtlayacağız. Not 7.9'a göre farklı a, b, c, $d \in \{1, \ldots, n\}$ noktaları için ya $(a\ b\ c)$ ya da $(a\ b)(c\ d)$ türünden elemanların H'de olduklarını kanıtlamak yeterli. Teorem 3.3'e göre bu elemanlardan sadece birinin H'de olduğunu göstermek yeterli. $1 \neq \alpha \in H$ olsun. α elemanı $i \in \{1, 2, \ldots, n\}$ noktasını yerinden oynatsın, yani $\alpha(i) \neq i$ olsun. i ve $\alpha(i)$ noktalarından farklı bir $j \in \{1, 2, \ldots, n\}$ seçelim. H'nin $\alpha(i\ j)\alpha^{-1}$ elemanını hesaplayalım. Bu eleman da $(i\ j)$ gibi bir makas olmalı. Kolayca görüleceği üzere $\alpha(i\ j)\alpha^{-1} = (\alpha(i)\ \alpha(j))$ olur. Demek ki

$$\alpha(i\ j)\alpha^{-1}(i\ j) = (\alpha(i)\ \alpha(j))(i\ j).$$

Ama $\alpha(i\ j)\alpha^{-1}(i\ j) = \alpha\alpha^{-(i\ j)} \in H$ çünkü $H \lhd \operatorname{Sym} n$. Demek ki,

$$(\alpha(i)\ \alpha(j))(i\ j) \in H.$$

$\alpha(i) \neq i$, j olduğunu biliyoruz. Eğer $\alpha(j) \neq i\,j$ ise H'de $(a\ b)(c\ d)$ türünden bir eleman buluruz. Eğer $\alpha(j) = i\,j$ ise $(\alpha(i)\ \alpha(j))(i\ j) \in H$ elemanı $(a\ b\ c)$ türünden bir elemandır. □

9.12. $H \leq G$ olsun. $K = \bigcap_{x\in G} H^x$ olsun. Elbette her $g \in G$ için $K^g \subseteq K$ olur. Alıştırma 5.39'a göre, $K \lhd G$ olur. Eğer G'nin bir G-normal L altgrubu H'nin altgrubuysa, o zaman her $x \in G$ için $L = L^x \leq H^x$ olduğundan, $L \leq K$ olur. Demek ki H'nin her G-normal altgrubu K'nın içindedir. K da H'nin bir G-normal altgrubu olduğundan, bundan K'nın H'nin en büyük G-normal altgrubu olduğu çıkar. K'ya H'nin G'deki ***göbeği***[2] adı verilir ve $K = \operatorname{Core}_G H$ ya da daha basit olarak $K = \operatorname{Core} H$ yazılır.

9.13. $H \leq G$ sonlu indeksli bir altgrup olsun. O zaman, Alıştırma 8.36'e göre,

$$|\{H^x : x \in G\}| = |G/N_G(H)| < \infty$$

olur. Örnek 8.21 ve bir önceki alıştırmadaki tanıma göre, $[G : \operatorname{Core}_G H] < \infty$ olur: *Sonlu indeksli bir altgrubun, sonlu indeksli bir G-normal altgrubu vardır.* İleride, eğer $[G : H] = n$ ise, $[G : \operatorname{Core}_G H]$ sayısının $n!$ sayısını böldüğünü kanıtlayacağız (bkz Teorem 10.16).

9.14. Bu notta $n \geq 5$ için $\operatorname{Alt} n$'nin basit bir grup olduğunu kanıtlayacağız.

Alıştırmalar

9.15. $H \lhd G$ önermesiyle $N_G(H) = H$ eşitliğinin aynı anlama geldiğini görün.

9.16. Her $x \in G$ için $xH \subseteq Hx$ ise, H'nin G'de normal olduğunu gösterin.

9.17. Eğer $H \lhd G$ ise, $C_G(H) \lhd G$ olduğunu gösterin.

9.18. Eğer $H \lhd G$ ve $K \leq G$ ise $\langle H, K\rangle = HK = KH$ eşitliklerini gösterin.

9.19. $X \subseteq G$ şu özelliği sağlasın: Her $g \in G$ için $gX \subseteq Xg$. Bu durumda $\langle X\rangle \lhd G$ olduğunu gösterin. (Bkz. Alıştırma 7.43.) Buradan $\{\mathrm{Id}_4, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \lhd \operatorname{Sym} 4$ olduğunu gösterin. (Teorem 3.3'ye de bakabilirsiniz.)

9.20. $X \subseteq G$ olsun. Eğer her $g \in G$ için $X^g = X$ ise, $\langle X\rangle \lhd G$ olduğunu gösterin (bkz. sayfa 124). Eğer her $g \in G$ için $X^g \subseteq X$ ise, $\langle X\rangle \lhd G$ olduğunu gösterin. $\left\langle \bigcup_{g\in G} X^g \right\rangle \lhd G$ olduğunu gösterin.

9.21. Sonlu ya da sonsuz sayıda normal altgrubun kesişiminin her zaman normal bir altgrup olduğunu gösterin. Buradan, eğer $X \subseteq G$ ise,

$$\bigcap_{X\subseteq H\lhd G} H$$

kümesinin X'i içeren en küçük normal altgrup olduğunu gösterin.

$$\bigcap_{X\subseteq H\lhd G} H = \left\langle \bigcup_{g\in G} X^g \right\rangle$$

eşitliğini gösterin. Bu gruba, X tarafından ***üretilmiş*** en küçük normal altgrup adı verilir. Bu grup $\langle\langle X\rangle\rangle$ olarak ya da $\langle X^G\rangle$ olarak yazılır.

9.22. $X \subseteq G$ altkümesi G'yi üretsin.

$$G_n = \left\{ x_1^{k_1} \cdots x_r^{k_r} : r \in \mathbb{N},\ x_i \in X,\ k_i \in \mathbb{Z},\ \sum_i k_i \equiv 0 \mod n \right\}$$

grubunun G'de normal olduğunu kanıtlayın. (Bu konuyla ilgili bkz. Alıştırma 8.38.)

[2] İngilizcesi *core*.

9.23. G bir grup, $A \lhd G$, $B \leq G$ ve $A \leq C \leq G$ olsun. $A < AB \cap C$ ile $B \cap C \not\leq A$ koşullarının eşdeğer olduklarını kanıtlayın.

9.24. Eğer $n \geq 3$ ise $Z(\operatorname{Sym} n) = \{\mathrm{Id}_n\}$ olduğunu kanıtlayın.

9.25. $Z_2(G) = \{z \in G : \text{her } g \in G \text{ için } g^{-1}z^{-1}gz \in Z(G)\}$ olsun. $Z_2(G) \lhd G$ olduğunu kanıtlayın.

9.26. $x, y \in G$ için $[x, y] = x^{-1}y^{-1}xy$ tanımını anımsayın. $G' = \langle [x, y] : x, y \in G \rangle$ olsun. $G' \lhd G$ olduğunu kanıtlayın. G' grubuna G'nin ***türevi*** ya da ***birinci türevi*** adı verilir.

9.27. $H, K \lhd G$ için $[H, K] = \langle [x, y] : x \in H, y \in K \rangle$ olsun. $[H, K] \lhd G$ olduğunu kanıtlayın.

9.28. $H_1 \lhd H$ ve $G_1 \lhd G$ koşullarıyla $H_1 \times G_1 \lhd H \times G$ koşulunun eşdeğer olduğunu kanıtlayın.

9.29. G bir grup olsun. $\{(g, g) \in G \times G\}$ ne zaman $G \times G$'nin normal bir altgrubu olur?

9.30. G bir grup ve $X = \{(g, g) \in G \times G\}$ olsun. $G' \times G' \leq \langle X^G \rangle$ olduğunu gösterin. (G' altgrubunun tanımı için bkz. Alıştırma 9.26.)

9.31. $\operatorname{Sym}^{<\omega} \mathbb{N}$ altgrubunun (bkz. Alıştırma 3.10) $\operatorname{Sym} n$'de normal olduğunu kanıtlayın.

9.32. (P. Hall, [H]) **a.** $x, y, z \in G$ için $[x, yz] = [x, z][x, y]^z$ and $[xy, z] = [x, z]^y[y, z]$ eşitliklerini gösterin. Buradan, eğer $H, K \leq G$ ise H ve K gruplarının $[H, K]$ altgrubunu normalize ettiğini gösterin ($[H, K]$ altgrubunun tanımı için bkz. Alıştırma 9.27). Buradan $[H, G] \lhd G$ olduğunu gösterin.

b. Eğer $A \leq G$ bir abel altgrubuysa ve $g \in N_G(A)$ ise $\operatorname{ad}_g(a) = [g, a]$ formülüyle tanımlanmış $\operatorname{ad}(g) : A \longrightarrow A$ fonksiyonunun bir homomorfizma olduğunu ve çekirdeğinin $C_A(g)$ olduğunu kanıtlayın.

c. $x, y, z \in G$ olsun.

$$[[x, y^{-1}], z]^y[[y, z^{-1}], x]^z[[z, x^{-1}], y]^x = 1$$

eşitliğini gösterin. Buradan eğer $H, K \leq G$ ise ve $[[H, K], K] = 1$ ise $[H, K'] = 1$ olduğunu kanıtlayın. ($K' = [K, K]$ olarak tanımlanmıştır; bkz. Alıştırma 9.26.)

d. P. Hall Üç Altgrup Önsavı. H, K ve L altgrupları G'de normal olsunlar. (c)'yi kullanarak

$$[[H, K], L] \leq [[K, L], H][[L, H], K]$$

içindeliğini kanıtlayın.

e. $G^0 = G$ ve $G^{i+1} = [G^i, G]$ olsun. $G^i \lhd G$ ve $G^{i+1} \leq G^i$ olduğunu kanıtlayın.

f. $G^{(0)} = G$ ve $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ olsun. $G^{(i)} \lhd G$ ve $G^{(i+1)} \leq G^{(i)}$ olduğunu kanıtlayın. (d)'yi kullanarak $[G^i, G^j] \leq G^{i+j+1}$ ve $G^{(i)} \leq G^{2^i-1}$ içindeliklerini kanıtlayın.

9.33. $H, K \leq G$ ve $A, B \leq Z(G)$ olsun. $[AH, BK] = [H, K]$ eşitliğini kanıtlayın. (Alıştırma 9.32.a'daki eşitliklerden yararlanabilirsiniz.)

9.34. $A, B, C, D \lhd G$ olsun. $[AB, CD] \leq [A, C][B, C][A, D][B, D]$ olduğunu kanıtlayın.

Not. G bir grup olsun. $\equiv$, G üzerine bir denklik ilişkisi olsun. Eğer $x \in G$ ise, x'in denklik sınıfını $[x]$ olarak yazalım, yani

$$[x] = \{a \in G : a \equiv x\}$$

olsun. $G/\equiv$, G'nin denklik sınıflarından oluşan küme olsun, yani

$$G/\equiv = \{[x] : x \in G\}.$$

$G/\equiv$ kümesi üzerine ikili bir işlem tanımlama deneyiminde bulunalım: $[x], [y] \in G/\equiv$ için

$$[x][y] = [xy] \tag{1}$$

olsun. Bunun geçerli bir tanım olması için her x, x_1, y, $y_1 \in G$ için

$$x \equiv x_1 \text{ ve } y \equiv y_1 \text{ ise } xy \equiv x_1 y_1 \tag{2}$$

önermesinin doğru olması gerekmektedir.

Teorem 9.5. *Her x, x_1, y, $y_1 \in G$ için (2) önermesinin doğru olması için, yani $G/\equiv$ kümesi üzerine (1)'deki tanımın geçerli olması için $H = [1]$ normal bir altgrup olmalı ve denklik ilişkisi*

$$x \equiv y \Leftrightarrow xH = yH$$

eşdeğerliği tarafından verilmeli. Bir başka deyişle $G/\equiv = G/H$ ve $[x] = xH$ olmalı.

Kanıt: x, $y \in [1]$ için, $x \equiv 1$ ve $y \equiv 1$ olduğundan, (2)'ye göre $xy \equiv 1$, yani $xy \in [1]$. Ayrıca $x \equiv 1$ ve $x^{-1} \equiv x^{-1}$ olduğundan, gene (2)'ye göre $1 \equiv x^{-1}$, yani $x^{-1} \in [1]$. Ayrıca 1 elemanının [1]'de olduğu belli. Demek ki [1] bir altgrup.

$x \in [1]$ ve $y \in G$ olsun. O zaman $y^{-1} \equiv y^{-1}$, $x \equiv 1$ ve $y \equiv y$ olduğundan, (2)'ye göre, $y^{-1}xy \equiv y^{-1}1y = 1$, yani $y^{-1}[1]y \subseteq [1]$ olur. Bu da [1] altgrubunun normal olduğunu gösterir.

Şimdi $x \equiv y$ varsayımını yapalım. $y^{-1} \equiv y^{-1}$ olduğundan (2)'ye göre, $y^{-1}x \equiv 1$, yani $y^{-1}x \in [1]$, yani $x[1] = y[1]$ olur.

Son olarak $x[1] = y[1]$ olsun. O zaman $y^{-1}x \in [1]$, yani $y^{-1}x \equiv 1$ olur. Ama $y \equiv y$ olduğundan, (2)'den $x \equiv y$ çıkar. □

9.2 Bölüm Grubuna Hazırlık

Okur muhtemelen modüler sayıları lise yıllarından biliyordur. Modüler sayılarda, bir n doğal sayısı seçilir ve birdenbire bu n'nin 0'a eşit olduğuna hükmedilir ve bu hükmün sonuçlarına katlanılır, örneğin $3(n+1)^2-7(n-1)+4$ sadece 14'e eşit olur. İşte bir G grubunu bir H normal altgrubuna "bölmek" demek, özünde H'nin elemanlarını 1'e eşitleyip bu eşitlemenin sonuçlarına katlanmak demektir. Bu altbölümde bu konuyu işleyeceğiz. Ama lütfen okur bu altbölümü bitirdiğinde konuyu hemen özümseyeceğini düşünmesin. Tecrübeyle sabittir ki, bu altbölümün konusu olan bölüm gruplarını özümsemek uzun uğraşlar gerektirir.

Tanımı vermeden önce örneklerle başlayalım. Örneklerde okur normal altgrup görmüyorsa, normal altgrubu gizlediğimizdendir.

Notlar ve Örnekler

9.35. **Serbest Grup.** a ve b iki yeni simge olsun. a^{-1} ve b^{-1} olarak göstereceğimiz iki yeni simge daha yaratalım. Bu dört simgeyle yazılmış sonlu uzunluktaki tüm ***kelimeleri*** (dizileri yani) ele alalım, ama kelimelerimizde a ve a^{-1} ya da b ve b^{-1} yanyana geliyorsa, bu iki terimi kelimeden silme hakkını kendimize tanıyalım. Örneğin

$$aabbbba^{-1}a^{-1}aa^{-1}bb^{-1}b = aabbbba^{-1}a^{-1}b$$

olsun. Ayrıca, kısalık uğruna, örneğin aa yerine a^2, $b^{-1}b^{-1}b^{-1}$ yerine b^{-3} yazalım. Böylece, yukarıdaki örneğimiz

$$aabbbba^{-1}a^{-1}aa^{-1}bb^{-1}b = aabbbba^{-1}a^{-1}b = a^2b^4a^{-2}b$$

olarak yazılır.

1 uzunluğunda 4 kelimemiz var: a, a^{-1}, b, b^{-1}.

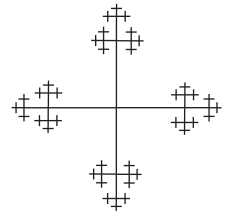
2 uzunluğunda 12 kelimemiz var:

$$a^2,\ ab,\ ab^{-1},\ ba,\ b^2,\ ba^{-1},\ a^{-1}b,\ a^{-2},\ a^{-1}b^{-1},\ b^{-1}a,\ b^{-1}a^{-1}, b^{-2}.$$

Bu kelimelerin sonuna sırasıyla a, b, a^{-1}, b^{-1} koyarak ve uzunluğu kısalanları atarak uzunluğu 3 olan kelimeler elde ederiz. Her bir kelimenin sonuna a, b, a^{-1}, b^{-1} harflerinden üçü geleceğinden (biri sadeleşir), bir sonraki aşamada $12 \times 3 = 36$ yeni kelime yaratırız.

0 uzunluğunda da bir kelime vardır. 0 uzunluğundaki kelime hiç tane simgeyle yazılır. Adına ***boşkelime*** diyebiliriz. Boşkelimeyi 1 olarak simgeleyelim.

Kolayca kanıtlanabileceği üzere, eğer $n \geq 1$ ise n uzunluğunda toplam $4 \times 3^{n-1}$ kelime vardır. Aşağıdaki şekilde tüm kelimeler görülüyor, boşkelime, yani 1 elemanı merkezde. xxxxxxxxx



Bu kümeyi F_2 olarak gösterelim. F_2 kümesi, "kelimeleri yanyana koyup sadeleştirme" işlemi altında bir grup olur. Örneğin $a^2b^2a^{-3}$ ile $ab^{-1}a^2$ elemanlarının bu sırayla çarpımları

$$(a^2b^2a^{-3})(ab^{-1}a^2) = a^2b^2a^{-2}ab^{-1}a^2$$

olur. Bir başka örnek:

$$(a^2b^2a^{-3})(a^4b^{-1}a^2) = a^2b^2ab^{-1}a^2.$$

Bu gruba ***iki eleman tarafından serbestçe üretilmiş grup*** adı verilir. Gruba serbest grup adı verilmesinin nedeni anlaşılmıştır sanıyorum: a ve b elemanları arasında özel hiçbir ilişki yok. Sonraki örneklerde a ve b arasında özel ilişkiler tanımlayacağız.

9.36. Yukarıdaki örneği alalım ama bundan böyle $ab = ba$, yani $a^{-1}b^{-1}ab = 1$ eşitliğini varsayalım. O zaman, en basit grup teorisi bize her n, $m \in \mathbb{Z}$ için $a^nb^m = b^ma^n$ eşitliğini verir. Bu yeni grubun elemanları bir ve bir tek n, $m \in \mathbb{Z}$ sayı çifti için a^nb^m biçiminde yazılırlar, çünkü ne de olsa artık $ba = ab$ eşitliğinden yararlanarak soldaki b'leri kelimelerin en sağına yığabiliriz. Çarpma kuralımız artık şöyledir:

$$(a^nb^m)(a^kb^\ell) = a^{n+k}b^{m+\ell}.$$

Yine bir grup elde ederiz, çünkü grup olma kurallarına riayet ediyoruz. Bu grubun $\mathbb{Z}\times\mathbb{Z}$ grubundan pek farkı yoktur, nitekim $(n, m) \mapsto a^nb^m$ birebir ve örten fonksiyonu bize $\mathbb{Z} \times \mathbb{Z}$ grubuyla bu yeni grup arasında bir tür sözlük görevini görür. Bu örnekteki grup

$$\langle a,\, b \mid a^{-1}b^{-1}ab\rangle$$

olareak yazılır. $\mid$ simgesinden önce gelen simgeler üreteçleri, bu simgeden sonra gelen kelimeler de 1'e eşitlenmesi gereken kelimeleri gösterir.

9.37. Örnek 9.35'ü tekrar ele alalım (artık bir önceki örnekteki $ab = ba$ eşitliği geçerli değil) ama bundan böyle $a^2 = 1$, $b^3 = 1$ eşitliklerini varsayalım. O zaman $a^{-1} = a$ ve $b^{-1} = b^2$ olur ve dolayısıyla a^{-1} ve b^{-1} terimlerine ihtiyacımız kalmaz, bu terimler yerine

sırasıyla a ve b^2 yazabiliriz. Ayrıca a^2 ve b^3 elemanları da yok olurlar, çünkü bunlar 1'e eşittirler. Böylece kelimelerde sadece a, b ve b^2 görünür olur; ve tabii bir de boşkelime olan 1 elemanı. Bu yeni grubun elemanlarını önce uzunluklarına göre, sonra alfabetik sıralamalarına göre dizebiliriz:

$$\begin{array}{c} 1, \\ a,\ b, \\ ab,\ ba,\ b^2, \\ aba,\ ab^2,\ bab,\ b^2a, \\ abab,\ ab^2a,\ baba,\ bab^2,\ b^2ab \\ \dots \end{array}$$

Bu küme üzerinde de bir çarpma işlemi var, ama çarpma yaparken olası sadeleştirmeleri yapmakta yarar var. Mesela,

$$(ababab^2abab^2)(bab^2abababb^2) = abab^2ab^2$$

olur, çünkü parantezleri kaldırdığımızda ortaya çıkan b^2b yok olur ve ardından başka terimler de yok olur. Böylece grubumuzun elemanları, $k \in \mathbb{N}$, $m_1, \dots, m_{k-1} \in \{1, 2\}$, $n \in \{0,\ 1\}$ ve $m_k \in \{0,\ 1,\ 2\}$ sayıları için bir ve bir tek biçimde

$$a^n b^{m_1} ab^{m_2} \cdots ab^{m_{k-1}} ab^{m_k}$$

olarak yazılır. Bu, sonsuz bir gruptur[3]. Bu grup,

$$\langle a,\ b \mid a^2,\ b^3 \rangle$$

olarak gösterilir.

9.38. Bir önceki örneği alalım, yani hâlâ daha $a^2 = 1 = b^3$ olsun, ama ayrıca $(ab)^2 = 1$ olsun. Böylece $abab = 1$, yani $aba = b^{-2} = b$, yani $ba = ab$ olur. Gene b'leri en sağa geçirebiliriz. Bu sefer geriye sonlu sayıda eleman kalır:

$$\{1,\ a,\ b,\ ab,\ b^2,\ ab^2\}.$$

Bu grup,

$$\langle a,\ b \mid a^2,\ b^3,\ (ab)^2 \rangle$$

olarak gösterilir.

9.39. Grubumuz yine F_2 olsun. Gene $a^2 = 1 = b^3$ hükümlerini verelim, ama bir de ayrıca $(ab)^3 = 1$ olsun. Bakalım F_2'den geriye neler kalacak. $1 = (ab)^3 = ababab$ eşitliğinden

$$b^2a = (ab)^{-1} = abab$$

elde edilir. Demek ki kelime listemizde $abab$ belirmeyecek, kelime olarak belirmeyeceği gibi herhangi bir kelimenin içinde de belirmeyecek. Onun yerine daha kısa olan (3 uzunluğunda olan) b^2a koyacağız. Kabul ettiğimiz eşitliklerin bir başka sonucu daha var:

$$baba = ab^2.$$

Dolayısıyla kelimelerde $baba$ yerine daha kısa olan ab^2 yazacağız. Bu eşitliklerden yola çıkarak tüm kelimeleri yazabiliriz. Kelimeleri uzunluklarına göre dizelim. Bir sonraki uzunluktaki kelimeleri bulmak için, bir önceki kelimelerin sonuna a ve b getirelim, ama

[3]Bu tür önermeleri kanıtlamak her zaman kolay değildir. Yöntemi ileri görürüz.

daha kısa gösterimi olan kelimeleri atalım, içinde $abab$ ve $baba$ beliren kelimeleri listeden silebiliriz.

0 uzunluğunda:	1
1 uzunluğunda:	a, b
2 uzunluğunda:	ab, ba, b^2
3 uzunluğunda:	aba, ab^2, bab, b^2a
4 uzunluğunda:	bab^2, b^2ab.

Liste bitti, çünkü 4 uzunluğunda kelimelerin sonuna a ya da b koyarsak daha kısa kelimeler elde ederiz. Elde edilen grubun 12 elemanını bulduk. Eleman sayısı daha da azalabilir mi? Hayır, çünkü $G = \operatorname{Sym} 4$ grubunda $a = (1\ 2)(3\ 4)$ ve $b = (1\ 2\ 3)$ elemanlarını alırsak, $a^2 = b^3 = (ab)^3 = 1$ olur ve bu iki elemanın ürettiği altgrubun tam 12 elemanı vardır (okura alıştırma); bu yüzden grubun eleman sayısı 12'den az olamaz. (Okura düşünmesi için malzeme... $a^2 = b^3 = (ab)^3 = 1$ eşitliklerinin sağlandığı a ve b tarafından üretilen *serbest* grubun eleman sayısı $(1\ 2)(3\ 4)$ ve $b = (1\ 2\ 3)$ tarafından üretilen eleman sayısından daha az olamaz.)
Bu grup,

$$\langle a, b \mid a^2, b^3, (ab)^3 \rangle$$

olarak gösterilir.

Alıştırmalar

9.40. $\langle a, b \mid a^2, b^3, (ab)^4 \rangle$ grubunu hesaplayın.

9.41. $\langle a, b \mid a^2, b^2, (ab)^3 \rangle$ grubunu hesaplayın.

9.42. $\langle a, b \mid a^2, b^2, (ab)^n \rangle$ grubunu hesaplayın.

9.43. $\langle a, b, c \mid a^2, b^2, c^2, (ab)^3, (bc)^3, (ac)^2 \rangle$ grubunu hesaplayın.

9.44. Alfabeyle serbestçe üretilen grupta, sınıfınızdaki öğrencilerin adlarını, soyadlarını ve göbek adlarını 1'e eşitleyin. Kaç elemanlı bir grup elde edersiniz?

9.3 Bölüm Grubu

G bir grup ve $H \lhd G$ olsun. Demek ki her $x \in G$ için $xH = Hx$ eşitliği geçerli. Daha da önemlisi

$$G/H = \{xH : x \in G\}$$

bölüm kümesi üzerinde doğal[4] bir grup yapısı var. Bu durumda xH altkümesini G'nin bir altkümesi olarak görmek yerine G/H grubunun bir elemanı olarak görmek istendiğinden, daha çok bir altkümeyi andıran xH yazılımı yerine bir elemanı daha çok andıran $\overline{x}$ yazılımı kullanılır. Tabii $\overline{x}$ yazılımında H'nin kaybolmuş olması bazen sorun yaratabilir. Mesela H ve K diye iki normal altgrubumuz varsa, $\overline{x}$ yazılımının xH yerine mi yoksa xK yerine mi yazıldığı kuşkuya neden olabilir. Bu gibi durumlarda $\tilde{x}$, $\hat{x}$ gibi varyasyonlar kullanacağız. Demek ki sayfa 116'de $\pi(x) = xH$ olarak tanımlanan $\pi : G \longrightarrow G/H$ izdüşüm fonksiyonunu artık bir üstçizgi ile gösteriyoruz:

$$\pi(x) = \overline{x}.$$

[4] "G'nin grup yapısından kaynaklanan" anlamında.

Eğer H normal altgrubunun ne olduğu konunun gelişinden belliyse ya da önemsizse, G/H yerine $\overline{G}$ yazılır. Ama dikkat, eğer H normal olmayan sade bir altgrupsa, çok mecbur kalmadıkça, xH yerine $\overline{x}$ ve G/H yerine $\overline{G}$ yazılımı tercih edilmez.

Bu yazılımla,

$$\begin{array}{l}(xH)(yH) = xyH \text{ yerine } \overline{x}\,\overline{y} = \overline{xy},\\ H \text{ yerine } \overline{1},\\ (xH)^{-1} = x^{-1}H \text{ yerine } \overline{x}^{\,-1} = \overline{x^{-1}}\\ (xH)^{n} = x^{n}H \text{ yerine } \overline{x}^{\,n} = \overline{x^{n}}\end{array}$$

yazılır. Örneğin, G/H bölüm grubunun $\overline{x}$, $\overline{y}$ ve $\overline{z}^{\,-1}$ elemanlarını çarpmak çok kolaydır:

$$\overline{x}\,\overline{y}\,\overline{z}^{\,-1} = \overline{xyz^{-1}}.$$

Yani G'de işlem yapmasını biliyorsak, G/H'de de işlem yapabiliriz: Elemanların üstündeki çizgiyi silip G'de işlem yapalım ve çıkan sonucun üstüne bir çizgi çekelim; bu kadar basit. Hatta G/H'de işlem yapmak G'de işlem yapmaktan çok daha kolaydır, çünkü G'de 1'e eşit olmayan elemanlar ya da çarpımlar G/H'de $\overline{1}$'e eşit olabilirler. Laf açılmışken,

$$\overline{x} = \overline{1} \Leftrightarrow x \in H$$

eşdeğerliğini unutmayalım, önemlidir. Örneğin,

$$\overline{a}^{\,2}\,\overline{b}^{\,-1}\,\overline{c}^{\,3} = \overline{1}$$

eşitliği, yani

$$\overline{a^{2}b^{-1}c^{3}} = \overline{1}$$

eşitliği ancak ve ancak

$$a^{2}b^{-1}c^{3} \in H$$

ise geçerlidir. Ya da

$$\overline{a}^{\,2}\,\overline{b}^{\,-1}\,\overline{c}^{\,3} = \overline{d}^{\,4}\overline{e}^{\,-3}$$

eşitliği, yani

$$\overline{a}^{\,2}\,\overline{b}^{\,-1}\,\overline{c}^{\,3}\overline{e}^{\,3}\overline{d}^{\,-4} = \overline{1}$$

eşitliği, yani

$$\overline{a^{2}b^{-1}c^{3}e^{3}d^{-4}} = \overline{1}$$

eşitliği ancak ve ancak

$$a^{2}b^{-1}c^{3}e^{3}d^{-4} \in H$$

ise geçerlidir. Yani $\overline{G}$ grubundaki her olguyu G ve H'yle ilgili bir olgu olarak yazabiliriz. Dolayısıyla G grubunun birçok özelliği G/H bölüm grubuna yansır. Aşağıda birçok örnek vereceğiz.

Eğer G toplamsal yazılıyorsa, o zaman çarpımsal yazılımla $\overline{x}\,\overline{y} = \overline{xy}$ olarak yazılan eşitlik

$$\overline{x} + \overline{y} = \overline{x+y}$$

eşitliğine, $\overline{x}^{\,n} = \overline{x^n}$ olarak yazılan eşitlik

$$n\overline{x} = \overline{nx}$$

eşitliğine dönüşür. Yukarıdaki $\overline{a}^{\,2}\,\overline{b}^{\,-1}\,\overline{c}^{\,3} = \overline{d}^{\,4} e^{\,-3}$ örneği de

$$2\overline{a} - \overline{b} + 3\overline{c} = 4\overline{d} - 3\overline{e} \text{ ise } 2a - b + 3c - 4d + 3e \in H$$

haline dönüşür.

Sık sık karşımıza çıkabilecek bir durum: Eğer $H \lhd G$ ve $[G : H] = n$ ise her $g \in G$ için $g^n \in H$ olur; çünkü Sonuç 8.6'ya göre her $g \in G$ için, $\overline{g}^n = \overline{1}$ olur.

Aşağıdaki örneklerde H her zaman G grubunun normal bir altgrubudur.

Notlar ve Örnekler

9.45. G hangi grup olursa olsun, G'nin G altgrubunun normal olduğunu biliyoruz. Yukarıda yapılanlarda $H = G$ alalım. O zaman G'nin tek bir ötelemesi vardır: G. Çünkü her $x \in G$ için $\overline{x} = xG = G$ olur. Demek ki her $x \in G$ için $\overline{x} = \overline{1} = G$ ve $G/G = \{\overline{1}\}$. Dolayısıyla G/G, tek elemanlı gruptur, sadece etkisiz elemanı vardır.

9.46. G hangi grup olursa olsun, G'nin sadece etkisiz elemanından oluşan $\{1\}$ altgrubunun normal olduğunu biliyoruz. Yukarıda yapılanlarda $H = \{1\}$ alalım. O zaman her $g \in G$ için

$$\overline{g} = g\{1\} = \{g\},$$

dolayısıyla

$$G/\{1\} = \{\{g\} : g \in G\}$$

olur. Ayrıca her $x, y \in G$ için, $G/\{1\}$ grubunda,

$$\{x\}\{y\} = \overline{x}\,\overline{y} = \overline{xy} = \{xy\}$$

olur. Bu durumda $G/\{1\}$ grubuyla G grubu arasında, elemanların ve işlemin adları dışında, hiçbir fark yoktur: G'nin x elemanı, $G/\{1\}$ grubunda $\{x\}$ elemanına dönüşür ve G grubundaki xy işlemi $G/\{1\}$ grubunda $\{x\}\{y\} = \{xy\}$ işlemine dönüşür.

9.47. $H \lhd G$, $g \in G$ ve p bir asal olsun. Eğer $g^p \in H$ ise ya $g \in H$ ya da $\deg(\overline{g}) = p$ olur, çünkü $g^p \in H$ ile $\overline{g}^p = \overline{1}$ eşdeğer önermelerdir ve Önsav 4.7'den istediğimiz çıkar.

9.48. G bölünür bir grup[5] ve $H \lhd G$ olsun. O zaman G/H grubu da bölünür bir gruptur. Nitekim eğer $x^n = g$ denklemini G'de çözümü varsa, $x^n = \overline{g}^n$ denkleminin G/H'de çözümü vardır: G'deki çözüm a ise, G/H'deki (bir) çözüm $\overline{a}$ olur.

9.49. Eğer G bir abel grubuysa, $\operatorname{Tor} G$, G'nin burulmalı elemanlarından oluşan küme olsun. $\operatorname{Tor} G$ bir altgruptur. $H \leq G$ olsun. Eğer $K = \{g \in G : \text{ bir } n > 0 \text{ için } g^n \in H\}$ ise $H \leq K \leq G$ ve $\operatorname{Tor}(G/H) = K/H$ olur.

9.50. G bir grup, $H \lhd G$ olsun. Her $h \in H$ için $h^n = 1$ olsun. Eğer $\deg \overline{g} = m$ ise, $g^m \in H$ olduğundan, $g^{mn} = 1$ olur. Okur m'nin $\deg g$'yi, $\deg g$'nin de nm'yi böldüğünü kanıtlamak isteyebilir. Aslında $\deg g = \deg \overline{g} \times \deg(g^{\deg \overline{g}})$ olur.

[5]Yani her $g \in G$ ve $n > 0$ tamsayısı için $x^n = g$ denkleminin G'de bir çözümü olsun. Örneğin $\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{R}^{>0}$ bölünür gruplardır.

9.51. $\mathbb{Z}/p\mathbb{Z}$ gruplarının elemanları

$$\overline{0},\ \overline{1},\ \ldots,\ \overline{p-1}$$

sınıflarıdır. Bildiğimiz gibi bu küme "toplama" işlemi altında bir gruptur; tanım şöyledir:

$$\overline{a}+\overline{b}=\overline{a+b}.$$

9.52. p bir asal olsun. (p'nin bir asal sayı alınması için hiçbir neden yoktur ama bu örnekte yapacaklarımız genelde p asalları için yapılır.) Bir $a\in\mathbb{N}$ doğal sayısı alalım. a sayısını p tabanında yazalım: $a_0,\ a_1,\ \ldots,\ a_k\in\{0,1,\ldots,p-1\}$ için

$$a=a_0+a_1p+\cdots+a_kp^k.$$

$n>k$ için $a_n=0$ olsun ve böylece a'yı

$$a=\sum_{i=0}^{\infty}a_ip^i=a_0+a_1p+\cdots+a_np^n+\cdots$$

olarak yazabilelim. O zaman $\mathbb{Z}/p^n\mathbb{Z}$ grubunda,th:pnisemerkez

$$\overline{a}=\overline{a_0+a_1p+\cdots+a_{n-1}p^{n-1}}$$

olur. Ayrıca bu elemanın $p_0,\ p_1,\ \ldots,\ p_k\in\{0,1,\ldots,p-1\}$ "rakamları" için

$$\overline{b}=\overline{b_0+b_1p+\cdots+b_{n-1}p^{n-1}}$$

biçiminde bir elemana eşit olması için, her $i=0,\ 1,\ \ldots,\ n-1$ için

$$a_i=b_i$$

olmalı. a'nın bu gösterimiyle,

$$p\overline{a}=\overline{a_0p+a_1p^2+\cdots+a_{n-2}p^{n-1}}$$

olur. Ve sağdaki biçimde yazılan her eleman bir başka elemanın p katıdır:

$$\overline{a_0p+a_1p^2+\cdots+a_{n-2}p^{n-1}}=p\overline{a_0+a_1p+\cdots+a_{n-2}p^{n-2}}.$$

Demek ki

$$p\cdot(\mathbb{Z}/p^n\mathbb{Z})=p\,\mathbb{Z}/p^n\mathbb{Z}$$

olur ve bu altgrubun tam p^{n-1} tane elemanı vardır. Benzer şekilde,

$$p^i\overline{a}=\overline{a_0p^i+a_1p^{i+1}+\cdots+a_{n-i-1}p^{n-1}}$$

olur ve Demek ki

$$p^i\cdot\mathbb{Z}/p^n\mathbb{Z}=p^i\mathbb{Z}/p^n\mathbb{Z}$$

olur ve $i\leq n$ için bu altgrubun tam p^{n-i} tane elemanı vardır.

9.53. p gene bir asal olsun. $\mathbb{Z}/p^n\mathbb{Z}$ grubunda çalışacağız. Bir $i\in\mathbb{N}$ için

$$\{\overline{a}\in\mathbb{Z}/p^n\mathbb{Z}:p^i\overline{a}=\overline{0}\}$$

altgrubunun elemanlarını bulacağız. Bunun için bir önceki örnekteki gösterim kullanışlı olacak.

$$\overline{a}=\overline{a_0+a_1p+\cdots+a_{n-1}p^{n-1}}$$

olsun. O zaman,

$$p^i\overline{a}=\overline{a_0p^i+a_1p^{i+1}+\cdots+a_{n-i-1}p^{n-1}}$$

olur. Demek ki $p^i\overline{a} = \overline{0}$ olması için

$$a_0 = a_1 = \ldots = a_{n-i-1} = 0$$

olmalıdır. Yani

$$\overline{a} = \overline{a_{n-i}p^{n-i} + \cdots + a_{n-1}p^{n-1}} = p^{n-i}\overline{a_{n-i} + \cdots + a_{n-1}p^{i-1}}$$

olmalı. Demek ki,

$$\{\overline{a} \in \mathbb{Z}/p^n\mathbb{Z} : p^i\overline{a} = \overline{0}\} = p^{n-i} \cdot \mathbb{Z}/p^n\mathbb{Z} = p^{n-i}\mathbb{Z}/p^n\mathbb{Z}$$

olur. Bu grubun tam p^i tane elemanı vardır.

9.54. $1 < H_1 < H_2 < \ldots < H_n = G$ olsun ve $[H_{i+1} : H_i] = p$ varsayımını yapalım. O zaman her $g \in G$ için $g^{p^n} = 1$ olur, ama g'nin derecesi daha düşük olabilir. Öte yandan derecesi p^i olan elemanlar $H_{i+1} \setminus H_i$ kümesindedir.

9.55. $\mathbb{Q}/\mathbb{Z}$ grubunun her elemanının derecesi sonludur. Nitekim eğer $n, m \in \mathbb{Z}$ için $q = n/m$ ise, $|m|q \in \mathbb{Z}$ olduğundan, $\mathbb{Q}/\mathbb{Z}$ grubunda $|m|\overline{q} = \overline{|m|q} = \overline{0}$ olur.Q/Z@Q/Z

9.56. G bir abel grubu olsun.

$$T(G) = \{g \in G : \text{ bir } n > 0 \text{ tamsayısı için } g^n = 1\}$$

olsun. $T(G)$, G'nin burulmalı elemanlarından oluşan altkümedir. Elbette $T(G) \leq G$ olur. $G/T(G)$ grubu burulmasızdır, yani 1'den başka burulmalı elemanı yoktur, çünkü bir $\overline{g} \in G/T(G)$ ve $m > 0$ için $\overline{g}^m = \overline{1}$ olursa, o zaman $g^m \in T(G)$ olur, dolayısıyla bir $n > 0$ için $g^{mn} = (g^m)^n = 1$ olur, ya $g \in T(M)$, bir başka deyişle $\overline{g} = \overline{1}$ olur.

9.57. $X \subseteq G$ kümesi G'yi üretsin. $H \lhd G$ ve $\overline{G} = G/H$ olsun. $\overline{X} = \{\overline{x} : x \in X\} \subseteq \overline{G}$ tanımını yapalım. O zaman $\overline{X}$ kümesi $\overline{G}$ grubunu üretir. Nitekim G'nin her elemanı X'in elemanlarının ve terslerinin çarpımı olduğundan, bu çarpımın izdüşümünü alınca $\overline{G}$ grubunun her elemanının $\overline{X}$ kümesinin elemanlarının ve terslerinin çarpımı olduğunu görürüz. Bunun özel bir durumu olarak, eğer G döngüsel bir grupsa, G/H grubunun da döngüsel olduğu çıkar.

9.58. Eğer G bir abel grubuysa, G/H de bir abel grubudur, çünkü ne de olsa her $x, y \in G$ için, $\overline{x}\,\overline{y} = \overline{xy} = \overline{yx} = \overline{y}\,\overline{x}$ olur.

9.59. G/H'nin komütatörleri, G'nin komütatörlerinin izdüşümüdür:

$$[\overline{x}, \overline{y}] = \overline{[x, y]}$$

olur. Bunun gibi,

$$\overline{x}^{\,\overline{y}} = \overline{x^y}$$

olur; yani $\overline{x}^{\,\overline{G}} = \overline{x^G}$ olur. Demek ki G/H'deki eşleniklik sınıfları G'deki eşleniklik sınıflarının $\pi : G \longrightarrow G/H$ doğal izdüşüm fonksiyonu altında imgesidir.

9.60. $\overline{G}$ grubunun bir abel grubu olması aslında G ve H'nin bir özelliğidir. $\overline{G}$ grubunun bir abel grubu olmasının ne demek olduğunu anlamaya çalışalım. $\overline{G}$ grubunun abel grubu olması demek, her $a, b \in G$ için $\overline{a}\,\overline{b} = \overline{b}\,\overline{a}$ eşitliğinin geçerli olması demektir; bu son eşitlik de $\overline{a}^{\,-1}\,\overline{b}^{\,-1}\overline{a}\,\overline{b} = \overline{1}$ eşitliğine denktir; ve nihayet bu son eşitlik $a^{-1}b^{-1}ab \in H$, yani $[a, b] \in H$ önermesine denktir. Demek ki G/H grubunun bir abel grubu olması için, yeter ve gerek koşul, her "$a, b \in G$ için $[a, b] \in H$" koşuludur.

9.61. Eğer her $x, y \in G$ için $[x, y]$ elemanı grubun merkezindeyse, aynı şey G/H grubunda da geçerlidir. Yani, her $x, y, z \in G$ için $[[x, y], z] = 1$ ise, aynı şey $\overline{G} = G/H$ grubunda da olur: Her $\overline{x}, \overline{y}, \overline{z} \in \overline{G}$ için $[[\overline{x}, \overline{y}], \overline{z}] = 1$ olur. Öte yandan $[[\overline{x}, \overline{y}], \overline{z}] = 1$ eşitliği, $[[x, y], z] = 1$ eşitliği sağlanmadan da sağlanabilir. Genel olarak,

$$[[\overline{x}, \overline{y}], \overline{z}] = 1 \Leftrightarrow [[x, y], z] \in H$$

önermesi doğrudur.

9.62. $\overline{G} = G/H$ grubunun merkezini betimlemeye çalışalım. Merkez,

$$Z(\overline{G}) = \{\zeta \in \overline{G} : \text{ her } \alpha \in \overline{G} \text{ için } \zeta\alpha = \alpha\zeta\}$$

olarak tanımlanmıştır. $\overline{G}$ grubunun her elemanı bir $g \in G$ için $\overline{g}$ olarak yazıldığından,

$$Z(\overline{G}) = \{\overline{z} \in \overline{G} : \text{ her } g \in G \text{ için } \overline{zg} = \overline{gz}\}$$

olur. Şimdi aşağıdaki eşdeğerlilikleri takip edin:

$$\overline{zg} = \overline{gz} \Leftrightarrow \overline{z}^{-1}\overline{g}^{-1}\overline{zg} = \overline{1} \Leftrightarrow z^{-1}g^{-1}zg \in H \Leftrightarrow [z,g] \in H.$$

Demek ki,

$$Z(\overline{G}) = \{\overline{z} \in \overline{G} : \text{ her } g \in G \text{ için } [z,g] \in H\}$$

Görüldüğü gibi $Z(\overline{G})$ altgrubunun z elemanları, G'de anlamlı olan

$$\text{her } g \in G \text{ için } [z,g] \in H$$

ilişkisiyle betimleniyorlar.

9.63. $x \in G$ olsun. $\overline{G}$ grubunda $\overline{x}$ elemanının merkezleyicisini, yani

$$C_{\overline{G}}(\overline{x}) = \{\overline{g} \in \overline{G} : \overline{gx} = \overline{xg}\}$$

altgrubunu bulalım. Aynen yukardaki gibi hareket ederek,

$$C_{\overline{G}}(\overline{x}) = \{\overline{g} \in \overline{G} : [g,x] \in H\}$$

buluruz.

9.64. $x, y \in G$ için $[x,y] = x^{-1}y^{-1}xy$ tanımını anımsayalım. $G' = \langle [x,y] : x, y \in G\rangle$ olsun. Alıştırma 9.26'da $G' \lhd G$ olduğunu kanıtlamıştık. G' grubuna G'nin ***türev altgrubu*** ya da ***birinci türevi*** adı verilir.
Eğer $G' \leq H \leq G$ ise, $H \lhd G$ olur çünkü her $h \in H$ ve $g \in G$ için

$$g^{-1}hg = hh^{-1}g^{-1}hg = h[h,g] \in HG' \subseteq HH = H$$

olur. Ayrıca G/H bir abel grubudur çünkü her $x, y \in G$ için $[x,y] \in G' \leq H$ olduğu için,

$$[\overline{x},\overline{y}] = \overline{[x,y]} = \overline{1}$$

olur.
Bunun tersi de doğrudur. $H \lhd G$ olsun. Eğer G/H bir abel grubuysa, $G' \leq H$ olur, çünkü her $x, y \in G$ için

$$\overline{[x,y]} = [\overline{x},\overline{y}] = \overline{1}$$

olduğundan, $[x,y] \in H$ olur. Demek ki $G' \leq H$ olur.

9.65. $H \lhd G$ olsun. H altgrubu X altkümesi tarafından, G/H grubu da bir $Y \subseteq G$ için $\{\overline{y} : y \in Y\}$ kümesi tarafından üretilsin. O zaman G grubu XY kümesi tarafından üretilir. Nitekim, $g \in G$ ise, $\overline{g}$ elemanı $y_1, \ldots, y_m \in Y$ için $\overline{g} = \overline{y_1^{\pm 1} \cdots y_m^{\pm 1}}$ olur. Dolayısıyla $gy_m^{\mp 1} \cdots y_1^{\mp 1} \in H$ olur. Ama H, X tarafından üretildiğinden, $x_1, \ldots, x_m \in X$ için $gy_m^{\mp 1} \cdots y_1^{\mp 1} = x_1^{\pm 1} \cdots x_n^{\pm 1}$ ve $g = x_1^{\pm 1} \cdots x_n^{\pm 1} y_1^{\pm 1} \cdots y_m^{\pm 1}$ olur.

9.66. *Eğer $G/Z(G)$ döngüselse, G bir abel grubudur.*
Kanıt: Nitekim eğer $G/Z(G)$ grubu $\overline{a}$ tarafından üretiliyorsa, bir önceki örneğe göre $G = \langle Z(G), a\rangle$ olur. Üreteçler birbiriyle değiştiğinden, G zorunlu olarak bir abel grubu olur (Alıştırma 7.37).

9.67. Bu örnekte $\mathbb{Q}/\mathbb{Z}$ abel grubunu çalışacağız. Eğer $q = k/n$ ise (k, $n \in \mathbb{Z}$ elbette), $nq = k \in \mathbb{Z}$ olduğundan, $\mathbb{Q}/\mathbb{Z}$ grubunda $n\overline{q} = \overline{0}$ olur. Demek ki $\mathbb{Q}/\mathbb{Z}$ burulmalı bir gruptur. Ayrıca k ve n aralarında asalsa, $\deg \overline{q} = n$ olduğunu ve $n\overline{q} = \overline{0}$ eşitliğini sağlayan elemanların, paydası n olarak yazılan q kesirli sayılarının sınıfları olduğunu kanıtlamak zor değil; okura alıştırma olarak bırakıyoruz. Demek ki,

$$A[n] = \{\overline{q} \in \mathbb{Q}/\mathbb{Z} : n\overline{q} = \overline{0}\}$$

altgrubunun tam n tane elemanı vardır ve bu elemanlar

$$\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$$

kesirli sayılarının sınıflarıdır. Bunlar arasında derecesi n olanlar, n'ye asal bir $k = 0, 1, \ldots, n-1$ tamsayısı için

$$\frac{k}{n}$$

biçiminde yazılan kesirli sayıların sınıflarıdır. $A[n]$ altgrubu döngüseldir, mesela $1/n$'nin sınıfı tarafından üretilir. $\mathbb{Q}/\mathbb{Z}$ grubunun, derecesi n olan her eleman bu altgruptadır ve bu altgrubu üretir.

Bu arada $A[n] \leq A[m]$ koşuluyla $n|m$ koşulunun eşdeğer olduğunu ve

$$\mathbb{Q}/\mathbb{Z} = \bigcup_{n \in \mathbb{N}} A[n!]$$

eşitliğini görelim.

Ayrıca $\mathbb{Q}$ bölünür bir grup olduğundan, $\mathbb{Q}/\mathbb{Z}$ grubu da bölünürdür. Nitekim eğer $\overline{q} \in \mathbb{Q}/\mathbb{Z}$ ve $n > 0$ ise, $q' = q/n$ olsun, o zaman $n\overline{q'} = \overline{q}$ olur.

Şimdi p bir asal olsun. $A[p^\infty]$, $\mathbb{Q}/\mathbb{Z}$ grubunun, derecesi p'nin bir kuvveti olan elemanlardan oluşan altkümesi olsun. Elbette,

$$A[p^\infty] = \{\overline{q} \in \mathbb{Q}/\mathbb{Z} : \text{bir } n \in \mathbb{N} \text{ için } p^n\overline{q} = \overline{0}\} = \bigcup_{n \in \mathbb{N}} A[p^n]$$

olur ve dolayısıyla $A[p^\infty]$ sonsuz bir altgruptur. Elemanları, paydası p'nin bir kuvveti olarak yazılan kesirli sayıların sınıflarıdır. $A[p^\infty]$ grubuna ***Prüfer p-grubu*** adı verilir ve bu grup $\mathbb{Z}_{p^\infty}$ olarak gösterilir. Kolaylıkla

$$pA[p^{n+1}] = A[p^n]$$

eşitliği kanıtlanır ve bu eşitlikten $A[p^\infty]$ grubunun p-bölünür olduğu çıkar. $A[p]$ grubu bir p-grup olduğundan, diğer asallara da bölünür, dolayısıyla $A[p]$ bölünür bir gruptur.

Alıştırmalar

9.68. $A \lhd G$ ve H, $K \leq G$, A'yı içeren iki altgrup olsun. $H/A \cap K/A = (H \cap K)/A$ olduğunu kanıtlayın.

9.69. $A \lhd G$ ve H, $K \leq G$, A'yı içeren iki altgrup olsun. $H/A \cap K/A \neq 1$ koşuluyla $A < H \cap K$ koşulunun eşdeğer olduğunu kanıtlayın.

9.70. p bir asal olsun. $\left(\prod_n \mathbb{Z}/p^n\mathbb{Z}\right) / \left(\bigoplus_n \mathbb{Z}/p^n\mathbb{Z}\right)$ grubunun burulmasız olduğunu kanıtlayın.

9.71. $H = \langle (2,3), (3,2) \rangle \leq \mathbb{Z}^2$ olsun. $\mathbb{Z}^2/H$ grubunun grup yapısını bulun.

9.72. $H = \langle (2,3), (5,1) \rangle \leq \mathbb{Z}^2$ olsun. $\mathbb{Z}^2/H$ grubunun grup yapısını bulun.

9.73. $\mathbb{Z} \times \mathbb{Z}$ grubunun altgruplarını Örnek 5.23'de sınıflandırmıştık. O sınıflandırmadan bir $H \leq \mathbb{Z} \times \mathbb{Z}$ altgrubu alalım. $\mathbb{Z} \times \mathbb{Z}/H$'nin kaç elemanı vardır? $(\mathbb{Z} \times \mathbb{Z})/H$ grubu hakkında neler söyleyebilirsiniz?

9.74. $\mathbb{Q}/\mathbb{Z}$ grubunun her özaltgrubunun sonlu olduğunu kanıtlayın. Eğer altgrubun n elemanı varsa, bu grubun $A[n]$ olduğunu kanıtlayın. (İpucu ve $A[n]$'nin tanımı için bkz. Örnek 9.67.)

9.75. $X \subseteq G$ altkümesi G'yi üretsin ve $1 < n \in \mathbb{N}$ olsun.

$$G_n = \left\{ x_1^{k_1} \cdots x_r^{k_r} : r \in \mathbb{N},\, x_i \in X,\, k_i \in \mathbb{Z},\, \sum_i k_i \equiv 0 \bmod n \right\}$$

altgrubunun normal olduğunu, G/G_n grubunun döngüsel olduğunu ve eleman sayısının n'yi böldüğünü kanıtlayın. (Eğer $1 \neq x \in X$ ise G/G_n grubu $\overline{x}$ tarafından üretilir.)

9.4 $\mathbb{Z}$'nin Bölüm Grupları

$\mathbb{Z}$'nin toplama altında bir grup olduğunu, hatta bir abel grubu olduğunu, dolayısıyla her altgrubunun normal olduğunu (bkz. Örnek 9.58) ve her altgrubunun bir ve bir tek $n \in \mathbb{N}$ için $n\mathbb{Z}$ biçiminde olduğunu (bkz. Teorem 2.1) biliyoruz. Bir önceki altbölümlerde G grubu yerine (toplamsal yazılan) $\mathbb{Z}$ grubunu ve H altgrubu yerine bir $n\mathbb{Z}$ altgrubu alacağız. n'yi de doğal sayı seçeceğiz.

İşlemimiz toplama olduğundan, bu durumda $n\mathbb{Z}$ altgrubunun ötelemeleri $k + n\mathbb{Z}$ ya da $n\mathbb{Z} + k$ biçiminde yazılırlar; biz ikinci yazılımı tercih edeceğiz.

Eğer $n = 0$ ise, o zaman $n\mathbb{Z} = 0\mathbb{Z} = \{0\}$ olur (bkz. Örnek 9.45) ve ötelemeler $\overline{k} = \{0\} + k = \{k\}$ olurlar, yani tek elemanlı her küme bir öteleme olur. Dolayısıyla

$$\mathbb{Z}/0\mathbb{Z} = \{\{k\} : k \in \mathbb{Z}\}$$

olur. $\mathbb{Z}/0\mathbb{Z}$ grubunda işlem şöyle ifade edilir:

$$\{k\} + \{\ell\} = \overline{k} + \overline{\ell} = \overline{k + \ell} = \{k + \ell\};$$

Dolayısıyla $\mathbb{Z}/0\mathbb{Z}$ grubunun $\mathbb{Z}$ grubundan pek farkı yoktur. Bundan böyle $n > 0$ olsun.

Farklı k sayıları için aynı ötelemeyi elde edebiliriz. Teorem 8.1'i toplamsal olarak yazarsak,

$$n\mathbb{Z} + k = n\mathbb{Z} + \ell \Leftrightarrow k - \ell \in n\mathbb{Z}$$

elde ederiz. Yani $n\mathbb{Z}+k$ ve $n\mathbb{Z}+\ell$ ötelemelerinin eşit olması için yeter ve gerek koşul n sayısının $k - \ell$ sayısını bölmesidir.

Şimdi herhangi bir $n\mathbb{Z}+k$ ötelemesi alalım. k'yı n'ye bölelim. Tamsayılarda çalıştığımız için bir kalan olacaktır: Öyle q ve r tamsayıları vardır ki hem

$$k = nq + r$$

hem de

$$0 \leq r < n$$

olur. Demek ki

$$n\mathbb{Z} + k = n\mathbb{Z} + nq + r = n(\mathbb{Z} + q) + r = n\mathbb{Z} + r$$

olur. Böylece

$$n\mathbb{Z} + k = n\mathbb{Z} + r$$

eşitliğini göstermiş olduk. Sağ taraftaki r, k sayısı n'ye bölündüğünde kalandır ve 0, 1, 2, $\ldots, n-1$ sayılarından biridir. Demek ki $\mathbb{Z}/n\mathbb{Z}$ kümesinde en fazla n tane eleman vardır:

$$n\mathbb{Z},\ n\mathbb{Z}+1,\ n\mathbb{Z}+2, \ldots, n\mathbb{Z}+(n-1).$$

Örneğin $n = 2$ ise, iki öteleme buluruz: Çift sayılar kümesi $2\mathbb{Z}$ ve tek sayılar kümesi $2\mathbb{Z}+1$. Eğer $n = 3$ ise üç öteleme buluruz:

3'e bölünen sayılar kümesi $3\mathbb{Z}$,
3'e bölündüğünde 1 kalan sayılar kümesi $3\mathbb{Z}+1$, ve
3'e bölündüğünde 2 kalan sayılar kümesi $3\mathbb{Z}+2$.

Eğer $n = 4$ ise

$$\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z},\ 4\mathbb{Z}+1,\ 4\mathbb{Z}+2,\ 4\mathbb{Z}+3\}$$

olur. Ama bir önceki altbölümde $n\mathbb{Z}+k$ yerine $\overline{k}$ yazmanın faziletlerini görmüştük. Öyle yapalım:

$$\mathbb{Z}/4\mathbb{Z} = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3}\}.$$

Genel olarak

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\ \overline{1},\ \overline{2},\ \ldots, \overline{n-1}\} = \{\overline{k} : 0 \leq k < n\}$$

olur. Yukarıda görünen k ötelemenin her birinin farklı olduklarını göstermek zor değildir, nitekim eğer $0 \leq k \leq \ell < n$ için, $n\mathbb{Z}+k = n\mathbb{Z}+\ell$ olsaydı, o zaman n'nin $\ell - k$ sayısını bölmesi gerekirdi, ama $0 \leq k - \ell < n$ eşitsizlikleri, bu durumda $\ell - k = 0$ yani $\ell = k$ verir. Demek ki $\mathbb{Z}/n\mathbb{Z}$ bölüm grubunun tam tamına n tane elemanı vardır ve bu elemanlar yukarıda sıralanmışlardır.

$\mathbb{Z}/n\mathbb{Z}$ grubunun elemanlarına "modülo n" sayılar denir. Lisede öğrenilen modüler sayılar aslında bunlardır, doğru tanım burada yapıldığı gibidir, ama lisede $n\mathbb{Z}+k$ ötelemesi yerine "k'nın kalan sınıfı"ndan sözedilir.

Önsav 9.6. *Her $n \in \mathbb{Z}$ için $\mathbb{Z}/n\mathbb{Z}$ devirli bir gruptur ve n'ye asal m sayıları için $\overline{m}$ elemanları tarafından üretilir ve başka elemanlar tarafından üretilmez.*

Kanıt: $\overline{1}$ elbette $\mathbb{Z}/n\mathbb{Z}$ grubunu üretir, çünkü ne de olsa her doğal sayıyı 1'i kendisiyle toplayarak elde ederiz. Örnek 9.57 de zaten aynı şeyi söylüyor: 1, $\mathbb{Z}$'yi ürettiğinden, $\overline{1}$ elemanı $\mathbb{Z}/n\mathbb{Z}$'yi üretir. Dolayısıyla $\mathbb{Z}/n\mathbb{Z}$ grubu devirli bir gruptur[6].

[6]İleride devirli gruplar için ayrı bir bölüm ayıracağız; dolayısıyla o zaman burada yapılanların hepsi o bölümün sonuçlarından çıkacak.

Şimdi $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ elemanının $\mathbb{Z}/n\mathbb{Z}$ grubunu ürettiğini varsayalım. O zaman $\mathbb{Z}/n\mathbb{Z}$'nin her elemanı $\overline{m}$ elemanının bir katıdır. Bunun özel bir durumu olarak, $\overline{1}$ elemanının $\overline{m}$ elemanının bir katı olduğunu görürüz. Yani öyle bir $k \in \mathbb{Z}$ vardır ki, $\overline{1} = k\overline{m} = \overline{km}$ olur. Demek ki n sayısı $km - 1$ sayısını böler; yani öyle bir $u \in \mathbb{Z}$ vardır ki $nu = km - 1$ olur. Dolayısıyla n ve m'nin ortak böleni 1'i de bölmek zorundadır. Bundan da n ve m'nin ortak bölenlerinin sadece 1 ve -1 olduğu çıkar, yani n ve m aralarında asaldır.

Şimdi tam tersine n ve m elemanlarının aralarında asal olduğunu varsayalım. Teorem 2.5'e göre, öyle u, v tamsayıları vardır ki $nu + mv = 1$ olur. Bu eşitliği $\mathbb{Z}/n\mathbb{Z}$ grubuna indirirsek,

$$\overline{1} = \overline{nu + mv} = \overline{nu} + \overline{mv} = \overline{mv} = v\overline{m}$$

olur, yani $\overline{1} \in \langle \overline{m} \rangle$ olur. Buradan da (bkz. Alıştırma 7.25)

$$\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle \leq \langle \overline{m} \rangle \leq \mathbb{Z}/n\mathbb{Z}$$

ve dolayısıyla $\langle \overline{m} \rangle = \mathbb{Z}/n\mathbb{Z}$ çıkar. Demek ki $\overline{m}$ elemanı $\mathbb{Z}/n\mathbb{Z}$ grubunu üretir. □

İleride bu gruptan çok daha fazla sözedeceğiz.

Not: $\mathbb{Z}/n\mathbb{Z}$ grubunda toplamayı $\overline{x} + \overline{y} = \overline{x + y}$ olarak tanımladık, daha doğrusu tanımlayabileceğimizi gösterdik. Aynı küme üzerinde benzer yöntemle bir çarpma işlemi de tanımlayabiliriz: $\overline{x}\,\overline{y} = \overline{xy}$. Nitekim eğer $\overline{x} = \overline{x_1}$ ve $\overline{y} = \overline{y_1}$ ise, yani n, $x - x_1$ ve $y - y_1$ sayılarını bölüyorsa, o zaman,

$$xy - x_1y_1 = x(y - y_1) + (x - x_1)y_1$$

eşitliğinden dolayı n, $xy - x_1y_1$ sayısını da böler, yani $\overline{xy} = \overline{x_1y_1}$ olur. Demek ki

$$\overline{x}\,\overline{y} = \overline{xy}$$

tanımını yapmaya hakkımız var. Böylece $\mathbb{Z}/n\mathbb{Z}$ kümesi üzerine ikili bir işlem (çarpma işlemi) tanımlamış oluruz. Örneğin eğer $n = 8$ ise,

$$\overline{5} \cdot \overline{6} = \overline{5 \cdot 6} = \overline{30} = \overline{6}$$

olur. Bu işlem değişme ve birleşme özelliğini sağlar, çünkü aynı özellikler $\mathbb{Z}$'de sağlanır. Benzer nedenden $\overline{0} \in \mathbb{Z}/n\mathbb{Z}$ ***yutan elemandır*** çünkü her $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ için $\overline{0} \cdot \overline{x} = \overline{0}$ olur. Ve gene aynı nedenden $\overline{1}$ etkisiz elemandır: her $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ için $\overline{1} \cdot \overline{x} = \overline{x}$ olur. Ama bu işlemle birlikte $\mathbb{Z}/n\mathbb{Z}$ bir grup olmaz, çünkü her elemanın çarpma işlemi için bir tersi yoktur. Örneğin $\mathbb{Z}/6\mathbb{Z}$'de, $\overline{0}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ elemanlarının çarpımsal tersleri yoktur. Öte yandan

$$(\mathbb{Z}/n\mathbb{Z})^\star = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} : \text{bir } y \in \mathbb{Z} \text{ için } \overline{x}\,\overline{y} = \overline{1}\}$$

kümesi çarpma altında bir grup olur. Bu grubun

$$\{\overline{x} \in \mathbb{Z}/n\mathbb{Z} : \text{ebob}(x, n) = 1\}$$

kümesine eşit olduğunu kanıtlamak zor değil. Örneğin Eğer p bir asalsa

$$(\mathbb{Z}/p\mathbb{Z})^\star = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

olur. Eğer ayrıca $n > 0$ bir doğal sayıysa, Örnek 9.52'deki yazılımla, $(\mathbb{Z}/p^n\mathbb{Z})^\star$ grubunun elemanları, $a_0, a_1, \ldots, a_{n-1} \in \{0, 1, \ldots, p-1\}$ ama $a_0 \neq 0$ için

$$\overline{a_0 + a_1 p + \cdots + a_{n-1}p^{n-1}}$$

biçiminde yazılırlar. Dolayısıyla bunlardan $(p-1)p^{n-1} = p^n - p^{n-1}$ tane vardır. Bu dediklerimizin bir başka sonucu, eğer p bir asalsa,

$$(\mathbb{Z}/p^n\mathbb{Z})^\star = (\mathbb{Z}/p^n\mathbb{Z}) \setminus (p\mathbb{Z}/p^n\mathbb{Z})$$

eşitliğidir. (Bkz. Örnek 9.52.) Bütün bunlardan şu sonuçlar çıkar:

Teorem 9.7 (Fermat'nın Küçük Teoremi)**.** *Eğer p bir asalsa her x için $x^p \equiv x \bmod p$ olur.*

Kanıt: x'in p'ye bölünmediğini varsayabiliriz. O zaman $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\star$ olur. Ama bu grubun derecesi $p-1$ olduğundan, Sonuç 8.6'ya göre $\overline{x}^{p-1} = \overline{1}$, yani $\overline{x}^p = \overline{x}$ olur. □

Euler-Fermat Teoremi adıyla bilinen Euler'in aşağıdaki teoremi Fermat'nın küçük teoremini genelleştirir:

Teorem 9.8 (Euler-Fermat Teoremi)**.** *n ve m birbirine asal iki doğal sayı olsun. n'den küçük eşit ve n'ye asal pozitif doğal sayı sayısı $\varphi(n)$ olsun. Bu durumda $m^{\varphi(n)} \equiv 1 \bmod n$ olur.*

Kanıt: Metinde $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\star$ olduğunu gördük. Ayrıca $|(\mathbb{Z}/n\mathbb{Z})^\star| = \varphi(n)$ olduğunu gördük. Demek ki Sonuç 8.6'ya göre $\overline{m}^{\varphi(n)} = \overline{1}$ olur. □

Bu son teoremdeki φ fonksiyonuna ***Euler φ fonksiyonu*** adı verilir. Teoremden de belli ki Euler φ fonksiyonunu hesaplayabilmek önemli. Yukarıda asal p sayıları için $\varphi(p^n) = p^n - p^{n-1}$ olduğunu gördük. Bu bilgi ve aşağıdaki olguyla Euler φ-fonksiyonunun aldığı değerleri hesaplayabiliriz, yeter ki sayıyı asallarına ayırabilelim.

Olgu 9.9. *Eğer n ve m birbirine asal iki doğal sayıysa $\varphi(nm) = \varphi(n)\varphi(m)$ olur.*

Bu olguyu kanıtlamak bu aşamada gerçekten zor değildir. kanıtı pek zor olamayan Teorem 10.19'in biraz fazlası kullanılarak kolaylıkla kanıtlanabilir. Ama bu kanıtı vermek bizi başka mecralara sürükleyebileceğinden, bu önemli olgunun (oldukça kolay) kanıtını halkalarla ilgili bir sonraki cilde saklayacağız.

$\mathbb{Z}/n\mathbb{Z}$ kümesi, toplama ve çarpma işlemleriyle birlikte bir "halka" olur. Halkalardan bir sonraki ciltte sözedeceğiz.

10. Homomorfiler

Bu bölümde soyut cebirin en önemli konusuyla tanışacağız.

10.1 Homomorfi

G ve H iki grup olsun. Eğer $\varphi : G \longrightarrow H$ fonksiyonu her g_1, $g_2 \in G$ için

$$\varphi(g_1 g_1) = \varphi(g_1)\varphi(g_2) \tag{1}$$

eşitliğini sağlıyorsa, φ fonksiyonuna ***homomorfi*** adı verilir. Bir başka deyişle, ***işlemlerle uyumlu*** ya da ***çarpmaya dağılan*** fonksiyonlara homomorfi denir. Tabii eğer G'nin işlemi toplamaysa (1) eşitliği

$$\varphi(g_1 + g_1) = \varphi(g_1)\varphi(g_2)$$

olarak yazılmalı. Benzer değişiklik eğer H'nin işlemi toplamaysa eşitliğin sağ tarafında da yapılmalı.

Homomorfi yerine homomorfizma, morfizma ya da eşyapı dönüşümü gibi tabirler de kullanılır. Başka cebirsel yapıların da homomorfileri olduğundan, diğerlerinden ayrıştırmak amacıyla homomorfi yerine ***grup homomorfisi*** de diyebiliriz.

Eğer $\varphi : G \longrightarrow H$ bir homomorfiyse, G'nin etkisiz elemanı φ altında H'nin etkisiz elemanına gitmek zorundadır, nitekim eğer $1_G \in G$ ve $1_H \in H$ etkisiz elemanlarsa,

$$\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G) \cdot \varphi(1_G)$$

olduğundan, $\varphi(1_G) = 1_H$ olur. Ayrıca her $g \in G$ için

$$1_H = \varphi(1_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$$

olduğundan,

$$\varphi(g^{-1}) = \varphi(g)^{-1}$$

olur. Bütün bunlardan kolaylıkla $\varphi(G) \leq H$ çıkar. Ayrıca her $n \in \mathbb{Z}$ için

$$\varphi(g^n) = \varphi(g)^n$$

eşitliği çıkar. Dolayısıyla eğer $g^n = 1$ ise, $\varphi(g)$ ancak, H'nin derecesi n'yi bölen bir eleman olabilir. Bir başka deyişle homomorfi olmak kolay değildir. Bu kadarla da kalmıyor: Eğer, örneğin, G'nin a, b, c elemanları arasında

$$a^2b^3c^{-2}ab = 1$$

gibi bir ilişki varsa, H'nin $\varphi(a)$, $\varphi(b)$, $\varphi(c)$ elemanları arasında da

$$\varphi(a)^2\varphi(b)^3\varphi(c)^{-2}\varphi(a)\varphi(b) = 1$$

gibi bir ilişki olmak zorundadır, yani örneğin $\varphi(a)$ ve $\varphi(c)$ elemanları belirlenmişse, $\varphi(b)$, H'nin herhangi bir elemanı olamaz, yukarıdaki eşitliği sağlamak zorundadır. Ya da eğer G değişmeli bir grupsa, $\varphi(G)$, G'nin değişmeli bir altgrubu olmak zorundadır. Ya da her $g \in G$ için $g^8 = 1$ oluyorsa, $\varphi(G)$'nin elemanları da bu ilişkiyi sağlamak zorundadır. Ya da her x, y, $z \in G$ için

$$y^{-1}x^{-1}yxz^{-1}x^{-1}y^{-1}xyz = 1$$

ise, $\varphi(G)$'nin herhangi üç elemanı da aynı eşitliği sağlamak zorundadır. Demek ki G'de elemanlar arasında çeşitli ilişkilerin bulunması homomorfilerin varlığını zorlaştırır. Öte yandan G'de $abc \neq 1$ ise, H'de bal gibi $\varphi(a)\varphi(b)\varphi(c) = 1$ olabilir. Yani φ, G'nin "olumlu (pozitif)" ilişkilerine duyarlı olmak zorundadır, olumsuz ilişkileri bozabilir.

Genel bir felsefi görüş olarak şunu söyleyebiliriz: G'nin elemanları arasında ne kadar az ilişki varsa ve H'nin elemanları arasında ne kadar fazla ilişki varsa, G'den H'ye giden o kadar çok homomorfi vardır. G'deki ilişki sayısı çoğaldığında ya da H'deki ilişki sayısı azaldığında, G'den H'ye giden homomorfi bulmak zorlaşır.

Bütün bunlardan bir de şu çıkar: Eğer $X \subseteq G$ altkümesi G'nin bir üreteç kümesiyse, o zaman herhangi bir $\varphi : G \longrightarrow H$ homomorfisi φ'nin X kümesi üzerinde alacağı değerler tarafından belirlenir. Nitekim φ'nin X üzerine aldığı değerleri biliyorsak, bir $g \in G$ elemanını, $n \in \mathbb{N}$, $x_i \in X$, $k_i \in \mathbb{Z}$ için

$$g = x_1^{k_1} \cdots x_n^{k_n}$$

olarak yazarsak,

$$\varphi(g) = \varphi(x_1)^{k_1} \cdots \varphi(x_n)^{k_n}$$

eşitliği doğru olur, yani $\varphi(g)$ elemanı $\varphi(x_1)$, ..., $\varphi(x_n)$ elemanları tarafından belirlenir. Ama tabii φ'nin X'te alacağı değerler de genellikle rastgele olamaz.

Homomorfilerin bileşkesinin bir homomorfi olduğu bariz olmalı.

Eğer $\varphi : G \longrightarrow H$ bir homomorfiyse, $\varphi(G) \leq H$ olur. Dolayısıyla G'nin altgruplarının imgeleri de H'nin altgrubu olurlar. Bu arada, eğer $K \leq G$ ise, φ'nin K'ya kısıtlaması $\varphi_{|K}$ fonksiyonunun da K'dan H'ye giden bir homomorfi olduğunu söyleyelim, kanıtı barizdir.

Tanım kümesi G olan bir φ homomorfisi için $\varphi(G)$ olarak yazılan gruplara G'nin ***homomorfik imgesi*** adı verilir. Homomorfik imgeler G'ye oldukça benzer, en azından G'nin izlerini taşır. Daha önce de söylediğimiz gibi G'nin tüm ilişkileri $\varphi(G)$'ye φ sayesinde yansır, mesela G burulmalı bir grupsa $\varphi(G)$ de burulmalı bir gruptur, G bir abel grubuysa, $\varphi(G)$ de abeldir vs ama $\varphi(G)$'de G'den daha fazla ilişki olabilir, mesela (uç örnek) $\varphi(G)$'de bütün elemanlar 1'e eşit olabilirler ama G'de böyle olmayabilir.

G grubundan H grubuna giden homomorfilerden oluşan kümeyi

$$\mathrm{Hom}(G, H)$$

olarak gösterelim. $\mathrm{Hom}(G, H)$ kümesi $H^G = \mathrm{Fonk}(G, H)$ grubunun (kartezyen çarpımının) bir altkümesidir (elbette), ama illa bir altgrubu değildir çünkü iki homomorfinin çarpımı illa bir homomorfi olmak zorunda değildir. İki homomorfinmin çarpımının bir homomorfi olması için yeter ve gerek koşulu bulmak çok zor değildir. Bulalım. φ, $\psi \in \mathrm{Hom}(G, H)$ olsun. $\varphi \cdot \psi : G \longrightarrow H$ fonksiyonunun, her $g \in G$ için

$$(\varphi \cdot \psi)(g) = \varphi(g)\psi(g)$$

kuralıyla tanımlandığını anımsayalım. (Fonksiyonların çarpımlarının bir noktadaki değeri, fonksiyonların o noktadaki değerlerinin çarpımıdır.) $\varphi \cdot \psi$ fonksiyonunun bir homomorfi olması için, homomorfinin tanımı gereği, her g_1, $g_2 \in G$ için

$$(\varphi \cdot \psi)(g_1 g_2) = (\varphi \cdot \psi)(g_1)(\varphi \cdot \psi)(g_2)$$

olmalıdır. İki fonksiyonun çarpımının tanımını uygularsak, bu koşul, her g_1, $g_2 \in G$ için

$$\varphi(g_1 g_2)\psi(g_1 g_2) = \varphi(g_1)\psi(g_1)\varphi(g_2)\psi(g_2)$$

eşitliğine denktir. Eşitliğin solunda φ ve ψ'nin birer homomorfi olduğunu kullanalım: Yukarıdaki koşul, her g_1, $g_2 \in G$ için

$$\varphi(g_1)\varphi(g_2)\psi(g_1)\psi(g_2) = \varphi(g_1)\psi(g_1)\varphi(g_2)\psi(g_2)$$

eşitliğine denktir. Eşitlikte sadeleştirmeleri yaparsak, koşulun, her g_1, $g_2 \in G$ için

$$\varphi(g_2)\psi(g_1) = \varphi(g_1)\varphi(g_2)$$

eşitliğine denk olduğunu görürüz. Demek ki $\varphi \cdot \psi$ fonksiyonunun bir homomorfi olması için yeter ve gerek koşul, her g_1, $g_2 \in G$ için

$$\varphi(g_2)\psi(g_1) = \varphi(g_1)\varphi(g_2)$$

eşitliğidir, yani $\varphi(G)$ ile $\psi(G)$'nin elemanları birbirleriyle değişmeli olmasıdır, yani $\varphi(G) \leq C_H(\psi(G))$ içindeliğidir. Eğer H değişmeli bir grupsa bu koşul elbette sağlanır. Bunu bir sonuç olarak kayda düşelim:

Önsav 10.1. *Eğer H değişmeli bir grupsa* $\mathrm{Hom}(G,H)$ *çarpma altında bir grup olur.* □

Notlar ve Örnekler

10.1. G ve H herhangi iki grup olsun. H'nin etkisiz elemanını alışık olduğumuz üzere 1 simgesiyle gösterelim. O zaman her $g \in G$ için $\varphi(g) = 1$ olarak tanımlanan $f : G \longrightarrow H$ fonksiyonu bir homomorfidir. Homomorfi olan tek sabit fonksiyon bu fonksiyondur. Demek ki $\mathrm{Hom}(G,H)$ kümesi hiçbir zaman boşküme değildir.

10.2. Tanımda $G = H$ alalım. Özdeşlik fonksiyonu Id_G, G'den G'ye giden bir homomorfidir.

10.3. $G \leq H$ olsun ve $i : G \longrightarrow H$ fonksiyonu, her $g \in G$ için $i(g) = g$ olarak tanımlansın. i bir homomorfidir. i'ye ***doğal gömme*** adı verilir.

10.4. Eğer G bir abel grubuysa ve $n \in \mathbb{Z}$ ise $x \mapsto x^n$ kuralı bize G'den G'ye giden bir homomorfi verir. Eğer G'nin işlemi toplamayla yazılıyorsa, bu kural $x \mapsto nx$ olarak gösterilir.

10.5. Yukarıdaki örneği $G = \mathbb{Z}$ grubuna uygulayalım. $a \in \mathbb{Z}$ sabit bir sayı olsun. $\varphi_a(n) = an$ kuralıyla tanımlanan $\varphi_a : \mathbb{Z} \longrightarrow \mathbb{Z}$ bir morfizmadır. Örnek 10.17'da $\mathbb{Z}$'den $\mathbb{Z}$'ye giden tüm homomorfilerin bu türden olduğunu göstereceğiz.

10.6. Analiz derslerinden bildiğimiz exp fonksiyonu $\mathbb{R}$ grubundan $\mathbb{R}^{>0}$ grubuna giden bir homomorfidir çünkü her $x, y \in \mathbb{R}$ için $\exp(x+y) = \exp x \exp y$ olur. ($\mathbb{R}$ toplama altında, $\mathbb{R}^{>0}$ ise çarpma altında bir gruptur.) ln fonksiyonu da $\mathbb{R}^{>0}$ grubundan $\mathbb{R}$ grubuna giden bir homomorfidir.

10.7. G herhangi bir grup ve $g \in G$ olsun. $\mathrm{Inn}_g(x) = gxg^{-1}$ kuralıyla tanımlanmış Inn_g fonksiyonu G'den gene G'ye giden bir homomorfizmadır (bkz. Örnek 1.30).

10.8. G herhangi bir grup ve H, $K \leq G$ olsun. $K \leq N_G(H)$ varsayımını yapalım. O zaman $k \in K$ ve $h \in H$ için $\varphi_k(h) = khk^{-1}$ kuralıyla tanımlanmış φ_k fonksiyonu H'den gene H'ye giden bir homomorfidir. Bu homomorfiler birebir ve örtendir. Ayrıca $\varphi_k \circ \varphi_{k'} = \varphi_{kk'}$ olur.

10.9. G bir grup olsun. $z \in G$ elemanı şu özelliği sağlasın: Her $g \in G$ için $[z,g] \in Z(G)$. O zaman $\mathrm{ad}_z(g) = [z,g]$ kuralıyla tanımlanmış fonksiyon bir grup homomorfizmasıdır.

10.10. G bir grup ve $H \lhd G$ olsun. Sayfa 116'da $\pi(g) = gH = \overline{g}$ kuralıyla tanımladığımız $\pi : G \longrightarrow G/H$ izdüşüm fonksiyonu bir homomorfidir. Bu homomorfizma ileride çok önemli olacaktır.

10.11. Eğer $\varphi : G \longrightarrow H$ ve $\psi : H \longrightarrow K$ birer homomorfiyse, $\psi \circ \varphi : G \longrightarrow H$ de bir homomorfidir.

10.12. $(\varphi_i : G_i \longrightarrow H_i)_i$ bir homomorfi ailesi olsun. O zaman,

$$\left(\prod_i \varphi_i\right)((g_i)_i) = (\varphi_i(g_i))$$

kuralı bize bir

$$\prod_i G_i \longrightarrow \prod_i H_i$$

homorfisi verir. Eğer φ_i'lerin her biri birebirse (ya da örtense), $\prod_i \varphi_i$ homomorfisi de birebirdir (örtendir) ama tabii bu olgu grup teorisiyle değil kümeler kuramıyla ilgili bir önermedir.

Ayrıca

$$\left(\prod_i \varphi_i\right)\left(\bigoplus_i G_i\right) \leq \bigoplus_i H_i$$

olduğundan (çünkü $\varphi_i(1) = 1$ olur), $\prod_i \varphi_i$, $\bigoplus_i G_i$ grubundan $\bigoplus_i H_i$ grubuna giden bir homomorfi tanımlar.

10.13. G, H_1 ve H_2 üç grup olsun. $\mathrm{Hom}(G, H_1 \times H_2)$, $\mathrm{Hom}(G, H_1)$ ve $\mathrm{Hom}(G, H_2)$ arasında bir ilişki bulalım. Eğer $\varphi_1 \in \mathrm{Hom}(G, H_1)$ ve $\varphi_2 \in \mathrm{Hom}(G, H_2)$ iki homomorfiyse,

$$(\varphi_1 \times \varphi_2)(g) = (\varphi_1(g), \varphi_2(g_1))$$

formülüyle tanımlanmış

$$\varphi_1 \times \varphi_2 : G \longrightarrow H_1 \times H_2$$

fonksiyonu bir homomorfidir. Böylece

$$\alpha(\varphi_1, \varphi_2) = \varphi_1 \times \varphi_2$$

kuralıyla tanımlanmış bir

$$\alpha : \mathrm{Hom}(G, H_1) \times \mathrm{Hom}(G, H_2) \longrightarrow \mathrm{Hom}(G, H_1 \times H_2)$$

fonksiyonu elde ederiz. Bu fonksiyonun tersi de vardır.

$$\pi_1 : H_1 \times H_2 \longrightarrow H_1 \text{ ve } \pi_2 : H_1 \times H_2 \longrightarrow H_2$$

doğal izdüşüm fonksiyonlarıysa o zaman

$$\beta(\varphi) = (\pi_1 \circ \varphi, \pi_2 \circ \varphi)$$

kuralı bize,

$$\beta : \mathrm{Hom}(G, H_1 \times H_2) \longrightarrow \mathrm{Hom}(G, H_1) \times \mathrm{Hom}(G, H_2)$$

fonksiyonunu verir. α ve β fonksiyonlarının birbirinin tersi olduklarını kontrol etmek zor değildir.

10.14. Bir önceki örneği somutlaştıralım. n, $m > 0$ tamsayı olsunlar. Eğer $x \in \mathbb{Z}$ ise, $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ ve $\tilde{x} \in \mathbb{Z}/m\mathbb{Z}$ tahmin edilen modüler sayıları simgelesinler. $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ fonksiyonu

$$\varphi(x) = (\overline{x}, \tilde{x})$$

olarak tanımlansın. Bu fonksiyon bir homomorfidir.

10.15. G bir grup ve $(H_i)_i$ bir grup ailesi olsun. $\mathrm{Hom}\left(G, \prod_i H_i\right)$ ve $\mathrm{Hom}(G, H_i)$ kümeleri arasında bir ilişki bulalım. Eğer her i göstergeci için $\varphi_i \in \mathrm{Hom}(G, H_i)$ homomorfisi verilmişse,

$$\left(\prod_i \varphi_i\right)(g) = (\varphi_i(g))_i$$

formülüyle tanımlanmış

$$\prod_i \varphi_i : G \longrightarrow \prod_i H_i$$

fonksiyonu bir homomorfidir. Böylece

$$\alpha((\varphi_i)_i) = \prod_i \varphi_i$$

kuralıyla tanımlanmış bir

$$\alpha : \prod_i \mathrm{Hom}(G, H_i) \longrightarrow \mathrm{Hom}\left(G, \prod_i H_i\right)$$

fonksiyonu elde ederiz. Bu fonksiyonun tersi de vardır. Eğer

$$\pi_i : \prod_i H_i \longrightarrow H_i$$

doğal izdüşüm fonksiyonlarıysa o zaman

$$\beta(\varphi) = (\pi_i \circ \varphi)_i$$

kuralı bize,

$$\beta : \operatorname{Hom}\left(G, \prod_i H_i\right) \longrightarrow \prod_i \operatorname{Hom}(G, H_i)$$

fonksiyonunu verir. α ve β fonksiyonlarının birbirinin tersi olduklarını kontrol etmek zor değildir.

Soru: Benzer bir şeyi $\operatorname{Hom}\left(G, \prod_i H_i\right)$ yerine $\operatorname{Hom}\left(G, \oplus_i H_i\right)$ için ya da $\prod_i \operatorname{Hom}(G, H_i)$ yerine $\oplus_i \operatorname{Hom}(G, H_i)$ için yapabilir miyiz?

10.16. $n > 0$ bir tamsayı olsun. $\mathbb{Z}/n\mathbb{Z}$ grubundan $\mathbb{Z}$ grubuna giden homomorfileri bulalım.

$\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}$ bir homomorfi olsun. $\mathbb{Z}/n\mathbb{Z}$ grubu $\overline{1}$ tarafından üretildiğinden, yukarıdaki metinde söylediklerimizden, φ'nin $\varphi(\overline{1})$ değeri tarafından belirlendiği anlaşılır. Nitekim, her $k \in \mathbb{Z}$ için,

$$\varphi(\overline{k}) = \varphi(k \cdot \overline{1}) = k\varphi(\overline{1})$$

olur. Burada $k = n$ alırsak,

$$0 = \varphi(\overline{0}) = \varphi(\overline{n}) = n\varphi(\overline{1}),$$

yani $n\varphi(\overline{1}) = 0$ buluruz. Ama n, $\varphi(\overline{1}) \in \mathbb{Z}$ ve $\mathbb{Z}$'de iki sayının çarpımı 0 ise, ikisinden biri 0 olmalıdır. Demek ki $\varphi(\overline{1}) = 0$ ve her $k \in \mathbb{Z}$ için,

$$\varphi(\overline{k}) = k\varphi(\overline{1}) = k \cdot 0 = 0$$

olmalı. Sonuç: $\mathbb{Z}/n\mathbb{Z}$ grubundan $\mathbb{Z}$ grubuna giden homomorfi sabit 0 fonksiyonu olmak zorundadır. Zaten $\mathbb{Z}/n\mathbb{Z}$ burulmalı bir grup olduğundan, homomorfik imgesi de burulmalı olmalıdır, ama $\mathbb{Z}$'nin burulmalı tek elemanı 0'dır.

10.17. H herhangi bir grup olsun. $\mathbb{Z}$ grubundan H'ye giden tüm homomorfileri bulalım.

$\varphi : \mathbb{Z} \longrightarrow H$ bir homomorfi olsun. $\mathbb{Z}$ grubu 1 tarafından üretildiğinden, yukarıdaki metinde söylediklerimizden, φ'nin $\varphi(1)$ değeri tarafından belirlendiği anlaşılır. Nitekim, her $n \in \mathbb{Z}$ için,

$$\varphi(n) = \varphi(n \cdot 1) = \varphi(1)^n$$

olur. (Toplamadan çarpmaya geçtiğimiz şaşırtmasın; H'nin işlemi çarpımsal olabilir.) Şimdi soru $\varphi(1)$'in H'nin hangi elemanı olabileceği. 1'in $\mathbb{Z}$ grubunda sağlamak zorunda olduğu özel bir ilişki olmadığından, $\varphi(1)$, H'nin herhangi bir elemanı olabilir. Eğer $h \in H$ verilmişse, $\varphi_h : \mathbb{Z} \longrightarrow H$ fonksiyonu $\varphi_h(n) = h^n$ olarak tanımlansın. O zaman φ_h bir homomorfidir, ne de olsa

$$\varphi(n+m) = h^{n+m} = h^n h^m = \varphi(n)\varphi(m)$$

olur. Demek ki H ile $\operatorname{Hom}(\mathbb{Z}, H)$ kümesi arasında $h \mapsto \varphi_h$ kuralıyla verilmiş bir eşleme vardır. Bu eşlemenin tersini bulalım: Eğer $\varphi = \varphi_h$ verilmişse, $h = \varphi(1)$ olur ve bu kural da $\operatorname{Hom}(\mathbb{Z}, H)$'den H'ye giden ters eşlemedir. Bir başka deyişle her $\varphi \in \operatorname{Hom}(\mathbb{Z}, H)$ için $\varphi = \varphi_{\varphi(1)}$ olur.

Bunun özel bir durumu olarak $\operatorname{Hom}(\mathbb{Z}, \mathbb{Z})$ kümesine bakalım. (Bu küme $\operatorname{End}\mathbb{Z}$ olarak yazılır ve bir kümeden çok daha fazladır, bir halkadır. Halka kavramını ileride ele alacağız.) $\mathbb{Z}$'den $\mathbb{Z}$'ye giden her homomorfizma bir $n \in \mathbb{Z}$ için

$$\varphi(x) = nx$$

formülüyle verilmiştir, yani homomorfi her sayıyı sabit n sayısı ile çarpar. 0 ile çarpma dışında her biri birebirdir ama sadece ikisi örtendir: 1 ile çarpma (ki özdeşlik fonksiyonu $\operatorname{Id}_{\mathbb{Z}}$'dir) ve -1 ile çarpma (ki $-\operatorname{Id}_{\mathbb{Z}}$ olarak gösterilir.)

10.18. Bu örnekte $G = \mathbb{Z} \times \mathbb{Z}$ olarak alalım. H herhangi bir grup ve $\varphi \in \mathrm{Hom}(\mathbb{Z} \times \mathbb{Z}, H)$ olsun. $e_1 = (1, 0)$ ve $e_2 = (0, 1)$ tanımlarını yapalım. $\mathbb{Z} \times \mathbb{Z}$'nin her x elemanı bir ve bir tane n ve m sayı çifti için $x = ne_1 + me_2$ olarak yazılır.

$$\varphi(x) = \varphi(ne_1 + me_2) = \varphi(e_1)^n \varphi(e_2)^m$$

olmak zorunda olduğundan, φ homomorfisi H'nin $\varphi(e_1)$ ve $\varphi(e_2)$ elemanları tarafından belirlenir. Dolayısıyla

$$\alpha(\varphi) = (\varphi(e_1), \varphi(e_2)$$

kuralıyla belirlenmiş

$$\alpha : \mathrm{Hom}(\mathbb{Z} \times \mathbb{Z}, H) \longrightarrow H \times H$$

fonksiyonu birebirdir. α örten midir? Her zaman değildir, çünkü

$$\varphi(e_1)\varphi(e_2) = \varphi(e_1 + e_2) = \varphi(e_2) + \varphi(e_1) = \varphi(e_2)\varphi(e_1)$$

eşitliği sağlanmak zorundadır. Yani α fonksiyonun imgesi

$$\{(h_1, h_2) \in H \times H : h_1 h_2 = h_2 h_1\}$$

kümesinde olmak zorundadır. Öte yandan, eğer h_1, $h_2 \in H$ elemanları $h_1 h_2 = h_2 h_1$ eşitliğini sağlıyorsa, o zaman $\varphi(e_1) = h_1$ ve $\varphi(e_2) = h_2$ eşitliklerini sağlayan bir ve bir tane $\varphi \in \mathrm{Hom}(\mathbb{Z} \times \mathbb{Z}, H)$ vardır; bu homomorfi de her $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ için

$$\varphi(n, m) = \varphi(ne_1 + me_2) = \varphi(e_1)^n \varphi(e_2)^m$$

eşitliği tarafından tanımlanmıştır elbette.

10.19. H herhangi bir grup ve $n > 0$ bir tamsayı olsun. $\mathbb{Z}/n\mathbb{Z}$ grubundan H'ye giden tüm homomorfileri bulalım.

$\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow H$ bir homomorfi olsun. $\mathbb{Z}/n\mathbb{Z}$ grubu $\overline{1}$ tarafından üretildiğinden, yukarıdaki metinde söylediklerimizden, φ'nin $\varphi(\overline{1})$ değeri tarafından belirlendiği anlaşılır. Nitekim, her $k \in \mathbb{Z}$ için,

$$\varphi(\overline{k}) = \varphi(k \cdot \overline{1}) = \varphi(\overline{1})^k$$

olur. Şimdi soru, $\varphi(\overline{1})$'in H'nin hangi elemanı olabileceği. $\overline{1}$ elemanının derecesi n olduğundan, $1 = \varphi(\overline{0}) = \varphi(\overline{n}) = \varphi(\overline{1})^n$ olmalı, yani H'nin $f(\overline{1})$ elemanı $\varphi(\overline{1})^n = 1$ eşitliğini sağlamalı (yani derecesi n'yi bölmeli.) $\varphi(\overline{1})$ üzerine başka da bir koşul yoktur. Demek ki derecesi n'yi bölen her h elemanı için, $\varphi_h(\overline{k}) = h^k$ kuralıyla tanımlanmış $\varphi_h : \mathbb{Z}/n\mathbb{Z} \longrightarrow H$ fonksiyonu bir homomorfidir ve bunlardan başka da $\mathbb{Z}/n\mathbb{Z}$'den H'ye giden bir homomorfi yoktur.

Sonuç olarak şunu bulduk: Eğer $H_n = \{h \in H : h^n = 1\}$ ise H_n ile $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, H)$ kümesi arasında $h \mapsto \varphi_h$ kuralıyla verilmiş bir eşleme vardır.

10.20. Bir önceki örnekten yararlanarak $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ kümesini bulalım. Demek ki, öyle $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$ elemanlarını arıyoruz ki, $n\overline{k} = \overline{0}$ olsun, yani m, nk sayısını bölsün. Böyle bir k tamsayısı seçelim. $d = \mathrm{ebob}(n, m)$ olsun. $n = dn_1$, $m = dm_1$ yazalım. Demek ki dm_1, $dn_1 k$'yı bölüyor, yani m_1, $n_1 k$'yı bölüyor. Ama n_1 ve m_1 aralarında asaldır tabii. Dolayısıyla m_1, k'yı böler, yani bir t sayısı için $k = tm_1$ olur. Kontrol edelim: Acaba $k = tm_1$ ise m, nk'yı bölüyor mu?

$$nk = ntm_1 = dn_1 tm_1 = n_1 t(dm_1) = (n_1 t)m$$

olduğundan, m sayısı nk'yı gerçekten de böler. $k = tm_1$ sayısını $\mathbb{Z}/m\mathbb{Z}$ grubunda hesaplayacağımızdan ve $m = dm_1$ olduğundan, t sayısını $\{0, 1, \ldots, d-1\}$ kümesinden alabiliriz. Demek ki böyle bir t için[1]

$$\psi_t(\tilde{x}) = \overline{tm_1 x}$$

[1] Eğer $x \in \mathbb{Z}$ ise, $\tilde{x} \in \mathbb{Z}/n\mathbb{Z}$ ve $\overline{x} \in \mathbb{Z}/m\mathbb{Z}$ elemanları x tamsayısının sırasıyla $\mathbb{Z}/n\mathbb{Z}$ ve $\mathbb{Z}/m\mathbb{Z}$ bölüm gruplarındaki izdüşümlerini simgelesin.

kuralı bize bir

$$\psi_t : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

homomorfisi verir ve başka da yoktur:

$$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \{\psi_t : t = 0,\, 1, \ldots, d-1\}.$$

Okur $n = m$ durumunu özellikle irdelemek isteyebilir. Bu özel durum için bkz. Örnek 10.51.

10.21. $\mathbb{Q}$ grubundan $\mathbb{Z}$ grubuna giden homomorfileri bulalım. $\varphi \in \mathrm{Hom}(\mathbb{Q}, \mathbb{Z})$ olsun. Her $a \in \mathbb{Q}$ ve her $n > 0$ için $nx = a$ denkleminin $\mathbb{Q}$'da bir çözümü olduğundan, bu denkleme φ'yi uygulayarak $n\varphi(x) = \varphi(a)$ eşitliğini elde ederiz. Demek ki $ny = \varphi(a)$ denkleminin $\mathbb{Z}$'de bir çözümü vardır. Ama n'yi $\varphi(a)$'ya asal alabilirsek, bu denklemin $\mathbb{Z}$'de çözümü olamaz. Demek ki $\varphi(a) = 0$ olmalı. Dolayısıyla $\mathrm{Hom}(\mathbb{Q}, \mathbb{Z})$ kümesi sadece sabit 0 fonksiyonundan ibarettir. Görüldüğü gibi homomorfi olmak kolay değil.

10.22. $\mathbb{Q}$ grubundan $\mathbb{Q}$ grubuna giden homomorfileri bulalım. $\varphi \in \mathrm{Hom}(\mathbb{Q}, \mathbb{Q})$ olsun. Her $n,\, m\, n\mathbb{Z}$ ve $m \neq 0$ için,

$$\varphi(n) = n\varphi(1)$$

ve

$$m\varphi(n/m) = \varphi(m \cdot (n/m)) = \varphi(n) = n\varphi(1)$$

olur. Demek ki

$$\varphi(n/m) = (n/m)\varphi(1)$$

olur. Bir başka deyişle, her $x \in \mathbb{Q}$ için,

$$\varphi(x) = x\varphi(1)$$

olur. Demek ki $\varphi(1) \in \mathbb{Q}$ değeri φ'yi belirliyor. Böylece

$$\alpha(\varphi) = \varphi(1)$$

kuralı bize birebir bir

$$\alpha : \mathrm{Hom}(\mathbb{Q}, \mathbb{Q}) \longrightarrow \mathbb{Q}$$

fonksiyonu veriyor. Bu fonksiyon örtendir de. Nitekim eqer $a \in \mathbb{Q}$ rastgele bir kesirli sayı ise

$$\varphi(x) = xa$$

kuralı $\mathbb{Q}$'dan $\mathbb{Q}$'ya giden bir homomorfi tanımlar.

10.23. H herhangi bir grup olsun. $\mathbb{Q}$ grubundan H'ye giden tüm homomorfileri bulmaya çalışalım. Çok kolay olmadığını göreceğiz. $\varphi \in \mathrm{Hom}(\mathbb{Q}, H)$ olsun. H bir abel grubu olmak zorunda olmadığından, H'nin işlemini toplamsal olarak değil çarpımsal olarak yazıyoruz. Demek ki her $q \in \mathbb{Q}$ için $\varphi(nq) = \varphi(q)^n$ olur. Buradan da φ'nin aslında $m \in \mathbb{N}$ için $\varphi(1/m)$ elemanları tarafından belirlendiği anlaşılır çünkü ne de olsa $\varphi(n/m) = \varphi(1/m)^n$ olur. $\varphi(1) = a$ tanımını yapalım ve $0 \neq m \in \mathbb{N}$ için $\varphi(1/m)$ değerini bulmaya çalışalım.

$$a = \varphi(1) = \varphi(m \cdot (1/m)) = \varphi(1/m)^m$$

olduğundan H'nin $\varphi(1/m)$ elemanı

$$a = \varphi(1/m)^m$$

eşitliğini sağlamak durumundadır. Yani H'de, her $0 \neq m \in \mathbb{N}$ için $a = x^m$ eşitliğinin bir çözümü olmalı, aksi halde $\varphi(1) = a$ olamaz. Bu eşitliği sağlayan bir a_m seçelim. Demek ki $a_m^m = a$. (Dolayısıyla $a_1 = a$.) Amacımızı anlamışsınızdır, amacımız $\varphi(1/m)$ elemanının a_m olarak tanımlamak. Ama

$$a_{nm}^n = \varphi(1/nm)^n = \varphi(n/nm) = \varphi(1/m) = a_m$$

olması gerektiğinden, seçtiğimiz bu elemanlar, her n ve m doğal sayıları için $a_{nm}^n = a_m$ eşitliğini sağlamalı. H grubunda böyle bir $(a_n)_n$ ailesi seçebilirsek $\mathbb{Q}$'dan H'ye giden bir homomorfiyi $\varphi(n/m) = a_m^n$ kuralıyla tanımlayabiliriz. Homomorfi bulmak kolay olmayabilir demiştik.

10.24. G burulmalı bir grup[2] ve $\varphi : G \longrightarrow H$ bir homomorfi olsun. O zaman $\varphi(G)$ grubu da burulmalı bir gruptur. Eğer G'nin her elemanının n'inci kuvveti 1 ise, G'nin homomorfik imgelerinin de aynı özelliği vardır.

10.25. G bölünür bir grup[3] ve $\varphi : G \longrightarrow H$ bir homomorfi olsun. O zaman $\varphi(G)$ grubu da bölünür bir gruptur. Nitekim eğer $x^n = g$ denklemini G'de çözümü varsa, $x^n = \varphi(g)^n$ denkleminin $\varphi(G)$'de çözümü vardır: G'deki çözüm a ise, $\varphi(G)$'deki (bir) çözüm $\varphi(a)$ olur.

Bu örnek ışığında Örnek 10.21'e bir daha bakalım. $\mathbb{Z}$'nin bölünür bir altgrubu $\{0\}$ olmak zorunda olduğundan, $\mathrm{Hom}(\mathbb{Q}, \mathbb{Z})$'de sadece sabit 0 fonksiyonu vardır.

Alıştırmalar

10.26. Eğer $\varphi : G \longrightarrow H$ bir homomorfiyse ve $A \leq G$ ise $\varphi(A) \leq H$ olduğunu kanıtlayın.

10.27. Eğer $\varphi : G \longrightarrow H$ bir homomorfiyse ve $B \leq H$ ise $\varphi^{-1}(B) \leq G$ olduğunu kanıtlayın.

10.28. $\varphi(x) = x^{-1}$ kuralıyla tanımlanmış fonksiyonun homomorfi olması için grubun abel grubu olması yeter ve gerek koşul olduğunu kanıtlayın.

10.29. Eğer $\varphi : G \longrightarrow H$ bir homomorfiyse ve $B \lhd H$ ise $\varphi^{-1}(B) \lhd G$ olduğunu kanıtlayın.

10.30. Eğer $\varphi : G \longrightarrow H$ bir homomorfiyse ve $A \lhd G$ ise $\varphi(A) \lhd H$ olduğu her zaman doğru değildir. Bunu görmek için bir H grubu ve H'nin normal olmayan bir A grubunu alalım. Mesela $A = \mathrm{Sym}\, 2$, $H = \mathrm{Sym}\, 3$ olabilir. $G = A$ olsun ve $\varphi : G \longrightarrow H$ gömme fonksiyonu olsun, yani her $g \in G$ için $\varphi(g) = g$ olsun. O zaman $A \lhd G$ olur (eşitler çünkü) ama $\varphi(A) \lhd H$ olmaz. Öte yandan Eğer $\varphi : G \longrightarrow H$ bir homomorfiyse ve $A \lhd G$ ise $\varphi(A) \lhd \varphi(G)$ olduğu doğrudur; kanıtlayın. Yani örten homomorfizmalarda normal altgrupların imgeleri de normaldir.

10.31. G bir grup ve A bir abel grubu olsun. $\mathrm{Hom}(G, A)$, G'den A'ya giden homomorfiler kümesi olsun. Eğer α, $\beta \in \mathrm{Hom}(G, A)$ ise, $\alpha\beta : G \longrightarrow H$ fonksiyonunu, her $g \in G$ için

$$(\alpha\beta)(g) = \alpha(g)\beta(g)$$

olarak tanımlayalım. $\alpha\beta$'nın da bir homomorfi olduğunu göstermek zor değil. Bunun için A'nın bir abel grubu olması önemlidir, aksi halde doğru değildir.

10.32. Eğer $\alpha : G \longrightarrow H$ bir homomorfiyse ve aynı zamanda bir eşlemeyse $\alpha^{-1} : H \longrightarrow G$ fonksiyonunun da bir homomorfi olduğunu kanıtlayın.

10.33. G ve G_1 birer grup, $\varphi : G \longrightarrow G_1$ bir homomorfi ve $(H_i)_{i\in I}$ ailesi G'nin bir altgrup ailesi olsun. Bu durumda $\varphi(\langle H_i : i \in I\rangle) = \langle \varphi(H_i) : i \in I\rangle$ eşitliğini gösterin.

10.34. G bir grup, $N \lhd G$ ve $(H_i)_{i\in I}$ ailesi G'nin bir altgrup ailesi olsun. Yukarıdaki alıştırmayı kullanarak $\langle H_i : i \in I\rangle N/N = \langle H_i N/N : i \in I\rangle$ eşitliğini gösterin.

10.35. H herhangi bir grup ise $\mathrm{Hom}(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, H)$ kümesinin elemanlarını betimleyin. (Bkz. Örnek 10.18.)

10.36. Örnek 10.18 ve 10.22'ten esinlenerek $\mathrm{Hom}(\mathbb{Q} \times \mathbb{Q}, \mathbb{Q})$ kümesinin elemanlarını belirleyin.

---

[2] Yani her $g \in G$ öyle bir $n > 0$ tamsayısı vardır ki $g^n = 1$ olur.

[3] Yani her $g \in G$ ve $n > 0$ tamsayısı için $x^n = g$ denkleminin G'de bir çözümü olsun. Örneğin $\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{R}^{>0}$ bölünür gruplardır.

10.2 Otomorfi Grubu

Homomorfilerin bileşkelerinin de homomorfi olduğunu kanıtlamak zor değil. Nitekim eğer $\varphi : G \longrightarrow H$ ve $\psi : H \longrightarrow K$ iki homomorfiyse,

$$\begin{aligned}(\psi \circ \varphi)(xy) &= \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) \\ &= \psi(f(x))\psi(f(y)) = (\psi \circ \varphi)(y)(\psi \circ \varphi)(y)\end{aligned}$$

eşitliği bize $\psi \circ \varphi : G \longrightarrow K$ fonksiyonunun da bir homomorfi olduğunu söyler.

Aynı zamanda eşleme olan $\varphi : G \longrightarrow H$ homomorfilerine ***izomorfi*** adı verilir. Aynı zamanda eşleşme olan $\varphi : G \longrightarrow G$ homomorfilerine ***otomorfi*** adı verilir. G'nin otomorfilerinden oluşan küme $\operatorname{Aut} G$ olarak yazılır. Bir önceki paragrafa göre izomorfilerin bileşkesi gene bir izomorfidir ve dolayısıyla $\operatorname{Aut} G$ kümesi bileşke altında kapalıdır. Bir G grubundan kendisine giden homomorfilere ***endomorfi*** adı verilir ve bu küme $\operatorname{Hom}(G, G)$ yerine $\operatorname{End} G$ olarak gösterilir. $\operatorname{End} G$ kümesi de $\operatorname{Aut} G$ kümesi gibi bileşke altında kapalıdır.

Eğer $\varphi : G \longrightarrow H$ bir izomorfiyse, o zaman φ'nin ters fonksiyonu olan $\varphi^{-1} : H \longrightarrow G$ de bir izomorfidir. Nitekim eğer $h_1, h_2 \in H$ ise, $\varphi(g_1) = h_1$ ve $\varphi(g_2) = h_2$ eşitliklerini, yani $\varphi^{-1}(h_1) = g_1$ ve $\varphi^{-1}(h_2) = g_2$ eşitliklerini sağlayan $g_1, g_2 \in G$ elemanlarını seçip hesap yapalım:

$$\begin{aligned}\varphi^{-1}(h_1h_2) &= f^{-1}(f(g_1)f(f_2)) = f^{-1}(f(g_1))f^{-1}(f(g_2)) \\ &= g_1g_2 = \varphi^{-1}(h_1)\varphi^{-1}(h_2)\end{aligned}$$

olur. Dolayısıyla otomorfilerin (bileşke işlemine göre) tersleri de bir otomorfidir.

Bunun dışında $\operatorname{Id}_G : G \longrightarrow G$ özdeşlik fonksiyonu elbette bir otomorfidir.

Yukarıdaki söylediklermizden şu sonuç çıkar:

Teorem 10.2. *Eğer G bir grupsa, $\operatorname{Aut} G$ kümesi de fonksiyonların bileşkesi işlemi altında bir gruptur.* □

Elbette $\operatorname{Aut} G$, $\operatorname{Sym} G$'nin bir altgrubudur, ne de olsa $\operatorname{Aut} G$'nin elemanları aynı zamanda G'nin eşleşmeleridir.

Notlar ve Örnekler

10.37. $\varphi \in \operatorname{End} \mathbb{Q}$ olsun. $\varphi(1) = a$ olsun. Her $q \in \mathbb{Q}$ için $\varphi(q) = aq$ eşitliğini kanıtlayacağız. $\varphi(n+1) = \varphi(n) + \varphi(1) = \varphi(n) + a$ eşitliğinden tümevarımla her $n \in \mathbb{N}$ için $\varphi(n) = an$ eşitliği çıkar. $\varphi(-n) = -\varphi(n)$ eşitliğinden de her $n \in \mathbb{N}$ için $\varphi(n) = an$ eşitliği çıkar. Şimdi $n, m \in \mathbb{Z}$ olmak üzere $q = n/m$ olsun. O zaman

$$an = \varphi(n) = \varphi\left(m\frac{n}{m}\right) = m\varphi\left(\frac{n}{m}\right) = m\varphi(q)$$

olur ve bundan da istenen $\varphi(q) = an/m = aq$ eşitliği çıkar.

10.38. $\mathbb{Z} \times \mathbb{Z}$ grubunun endomorfilerini bulalım. $\varphi \in \mathrm{End}(\mathbb{Z} \times \mathbb{Z})$ olsun. $\mathbb{Z} \times \mathbb{Z}$ grubu $e_1 = (1, 0)$ ve $e_2 = (0, 1)$ elemanları tarafından üretildiğinden, φ endomorfisi bu elemanların imgeleri tarafından belirlenir. Nitekim eğer

$$\varphi(e_1) = (a,\, b) \text{ ve } \varphi(e_2) = (c,\, d)$$

ise her $(x,\, y) \in \mathbb{Z} \times \mathbb{Z}$ için,

$$\varphi(x,\, y) = \varphi(xe_1 + ye_2) = x\varphi(e_1) + y\varphi(e_2) = x(a,\, b) + y(c,\, d) = (xa + yc,\, xb + yd)$$

olur. Ayrıca her $(a,\, b)$ ve $(c,\, d)$ seçimi bize bir endomorfi verir.

10.39. exp fonksiyonu $\mathbb{R}$ grubundan $\mathbb{R}^{>0}$ grubuna giden bir izomorfidir ve tersi olan ln fonksiyonu $\mathbb{R}^{>0}$ grubundan $\mathbb{R}$ grubuna giden bir izomomorfidir.

10.40. $\mathrm{Aut}\,\mathbb{Z}$ iki elemandan oluşur: $\mathrm{Id}_{\mathbb{Z}}$ ve $-\mathrm{Id}_{\mathbb{Z}}$. (Bkz. Örnek 10.17.) Birincisi $x \mapsto x$, ikincisi $x \mapsto -x$ kuralıyla verilir. Şimdi $\mathbb{Z}$ yerine, bir a için $A = \{a^n : n \in \mathbb{Z}\}$ biçiminde yazılan **sonsuz** döngüsel grubu ele alalım. Bu grup elbette $\mathbb{Z}$ grubuna izomorftur. Dolayısıyla $\mathrm{Aut}\, A \simeq \mathrm{Aut}\,\mathbb{Z}$ olmalı, dolayısıyla A'nın iki otomorfisi olmalı. Bunlardan biri $x \mapsto x$, diğeri $x \mapsto x^{-1}$ kuralıyla verilmiştir.

10.41. $H \lhd G$ olsun. O zaman G'nin her g elemanı $x \mapsto x^g$ kuralıyla H'nin bir otomorfisini doğurur. H'nin bu otomorfisine φ_g diyelim. Kolaylıkla $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$ eşitliği kanıtlanabilir. Demek ki $\varphi(g) = \varphi_g$ kuralıyla tanımlanmış $\varphi : G \longrightarrow \mathrm{Aut}\, H$ fonksiyonu bir homomorfidir.

10.42. Yukarıdaki örneği genelleştirebiliriz. G herhangi bir grup ve $H,\, K \leq G$ olsun. $K \leq N_G(H)$ varsayımını yapalım. O zaman $k \in K$ ve $h \in H$ için $\varphi_k(h) = khk^{-1}$ kuralıyla tanımlanmış φ_k fonksiyonu H'den gene H'ye giden bir otomorfidir. Ayrıca $\varphi_k \circ \varphi_{k'} = \varphi_{kk'}$ olur; yani $\varphi(k) = \varphi_k$ kuralı bize bir $\varphi : K \longrightarrow \mathrm{Aut}\, H$ homomorfisi verir.

10.43. G herhangi bir grup, $n > 0$ bir tamsayı ve $\sigma \in \mathrm{Sym}\, n$ olsun. O zaman G^n kartezyen grubunun koordinatlarını σ elemanına göre kararsak, yani $(g_i)_i$ elemanını $(g_{\sigma(i)})_i$ elemanına dönüştürürsek, G^n'nin bir φ_σ otomorfisini elde ederiz. Örneğin $n = 6$ ve $\sigma = (1\ 2\ 3)(5\ 6)$ ise

$$\varphi_\sigma(g_1, g_2, g_3, g_4, g_5, g_6) = (g_2, g_3, g_1, g_4, g_6, g_5)$$

olur. Her $\alpha,\, \beta \in \mathrm{Sym}\, n$ için $\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha\beta}$ olur. Böylece $\varphi(\sigma) = \varphi_\sigma$ kuralıyla verilmiş bir $\varphi : \mathrm{Sym}\, n \longrightarrow \mathrm{Aut}\, G^n$ homomorfisi elde ederiz.

Bu örnekte endis kümesini sonlu olmak zorunda değildik, endis kümesi herhangi bir I kümesi olabilirdi. Bu durumda σ'yı $\mathrm{Sym}\, n$'den seçmek durumunda olurduk.

Alıştırmalar

10.44. G bir grup olsun. $x \mapsto x^{-1}$ fonksiyonunun bir otomorfi olmasıyla G'nin abel grubu olmasının eşdeğer koşullar olduğunu gösterin.

10.45. G bir grup olsun. $x \mapsto x^2$ fonksiyonunun bir endomorfi olmasıyla G'nin abel grubu olmasının eşdeğer koşullar olduğunu gösterin. (Aynı alıştırma, 2 yerine 3 sayısı için doğru değildir.)

10.46. G bir grup olsun. $(g_1, g_2) \mapsto (g_2, g_1)$ fonksiyonunun $G \times G$ grubunun bir otomorfisi olduğunu gösterin.

10.47. G bir grup olsun. $G^n = G \times \ldots \times G$ (n defa) olsun. $\mathrm{Sym}\, n$ grubundan $\mathrm{Aut}\, G^n$ grubunun içine giden birebir homomorfi olduğunu gösterin. (İpucu: $\mathrm{Sym}\, n$'nin elemanları G^n grubunun koordinatlarını tahmin edildiği gibi değiştirsin.)

10.48. $\mathbb{Z} \times \mathbb{Z}$ grubunu ele alalım. $e_1 = (1, 0)$ ve $e_2 = (0, 1)$ olsun. Rastgele bir G grubu olsun ve $\varphi : \mathbb{Z} \times \mathbb{Z} \longrightarrow G$ bir homomorfi olsun. $\varphi(e_1)\varphi(e_2) = \varphi(e_2)\varphi(e_1)$ eşitliğini kanıtlayın.

Şimdi G grubundan g_1 ve g_2 elemanları alalım. Bu elemanların birbirileriyle değiştiğini varsayalım, yani $g_1 g_2 = g_2 g_1$ olsun. $\mathbb{Z} \times \mathbb{Z}$ grubundan G grubuna giden ve $\varphi(e_1) =$

g_1 ve $\varphi(e_2) = g_2$ eşitliklerini sağlayan bir homomorfi olduğunu kanıtlayın; ayrıca bu homomorfinin biricik olduğunu kanıtlayın.

Yukarıdaki alıştırmayı $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ ve herhangi bir I göstergeç kümesi için $\oplus_I \mathbb{Z}$ gruplarına genelleştirin.

10.49. $A = \mathbb{Z} \times \mathbb{Z}$ grubunu ele alalım. $e_1 = (1, 0)$ ve $e_2 = (0, 1)$ olsun. A'dan A'ya giden ve $\varphi(e_1) = (1, 2)$, $\varphi(e_2) = (1, 1)$ eşitliklerini sağlayan bir $\varphi \in \operatorname{End} A$ olduğunu bir önceki alıştırmadan biliyoruz. Bu endomorfinin bir izomorfi olduğunu kanıtlayın.

$\varphi(e_1) = (1, 2)$, $\varphi(e_2) = (3, 1)$ eşitliklerini sağlayan $\varphi \in \operatorname{End} A$ endomorfisinin birebir olduğunu ama örten olmadığını kanıtlayın.

$\varphi(e_1) = (1, 2)$, $\varphi(e_2) = (2, 1)$ eşitliklerini sağlayan $\varphi \in \operatorname{End} A$ endomorfisinin ne birebir ne örten olduğunu kanıtlayın.

Hangi a, b, c, $d \in \mathbb{Z}$ sayıları için $\varphi(e_1) = (a, b)$, $\varphi(e_2) = (c, d)$ eşitliklerini sağlayan $\varphi \in \operatorname{End} A$ endomorfisi birebirdir, ya da örtendir?

10.50. Bu alıştırmada bir abel grubunun endomorfilerinin bir "halka" oluşturduğunu göstereceğiz. $A \neq 1$ bir abel grubu olsun. Kolaylık olması açısından A'nın işlemini toplamayla yazalım. Eğer α, $\beta \in \operatorname{End} A$ ise $\alpha + \beta : A \longrightarrow A$ fonksiyonu da bir endomorfi olur. (Bkz. Alıştırma 10.31.) Ayrıca $\alpha \circ \beta$ fonksiyonunun da bir endomorfizma olduğunu biliyoruz. Bundan böyle $\alpha \circ \beta$ yerine $\alpha\beta$ yazalım ve bunu α ile β'nın çarpımı olarak algılayalım.

a. $\operatorname{End} A$ kümesinin toplama altında bir abel grubu olduğunu gösterin. Toplamanın etkisiz elemanı olan sabit 0 fonksiyonunu gene 0 olarak göstereceğiz.

b. Her α, β, $\gamma \in \operatorname{End} A$ için $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ olduğunu zaten biliyoruz; bu eşitlik sadece endomorfiler için değil, tüm fonksiyonlar için geçerlidir.

c. Her α, β, $\gamma \in \operatorname{End} A$ için $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ ve $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ eşitliklerini gösterin.

d. $\mathrm{Id}_A \in \operatorname{Aut} A \subseteq \operatorname{End} A$ elemanı çarpmanın etkisiz elemanıdır. Bu elemanı 1 olarak göstereceğiz. $1 \neq 0$ olduğunu gözlemleyin.

Yukarıdaki özellikleri olan bir $(\operatorname{End} A, +, \circ, 0, 1)$ yapısına ***halka*** denir.

10.51. Her x, $t \in \mathbb{Z}$ için $\psi_t(\overline{x}) = \overline{tx}$ kuralı bize bir $\psi_t : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ grup endomorfisi verir. $\operatorname{End}(\mathbb{Z}/n\mathbb{Z}) = \{\psi_t : t = 0, 1, \ldots, n-1\}$ eşitliğini kanıtlayın. (Bkz. Örnek 10.20.)

$\psi(\overline{t}) = \psi_t$ kuralıyla tanımlanmış $\psi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \operatorname{End}(\mathbb{Z}/n\mathbb{Z})$ fonksiyonunun (gerçekten) iyi tanımlı, birebir ve örten olduğunu kanıtlayın. $\psi(\overline{t} + \overline{s}) = \psi(\overline{t}) + \psi(\overline{s})$ ve $\psi(\overline{t}\,\overline{s}) = \psi(\overline{t}) \circ \psi(\overline{s})$ eşitliklerini kanıtlayın.

$\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) = \{\psi_t : t = 0, 1, \ldots, n-1 \text{ ve } \operatorname{ebob}(t, n) = 1\}$ eşitliğini kanıtlayın.

10.52. Bir önceki alıştırmadan esinlenerek $\operatorname{End} \mathbb{Z}$ halkasını (kümesini ve toplama ve bileşke işlemlerini) bulun.

10.53. Örnek 10.15'deki H_i grupları abel grupları olsun. O örnekte bulunan α ve β fonksiyonları homomorfilerin toplamasıyla uyumlu mudur, yani bir grup homomorfisi midir?

10.54. $\operatorname{Aut} D_8$ gurubunu bulun.

10.55. $\mathbb{Z} \times \mathbb{Z}$ grubunun otomorfi grubunu ve bu grubun merkezini bulun.

10.56. $A \subseteq G$ bir altküme ve $X = \{A^x : x \in G\}$ olsun. Eğer $g \in G$ ise ve $B \in X$ ise $\tilde{g}(B) = B^g$ tanımını yapalım. $\tilde{g} \in \operatorname{Sym} X$ olduğunu kanıtlayın. $\gamma \mapsto \tilde{g}$ fonksiyonunun G'den $\operatorname{Sym} X$'e giden bir homomorfi olduğunu kanıtlayın.

10.57. G sonlu bir grup olsun. $\varphi \in \operatorname{Aut} G$, derecesi 2 olan bir otomorfi olsun, yani $\varphi \circ \varphi = \mathrm{Id}_G$ olsun. Eğer $\varphi(g) = g$ olduğunda $g = 1$ oluyorsa, yani φ'nin 1'den başka sabitlediği nokta yoksa, o zaman her $g \in G$ için $\varphi(g) = g^{-1}$ olduğunu (dolayısıyla G'nin abel olduğunu, bkz. Alıştırma 10.44) kanıtlayın. İpucu: Önce G'nin her elemanının $g^{-1}\varphi(g)$ olarak yazıldığını gösterin; sonra bu tür elemanlara φ'yi uygulayın.

İç Otomorfiler. Şimdi bir G grubunun özel otomorfilerinden sözedeceğiz. Kolayca kanıtlanabileceği üzere, $g \in G$ ise, $x \mapsto gxg^{-1}$ kuralıyla tanımlanmış $\mathrm{Inn}_g : G \longrightarrow G$ fonksiyonu G'nin bir otomorfisidir. Bunu kanıtlamak için, Inn_g fonksiyonunun birebir ve örten olduğunu ve $\mathrm{Inn}_g(xy) = \mathrm{Inn}_g(x)\,\mathrm{Inn}_g(y)$ eşitliğini göstermek gerekir, ki bunlar da oldukça basit hesaplardır. Inn_g türünden otomorfilere G'nin ***iç otomorfisi*** adı verilir. Buradan, G'den $\mathrm{Aut}\,G$'ye giden bir $\mathrm{Inn} : G \longrightarrow \mathrm{Aut}\,G$ fonksiyonu elde ederiz: $\mathrm{Inn}(g) = \mathrm{Inn}_g$. Bu fonksiyon da bir homomorfidir, ancak birebir ya da örten olmayabilir. Inn fonksiyonunun homomorfi olduğunu kanıtlamak kolay: Her g, h, $x \in G$ için,

$$\begin{aligned}(\mathrm{Inn}_g \circ \mathrm{Inn}_h)(x) &= \mathrm{Inn}_g((\mathrm{Inn}_h)(x)) = \mathrm{Inn}_g(hxh^{-1}) = ghxh^{-1}g^{-1} \\ &= (gh)x(gh)^{-1} = \mathrm{Inn}_{gh}(x)\end{aligned}$$

ve dolayısıyla her g, $h \in G$ için

$$\mathrm{Inn}_g \circ \mathrm{Inn}_h = \mathrm{Inn}_{gh}$$

olur. Inn fonksiyonunun bir homomorfi olmasından,

$$(Inn_g)^{-1} = \mathrm{Inn}_{g^{-1}}$$

eşitliği çıkar, ama bunu doğrudan göstermek de çok kolay.

Bir grubun iç otomorfilerinden başka otomorfileri de olabilir; ama bazen de olmayabilir. Mesela $n \geq 3$ amd $n \neq 6$ ise, $\mathrm{Sym}\,n$'nin sadece iç otomorfileri vardır ama bunu göstermek hiç kolay değildir.

İç otomorfiler kümesi $\mathrm{Inn}\,G$ elbette $\mathrm{Aut}\,G$ grubunun bir altgrubudur. Bu altgrubun normal bir altgrup olduğunu iddia edip kanıtlıyoruz. g, $x \in G$ ve $\varphi \in \mathrm{Aut}\,G$ olsun. Hesap yapalım:

$$(\varphi^{-1}\,\mathrm{Inn}_g\,\varphi)(x) = \varphi^{-1}(g\varphi(x)g^{-1}) = \varphi^{-1}(g)x\varphi^{-1}(g)^{-1} = \mathrm{Inn}_{\varphi^{-1}(g)}(x)$$

ve dolayısıyla

$$\varphi^{-1}\,\mathrm{Inn}_g\,\varphi = \mathrm{Inn}_{\varphi^{-1}(g)},$$

yani $\mathrm{Inn}\,G \lhd \mathrm{Aut}\,G$.

Alıştırmalar

10.58. $g \in Z(G)$ koşuluyla $\mathrm{Inn}_g = \mathrm{Id}_G$ koşulunun eşdeğer olduğunu kanıtlayın.

10.59. $\mathrm{Inn}_g = \mathrm{Inn}_h$ eşitliğinin doğru olması için $gh^{-1} \in Z(G)$ koşulunun gerek ve yeter olduğunu kanıtlayın. Dolayısıyla eğer $Z(G) = 1$ ise $\mathrm{Inn} : G \longrightarrow \mathrm{Aut}\,G$ homomorfisi birebirdir.

10.60. $H \lhd G$ olsun. O zaman G'nin her g elemanı $x \mapsto x^g$ kuralıyla H'nin bir otomorfisini doğurur. H'nin bu otomorfisine φ_g diyelim. Kolaylıkla $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_1}$ eşitliği kanıtlanabilir. Demek ki $\varphi(g) = \varphi_g$ kuralıyla tanımlanmış $\varphi : G \longrightarrow \mathrm{Aut}\,H$ fonksiyonu bir homomorfidir.

$$\varphi(g) \in \mathrm{Inn}\,H \Leftrightarrow g \in C_G(H)H$$

önermesini kanıtlayın.

Karakteristik Altgruplar. G bir grup ve $H \leq G$ olsun. Eğer her $\varphi \in \operatorname{Aut} G$ için $\varphi(H) \subseteq H$, dolayısıyla $\varphi(H) = H$ oluyorsa, H'ye ***karakteristik altgrup*** denir. Bu durumda $H \operatorname{char} G$ yazılır. Karakteristik altgruplar iç otomorfiler altında değişmediğinden normal olurlar.

Eğer $X \subseteq G$ altkümesi G'nin otomorfileri altında yerinden kımıldamıyorsa, X'e ***karakteristik altküme*** denir. Karakteristik altkümeler tarafından üretilen altgruplar karakteristik altgruplar olurlar elbet.

Alıştırmalar

10.61. $\mathbb{Z}$'nin her altgrubu karakteristiktir.

10.62. $\mathbb{Z} \times \mathbb{Z}$ grubunun karakteristik olmayan bir altgrubunu bulun.

10.63. $\mathbb{Z} \times \mathbb{Z}$ grubunun karakteristik olan sonsuz sayıda altgrubunu bulun.

10.64. $Z(G) \operatorname{char} G$ olduğunu gösterin.

10.65. $K \operatorname{char} H \operatorname{char} G$ ise $K \operatorname{char} G$ olduğunu gösterin.

10.66. Eğer $H \operatorname{char} G$ ise $C_G(H) \operatorname{char} G$ olduğunu gösterin.

10.67. Eğer H, $K \operatorname{char} G$ ise $HK \operatorname{char} G$ olduğunu gösterin.

10.68. Eğer H, $K \operatorname{char} G$ ise $[H, K] \operatorname{char} G$ olduğunu gösterin.

10.69. π bir asallar kümesiyse, $\langle h : h \text{ bir } \pi\text{-eleman} \rangle \operatorname{char} G$ olduğunu gösterin.

10.70. $n \in \mathbb{N}$ ise $\langle h^n : h \in G \rangle \operatorname{char} G$ olduğunu gösterin.

10.71. $h \in G$ ise $\langle \varphi(h) : \varphi \in \operatorname{Aut} G \rangle \operatorname{char} G$ olduğunu gösterin.

10.72. G bir grup, $t \in G$ derecesi 2 olan bir eleman olsun. $X = \{[t, g] : g \in G\}$ olsun. Bu alıştırmada X'in bir abel grubu olduğunu (ve fazlasını) kanıtlayacağız.
a. $x \in X$ için $x^t = x^{-1}$ olduğunu kanıtlayın. Elbette $t \notin X$. Buradan, tX'in elemanlarının derecesinin 2 olduğunu gösterin.
b. $\varphi(gC_G(t)) = [t, g^{-1}]$ kuralıyla tanımlanmış $\varphi : G/C_G(t) \longrightarrow X$ fonksiyonunun iyi tanımlanmış olduğunu ve bir eşleme olduğunu kanıtlayın.
Bundan böyle G'nin sonlu olduğunu ve $C_G(t) = \{1, t\}$ varsayımını yapalım.
c. (b)'den dolayı $|X| = |G|/2$ olduğunu gösterin.
d. (a)'dan dolayı X'te derecesi 2 olan bir elemanının olmadığını gösterin.
e. Yukarıdakilerden $X \cap tX = \emptyset$ olduğunu gösterin.
f. Buradan $G = X \sqcup tX$ eşitliğini ve X'in derecesi $\neq 2$ olan elemanlardan oluştuğunu gösterin.
g. Demek ki X, G'nin karakteristik bir altkümesidir, yani otomorfiler tarafından yerinden oynatılamaz.
h. $x \in X \setminus \{1\}$ sabit bir eleman olsun. t^x'in de X'in elemanlarını terslerine yolladığını yani her $y \in X$ için $y^{t^x} = y^{-1}$ olduğunu kanıtlayın.
i. Buradan $1 \neq x^2 = tt^x$ elemanının X'in elemanlarını merkezlediğini gösterin.
j. Buradan $X = C_G(x^2) \leq G$ çıkar.
k. (1)'den dolayı X bir abel grubudur.

10.73. G derecesi 2 olan elemanı bulunmayan burulmalı bir grup olsun. G'nin derecesi 2 olan bir φ otomorfisi olduğunu ve bu otomorfinin 1'den başka eleman sabitlemediğini varsayalım. Her $g \in G$ için $\varphi(g) = g^{-1}$ olduğunu (dolayısıyla G'nin bir abel grubu olduğunu) kanıtlayacağız.
a. Her $a, b \in G$ için eğer $a^2 = b^2$ ise $a = b$ olduğunu gösterin.
Bundan böyle bir $g \in G$ sabitleyelim. G'nin 2-bölünür olduğunu biliyoruz (Sonuç 4.9). $h^2 = \varphi(g^{-1})g$ eşitliğini sağlayan bir $h \in G$ alalım.
b. $\varphi(h)^2 = h^{-2}$ olduğunu, buradan da $\varphi(h) = h^{-1}$ eşitliğini kanıtlayın.

c. $\varphi(gh^{-1}) = gh^{-1}$ eşitliğini, buradan da $g = h$ eşitliğini kanıtlayın. Bu da istediğimiz sonucu verir.

10.3 İzomorfik Gruplar

İki izomorfik grup arasında grupların elemanlarının ve işlemlerinin adları ve gösterimleri dışında grup teori açısından hiçbir fark yoktur. Nitekim eğer $f : G \longrightarrow H$ bir izomorfiyse, φ'yi bir sözlük gibi kullanıp G dilinde yazılan önermeleri H dilinde yazılmış önermeler haline dönüştürebiliriz ve birinde doğru olan önermenin çevrilmiş hali diğerinde de doğru olur. Örneğin a, b, $c \in G$ gibi elemanlar arasındaki her türlü ilişki $\varphi(a)$, $\varphi(b)$, $f(c) \in H$ elemanları arasında da geçerlidir. Ya da a, b, $c \in G$ gibi elemanlar içeren $xayabxyxc = 1$ benzeri herhangi bir denklemin G'de çözümü varsa, bu denklemin muadili olan (örneğimizde $x\varphi(a)y\varphi(a)\varphi(b)xyx\varphi(c) = 1$) denkleminin H'de de çözümü vardır ve G'de ne kadar çözüm varsa, H'de de o kadar çözüm vardır. Ya da G bir abel grubuysa H'de bir abel grubudur. G'de her x, y, z için $[[x, y], [x, z]] = 1$ eşitliği geçerliyse, aynı eşitlik H'nin her x, y, z elemanı için de geçerlidir. Bu dediklerimizin ters istikameti de doğrudur: H'de doğru olan her önerme, φ^{-1} sözlüğüyle G'nin diline çevrildiğinde G'de de doğru olur.

Dolayısıyla izomorfik gruplar grup teori açısından eşit sayılmalıdır. Eşit olmadıklarından, eşitlik yerine $\simeq$ işaretini kullanacağız ve G ve H grupları izomorfikse $G \simeq H$ yazacağız. $\simeq$ ilişkisi gruplar sınıfı[4] üzerine bir denklik ilişkisidir: Her G, H, K grubu için,

$G \simeq G$

$G \simeq H$ ise $H \simeq G$

$G \simeq H$ ise $H \simeq K$ ise $G \simeq K$

önermeleri geçerlidir.

Notlar ve Örnekler

10.74. Tüm 1 elemanlı gruplar birbirine izomorfiktir.

10.75. $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ grubuyla çarpma altında bir grup olan $\mathbb{R}^\star$ grubunun $\{1, -1\}$ altgrubu izomorfiktirler. Nitekim $\overline{0}$ elemanını 1'e (etkisiz eleman etkisiz elemana gitmek zorunda), $\overline{1}$ elemanını -1'e götüren φ fonksiyonu bir izomorfidir, $\varphi(x + y) = f(x)\varphi(y)$ eşitliğini sağlar.

10.76. İki elemanlı tüm gruplar izomorfiktirler. Nitekim $\{1, x\}$, iki elemanlı bir grup olsun. 1 etkisiz eleman olduğundan, x'in tersi 1 olamaz; x'in tersi gene x olmalı. Demek ki $x^2 = 1$ olmalı. Görüldüğü gibi grubun çarpması tamamen belirlendi. Bu yaptığımız tabii ki tüm gruplar için geçerli. (Eğer grubun işlemi toplamaysa, yaptıklarımızı toplamanın diline çevirmek gerekir.) Dolayısıyla tüm iki elemanlı gruplar izomorfiktirler ve hatta birinden

[4] Gruplar bir küme oluşturmazlar. Ne de olsa her x kümesi için bir elemanlı $\{x\}$ kümesi vardır, yani çok fazla grup vardır, küme olamayacak kadar. Küme olan ya da olmayan topluluklara genel olarak ***sınıf*** adı verilir. Mesele tüm kümeler topluluğu küme olmayan bir sınıftır.

diğerine giden tek bir izomorfi vardır. Eğer gruplardan biri $\{1, x\}$ diğeri $\{1, y\}$ ise, izomorfi 1'i 1'e, x'i y'ye götürmek zorundadır.

10.77. Üç elemanlı tüm gruplar da izomorfiktirler, ama bu sefer üç elemanlı iki grup arasında iki farklı izomorfi vardır. Eğer gruplardan biri $\{1, x, x^2\}$ diğeri $\{1, y, y^2\}$ ise $x \mapsto y$ ve $x \mapsto y^2$ iki farklı izomorfiye yol açar.

10.78. $\mathbb{P} \subseteq \mathbb{N}$, asallar kümesi olsun. $0 \neq x \in \mathbb{N}$ olsun. x'i asallarına ayıralım:

$$x = \prod_{p \in \mathbb{P}} p^{\mathrm{val}_p\, x}.$$

Burada $\mathrm{val}_p\, x$, p'nin x'i bölen en büyük kuvvetidir. Örneğin, her $p \in \mathbb{P}$ için

$$\mathrm{val}_3\, 18 = 2,\ \mathrm{val}_2\, 18 = 1,\ \mathrm{val}_5\, 1000 = 3,\ \mathrm{val}_7\, 121 = 0,\ \mathrm{val}_p\, 1 = 0,\ \mathrm{val}_p\, p^n = n$$

olur. Eğer p asalı x'i bölmüyorsa, $\mathrm{val}_p\, x = 0$ olur; dolayısıyla yukarıdaki çarpım aslında sonlu bir çarpımdır, çarpılan terimlerin hemen hepsi 1'e eşittir. Elbette

$$\mathrm{val}_p\, xy = \mathrm{val}_p\, x + \mathrm{val}_p\, y$$

olur; bir başka deyişle eğer $\mathbb{N}$'de elemanları asallarına ayırabilirsek, çarpma işlemi aslında elemanları bölen asalların en büyük kuvvetlerinin toplamasıyla elde edilir;örneğin

$$(2^{754}3^{24}5^{76})(2^{141}5^{15}7^{14}) = 2^{895}3^{24}5^{91}7^{14}$$

olur. Şimdi $q \in \mathbb{Q}^{>0}$ olsun. $x,\ y \in \setminus\{0\}$ için $q = x/y$ olarak yazalım. O zaman,

$$q = \frac{x}{y} = \frac{\prod_{p \in \mathbb{P}} p^{\mathrm{val}_p\, x}}{\prod_{p \in \mathbb{P}} p^{\mathrm{val}_p\, y}} = \prod_{p \in \mathbb{P}} p^{\mathrm{val}_p\, x - \mathrm{val}_p\, y}$$

olur.

$$\mathrm{val}_p\, q = \mathrm{val}_p\, x - \mathrm{val}_p\, y$$

tanımını yapalım. Bu tanımın iyi bir tanım olduğu, yani $x/y = x_1/y_1$ ise

$$\mathrm{val}_p\, x - \mathrm{val}_p\, y = \mathrm{val}_p\, x_1 - \mathrm{val}_p\, y_1$$

olduğu belli. Yukarıda elde ettiğimiz eşitliği bu tanımla tanıştıralım: Aynen doğal sayılarda olduğu gibi

$$q = \prod_{p \in \mathbb{P}} p^{\mathrm{val}_p\, q}$$

elde ederiz, ama bu sefer $\mathrm{val}_p\, q$ sayıları negatif de olabilirler. Gene aynen doğal sayılarda olduğu gibi,

$$\mathrm{val}_p\, qq' = \mathrm{val}_p\, q + \mathrm{val}_p\, q'$$

olur; ama bunun dışında bir de,

$$\mathrm{val}_p\, \frac{q}{q'} = \mathrm{val}_p\, q - \mathrm{val}_p\, q'$$

olur. Şimdi,

$$\varphi : \mathbb{Q}^{>0} \longrightarrow \bigoplus_{\mathbb{P}} \mathbb{Z}$$

fonksiyonunu

$$\varphi(q) = (\mathrm{val}_p\, q)_p$$

olarak tanımlayalım. φ fonksiyonu birebir ve örtendir. Ayrıca $\varphi(qq') = \varphi(q) + \varphi(q')$ olur. Demek ki φ bir izomorfidir:

$$\mathbb{Q} \simeq \bigoplus_{\mathbb{P}} \mathbb{Z}.$$

10.79. G bir grup, X bir küme olsun. $f : G \longrightarrow X$ bir eşleme olsun. $x, y \in X$ için $x \star y = f(f^{-1}(x)f^{-1}(y))$ tanımını yapalım. $(X, \star)$ ikilisi bir grup olur ve böylece $f : G \longrightarrow X$ bir izomorfiye dönüşür. (Bkz. Alıştırma 1.79.)

10.80. A, $\oplus_{i\in I}\mathbb{Z}$ grubunun koordinatları çift sayılardan oluşan altkümesi olsun. A'nın bir grup olduğu bariz olmalı. A ile $\oplus_{i\in I}\mathbb{Z}$ grubunun izomorfik olduklarını gösterin.

10.81. Aynı eleman sayısına sahip (sonlu ya da sonsuz) tüm döngüsel gruplar izomorfiktirler. Eğer grubun n elemanı varsa, grup $\{1, x, x^2, \ldots, x^{n-1}\}$ biçimindedir ve $x^r x^s = x^{r+s}$ olduğundan, $\overline{r} \mapsto x^r$ fonksiyonu $\mathbb{Z}/n\mathbb{Z}$ grubundan bu guruba giden bir izomorfidir. Eğer grubun sonsuz sayıda elemanı varsa, o zaman grubun x^n türünden elemanları farklı n tamsayıları için farklı elemanlardır ve $n \mapsto x^n$ fonksiyonu $\mathbb{Z}$'den gruba giden bir izomorfidir.

Teorem 10.3. *Aynı elemana sahip iki döngüsel grup birbirine izomorfiktir. Eleman sayısı $n < \infty$ olan bir döngüsel grup $\mathbb{Z}/n\mathbb{Z}$ grubuna, eleman sayısı sonsuz olan döngüsel bir grup $\mathbb{Z}$ grubuna izomorfiktir.* □

10.82. Asal sayıda elemanı olan bir grup döngüsel olmak zorundadır. Dolayısıyla bir p asalı için p tane elemanı olan bir grup $\mathbb{Z}/p\mathbb{Z}$ grubuna izomorftur.

Teorem 10.4. *Eğer p bir asalsa, p elemana sahip her grup $\mathbb{Z}/p\mathbb{Z}$ grubuna izomorfiktir.* (*Dolayısıyla döngüseldir, dolayısıyla abel grubudur.*) □

10.83. G bir grup ve $A, B \leq G$ olsun. Her $a \in A$ ve her $b \in B$ için $ab = ba$ varsayımını yapalım. O zaman $AB \leq G$ olur. Bir de ayrıca $A \cap B = 1$ varsayımını yapalım. O zaman $(a, b) \mapsto ab$ kuralı bize $A \times B$ grubuyla (kartezyen çarpım, bkz. Alıştırma 1.7) AB altgrubu arasında bir homomorfi verir (kontrol edilmeli; bunun için A ve B'nin elemanlarının birbirleriyle değişmeleri önemlidir). Bu homomorfi örtendir elbette, ama aynı zamanda birebirdir: $a, a_1 \in A$ ve $b, b_1 \in B$ için $ab = a_1b_1$ ise o zaman $a_1^{-1}a = b_1b^{-1} \in A \cap B = 1$ olur, yani $a = a_1$ ve $b = b_1$ olur. Demek ki bu durumda $A \times B \simeq AB$ olur. Aşağıdaki teoremi kanıtladık:

Teorem 10.5. *G bir grup ve $A, B \leq G$ olsun. Her $a \in A$ ve her $b \in B$ için $ab = ba$ ve $A \cap B = 1$ varsayımlarını yapalım. O zaman $(a, b) \mapsto ab$ kuralı bize $A \times B$ grubuyla G'nin AB altgrubu arasında bir izomorfi verir.* □

10.84. G, kendisinden ve 1'den başka altgrubu olmayan bir grup olsun. Diyelim $G \neq 1$. O zaman her $1 \neq x \in G$ için $\langle x\rangle = G$ olur. Demek ki bir $1 \neq n \in \mathbb{N}$ için $G \simeq \mathbb{Z}/n\mathbb{Z}$. Ama n asal değilse $\mathbb{Z}/n\mathbb{Z}$'nin 1'den farklı özaltgrupları vardır. Demek ki bir p asalı için $G \simeq \mathbb{Z}/p\mathbb{Z}$. Bunu da teorem olarak yazalım:

Teorem 10.6. *Kendisinden ve 1'den başka altgrubu olmayan bir grup bir p asalı için $\mathbb{Z}/p\mathbb{Z}$ grubuna izomorftur.* □

10.85. G bir grup, I bir index kümesi ve $(A_{i\in I})$, G'nin bir altgrup ailesi olsun. Her $i \neq j$ ve her $a_i \in A_i$ ve $a_j \in A_j$ için $a_ia_j = a_ja_i$ varsayımını yapalım. Bu durumda $\langle A_i : i \in I\rangle$ grubunun elemanlarını birbirinden farklı $i_1, \ldots, i_k \in I$ göstergeçleri ve $a_{i_j} \in A_{i_j}$ elemanları için $a_{i_1} \cdots a_{i_k}$ biçiminde yazabiliriz. Yani A_i altgruplarının elemanlarını herhangi bir sıra gözetmeksizin dilediğimiz gibi çarpabiliriz. Dolayısıyla $(a_i)_i \mapsto \prod_i a_i$ kuralı bize $\oplus A_i$ grubundan $\langle A_i : i \in I\rangle$ altgrubuna giden bir fonksiyon verir. Bu fonksiyon elbette örten bir homomorfidir. Ama birebir olmayabilir. Birebir olabilmesi için A_i'lerden birinin 1'den farklı bir elemanını diğerlerinin elemanlarının çarpımı olarak yazamamız gerekir, yani $\langle A_i : i \in I \setminus \{j\}\rangle \cap A_j = 1$ eşitliğinin olması gerekir (neden?) O zaman $(a_i)_i \mapsto \prod_i a_i$ kuralı bize $\oplus A_i$ grubuyla G'nin $\langle A_i : i \in I\rangle$ altgrubu arasında bir izomorfi verir.

Bunu da bir teorem olarak yazabiliriz.

Teorem 10.7. *G bir grup, I bir index kümesi ve $(A_{i\in I})$, G'nin bir altgrup ailesi olsun. Her $i \neq j$ ve her $a_i \in A_i$ ve $a_j \in A_j$ için $a_i a_j = a_j a_i$ ve $\langle A_i : i \in I \setminus \{j\}\rangle \cap A_j = 1$ varsayımını yapalım. O zaman $(a_i)_i \mapsto \prod_i a_i$ kuralı bize $\oplus A_i$ grubuyla G'nin $\langle A_i : i \in I\rangle$ altgrubu arasında bir izomorfi verir.* □

10.86. $\langle a, b \mid a^2, b^3, (ab)^2\rangle$ grubunun

$$\{1, a, b, ab, b^2, ab^2\}$$

kümesinden ibaret olduğunu biliyoruz (bkz. Örnek 9.86). Bu grubun Sym 3 grubuna izomorf olduğunu kanıtlayın.

10.87. $\langle a, b \mid a^4, b^2, (ab)^2\rangle$ grubunun D_8 grubuna izomorf olduğunu kanıtlayın.

10.88. $n > 2$ bir doğal sayı olsun. $\langle a, b \mid a^n, b^2, (ab)^2\rangle$ grubunun D_{2n} grubuna izomorf olduğunu kanıtlayın.

10.89. $n > 2$ bir doğal sayı olsun. $\langle a, b \mid a^2, b^2, (ab)^n\rangle$ grubunun da D_{2n} grubuna izomorf olduğunu kanıtlayın.

10.90. *G bir grup olsun. $\mathbb{Z} \simeq A \lhd G$ olsun. Ayrıca $[G : A] = 2$ olsun. G grubu hakkında ne söyleyebiliriz?*

Yanıt: A grubu a elemanı tarafından üretilsin. $b \in G \setminus A$ olsun. Demek ki

$$G = \langle a, b\rangle = A \sqcup Ab$$

olur. A'nın indeksi 2 olduğundan, $b^2 \in A$ olur (bkz. sayfa 134). Dolayısıyla bir $n \in \mathbb{N}$ için $b^2 = a^n$ olur. n'nin tek ya da çift olması önemli olacak, bu yüzden,

$$n = 2m + e$$

olacak biçimde $m \in \mathbb{N}$ ve $e = 0, 1$ sayılarını seçelim. Demek ki

$$b^2 = a^2 a^e. \tag{1}$$

Ayrıca, b elemanı, $x \mapsto x^b$ kuralıyla A grubunun bir otomorfisine yol açar. Ama A'nın sadece iki otomorfisi vardır (Örnek 10.40); bunlardan biri özdeşlik fonksiyonu $x \mapsto x$, diğeri de $x \mapsto x^{-1}$ kuralıyla verilmiş tersini alma fonksiyonudur; bir başka deyişle

$$a^b = a^{\pm 1}$$

olur. İki durumu ayrı ayrı irdeleyelim.

Önce her $x \in A$ için $x^b = x$ durumunu ele alalım. Bu durumda G abel grubu olmak zorundadır. Dolayısıyla (1)'den dolayı,

$$(ba^{-1})^2 = a^e$$

olur. $ba^{-1} \in G \setminus A$ olduğundan, ta en başta seçtiğimiz b yerine ba^{-1} elemanını alıp

$$b^2 = a^e$$

varsayımını yapabiliriz. Şimdi iki ayrı altdurum var: $e = 0$ ya da $e = 1$. Birinci altdurumda $b^2 = 1$ olur. Bu durumda $B = \{1, b\}$ bir altgruptur ve elbette $\mathbb{Z}/2\mathbb{Z} \simeq B \leq G$ olur. Dolayısıyla, Teorem 10.5 ve Alıştırma 10.105'den dolayı

$$G = \langle a, b\rangle = \langle a\rangle\langle b\rangle = AB \simeq A \oplus B \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

olur. Bu izomorfide a elemanı $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ grubunun $(\pm 1, 0)$ elemanına (ikisinden birine) ve b elemanı $(0, \overline{1})$ elemanına tekabül etmektedir. Şimdi $e = 1$ altdurumunu ele alalım. Bu altdurumda $b^2 = a$ olduğundan,

$$G = \langle a, b\rangle = \langle b\rangle \simeq \mathbb{Z}$$

olur. Bu izomorfide b elemanı $\mathbb{Z}$'nin ± 1 elemanına tekabül eder ($\mathbb{Z}$'nin ± 1'den başka üreteci yoktur çünkü); a ise ± 2 elemanına ve A altgrubu $\mathbb{Z}$'nin $2\mathbb{Z}$ altgrubuna tekabül eder.

Şimdi her $x \in A$ için $x^b = x^{-1}$ durumunu ele alalım. Bu durumda,

$$a^n = b^2 = (b^2)^b = (a^n)^b = (a^n)^{-1} = a^{-n}$$

olduğundan, $a^n = 1$ olur. Demek ki $b^2 = 1$ olur. Bu son eşitlik grubun yapısını tamamen ortaya çıkarır:

$$G = \{a^n b^\epsilon : n \in \mathbb{Z},\ \epsilon = 0, 1\}$$

ve

$$ba = babb = b^{-1}abba^b b = a^{-1}b.$$

Bulduğumuz bu $ba = a^{-1}b$ (ya da $baba = 1$) eşitliği ve varsayımımız olan $b^2 = 1$ eşitliği, grubun $a^n b^\epsilon$ ve $a^m b^{\epsilon'}$ elemanlarını çarpmak için yeterlidir. Şu teoremi kanıtladık.

Teorem 10.8. *G bir grup olsun. G'nin $\mathbb{Z}$'ye izomorfik indeksi 2 olan bir altgrubu olduğunu varsayalım. O zaman $G \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $G \simeq \mathbb{Z}$ ya da $G = \langle a, b \mid b^2 = baba = 1\rangle$ olur. Her üç durumda da $\mathbb{Z}$'ye izomorf olan altgrup sırasıyla $\mathbb{Z} \oplus \{0\}$, $\mathbb{Z} = 2\mathbb{Z}$ ve $\langle a\rangle$ olur.* □

Alıştırmalar

10.91. $\mathbb{Z}$ ile $\mathbb{Z} \oplus \mathbb{Z}$ grubunun izomorfik olmadıklarını gösterin.

10.92. $\mathbb{Z}/4\mathbb{Z}$ ile $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}72\mathbb{Z}$ grubunun izomorfik olmadıklarını gösterin.

10.93. D_6 ile $\operatorname{Sym} 3$ gruplarının izomorfik olduklarını gösterin.

10.94. $\mathbb{Z}$'nin 0'dan farklı her altgrubunun $\mathbb{Z}$'ye izomorfik olduğunu gösterin.

10.95. $\mathbb{Q}$ grubunun $\mathbb{Q}$'ya izomorfik bir öz altgrubu olmadığını gösterin.

10.96. $\bigoplus_n \mathbb{Z}/n\mathbb{Z}$ ile $\prod_n \mathbb{Z}/n\mathbb{Z}$ gruplarının izomorfik olmadıklarını gösterin.

10.97. $n \geq 3$ için $\operatorname{Sym} n$'nin $\langle(1\ 2\ 3)\rangle$ altgrubunun $\mathbb{Z}/3\mathbb{Z}$'ye izomorf olduğunu gösterin.

10.98. $m \leq n$ için $\operatorname{Sym} n$'nin $\langle(1\ 2\ \ldots\ m)\rangle$ altgrubunun $\mathbb{Z}/m\mathbb{Z}$'ye izomorf olduğunu gösterin.

10.99. $6 \leq n$ için $\operatorname{Sym} n$'nin

$$\langle(1\ 2\ 3),\ (4\ 5\ 6)\rangle$$

altgrubunun $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$'ye izomorf olduğunu gösterin.

10.100. $9 \leq n$ için $\operatorname{Sym} n$'nin

$$\langle(1\ 2\ 3),\ (4\ 5\ 6),\ (7\ 8\ 9),\ (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)\rangle$$

altgrubunun 81 elemanlı olduğunu gösterin. Bu grubun abel olmadığını gösterin. Bu grubun 27 elemanlı bir abel altgrubunu bulun.

$\operatorname{Sym} 9$, $\operatorname{Sym} 10$ ve $\operatorname{Sym} 11$'e gelince. Bu gruplar 3^4 sayısına bölünürler ama 3^5 sayısına bölünmezler. Acaba 3^4 elemanlı bir altgrupları var mı? Evet var: böyle bir altgruptur. Bu altgrup diğerleri gibi abel grubu değildir.

$$\langle(1\ 2\ 3),\ (4\ 5\ 6),\ (7\ 8\ 9)\rangle$$

altgrubu $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ grubuna izomorftur ama sonuncu üreteç abelliği bozar.

10.101. $\varphi : G \longrightarrow G_1$ bir izomorfi olsun. $H \leq G$ olsun. $[G : H] = [G_1 : \varphi(H)]$ olduğunu kanıtlayın.

10.102. $\varphi_0 : G \longrightarrow H$ bir izomorfi olsun. G'den H'ye giden tüm izomorfilerin bir $\alpha \in \operatorname{Aut} H$ için $\alpha \circ \varphi_0$ şeklinde olduğunu kanıtlayın.

10.103. $\varphi_0 : G \longrightarrow H$ bir izomorfi olsun. G'den H'ye giden tüm izomorfilerin bir $\beta \in \operatorname{Aut} G$ için $\varphi_0 \circ \beta$ şeklinde olduğunu kanıtlayın.

10.104. Eğer $A \simeq A_1$ ve $B \simeq B_1$ ise $A \times B \simeq A_1 \times B_1$ olduğunu kanıtlayın.

10.105. İzomorfik grupların kartezyen çarpımlarının izomorfik olduğunu kanıtlayın, yani her i için $G_i \simeq H_i$ ise $\prod_i G_i \simeq \prod_i H_i$ olduğunu kanıtlayın. (Bkz. Örnek 10.12.)

10.106. $\operatorname{Aut} D_8$'in D_8'e izomorfik olduğunu gösterin.

10.107. G bir grup olsun. $\mathbb{Z}/3\mathbb{Z} \simeq H \overset{2}{\leq} G$ olsun. G'nin ya $\mathbb{Z}/6\mathbb{Z}$'ye ya da $\operatorname{Sym} 3$'e izomorf olduğunu kanıtlayın.

10.108. G bir grup, $p > 2$ bir asal olsun. $\mathbb{Z}/p\mathbb{Z} \simeq H \overset{2}{\leq} G$ olsun. G'nin $\mathbb{Z}/2p\mathbb{Z}$ ya da D_{2p} gruplarından birine izomorf olduğunu kanıtlayın.

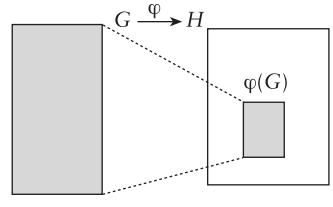
10.109. G bir grup olsun. $\mathbb{Z}/4\mathbb{Z} \simeq H \overset{2}{\leq} G$ olsun. G'nin $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, D_8 ve Q gruplarından birine izomorf olduğunu kanıtlayın.

10.110. G bir grup olsun. $\mathbb{Z}/8\mathbb{Z} \simeq H \overset{2}{\leq} G$ olsun. G'nin olası grup yapılarını sınıflandırın. (Bu aşamada biraz zordur. Sınıflandırma için $\operatorname{Aut}(\mathbb{Z}/8\mathbb{Z}) \simeq (\mathbb{Z}/8\mathbb{Z})^\star$ grubunun derecesi ≤ 2 olan elemanlarını bulmanız gerekir. Ama yetmez, daha fazlası gerekir.)

10.111. $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ olsun. $x, y, z \in \mathbb{Z}$ için $\overline{x} \in \mathbb{Z}/2\mathbb{Z}$, $\tilde{y} \in \mathbb{Z}/4\mathbb{Z}$, $\hat{z} \in \mathbb{Z}/8\mathbb{Z}$ yazacağız. $K = \langle(\overline{1}, \tilde{1}, \hat{1})\rangle \leq G$ olsun. $G/K \simeq G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ olduğunu gösterin. (Bkz Alıştırma 10.111.)

10.4 Çekirdek

G ve H iki grup ve $\varphi : G \longrightarrow H$ bir homomorfi olsun. φ'nin imgesinin, yani $\varphi(G)$'nin H'nin bir altgrubu olduğunu kanıtlamak kolay. Dolayısıyla H yerine $\varphi(G)$ alırsak, φ homomorfisinin örten olduğunu varsayabiliriz. Demek ki homomorfileri örten yapmak kolay, bunun için değer grubunu küçültmek yeterli.



Şimdi φ'nin birebirliğiyle ya da tam tersine ne kadar birebir olmadığıyla ilgilenelim.

$h \in H$ olsun. h'nin önimgesi $\varphi^{-1}(h)$ kümesini bulmak istiyoruz. Eğer h, φ'nin imgesinde değilse, yani $h \notin \varphi(G)$ ise, elbette $\varphi^{-1}(h) = \emptyset$ olur. Şimdi $h \in \varphi(G)$ varsayımını yapalım. Demek ki bir $g \in G$ için $\varphi(g) = h$. Böyle bir g sabitleyelim. h'nin φ-önimgesinden bir başka eleman alalım, diyelim x, yani $\varphi(x) = h$ eşitliği de sağlansın. x'in ne olabileceğini anlamaya çalışalım.

$$\varphi(x) = h = \varphi(g)$$

olduğundan,

$$\varphi(g^{-1}x) = 1$$

olur, yani

$$g^{-1}x \in \varphi^{-1}(1)$$

olur. $\varphi^{-1}(1)$ kümesi, aslında H'nin $\{1\}$ altgrubunun önimgesi olduğu için G'nin bir altgrubudur, nitekim $1 \in \varphi^{-1}(1)$ ve eğer $x, y \in f^{-1}(1)$ ise, $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = 1 \cdot 1 = 1$ ve $xy^{-1} \in f^{-1}(1)$ olur. Bu altgruba φ'nin ***çekirdeği*** adı verilir ve altgrup $\operatorname{Ker}\varphi$ olarak yazılır. Demek ki,

$$g^{-1}x \in \operatorname{Ker}\varphi.$$

Bu son koşul da elbette,

$$x \in g\operatorname{Ker}\varphi$$

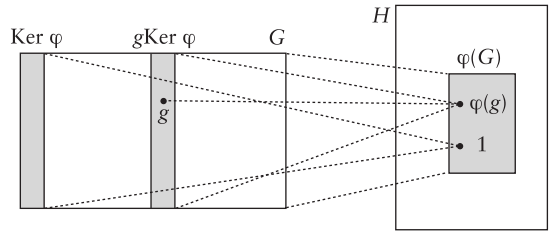
anlamına gelir. Şimdi ters istikametten gidelim, $x \in g\operatorname{Ker}\varphi$ varsayımını yapalım. O zaman bir $a \in \operatorname{Ker}\varphi$ için $x = ga$ olur. Bu eşitliğin iki tarafına φ uygularsak, $\varphi(a) = 1$ olduğundan,

$$\varphi(x) = \varphi(ga) = \varphi(g)\varphi(a) = \varphi(g)$$

elde ederiz. Böylece,

$$\{x \in G : \varphi(x) = \varphi(g)\} = g\operatorname{Ker}\varphi$$

eşitliğini bulmuş olduk. Öte yandan φ'nin birebir olması demek soldaki kümenin, dolayısıyla sağdaki kümenin de tek elemanlı olması demektir. Demek ki φ'nin birebir olmasıyla $\operatorname{Ker}\varphi = 1$ eşitliği eşdeğer önermelerdir[5].



$\operatorname{Ker}\varphi$ altgrubu, H-normal olduğunu bildiğimiz $\{1\}$ altgrubunun önimgesi olduğundan G-normaldir (bkz. Alıştırma 10.29). Aynı olguyu doğrudan da kanıtlayabiliriz: $x \in \operatorname{Ker}\varphi$ ve $g \in G$ olsun. O zaman

$$\varphi(g^{-1}xg) = \varphi(g^{-1})\varphi(x)\varphi(g) = \varphi(g^{-1})\varphi(g) = \varphi(g)^{-1}\varphi(g) = 1$$

olduğundan, $g^{-1}xg \in \operatorname{Ker}\varphi$, yani her $g \in G$ için $g^{-1}\operatorname{Ker}\varphi\, g \subseteq \operatorname{Ker}\varphi$ olur, ki bu da $\operatorname{Ker}\varphi$'nin normal olması demektir (bkz. sayfa 124).

Kanıtladıklarımızı teorem olarak yazalım.

[5]Bundan böyle $\{1\}$ altgrubu yerine gelenek olduğu üzere 1 yazacağız. Yazının gelişinden okur 1 ile elemanı mı yoksa altgrubu mu kastettiğimizi anlayacaktır.

Teorem 10.9. *$\varphi : G \longrightarrow H$ bir grup homomorfisi olsun. O zaman* $\operatorname{Ker}\varphi \lhd G$ *olur ve φ'nin birebir olması için yeter ve gerek koşul* $\operatorname{Ker}\varphi = 1$ *eşitliğidir.* □

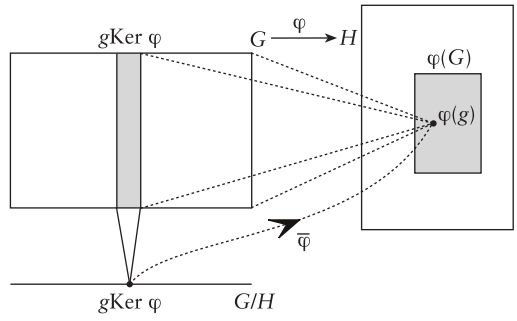
Teoremin ikinci önermesi pratikte çok işe yarar; gelecekte sık sık kullanacağız.

Eğer $\varphi : G \longrightarrow H$ birebir bir homomorfiyse, φ'ye bazen ***gömme*** adı verilir. Eğer G'den H'ye giden bir gömme varsa, G'nin H'nin içine ***gömüldüğü*** söylenir. Bu durumda bazen $G \hookrightarrow H$ ya da daha açık olmak isteniyorsa $G \overset{\varphi}{\hookrightarrow} H$ yazılır.

Şimdi biraz geriye gidelim ve biraz önce kanıtladığımız

$$\{x \in G : \varphi(x) = \varphi(g)\} = g \operatorname{Ker}\varphi$$

eşitliğini gözden geçirelim. $g\operatorname{Ker}\varphi$ kümesinin tüm elemanlarının φ-imgesi birbirine eşit (hepsi $\varphi(g)$'ye eşit) ve birebirliği bozan da $\operatorname{Ker}\varphi$'nin 1'den fazla elemanı olması. Demek ki eğer $g\operatorname{Ker}\varphi$ ötelemelerini tek bir eleman yaparsak φ birebir bir fonksiyona dönüşür. Ama $G/\operatorname{Ker}\varphi$ grubunda $g\operatorname{Ker}\varphi$ ötelemesi tek bir eleman, $\overline{g}$ olarak yazdığımız tek bir eleman.



$G/\operatorname{Ker}\varphi$ ibaresi eksik xxx

Yukarıdaki resimden takip edelim. $\overline{g} \in G/\operatorname{Ker}\varphi$ için,

$$\overline{\varphi}(\overline{g}) = \varphi(g)$$

tanımını yapalım. Bu, gerçekten bir tanımdır çünkü, $\overline{g} = \overline{g_1}$ ise $g \in g_1 \operatorname{Ker}\varphi$ ve dolayısıyla $\varphi(g) = \varphi(g_1)$ olur. Böylece bir

$$\overline{\varphi} : G/\operatorname{Ker}\varphi \longrightarrow H$$

fonksiyonunu elde ederiz. Bu fonksiyon bir grup homomorfisidir, nitekim, her $\overline{g}$, $g_1 \in G/\operatorname{Ker}\varphi$ için

$$\overline{\varphi}(\overline{g}\,\overline{g_1}) = \overline{\varphi}(\overline{gg_1}) = \varphi(gg_1) = \varphi(g)\varphi(g_1) = \overline{\varphi}(\overline{g})\overline{\varphi}(\overline{g_1}) = \overline{\varphi}(\overline{g})\overline{\varphi}(\overline{g_1})$$

olur. Ayrıca φ birebirdir, çünkü

$$\operatorname{Ker}\overline{\varphi} = \{\overline{x} : \overline{\varphi}(\overline{x}) = 1\} = \{\overline{x} : \varphi(x) = 1\} = \{\overline{x} : x \in \operatorname{Ker}\varphi\} = \{\overline{1}\}$$

ve çekirdeği tek elemanlı olduğundan $\overline{f}$ birebir; nitekim $\overline{\varphi}$'nin birebir olması için elimizden geleni yaptık: φ'nin birebirliğini bozan elemanları $G/\operatorname{Ker}\varphi$ grubunda tek bir eleman olarak gördük.

Sonuç olarak $\overline{\varphi}$ fonksiyonu $G/\operatorname{Ker}\varphi$ ile $\varphi(G)$ arasında bir izomorfi oldu.

Şimdi yukarda yaptığımızı biraz genelleştirmeye çalışalım. $\overline{\varphi}$ fonksiyonunu $G/\operatorname{Ker}\varphi$ grubunda tanımladık, ama dikkat ederseniz $\overline{\varphi}$ fonksiyonunu tanımlamak için G grubunu illa $\operatorname{Ker}\varphi$ normal altgrubuna bölmek zorunda olmadığımızı görürsünüz; $\operatorname{Ker}\varphi$ altgrubundan daha küçük bir G-normal altgrup da işimizi görebilirdi. Nitekim, $K \leq \operatorname{Ker}\varphi$ bir G-normal altgrup ise $\overline{x} \in G/K$ için,

$$\overline{\varphi}(\overline{x}) = f(x)$$

kuralı bize bir

$$\overline{\varphi} : G/K \longrightarrow H$$

tanımlar, gerçekten de eğer G/K grubunda $\overline{x} = \overline{x_1}$ ise, $x_1x^{-1} \in K \leq \operatorname{Ker}\varphi$, dolayısıyla $1 = \varphi(x_1x^{-1}) = \varphi(x_1)\varphi(x^{-1}) = \varphi(x_1)\varphi(x)^{-1}$ ve $\varphi(x_1) = \varphi(x)$ olur; demek ki $\overline{\varphi}$ iyitanımlı. Tanımladığımız bu $\overline{\varphi} : G/K \longrightarrow H$ fonksiyonunun ne kadar birebir olduğunu ölçebiliriz:

$$\begin{aligned} \operatorname{Ker}\overline{\varphi} &= \{\overline{x} \in G/K : \overline{\varphi}(\overline{x}) = 1\} = \{\overline{x} \in G/K : f(x) = 1\} \\ &= \{\overline{x} \in G/K : x \in \operatorname{Ker}\varphi\} = \operatorname{Ker}\varphi/K. \end{aligned}$$

Bütün bunları teorem olarak yazalım, önemlidir çünkü:

Teorem 10.10. *$\varphi : G \longrightarrow H$ bir homomorfi ve $K \leq \operatorname{Ker}\varphi$ bir G-normal altgrup olsun. O zaman $\overline{x} \in G/K$ için*

$$\overline{\varphi}(\overline{x}) = \varphi(x)$$

formülüyle tanımlanmış $\overline{\varphi} : G/K \longrightarrow H$ fonksiyonu bir homomorfidir ve

$$\operatorname{Ker}\overline{\varphi} = \operatorname{Ker}\varphi/K$$

olur. Bunun özel bir durumu olarak, $K = \operatorname{Ker}\varphi$ alırsak, $\overline{\varphi} : G/\operatorname{Ker}\varphi \longrightarrow \varphi(G)$ bir izomorfi olur. Sonuç olarak

$$G/\operatorname{Ker}\varphi \simeq \varphi(H)$$

izomorfisini elde ederiz. □

Notlar ve Örnekler

10.112. G bir grup, A bir abel grubu ve $\varphi : G \longrightarrow A$ bir homomorfi olsun. O zaman $G' \leq \operatorname{Ker}\varphi$ olur. Nitekim her $x,\ y \in G$ için, A abel olduğundan,

$$\varphi([x,y]) = \varphi(x^{-1}y^{-1}xy) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y) = \varphi(x)^{-1}\varphi(x)\varphi(y)^{-1}\varphi(y) = 1$$

olur.

10.113. G bir grup ve $A,\ B \leq G$ olsun. $B \leq N_G(A)$ olsun, yani her $b \in B$ için $A^b = A$ olsun. (Bu durumda, B, A'yı ***normalize*** eder denir.) O zaman $\langle A, B\rangle = AB$ olduğunu biliyoruz (bkz. Önsav 5.3). $A \lhd AB$ olduğunu kanıtlamak kolay, çünkü $a \in A,\ b \in B$ için $A^{ab} = A^b = A$ olur. Demek ki AB/A grubundan sözedebiliriz. $\varphi(a) = \overline{a}$ eşitliğiyle tanımlanan $\varphi : B \longrightarrow AB/A$ fonksiyonunu ele alalım. Bu fonksiyon elbette örten bir homomorfidir. Çekirdeğini bulalım:

$$\operatorname{Ker}\varphi = \{b \in B : \varphi(b) = \overline{1}\} = \{b \in B : \overline{b} = \overline{1}\} = \{b \in B : b \in A\} = A \cap B.$$

Yukarıdaki teoreme göre, bundan,

$$AB/A \simeq B/(A \cap B)$$

çıkar. Bu izomorfi bir teorem olmayı hakeder.

Teorem 10.11. *G bir grup ve $A,\ B \leq G$ olsun. Eğer B, A'yı normalize ediyorsa, $A \lhd AB$ ve $AB/A \simeq B/(A \cap B)$ olur.*

10.114. Yukarıdaki teoremin bir uygulamasını görelim. Eğer A ve B altgrupları ayrıca bir p asalı için sonlu p-altgruplarsa (yani eleman sayısı p'nin bir kuvvetiyse ya da elemanları p-elemansa), o zaman AB de bir p-altgrup olur, çünkü bir önceki teoreme göre,

$$|AB| = |A||B|/|A \cap B|$$

olur ve eşitliğin sağındaki üç sayı da p'nin kuvvetleridir.

10.115. Yukarıdaki sonucun sonsuz p-altgruplar için de geçerli olduğu biraz zahmetle gösterilebilir:

Teorem 10.12. *G bir grup ve $A,\ B \leq G$ olsun. Eğer B, A'yı normalize ediyorsa ve A ve B birer p-altgrupsa (yani elemanları p-elemanlarsa), o zaman $\langle A, B\rangle = AB$ de bir p-altgrubu olur. Dolayısıyla maksimal bir p-altgrup normalse, bu altgrup grubun tüm p-elemanlarını içerir.*

Kanıt: $\langle A, B\rangle = AB$ eşitliğini biliyoruz. Şimdi $a \in A,\ b \in B$ olsun. ab'nin bir p-eleman olduğunu kanıtlayacağız. $(ab)^k$ elemanını hesaplayalım. Bir $a_k \in A$ için

$$(ab)^k = a_k b^k$$

eşitliğini kanıtlayalım. $k = 0,\ 1$ için eşitlik bariz. $(ab)^k = a_k b^k$ eşitliğini varsayalım. O zaman

$$(ab)^{k+1} = (ab)^k(ab) = a_k b^k ab = a_k b^k a b^{-k} b^{k+1} = a_k a^{b^{-k}} b^{k+1}$$

olur. $a_{k+1} = a_k a^{b^{-k}} \in A$ olduğundan istediğimiz kanıtlanır. Demek ki $\deg b = p^k$ ise,

$$(ab)^{p^k} = a' b^{p^k} = a' \in A$$

olur. Eğer $\deg a' = p^\ell$ ise,

$$(ab)^{p^{k+\ell}} = ((ab)^{p^k})^{p^\ell} = a'^{p^\ell} = 1$$

olur. İkinci önerme birincinin doğrudan bir sonucudur. □

10.116. p bir asal olsun. H, G'nin maksimal bir p-altgrubu olsun. Eğer G sonluysa, maksimal p-altgrup elbette vardır. Eğer G sonsuzsa, maksimal p-altgrubun varlığı Zorn Önsavı sayesinde gösterilebilir (bkz.Alıştırma 529). Eğer $H \lhd G$ ise, Teorem 10.12'e göre, H, G'nin tüm p-elemanlarından oluşan kümedir, dolayısıyla G'nin biricik maksimal p-altgrubudur ve G'nin tüm p-altgruplarını kapsar.

10.117. G bir grup ve $(H_i)_i$ bir normal altgrup ailesi olsun. $\pi_i : G \longrightarrow G/H_i$ doğal izdüşüm fonksiyonu olsun. $(\pi_i)_i : G \longrightarrow \prod_i G/H_i$ bu homomorfilerin çarpımı olsun, yani her $g \in G$ için

$$(\pi_i)_i(g) = (\pi_i(g))_i$$

olarak tanımlansım (bkz. Örnek 10.15).

$$\operatorname{Ker}(\pi_i)_i = \bigcap_i H_i$$

olur. Dolayısıyla $(\pi_i)_i$ homomorfisinin birebir olması için $\bigcap_i H_i = 1$ eşitliği yeter ve gerek koşuldur.

Bunun özel bir durumu olarak $G = \mathbb{Z}$, $I = \mathbb{N}$ ve $H_n = n\mathbb{Z}$ alalım. Böylece $\mathbb{Z}$ grubunu $\prod_n \mathbb{Z}/n\mathbb{Z}$ grubuna gömebiliriz.

Bir başka özel durum: $G = \mathbb{Z}$, $I = \mathbb{N}$, $p > 1$ bir doğal sayı olsun. (Genelde p bir asal olur.) Bu örnekte açıklanan yöntemle $\mathbb{Z}$ grubunu $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ grubuna gömebiliriz.

10.118. $H \lhd G$ olsun. O zaman G'nin her g elemanı $x \mapsto x^g$ kuralıyla H'nin bir otomorfisini doğurur. H'nin bu otomorfisine φ_g diyelim. Kolaylıkla $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_1}$ eşitliği kanıtlanabilir. Demek ki $\varphi(g) = \varphi_g$ kuralıyla tanımlanmış $\varphi : G \longrightarrow \operatorname{Aut} H$ fonksiyonu bir homomorfidir. Bu homomorfinin çekirdeği,

$$\operatorname{Ker}\varphi = \{g \in G : \overline{g} = \mathrm{Id}_H\} = \{g \in G : \text{her } x \in H \text{ için } x^g = x\} = C_G(H)$$

olur.

10.119. Yukarıdaki örneği genelleştirebiliriz. G herhangi bir grup ve H, $K \leq G$ olsun. $K \leq N_G(H)$ varsayımını yapalım. O zaman $k \in K$ ve $h \in H$ için $\varphi_k(h) = khk^{-1}$ kuralıyla tanımlanmış φ_k fonksiyonu H'den gene H'ye giden bir otomorfidir. Ayrıca $\varphi_k \circ \varphi_{k'} = \varphi_{kk'}$ olur; yani $\varphi(k) = \varphi_k$ kuralı bize bir $\varphi : K \longrightarrow \operatorname{Aut} H$ homomorfisi verir. Çekirdeğini bulmak zor değil: $\operatorname{Ker}\varphi = C_K(H)$ olur.

10.120. *$A = \oplus_I \mathbb{Z}$ ve $n > 0$ bir doğal sayı olsun. $A/nA \simeq \oplus_I \mathbb{Z}/n\mathbb{Z}$ olur.*

Kanıt: A grubundan $\oplus_I \mathbb{Z}/n\mathbb{Z}$ grubuna giden

$$(a_i)_i \mapsto (\overline{a_i})_i$$

kuralıyla tanımlanmış doğal φ homomorfisine bakalım. φ elbette örtendir. Eğer $(a_i)_i \in \operatorname{Ker}\varphi$ ise, her $i \in I$ için $a_i \in n\mathbb{Z}$ olur; bir $b_i = a_i/n \in \mathbb{Z}$ olsun; o zaman $a_i = nb_i$ ve $(a_i)_i = n(b_i)_i \in nA$ olur. Demek ki $\operatorname{Ker}\varphi \leq nA$. Ters içindelik bariz. □

10.121. p bir asal olsun. Eğer bir grup burulmalıysa ve derecesi p olan bir elemanı yoksa, o zaman grubun p-bölünebilir olduğunu gösterelim. Gruptan bir a elemanı alalım. $x^p = a$ denkleminin grupta çözümü olduğunu göstereceğiz. $H = \langle a \rangle$ sonlu grubundan yine kendisine giden $x \mapsto x^p$ fonksiyonuna bakalım. H abel grubu olduğundan bu bir homomorfidir. Grupta derecesi p olan bir eleman olmadığından bu fonksiyon birebirdir (bkz. Sonuç 4.7). H sonlu olduğundan bu fonksiyon ayrıca örtendir. Demek ki bir x için $x^p = a$ olur.

Teorem 10.13. *Derecesi p olan elemanı bulunmayan burulmalı gruplar p-bölünebilir gruplardır.* □

10.122. Bu örnekte aşağıdaki teoremi kanıtlayacağız.

Teorem 10.14. *Sonlu bir grubun eleman sayısı p asalına bölünmüyorsa grup p-bölünebilirdir.*

Kanıt: G grup, $g \in G$ olsun. Lagrange Teoremi'ne (Sonuç 8.5) göre $H = \langle g \rangle$ abel grubunun eleman sayısı p'ye bölünmez ve Sonuç 8.6'ya göre H grubunun derecesi p olan bir elemanı yoktur. Demek ki H'den H'ye giden $x \mapsto x^p$ kuralıyla tanımlanmış homomorfinin çekirdeği 1'dir, dolayısıyla bu homomorfi birebirdir (Sonuç 4.7). Ama H sonlu olduğundan bundan homomorfinin örten olduğu çıkar. Demek ki bir $x \in H \leq G$ için $x^p = g$ olur. □

10.123. G bir grup, $H \leq G$, $g \in G \setminus H$, p bir asal olsun. $g^p \in H$, $|H| < \infty$ ve $|H|$'nin p'ye asal olduğu varsayımlarını yapalım. gH ötelemesinde derecesi p olan bir eleman bulacağız. Elbette $g^p \in C_H(g)$, hatta $g^p \in Z(C_H(g))$. (Bundan emin olun.) $C_H(g)$ sonlu bir grup olduğundan ve eleman sayısı p'ye bölünmediğinden, p-bölünebilir bir altgruptur (Teorem 10.14). Demek ki bir $c \in C_H(g) \leq H$ için $c^p = g^p$ olur. Ama $cg = gc$ olduğundan $(gc^{-1})^p = 1$ olur. $g \notin H$ olduğundan $gc^{-1} \neq 1$ ve bundan de $\deg gc^{-1} = p$ çıkar.

10.124. **Cauchy Teoremi.** Eleman sayısı p asalına bölünen sonlu bir grubun derecesi p olan bir elemanı olduğunu daha önce (örnek olarak) Teorem 4.11'da kanıtlamıştık. Bu paragrafta aynı teoremin daha uzun ve daha standart bir kanıtını vereceğiz. Okurun bu kanıtı tüm ayrıntılarıyla anlaması önemlidir; böylece bu ana kadar edindiği teorik birçok bilginin uygulamasını görecektir.

Teorem 10.15 (Cauchy Teoremi)**.** *Eleman sayısı p asalına bölünen sonlu bir grubun derecesi p olan bir elemanı vardır.* □

Kanıt: Grubuza G diyelim. $|G| = n$ olsun. Teoremi n üzerine tümevarımla kanıtlayacağız. Dolayısıyla eğer G'nin bir özaltgrubunun eleman sayısı p'ye bölünüyorsa, o zaman tümevarımla bu özaltgrubun derecesi p olan bir elemanı olduğuna hükmederiz ve bu durumda kanıt biter. Dolayısıyla bundan böyle G'nin özaltgruplarının eleman sayısının p'ye bölünmediğini varsayabiliriz.
$g \in G$ olsun. g'nin G'deki merkezleyicisi olarak tanımlanan

$$C_G(g) = \{c \in G : cg = gc\}$$

altgrubunu anımsatırız.

$$G/C_G(g) = \{C_G(g)x : x \in G\}$$

sol ötelemeler kümesiyle g^G eşleniklik sınıfı arasında

$$f(C_G(H)x) = g^x$$

kuralıyla verilmiş bir eşleme vardır. (Kanıt: Eğer $C_G(g)x = C_G(g)y$ ise $xy^{-1} \in C_G(g)$ olduğundan, $g^{xy^{-1}} = g$ ve dolayısıyla $g^x = g^y$ olur, dolayısıyla f fonksiyonu iyi tanımlıdır. Bu adımların geriye dönüşü olduğundan f ayrıca birebirdir; örtenlik bariz. Bkz. Örnek 8.33.) Demek ki

$$|g^G| = |G/C_G(g)| = |G|/|C_G(g)|$$

olur. Eğer $g \notin Z(G)$ ise $C_G(g) < G$ olur, ve p asalı $C_G(g)$'nin eleman sayısını bölmediğinden, p asalı g^G eşleniklik sınıfının eleman sayısını böler.
Öte yandan g^G eşleniklik sınıfları ya birbirine eşittir ya da ayrıktır. (Kanıt: Eğer $g^x = h^y$ ise her z için $g^z = (h^{yx^{-1}})^z = h^{yx^{-1}z} \in h^G$ olur. Ters içindelik de benzer şekilde kanıtlanır. Bkz. Alıştırma 1.26.) Sadece 1 elamanı olan g^G eşleniklik sınıfları $Z(G)$'nin elemanlarının eşleniklik sınıflarıdır; 1'den fazla elemanı olanların eleman sayısı da p'ye bölünür. Böylece

$$G = Z(G) \sqcup \bigsqcup_{Z(G)\text{'de olmayan bazı } g\text{'ler için}} g^G$$

olur. p en soldaki ve en sağdaki kümelerin eleman sayısını böldüğünden, buradan p'nin $|Z(G)|$ sayısını da böldüğü çıkar. Dolayısıyla $Z(G)$, G'nin bir özaltgrubu olamaz, yani $Z(G) = G$ olmalı. Demek ki G bir abel grubu olmak zorundadır.

$1 < A < G$ olsun. A'nın eleman sayısı p'ye bölünmediğinden G/A grubunun eleman sayısı p'ye bölünür. Tümevarımla G/A grubunun derecesi p olan bir elemanı olduğunu buluruz. Bu elemana $\overline{g}$ diyelim. Demek ki $g \notin A$ ama $g^p \in A$. Öte yandan Teorem 10.14'e göre A'nın elemanları p-bölünebilir. Böylece bir $a \in A$ için $g^p = a^p$ olur ve buradan da $(ga^{-1})^p = 1$ çıkar çünkü G artık bir abel grubu. Demek ki $\deg(ga^{-1}) = 1$, p. Ama derece 1 olsaydı, $g = a \in A$ olurdu, çelişki. □

10.125. $H \leq G$ olsun. $X = G/H = \{xH : x \in G\}$ olsun (sol ötelemeler kümesi). Eğer $g \in G$ ise,

$$\varphi_g(xH) = gxH$$

kuralı bize bir $\varphi_g : X \longrightarrow X$ fonksiyonu verir. Bu fonksiyonun birebir ve örten olduğunu kanıtlamak zor değildir. Demek ki $\varphi_g \in \operatorname{Sym} X$. Böylece

$$\varphi(g) = \varphi_g$$

kuralıyla tanımlanmış $\varphi : G \longrightarrow \operatorname{Sym} X$ fonksiyonunu elde ettik. Bu fonksiyon aslında bir homomorfidir çünkü her g_1, $g_2 \in G$ ve $xH \in X$ için,

$$\varphi(g_1g_2)(xH) = (g_1g_2)xH = g_1(g_2(xH)) = (\varphi(g_1) \circ \varphi(g_2))(xH),$$

dolayısıyla

$$\varphi(g_1g_2) = \varphi(g_1) \circ \varphi(g_2)$$

olur. Şimdi φ'nin çekirdeğini bulalım:

$$\begin{aligned}
\operatorname{Ker}\varphi &= \{g \in G : \varphi_g = \mathrm{Id}_X\} = \{g \in G : \text{ her } x \in G \text{ için } gxH = xH\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } gxH = xH\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } x^{-1}gx \in H\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } g \in xHx^{-1}\} \\
&= \bigcap H^x.
\end{aligned}$$

Örnek 9.12'de $\operatorname{Core}_G H = \bigcap H^x$ tanımını yapmıştık (H'nin G'deki göbeği, H'nin en büyük G-normal altgrubu). Demek ki, $G/\operatorname{Core}_G H$ grubundan $\operatorname{Sym} G/H$ grubuna giden birebir bir homomorfizma var. Buradan da şu teorem çıkar:

Teorem 10.16. *Eğer $[G : H] = n$ ise $[G : \operatorname{Core}_G H]$ sayısı $n!$ sayısını böler.* □

10.126. Yukarıdaki teoremin (Örnek 9.5'yı genelleştiren) şaşırtıcı bir uygulaması vardır:

Sonuç 10.17. *Eğer p asalı bir grubun eleman sayısını bölen en küçük asalsa, o zaman grubun endisi p olan her altgrubu normaldir.*

Kanıt: Gruba G, altgruba H diyelim. $[G : H] = p$ olsun. Bir önceki teoreme göre $[G : \operatorname{Core}_G H]$ sayısı $p!$ sayısını böler. Ama $[G : \operatorname{Core}_G H]$ sayısı $|G|$'yi de böler. Önermenin hipotezine göre $[G : \operatorname{Core}_G H] = 1$ ya da p olmak zorundadır. $\operatorname{Core}_G H \leq H \leq G$ olduğundan $\operatorname{Core}_G H = H$ (bkz. Örnek 8.20) ve $H \lhd G$ olur. □

10.127. Asal sayıda elemanı olan bir grubun döngüsel, dolayısıyla bir abel grubu olduğunu biliyoruz (Teorem 10.4). Derecesi bir asalın karesi olan gruplar da abel gruplarıdır:

Sonuç 10.18. *p bir asal olsun. Eğer $|G| = p^2$ ise G bir abel grubudur.*

Birinci Kanıt: Eğer $Z(G) = p^2$ ise $Z(G) = G$ ve G abel olamak zorunda.
Eğer $|Z(G)| = p$ ise, $|G/Z(G)| = p$ olur. Dolayısıyla Teorem 10.4'e göre $G/Z(G)$ döngüseldir ve Örnek 9.66'ya göre G bir abel grubu olur.
Şimdi $Z(G) = 1$ olsun. $1 \neq a \in G$ olsun. Eğer $A = \langle a \rangle = G$ ise, G bir abel grubudur, çelişki. Demek ki A'nın eleman sayısı p'dir, dolayısıyla endisi $p^2/p = p$ olur. Sonuç 10.17'e göre $A \lhd G$ olur. Bir $b \in G \setminus A$ alalım. Aynen A ile olduğu gibi $B = \langle b \rangle \lhd G$ olur ve p tane elemanı vardır. $A = B$ olamayacağından, $A \cap B = 1$ olur (bkz. Örnek 8.15).

Bütün bunlardan $G = \langle A, B\rangle = AB$ çıkar (Örnek 9.8). Ama daha da önemlisi, Örnek 9.9'dan $x \in A$ ve $y \in B$ için $xy = yx$ çıkar, yani $G = AB$ bir abel grubudur (Teorem 10.5). □

İkinci Kanıt: Teorem 8.10'a göre $Z(G) \neq 1$ olur. Dolayısıyla $G/Z(G)$ grubunun 1 ya da p elemanı vardır. Dolayısıyla Teorem 10.4'e göre $G/Z(G)$ döngüseldir ve Örnek 9.66'e göre G bir abel grubu olur. □

10.128. p^2 elemanlı bir grup ya $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ grubuna ya da $\mathbb{Z}/p^2\mathbb{Z}$ grubuna izomorftur. Bunun artık kolay olan kanıtını okura bırakıyoruz.

10.129. $A \subseteq G$ bir altküme ve $X = \{A^x : x \in G\}$ olsun. Eğer $g \in G$ ise ve $B \in X$ ise $\tilde{g}(B) = B^g$ tanımını yapalım. $\tilde{g} \in \operatorname{Sym} X$ olduğunu kanıtlayın. $\gamma \mapsto \tilde{g}$ fonksiyonunun G'den $\operatorname{Sym} X$'e giden bir homomorfi olduğunu kanıtlayın. Eğer $|X| = n$ ise, bundan G'nin,

$$[G : N] | n!,$$
$$N \lhd G,$$
$$N \leq \{x \in G : A^x = A\} \leq G$$

özelliklerini sağlayan bir N altgrubunun varlığını kanıtlayın. Eğer $A \leq G$ ise, $|X| = |G/N_G(A)|$ eşitliği yararlı olabilir.

Alıştırmalar

10.130. $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ ve $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ olsun.

$$\varphi : G \longrightarrow H$$

fonksiyonu şöyle tanımlansın:

$$\varphi(\overline{x}, \tilde{y}, \hat{z}) = (\overline{x+y}, \widetilde{z-y}).$$

Burada x, y, $z \in \mathbb{Z}$ ve $\overline{x} \in \mathbb{Z}/2\mathbb{Z}$, $\tilde{y} \in \mathbb{Z}/4\mathbb{Z}$, $\hat{z} \in \mathbb{Z}/8\mathbb{Z}$.

a. φ fonksiyonunun iyi tanımlı olduğunu gösterin.
b. φ fonksiyonunun bir homomorfi olduğunu gösterin.
c. φ fonksiyonunun örten olduğunu gösterin.
d. $(\overline{1}, \tilde{1}, \hat{1}) \in \operatorname{Ker}\varphi$ olduğunu gösterin.
e. $K = \langle(\overline{1}, \tilde{1}, \hat{1})\rangle \leq G$ olsun.
f. $|K| = 8$ olduğunu gösterin.
g. $G/K \simeq H$ olduğunu gösterin.

10.5 $\mathbb{Z}$, Yeniden

Bu yaptıklarımızın önemli bir uygulamasını görelim. $n, m > 0$ iki tamsayı olsun. Eğer $x \in \mathbb{Z}$ ise, $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ ve $\tilde{x} \in \mathbb{Z}/m\mathbb{Z}$ tahmin edilen modüler sayıları simgelesin. $\varphi(x) = (\overline{x}, \tilde{x})$ formülüyle tanımlanmış $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ homomorfisini ele alalım (bkz. Örnek 10.14). Bu homomorfizmanın çekirdeğini bulalım: Eğer $e = \text{ekok}(n, m)$ ise,

$$\begin{aligned}\operatorname{Ker}\varphi &= \{x \in \mathbb{Z} : \varphi(x) = 0\} = \{x \in \mathbb{Z} : \overline{x} = \overline{0} \text{ ve } \tilde{x} = \tilde{0}\} \\ &= \{x \in \mathbb{Z} : x \in n\mathbb{Z} \cap m\mathbb{Z}\} = n\mathbb{Z} \cap m\mathbb{Z} = e\mathbb{Z}\end{aligned}$$

olur. Böylece, eğer $x \in \mathbb{Z}$ için $\hat{x} \in \mathbb{Z}/e\mathbb{Z}$ malum elemanı simgeliyorsa,

$$\overline{\varphi}(\hat{x}) = (\overline{x}, \tilde{x})$$

kuralı bize birebir bir

$$\mathbb{Z}/e\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

homomorfisini verir.

Bunun özel durumu olarak $(n, m) = 1$ alalım. O zaman $e = nm$ olur. Bu örnekten

$$\overline{\varphi}(\hat{x}) = (\overline{x}, \tilde{x})$$

kuralıyla tanımlanmış

$$\mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

birebir bir grup homomorfisini elde ederiz. Eleman sayıları aynı ($= nm$) olduğundan homomorfi aynı zamanda örtendir, yani bir izomorfidir. Elde ettiğimiz teoremi yazalım.

Teorem 10.19. *n ve m birbirine asal iki doğal sayı olsun. O zaman*

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

olur. Ayrıca,

$$\overline{\varphi}(\hat{x}) = (\overline{x}, \tilde{x})$$

formülüyle (doğal olarak) tanımlanmış $\mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ fonksiyonu bir izomomorfidir. □

Sonuç 10.20. *Birbirine asal sayıda elemanı olan iki döngüsel grubun kartezyen çarpımı da döngüseldir.* □

Sonuç 10.21. *$n > 1$ doğal sayısını asallarına ayıralım: $n = p_1^{k_1} \cdots p_r^{k_r}$. Bu durumda*

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{k_r}\mathbb{Z}$$

olur. □

Sonuç 10.22 (Çin Kalan Teoremi)**.** *Eğer $n_1, \ldots, n_r$ birbirine ikişer ikişer asal doğal sayılarsa ve $a_1, \ldots, a_r$ tamsayılarsa,*

$$(x \equiv a_i \mod n_i)_{i=1,\ldots,r}$$

denklem sisteminin bir çözümü vardır ve iki çözümün farkı $n_1 \cdots n_r$ sayısına bölünür.

Kanıt: $n = n_1 \cdots n_r$ olsun.

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

izomorfisini biliyoruz. $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ elemanı, bu izomorfizma altında sağ taraftaki $(\overline{a_1}, \ldots, \overline{a_r})$ elemanına tekabül etsin. $x = a$ sistemin bir çözümüdür. İki çözümün farkı elbette n'ye bölünecektir. □

Teorem 4.10'u bir kez daha kanıtlayabiliriz:

Sonuç 10.23. *Bir grupta her burulmalı eleman, asal p sayıları için birbirleriyle değişen p-elemanların çarpımıdır.*

Kanıt: G bir grup ve $g \in G$ derecesi n olan bir eleman olsun. Teoremi $\langle g \rangle$ altgrubunda kanıtlamak yeterli. Ama $\langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ olduğundan teoremi $\mathbb{Z}/n\mathbb{Z}$ grubunda kanıtlamak yeterli. Bu da Sonuç 10.21 tarafından verilmiştir. □

Notlar ve Örnekler

10.131. G bir grup olsun. $g, x \in G$ için $\mathrm{Inn}_g(x) = gxg^{-1}$ tanımının bize iç otomorfi denen bir $\mathrm{Inn}_g : G \longrightarrow G$ otomorfisi verdiğini gördük (bkz sayfa 154). Ayrıca $\mathrm{Inn}(g) = \mathrm{Inn}_g$ kuralıyla tanımlanan $\mathrm{Inn} : G \longrightarrow \mathrm{Aut}\, G$ fonksiyonunun bir grup homomorfisi olduğunu da biliyoruz. Inn homorfisinin çekirdeğini bulalım:

$$\begin{aligned} \mathrm{Ker}\,\mathrm{Inn} &= \{g \in G : \mathrm{Inn}_g = \mathrm{Id}_G\} \\ &= \{g \in G : \text{her } x \in G \text{ için } \mathrm{Inn}_g(x) = x\} \\ &= \{g \in G : \text{her } x \in G \text{ için } gxg^{-1} = x\} = Z(G). \end{aligned}$$

Demek ki

$$G/Z(G) \simeq \mathrm{Inn}(G).$$

10.132. Örnek 10.81'de aynı (sonlu) sayıda elemanı olan tüm döngüsel grupların izomorfik olduğu söylenmiş ve okurdan bunu kanıtlaması istenmişti. Bu kanıt aslında şu şekilde yapılmalı: n elemanlı döngüsel gruba G diyelim. O zaman grup, bir $x \in G$ için, $G = \{1, x, x^2, \ldots, x^{n-1}\}$ biçimindedir. Her $r, s \in \mathbb{Z}$ için $x^r x^s = x^{r+s}$ olduğundan, $\varphi(r) = x^r$ fonksiyonu $\mathbb{Z}$ grubundan bu guruba giden örten bir homomorfidir. Bu homomorfinin çekirdeğini bulalım:

$$\mathrm{Ker}\,\varphi = \{r \in \mathbb{Z} : \varphi(r) = 1\} = \{r \in \mathbb{Z} : x^r = 1\} = \{r \in \mathbb{Z} : n|r\} = n\mathbb{Z}.$$

Dolayısıyla $G \simeq \mathbb{Z}/n\mathbb{Z}$ olur.

Çarpma. Şimdi biraz da çarpmayla ilgilenelim. $\mathbb{Z}/n\mathbb{Z}$ kümesi üzerinde bir toplama işlemi tanımladık. Toplamayı $\overline{x} + \overline{y} = \overline{x+y}$ eşitliğiyle tanımladık. Bu toplama tanımı geçerli çünkü gördüğümüz ve kanıtlaması kolay olduğu üzere $\overline{x} = \overline{x_1}$ ve $\overline{y} = \overline{y_1}$ ise $\overline{x+y} = \overline{x_1+y_1}$ olur. Benzer tanımı çarpma için de yapabiliriz, çünkü $\overline{x} = \overline{x_1}$ ve $\overline{y} = \overline{y_1}$ ise $\overline{xy} = \overline{x_1 y_1}$ olur; nitekim eğer n sayısı $x - x_1$ ve $y - y_1$ sayısını bölüyorsa, o zaman

$$xy - x_1 y_1 = x(y - y_1) + (x - x_1)y_1$$

eşitliğinden dolayı n sayısı $xy - x_1 y_1$ sayısını da böler. Demek ki artık $\mathbb{Z}/n\mathbb{Z}$ kümesinde toplama dışında bir de

$$\overline{x}\,\overline{y} = \overline{xy}$$

eşitliğiyle tanımlanmış çarpma işlemimiz var. Aslında çarpma işlemi toplama işleminden çok çok farklı değil, nasıl, doğal sayılarda xy, x'i kendisiyle y defa toplamak ya da y'yi kendisiyle x defa toplamak anlamına geliyorsa, $\mathbb{Z}/n\mathbb{Z}$ kümesinde de

$$\overline{x}\,\overline{y} = x \cdot \overline{y} = y \cdot \overline{x}$$

eşitliği geçerlidir. Buradan, $\mathbb{Z}$'den $\mathbb{Z}/n\mathbb{Z}$'ye giden

$$x \mapsto \overline{x}$$

formülüyle tanımlanmış doğal fonksiyonun sadece toplamaya değil, çarpmaya da dağıldığı anlaşılır.

Çarpmanın bir de etkisiz elemanı vardır: $\overline{1}$. Nitekim her $x \in \mathbb{Z}$ için $\overline{x}\,\overline{1} = \overline{x1} = \overline{x}$ olur.

Şimdi şu tanımı yapalım:

$$(\mathbb{Z}/n\mathbb{Z})^\star = \{\alpha \in \mathbb{Z}/n\mathbb{Z} : \text{ bir } \beta \in \mathbb{Z}/n\mathbb{Z} \text{ için } \alpha\beta = \overline{1}\}.$$

Bu kümenin elemanlarına ***tersinir elemanlar*** denir. Tersinir elemanlar kümesi $(\mathbb{Z}/n\mathbb{Z})^\star$ bir gruptur. Nitekim α, α_1 elemanları tersinirse, o zaman $\alpha\alpha_1$ elemanı da tersinirdir çünkü eğer $\alpha\beta = \overline{1}$ ve $\alpha_1\beta_1 = \overline{1}$ ise $(\alpha\beta)(\beta_1\overline{a}_1) = \overline{1}$ olur; ayrıca $\overline{1}$ tersinirdir (tersi gene kendisidir) ve $(\mathbb{Z}/n\mathbb{Z})^\star$ kümesinin her elemanının (kümenin tanımı gereği) bir tersi vardır ve tersi gene $(\mathbb{Z}/n\mathbb{Z})^\star$ kümesindedir (çünkü α'nın tersi β ise, β'nın tersi elbette α'dır).

Notlar ve Örnekler

10.133. $(\mathbb{Z}/2\mathbb{Z})^\star = \{\overline{1}\}$.

10.134. $(\mathbb{Z}/3\mathbb{Z})^\star = \{\overline{1}, \overline{2}\}$.

10.135. $(\mathbb{Z}/4\mathbb{Z})^\star = \{\overline{1}, \overline{3}\}$.

10.136. $(\mathbb{Z}/5\mathbb{Z})^\star = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

10.137. $(\mathbb{Z}/6\mathbb{Z})^\star = \{\overline{1}, \overline{5}\}$.

10.138. $(\mathbb{Z}/8\mathbb{Z})^\star = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

10.139. $(\mathbb{Z}/9\mathbb{Z})^\star = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$.

10.140. Bu örnekte aşağıdaki teoremi kanıtlayacağız:

Teorem 10.24. *$\mathbb{Q}$'nün sonlu sayıda elemanı tarafından üretilen altgrupları ya 0'dır ya da $\mathbb{Z}$'ye izomorftur.*

Kanıt: Üreteçlerden en az biri 0 olmasın. Atgrubun $\mathbb{Z}$'ye izomorf olduğunu göstermeliyiz. Elemanlara $q_1, \ldots, q_n$ diyelim. a_i, $b_i \in \mathbb{Z}$ olmak üzere

$$q_i = \frac{a_i}{b_i}$$

yazalım.

$$b = \text{ekok}(b_1, \ldots b_n)$$

olsun. $c_i = b/b_i \in \mathbb{Z}$ ise,

$$q_i = \frac{a_i}{b_i} = \frac{c_i a_i}{b}$$

olur. Dolayısıyla

$$b_1 = \ldots = b_n = b$$

varsayımını yapabiliriz. O zaman

$$\langle q_1, \ldots, q_n \rangle = \left\langle \frac{a_1}{b}, \ldots, \frac{a_n}{b} \right\rangle = \frac{1}{b} \langle a_1, \ldots, a_n \rangle$$

olur. $\langle a_1, \ldots, a_n \rangle \leq \mathbb{Z}$ olduğundan, bir $a \in \mathbb{Z}$ için $a\mathbb{Z}$ grubuna eşittir. Demek ki grup a/b tarafından üretilmiştir.

$(\mathbb{Z}/n\mathbb{Z})^\star$ grubunun elemanlarını bulmak zor değildir:

Teorem 10.25. $(\mathbb{Z}/n\mathbb{Z})^\star = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} : \text{ebob}(x,n) = 1\}$ *olur.*

Kanıt: Eğer $\text{ebob}(x,n) = 1$ ise, Teorem 2.5'e göre $nu + xv = 1$ eşitliğini sağlayan u ve v tamsayıları vardır. Bu eşitliği $\mathbb{Z}/n\mathbb{Z}$ grubuna indirgersek,

$$\overline{1} = \overline{nu + xv} = \overline{nu} + \overline{xv} = \overline{xv} = \overline{x}\,\overline{v}$$

olur; dolayısıyla $\overline{x}$ tersinirdir.

Şimdi $\overline{x}$ elemanının tersinir olduğunu varsayalım. Demek ki bir $\overline{y}$ için $\overline{x}\,\overline{y} = \overline{1}$ olur, yani $xy - 1 \in n\mathbb{Z}$ olur. Demek ki bir $z \in \mathbb{Z}$ için $xy - 1 = nz$, yani $xy + n(-z) = 1$. Gene Teorem 2.5'e göre n ve x sayıları aralarında asaldır. □

Notlar ve Örnekler

10.141. p bir asal olsun. $k \in \mathbb{Z}$ için $\varphi(k) = \overline{1 + kp} \in (\mathbb{Z}/p^2\mathbb{Z})^\star$ olsun.

$$\varphi(k)f(\ell) = \overline{(1+kp)(1+\ell p)} = \overline{1 + (k+\ell)p} = \phi(k+\ell)$$

olduğundan, $\varphi : \mathbb{Z} \longrightarrow (\mathbb{Z}/p^2\mathbb{Z})^\star$ grubuna giden bir homomorfidir (toplamayı çarpmaya dönüştürür). Çekirdeği hesaplayalım:

$$\text{Ker}\,\varphi = \{k \in \mathbb{Z} : p|k\} = p\mathbb{Z}.$$

İmgesi de kolay:

$$\varphi(\mathbb{Z}) = \overline{1} + p\mathbb{Z}/p^2\mathbb{Z} \leq (\mathbb{Z}/p^2\mathbb{Z})^\star.$$

Demek ki

$$\mathbb{Z}/p\mathbb{Z} \simeq \overline{1} + p\mathbb{Z}/p^2\mathbb{Z}$$

olur.

10.142. p bir asal ve n bir doğal sayı olsun. Her $k = 1, \ldots, n-1, n$ için

$$U_k = \overline{1} + p^k\mathbb{Z}/p^n\mathbb{Z}$$

olsun. U_k kümesi çarpma altında kapalı olduğundan $U_k \leq (\mathbb{Z}/p^n\mathbb{Z})^\star$ olur (bkz Teorem 5.1). U_k altgrubunun p^{n-k} tane elemanı vardır ve

$$\overline{1} = U_n < U_{n-1} < \ldots < U_{k+1} < U_k < \ldots < U_1 = \overline{1} + p\mathbb{Z}/p^n\mathbb{Z}$$

olur. Dolayısıyla

$$U_k/U_{k+1} \simeq \mathbb{Z}/p\mathbb{Z}$$

ve her $x \in U_1$ için $x^{p^{n-1}} = \overline{1}$ olur. Ayrıca,

$$U_k \setminus U_{k+1} = 1 + p^k(\mathbb{Z}/p^k\mathbb{Z})^\star$$

eşitliğini göstermek zor değil. Buradan kolaylıkla şu kanıtlanır: Eğer $p > 2$ ve $1 + p^k x \in U_k \setminus U_{k+1}$ ise $(1 + p^k x)^p \in U_{k+1} \setminus U_{k+2}$ olur. Demek ki $\deg \overline{1+p} = p^{n-1}$ ve dolayısıyla

$$U_1 = \langle \overline{1+p} \rangle \simeq \mathbb{Z}/p^{n-1}\mathbb{Z}$$

ve her k için

$$U_k = \langle \overline{(1+p)}^k \rangle \simeq \mathbb{Z}/p^{n-k}\mathbb{Z}$$

olur.

$p = 2$ için U_k gruplarının yapısı biraz daha farklıdır. Bu yapıyı keşfetmeyi okura alıştırma olarak bırakıyoruz.

Alıştırmalar

10.143. $\mathbb{Q}$ grubunun $1/3$ ve $2/7$ tarafından üretilen altgrubunu bulun.

10.144. $\mathbb{Q}$ grubunun $2/5$, $4/7$ ve $6/13$ elemanları tarafından üretilen altgrubunu bulun.

10.145. $\mathbb{Z}/6\mathbb{Z}$'de $x^2 + x$ polinomunun kaç kökü vardır?

10.146. $\mathbb{Z}/8\mathbb{Z}$'de $x^2 - 1$ polinomunun kaç kökü vardır?

10.147. Eğer $p > 2$ asalsa $\mathbb{Z}/p\mathbb{Z}$'de $x^2 - 1$ polinomunun iki kökü olduğunu kanıtlayın.

10.148. $n = 2, \ldots, 16$ için $(\mathbb{Z}/n\mathbb{Z})^\star$ gruplarından döngüsel olanlarını bulun ve her biri için grubu üreten bir eleman bulun. (Bu sonuncu soru ancak elemanları teker teker deneyerek yapılabilir.)

10.149. $(\mathbb{Z}/8\mathbb{Z})^\star$ grubunun döngüsel olmadığını ama $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ grubuna izomorfik olduğunu kanıtlayın.

10.150. $(\mathbb{Z}/16\mathbb{Z})^\star$ ve $(\mathbb{Z}/24\mathbb{Z})^\star$ grupları nasıl gruplardır?

10.151. $\text{ebob}(n, m) = 1$ ise,

$$(\mathbb{Z}/nm\mathbb{Z})^\star \simeq (\mathbb{Z}/n\mathbb{Z})^\star \times (\mathbb{Z}/m\mathbb{Z})^\star$$

olduğunu kanıtlamaya çalışın. Bu aşamada bu alıştırma kolay olmayabilir ama bir ipucu verelim: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ kümesi üzerinde doğal bir çarpma işlemi tanımlayıp Teorem 10.19'yi kullanın. Halkalar kuramı aşamasına geldiğimizde bu konuyu dikkatlice işleyeceğiz.

11. Bölüm Grubu Üzerine Daha Fazla

Bu bölümde soyut cebirin en önemli konusuyla tanışacağız.

11.1 Bölüm Gruplarının Altgrupları

G bir grup ve $H \lhd G$ olsun. G/H grubu G ve H tarafından belirleniyor, dolayısıyla G/H grubunun tüm özellikleri aslında G ve H gruplarını özelliklerdir. Bu bölümde amacımız G/H grubunun altgruplarını G ve H cinsinden belirlemek.

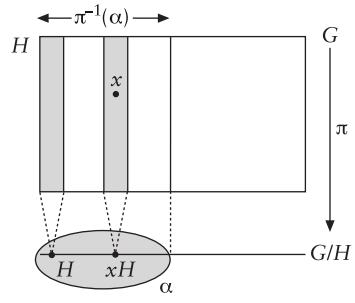
G/H yerine $\overline{G}$ yazalım. Eğer $g \in G$ ise, $\overline{G}$ grubunun gH elemanı yerine alışılageldiği üzere $\overline{g}$ yazacağız. $\pi : G \longrightarrow \overline{G}$ de doğal izdüşüm homomorfizması olsun:

$$\pi(g) = \overline{g}.$$

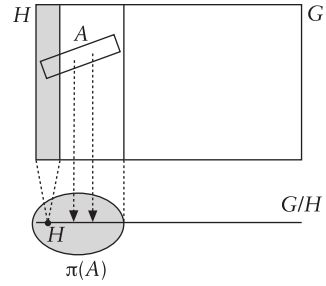
$\alpha \leq \overline{G}$ bir altgrup olsun. O zaman $\pi^{-1}(\alpha) \leq G$ olur çünkü bir altgrubun bir homomorfi altında önimgesi de bir altgruptur. Ayrıca $H = \pi^{-1}(1) \leq \pi^{-1}(\alpha)$ olur. Demek ki

$$\alpha \mapsto \pi^{-1}(\alpha)$$

kuralı $\overline{G}$ grubunun altgrupları kümesinden G'nin (H'yi içeren) altgrupları kümesine giden bir fonksiyon tanımlar. Bu fonksiyonu da π^{-1} olarak gösterelim.



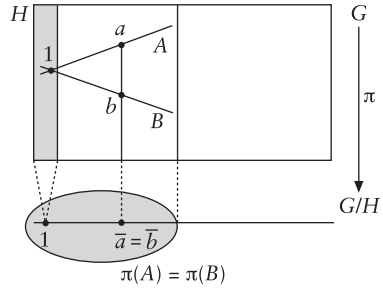
Şimdi G'nin herhangi bir A altgrubunun π-imgesini, yani $\overline{G}$ grubundaki izdüşümünü alalım: $\pi(A)$. Elbette $\pi(A) \leq \overline{G}$ olur. Bu sefer $A \mapsto \pi(A)$ kuralı G'nin altgrupları kümesinden $\overline{G}$ grubunun altgrupları kümesine giden bir fonksiyon tanımlar. Bu fonksiyonu da π olarak gösterelim.



Böylece G'nin altgrupları kümesiyle, G/H'nin altgrupları kümesi arasında biri soldan sağa, diğeri sağdan sola giden iki fonksiyon elde ettik: π ve π^{-1}. Bakalım bunlar ne kadar birbirinin tersi. Elbette $\overline{G}$ grubunun her α altgrubu için

$$\pi(\pi^{-1}(\alpha)) = \alpha$$

olur, yani $\pi \circ \pi^{-1} = \mathrm{Id}$ olur. Demek ki π örten ve π^{-1} birebir. Ama $\pi^{-1} \circ \pi = \mathrm{Id}$ eşitliği doğru olmayabilir, çünkü mesela π birebir olmayabilir, ne de olsa H'nin **her** altgrubunun izdüşümü (mesela 1 ve H altgruplarının izdüşümü) $\overline{G}$ grubunun $\{\overline{1}\}$ altgrubudur ve H'nin birçok altgrubu olabilir; demek ki $H = 1$ olmadıkça π birebir olamaz ve π^{-1} fonksiyonunun tersi olması beklenemez.



Ayrıca π^{-1} fonksiyonu örten olmayabilir, çünkü $\alpha \leq \overline{G}$ ise o zaman $\pi^{-1}(\alpha) \geq H$ olur, ama G'nin her altgrubu H'yi içermek zorunda değildir, mesela 1 altgrubu genellikle H'yi içermez, demek ki $H \neq 1$ ise π^{-1} örten olamaz. Madem π^{-1} fonksiyonu örten değil, bu fonksiyonun imgesini bulalım ve π'yi bu imgeye kısıtlayalım, belki bu kısıtlamayla $\pi^{-1} \circ \pi = \mathrm{Id}$ eşitliği doğru olur. $\pi^{-1}(G)$ fonksiyonunun imgesini bulmak için, π örten olduğundan, $A \leq G$ için G'nin $\pi^{-1}(\pi(A))$ altgrubunu bulmak yeterli.

Sav: *Eğer $A \subseteq G$ ise $\pi^{-1}(\pi(A)) = HA$ olur.*

Kanıt: $x \in \pi^{-1}(\pi(A))$ olsun. O zaman $\pi(x) \in \pi(A)$ olur. Demek ki bir $a \in A$ için $\pi(x) = \pi(a)$, yani $\overline{x} = \overline{a}$, yani $a^{-1}x \in H$ olur. Demek ki $x \in Ha \subseteq HA$. Ters istikameti kanıtlamak daha da kolay $\pi(HA) = \pi(H)\pi(A) = \overline{1} \cdot \pi(A) = \pi(A)$ olduğundan, $HA \subseteq \pi^{-1}(\pi(A))$ olur. □

Bu arada $A \leq G$ olduğunda, $HA \leq G$ olduğunu da anımsayalım (Alıştırma 9.18).

Yukarıdaki savdan, eğer $H \leq A \leq G$ ise, $\pi^{-1}(\pi(A)) = HA = A$ çıkar. Yani eğer π fonksiyonunu H'yi içeren altgruplar kümesine kısıtlarsak, $\pi^{-1} \circ \pi = \mathrm{Id}$ olur. Bu önemli sonucu teorem olarak yazalım.

Teorem 11.1. *$H \lhd G$ olsun.*

$$\pi : \textit{G'nin H'yi içeren altgrupları kümesi} \longrightarrow \textit{G/H'nin altgrupları kümesi}$$

ve

$$\pi^{-1} : \textit{G/H'nin altgrupları kümesi} \longrightarrow \textit{G'nin H'yi içeren altgrupları kümesi}$$

fonksiyonları birbirinin tersidir. Yani G/H'nin her altgrubu, G'nin H'yi içeren bir ve bir tek altgrubunun π-imgesidir. Ayrıca eğer $A \leq G$ ise,

$$\pi^{-1}(\pi(A)) = HA$$

olur. Ayrıca yukarıdaki π ve π^{-1} fonksiyonları, G'nin H'yi içeren normal altgrupları ve G/H'nin normal altgrupları arasında bir eşleme verir.

Kanıt: Sadece son kısmı kanıtlamamız lazım. Son kısım da Alıştırma 10.29 ve 10.30'dan çıkar. □

Notlar ve Örnekler

11.1. *$A \lhd G$ ve $A \leq B \leq G$ olsun. $\overline{G} = G/A$ ve $\overline{B} = B/A$ tanımlarını yapalım. O zaman $N_G(B)/A = N_{\overline{G}}(\overline{B})$ olur.*
Kanıt: $N_G(B)/A \leq N_{\overline{G}}(\overline{B})$ içindeliğinin doğru olduğu bariz. Diğer içindeliği kanıtlayalım. $\overline{g} \in N_{\overline{G}}(\overline{B})$ olsun. O zaman $B^gA/A = \overline{B}^{\overline{g}} = \overline{B} = B/A$ olur. (İlk eşitlikten emin olun.) Demek ki Teorem 11.1'e göre $B^gA = B$ ama $A = A^g \leq B^g$ ve dolayısıyla $B^gA = B^g$. Buradan $B^g = B^gA = B$ ve $g \in N_G(B)$ çıkar. □

11.2. G sonlu bir p-grup olsun.
$$1 = A_0 < A_1 < \ldots < A_n$$
ve $A_{i+1}/A_i \simeq \mathbb{Z}/p\mathbb{Z}$ özelliklerini sağlayan G-normal altgruplar olduğunu kanıtlayın. (İpucu: Teorem 8.10 ve tümevarım.)

11.3. G sonlu bir p-grubu ve $H \leq G$ olsun.
$$H = A_0 \lhd A_1 \lhd \ldots \lhd A_n$$
ve $A_{i+1}/A_i \simeq \mathbb{Z}/p\mathbb{Z}$ özelliklerini sağlayan altgruplar olduğunu kanıtlayın.

11.4. Teorem 11.1'i kullanarak, n bir doğal sayı olmak üzere, $\mathbb{Z}/n\mathbb{Z}$ grubunun altgruplarını bulalım. Teoremde $G = \mathbb{Z}$, $H = n\mathbb{Z}$ alırsak, bunlar, $n\mathbb{Z} \leq A \leq \mathbb{Z}$ için, $A/n\mathbb{Z}$ biçimindedir. Tabii A, bir $m > 0$ için $m\mathbb{Z}$ biçiminde olmalıdır; ayrıca $n\mathbb{Z} \leq A = m\mathbb{Z}$ olması gerektiğinden, m sayısı n'yi bölmelidir. Demek ki, $\mathbb{Z}/n\mathbb{Z}$ grubunun altgrupları, n'yi bölen bir m sayısı için $m\mathbb{Z}/n\mathbb{Z}$ biçimindedir[1]. Ama $m\mathbb{Z}$, m tarafından üretildiğinden, $m\mathbb{Z}/n\mathbb{Z}$ grubu da m'nin imgesi tarafından üretilir, yani döngüseldir (Örnek 9.57). Tüm döngüsel gruplar bir n doğal sayısı için $\mathbb{Z}/n\mathbb{Z}$'ye izomorf olduklarından (Teorem 10.3), bundan, daha önce Teorem 7.2 olarak kanıtladığımız şu teorem çıkar:

Teorem 11.2. *Döngüsel bir grubun altgrupları da döngüseldir.* □

11.5. m doğal sayısı n doğal sayısını bölsün ve $d = n/m$ olsun. Bir önceki örneğe göre $m\mathbb{Z}/n\mathbb{Z} \leq \mathbb{Z}/n\mathbb{Z}$ olur. $m\mathbb{Z}/n\mathbb{Z}$ grubunun yapısını bulalım. $\overline{m}$ tarafından üretildiğinden $m\mathbb{Z}/n\mathbb{Z}$ grubu döngüseldir. Elemanları da belli:

$$\overline{0},\ \overline{m},\ 2\overline{m},\ \ldots,\ (d-1)\overline{m};$$

ya da

$$\overline{0},\ \overline{m},\ \overline{2m},\ \ldots,\ \overline{(d-1)m}.$$

Bu elemanların herbiri diğerinden farklı olduğundan tam tamına d tane eleman bulmuş olduk. Demek ki $m\mathbb{Z}/n\mathbb{Z}$ grubu döngüsel ve d tane elemanı var. Dolayısıyla $\mathbb{Z}/d\mathbb{Z}$ grubuna izomorfik olmalıdır (Teorem 10.3).

Teorem 11.3. *Eğer $m|n$ ise $m\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/(n/m)\mathbb{Z}$ olur.* □

Bu teoremin daha üst düzey ve daha şık bir kanıtını verelim.

Kanıt: $n = md$ olsun. Şu doğal homomorfileri takip edelim:

$$\mathbb{Z} \longrightarrow m\mathbb{Z} \longrightarrow m\mathbb{Z}/n\mathbb{Z}.$$

Bu homomorfiye φ diyelim. Tanım gereği $\varphi(x) = \overline{mx}$. Elbette φ örtendir. Çekirdeğini hesaplayalım:

$$\begin{aligned} \operatorname{Ker}\varphi &= \{x \in \mathbb{Z} : \varphi(x) = \overline{0}\} = \{x \in \mathbb{Z} : \overline{mx} = \overline{0}\} \\ &= \{x \in \mathbb{Z} : n|mx\} = \{x \in \mathbb{Z} : d|x\} = d\mathbb{Z}. \end{aligned}$$

Demek ki, Teorem 10.10'a göre, $\mathbb{Z}/d\mathbb{Z} \simeq m\mathbb{Z}/n\mathbb{Z}$ olur. □

11.6. Bir sonraki doğal soru şu: Eğer m sayısı n'yi bölmüyorsa, $m \cdot \mathbb{Z}/n\mathbb{Z}$ grubunun yapısı nedir? Teorem 11.2'ye göre bu grubun döngüsel olduğunu biliyoruz. Ayrıca Lagrange teoremine göre (Teorem 8.5), grubun eleman sayısı n'yi böler. Demek ki bir $d|n$ için, $m \cdot \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$. Amacımız d'yi n ve m cinsinden bulmak.

$d = \text{ebob}(n, m)$ alabileceğimizi görelim. $m = dm_1$ ve $n = dn_1$ olarak yazalım. $(m_1, n) = 1$ olduğundan, Teorem 10.25'e göre $\overline{m_1}$ elemanı $\mathbb{Z}/n\mathbb{Z}$'de tersinir olur. Demek ki

$$m_1 \cdot \mathbb{Z}/n\mathbb{Z} = \overline{m_1} \cdot \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$$

olur. Ayrıca d, n'yi böldüğünden, bir önceki teoreme göre,

$$m \cdot \mathbb{Z}/n\mathbb{Z} = dm_1 \cdot \mathbb{Z}/n\mathbb{Z} = d \cdot \mathbb{Z}/n\mathbb{Z} = d\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z}$$

olur. Şu teoremi kanıtladık:

[1] Dikkat: $m \cdot \mathbb{Z}/n\mathbb{Z}$ ile $m\mathbb{Z}/n\mathbb{Z}$ arasında (tanım itibariyle) bir ayrım gözetilmelidir. Birinci grup $m \cdot \mathbb{Z}/n\mathbb{Z} = \{m\overline{x} : \overline{x} \in \mathbb{Z}/n\mathbb{Z}\}$ anlamına gelir ama ikinci grup $m\mathbb{Z}/n\mathbb{Z} = (m\mathbb{Z})/(n\mathbb{Z}) = \{\overline{y} : y \in m\mathbb{Z}\} = \{\overline{mx} : x \in \mathbb{Z}\}$ anlamına gelir. Neyse ki $m\overline{x} = \overline{mx}$ olduğundan kümeler birbirine eşittir. Öte yandan eğer m, n'yi bölmezse $m\mathbb{Z}/n\mathbb{Z}$ yazılımı pek hoş karşılanmaz, çünkü grup teoride G/H yazıldığında H'nin G'nin altgrubu olduğu varsayımı yapılır. Mesela $n = 4$, $m = 3$ ise $3 \cdot \mathbb{Z}/4\mathbb{Z} = (-1) \cdot \mathbb{Z}/4\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}$ olur. Ama $4\mathbb{Z} \not\subseteq 3\mathbb{Z}$ olduğundan $3\mathbb{Z}/4\mathbb{Z}$ yazılmaz.

Teorem 11.4. *$d = \text{ebob}(n, m)$ olsun. O zaman*

$$m \cdot \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/(n/d)\mathbb{Z}$$

olur. □

Bu teoremin de daha şık bir kanıtını verelim.

Kanıt: $n = dn_1$ ve $m = dm_1$ olsun. Aşağıdaki homomorfileri takip edelim:

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow m \cdot \mathbb{Z}/n\mathbb{Z}.$$

Bu homomorfilerin bileşkesine φ diyelim. φ örten bir homomorfidir. Çekirdeğini hesaplayalım:

$$\begin{array}{rcl} \text{Ker}\,\varphi & = & \{x \in \mathbb{Z} : \varphi(x) = \overline{0}\} = \{x \in \mathbb{Z} : m\overline{x} = \overline{0}\} = \{x \in \mathbb{Z} : \overline{mx} = \overline{0}\} \\ & = & \{x \in \mathbb{Z} : n|mx\} = \{x \in \mathbb{Z} : n_1|m_1x\} = \{x \in \mathbb{Z} : n_1|x\} = n_1\mathbb{Z}. \end{array}$$

Demek ki, Teorem 10.10'a göre, $\mathbb{Z}/n_1\mathbb{Z} \simeq m \cdot \mathbb{Z}/n\mathbb{Z}$ olur. □

11.7. $m|n$ olsun. Demek ki $m\mathbb{Z}/n\mathbb{Z} \leq \mathbb{Z}/n\mathbb{Z}$. Dolayısıyla $(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z})$ bölüm grubu vardır. Bu grubun grup yapısını bulalım. $\mathbb{Z}/n\mathbb{Z}$ döngüsel olduğundan $(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z})$ grubu da döngüseldir (bkz. Örnek 9.57). Ayrıca Teorem 11.3'e göre

$$|(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z})| = |\mathbb{Z}/n\mathbb{Z}|/|m\mathbb{Z}/n\mathbb{Z}| = n/(n/m) = m$$

olur. Demek ki

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z}$$

olmalıdır.

Şu teoremi kanıtladık:

Teorem 11.5. *$m|n$ ise*

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z}$$

olur.

Bu teoremin de daha şık bir kanıtını verelim.

Kanıt: Aşağıdaki homomorfileri takip edelim:

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow (\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}).$$

Bileşkeye φ diyelim. Bileşkesini aldığımız homomorfiler örten olduğundan φ de örtendir. φ'nin çekirdeğini hesaplayacağız. Ama önce notasyonumuzu sabitleyelim. $x \in \mathbb{Z}$ için $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ gösterimi, x'in $\mathbb{Z}/n\mathbb{Z}$ grubu üzerine tahmin edilen doğal izdüşümünü simgeleyecek. Ayrıca, $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ için, $\hat{\overline{x}} \in (\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z})$ gösterimi, $\overline{x}$ elemanının $(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z})$ grubu üzerine tahmin edilen doğal izdüşümünü simgeleyecek. Demek ki her $x \in \mathbb{Z}$ için

$$\varphi(x) = \hat{\overline{x}}.$$

$m\mathbb{Z} \leq \text{Ker}\,\varphi$ içindeliği bariz çünkü her $x \in \mathbb{Z}$ için

$$\varphi(mx) = \hat{\overline{mx}} = \hat{\overline{mx}} = \hat{\overline{0}}$$

olur. Diğer içindeliği kanıtlayalım:

$$\begin{array}{rcl} \text{Ker}\,\varphi & = & \{x \in \mathbb{Z} : \hat{\overline{x}} = \hat{\overline{0}}\} = \{x \in \mathbb{Z} : \overline{x} \in m\mathbb{Z}/n\mathbb{Z}\} \\ & = & \{x \in \mathbb{Z} : \text{ bir } y \in \mathbb{Z} \text{ için } \overline{x} = \overline{my}\} \\ & = & \{x \in \mathbb{Z} : \text{ bir } y \in \mathbb{Z} \text{ için } n|(x - my)\} \\ & \subseteq & \{x \in \mathbb{Z} : m|x\} = m\mathbb{Z}. \end{array}$$

Demek ki $\text{Ker}\,\varphi = m\mathbb{Z}$ ve Teorem 10.10'a göre, $\mathbb{Z}/m\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z})$ olur. □

Birazdan bu teoremdeki anafikri sömürüp çok daha genel bir teorem kanıtlayacağız. (Bkz. Teorem 11.6.)

11.2 Bölüm Gruplarının Bölüm Grupları

G bir grup ve $H \lhd G$ olsun. G/H'nin bir normal altgrubunu alalım. Teorem 11.1'e göre bu normal altgrup, bir $H \leq K \lhd G$ için K/H biçimindedir. Dolayısıyla G/H grubunu K/H grubuna bölüp, $(G/H)/(K/H)$ grubunu bulabiliriz. Okurun içinden gereken sadeleştirmeyi yapıp (!)

$$(G/H)/(K/H) \simeq G/K$$

yazmak geçiyorsa, okur kendini içgüdülerine bırakısın yanılmayacaktır:

Teorem 11.6. *$H \lhd G$ olsun. $H \leq K \lhd G$ olsun. Bu durumda $K/H \lhd G/H$ olduğunu biliyoruz.*

$$(G/H)/(K/H) \simeq G/K$$

olur ve bu iki grup arasında $\tilde{x} \in G/K$ elemanının $\hat{\overline{x}} \in (G/H)/(K/H)$ elemanına götüren doğal bir izomorfi vardır.

Kanıt: Önce notasyon konusunda anlaşalım: Eğer $x \in G$ ise $\tilde{x} \in G/K$ elemanı x'in G/K grubundaki doğal izdüşümünü, $\overline{x} \in G/K$ elemanı x'in G/H grubundaki doğal izdüşümünü ve $\alpha \in G/H$ ise, $\hat{\alpha} \in (G/H)/(K/H)$ elemanı α'nın $(G/H)/(G/K)$ grubundaki doğal izdüşümünü temsil edecek. Şimdi $G \longrightarrow G/H \longrightarrow (G/H)/(K/H)$ doğal homomorfilerini izleyelim: $x \in G$ elemanı önce $\overline{x} \in G/H$ elemanına gider, ardından da ikinci homomorfiyi takip ederek $\hat{\overline{x}}$ elemanına gider. Bu iki homomorfinin bileşkesine φ diyelim. Demek ki

$$\varphi(x) = \hat{\overline{x}}.$$

Bu homomorfilerin bileşimi bir homomorfidir. Ayrıca bileşkesi alınan homomorfiler örten olduğundan φ de örtendir. φ'nin çekirdeğini hesaplamak farz oldu:

$$\begin{aligned}
\operatorname{Ker}\varphi &= \{x \in G : \varphi(x) = \hat{\overline{1}}\} \\
&= \{x \in G : \hat{\overline{x}} = \hat{\overline{1}}\} \\
&= \{x \in G : \overline{x} \in K/H\} \\
&= \{x \in G : \text{ öyle bir } y \in K \text{ var ki } \overline{x} = \overline{y} \text{ olur}\} \\
&= \{x \in G : \text{ öyle bir } y \in K \text{ var ki } xy^{-1} \in H \text{ olur}\} \\
&= \{x \in G : \text{ öyle bir } y \in K \text{ var ki } x \in Hy \text{ olur}\} \\
&= \{x \in G : x \in HK\} \\
&= \{x \in G : x \in K\} = K
\end{aligned}$$

Teorem 10.10'a göre, $G/K \simeq \operatorname{Im}\varphi = (G/H)/(K/H)$ olur. □

Kanıtımızın aynen Teorem 11.5'in kanıtı gibi olduğuna dikkatinizi çekerim.

Notlar ve Örnekler

11.8. $\mathbb{Q}/\mathbb{Z}$ elbette $\mathbb{R}/\mathbb{Z}$'nin bir altgrubu. Yukarıdaki teoreme göre $(\mathbb{R}/\mathbb{Z})/(\mathbb{Q}/\mathbb{Z}) \simeq \mathbb{R}/\mathbb{Q}$ olur.

11.9. Aşağıdaki teorem, tümevarıma izin verdiğinden, sonlu p-grupların analizinde çok önemli olabilir.

Teorem 11.7. *p bir asal ve G sonlu bir p-grubu olsun. O zaman G'nin $A_{i+1}/A_i \simeq \mathbb{Z}/p\mathbb{Z}$ önermesini sağlayan*

$$A_0 = 1 < A_1 < \ldots < A_n = G$$

normal altgrupları vardır.

Kanıt: Teorem 8.10'a ya da 14.6'ya göre $Z(G) \neq 1$ olur. Cauchy Teoremi'ne göre $Z(G)$'de derecesi p olan bir eleman vardır. Bu elemanla üretilmiş grup elbette p elemanlıdır, dolayısıyla $\mathbb{Z}/p\mathbb{Z}$ grubuna izomorftur, ve merkezde olduğundan G-normaldir. Bu altgruba A_1 diyelim. $|G|$ üzerine tümevarımla, G/A_1 grubunun istenen özelliği sağlayan normal altgrupları vardır. Teorem 11.1'e göre bu altgrupları $A_1 \leq A_i \lhd G$ için, A_i/A_1 olarak yazabiliriz. Demek ki, Teorem 11.6'ya göre

$$\mathbb{Z}/p\mathbb{Z} \simeq (A_{i+1}/A_1)/(A_i/A_1) \simeq A_{i+1}/A_i$$

olur. İstediğimiz kanıtlanmıştır. □

Sonuç 11.8. *p bir asalsa p^n elemanlı bir grubun her $i = 0, 1, \ldots, n$ için p^i elemanlı bir altgrubu vardır.*

11.10. G bir abel grubu olsun. $H < G$, G'nin maksimal bir (öz)altgrubu olsun. (Maksimal özaltgrup olmayabilir ama biz olduğunu varsayıyoruz.) Bu, Teorem 11.1'den dolayı, G/H'nin sadece iki altgrubu var anlamına gelir. Teorem 10.6'ten dolayı, bir p asalı için $G/H \simeq \mathbb{Z}/p\mathbb{Z}$ olur. Dolayısıyla Alıştırma 5.7 ve Örnek 9.48'e göre, bölünür bir grubun maksimal özaltgrubu yoktur. Örneğin $\mathbb{Q}$ grubunun maksimal altgrubu yoktur. Öte yandan $\mathbb{Q}$ grubunun, 1'i (ya da 0'dan farklı herhangi bir elemanı) içermeyen altgruplar arasında maksimal olan vardır (ve birkaç tane vardır; bir başka deyişle $\mathbb{Q}$'nun 1'i içermeyen öyle altgrupları vardır ki bu altgruplardan daha büyük her altgrup 1'i içerir). Okur alıştırma olarak bu altgrubu bulmaya çalışabilir. (Bkz. Teorem F.3.)

11.11. Burada yukarıdaki soruyu yanıtlayalım. $\mathbb{Q}$ grubunun 1'içermeyen en az bir altgrubu vardır, mesela $\{0\}$ altgrubu. $2\mathbb{Z}$ bir başkasıdır. $\mathbb{Q}$ grubunun 1'i içermeyen altgrupları arasında en büyüklerinin olduğunu kanıtlayacağız. Böyle bir altgrup, $1/2$, $1/3$ gibi sayıları da içeremez elbet. Şöyle bir tanım yapalım:

$$A = \left\{ \frac{a}{b} : a \in 2\mathbb{Z},\ b \notin 2\mathbb{Z} \right\}.$$

Yani A payı çift paydası tek olan kesirli sayılar olsun. Bu küme toplama ve çıkarma altında kapalıdır ve boşküme değildir, dolayısıyla bir altgruptur. 1'i içermediği bariz, hatta hiçbir tek tamsayıyı içermediği bariz. Ama A çift tamsayıları içerir Şimdi $A < B$ olsun. B'nin 1'i içerdiğini kanıtlayacağız. B'den A'da olmayan bir eleman alalım: u/v. Pay ve paydayı sadeleştirilmiş olarak alalım. O zaman u çift sayı olamaz, çünkü aksi halde v de çift sayı olmak zorunda olurdu. u/v elemanını kendisiyle v defa toplayarak $u \in B$ varsayımını yapabiliriz. $u = 2u_1 + 1$ olarak yazalım. $2u_1 \in 2\mathbb{Z} \leq A$ olduğundan, $1 - u - 2u_1 \in B$ olur ve böylece istediğimiz kanıtlanmış olur.

Okur, yukarıda 2 ile yaptığımızı rastgele bir p asalı için yapabilir. Ayrıca alıştırma olarak $\mathbb{Q}/A$ grubunun grup yapısını anlamaya çalışabilir. Birkaç ipucu: $\mathbb{Q}$ bölünür olduğundan, $\mathbb{Q}/A$ elbette bölünür bir gruptur. Eğer A'yı p asalı için tanımlamışsak, $\mathbb{Q}/A$ grubunun her elemanı bir p-elemandır. Ayrıca $\mathbb{Q}/A$'nın her özaltgrubu sonludur ve bir $n \in \mathbb{N}$ için $\mathbb{Z}/p^n\mathbb{Z}$ grubuna izomorftur. $\mathbb{Z}_{p^\infty}$ olarak gösterilen bu gruba ***Prüfer p-grubu*** adı verilir.

12. Direkt ve Yarıdirekt Çarpımlar

12.1 İki Grubun Kartezyen Çarpımı

Eğer G_1 ve G_2 iki grupsa, $G_1 \times G_2$ kümesini bir gruba dönüştürmeyi biliyoruz. Bunun için çarpımı (olabilecek en doğal biçimde),

$$(a, b)(c, d) = (ac, bd)$$

olarak tanımlamak yeterli. Bu altbölümde ters problemi ele alacağız, yani bir grubun hangi koşullarda $G_1 \times G_2$ türünden bir gruba izomorfik olduğunu bulacağız.

Önce $G = G_1 \times G_2$ grubu üzerine bir iki kelime söyleyelim.

$$H_1 = G_1 \times \{1\} \text{ ve } H_2 = \{1\} \times G_2$$

tanımlarını yapalım. O zaman

$$H_1 \simeq G_1,\ H_2 \simeq G_2$$

önermeleri ve dolayısıyla

$$G = G_1 \times G_2 \simeq H_1 \times H_2$$

önermesi doğrudur. Bunların kolay kanıtını okur teyit edebilir. Ayrıca, kolayca kanıtlanabileceği üzere,

$$H_1 \lhd G,\ H_2 \lhd G,\ G = H_1 H_2, \text{ ve } H_1 \cap H_2 = 1 \tag{1}$$

olur[1]. Şimdi, (1) koşullarını sağlayan H_1 ve H_2 altgruplarının varlığının, G grubunun $H_1 \times H_2$ grubuna izomorf olması için yeterli olduğunu göreceğiz.

[1]En sondaki 1, $G = G_1 \times G_2$ grubunun tek elemanlı altgrubunu simgelemektedir, yani $\{(1, 1)\}$ anlamınadır.

G bir grup olsun. Diyelim G'nin H_1 ve H_2 altgrupları (1) koşullarını sağlıyor. O zaman, H_2 normal bir altgrup olduğundan, $h_1 \in H_1$ ve $h_2 \in H_2$ için,

$$h_1^{-1}h_2^{-1}h_1h_2 = (h_1^{-1}h_2^{-1}h_1)h_2 \in H_2H_2 \subseteq H_2$$

olur; benzer şekilde

$$h_1^{-1}h_2^{-1}h_1h_2 = h_1^{-1}(h_2^{-1}h_1h_2) \in H_1H_1 \subseteq H_1$$

olduğundan,

$$h_1^{-1}h_2^{-1}h_1h_2 \in H_1 \cap H_2 = 1$$

olur; buradan da önce $h_1^{-1}h_2^{-1}h_1h_2 = 1$, sonra

$$h_1h_2 = h_2h_1 \tag{2}$$

çıkar. Şimdi

$$\varphi(h_1, h_2) = h_1h_2$$

kuralıyla tanımlanmış

$$\varphi : H_1 \times H_2 \longrightarrow G$$

fonksiyonuna bakalım. $H_1H_2 = G$ olduğundan bu fonksiyon örtendir. Ayrıca (2)'den dolayı φ bir homomorfidir:

$$\begin{aligned} \varphi((h_1, h_2)(h_1', h_2')) &= \varphi(h_1h_1', h_2h_2') = h_1h_1'h_2h_2' \\ &= h_1h_2h_1'h_2' = \varphi(h_1, h_2)\varphi(h_1'h_2'). \end{aligned}$$

φ'nin çekirdeğini hesaplayalım:

$$\begin{aligned} \operatorname{Ker}\varphi &= \{(h_1, h_2) \in H_1 \times H_2 : \varphi(h_1h_2) = 1\} \\ &= \{(h_1, h_2) \in H_1 \times H_2 : h_1h_2 = 1\} \\ &= \{(h_1, h_2) \in H_1 \times H_2 : h_1 = h_2^{-1}\} \\ &= \{(h_1, h_2) \in H_1 \times H_2 : h_1 = h_2^{-1} \in H_1 \cap H_2 = 1\} \\ &= \{(h_1, h_2) \in H_1 \times H_2 : h_1 = h_2^{-1} = 1\} \\ &= \{(1, 1)\}. \end{aligned}$$

Demek ki φ ayrıca birebirmiş. Böylece $H_1 \times H_2 \simeq G$ izomorfisi kanıtlanmış oldu. Kanıtladığımızı bir teorem olarak yazalım.

Teorem 12.1. *G grubunun H_1 ve H_2 altgrupları*

$$H_1 \lhd G,\ H_2 \lhd G,\ G = H_1H_2,\ \text{ve } H_1 \cap H_2 = 1 \tag{1}$$

önermelerini sağlıyorsa,

$$G \simeq H_1 \times H_2$$

olur. □

Varsayımlardan $G = H_1H_2$ koşulunu atarsak da bir sonuç elde ederiz.

Teorem 12.2. *Bir grubun H_1 ve H_2 altgrupları birbirlerini normalize ediyorsa ve $H_1 \cap H_2 = 1$ ise, o zaman*

$$\langle H_1, H_2 \rangle = H_1H_2 \simeq H_1 \times H_2$$

olur.

Kanıt: $\langle H_1, H_2 \rangle = H_1H_2$ eşitliğini biliyoruz. Bir önceki teoremde $G = H_1H_2$ alalım. □

Hemen bir uygulama görelim.

Sonuç 12.3. *G bir abel grubu, n ve m birbirine asal pozitif doğal sayılar ve her $g \in G$ için $g^{nm} = 1$ olsun.*

$$G[n] = \{g \in G : g^n = 1\} \text{ ve } G[m] = \{g \in G : g^m = 1\}$$

tanımlarını yapalım. O zaman $G \simeq G[n] \times G[m]$ olur.

Kanıt: Önce, her $g \in G$ için $g^n \in G[m]$ ve $g^m \in G[n]$ olduğunu görelim. Sonra, Bézout Teoremi'ne göre $nu + mv = 1$ eşitliğini sağlayan u, $v \in \mathbb{Z}$ tamsayıları olduğunu farkedelim. Şimdi her $g \in G$ için,

$$g = g^1 = g^{nu+mv} = (g^n)^u(g^m)^v$$

olur. Demek ki $G = G[m]G[n]$. Teorem 12.1'i uygulayabilmek için son olarak $G[n] \cap G[m] = 1$ eşitliğini kanıtlamamız lazım. Bu da kolay: Eğer $g^n = g^m = 1$ ise,

$$g = g^1 = g^{nu+mv} = (g^n)^u(g^m)^v = 1$$

olur. □

Sonuç 12.4. *G, sonlu eksponentli bir abel grubu olsun. Her p asalı için*

$$G[p^\infty] = \{g \in G : \text{ bir } i \in \mathbb{N} \text{ için } g^{p^i} = 1\}$$

tanımını yapalım. O zaman $G[p^\infty] \leq G$ ve sadece n'yi bölen p asalları için $G[p^\infty] \neq 1$ olur. Ve $G \simeq \prod_p G[p^\infty]$ olur.

Kanıt: $\exp G = n$ olsun. Tabii sadece n'yi bölen p asalları için $G[p^\infty] \neq 1$ olur; dolayısıyla n'yi bölen farklı asallara $p_1, \ldots, p_k$ dersek, önermeyi

$$G \simeq G[p_1^\infty] \times \ldots \times G[p_k^\infty]$$

olarak yazabilirdik.

Eğer n sayısı p^i'ye bölünüyorsa ama p^{i+1}'e bölünmüyorsa, $m = n/p^i$ tanımını yaparak, Sonuç 12.3'ten

$$G \simeq G[p^i] \times G[m]$$

elde ederiz. $G[p^i] = G[p^\infty]$ olduğundan, sonuç tümevarımla kolaylıkla kanıtlanır. □

Bu teoremin bir benzeri daha genel olarak burulmalı abel grupları için doğrudur, bkz. Sonuç 12.9.

Notlar ve Örnekler

12.1. $\operatorname{Alt} 1 = \{\mathrm{Id}_1\}$, $\operatorname{Alt} 2 = \{\mathrm{Id}_2\}$, $\operatorname{Alt} 3 = \{\mathrm{Id}_3, (1\ 2\ 3)(1\ 3\ 2)\}$ grupları basit gruplardır. Ama $\operatorname{Alt} 4$ basit birgrup değildir; örneğin,

$$\{\mathrm{Id}_4, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \lhd \operatorname{Alt} 4$$

olur. Ama $\operatorname{Alt} 5$ ve sonrası basittir. Şimdi bu teoremi kanıtlayacağız.

Sonuç 12.5. *$n \geq 5$ için $\operatorname{Alt} n$ basit bir gruptur.*

Kanıt: H, $\operatorname{Alt} n$'nin minimal bir normal altgrubu olsun. $H \neq \operatorname{Alt} n$ varsayımını yapalım. $\alpha \in \operatorname{Sym} n$ rastgele bir makas olsun. $H^\alpha \lhd \operatorname{Alt} n$ olur. Eğer $H^\alpha = H$ ise, H, $\operatorname{Sym} n = \langle \operatorname{Alt} n, \alpha \rangle$ tarafından normallenir. Bu durumda Teorem 9.4'e göre $H = \operatorname{Alt} n$ olur. Bundan böyle her α makası için $H^\alpha \neq H$ varsayımını yapalım. H minimal normal altgrup olduğundan, $H \cap H^\alpha = 1$ olur. Demek ki H ile H^α'nın elemanları birbirleriyle değişirler. Dolayısıyla

$$\langle H, H^\alpha \rangle = H \oplus H^\alpha$$

olur. Ama bu altgrup hem $\operatorname{Alt} n$ tarafından hem de α tarafından,dolayısıyla $\operatorname{Sym} n$ tarafından normallenir. Gene Teorem 9.4'e göre $\operatorname{Alt} n = H \oplus H^\alpha$ olur. Demek ki $|H|^2 = n!/2$ ve dolayısıyla $|H|$ bir çift sayı olmak zorunda. Demek ki H'de derecesi 2 olan bir h elemanı vardır. Bu eleman makasların çarpımıdır. Eğer α'yı bu makaslardan biri olarak alırsak, $h^\alpha = h$ ve dolayısıyla $h \in H \cap H^\alpha = 1$ olur. Çelişki. □

12.2 Çok Sayıda Grubun Direkt Toplamı

Verilmiş bir $(G_i)_{i\in I}$ grup ailesiyle $\bigoplus_I G_i$ olarak gösterdiğimiz bir grup yaratmıştık. Anımsatalım. Küme olarak tanım şöyleydi:

$$\bigoplus_I G_i = \left\{ (g_i)_{i\in I} \in \prod_I G_i : \{i \in I : g_i \neq 1\} \text{ sonlu} \right\}.$$

Kolaylık açısından $(g_i)_{i\in I}$ elemanını $(g_i)_i$ olarak gösterelim. Çarpımı tahmin edildiği gibi:

$$(g_i)_i (h_i)_i = (g_i h_i)_i.$$

Şimdi $G = \bigoplus_I G_i$ ve her $j \in I$ için

$$H_j = \{(g_i)_i \in G : \text{ her } i \in I \text{ için eğer } i \neq j \text{ ise } g_i = 1\}$$

tanımlarını yapalım. Yani H_j kümesi, belki j'inci terim dışında, her terimi 1 olan elemanlardan oluşsun. Her $j \in I$ için, $G_j \simeq H_j \leq G$ ve

$$G = \bigoplus_I G_i \simeq \bigoplus_I H_i$$

olduğu bariz olmalı. Ayrıca her $j \in I$ için

$$H_j \lhd G, \tag{3}$$

$$G = \langle H_i : i \in I \rangle \tag{4}$$

ve

$$H_j \cap \langle H_i : i \in I \setminus \{j\} \rangle = 1 \tag{5}$$

olur. (3) bariz olmalı. (4) de zor değil, çünkü $G = \bigoplus_I G_i$ grubunun bir $g = (g_i)_i$ elemanında sonlu sayıda 1'den farklı terim vardır. Eğer $i_1, \ldots, i_n$ göstergeçleri için $g_{i_1} \neq 1, \ldots, g_{i_n} \neq 1$ ve diğer göstergeçler için terimler 1 ise, $g \in H_{i_1} \cdots H_{i_n}$ olur. (5)'i kanıtlayalım: $\langle H_i : i \in I \setminus \{j\} \rangle$ altgrubunun her elemanının j'inci koordinatı 1'dir; ama H_j grubunun j'inci koordinat dışında her koordinatı 1'dir; demek ki kesişimdeki bir elemanın tüm koordinatları 1'dir, yani kesişim 1'dir.

Çoğu zaman (5)'i başka türlü yazmak daha kullanışlı olur. (5) ile şu koşul eşdeğerdir:

Eğer $i_1, \ldots, i_n \in I$ farklı göstergeçlerse, $h_{i_1} \in H_{i_1}, \ldots, h_{i_n} \in H_{i_n}$ ise ve $h_{i_1} \cdots h_{i_n} = 1$ ise $h_{i_1} = \ldots = h_{i_n} = 1$ olur.

Bu iki koşulun eşdeğer olduğunun kanıtı çok kolaydır: Eğer $1 = \prod_i h_i$ ise, her j için,

$$h_j^{-1} = \prod_{i \neq j} h_i \in H_j \cap \langle H_i : i \in I \setminus \{j\} \rangle = 1,$$

dolayısıyla $h_j = 1$ olur. Diğer istikamet de kolay.

Şimdi problemi tersten ele alalım. G herhangi bir grup olsun. G'nin bir $(H_i)_{i \in I}$ altgrup ailesi verilmiş olsun. (3), (4) ve (5) koşullarının $G \simeq \bigoplus_I H_i$ olması için yeter koşullar olduğunu kanıtlayalım. Bunun için önce $i \neq j$ ve $h_i \in H_i$, $h_j \in H_j$ için $h_i h_j = h_j h_i$ eşitliğini kanıtlamalıyız. (5)'ten dolayı $H_i \cap H_j = 1$ olduğundan, bu aynen bir önceki altbölümdeki gibi (3) kullanılarak kanıtlanır (bkz. Örnek 9.9): $[H_i, H_j] \leq H_i \cap H_j = 1$. Şimdi

$$\varphi((h_i)_i) = \prod_i h_i$$

kuralıyla tanımlanmış

$$\varphi : \bigoplus_I H_i \longrightarrow G$$

fonksiyonuna bakalım. h_i'ler arasında sonlu sayıda 1'den farklı eleman olduğundan ve h_i'ler aralarında değiştiğinden, $\prod_i h_i$ çarpımı anlamlıdır, sonuçta sonlu sayıda eleman çarpılmaktadır. φ elbette bir homomorfidir ve (4)'ten dolayı örten bir homomorfidir. Birebir olduğu da, yukarıda (5)'e eşdeğer olduğu kanıtlanan önermeden çıkıyor: Eğer $1 = \varphi((h_i)_i) = \prod_i h_i$ ise, her j için $h_j = 1$ olur.

Teorem 12.6. *Eğer bir G grubunun $(H_i)_i$ altgrup ailesi* (3), (4) *ve* (5) *koşullarını sağlıyorsa*

$$\varphi((h_i)_i) = \prod_i h_i$$

formülüyle tanımlanan $\varphi : \bigoplus_I H_i \longrightarrow G$ fonksiyonu bir izomorfidir. □

Teorem 12.7. *Eğer bir grubun birbirini normalize eden $(H_i)_i$ altgrup ailesi*

$$H_j \cap \langle H_i : i \in I \setminus \{j\} \rangle = 1 \tag{5}$$

koşulunu sağlıyorsa $\langle H_i : i \in I \rangle \simeq \bigoplus_I H_i$ olur. □

Bazen $(H_i)_i$ altgrup ailesi karşımıza bir küme olarak çıkar. Zaten bir önceki teoremdeki H_i'lerden ikisi eşit olamayacaklarından (hatta kesişemeyeceklerinden), teoremdeki aileyi bir küme olarak almak sonucu zayıflatamaz. Bu durumu da kaydedelim:

Teorem 12.8. *G bir grup ve X, elemanları G'nin birbirini normalize eden (bazı) altgruplarından oluşan bir küme olsun. Diyelim birbirinden farklı her $H_1, \ldots, H_n \in X$ ve her $h_i \in H_i$ için $h_1 \cdots h_n = 1$ eşitliği ancak $h_1 = \ldots = h_n = 1$ için doğru olabiliyor. Bu durumda $\langle H : H \in X \rangle \simeq \bigoplus_{H \in X} H$ olur.* □

Bu teoremi burulmalı abel gruplarına uygulayalım:

Sonuç 12.9. *G burulmalı bir abel grubu olsun. Her p asalı için*

$$G[p^\infty] = \{g \in G : \textit{bir } i \in \mathbb{N} \textit{ için } g^{p^i} = 1\}$$

tanımını yapalım. O zaman $G[p^\infty] \leq G$ ve $G \simeq \bigoplus_{p \ \ asal} G[p^\infty]$ olur.

Kanıt: $G[p^\infty]$ altkümesinin bir altgrup olduğu bariz olmalı. Teorem 4.10 ya da Sonuç 10.23'den dolayı $G[p^\infty]$ altgrupları G'yi üretir. Sabit bir q asalı için $\langle G[p^\infty] : p \neq q \rangle$ grubunun elemanlarının dereceleri q asalına bölünmezler. Demek ki bu altgrubun $G[q^\infty]$ ile kesişimi 1'dir. Teorem 12.6 istediğimiz izomorfiyi verir. □

Notlar ve Örnekler

12.2. Örnek 9.55'e göre $\mathbb{Q}/\mathbb{Z}$ burulmalı bir gruptur. $G = \mathbb{Q}/\mathbb{Z}$ ve p bir asal olsun. O zaman Sonuç 12.9'de tanımlanan $G[p^\infty]$ altgrubu,

$$\{\overline{\alpha} : \alpha = a/p^n : n \in \mathbb{N},\, a \in \mathbb{Z}\}$$

grubuna, yani

$$\{\overline{\alpha} : \alpha = a/p^n : n \in \mathbb{N},\, a = 0, 1, 2, \ldots, p^n - 1\}$$

grubuna eşittir. Dolayısıyla $\mathbb{Q}/\mathbb{Z}$ bölüm grubu bu altgrupların direkt toplamına izomorftur. Bu kitapta arada bir sözedeceğimiz ve matematikte önemli bir yer tutan $G[p^\infty]$ gruplarına ***Prüfer p-grubu*** adı verilir ve bu altgruplar $\mathbb{Z}_{p^\infty}$ olarak gösterilir.

12.3. G bir abel grubu ve $H \leq G$ olsun. p bir asal olsun. Elbette $H[p^\infty] = G[p^\infty] \cap H$ olur.

12.4. G burulmalı bir abel grubu $H \leq G$ olsun. Sonuç 12.9'e ve bir önceki örneğe göre, $H_p \leq G[p^\infty]$ altgrupları için,

$$H \simeq \bigoplus_{p \text{ asal}} H_p$$

olur. Elbette $H_p = G[p^\infty] \cap H$ olur.

12.5. Eğer $G = \langle g \rangle$, n elemanlı döngüsel bir grupsa, her $d|n$ için G'nin d elemanlı tek bir altgrubu vardır:

$$\left\langle g^{n/d} \right\rangle = \{x^{n/d} : x \in G\} = \{x \in G : x^d = 1\}.$$

Bunun tersi de doğrudur:

Her d için d elemanlı en fazla bir altgrubu olan sonlu gruplar döngüseldir.

Kanıt: Önermeyi grubun eleman sayısı üzerine tümevarımla kanıtlayacağız, ne de olsa altgruplarının da aynı özelliği vardır. Teoremi önce asal sayıların kuvvetleri için kanıtlayalım. p bir asal, $n \in \mathbb{N}$ ve G grubunun p^n elemanı olsun. Merkezden derecesi p olan bir a elemanı alalım (Teorem 8.10 ya da 14.6). $\langle a \rangle$ grubu G'nin eleman sayısı p olan yegâne altgrubudur, demek ki trişkadan olmayan her altgrubun altgrubudur, yani a, trişkadan olmayan her altgrubun elemanıdır. $G/\langle a \rangle$ grubu da önermenin hipotezini sağlar. Demek ki tümevarımla $G/\langle a \rangle$ grubunun döngüsel olduğunu anlarız. $b \in G$ için $G/\langle a \rangle = \langle \bar{b} \rangle$ olsun. Demek ki $G = \langle a \rangle \langle b \rangle$. Ama $\langle a \rangle \leq \langle b \rangle$. Demek ki $G = \langle b \rangle$.

Şimdi G'nin eleman sayısı bir asalın bir kuvveti olmasın. O zaman her p için G'de tek bir maksimal p-altgrubu vardır (iki tane olsa eleman sayıları farklı olmak zorunda; Sonuç 11.8'den dolayı da az sayıda elemanı olan diğerinin içinde olmak zorunda, bu da maksimallikle çelişir). Dolayısıyla maksimal p-altgrupları grubun tüm p-elemanlarından oluşur. Buradan da grubun maksimal p-altgruplarının direkt toplamı olduğu anlaşılır (Alıştırma 12.11). Ama her p-altgrubun döngüsel olduğunu bir paragraf önce kanıtladık. Çin Kalan Teoremi'ne göre (Teorem 10.22) G döngüseldir. □

12.6. *G sonlu bir grup olsun. Eğer $|G|$'yi bölen her d doğal sayısı için $x^d = 1$ denkleminin G'de en fazla d tane çözümü varsa G döngüseldir.*

Kanıt: Varsayım altgruplara geçtiğinden, grubun eleman sayısı üzerine tümevarım yapabiliriz. Önce G'nin bir asal p sayısı için bir p-grubu olduğunu varsayalım. Diyelim $|G| = p^n$. Teorem 11.7'ye göre G'nin p^{n-1} elemanlı bir H altgrubu vardır. Tümevarımla H altgrubu, G'nin derecesi $\leq p^{n-1}$ olan elemanlardan oluşur. Dolayısıyla $G \setminus H$ kümesinde derecesi p^{n-1}'den küçükeşit bir eleman olamaz. Eğer $g \in G \setminus H$ ise, g'nin derecesi tam tamına p^n olmalıdır ve dolayısıyla G'yi üretir.

Şimdi G bir p-grup olmasın. $|G|$'yi bölen asal bir p alalım. G'nin en fazla elemanlı bir p-altgrubunu alalım, diyelim P. Yukarıda yapılandan dolayı P döngüseldir. P'nin eleman sayısı p^n olsun. p^n maksimal olduğundan, G'de derecesi p^n'den büyük eleman olamaz, aksi halde bu elemanın ürettiği altgrubun eleman sayısı p^n'den büyük olurdu. P döngüsel olduğundan, her $k \leq n$ için P'de $x^{p^k} = 1$ denklemini sağlayan tam p^k

tane eleman vardır, demek ki G'nin derecesi p^k olan tüm elemanları P'dedir. Bundan da P'nin G'nin p-elemanlarından oluştuğu çıkar. Buradan da grubun p-altgruplarının direkt toplamı olduğu anlaşılır (Alıştırma 12.11). Her p-altgrubun döngüsel olduğunu bildiğimizden Çin Kalan Teoremi'ne göre (Teorem 10.22) G döngüseldir. □

Aşağıdaki sonuca ileride sık sık ihtiyacımız olacak. Aradan çıkarmanın tam zamanı.

Önsav 12.10. *G bir grup, I bir göstergeç kümesi ve her $i \in I$ için X_i, G'nin birbirini normalize eden bir altgrup kümesi olsun. Ayrıca $i, j \in I$ için ya $X_i \subseteq X_j$ ya da $X_j \subseteq X_i$ varsayımını yapalım. $X = \bigcup_i X_i$ olsun. Eğer her i için*

$$\langle H : H \in X_i \rangle = \bigoplus_{H \in X_i} H$$

oluyorsa

$$\langle H : H \in X \rangle = \bigoplus_{H \in X} H$$

olur.

Kanıt: Teorem 12.8'yi kullanacağız. Farklı $H_1, \ldots, H_n \in X$ ve $h_j \in H_j$ için

$$h_1 \cdots h_n = 1$$

olsun. Her $H_j \in X_{i_j}$ olsun. Hipoteze göre, X_{i_j}'lerden biri diğerlerini kapsar, diyelim X_{i_k} hepsini kapsıyor. O zaman $h_1 \cdots h_n = 1$ eşitliği $\langle H : H \in X_{i_k} \rangle$ grubunda yer aldığından, diğer hipoteze göre $H_1 = \ldots = h_n = 1$ olur. □

Alıştırmalar

12.7. $Z\left(\prod_I G_i\right) = \prod_I Z(G_i)$ ve $Z\left(\bigoplus_I G_i\right) = \bigoplus_I Z(G_i)$ eşitliklerini kanıtlayın.

12.8. I ve J ayrık göstergeç kümeleri olsun. $K = I \cup J$ olsun. Son olarak $(G_k)_{k \in K}$ bir grup ailesi olsun.

$$\bigoplus_K G_k \simeq \left(\bigoplus_I G_i\right) \oplus \left(\bigoplus_J G_j\right)$$

izomorfisini kanıtlayın.

12.9. $\alpha \in A$ için $(I_\alpha)_\alpha$ ikişer ikişer ayrık göstergeç kümeleri olsun. $J = \bigcup_A I_\alpha$ olsun. Son olarak $(G_j)_{j \in J}$ bir grup ailesi olsun.

$$\prod_J G_j \simeq \prod_{\alpha \in A} \left(\prod_{I_\alpha} G_i\right)$$

izomorfisini kanıtlayın. Aynı önermeyi $\prod$ yerine $\bigoplus$ ile kanıtlayın.

12.10. $A = \mathbb{Q}/\mathbb{Z}$ olsun. Her p asalı için $A[p^\infty]$, A'nın, derecesi p'nin bir kuvveti olan elemanlardan oluşan altkümesi olsun.

$$A[p^n] = \{\overline{q} \in \mathbb{Q}/\mathbb{Z} : p^n \overline{q} = \overline{0}\}$$

olsun. Ayrıca $A[p^n]$ ve $A[p^\infty]$ birer altgruptur. İkincisine ***Prüfer p-grubu*** denir. Elbette,

$$A[p^n] \leq A[p^{n+1}] \leq A[p^\infty] \leq A$$

ve ayrıca

$$A[p^\infty] = \{\overline{q} \in \mathbb{Q}/\mathbb{Z} : \text{bir } n \in \mathbb{N} \text{ için } p^n\overline{q} = \overline{0}\} = \bigcup_{n\in\mathbb{N}} A[p^n]$$

olur.

$$\mathbb{Q}/\mathbb{Z} = \bigoplus_{p \text{ asal}} A[p^\infty]$$

eşitliğini kanıtlayın. Eğer $q = 1/6$ ise, $\overline{q}$ elemanının p asalları için $A[p^\infty]$ bileşenlerine ayırın. (Bkz. Örnek 9.67.)

12.11. G burulmalı bir grup olsun. Her p asalı için grubun p-elemanlarının kümesinin bir altgrup olduğunu varsayalım, diyelim G_p. Bu durumda $G = \bigoplus_{p\text{asal}} G_p$ olduğunu kanıtlayın. (Bkz. Teorem 4.10.)

Direkt Toplamın Kategorik Özelliği

$(H_i)_{i\in I}$ bir grup ailesi olsun. $\bigoplus_I H_i$ grubunun "kategorik" olarak adlandırılacak bir özelliği vardır. Bu paragrafta $\bigoplus_I H_i$ grubunun bu özelliğini açıklayacağız.

Her $j \in I$ için H_j'den $\bigoplus_I H_i$ grubuna giden doğal bir gömme vardır: Eğer $h \in H_j$ ise, $e_j(h) \in \bigoplus_I H_i$ elemanı, j'inci koordinatı h olan, diğer koordinatları 1 olan elemanı temsil etsin. Her $i \neq j$ ve her $h_i \in H_i$ ve $h_j \in H_j$ için

$$e_i(h_i)e_j(h_j) = e_j(h_j)e_i(h_i)$$

eşitliğini biliyoruz.

Şimdi rastgele bir G grubu ve bir $(f_i : H_i \longrightarrow G)_{i\in I}$ homomorfi ailesi alalım. Her $i \neq j$ ve her $h_i \in H_i$ ve $h_j \in H_j$ için

$$f_i(h_i)f_j(h_j) = f_j(h_j)f_i(h_i)$$

eşitliğini varsayalım. $(h_i)_i \in \oplus_I H_i$ için

$$f\left((h_i)_i\right) = \prod_i f_i(h_i)$$

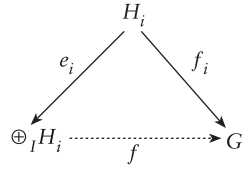
tanımını yapalım. Sadece sonlu sayıda $h_i \neq 1$ olduğundan ve çarpılan elemanlar aralarında değiştiğinden, sağdaki ifade anlamlıdır. Böylece bir

$$f : \bigoplus_I H_i \longrightarrow G$$

fonksiyonu elde ettik. Bu fonksiyonun bir homomorfi olduğunu ve her $i \in I$ için

$$f \circ e_i = f_i \tag{6}$$

eşitliğini kontrol etmek zor değildir. Ayrıca (elbette) f homomorfisi (6) eşitliklerini sağlayan biricik homomorfidir çünkü (6), f'nin her koordinatında alması gerektiği değeri söylemektedir.



Demek ki:

Teorem 12.11. *$(H_i)_{i\in I}$ bir grup ailesi ve her $j \in I$ için $e_j : H_j \longrightarrow \oplus_I H_i$ doğal gömme olsun. O zaman*

$$\left((H_i)_i, \bigoplus_I H_i, \left(e_i : H_i \longrightarrow \bigoplus_I H_i \right)_i \right)$$

üçlüsünün şu özelliği vardır: Rastgele bir G grubu alalım. Her $i \neq j$ ve her $h_i \in H_i$ ve $h_j \in H_j$ için

$$f_i(h_i)f_j(h_j) = f_j(h_j)f_i(h_i)$$

eşitliğini sağlayan bir $(f_i : H_i \longrightarrow G)_{i\in I}$ homomorfi ailesi alalım. O zaman öyle bir ve bir tane

$$f : \bigoplus_I H_i \longrightarrow G$$

homomorfisi vardır ki her $i \in I$ için

$$f \circ e_i = f_i$$

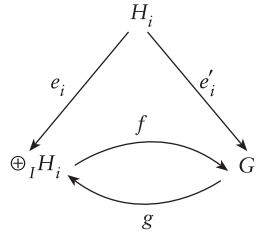
olur. □

Teoremdeki "bir ve bir tane" sözleri önemlidir, hafife alınmamalıdır. Şimdi yukarıdaki teoreme bir ek yapalım:

Teorem 12.12. *$(H_i)_i$ bir grup ailesi, H bir grup ve $(e'_i : H_i \longrightarrow H)_i$ bir homomorfi ailesi olsun. Eğer*

$$((H_i)_i, H, (e'_i : H_i \longrightarrow H)_i)$$

üçlüsü bir önceki teoremdeki özelliği sağlıyorsa, o zaman $H \simeq \bigoplus_I H_i$ olur. Ayrıca öyle bir $g : H \longrightarrow \bigoplus_I H_i$ izomorfisi vardır ki her $i \in I$ için $g \circ e'_i = e_i$ olur.



Kanıt: Yukarıdaki şemadan takip edin. Teorem 12.11'dan dolayı

$$f \circ e_i = e'_i$$

eşitliklerini sağlayan bir

$$f : \bigoplus_I H_i \longrightarrow H$$

homomorfisi vardır. Kanıtlamak istediğimiz teoremin hipotezine göre

$$g \circ e'_i = e_i$$

eşitliklerini sağlayan bir

$$g : H \longrightarrow \bigoplus_I H_i$$

homomorfisi vardır. Demek ki $f \circ g : H \longrightarrow H$ homomorfisi her $i \in I$ için

$$(f \circ g) \circ e_i' = f \circ (g \circ e_i') = f \circ e_i = e_i'$$

eşitliğini sağlar. $f \circ g : H \longrightarrow H$ homomorfisinin sağladığı bu eşitliği Id_H özdeşlik fonksiyonu da sağlar. Teoremdeki "bir ve bir tane" nitelemesinden dolayı $f \circ g = \mathrm{Id}_H$ olmalı. Benzer nedenden $g \circ f : \bigoplus_I H_i \longrightarrow \oplus_I H_i$ fonksiyonu da birim fonksiyondur. Böylece f ve g'nin birbirinin tersi izomorfiler olduklarını kanıtladık. □

Kartezyen Çarpımın Kategorik Özelliği

$(H_i)_{i\in I}$ bir grup ailesi olsun. $\prod_I H_i$ grubunun da "kategorik" olarak adlandırılacak bir özelliği vardır. Bu paragrafta bu özelliğini açıklayacağız.

Her $j \in I$ için $\prod_I H_i$ grubundan H_j grubuna giden izdüşüm fonksiyonu vardır: $\pi_j((h_i)_i) = h_j$. Bu fonksiyon elbette örten bir homomorfidir.

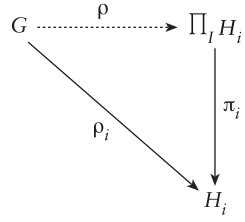
Şimdi herhangi bir G grubu ve bir $(\rho_i : G \longrightarrow H_i)_i$ homomorfi ailesi alalım. Amacımız her $i \in I$ için $\pi_i \circ \rho = \rho_i$ eşitliğini sağlayan $\rho : G \longrightarrow \prod_I H_i$ homomorfisi bulmak. Eğer gerçekten böyle bir ρ varsa, ve $g \in G$ için

$$\rho(g) = (h_i)_i$$

ise, o zaman $(\pi_i \circ \rho)(g) = \rho_i(g)$, yani $h_i = \rho_i(g)$ olmalı. Demek ki tek çaremiz

$$\rho(g) = (\rho_i(g))_i$$

tanımını yapmak. Nitekim bu tanım istediğimiz özellikleri sağlar. Önce bunu bir teorem olarak yazalım. Sonra daha fazlasını ekleyeceğiz.



Teorem 12.13. *$(H_i)_{i\in I}$ bir grup ailesi ve her $j \in I$ için $\pi_j : \prod_I H_i \longrightarrow H_j$ izdüşüm fonksiyonu olsun. O zaman*

$$\left((H_i)_i, \prod_I H_i, \left(\pi_i : \prod_I H_i \longrightarrow H_i\right)_i\right)$$

üçlüsünün şu özelliği vardır: Rastgele bir G grubu ve bir $(\rho_i : G \longrightarrow H_i)_i$ homomorfi ailesi alalım. O zaman öyle bir ve bir tane

$$\rho : G \longrightarrow \prod_I H_i$$

homomorfisi vardır ki her $i \in I$ için

$$\pi_i \circ \rho = \rho_i$$

olur. ρ homomorfisi her $g \in G$ için

$$\rho(g) = (\rho_i(g))_i$$

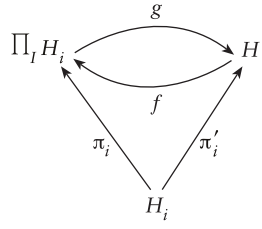
olarak tanımlanmıştır. □

Bu teoremdeki "bir ve bir tane" sözleri de önemlidir, şimdi bu sözlerin önemini görelim:

Teorem 12.14. *$(H_i)_i$ bir grup ailesi, H bir grup ve $(\pi'_i : H \longrightarrow H_i)_i$ bir homomorfi ailesi olsun. Eğer*

$$((H_i)_i,\ H,\ (\pi'_i : H \longrightarrow H_i)_i)$$

üçlüsü bir önceki teoremdeki özelliği sağlıyorsa, o zaman $H \simeq \prod_I H_i$ olur. Ayrıca öyle bir $g : H \longrightarrow \prod_I H_i$ izomorfisi vardır ki her $i \in I$ için $\pi'_i = \pi_i \circ g$ olur.



Kanıt: Yukarıdaki şemadan takip edin. Teorem 12.13'den dolayı

$$\pi_i \circ g = \pi'_i$$

eşitliklerini sağlayan bir $g : H \longrightarrow \prod_I H_i$ homomorfisi vardır. Kanıtlamak istediğimiz teoremin hipotezine göre

$$\pi'_i \circ f = \pi_i$$

eşitliklerini sağlayan bir

$$f : \prod_I H_i \longrightarrow H$$

homomorfisi vardır. O zaman $f \circ g : H \longrightarrow H$ homomorfisi

$$\pi'_i \circ (f \circ g) = \pi'_i$$

eşitliğini sağlar. $f \circ g : H \longrightarrow H$ homomorfisinin sağladığı bu eşitlik $\mathrm{Id}_H : H \longrightarrow H$ tarafından da sağlanır. Ama varsayımdaki biriciklikten dolayı bundan $f \circ g = \mathrm{Id}_H$ çıkar. Benzer nedenden $g \circ f = \mathrm{Id}_{\prod_I H_i}$ olur. Demek ki f ve g birer izomorfidir. □

12.3 Yarıdirekt Çarpım

Bir grubun iki altgrubunun direkt çarpımı olması oldukça basit gruplarda rastlanan bir durumdur. Bu altbölümde çok daha sık rastlanan bir durumdan sözedeceğiz. G bir grup olsun. H, $K \leq G$ olsun. Diyelim K, H'yi normalize ediyor, yani $K \leq N_G(H)$. Bu durumda

$$\langle H, K\rangle = HK = \{hk : h \in H, k \in K\}$$

eşitliğini ve $H \lhd HK$ olduğunu biliyoruz. Bundan sonra yapacağımız için G'yi HK altgrubuna eşit almanın bir sakıncası olmayacak, istersek $G = HK$ varsayımını yapabiliriz. Demek ki HK grubunun her elemanı bir $h \in H$ ve $k \in K$ için hk biçiminde yazılabilir. Bir başka deyişle

$$f : (h, k) \mapsto hk$$

kuralıyla tanımlanan $H \times K$ kümesinden HK grubuna giden fonksiyon örten bir fonksiyondur. Ama birebir olmayabilir. Altbölüm 12.1'de bu fonksiyonun bir grup izomorfisi olduğu durumu ele almıştık. Bu altbölümde bu fonksiyonun sadece birebir olduğu daha genel durumu ele alacağız.

f fonksiyonunda birebirliği bozanın ne olduğu çok belli: $H \cap K$ altgrubunun 1 olmaması birebirliğin önündeki yegâne engeldir. Nitekim eğer $a \in H \cap K$ ise, $(ha, a^{-1}k)$ ile (h, k) elemanlarının f-imgeleri aynıdır. Bundan böyle $H \cap K = 1$ varsayımını yapalım. Bu durumda $H \times K$ kümesiyle (grubuyla değil!) HK altgrubu arasında birebir ve örten bir eşleme vardır. Amacımız HK altgrubunun çarpmasını f eşlemesini kullanarak $H \times K$ kümesine çekmek, bir başka deyişle, verilmiş (h, k), $(h_1, k_1) \in H \times K$ elemanları için

$$f^{-1}(f(h, k)f(h_1, k_1)) \in H \times K$$

elemanını bulmak. Nitekim bir grupla bir küme arasında bir eşleme varsa, bu eşlemeyi kullanarak grubun işlemini küme üzerinde tanımlayarak kümeyi bir gruba dönüştürebiliriz; eşleme de böylece bir izomorfi olur (bkz. Alıştırma 10.79).

Bu amaçla, h, $h_1 \in H$ ve k, $k_1 \in K$ elemanları için $(hk)(h_1k_1)$ çarpımını hesaplayalım:

$$(hk)(h_1k_1) = hkh_1k_1 = hkh_1k^{-1}kk_1 = (hkh_1k^{-1})(kk_1).$$

Eşitliğin en sağındaki ifadenin birinci parantezindeki hkh_1k^{-1} elemanı H'nin bir elemanı çünkü K altgrubu H'yi normalize ediyor. $k \in K$ için

$$\varphi_k : H \longrightarrow H$$

fonksiyonu

$$\varphi_k(h) = khk^{-1}$$

olarak tanımlansın. Bildiğimiz ve kanıtlaması kolay olduğu üzere $\varphi_k \in \operatorname{Aut} H$ olur. Demek ki,

$$(hk)(h_1k_1) = (h\varphi_k(h_1))(kk_1)$$

eşitliği geçerlidir. Buradan hareketle $H \times K$ kümesi üzerinde bir işlem tanımlayabiliriz:

$$(h,k) \star (h_1,k_1) = (h\varphi_k(h_1), kk_1).$$

Böylece $H \times K$ kümesi HK grubuna izomorfik bir grup yapısına kavuşmuş olur. İzomorfizma da elbette $f : (h,k) \mapsto hk$ fonksiyonuyla verilmiştir.

Dikkat ederseniz yukarıda tanımlanan çarpım kartezyen çarpımdaki çarpıma çok benziyor. İkinci koordinatta gerçekten K'daki çarpmayı kullanıyoruz, ama birinci koordinatta hh_1 yerine h_1'e hafif bir değişim uygulayarak $h\varphi_k(h_1)$ yazdık. Eğer $\varphi_k = \mathrm{Id}_H$ ise (yani k, H'nin elemanlarıyla değişiyorsa, yani $k \in C_K(H)$ ise), aynen kartezyen çarpımı elde ederiz. Çarpmada

$$kh_1 = kh_1k^{-1}k = \varphi_k(h_1)k$$

eşitliğini kullandığımız gözden kaçmamalı; k'yı h_1'in solundan sağına geçirirken h_1'e gereken dönüşümü uyguluyoruz.

Her $k \in K$ için tanımlanmış olan $\varphi_k : H \longrightarrow H$ otomorfilerine dikkatimizi çevirelim konuyu daha soyut haliyle ele almadan önce.

$$\varphi : K \longrightarrow \operatorname{Aut} H$$

fonksiyonunu

$$\varphi(k) = \varphi_k$$

kuralıyla tanımlanmış olsun. φ'nin bir grup homomorfisi olduğunu biliyoruz.

Sonuç olarak, HK grubunun çarpım tablosu, H ve K gruplarının çarpım tabloları ve φ homomorfisi tarafından tamamen belirleniyor. İşte bu olguyu bir sonra paragraftan itibaren sömüreceğiz. Ama önce G yerine HK grubunu alarak yukarıdaki varsayımlarımızın bir listesini çıkaralım, ileride gerekecek:

$$G = HK,\ H \lhd G,\ K \leq G,\ H \cap K = 1. \tag{6}$$

Ters Problem. Şimdi yukarıda yaptıklarımızı unutmuş gibi yapıp problemi tersten ele alalım. Ortada G grubu yok ama onun yerine K ve H grupları ve bir $\varphi : K \longrightarrow \operatorname{Aut} H$ homorfisi verilmiş olsun. $k \in K$ için $\varphi(k)$ yerine φ_k yazmayı tercih edeceğiz[2]. $H \times K$ kümesi üzerine şu işlemi tanımlayalım:

$$(h,k)(h_1,k_1) = (h\varphi_k(h_1), kk_1).$$

[2]Aksi halde $(\varphi(k))(h)$ gibi bol parantezli ifadeler oluşur, oysa $f(k)$ yerine φ_k yazarak bu ifade $\varphi_k(h)$ olarak gösterilebilir.

Bu işlemin $H \times K$ kümesini bir gruba dönüştürdüğünü kanıtlayacağız.

Önce birleşme özelliğini kanıtlayalım.

$$\begin{aligned}(h,k)((h_1,k_1)(h_2,k_2)) &= (h,k)(h_1\varphi_{k_1}(h_2), k_1k_2)\\ &= (h\varphi_k(h_1\varphi_{k_1}(h_2)), kk_1k_2)\\ &= (h\varphi_k(h_1)\varphi_k(\varphi_{k_1}(h_2)), kk_1k_2)\\ &= (h\varphi_k(h_1)(\varphi_k\varphi_{k_1})(h_2), kk_1k_2)\\ &= (h\varphi_k(h_1)\varphi_{kk_1}(h_2), kk_1k_2).\end{aligned}$$

Diğer yandan

$$((h,k)(h_1,k_1))(h_2,k_2) = (h\varphi_k(h_1), kk_1)(h_2,k_2) = (h\varphi_k(h_1)\varphi_{kk_1}(h_2), kk_1k_2).$$

Aynı sonucu bulduk. Demek ki birleşme özelliği sağlanıyor.

Şimdi $(1,1)$ elemanının etkisiz eleman olduğunu gözlemleyelim:

$$(1,1)(h,k) = (1\cdot\varphi_1(h), 1\cdot k) = (\varphi_1(h), k) = (\mathrm{Id}_H(h), k) = (h,k)$$

(çünkü φ bir homomorfi olduğundan $\varphi_1 = \varphi(1) = \mathrm{Id}_H$ olur) ve

$$(h,k)(1,1) = (h\varphi_k(1), k\cdot 1) = (h\cdot 1, k) = (h,k)$$

(çünkü φ_k bir homomorfi olduğundan $\varphi_k(1) = 1$ olur) olur.

Son olarak bir (h,k) elemanının tersinin olduğunu kanıtlayalım, hatta daha iyisini yapıp tersini bulalım. Eğer (h,k)'nin ters elemanına (h_1,k_1) dersek,

$$(1,1) = (h,k)(h_1,k_1) = (h\varphi_k(h_1), kk_1)$$

olmalı. Demek ki $k_1 = k^{-1}$ ve $h_1 = (\varphi_k)^{-1}(h^{-1}) = \varphi_{k^{-1}}(h)^{-1}$ olmalı, yani (h,k) elemanının tersi – eğer varsa –

$$(\varphi_{k^{-1}}(h)^{-1}, k^{-1})$$

olmalı. Son olarak $(\varphi_{k^{-1}}(h)^{-1}, k^{-1})$ elemanının (h,k) elemanının sağdan da ters elemanı olduğunu gösterelim:

$$\begin{aligned}(h,k)(\varphi_{k^{-1}}(h)^{-1}, k^{-1}) &= (h\varphi_k(\varphi_{k^{-1}}(h)^{-1}), kk^{-1})\\ &= (h\varphi_k(\varphi_{k^{-1}}(h))^{-1}, 1)\\ &= (h(\varphi_k\varphi_{k^{-1}})(h)^{-1}, 1)\\ &= (h\varphi_{kk^{-1}}(h)^{-1}, 1)\\ &= (h\varphi_1(h)^{-1}, 1)\\ &= (h\,\mathrm{Id}(h)^{-1}, 1)\\ &= (hh^{-1}, 1)\\ &= (1,1).\end{aligned}$$

Yukarıda inşa ettiğimiz $H \times K$ grubuna H ve K'nın (bu sırayla) φ'ye göre ***yarıçarpımı*** adı verilir ve bu grup $H \rtimes_\varphi K$ olarak yazılır. φ fonksiyonu hep Id_H değerini alan sabit fonksiyon olduğunda bildiğimiz $H \times K$ kartezyen çarpım grubunu elde ederiz, yani direkt çarpım yarıdirekt çarpımın özel bir halidir.

$G = H \rtimes_\varphi K$ grubunun $H_1 = H \times \{1\}$ ve $K_1 = \{1\} \times K$ altkümelerine bakalım. Elbette $H_1 \cap K_1 = 1$ olur. Ayrıca $H_1, K_1 \leq G$ olduğu çarpımın tanımına bakınca bariz olmalı. $H_1 \lhd G$ olgusunu kanıtlamak da zor değil. $H_1K_1 = G$ eşitliği ise şu hesaptan çıkıyor:

$$(h,1)(1,k) = (h\varphi_1(1), 1 \cdot k) = (h,k). \tag{7}$$

Demek ki G'nin H_1 ve K_1 altgrupları (6)'yı sağlıyor.

$H \rtimes_\varphi K$ yarıçarpımında (eğer bir karışıklığa neden olmayacaksa) $(h,1)$ yerine de h, $(1,k)$ yerine de k yazılabilir; dolayısıyla (7)'den dolayı (h,k) yerine hk yazılabilir. Bu durumda çarpmayı

$$(hk)(h_1k_1) = hkh_1k^{-1}kk_1 = h\varphi_k(h_1)kk_1$$

olarak gösterebilriz. Ama tabii $1 \neq a \in H \cap K$ ise, $(1,a)$ elemanıyla $(a,1)$ elemanı farklı elemanlar olduğundan, bu elemanları a olarak göstermek yanlış olur; bu elemanları sırasıyla $1a$ ve $a1$ olarak göstermek gerekir ki bu yazım biçimi de kolaylıkla hataya yol açabilir. Bu durumda K'nın a elemanını a' gibi başka bir simgeyle göstermek düşünülebilir. Bir başka sorun da şu olabilir: H toplamsal, K çarpımsal bir grupsa $(hk)(h_1k_1) = hkh_1k^{-1}kk_1 = h\varphi_k(h_1)kk_1$ yerine

$$(hk)(h_1k_1) = (h + kh_1k^{-1})kk_1 = (h + \varphi_k(h_1))kk_1$$

yazmak gerekir, ki bu yazım da tecrübesiz biri için kafa karıştırıcı olabilir. Sonuç olarak hk yazılımı kolaylıklar sağlasa da tehlikesiz değildir, dikkatle kullanılmalı. Matris çarpımını bilen biri (h,k) elemanını

$$\begin{pmatrix} k & h \\ 0 & 1 \end{pmatrix}$$

olarak görürse, H'nin toplamsal bir grup olduğu durumlarda çarpım çok daha kolay biçimde akla yerleşebilir:

$$\begin{pmatrix} k & h \\ 0 & 1 \end{pmatrix} \begin{pmatrix} k_1 & h_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} kk_1 & kh_1 + h \\ 0 & 1 \end{pmatrix};$$

ama tabii burada kh_1 çarpımı $\varphi_k(h_1)$ olarak düşünülmeli. Okur bu aşamada Örnek 12.23'e göz atabilir.

Artık teoremi yazabiliriz:

Teorem 12.15. *H ve K birer grup ve $\varphi : K \longrightarrow \operatorname{Aut} H$ bir homomorfi olsun. $\varphi(k)$ yerine φ_k yazalım. O zaman,*

$$(h,k)(h_1,k_1) = (h\varphi_k(h_1), kk_1)$$

işlemi $G = H \times K$ kümesini ($H \rtimes_\varphi K$ olarak yazılan) bir gruba dönüştürür. Eğer $H_1 = H \times \{1\}$ ve $K_1 = \{1\} \times K$ tanımlarını yaparsak, G'nin bu altkümeleri (6)'yı sağlarlar.

Aksine, bir G grubu ve G'nin (6)'yı sağlayan H ve K altgrupları verilmiş olsun. O zaman bir $\varphi : K \longrightarrow \operatorname{Aut} H$ homomorfisi için $G \simeq H \rtimes_\varphi K$ olur. Burada φ homomorfisini her $k \in K$ ve $h \in H$ için $(\varphi(k))(h) = khk^{-1}$ olarak alabiliriz. □

Ama dikkat, iki farklı φ ve ψ için $H \rtimes_\varphi K \simeq H \rtimes_\psi K$ olabilir. Alıştırmalarda buna örnek göstereceğiz.

Eğer φ'nin ne olduğu belliyse ya da önemi yoksa, o zaman $H \rtimes_\varphi K$ yerine $H \rtimes K$ yazılır.

$H \leq G$ olsun. Eğer bir $K \leq G$ için $G = H \rtimes K$ oluyorsa, K'nın H'nin bir ***tümleyeni*** olduğu söylenir; H'nin de G'de ***ayrıştığı*** söylenir.

Notlar ve Örnekler

12.12. $H \times K$ grubunun bir yarıçarpım olduğunu söylemiştik. Bunun için $H \rtimes_\varphi K$ grubunun inşasında her $k \in K$ için $\varphi_k = \mathrm{Id}_H$ almak yeterli.

12.13. H herhangi bir abel grubu olsun. H'nin τ otomorfisi her $h \in H$ için $\tau(h) = h^{-1}$ formülüyle verilsin. $K = \{\mathrm{Id}_H, \tau\}$ olsun. $\varphi : K \longrightarrow \operatorname{Aut} H$ doğal gömme fonksiyonu olsun. Böylece $H \rtimes_\varphi K$ grubu elde ederiz. Grubun elemanlarını $h \in H$ ve $\epsilon = 0, 1$ için $h\tau^\epsilon$ biçiminde yazabiliriz. Çarpma şu kuralla belirlenir:

$$\tau h = h^{-1}\tau.$$

Dolayısıyla

$$(h\tau^\epsilon)(h_1\tau^{\epsilon_1}) = (hh_1^{-\epsilon})\tau^{\epsilon+\epsilon_1}$$

olur. Ama tabii ayrıca $\tau^2 = 1$ olur.

Eğer $H = \mathbb{Z}/n\mathbb{Z}$ ise, elde edilen grubun D_{2n} dihedral grubuna izomorf olur.

12.14. Yukarıdaki alıştırmayı tersten ele alalım. $G = D_{2n}$ olsun. Önce bu grubun yapısını anımsayalım:

$$D_{2n} = \langle r, s : r^n = s^2 = 1,\ srs = r^{-1} \rangle.$$

Ya da şöyle:

$$D_{2n} = \{r^i s^\epsilon : i = 0, 1, \ldots n-1,\ \epsilon = 0, 1\}$$

ve çarpma $r^n = s^2 = 1$ ve $sr = r^{-1}s$ ilişkileriyle belirlenmiştir.

$R = \langle r \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ ve $S = \langle s \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ olsun. $[D_{2n} : R] = 2$ olduğundan, $R \lhd D_{2n}$ olur. Ama bunu şöyle de görebiliriz: $r \in R$ olduğundan r, R'yi normalize eder; $s^{-1}rs = srs = r^{-1}ss = r^{-1}$ olduğundan $s^{-1}r^i s = (s^{-1}rs)^i = (r^{-1})^i = r^{-i}$ olur ve dolayısıyla s de R'yi normalize eder; hem r hem de s tarafından normalize edilen R, $D_{2n} = \langle r, s \rangle$ tarafından da normalize edilir.

(6)'daki her şey sağlanmıştır, dolayısıyla $D_{2n} = R \rtimes S$ olur. S'nin 1'den farklı elemanı R'nin elemanlarını eşleniklik altında ters çevirdiğinden, bu aynen bir önceki örnektir.

12.15. $G = \operatorname{Sym} 3$ olsun. $H = \{\mathrm{Id}_3, (1\ 2\ 3), (1\ 3\ 2)\} \simeq \mathbb{Z}/3\mathbb{Z}$ ve $K = \{\mathrm{Id}_2, (1\ 2)\} \simeq \mathbb{Z}/2\mathbb{Z}$ olsun. O zaman $G = H \rtimes K$ olur. Bu örneğin bir önceki örneğin $n = 3$ durumu olduğu gözden kaçmasın.

12.16. $G = \operatorname{Sym} n$ olsun. Teorem 3.2'ye göre

$$K = \{\mathrm{Id}_4, (1\ 2)\}$$

için, $G = \operatorname{Alt} n \rtimes K$ olur.

12.17. $\operatorname{Alt} 4$ altgrubunun kendisi de başka altgrupların yarıçarpımıdır. Nitekim,

$$H_1 = \{\mathrm{Id}_4, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

ve

$$K_1 = \langle (1\ 2\ 3) \rangle$$

ise $\operatorname{Alt} 4 = H_1 \rtimes K_1$ olur. Okur bunun neden böyle olduğunu kanıtlayabilir ama sanırız bir sonraki örnek buna ve bundan önceki örneklerin hepsine birden açıklık getirecek.

12.18. $H \lhd G$ olsun. $[G : H] = p$ bir asal olsun. $G \setminus H$ kümesinde derecesi p olan bir k elemanının olduğunu varsayalım. O zaman $\langle k \rangle \cap H = 1$ olmak zorundadır (bkz. Örnek 5.31) ve dolayısıyla $G = HK$ olur. Bu durumda $G = H \rtimes K$ olur. Yukarıdaki her yarıçarpım örneği bu olgunun bir sonucudur.

12.19. $\alpha = (1\ 2\ 3)$, $\beta = (4\ 5\ 6) \in \operatorname{Sym} 6$ olsun. Bu iki eleman $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ grubuna izormorf bir altgrup üretirler. $\gamma = (1\ 4)(2\ 5)(3\ 6)$ olsun. $\langle \gamma \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ ve $\alpha^\gamma = \beta$ ve $\beta^\gamma = \alpha$ olur. Demek ki γ elemanı $\langle \alpha, \beta \rangle$ altgrubunu normalize eder.

$$G = \langle \alpha, \beta, \gamma \rangle = \langle \alpha, \beta \rangle \rtimes \langle \gamma \rangle \simeq (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$$

olur.

$$(\alpha\beta^{-1})^\gamma = (\alpha\beta^{-1})^{-1} \text{ ve } (\alpha\beta)^\gamma = \alpha\beta$$

olduğundan,

$$G = \langle \alpha\beta^{-1} \rangle \rtimes \langle \gamma \rangle \oplus \langle \alpha\beta \rangle \simeq \operatorname{Sym} 3 \times \mathbb{Z}/3\mathbb{Z}$$

olur. Ayrıntıları okura bırakıyoruz.

12.20. Yukarıdaki örneği kolaylıkla çeşitlendirebiliriz: $\alpha = (1\ 2\ 3)$, $\beta = (4\ 5\ 6)$, $\gamma = (7\ 8\ 9) \in \operatorname{Sym} 9$ olsun. Bu elemanlar $H \simeq (\mathbb{Z}/3\mathbb{Z})^3$ grubunu üretirler. Şimdi H grubunun bu üreteçlerini eşleniklik etkisiyle karan, dolayısıyla H'yi normalize eden şu elemana bakalım: $\sigma = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$. Kolaylıkla görüleceği üzere,

$$G = \langle \alpha,\ \beta,\ \gamma,\ \sigma \rangle = \langle \alpha,\ \beta,\ \gamma \rangle \rtimes \langle \sigma \rangle \simeq (\mathbb{Z}/3\mathbb{Z})^3 \rtimes \mathbb{Z}/3\mathbb{Z}$$

olur.

$$C_G(\sigma) = \langle \alpha\beta\gamma,\ \sigma \rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

olduğunun kanıtını okura bırakıyoruz.

12.21. G bir grup olsun. $\operatorname{Inn} : G \longrightarrow \operatorname{Aut} G$ homomorfisini anımsayalım: $\operatorname{Inn}_g(x) = gxg^{-1}$. Böylece $G \rtimes_{\operatorname{Inn}} G$ grubunu elde ederiz. Bu grubun elemanları $G \times G$ kümesinin elemanlarıdır ve çarpım şöyle yapılır:

$$(g, h)(x, y) = (g \operatorname{Inn}_h(x), hy) = (ghxh^{-1}, hy).$$

12.22. G bir grup, $n > 0$ bir doğal sayı olsun. G^n grubunun elemanlarının koordinatlarını belli bir $\sigma \in \operatorname{Sym} n$ elemanına göre değiştirmek G^n grubunun bir otomorfisini verir:

$$\tilde{\sigma}(g_1, \ldots, g_n) = (g_{\sigma(1)}, \ldots, g_{\sigma(1)}).$$

Böylece $\operatorname{Sym} n \longrightarrow \operatorname{Aut} G^n$ ve bu sayede $G^n \rtimes \operatorname{Sym} n$ elde ederiz. Eğer $H \leq \operatorname{Sym} n$ ise, $G^n \rtimes H$ grubu da aynı yöntemle tanımlanır. Tabii burada $\{1, \ldots, n\}$ kümesi için yapılan sonlu ya da sonsuz herhangi bir X kümesi için de yapılabilir; o zaman her $H \leq \operatorname{Sym} X$ için $\left(\bigoplus_{x \in X} G_x\right) \rtimes H$ ve $\left(\prod_{x \in X} G_x\right) \rtimes H$ gruplarını elde ederiz.

12.23. p bir asal, $K = \mathbb{Z}/p\mathbb{Z}$ ve $K^\star = \mathbb{Z}/p\mathbb{Z}\setminus\{0\}$ olsun. K toplama altında, $K^\star$ çarpma altında bir gruptur[3]. Her $k = 1, \ldots, p-1$ için $\varphi_k(x) = kx$ formülü bir $\varphi_k : K \longrightarrow K$ otomorfisi verir ve $\varphi : K^\star \longrightarrow \operatorname{Aut} K$ bir grup homomorfisidir. Böylece $K \rtimes_\varphi K^\star$ grubunu elde ederiz. Çarpma şöyledir:

$$(x, y)(z, t) = (x + yz, yt).$$

Matrisleri bilenler, bu grubun

$$\left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} : x \in K,\, y \in K^\star \right\}$$

grubu olduğunu farkedeceklerdir.

Şimdi bu örneği biraz değiştirelim. $\alpha_i : x \mapsto x^i$ formülü $K^\star$ grubunun bir andomorfisini verir. Dolayısıyla $\varphi_i = \varphi \circ \alpha_i : K^\star \longrightarrow \operatorname{Aut} K$ bir grup homomorfisidir. Böylece $K \rtimes_{\varphi_i} K^\star$ grubunu elde ederiz. Çarpma bu sefer şöyledir:

$$(x, y)(z, t) = (x + y^i z, yt).$$

Eğer $i = 1$ ise bir önceki örneği elde ederiz. Eğer $i = 0$ ise direkt çarpımı elde ederiz. Buradaki i'leri $\{0, 1, \ldots, p-2\}$ arasından seçmek yeterlidir, daha doğrusu i'yi modülo $p-1$ almak yeterlidir, çünkü her $y \in K^\star$ için Fermat'nın Küçük Teoremi'nden dolayı (Teorem 9.7) $y^{p-1} = 1$ olur.

$\psi_i : (x, y) \mapsto (x, y^i)$ fonksiyonu $K \rtimes_{\varphi_i} K^\star$ grubundan $K \rtimes_\varphi K^\star$ grubuna giden bir homomorfidir, nitekim

$$\psi_i((x, y)(z, t)) = \psi_i(x + y^i z, yt) = (x + y^i z, y^i t^i)$$

ve

$$\psi_i(x, y)\psi_i(z, t) = (x, y^i)(z, t^i) = (x + y^i z, y^i t^i)$$

olur. Daha genel olarak, $\psi_i : (x, y) \mapsto (x, y^i)$ fonksiyonu $K \rtimes_{\varphi_{ij}} K^\star$ grubundan $K \rtimes_{\varphi_j} K^\star$ grubuna giden bir homomorfidir. Bu homomorfinin çekirdeği

$$\operatorname{Ker} \psi_i = \{(0, y) : y^i = 1\}$$

olur elbette. Demek ki ψ_i'nin bir izomorfi olması için $(i, p-1) = 1$ olmalıdır çünkü ancak bu durumda $\operatorname{Ker} \psi_i = \{(0, 1)\}$ olur. Demek ki eğer $i \in (\mathbb{Z}/(p-1)\mathbb{Z})^\star$ için $k = ij$ oluyorsa ψ_i, $K \rtimes_{\varphi_k} K^\star$ ile $K \rtimes_{\varphi_j} K^\star$ grupları arasında bir izomorfidir.

12.24. Her p asalı ve her $k \in \mathbb{N}$ için $(1 + p)^k \equiv 1 + pk \bmod p^2$ ve $(1 + pk)^p \equiv 1 \bmod p^2$ olur. Binom açılımını kullanarak bu eşitlikleri kanıtlamak oldukça kolaydır. (Hatta eğer $p = 2$ ise $(1+pk)^p \equiv 1 \bmod p^3$ olur.) Dolayısıyla $\sigma_k(x) = (1+pk)x$ kuralıyla tanımlanmış fonksiyon $\mathbb{Z}/p^2\mathbb{Z}$ grubunun derecesi p olan bir otomorfisidir. Buradan eleman sayısı p^3 olan $\mathbb{Z}/p^2\mathbb{Z} \rtimes \langle\sigma_k\rangle$ grubunu elde ederiz. $k = 0, 1, \ldots, p-1$ alınabilir. Eğer $k = 0$ ise elde edilen grup $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ abel grubudur ama aksi halde grup abel değildir. Grubun işleminin açılımı şöyledir:

$$(\overline{a}, \hat{b})(\overline{c}, \hat{d}) = (\overline{a + (1 + pk)^b c}, \widehat{bd}).$$

Bu arada $\sigma_k = \sigma_1^k$ eşitliğine dikkatinizi çekeriz.

[3]Bilenler için: Bu örneğin bir kısmı herhangi bir K cismi için de geçerlidir. Mesela kk'yı $\mathbb{Q}$, $\mathbb{R}$ alabilirsiniz.

13. Abel Grupları

Bu bölümde amacımız en basit gruplar olarak addedilebilecek olan abel gruplarını anlamaya çalışmak. Grubu bazen çarpımsal yazılımla yazacağız çünkü genel olarak abel grupları abel olmayan grupların altgrupları olarak, yani çarpımsal yazılımla belirirler. Ama okur kanıtladığımız her sonucu çarpımsal dilden toplamsal dile çevirmelidir.

Ne yazık ki Abel gruplarını sınıflandırmak mümkün değildir; konu matematiğin temelleriyle ve kümeler kuramının kabul edilen aksiyomlarıyla yakın ilişkidedir. Tüm abel grupları sınıflandıramasak da birçok abel grubunu sınıflandıracağız, sonlu ya da bölünür abel gruplarını mesela. Hatta çok daha fazlasını yapacağız. Bazen Zorn Önsavı'nı kullanmak zorunda kalacağız. İhtiyacı olan okur için kitabın ekinde Zorn Önsavı'na uzunca bir yer ayırdık.

Burada kanıtlananların hepsi çok daha genel bir kapsamda (tek üreteçli bölgeler üzerine modüller kapsamında) ve aynı yöntemlerle kanıtlanabilir ve daha sonraki ciltlerde kanıtlayacağız. Ama okurları o kadar bekletmenin doğru olmayacağını düşündük.

Her ne kadar bu kitabın varsayımı değilse de temel lineer cebir bilgisi olan bir okur, bu bölümü çok daha rahat okuyacaktır. (Öte yandan bu kitabın okurunun, hele hele kitabın bu aşamasına kadar gelebilmiş bir okurun temel lineer cebir bildiği de bir başka gerçektir.) Gelecekte bu kitapta bu bölüme esaslı bir biçimde ihtiyacımız olmayacağından okur ilk okuyuşta bu bölümü atlayabilir.

13.1 Serbest Abel Grupları

13.1.1 $\mathbb{Z}$'nin Direkt Toplamları

$\oplus_I \mathbb{Z}$ grupları, tabiri caizse, diğer tüm abel gruplara tepeden bakan gruplardır çünkü bu gruplardan tüm abel gruplarına giden ve istediğimiz tüm makul değerleri alan homomorfiler bulmak mümkündür. Bunun nedeni de $\oplus_I \mathbb{Z}$ grubunda $xy = yx$ dışında, daha doğrusu $x+y = y+x$ dışında elemanlar arasında hiçbir ilişki bulunmamasıdır. (Hatırlarsanız bir grupta elemanlar arasında ne kadar çok ilişki varsa, o gruptan başka gruplara giden homomorfiler bulmak o kadar zordur.)

En basit örnekten başlayalım; I'nın sadece bir elemanı olsun, yani bu tür grupların en basiti olan $\mathbb{Z}$ grubuna bakalım. Rastgele bir G grubu ve bu G grubundan rastgele bir eleman seçelim. O zaman $\mathbb{Z}$'den G'ye giden ve $\mathbb{Z}$'nin 1 elemanını G'nin g elemanına götüren bir ve bir tane homomorfi vardır. 1'i g'ye götürdüğüne göre, bu homomorfinin n tamsayısını g^n elemanına götürmekten başka çaresi yoktur, yani homomorfi

$$n \mapsto g^n$$

kuralıyla belirlenir. Sonuç olarak, G'de ne kadar eleman varsa $\mathbb{Z}$'den G'ye giden o kadar homomorfi vardır. Bunu Örnek 10.17'da da görmüştük.

Şimdi işler biraz daha zorlaşsın, bu sefer I'da iki eleman olsun, yani $\mathbb{Z} \times \mathbb{Z}$ grubunu ele alalım. $e_1 = (1,0)$ ve $e_2 = (0,1)$ tanımlarını yapalım. $\mathbb{Z} \times \mathbb{Z}$ grubunun her elemanı bir ve bir tane n, m tamsayı çifti için $ne_1 + me_2$ olarak yazılır, nitekim,

$$(n,m) = (n,0) + (0,m) = n(1,0) + m(0,1) = ne_1 + me_2$$

olur. Dolayısıyla eğer $\varphi : \mathbb{Z} \oplus \mathbb{Z} \longrightarrow G$ bir homomorfiyse,

$$\varphi(n,m) = \varphi(ne_1 + me_2) = \varphi(e_1)^n \varphi(e_2)^m \tag{1}$$

olmak zorundadır. (G grubunu gene çarpımsal aldık; toplamsal alsaydık (1) yerine $\varphi(n,m) = n\varphi(e_1) + m\varphi(e_2)$ yazardık.) Yani $\varphi(n,m)$ elemanı $\varphi(e_1)$ ve $\varphi(e_2)$ elemanları tarafından belirlenmiştir. Ama $\varphi(e_1)$ ve $\varphi(e_2)$ elemanları rastgele olamazlar, çünkü $e_1 + e_2 = e_2 + e_1$ olduğundan,

$$\varphi(e_1)\varphi(e_2) = \varphi(e_2)\varphi(e_1) \tag{2}$$

eşitliği sağlanmak zorunda, yani $\varphi(e_1)$ ve $\varphi(e_2)$ elemanları birbirleriyle değişmeli. Şimdi soru şu: Birbiriyle değişen her $g_1, g_2 \in G$ elemanı için, (1) kuralı bir $\varphi : \mathbb{Z} \oplus \mathbb{Z} \longrightarrow G$ homomorfisi tanımlar mı? Yanıt olumludur. (1) formülünün gerçekten bir homomorfi tanımladığını görmek zor değil. Birazdan daha genelini yapacağız.

En genel durumu ele alalım. I rastgele bir göstergeç kümesi olsun. I sonlu da olabilir sonsuz da. $A = \oplus_I \mathbb{Z}$ olsun. Her $j \in I$ için $e_j \in A$ elemanı, j'inci terim (ya da koordinat) dışında her terimi 0 olan ve j'inci terimi 1 olan eleman olsun. Eğer

$$\delta_{i,j} = \begin{cases} 1 & \text{eğer } i = j \text{ ise} \\ 0 & \text{eğer } i \neq j \text{ ise} \end{cases}$$

tanımını yaparsak (Kronecker delta sembolü),

$$e_j = (\delta_{j,i})_i$$

olur. Eğer I sonlu bir kümeyse ya da $\mathbb{N}$ ise, e_j elemanlarını

$$(0, 0, \ldots, 0, 1, 0, \ldots)$$

olarak çok daha anlaşılır bir biçimde gösterebilirdik. (Burada j'inci bileşen 1, diğerleri 0'dır.) Ama I kümesi çok çok vahşi bir küme olabilir, örneğin $\mathbb{R}$'nin altkümeleri kümesinin sonlu altkümelerinden $\mathbb{Z}$'ye giden fonksiyonlardan oluşan küme olabilir; o zaman I'nın elemanlarını makul bir yöntemle sıralamak mümkün olmaz. Bu durumları es geçmemek için $e_j = (\delta_{j,i})_i$ gösterimini kullanacağız. Bu tanımla A'nın her a elemanı

$$a = \sum_{i \in I} a_i e_i$$

olarak tek bir biçimde yazılır. Bu toplamdaki a_i'ler birer tamsayıdır ve sadece sonlu tanesi 0'dan farklıdır, yani aslında yukarıdaki toplam sonlu bir toplamdır.

Şimdi G herhangi bir grup olsun ve her $i \in I$ için G'den bir g_i elemanı seçelim. Her $i, j \in I$ için $g_i g_j = g_j g_i$ varsayımını yapalım. Mesela g_i'lerin hepsi aynı elemansa bu eşitlik sağlanır. Şimdi

$$\varphi : A \longrightarrow G$$

fonksiyonunu

$$\varphi\left(\sum_i a_i e_i\right) = \prod_i g_i^{a_i} \tag{3}$$

formülüyle tanımlayalım. Bu formülün gerçekten bir fonksiyon tanımladığı belli:

a. Eğer $a_i = 0$ ise $g_i^{a_i} = 1$ olduğundan ve sadece sonlu sayıda i için $a_i \neq 0$ olduğundan, sağdaki çarpımda sonlu sayıda terim çarpılmaktadır, yani sağdaki çarpma anlamlıdır[1].

b. $\oplus_I \mathbb{Z}_i$ grubunun her eleman tek bir biçimde $\sum_i a_i e_i$ olarak yazılabilir, yani $\sum_i a_i e_i = \sum_i b_i e_i$ ise $a_i = b_i$ olmak zorundadır; dolayısıyla $f(a)$ değerini bulmak için önce a'yı $\sum_i a_i e_i$ olarak (tek bir biçimde) yazıp, sonra 0 olmayan sonlu sayıdaki a_i için G grubunun $g_i^{a_i}$ elemanlarını hesaplayıp, bu elemanları çarpmak yeterli; üstelik çarpmayı herhangi bir sırada yapabiliriz, çünkü g_i'ler birbirleriyle değişiyorlar.

Bu uzun açıklamalardan, φ fonksiyonunun tanımlı olduğu anlaşılıyor. Ve elbette her $i \in I$ için $\varphi(e_i) = g_i$ olur. Şimdi φ'nin bir homomorfi olduğunu

[1] Mesela aynı fonksiyonu, sonsuz sayıda $i \in I$ için $g_i \neq 1$ ise ve G'de sonsuz sayıda elemanın çarpımını tanımlayacak (metrik gibi) bir aygıt yoksa, $\prod_I \mathbb{Z}_i$ grubu üzerinde tanımlayamazdık.

kanıtlayalım. A'dan a ve b elemanları alalım. Amacımız $\varphi(a+b)=\varphi(a)\varphi(b)$ eşitliğini kanıtlamak. Bu elemanları $(e_i)_i$ cinsinden yazalım, diyelim hemen hemen her terimi 0 olan[2] $(a_i)_i$ ve $(b_i)_i$ tamsayı dizileri için

$$a=\sum_i a_i e_i \text{ ve } b=\sum_i b_i e_i.$$

O zaman

$$a+b=\sum_i (a_i+b_i)e_i$$

olur. Şimdi

$$\varphi(a+b)=\varphi\left(\sum_i (a_i+b_i)e_i\right)=\prod_i g_i^{a_i+b_i}=\prod_i g_i^{a_i}g_i^{b_i}$$

olur. Ama $g_ig_j=g_jg_i$ olduğundan, sağdaki çarpımı

$$\prod_i g_i^{a_i}\prod_i g_i^{b_i}=\varphi(a)\varphi(b)$$

olarak yazabiliriz. Demek ki gerçekten de $\varphi(a+b)=\varphi(a)\varphi(b)$ imiş, yani φ gerçekten bir homomorfi imiş.

13.1.2 Taban

Yukarıda yaptıklarımız üzerine biraz durup düşünelim. φ'nin varlığı için A'nın e_i elemanlarını kullandık. Aslında A'nın e_i elemanlarını değil, bu elemanların bazı özelliklerini kullandık. O özellikler de şunlardı:

a. A grubunun her elemanı $\sum_i a_ie_i$ biçiminde yazılabilir, yani $\{e_i : i\in I\}$ kümesi A grubunu üretir.

b. $\sum_i a_ie_i=\sum_i b_ie_i$ eşitliği ancak (ve ancak) her $i\in I$ için $a_i=b_i$ ise doğrudur. Bunun eşdeğer bir biçimi şöyledir: $\sum_i c_ie_i=0$ eşitliği ancak ve ancak her $i\in I$ için $c_i=0$ ise mümkündür.

Üreteç Kümeleri. Bir A grubunun birinci özelliği sağlayan bir $\{e_i : i\in I\}$ altkümesine A'nın ***üreteç kümesi*** dendiğini biliyoruz. $\sum_i a_ie_i$ biçiminde bir ifadeye e_i'lerin (üreteçlerin) ***doğrusal kombinasyonu*** adı verilir. Demek ki A'nın her elemanı üreteç kümesinin bir kombinasyonudur. Eğer $E\subseteq A$ bir üreteç kümesiyse ve $E\subseteq F\subseteq A$ ise, F de elbette bir üreteç kümesidir. $a=a$ eşitliğinden dolayı (!) A bariz biçimde A'nın üreteç kümesidir. Dolayısıyla büyük üreteç kümeleri bulmak zor değildir, marifet küçük üreteç kümeleri bulmaktır ya da bulunmuş bir üreteç kümesini olabildiğince küçültmektir. Üreteç

[2] "Hemen hemen her terim" sözleri, aksi söylenmedikçe "sonlu sayıda her terim" anlamına gelmektedir.

kümeleri hakkında bir önemli not: Eğer E, A'nın bir üreteç kümesiyse ve E'nin her elemanı $F \subseteq A$ kümesinin bir doğrusal kombinasyonuysa, o zaman F de A'nın bir üreteç kümesidir (bkz. Alıştırma 7.30).

Bağımsız Kümeler. İkinci özelliği sağlayan bir $\{e_i : i \in I\}$ altkümesine A'nın ***doğrusal bağımsız*** ya da $\mathbb{Z}$-***bağımsız*** ya da daha kısa olarak sadece ***bağımsız*** altkümesi denir. Bir $\{e_i : i \in I\}$ altkümesinin bağımsız olduğunu göstermek için $\sum_i c_i e_i = 0$ varsayımı yapılıp her $i \in I$ için $c_i = 0$ eşitliği kanıtlanır. Eğer $E \subseteq A$ bağımsız bir altkümeyse, E'nin altkümeleri de bağımsız altkümelerdir. $\emptyset$ bağımsız bir altkümedir, çünkü bağımlılığa yol açacak elemanı yoktur. Dolayısıyla küçük bağımsız altkümeler bulmaktan ziyade büyük bağımsız altkümeler bulmak marifettir. Bağımsız kümeler hakkında basit ama önemli bir olgu: İçinde 0 elemanı olan bir küme bağımsız olamaz. Son bir not: Bağımsız bir altkümenin bir elemanı altkümenin diğer elemanlarının doğrusal kombinasyonu olamaz.

$\mathbb{Z}$ grubunun $\{2\}$ kümesi bağımsızdır ama $\mathbb{Z}$'yi üretmez. Öte yandan $\{1\}$ kümesi hem bağımsızdır hem de $\mathbb{Z}$'yi üretir. Aynı şekilde $\{-1\}$ kümesi hem bağımsızdır hem de $\mathbb{Z}$'yi üretir. Ama $\mathbb{Q}$ grubunun $\{1\}$ kümesi $\mathbb{Q}$ grubunu üretmez. Hatta $\mathbb{Q}$'nün sonlu sayıda üreteci yoktur, çünkü paydalar yeterince büyüyemez.

Taban. Bir A grubunun bağımsız olan bir üreteç kümesine ***taban*** adı verilir. Eğer T bir tabansa ve $S \subset T \subset U \subseteq A$ ise, ne S ne de U bir taban olabilir, çünkü S artık üreteç kümesi değildir ve U bağımsız olamaz.

Eğer T bir serbest abel grubunun tabanıysa, bazen T'nin abel grubunu ***serbestçe ürettiği*** söylenir. Serbestçe üretilmek kavramından Altaltbölüm 13.1.6'da daha etraflıca sözedeceğiz.

Alıştırmalar

13.1. $A = \mathbb{Z}^{(\mathbb{N})}$ olsun. Her $n \in \mathbb{N}$ için $e_n \in A$ metindeki gibi olsun. $\varphi : A \longrightarrow \mathbb{Q}$ homomorfisi $\varphi(e_n) = 1/n!$ eşitlikleriyle tanımlansın. φ'nin örten olduğunu kanıtlayın. $\operatorname{Ker}\varphi$'nin üreteçlerini bulun. Demek ki $A/\operatorname{Ker}\varphi \simeq \mathbb{Q}$.

13.2. $A = \bigoplus_{n=1}^{\infty} \mathbb{Z}$ olsun. Her $n \geq 1$ için $e_n \in A$ metindeki gibi olsun.

$$B = \langle ne_n - e_1 : n \geq 1 \rangle$$

tanımını yapalım. A/B grubunun bölünür olduğunu kanıtlayın. A/B grubu $\mathbb{Q}$ grubuna izomorf mudur?

13.1.3 Serbest Abel Grupları

Tabanı olan bir abel grubuna ***serbest abel grubu*** adı verilir. Demek ki $\mathbb{Z}^{(I)}$ grubu serbest bir abel grubu ve metinde tanımladığımız $\{e_i : i \in I\}$ kümesi bu grubun bir tabanı. Bu tabana A grubunun ***doğal tabanı*** denir. Birazdan her serbest abel grubunun bir I kümesi için $\oplus_I \mathbb{Z}$ grubuna izomorf olduğunu kanıtlayacağız.

$\oplus_\emptyset \mathbb{Z} = 0$ olduğundan, tanıma göre 0 grubu serbest bir abel grubudur ve $\emptyset$, 0'ın bir tabanıdır. $\mathbb{Z}$ serbest abel grubunun iki farklı tabanı vardır: $\{1\}$ ve $\{-1\}$; başka da yoktur. Ama bu iki serbest abel grubu dışında, her serbest abel grubunun sonsuz sayıda tabanı vardır. Örnekler aşağıda. Birazdan bir serbest abel grubunun tabanının eleman sayısının değişmediğini kanıtlayacağız.

Notlar ve Örnekler

13.3. $e_1 = (1, 0)$ ve $e_2 = (0, 1)$ elemanları $\mathbb{Z} \oplus \mathbb{Z}$ grubunun bir tabanı olduğu gibi,

$$f_1 = (1, 1) \text{ ve } f_2 = (2, 1)$$

elemanları da aynı grubun bir tabanıdır. Nitekim her $(x, y) \in \mathbb{Z} \oplus \mathbb{Z}$ elemanı

$$(x, y) = (2y - x)f_1 + (x - y)f_2$$

olarak yazılır. Demek ki f_1 ve f_2 elemanları $\mathbb{Z} \oplus \mathbb{Z}$ grubunu üretiyorlar. Ayrıca eğer

$$xf_1 + yf_2 = (0, 0)$$

ise, o zaman

$$(0, 0) = xf_1 + yf_2 = x(1, 1) + y(2, 1) = (x, x) + (2y, y) = (x + 2y, x + y),$$

yani

$$\begin{array}{rcl} x + 2y & = & 0 \\ x + y & = & 0 \end{array}$$

olur. Bu sistemin de yegâne çözümü $x = y = 0$'dır.

13.4. $f_1 = (2, 1)$, $f_2 = (3, 6)$ elemanları $\mathbb{Z} \oplus \mathbb{Z}$ grubunu üretmezler, çünkü

$$xf_1 + yf_2 = (2x + 3y, x + 6y)$$

elemanlarının koordinatlarının toplamı

$$(2x + 3y) + (x + 6y) = 3x + 9y$$

sayısıdır ve bu toplam her zaman 3'e bölünür. Demek ki koordinatlarının toplamı 3'e bölünmeyen bir eleman f_1 ve f_2 cinsinden yazılamaz. Öte yandan $\{f_1, f_2\}$ bağımsız bir kümedir. Bunun kolay kanıtını okura bırakıyoruz.

13.5. $f_1 = (4, 2)$ ve $f_2 = (6, 3)$ ise, $\{f_1, f_2\}$ bağımsız bir küme değildir, f_1 ile f_2 arasında

$$3f_1 + (-2)f_2 = 0$$

ilişkisi vardır.

13.6. $\oplus_{\mathbb{N}} \mathbb{Z}$ kümesinin doğal tabanını (aynen metindeki gibi) $e_0, e_1, e_2, \ldots$ olarak gösterelim. $i = 1, 2, \ldots$ için

$$f_i = (1, 1, \ldots, 1, 0, 0, \ldots) = e_0 + \ldots + e_{i-1}$$

elemanlarını tanımlayalım. (Burada i tane 1 vardır.) $e_0 = f_1$ ve $i \geq 1$ için

$$e_i = f_{i+1} - f_i$$

olduğundan, $(f_i)_i$ ailesi de bir tabandır.

Alıştırmalar

13.7. $A = \mathbb{Z}^3$ olsun. Herhangi bir a, b, $c \in \mathbb{Z}$ için (a, b, c), (b, c, a) ve (c, a, b) elemanlarının bağımsız olamayacaklarını gösterin.

13.8. $(1, 3)$ ve $(2, 2)$ elemanlarının $\mathbb{Z}^2$'nin bir tabanı olduğunu gösterin.

13.9. $(1, 3)$ ve $(5, 3)$ elemanlarının $\mathbb{Z}^2$'yi üretemeyeceğini gösterin.

13.10. $\mathbb{Z}^2$ grubunun (a, b) ve (c, d) elemanlarının bağımsız olmaları için $ad - bc \neq 0$ koşulunun yeter ve gerek olduğunu kanıtlayın.

13.11. (a, b) ve (c, d) elemanlarının $\mathbb{Z}^2$ grubunu üretmeleri için $e_1 = (1, 0)$ ve $e_2 = (0, 1)$ elemanlarının bu iki eleman cinsinden yazılmalarının yeter ve gerek koşul olduğunu kanıtlayın.

13.12. (a, b) ve (c, d) elemanlarının $\mathbb{Z}^2$ grubunu üretmeleri için $ad - bc = \pm 1$ eşitliğinin yeter ve gerek koşul olduğunu kanıtlayın.

13.13. $(e_n)_{n\in\mathbb{N}}$ ailesi $\oplus_{\mathbb{N}}\mathbb{Z}$ grubunun bir tabanı olsun. $a \in \prod_{\mathbb{N}} \mathbb{Z}$ elemanı her koordinatı 1 olan eleman olsun. $\{e_n : n \in \mathbb{N}\} \cup \{a\}$ kümesinin $\prod_{\mathbb{N}} \mathbb{Z}$ grubunun bağımsız bir altgrubu olduğunu kanıtlayın. Bu küme tarafından üretilen grubun elemanlarını betimleyin.

13.14. A, $\prod_{\mathbb{N}} \mathbb{Z}$ kümesinin bir zaman sonra sabitleşen elemanlardan oluşan altkümesi olsun. Bu kümenin $\prod_{\mathbb{N}} \mathbb{Z}$ grubunun bir altgrubu olduğu bariz olmalı. Bu grubun serbest abel grubu olduğunu kanıtlayın ve grubun bir tabanını bulun.

13.1.4 Boyut

Şimdi tüm serbest abel gruplarının bir I için $\oplus_I\mathbb{Z}$ grubuna izomorf olduğunu kanıtlayalım. Daha sonra I'nın kardinalitesinin serbest abel grubunun bir değişmezi olduğunu göstereceğiz.

Teorem 13.1. *G bir serbest abel grubu olsun. G'nin bir tabanının kardinalitesi I ise[3] $G \simeq \mathbb{Z}^{(I)}$ olur.*

Kanıt: Toplamsal olarak yazacağımız G grubunun tabanını $(g_i)_{i\in I}$ olarak gösterelim. $A = \mathbb{Z}^{(I)}$ olsun. Her $i \in I$ için $e_i \in A$ elemanı metindeki gibi olsun. $(e_i)_{i\in I}$ ailesinin A grubunun bir tabanı olduğunu biliyoruz. Metindeki gibi, her $i \in I$ için $\varphi(e_i) = g_i$ eşitliğini sağlayan (yegâne) homomorfiyi tanımlayalım. Yani (3)'te (çarpımsal yazılımla) gösterdiğimiz üzere

$$\varphi\left(\sum_i a_i e_i\right) = \sum_i a_i g_i$$

olsun. $(g_i)_{i\in I}$ ailesi G'yi ürettiğinden φ örten olur. $(g_i)_{i\in I}$ ailesi bağımsız olduğundan φ birebirdir. Demek ki φ bir izomorfidir. İstediğimiz kanıtlanmıştır. □

Serbest abel grubunun bir tabanının kardinalitesi grubun bir değişmezidir. Şimdi bunu kanıtlayacağız.

Teorem 13.2. *Eğer $\mathbb{Z}^{(I)} \simeq \mathbb{Z}^{(J)}$ ise $|I| = |J|$ olur.*

[3]Kardinalitenin tanımını bilmeyen okur bunu "Eğer bir $(g_i)_{i\in I}$ ailesi G'nin bir tabanıysa" olarak okuyabilir.

Kanıt: $A = \mathbb{Z}^{(I)} \simeq \mathbb{Z}^{(J)}$ olsun. Örnek 10.120'e göre, $A/2A$ grubu hem $(\mathbb{Z}/2\mathbb{Z})^{(I)}$ hem de $(\mathbb{Z}/2\mathbb{Z})^{(J)}$ grubuna izomorf olur. Eğer $|I| < \infty$ ise, bundan

$$2^{|I|} = \left|(\mathbb{Z}/2\mathbb{Z})^{(I)}\right| = \left|(\mathbb{Z}/2\mathbb{Z})^{(J)}\right|$$

ve dolayısıyla $|I| = |J|$ çıkar[4]. Eğer J sonluysa aynı kanıt teoremi kanıtlar. Bundan böyle I ve J'nin sonsuz olduklarını varsayalım. $(e_i)_{i\in I}$, A'nın doğal tabanı olsun. $\mathbb{Z}^{(I)}$ ile $\mathbb{Z}^{(J)}$ arasındaki izomorfiyi kullanarak, A'da bir $(f_j)_{j\in J}$ tabanı bulabiliriz. Teorem 7.4'e göre $|I| = |J|$ olur. □

Yukarıdaki teorem sayesinde, serbest abel gruplarının tabanlarının aynı kardinalitede olduklarını anlıyoruz. Bu kardinaliteye grubun ***boyutu*** adı verilir ve eğer gruba A dersek, bu kardinalite $\dim A$ bazen de $\dim_{\mathbb{Z}} A$ olarak gösterilir.

13.1.5 Sonuçlar

Son derece basit ama aynı derecede güçlü bir sonuçla başlayalım:

Teorem 13.3. *G bir abel grubu ve $H \leq G$ olsun. G/H grubunun bir serbest abel grubu olduğunu varsayalım. O zaman H'nin (serbest) bir tümleyeni vardır, yani serbest bir $A \leq G$ altgrubu için $G = H \oplus A$ olur. Hatta eğer $e_i \in G$ için $\{\overline{e_i} : i \in I\}$ kümesi G/H bölüm grubunun herhangi bir tabanıysa, o zaman A'yı $\langle e_i : i \in I\rangle$ olarak alabiliriz; bu durumda $A = \langle e_i : i \in I\rangle = \oplus\mathbb{Z}e_i$ olur.*

Kanıt: G grubunu toplamsal alalım. $(e_i)_i$ ailesi önermedeki gibi seçilsin. $A = \langle e_i : i \in I\rangle = \sum_i \mathbb{Z}e_i$ olsun. Eğer $\sum_i n_i e_i \in H$ ise, $\sum n_i \overline{e}_i = 0$ olur ve dolayısıyla her i için $n_i = 0$ ve $\sum_i n_i e_i = 0$ olur. Demek ki $A \cap H = 0$. Bu yaptığımızdan ayrıca

$$A = \langle e_i : i \in I\rangle = \oplus_i \mathbb{Z}e_i$$

çıkar, çünkü eğer $\sum_i n_i e_i = 0$ ise $\sum_i n_i e_i \in H$ olur. Şimdi $G = H + A$ eşitliğini kanıtlayalım. $g \in G$ olsun. O zaman $(\overline{e_i})_{i\in I}$ ailesi G/H grubunu ürettiğinden, bir $a \in A$ elemanı için $\overline{g} = \overline{a}$, yani $g - a \in H$ olur. Buradan da $g \in a + H \subseteq A + H$ çıkar. □

Teoremde varlığı söylenen A altgrubunun genellikle biricik olmadığına dikkatinizi çekeriz.

Aşağıdaki sonuçla bu teorem arasında aslında bir fark yok, $H = \operatorname{Ker}\varphi$ alırsak, teoremden aşağıdaki kanıtı elde ederiz. Biz gene de kanıtı tekrarayacağız.

Sonuç 13.4. *G bir abel grubu, F serbest bir abel grubu ve $\varphi : G \longrightarrow F$ örten bir homomorfi olsun. O zaman bir $A \leq G$ altgrubu için $G = \operatorname{Ker}\varphi \oplus A$ olur.*

[4] Vektör uzaylarını bilen bir okur, bu argümanın $|I|$ sonsuz olduğunda da teoremi kanıtladığını görecektir.

Elbette $A \simeq G/\operatorname{Ker}\varphi = \varphi(G) = F$ olur, yani A da serbest bir abel grubudur. Hatta eğer $f_i \in F$ elemanları için $(f_i)_{i\in I}$, F'nin bir tabanıysa ve $e_i \in \varphi^{-1}(f_i)$ elemanları rastgele seçilmişlerse, o zaman A'yı $\langle e_i : i \in I\rangle$ olarak alabiliriz; bu durumda $A = \langle e_i : i \in I\rangle = \oplus\mathbb{Z}e_i$ olur. □

Kanıt: G grubunu toplamsal alalım. $(e_i)_i$ ailesi önermedeki gibi seçilsin. $A = \langle e_i : i \in I\rangle = \sum_i \mathbb{Z}e_i$ olsun. Eğer $\sum_i n_i e_i \in \operatorname{Ker}\varphi$ ise,

$$0 = \varphi(0) = \varphi\left(\sum n_i e_i\right) = \sum n_i \varphi(e_i) = \sum n_i f_i$$

olur. Dolayısıyla her i için $n_i = 0$ ve $\sum_i n_i e_i = 0$ olmak zorundadır. Demek ki $A \cap H = 0$. Bu yaptığımızdan ayrıca

$$A = \langle e_i : i \in I\rangle = \oplus_i \mathbb{Z}e_i$$

çıkar, çünkü eğer $\sum_i n_i e_i = 0$ ise $\sum_i n_i e_i \in \operatorname{Ker}\varphi$ olur. Şimdi $G = \operatorname{Ker}\varphi + A$ eşitliğini kanıtlayalım. $g \in G$ olsun. O zaman $n_i \in \mathbb{Z}$ için

$$\varphi(g) = \sum_i n_i f_i = \sum_i n_i \varphi(e_i) = \varphi\left(\sum_i n_i e_i\right),$$

yani

$$g - \sum_i n_i e_i \in \operatorname{Ker}\varphi$$

olur. Buradan da

$$g = \left(g - \sum_i n_i e_i\right) + \sum_i n_i e_i \in \operatorname{Ker}\varphi + A$$

çıkar. □

Sonuç 13.5. *G bir abel grubu, $H \leq G$ olsun. Eğer H ve G/H serbest gruplarsa, G de serbest bir gruptur. Hatta $(h_i)_{i\in I}$ ailesi H'nin bir tabanı, $(\overline{g_j})_{j\in J}$ ailesi G/H'nin bir tabanıysa, $\{h_i : i \in I\} \cup \{g_j : j \in J\}$ kümesi, G'nin bir tabanı olur. Yani $\dim G = \dim H + \dim G/H$ olur.* □

Notlar ve Örnekler

13.15. Yukarıdaki teoremi kullanarak şu olguyu kanıtlayacağız: *G bir grup, $\mathbb{Z} \simeq H \lhd G$ ve $G/H \simeq \mathbb{Z}$ olsun. O zaman öyle $a, b \in \mathbb{Z}$ vardır ki, her $g \in G$ bir ve bir tek $n, m \in \mathbb{Z}$ tamsayıları için $a^n b^m$ biçiminde yazılır. Ayrıca ya G bir abel grubudur ve dolayısıyla $\mathbb{Z} \oplus \mathbb{Z}$ grubuna izomorfiktir ya da $ba = a^{-1}b$ olur.*

Kanıt: Birinci önerme teoremden hemen çıkıyor: a'yi H'nin bir üreteci olarak alalım. $b \in G$ de, $\overline{b}$ elemanı G/H'nin üreteci olacak biçimde seçilsin. b elemanı, $h \mapsto h^b$ kuralıyla H'nin bir otomorfisine yol açar. Ama $H \simeq \mathbb{Z}$ olduğundan H'nin iki otomorfisi vardır: $h \mapsto h$ ve $h \mapsto h^{-1}$. Bu, istediğimizi verir. □

13.16. Bu örneğin oldukça aydınlatıcı olacağını düşünüyoruz, özellikle birazdan kanıtlayacağımız teoremlerin kanıtlarında ne kadar dikkatli olmamız gerektiği konusunda uyarıcı olacak. $\mathbb{Q}$ grubu serbest abel grubu değildir, çünkü $\mathbb{Q}$ bölünür oysa bir serbest abel grubu hiçbir doğal sayıya bölünemez. Öte yandan $\mathbb{Q}$ grubunu, her biri $\mathbb{Z}$'ye izomorfik A_n altgruplarının bileşimi olarak yazabiliriz. Nitekim,

$$A_n = \frac{1}{n!}\mathbb{Z}$$

olsun. Elbette, $A_n \simeq \mathbb{Z}$, $A_n \leq A_{n+1}$ ve $\bigcup_n A_n = \mathbb{Q}$ olur. Demek ki bir serbest abel grubu zincirinin bileşimi serbest olmayabiliyor.

Teorem 13.6. *Serbest abel gruplarının altgrupları da serbesttir ve altgrupların boyutları grubun boyutunu aşamaz.*

Kanıt: Önce teoremin 1 boyutlu serbest abel grupları için, yani $\mathbb{Z}$'ye izomorf gruplar için doğru olduğundan emin olalım: $\mathbb{Z}$'nin bir altgrubu $n\mathbb{Z}$ biçiminde olduğundan, teorem bu durumda bariz olmalı, nitekim eğer $n = 0$ ise altgrubun boyutu 0'dır, aksi halde 1'dir.

Şimdi A rastgele bir serbest abel grubu olsun. Diyelim bir α kardinali için $(a_\beta)_{\beta<\alpha}$ ailesi A'nın bir tabanı[5]. Her $\beta \leq \alpha$ için

$$A_\beta = \langle a_\gamma : \gamma < \beta \rangle$$

olsun. A_β, $|\beta|$ boyutlu serbest bir abel grubudur. Ayrıca $\beta_1 < \beta$ için $A_{\beta_1} < A_\beta$ olur ve her λ limit ordinali için (ve özellikle $\lambda = \alpha$ için) $A_\lambda = \bigcup_{\beta<\lambda} A_\beta$ olur.

Birinci Adım. *Eğer teorem A_γ için doğruysa $A_{\gamma+1}$ için de doğrudur. Ayrıca eğer $B \leq A_{\gamma+1}$ ise ama $B \not\leq A_\gamma$ ise, o zaman bir $b \in B$ elemanı için $B = (B \cap A_\gamma) \oplus \mathbb{Z}b$ olur. Bir başka deyişle $B \cap A_\gamma$ grubunu serbestçe üreten bir altkümeye en fazla bir eleman daha ekleyerek B'nin bir tabanını elde ederiz.*
Birinci Adımın Kanıtı: $B \leq A_{\gamma+1}$ olsun. Varsayıma göre $B \cap A_\gamma$ serbest bir gruptur ve boyutu $|\gamma|$ kardinalitesinden büyük değildir. Eğer $B \leq A_\gamma$ ise, sorun yok. Bundan böyle $B \not\leq A_\gamma$ varsayımını yapalım.

$$0 \neq B/(B \cap A_\gamma) \simeq BA_\gamma/A_\gamma \leq A_{\gamma+1}/A_\gamma = (A_\gamma \oplus \mathbb{Z}a_\gamma)/A_\gamma \simeq \mathbb{Z}$$

olduğundan, $B/(B \cap A_\gamma) \simeq \mathbb{Z}$ olur, dolayısıyla Sonuç 13.5'e göre, bir $b \in B \setminus (B \cap A_\gamma)$ için

$$B = (B \cap A_\gamma) \oplus \mathbb{Z}b$$

olur. Birinci adımın kanıtı tamamlanmıştır.

[5]Ordinal ve kardinalleri bilmeyen okur, teoremi ancak sayılabilir eleman tarafından üretilmiş serbest abel grupları için kanıtlayabilir. Sadece bu durumla ilgilenen okur, eğer grup n tane (sonlu sayıda) elemanla üretilmişse, $\alpha = \{0, 1, \ldots, n-1\}$ alabilir. Bu durumda kanıttaki ikinci adım (limit ordinal adımı) atlanabilir, çünkü gerek yoktur. Sayılabilir sonsuzlukta eleman tarafından üretilen serbest abel grubu için $\alpha = \mathbb{N}$ ve ikinci adımda $\lambda = \mathbb{N}$ alınmalı.

İkinci Adım. *λ bir limit ordinal olsun. Eğer teorem her A_β $(\beta < \lambda)$ için doğruysa A_λ için de doğrudur.*
İkinci Adımın Kanıtı: $B \leq A_\lambda$ olsun. Varsayıma göre, her $\beta < \lambda$ için

$$B_\beta = B \cap A_\beta$$

serbest bir gruptur ve boyutu $|\beta|$ kardinalitesinden büyük değildir. Ayrıca

$$B = \bigcup_{\beta<\lambda} B_\beta = \bigcup_{\beta<\lambda} (B \cap A_\beta)$$

olur. Ancak bu iki olgu ikinci adımın kanıtlanması için yeterli değildir (bkz. Örnek 13.16). Fazlasına ihtiyacımız var, şun kanıtlamamız gerekiyor: *Her $\beta < \lambda$ için öyle bir $X_\beta \subseteq B_\beta$ vardır ki, X_β, B_β'yı serbestçe üretir ve her $\gamma \leq \beta$ için $X_\gamma \subseteq X_\beta$ olur.* X_β'yı tümevarımla bulmak hiç zor değil: Eğer $\beta = \gamma + 1$ ise ve X_γ bulunmuşsa, Birinci Adım'da X_γ'ya en fazla bir eleman ekleyerek X_β'yı nasıl bulacağımızı göstermiştik. Eğer β bir limit ordinalse ve $\gamma < \beta$ için X_γ bulunmuşsa, $X_\beta = \bigcup_{\gamma<\beta} X_\gamma$ tanımını yapalım. X_γ kümeleri bağımsız olduğundan ve bağımlılık sadece sonlu sayıda elemanı bağladığından X_β da bağımsızdır (nitekim X_β'nın elli elemanı arasında doğrusal bir bağıntı varsa, bu elli eleman X_γ'lardan birinde olmalı.) X_β'nın B_β'yı ürettiğine gelince:

$$\langle X_\beta \rangle = \left\langle \bigcup_{\gamma<\beta} X_\gamma \right\rangle = \bigcup_{\gamma<\beta} \langle X_\gamma \rangle = \bigcup_{\gamma<\beta} B_\gamma = B_\beta$$

(Bkz. Alıştırma 7.52). Demek ki $B = B_\alpha$ grubu X_α tarafından üretilmiştir. X_α kümesinin eleman sayısının α'dan büyük olamayacağı teoremin kanıtından hemen anlaşılıyor. Teorem kanıtlanmıştır. □

Sonuç 13.7. *A serbest abel grubu $(a_i)_{i\in I}$ tarafından üretilirse* $\dim A \leq |I|$ *olur.*

Kanıt: $F = \mathbb{Z}^{(I)}$ olsun. $(e_i)_{i\in I}$ ailesi bu grubun doğal tabanı olsun. $\varphi(e_i) = a_i$ kuralıyla, F serbest abel grubundan A serbest abel grubuna giden homomorfiyi ele alalım. Bu homomorfi örtendir. Sonuç 13.4'e göre A'ya izomorf bir B (serbest abel) altgrubu için $F = \operatorname{Ker}\varphi \oplus B$ olur. Teorem 13.6'ya göre $\operatorname{Ker}\varphi$ serbest bir abel grubudur. Elbette

$$|I| = \dim F = \dim \operatorname{Ker}\varphi + \dim B = \dim \operatorname{Ker}\varphi + \dim A$$

olur. □

Sonuç 13.8. *$A \simeq \bigoplus_{i=1}^{n} \mathbb{Z}$ olsun. A'yı üreten n tane eleman doğrusal bağımsız olmak zorundadır.*

Kanıt: $a_1, \ldots, a_n$ elemanları A'yı üretsin. O zaman

$$\varphi(k_1, \ldots, k_n) = \sum_{i=1}^{n} k_i a_i$$

kuralı bize $\bigoplus_{i=1}^{n} \mathbb{Z}$ grubundan A'ya giden örten bir homomorfi verir. Sonuç 13.4'e göre A'ya, dolayısıyla $\bigoplus_{i=1}^{n} \mathbb{Z}$ grubuna izomorf bir B (serbest abel) altgrubu için $A = \operatorname{Ker}\varphi \oplus B$ olur. Teorem 13.6'ya göre $\operatorname{Ker}\varphi$ serbest bir abel grubudur. Elbette

$$n = \dim A = \dim \operatorname{Ker}\varphi + \dim B = \dim \operatorname{Ker}\varphi + n$$

olur. Demek ki $\dim \operatorname{Ker}\varphi = 0$ ve $\operatorname{Ker}\varphi = 0$. Bu da aynen $a_1, \ldots, a_n$ elemanlarının doğrusal bağımsızlığı anlamına gelir. □

Serbest abel grupları burulmasız abel gruplarıdır. Ama burulmasız her abel grubu serbest değildir. Bölüm B'de buna bir örnek verdik: $\mathbb{Z}^{\mathbb{N}}$. Öte yandan eğer grup sonlu eleman tarafından üretiliyorsa, bu doğrudur.

Teorem 13.9. *Burulmasız ve sonlu sayıda eleman tarafından üretilen bir abel grubu serbest abel grubudur. Ayrıca grubun boyutu grubun üreteç sayısını geçemez.*

Kanıt: Gruba A diyelim. Grubu üreten eleman sayısı n olsun, üreteçlere de $a_1, \ldots, a_n$ diyelim. Teoremi n üzerine tümevarımla kanıtlayacağız. Eğer $n = 0$ ise $A = 0$ olur ve sorun yok. $n = 1$ ise, $A = \langle a_1 \rangle \simeq \mathbb{Z}$ olur ve gene sorun yok. Şimdi $B = \langle a_1, \ldots, a_{n-1} \rangle$ altgrubunun serbest olduğunu ve boyutunun en fazla $n-1$ olduğunu varsayalım. $B < A$ varsayımını yapabiliriz, aksi halde teoremin kanıtı zaten bitmiştir. A/B elemanı $\overline{a_n}$ tarafından üretilir. Eğer A/B burulmasızsa, o zaman A/B grubu $\mathbb{Z}$'ye izomorftur ve sonuç Sonuç 13.5'ten çıkar. Eğer A/B burulmalıysa, o zaman bir $k > 0$ tamsayısı için $ka_n \in B$, ve dolayısıyla $kA \leq B$ olur. Ama bu durumda, Teorem 13.6'dan dolayı kA serbest bir grup olur. Ayrıca A burulmasız olduğundan $A \simeq kA$ olur. Demek ki A da serbest bir gruptur. □

Notlar ve Örnekler

13.17. $\mathbb{Q}/\mathbb{Z}$ grubunun burulmalı olduğunu biliyoruz. Bu örnekte bu olguyu genelleştiren şu teoremi kanıtlayacağız:

Teorem 13.10. *A bir abel grubu olsun. O zaman A'nın maksimal boyutlu serbest bir altgrubu vardır. Eğer B böyle bir altgrupsa A/B burulmalı olur.*

Kanıt: Zorn Önsavı'nı kullanacağız. $\mathcal{Z}$, G'nin doğrusal bağımsız altkümelerinden oluşsun. $\mathcal{Z}$'yi içindelik ilişkisiyle küçükten büyüğe sıralayalım. Eğer $\mathcal{C} \subseteq \mathcal{Z}$ bir zincirse (yani her $X, Y \in \mathcal{C}$ için ya $X \subseteq Y$ ya da $Y \subseteq X$ ise), o zaman $\bigcup \mathcal{C} \in \mathcal{Z}$ olur, çünkü lineer bağımlılık sonlu sayıda elemanı ilgilendiren bir özelliktir. Bu dediğimizi açıklayalım, çünkü benzer akıl yürütmeler sık sık yapılır matematikte. $x_1, \ldots, x_n \in \bigcup \mathcal{C}$ birbirinden

farklı elemanlar olsun. Diyelim $k_1, \ldots, k_n \in \mathbb{Z}$ için $k_1x_1 + \cdots + k_nx_n = 0$. Her k_i'nin 0'a eşit olduğunu kanıtlayacağız. Her $i = 1, \ldots, n$ için, x_i'nin elemanı olduğu bir $X_i \in \mathcal{C}$ seçelim. Bu X_i'lerden biri diğerlerini kapsar. Diyelim X_j diğerlerini kapsıyor. O zaman $x_1, \ldots, x_n \in X_j$ olur. Ama X_j doğrusal bağımsız bir küme olduğundan, bundan $k_1 = \ldots = k_n = 0$ çıkar.

Böylece Zorn Önsavı sayesinde $\mathcal{Z}$'den maksimal bir küme seçebiliriz, diyelim X. Bu küme maksimal lineer bağımsızdır. Dolayısıyla, eğer B bu altküme tarafından üretilen altgrupsa,

$$B = \langle X \rangle = \bigoplus_{x \in X} \mathbb{Z}x \simeq \bigoplus_{X} \mathbb{Z}$$

olur. Şimdi A/B grubuna bakalım. Diyelim $\overline{x} \in A/B$ burulmasız bir eleman. Bu durumda,

$$\langle B, x \rangle / B \simeq \langle \overline{x} \rangle \simeq \mathbb{Z}$$

olduğundan, Sonuç 13.5'e göre,

$$\langle B, x \rangle / B = B \oplus \langle x \rangle$$

olur, yani $X \sqcup \{x\}$ doğrusal bağımsızdır. Ama bu da X'in maksimalliğiyle çelişir. Demek ki B/A torsion bir gruptur. □

Ama dikkat, A'da B'den daha büyük bir serbest abel grubu olabilir. Örneğin $A = \mathbb{Q}$, $B = \mathbb{Z}$ ise, $B_1 = \frac{1}{2}\mathbb{Z}$ altgrubu serbesttir ve B'den daha büyüktür. Ama $B \leq B_1$ için B_1/B burulmasız bir eleman içeremez.

13.1.6 Evrensel Özellik

Bu altbölümde serbest abel gruplarının I göstergeç kümesini X olarak yazacağız, çünkü göstergeç kümesini "gerçek" bir küme olarak görmek istiyoruz, o kadar ki elemanlarına göstergeç yerine "nokta" demeyi tercih edeceğiz. X herhangi bir küme olsun. $\mathbb{Z}^{(X)} = \bigoplus_X \mathbb{Z}$ grubunun X'ten $\mathbb{Z}$'ye giden ve kaidesi sonlu olan fonksiyonlar kümesi olarak tanımlandığını anımsayalım (bkz. Örnek 1.11). Geçmişte, eğer $f \in \mathbb{Z}^{(X)}$ ise, $f(x)$ yerine f_x yazmış ve f'yi değerleriyle göstermeyi yeğleyip f yerine $(f_x)_x$ yazmıştık. Bazen $(f_x)_x$ yazılımı yerine $\sum_x f_x x$ ve $\mathbb{Z}^{(X)}$ yerine $\bigoplus_X \mathbb{Z}x$ yazılımları kullanılır. Bu yeni yazılımların birden çok nedeni vardır. Açıklamaya çalışalım. Birazdan kanıtlayacağımız teorem bu yeni yazılımın nedenini çok daha iyi gözler önüne serecek.

Eğer $X = \mathbb{N}$ ise, $\mathbb{Z}^{(X)}$ grubunun bir elemanını bir dizi olarak gösterebiliriz. Örneğin,

$$(0, 0, 0, 3, 0, 5, 0, 0, \ldots)$$

gösteriminin hangi elemanı simgelediği barizdir. Ama eğer X kümesi üzerine $\mathbb{N}$'deki gibi bir iyisıralama yoksa, hatta eğer sayılamaz sonsuzluktaysa, o zaman $\mathbb{Z}^{(X)}$ grubunun elemanlarını yukarıdaki gibi bir dizi olarak gösteremeyiz. Örneğin eğer X kümesi üzerinde bir iyisıralama yoksa, bu yazılımla x'inci koordinatı 5, bir başka y'inci koordinatı 3, diğer koordinatları 0 olan bir elemanın nasıl gösterileceği belli değildir. Şimdi, X ne olursa olsun, $\mathbb{Z}^{(X)}$ grubunun elemanlarını daha kolay bir biçimde yazmanın yolunu göstereceğiz.

$f = (f_x)_x$ gösterimi yerine $f = \sum_x f_x x$ yazalım. O zaman bir önceki paragrafta verdiğimiz örnekteki elemanı $5x + 3y$ olarak gösterilir ve bu yazılımla x'inci koordinatın 5, y'inci koordinatın 3, diğer koordinatların 0 olduğu hemen anlaşılır. Bu durumda, eskiden $\mathbb{Z}^{(X)}$ ya da $\bigoplus_X \mathbb{Z}$ olarak gösterdiğimiz grup $\bigoplus_{x\in X} \mathbb{Z}x$ olarak gösterilir ve elemanları $(f_x)_x$ yerine

$$\sum_x f_x x$$

biçiminde yazılır[6].

Bu yazılımın teorik olarak nasıl mümkün olduğunu gösterelim: $x \in X$ olsun. $\mathbb{Z}^{(X)}$ grubunun, x'te 1 değerini alan, diğer noktalarda 0 değerini alan

$$\widetilde{x} : X \longrightarrow \mathbb{Z}$$

elemanını ele alalım. Sadece bir kez 0'dan farklı bir değer aldığından, $\widetilde{x} \in \mathbb{Z}^{(X)}$ olur. Fonksiyonları bir tamsayıyla çarpmayı ve iki fonksiyonu toplamayı biliyoruz: Bu işlemleri fonksiyonun değerleri üzerinden yapıyoruz. Örneğin, eğer x ve y elemanları X'in iki farklı elemanıysa, $5\widetilde{x} + 3\widetilde{y}$ fonksiyonu x'te 5 değerini alan, y'de 3 değerini alan ve X'in diğer noktalarında 0 değerini alan fonsiyondur. Böylece eğer $f \in \bigoplus_X \mathbb{Z}$ fonksiyonu birbirinden farklı $x_1, \ldots, x_n \in X$ noktalarında sırasıyla $f_{x_1}, \ldots, f_{x_n}$ değerlerini alıyorsa ve diğer noktalarda 0 değerini alıyorsa, f fonksiyonunu

$$f_{x_1}\widetilde{x_1} + \cdots + f_{x_n}\widetilde{x_n}$$

yani

$$\sum_{i=1}^{n} f_{x_i}\widetilde{x}_i$$

olarak gösterebiliriz. Böylece $\mathbb{Z}^{(X)}$ grubunun her elemanı

$$\sum_x f_x\widetilde{x}$$

olarak gösterilebilir. Tabii buradaki toplam sonlu bir toplam olmalıdır, aksi halde direkt toplamın bir elemanını elde etmeyiz.

Ayrıca

$$x \mapsto \widetilde{x}$$

fonksiyonu X'ten $\mathbb{Z}^{(X)}$ grubuna giden birebir bir fonksiyondur. Bu birebir fonksiyon sayesinde $x \in X$ noktasıyla (ya da göstergeciyle) $\widetilde{x} \in \mathbb{Z}^{(X)}$ elemanını özdeşleştirebiliriz. Böylece,

$$\sum_x f_x\widetilde{x}$$

[6]Tabii $X = \mathbb{N}$ ise, $5x$ yazmak sakıncalıdır! Bu durumda eski yazılım tercih edilmelidir, ya da, anlamsız bir x simgesi uydurup, $\bigoplus_{\mathbb{N}} \mathbb{Z}$ yerine $\bigoplus_i \mathbb{Z}x_i$ yazılmalıdır.

yerine

$$\sum_x f_x x$$

yazma hakkını kendimizde görebiliriz. Bu yazılımla,

$$\left(\sum_x f_x x\right) + \left(\sum_x g_x x\right) = \sum_x (f_x + g_x)x$$

ve

$$n\sum_x f_x x = \sum_x (nf_x)x$$

olur. Daha da önemlisi, böylece X'i,

$$\mathbb{Z}^{(X)} = \bigoplus_X \mathbb{Z} = \bigoplus_X \mathbb{Z}x$$

grubunun bir altkümesi olarak görebiliriz; hatta X altkümesi serbest grubun tabanı olur.

Rastgele bir X kümesi için $\bigoplus_{x\in X} \mathbb{Z}x$ grubuna X tarafından ***serbestçe üretilmiş grup*** adı verilir.

Hayatı kolaylaştıracağını düşündüğümüz bütün bu açıklamalardan sonra bu altaltbölümün amacı olan teoremi kanıtlayalım.

Teorem 13.11. *X bir küme, A herhangi bir abel grubu ve $\alpha : X \longrightarrow A$ bir fonksiyon olsun. O zaman $\mathbb{Z}^{(X)} = \bigoplus_{x\in X} \mathbb{Z}x$ serbest abel grubundan A grubuna giden, ve her $x \in X$ için $\varphi(x) = \alpha(x)$ eşitliğini sağlayan bir ve bir tane homomorfi vardır.*

Ayrıca eğer F abel grubu X'i kapsıyorsa ve F'nin yukarıda $\mathbb{Z}^{(X)}$ için belirtilen özelliği varsa, o zaman $F \simeq \bigoplus_X \mathbb{Z}x$ olur.

Kanıt: A grubunu toplamsal yazalım. $\bigoplus_{x\in X} \mathbb{Z}x$ serbest abel grubunun her f elemanı tek bir biçimde

$$f = \sum_{x\in X} f_x x$$

olarak yazılır. Şimdi $\varphi : \bigoplus_{x\in X} \mathbb{Z}x \longrightarrow A$ fonksiyonunu

$$\varphi(f) = \sum_{x\in X} f_x \alpha(x) \in A$$

olarak tanımlayalım. Sağ taraftaki toplam elbette A'da hesaplanmaktadır[7]. φ fonksiyonunun iyi tanımlı olduğu belli, çünkü $\bigoplus_{x\in X} \mathbb{Z}x$ serbest abel grubunun

[7] $X \subseteq A$ ve $\alpha(x) = x$ olsa da bu fonksiyonun $\varphi(f) = f$ formülüyle tanımlandığını söylemek yanlışların en büyüğü olur. Örneğin, $\bigoplus_{x\in X} \mathbb{Z}x$ serbest abel grubunda $\sum_{x\in X} f_x x \neq \sum_{x\in X} g_x x$ olabilir ama A grubunda, $\sum_{x\in X} f_x x = \sum_{x\in X} g_x x$ olabilir.

her f elemanı tek bir biçimde

$$f = \sum_{x \in X} f_x x$$

olarak yazılır ve A abel olduğundan $\varphi(f)$'nin tanımındaki toplamın sırası önemli değildir. φ'nin homomorfi olduğu da bariz. $\varphi(x) = x$ eşitliği de. Bu koşulları sağlayan ikinci bir homomorfinin olmadığı da.

İkinci önermeyi kanıtlayalım. Varsayıma göre $\psi(x) = x$ eşitliğini sağlayan bir $\psi : F \longrightarrow \bigoplus_X \mathbb{Z}x$ homomorfisi vardır. Aynı şekilde $\varphi(x) = x$ eşitliğini sağlayan bir $\psi : \bigoplus_X \mathbb{Z}x \longrightarrow F$ homomorfisi vardır. Demek ki,

$$\varphi \circ \psi : \bigoplus_X \mathbb{Z}x \longrightarrow \bigoplus_X \mathbb{Z}x$$

homomorfisi x'i x'e götürür. Aynı şeyi,

$$\mathrm{Id} : \bigoplus_X \mathbb{Z}x \longrightarrow \bigoplus_X \mathbb{Z}x$$

homomorfisi de yapar. Bu aşamada, ilk önermedeki "bir ve bir tane" sözleri önemli olacak: $\varphi \circ \psi = \mathrm{Id}$ olmalı. Benzer şekilde $\psi \circ \varphi = \mathrm{Id}$ olmalı. Demek ki φ ve ψ birer izomorfidirler. □

13.2 Sonlu Sayıda Üreteçli Abel Grupları (1)

Bir önceki altbölümde kanıtlanan teoremlerin sonuçlarını bulalım.

Sonuç 13.12. *Sonlu eleman tarafından üretilmiş bir abel grubunun altgrupları da sonlu eleman tarafından üretilir ve altgrubun üreteç sayısı grubu üreten eleman sayısından küçükeşit alınabilir.*

Kanıt: Gruba G diyelim. Grup $g_1, \ldots, g_n$ elemanları tarafından üretilsin. $A = \bigoplus_{i=1}^{n} \mathbb{Z}$ olsun. $e_1, \ldots, e_n$ elemanları A'nın bir tabanı olsun, doğal üreteçleri olabilirler mesela. $\varphi : A \longrightarrow G$ fonksiyonu e_i'yi g_i'ye götüren örten homomorfi olsun. $H \leq G$ olsun. Teorem 13.6'ya göre $\varphi^{-1}(H)$ altgrubu en fazla n eleman tarafından üretilir. Ama H bu altgrubun φ-imgesidir. Demek ki H de en fazla n eleman tarafından üretilir. □

Alıştırmalar

13.18. κ tane eleman tarafından üretilmiş bir abel grubunun altgruplarının en fazla κ elemanlı bir üreteç kümesi olduğunu kanıtlayın.

Yukarıdaki teorem abel olmayan gruplar için doğru değildir. Örneğin iki eleman tarafından üretilmiş serbest grupların sonlu eleman tarafından üretilmeyen altgrupları vardır, bkz. Örnek E.3.

Sonuç 13.13. *G, n tane eleman tarafından üretilmiş bir abel grubu olsun. T, G'nin derecesi sonlu olan elemanlarından oluşsun. O zaman $T \leq G$ olur ve T en fazla n eleman tarafından üretilir. Demek ki T'nin eksponenti sonludur. Ayrıca boyutu n'den küçükeşit bir A serbest abel grubu için $G = T \oplus A$ olur.*

Kanıt: T'nin bir altgrup olduğu bariz (bkz. Örnek 9.56). Sonuç 13.12'ye göre T, en fazla n eleman tarafından üretilir. Eğer T'nin bu sonlu sayıdaki üreteçlerinin derecelerinin en küçük ortak katı m ise, het $t \in T$ için $t^m = 1$ olur.

G/T burulmasız bir gruptur ve en fazla n eleman tarafından üretilir. Demek ki Teorem 13.9'a göre G/T serbest abel grubudur. Teorem 13.3'e göre boyutu en fazla n olan bir A serbest abel grubu için $G = T \oplus A$ olur. □

Demek ki sonlu abel gruplarını sınıflandırmak için elemanlarının derecelerinin üst sınırının olduğu burulmalı abel gruplarını sınıflandırmak yeterli. Bu tür gruplara ***sonlu eksponantlı*** abel grupları denir. Bu tür grupları sınıflandırmak mümkündür. Bir sonraki altbölümde bunu yapacağız.

13.3 Burulmalı Abel Grupları

Sonuç 12.9'u anımsatalım:

Olgu 13.14. *G burulmalı bir abel grubu olsun. Her p asalı için*

$$G[p^\infty] = \{g \in G : \text{ bir } i \in \mathbb{N} \text{ için } g^{p^i} = 1\}$$

tanımını yapalım. O zaman $G[p^\infty] \leq G$ ve $G \simeq \bigoplus_p G[p^\infty]$ olur. □

Demek ki burulmalı abel gruplarını sınıflandırmak için, p asalları için abel p-gruplarını sınıflandırmak yeterli. Bunu yapamayacağız ama eğer eksponent sonluysa üstesinden gelebileceğiz.

Teorem şöyle:

Teorem 13.15. *Eksponenti sonlu olan abel p-grupları döngüsel (dolayısıyla $\mathbb{Z}/p^n\mathbb{Z}$ gruplarına izomorfik) altgrupların direkt toplamıdır.* □

Birazdan kanıtlayacağımız bu teoremden ve Olgu 13.14'ten şu çıkar:

Sonuç 13.16. *Eksponenti sonlu olan abel grupları her biri bir p asalı ve bir $n > 0$ doğal sayısı için $\mathbb{Z}/p^n\mathbb{Z}$ grubuna izomorfik altgrupların direkt toplamıdır.* □

Bu teoremin kanıtı biraz zaman alacak. Eğer grup sonluysa (ya da aynı şey, sonlu eleman tarafından üretilmişse), kanıt çok daha kolay. Teoremi en genel haliyle kanıtlamak için Seçim Aksiyomu'na ihtiyaç vardır. Sadece sonlu

gruplarla ilgilenen okura Seçim Aksiyomu'na toslamaması için yol göstermeye çalışacağız.

Aşağıdaki önsav teoremin kanıtında tahmin edildiği üzere çok önemli olacak. Önsav'ın kanıtının yöntemi de önemlidir, çünkü bu yönteme sık sık başvurulur, biz de ileride aynı yöntemle başka derin sonuçlar kanıtlayacağız. Teorem 13.33, bu önsavın bir genellemesi olacak.

Önsav 13.17. *p bir asal ve G, eksponenti p^n olan bir abel grubu olsun. $H \leq G$ altgrubu bir I göstergeç kümesi için $\oplus_I \mathbb{Z}/p^n\mathbb{Z}$ grubuna izomorf olsun. O zaman bir $K \leq G$ altgrubu için $G = H \oplus K$ olur.*

Kanıt: Eğer G sonluysa, o zaman $H \cap K = 1$ eşitliğini sağlayan maksimal bir K altgrubu vardır elbette. Eğer G sonsuzsa bu eşitliği sağlayan bir K altgrubunun varlığı ancak Seçim Aksiyomu'yla, daha doğrusu Zorn Önsavı ile gösterilebilir ve şimdi bunu yapıyoruz. (Sonlu gruplarla ilgilenen okur bu paragrafın gerisini atlayabilir.) Grubun işlemini çarpımsal yazacağız.

$$\mathcal{Z} = \{K \leq G : K \cap H = 1\}$$

olsun. $1 \in \mathcal{Z}$ olduğundan $\mathcal{Z} \neq \emptyset$ olur. $\mathcal{Z}$'yi altgrup (ya da altküme) olma ilişkisiyle sıralayalım, altgruplar üstgruplardan küçük olsun. Eğer $(K_i)_i$, $\mathcal{Z}$'nin bir zinciriyse, $\bigcup_i K_i \in \mathcal{Z}$ olur, çünkü $\bigcup_i K_i$ altgrubunun H ile 1'den farklı bir elemanda kesişmesi için, K_i altgruplarından birinin H ile 1'den farklı bir elemanda kesişmesi lazım. Dolayısıyla, Zorn Önsavı'na göre $\mathcal{Z}$'nin maksimal bir elemanı vardır. Bu altgruba K diyelim. Demek ki

$$\langle H, K\rangle = HK = H \oplus K \leq G.$$

$HK = G$ eşitliğini kanıtlayacağız. Diyelim eşitlik yok ve $HK < G$. Amacımız $\langle K, g\rangle \cap H = 1$ eşitliğinin doğru olduğu bir $g \in G \setminus K$ elemanının varlığını kanıtlamak; böylece $K < \langle K, g\rangle$ olacak ve K'nın maksimalliğiyle çelişeceğiz.

Önce rastgele bir $g \in G \setminus HK$ alalım. Bu elemanı istediğimizi sağlaması için yavaş yavaş değiştireceğiz. İlk olarak

$$g,\ g^p,\ g^{p^2},\ \ldots,\ g^{p^n} = 1$$

dizisine bakalım. İlk terim, g yani, HK'da değil. Ama son terim, g^{p^n} yani, 1'e eşit olduğundan HK'da. Bu dizinin elemanlarını soldan sağa doğru tararken, bir $i = 0, 1, \ldots, n-1$ için

$$g^{p^i} \notin HK \text{ ama } g^{p^{i+1}} \in HK$$

olmalı. g yerine bu g^{p^i} elemanını alarak,

$$g \notin HK \text{ ama } g^p \in HK \tag{1}$$

varsayımını yapabiliriz; öyle yapalım. Şimdi, $h \in H$ ve $k \in K$ için

$$g^p = hk \tag{2}$$

olur. Grubun eksponenti p^n olduğundan,

$$1 = g^{p^n} = (g^p)^{p^{n-1}} = (hk)^{p^{n-1}} = h^{p^{n-1}} k^{p^{n-1}}$$

olur ve bu durumda, $h^{p^{n-1}} = k^{-p^{n-1}} \in H \cap K = 1$ ve

$$h^{p^{n-1}} = 1$$

elde ederiz.

Şimdi H grubunda hangi elemanların p^{n-1}'inci kuvvetinin 1'e eşit olduğunu görelim. Teoremin hipotezine göre $H \simeq (\mathbb{Z}/p^n\mathbb{Z})^{(I)}$. Ama

$$\{x \in \mathbb{Z}/p^n\mathbb{Z} : p^{n-1}x = 0\} = p\mathbb{Z}/p^n\mathbb{Z}$$

eşitliğini Örnek 9.53'de kanıtlamıştık; demek ki aynı şey $(\mathbb{Z}/p^n\mathbb{Z})^{(I)}$ grubunda da doğru:

$$\{x \in (\mathbb{Z}/p^n\mathbb{Z})^{(I)} : p^{n-1}x = 0\} = (p\mathbb{Z}/p^n\mathbb{Z})^{(I)} = p \cdot (\mathbb{Z}/p^n\mathbb{Z})^{(I)}.$$

Sonuç olarak benzer önerme (çarpımsal bir grup olan) H için de geçerlidir ve $h^{p^{n-1}} = 1$ olduğundan, bir $h_1 \in H$ için $h = h_1^p$ eşitliğinin doğru olduğunu görürüz. (2)'den dolayı, $g^p = hk = h_1^p k$ ve $(h_1^{-1}g)^p = k \in K$ elde ederiz. $h_1^{-1}g \in G \setminus HK$ olduğundan (aksi halde $g = h_1(h_1^{-1}g) \in H(HK) = HK$ olurdu), g yerine $h_1^{-1}g$ elemanını alıp,

$$g \in G \setminus HK \text{ ve } g^p \in K \tag{3}$$

varsayımını yapabiliriz.

Bu aşamada $\langle K, g\rangle$ altgrubuna bakalım. Bu altgrubun elemanları bir $k \in K$ ve $m \in \mathbb{Z}$ için kg^m biçimindedir (daha önceki k'yı artık unutun). K'nın seçiminden dolayı, $\langle K, g\rangle \cap H \neq 1$ olmalı. Kesişimden 1'e eşit olmayan bir eleman seçelim:

$$1 \neq kg^m \in H$$

olsun. Demek ki $g^m \in HK$. Eğer p asalı n'yi bölmezse, g^p de HK'da olduğundan,

$$g = g^1 = g^{\mathrm{obeb}(n,p)} \in HK$$

olur (bkz. Alıştırma 5.31), ki bu da g'nin seçimiyle çelişir. Demek ki $p|m$, diyelim $ps = m$. Bu durumda, $g^p \in K$ olduğundan,

$$kg^m = kg^{ps} = k(g^p)^s \in K$$

olur. Ama aynı zamanda $kg^m \in H$. Demek ki $kg^m \in H \cap K = 1$, çelişki. $\square$

Uyarı. Eğer $m < n$ için $H \simeq \oplus_I \mathbb{Z}/m\mathbb{Z}$ olursa yukarıdaki teorem doğru olmaz. Örneğin $G = \mathbb{Z}/9\mathbb{Z}$ ve $H = 3\mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z}$ olsun. Bu durumda teorem doğru değildir. Teoremin yanlış olduğu bir başka örnek: $G = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ ve $H = \langle (2,1) \rangle$.

Aşağıdaki önsavla Teorem 13.15'in kanıtına öldürücü darbeyi indireceğiz.

Önsav 13.18. *p bir asal, $n > 0$ bir doğal sayı ve G, eksponenti p^n olan bir abel grubu olsun. O zaman G'nin $(\mathbb{Z}/p^n\mathbb{Z})^{(I)}$ grubuna izomorfik öyle bir H altgrubu ve bir $m < n$ doğal sayısı için eksponenti p^m olan öyle bir K altgrubu vardır ki $G = H \oplus K$ olur.*

Kanıt: Teorem aslında, $(\mathbb{Z}/p^n\mathbb{Z})^{(I)}$ grubuna izomorfik maksimal bir altgrup olduğunu söylüyor. H altgrubunun bir A altkümesinin şu özellikleri varsa:

1. $\langle A \rangle = \bigoplus_{a \in A} \langle a \rangle$
2. Her $a \in A$ için $\langle a \rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$

o zaman A'ya bu kanıtlık güzel küme diyelim.

Önce G'nin sonlu eleman tarafından üretildiğini, yani sonlu olduğunu varsayalım. O zaman maksimal bir güzel A kümesi vardır elbette. Eğer G sonsuzsa, maksimal bir güzel A kümesi bulmak için Seçim Aksiyomu'nu kullanmalıyız. G'nin sonsuz olduğu durumla ilgilenmek istemeyen okur bu paragrafın devamını atlayabilir. Eksponent p^n olduğundan, derecesi p^n olan bir eleman mutlaka vardır, dolayısıyla, tek elemanlı da olsa güzel bir küme vardır. (Aslında boşküme de güzel kümedir!) $\mathcal{Z}$ kümesi G'nin güzel altkümelerinden oluşan küme olsun. Bu kümenin boş olmadığını biraz önce gördük. $\mathcal{Z}$ kümesi üzerine altküme olma yarısıralamasını koyalım ve bu yarısıralamayla $\mathcal{Z}$'nin tümevarımsal bir küme olduğunu gösterelim. Bu amaçla $\mathcal{Z}$'den bir $(A_j)_{j \in J}$ zinciri alalım. $\bigcup_J A_j$ kümesinin de bir güzel küme olduğunu savlıyoruz ve hemen kanıtlıyoruz. Her $a \in \bigcup_J A_j$ için $\langle a \rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$ olduğu belli. Eğer $\langle \bigcup_J A_j \rangle = \bigoplus_{a \in A} \langle a \rangle$ olmasaydı, o zaman oyunbozanlık yapan sonlu sayıda eleman A_j'lerin birinde belirirdi ki, bu da imkânsızdır. Demek ki $\bigcup_J A_j \in \mathcal{Z}$ olur. Demek ki $\mathcal{Z}$ kümesine Zorn Önsavı'nı uygulayabiliriz. Böylece, Zorn Önsavı sayesinde, $\mathcal{Z}$ kümesinin maksimal bir elemanı olduğu çıkar. Bu maksimal güzel kümeye A diyelim.

Şimdi

$$H = \langle A \rangle = \bigoplus_{a \in A} \langle a \rangle \simeq \bigoplus_{a \in A} \mathbb{Z}/p^n\mathbb{Z}$$

tanımını yapalım. Önsav 13.17'ye göre $G = H \oplus K$ eşitliğini sağlayan bir $K \leq G$ vardır. A'nın maksimalliğinden dolayı, K'da derecesi p^n olan bir eleman olamaz. Demek ki $\exp K < p^n$ ve dolayısıyla bir $m < n$ için $\exp K = p^m$. $\square$

Bu iki önsav teoremi n üzerine tümevarımla kanıtlar.

Sonuç 13.19. *Eksponenti p^n olan bir grup, $I_1, \ldots, I_n$ kümeleri (ya da kardinalleri) için*

$$\bigoplus_{k=1}^{n} \left(\bigoplus_{I_k} \mathbb{Z}/p^k\mathbb{Z} \right)$$

grubuna izomorfturlar. □

13.4 Sonlu Sayıda Üreteçli Abel Grupları (2)

Yukarıda yapılanlardan şu teorem çıkar:

Teorem 13.20. *Sonlu eleman tarafından üretilen bir abel grubu sonlu sayıda döngüsel altgrubun direkt toplamıdır. Bu döngüsel altgrupların her biri $\mathbb{Z}$'ye ya da bir p^n asal kuvveti için $\mathbb{Z}/p^n\mathbb{Z}$ grubuna izomorf olarak alınabilir.*

Kanıt: Gruba G diyelim. T, G'nin burulmalı elemanlarından oluşan küme olsun. Elbette $T \leq G$ olur. Sonuç 13.13'e göre bir A serbest abel grubu için $G = T \oplus A$ olur. Sonuç 13.12'ye göre T ve A sonlu sayıda eleman tarafından üretilirler. Teorem 7.4'e göre A'nın ancak sonlu bir tabanı olabilir. T sonlu sayıda eleman tarafından üretildiğinden, eksponenti sonludur. Sonuç 13.16'ya göre T de döngüsel altgrupların direct toplamıdır. Sonuç olarak G, ya $\mathbb{Z}$'ye ya da bir p^n asal kuvveti için $\mathbb{Z}/p^n\mathbb{Z}$ grubuna izomorf sonlu sayıda altgrubun direkt toplamıdır. □

Uyarı. n eleman tarafından üretilen bir abel grubu daha fazla döngüsel grubun direkt toplamı olabilir. Örneğin, $p \neq q$ birbirine asal iki doğal sayıysa, $\mathbb{Z}/pq\mathbb{Z}$ grubu 1 elemanı tarafından üretilir ama $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ grubuna izomorftur.

Öte yandan bir p asalı için, n eleman tarafından üretilen bir G abel p-grubu, en fazla n tane altgrubun direkt toplamı olabilir. Bunu görmek için, eğer

$$G \simeq \bigoplus_{i=1}^{k} \mathbb{Z}/p^{k_i}\mathbb{Z}$$

ise, grubu

$$\bigoplus_{i=1}^{k} \mathbb{Z}/p^{k_i-1}\mathbb{Z}$$

altgrubuna bölerek,

$$G \simeq \bigoplus_{i=1}^{k} \mathbb{Z}/p\mathbb{Z}$$

olduğunu varsayabiliriz. Eksponenti p olan ve n eleman tarafından üretilen bir grubun en fazla p^n tane elemanı olabilir. Demek ki $p^k \leq p^n$ ve $k \leq n$.

Notlar ve Örnekler

13.19. Bu alıştırmalarda p hep bir asal sayı olacak. p elemanlı tüm gruplar $\mathbb{Z}/p\mathbb{Z}$ grubuna izomorfturlar. Bunu biliyoruz. Bundan sonraki alıştırmalarda küçük n sayıları için p^n elemanlı birbirine izomorf olmayan abel grubu sayısını bulacağız.

13.20. p^2 elemanlı tüm gruplar abeldirler (Sonuç 8.11). Dolayısıyla sadece iki tip p^2 elemanlı grup vardır: $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ve $\mathbb{Z}/p^2\mathbb{Z}$.

13.21. p^3 elemanlı bir grup abel grubu olmak zorunda değil. Örneğin, G küme olarak

$$G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

ise ve işlemi

$$(x, y, z)(x', y', z') = (x + x', y + y', z + xy' + z')$$

formülüyle verilmişse ve eğer $p > 2$ ise, G abel olmayan bir gruptur. 8 elemanlı abel olmayan gruplar biliyoruz. Eğer G abel olmayan bir grupsa ve $|G| = p^3 > 8$ ise, G'nin bu paragrafta açıklanan gruba izomorf olduğunu kanıtlamak çok zor değildir; en son bölümde bunu yapacağız, şimdilik okura bırakıyoruz.

p^3 elemanlı abel gruplara gelince: Birbirine izomorf olmayan üç grup vardır:

$$(\mathbb{Z}/p\mathbb{Z})^3,\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z},\ \mathbb{Z}/p^3\mathbb{Z}.$$

13.22. p^4 elemanlı izomorfik olmayan gruplar şunlardır: Önce,bir önceki grupları $\mathbb{Z}/p\mathbb{Z}$ ile direkt toplamını alabiliriz:

$$(\mathbb{Z}/p\mathbb{Z})^4,\ (\mathbb{Z}/p\mathbb{Z})^2 \times \mathbb{Z}/p^2\mathbb{Z},\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^3\mathbb{Z}.$$

Bunlar içinde $\mathbb{Z}/p\mathbb{Z}$ faktörünü barındıran gruplardır. Bunların dışında iki tane daha vardır:

$$(\mathbb{Z}/p^2\mathbb{Z})^2,\ \mathbb{Z}/p^4\mathbb{Z}.$$

13.23. p^5 ve p^6 elemanlı izomorf olmayan abel gruplarını bulmayı okura bırakıyoruz.

13.5 Bölünür Abel Grupları

G bir abel grubu olsun. Eğer her $g \in G$ elemanı ve her $n > 0$ doğal sayısı için $x^n = g$ denkleminin g'de bir çözümü varsa, G'ye ***bölünür grup*** denir. Bir grubun, kendi başına bir grup olarak bölünür altgruplarına ***bölünür altgrup*** adı verilir.

Notlar ve Örnekler

13.24. $\mathbb{Q}$ bölünür bir gruptur.

13.25. G bölünür bir grup ve $H \leq G$ ise G/H bölünür bir gruptur.

13.26. Bölünür grupların direkt toplamları ve kartezyen çarpımları bölünürdür.

13.27. Bir G abel grubunun bölünür altgrupların ürettiği altgrup bölünürdür. Dolayısıyla G'nin tüm bölünür altgrupların ürettiği altgrup en büyük bölünür altgruptur. Bu altgruba $D(G)$ diyelim.

13.28. Eğer bir direkt toplam bölünürse, direkt toplamı alınan her grup bölünürdür. Dolayısıyla bölünür bir abel grubunda tümleyeni olan her altgrup bölünürdür.

13.29. (Geçmişte sözettiğimiz ama birazdan bir daha ele alacağımız) Prüfer p-grupları $\mathbb{Z}_{p^\infty}$ bölünür gruplardır.

13.30. G toplama altında yazılmış bir abel grubu olsun. $E(G) = \bigcap_{n=1}^{\infty} nG$ olsun. $E(G)$, G'de her pozitif tamsayıya bölünen elemanlar kümesidir ve elbette bir altgruptur. $E(G)$, G'nin bütün bölünür altgruplarını, dolayısıyla G'nin en büyük bölünür altgrubu olan $D(G)$'yi kapsar (bkz. Örnek 13.27). Dikkat: Eğer G burulmalıysa, $E(G)$'nin 1'e eşit olduğunu sanmayın; örneğin $E(\mathbb{Z}_{p^\infty}) = \mathbb{Z}_{p^\infty}$ olur. $(n+1)!G \leq n!G$ olduğundan, $E(G) = \bigcap_n n!G$ yazılımı $E(G)$'nin daha sarih bir gösterimi olabilir. Eğer G burulmasız bir grupsa, $E(G) = D(G)$ olur, çünkü bu durumda her $k > 0$ tamsayısı için $g \mapsto kg$ fonksiyonu birebirdir, dolayısıyla

$$E(G) \geq kE(G) = k \bigcap_{n=1}^{\infty} nG = \bigcap_{n=1}^{\infty} knG \geq \bigcap_{n=1}^{\infty} nG = E(G)$$

(G'nin burulmasızlığını üçüncü adımdak eşitlikte kullandık), yani $E(G) = kE(G)$, yani $E(G)$ bölünür, yani $E(G) = D(G)$ olur. Öte yandan G burulmalıysa, $D(G) < E(G)$ olabilir. Bunun bir örneğini aşağıda bulacaksınız.

13.31. $A = \bigoplus_{k=1}^{\infty} \mathbb{Z}/2^k\mathbb{Z}$ olsun. e_k, k'ıncı koordinatı 1, diğer koordinatları 0 olan eleman olsun. A, bu elemanlar tarafından üretilir. $\mathbb{Z}/2^k$'nın elemanlarıyla e_k'yı çarpmanın anlamlı olduğunu belirtelim. Her $a \in A$ elemanı, $a_k \in \mathbb{Z}/2^k\mathbb{Z}$ sayıları için $\sum_k a_k e_k$ olarak tek bir biçimde yazılır. Buradaki a_k'ların sonlu tanesi dışında hepsi 0'dır elbette.

$$B = \langle 2^{k-1}e_k - e_1 : k = 1, 2, \ldots \rangle$$

olsun. $G = A/B$ tanımını yapalım ve $D(G)$'yi bulalım. Her $p > 2$ asalı için A grubu p-bölünür olduğundan, G de p-bölünürdür, dolayısıyla 2-bölünürlüğe odaklanmalıyız. $|D(G)| = 2$ bulacağız, dolayısıyla $D(G)$ bölünür olamayacak. Hatta $D(G) = \{1, \overline{e_1}\}$ bulacağız.

$\overline{e_1}$ elemanı 2^k-bölünür olduğundan, belli ki $\overline{e_1} \in D(G)$. Aksi istikamete odaklanalım. Önce B'nin elemanlarını daha iyi betimleyelim. B'nin rastgele bir b elemanı

$$b = \sum_{k=1}^{\infty} b_k(2^{k-1}e_k - e_1)$$

olarak yazılır. $k = 1$ iken toplanan terim 0 olduğundan, toplamı 2'den başlatabiliriz:

$$b = \sum_{k=2}^{\infty} b_k(2^{k-1}e_k - e_1).$$

Ayrıca $2(2^{k-1}e_k) = 0$ ve $2e_1 = 0$ olduğundan, b_k'yı ya 0'a ya da 1'e eşit alabiliriz. Demek ki $b_k = 0, 1$ için $(k \geq 2)$,

$$b = -\left(\sum_{k\geq 2} b_k\right) e_1 + \sum_{k\geq 2} 2^{k-1}e_k$$

olur. Bu elemanı daha görsel biçimde yazalım. $\epsilon_k = 2^{k-1} \in \mathbb{Z}/2^k\mathbb{Z}$ olsun. ϵ_k, $\mathbb{Z}/2^k\mathbb{Z}$ grubunun derecesi 2 olan yegâne elemanıdır. Demek ki b elemanı koordinatlarıyla şöyle gösterilir: $b_k \in \{0, 1\}$ için $(k \geq 2)$,

$$b = \left(-\left(\sum_{k\geq 2} b_k\right), b_2\epsilon_2, b_3\epsilon_3, \ldots\right).$$

Şimdi $\overline{x} \in D(G)$ olsun. Bir $k > 0$ tamsayısı seçelim. O zaman bir $\overline{y} \in G$ için,

$$\overline{x} = 2^k\overline{y},$$

yani

$$x - 2^k y \in B$$

olur. x'in k'ıncı koordinatına bakalım. B'nin elemanlarının olası k'ıncı koordğinatları ya 0 ya ϵ_k olduğundan, bu son eşitlikten

$$x_k = 0, \epsilon_k$$

çıkar.

Şimdi

$$b = \left(\left(\sum_{k \geq 2} x_k \right), x_2, \, x_3, \, \ldots \right) \in B$$

ve

$$a = \left(x_1 - \left(\sum_{k \geq 2} x_k \right), 0, \, 0, \, \ldots \right) \in \{0, e_1\}$$

olsun. Ya $a = 0$ ya da $a = e_1$ olur.

$$\overline{x} = \overline{x - b} = \overline{a}$$

eşitliğinden sayesinde istediğimizi elde ederiz.

Bu altbölümde[8] bölünür abel gruplarını sınıflandıracağız. Ama ilk olarak önemli bir bölünür abel grubu ailesi tanıtalım: Prüfer p-grupları. Daha sonra bölünür grupların (çeşitli p asalları için) Prüfer p-gruplarının ve $\mathbb{Q}$ grubunun direkt toplamlarına izomorf olduğunu kanıtlayacağız.

13.5.1 Prüfer p-Grupları

Prüfer p-gruplarından daha önce Örnek 9.67 ve 11.11'de sözetmiştik. Ayrıca bu gruptan Örnek D2'de de sözedildi. Bu bölümde tanımı yeniden yapacağız ve biraz daha ayrıntıya gireceğiz.

Prüfer p-gruplarının çeşitli tanımları vardır ve her birini bilmek gerekir.

Birinci Tanım. Eğer karmaşık sayıları biliyorsanız tanımı şöyle verebiliriz[9]: Küme olarak,

$$\mathbb{Z}_{p^\infty} = \{e^{2k\pi i/p^n} : n, \, k \in \mathbb{N}\}.$$

Ama tabii bu tanımda $n > 0$ ve $k = 0, 1, \ldots, p^n - 1$ olarak alınabilir. Çarpma olarak da karmaşık sayıların çarpmasını alacağız, yani e'nin kuvvetlerini toplayacağız. $\mathbb{Z}_{p^\infty}$ kümesinin çarpma altında bir grup olduğunun kolay kanıtını okura bırakıyoruz. Bu grupta,

$$\alpha_n = e^{2\pi i/p^n}$$

tanımını yapalım. O zaman, α_n'nin derecesi p^n'dir; dolayısıyla ürettiği

$$A_n = \left\langle e^{2\pi i/p^n} \right\rangle = \{e^{2k\pi i/p^n} : k = 0, 1, \ldots, p^n - 1\}$$

[8]Bu altbölüm ve sonrası grup teoriye yeni başlayanlar tarafından şimdilik atlanabilir.

[9]Karmaşık sayıları bilmeyenler bu paragrafı atlayabilirler.

altgrubu $\mathbb{Z}/p^n\mathbb{Z}$ grubuna izomorftur. Ayrıca her n için,

$$\alpha_n^p = \alpha_{n-1}$$

ve

$$A_n = \{x^p : x \in A_{n+1}\} \leq A_{n+1}$$

ve

$$[A_{n+1} : A_n] = p$$

olur. Dahası,

$$\mathbb{Z}_{p^\infty} = \bigcup_{n=1}^{\infty} A_n$$

olur. Yani $\mathbb{Z}_{p^\infty}$ grubu, $\mathbb{Z}/p^n\mathbb{Z}$ gruplarına izomorf altgrupların bileşimidir. Her elemanının derecesi p asalının bir kuvvetidir; dolayısıyla bir p-gruptur; ama grubun eksponenti sonlu değildir. $A_n = \{x^p : x \in A_{n+1}\}$ ve $\mathbb{Z}_{p^\infty} = \bigcup_{n=1}^{\infty} A_n$ eşitliklerinden $\mathbb{Z}_{p^\infty}$ grubunun p-bölünür olduğu anlaşılıyor. Ayrıca bir p-grubu olduğundan, $\mathbb{Z}_{p^\infty}$ grubu her $q \neq p$ asalı için de q-bölünürdür. Demek ki $\mathbb{Z}_{p^\infty}$ grubu bölünür bir gruptur.

İkinci Tanım. $\mathbb{Z}_{p^\infty}$ grubunun bir başka tanımı direkt limitle yapılabilir ve bu matematikçilerin favori tanımıdır. (Direkt limit için bkz. Altbölüm D.2 ve Örnek D.2. Ama bu paragrafın o ek okunmadan da hissedileceğini umuyoruz.) $\mathbb{Z}/p_n\mathbb{Z}$ grubunu $\mathbb{Z}/p^{n+1}\mathbb{Z}$ grubunun içine şu şekilde gömebiliriz:

$$\overline{x} \mapsto \hat{x}.$$

Bu fonksiyon gerçekten iyitanımlıdır çünkü $\overline{x} = \overline{y}$ ise, yani $x - y$ sayısı p^n sayısına bölünüyorsa, $px - py$ sayısı p^{n+1} sayısına gömülebilir. Böylece şu gömmeleri elde ederiz:

$$0 \hookrightarrow \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p^2\mathbb{Z} \hookrightarrow \ldots \hookrightarrow \mathbb{Z}/p^{\mathbb{Z}} \hookrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z} \hookrightarrow \ldots$$

Bu gömmelerin bileşimini alın, $\mathbb{Z}_{p^\infty}$ grubunu elde edersiniz. Eğer bunu yapmakta matematiksel olarak zorlanıyorsanız kitabın ekindeki Bölüm D.2'i okuyun.

Üçüncü Tanım. $\mathbb{Z}_{p^\infty}$ grubunun üçüncü (anlaşılması en kolay) tanımı şöyle yapılabilir: P, paydası p'nin bir kuvveti olarak yazılabilen kesirli sayılar kümesi olsun:

$$P = \{a/p^n : n \in \mathbb{Z},\, a \in \mathbb{Z}\}.$$

P toplama altında bir gruptur. Tanımda $n = 0$ alırsak $\mathbb{Z} \leq P$ olduğu görülecektir. Şimdi $\mathbb{Z}_{p^\infty}$ grubunu

$$\mathbb{Z}_{p^\infty} = P/\mathbb{Z}$$

olarak tanımlayabiliriz.

$$p^n \cdot a/p^n = a \in \mathbb{Z}$$

olduğundan, $\mathbb{Z}_{p^\infty}$ bir p-gruptur. Hatta $\mathbb{Z}_{p^\infty}$ grubu $\mathbb{Q}/\mathbb{Z}$ grubunun p-elemanlarından oluşan altgruptur, yani eğer $G = \mathbb{Q}/\mathbb{Z}$ ise, Sonuç 12.9'daki tanımla

$$G[p^\infty] = \mathbb{Z}_{p^\infty}$$

olur. O sonuca göre de,

$$\mathbb{Q}/\mathbb{Z} \simeq \bigoplus_{p\text{asal}} \mathbb{Z}_{p^\infty}$$

olur.

$$a_n = 1/p^n \in P$$

ve

$$\alpha_n = \overline{a_n}$$

tanımlarını yapalım. α_n derecesi p^n olan bir elemandır; dolayısıyla ürettiği

$$A_n = \langle \alpha_n \rangle = \{k\alpha_n : k = 0, 1, \ldots, p^n - 1\}$$

altgrupu $\mathbb{Z}/p^n\mathbb{Z}$ grubuna izomorftur. Ayrıca, her n için,

$$p\alpha_n = \alpha_{n-1}$$

ve

$$A_n = \{px : x \in A_{n+1}\} \leq A_{n+1}$$

olur. Dahası,

$$\mathbb{Z}_{p^\infty} = \bigcup_{n=1}^{\infty} A_n$$

olur. Yani $\mathbb{Z}_{p^\infty}$ grubu, $\mathbb{Z}/p^n\mathbb{Z}$'ye izomorf altgrupların bileşimidir, dolayısıyla bir p-gruptur; ama grubun eksponenti sonlu değildir. $A_n = \{px : x \in A_{n+1}\}$ ve $\mathbb{Z}_{p^\infty} = \bigcup_{n=1}^{\infty} A_n$ eşitliklerinden $\mathbb{Z}_{p^\infty}$ grubunun p-bölünür olduğu anlaşılıyor. Ayrıca bir p-grubu olduğundan, $\mathbb{Z}_{p^\infty}$ grubu her $q \neq p$ asalı için de q-bölünürdür. Demek ki $\mathbb{Z}_{p^\infty}$ grubu bölünür bir gruptur. Ayrıca $\mathbb{Z}_{p^\infty}$ grubunun her elemanı α_n^k olarak yazılabilir. Eğer dilersek n'yi elemanın derecesine eşit ve k'yı da p'ye asal alabiliriz.

Önsav 13.21. *$\mathbb{Z}_{p^\infty}$ grubunun özaltgrupları, yukarıda tanımı verilen A_n altgruplarıdır. Dolayısıyla $\mathbb{Z}_{p^\infty}$ grubunun özaltgrupları $\mathbb{Z}/p^n\mathbb{Z}$ gruplarına izomorfturlar.*

Kanıt: Önce,

$$\{x \in \mathbb{Z}_{p^\infty} : p^n x = 0\} = A_n$$

eşitliğinin farkına varalım. Bu eşitlik $\mathbb{Z}_{p^\infty}$ grubunun tanımından hemen çıkar. $A \leq \mathbb{Z}_{p^\infty}$ olsun. Eğer A sonluysa, A'da derecesi en büyük olan bir eleman seçelim. Eğer bu eleman a ve derecesi de p^n ise, $A = A_n$ olur. Eğer A sonsuzsa, o zaman A'da dereceleri sonsuza kadar artan elemanlar bulunur. Demek ki her $n \in \mathbb{N}$ için $A_n \leq A$ olur. Bundan da $\mathbb{Z}_{p^\infty} = \bigcup_n A_n \leq A \leq \mathbb{Z}_{p^\infty}$, yani $A = \mathbb{Z}_{p^\infty}$ eşitliği çıkar. □

Birazdan bölünür p-gruplarının $\mathbb{Z}_{p^\infty}$ grubuna izomorf altgruplarının direkt toplamı olduğunu kanıtlayacağız. Şimdilik, ileride de kullanacağımız aşağıdaki sonuçla yetinelim.

Önsav 13.22. *Bölünür ve* 1*'den farklı bir* p*-grupta* $\mathbb{Z}_{p^\infty}$ *grubuna izomorf bir altgrup vardır.*

Kanıt: Gruba G diyelim ve G'yi toplamsal yazalım. $x_1 \in G$ derecesi p olan bir eleman olsun. Tümevarımla $px_{n+1} = x_n$ eşitliğini sağlayan elemanlar bulalım.

$$H = \langle x_1, \ldots, x_n, \ldots \rangle$$

olsun. Metindeki α_n elemanlarını anımsayalım.

$$\alpha_n \mapsto x_n$$

fonksiyonu $\mathbb{Z}_{p^\infty}$'ten H'ye giden bir izomorfidir. Ayrıntıları okura bırakıyoruz. □

Alıştırmalar

13.32. $\mathbb{Z}_{p^\infty}$ grubunun sonlu sayıda elemanla üretilemediğini kanıtlayın.

13.33. Bölünür ve 1'den farklı bir grubun sonlu sayıda eleman tarafından üretilemeyeceğini kanıtlayın.

13.34. $\mathbb{Z}_{p^\infty}$ grubunun üçüncü tanımından ve $\mathbb{Q}/\mathbb{Z}$ grubunun Prüfer p-gruplarının altgruplarının direkt toplamına izomorf olduğu çıkar. Önsav 13.21'de $\mathbb{Z}_{p^\infty}$ grubunun altgruplarının ya $\mathbb{Z}_{p^\infty}$ grubunun kendisi olduğunu ya da bir $n \in \mathbb{N}$ doğal sayısı için

$$\{\overline{q} : \text{bir } a \in \mathbb{Z} \text{ ve } n \in \mathbb{N} \text{ için } q = a/p^n\} = \{x \in \mathbb{Z}_{p^\infty} : p^n x = 0\} \simeq \mathbb{Z}/p^n\mathbb{Z}$$

grubuna izomorf olduğunu gösterdik.

13.35. $\mathbb{Q}$ toplamsal grubunun altgruplarını sınıflandıralım. $0 \neq A \leq \mathbb{Q}$ olsun. O zaman $A \cap \mathbb{Z} \neq 0$ olur. Diyelim $n > 0$ doğal sayısı için $A \cap \mathbb{Z} = n\mathbb{Z}$ oluyor. A yerine $\frac{1}{n}A$ altgrubunu alarak, n'nin 1 olduğunu, yani $\mathbb{Z} \leq A$ varsayımını yapabiliriz. (Bu varsayımla A'yı bulursak, genel durumdaki altgrubu bulduğumuz grubun elemanlarını n ile çarparak buluruz.) Dolayısıyla $\mathbb{Z} \leq A$ varsayımını yaparak $\mathbb{Q}/\mathbb{Z}$'nin $A/\mathbb{Z}$ altgrubunun hangi kesirli sayılardan oluştuğunu bulmak yeterli (bkz. Teorem 11.1). Örnek 12.2 ve hemen sonrasından, eğer $\mathbb{P}$ tüm asal sayılardan oluşan kümeyse, bir $\mathbb{P}_1 \subseteq \mathbb{P}$ ve (sonlu ya da sonsuz) bir $(n(p))_{p \in \mathbb{P}_1}$ doğal sayı dizisi için,

$$A \simeq \left(\bigoplus_{\mathbb{P}_1} \mathbb{Z}/p^{n(p)}\mathbb{Z} \right) \oplus \left(\bigoplus_{\mathbb{P}_2} \mathbb{Z}_{p^\infty} \right)$$

olduğu anlaşılır. Yani,

$$A = \{a/b : a,\, b \in \mathbb{Z},\ \text{eğer } p \in \mathbb{P}_1 \text{ asalı } b\text{'yi bölüyorsa, } p^{n(p)+1} \text{ sayısı } b\text{'yi bölmez}\}$$

olur. Demek ki $\mathbb{Q}$ grubunun altgrupları, $n \in \mathbb{N}$ ve $\mathbb{P}_1 \subseteq \mathbb{P}$ için,

$$A = \{a/b : a \in n\mathbb{Z},\ b \in \mathbb{Z},\ \text{eğer } p \in \mathbb{P}_1 \text{ asalı } b\text{'yi bölüyorsa, } p^{n(p)+1} \text{ sayısı } b\text{'yi bölmez}\}$$

biçimindedir.

13.36. Bundan sonraki alıştırmalarda amacımız $\operatorname{End}\mathbb{Z}_{p^\infty}$ yapısını (toplama ve bileşke altında) anlamak olacak. $\mathbb{Z}_{p^\infty}$ grubunun ikinci tanımını kabul edeceğiz, yani $\mathbb{Z}_{p^\infty} = P/\mathbb{Z}$ olacak; dolayısıyla grup işlemini toplama olarak yazacağız. $A_n \simeq \mathbb{Z}/p^n\mathbb{Z}$ metindeki gibi olacak. Eğer $a \in \mathbb{Z}/p^n\mathbb{Z}$ ise

$$\lambda_a : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

fonksiyonu

$$\lambda_a(x) = ax$$

olarak tanımlansın.

$$\operatorname{End}(\mathbb{Z}/p^n\mathbb{Z}) = \{\lambda_a : a \in \mathbb{Z}/p^n\mathbb{Z}\}$$

olduğunu biliyoruz (bkz. Örnek 10.51). Bir abel grubunun andomorfi kümesinin toplama altında bir grup olduğunu ve ayrıca bileşke işlemi altında kapalı olduğunu biliyoruz (bkz. Örnek 10.50). Ayrıca $\lambda_a + \lambda_b = \lambda_{a+b}$ ve $\lambda_a \circ \lambda_b = \lambda_{ab}$ olur. $\lambda_a(1) = a$ olduğundan, eğer $f \in \operatorname{End}\mathbb{Z}/p^n\mathbb{Z}$ ise $f = \lambda_{f(1)}$ olur. Aşağıdaki alıştırmalara geçmeden önce okur bu olguları özümsemeli.

13.37. Eğer $f \in \operatorname{End}\mathbb{Z}_{p^\infty}$ ise, $f(A_n) \leq A_n$ içindeliğini kanıtlayın (demek ki $f_{|A_n} \in \operatorname{End} A_n$ olur). Eğer $f \in \operatorname{Aut}\mathbb{Z}_{p^\infty}$ ise, $f(A_n) = A_n$ eşitliğini kanıtlayın (demek ki $f_{|A_n} \in \operatorname{Aut} A_n$ olur). Bundan böyle $f \in \operatorname{End}\mathbb{Z}_{p^\infty}$ için $f_n = f_{|A_n} \in \operatorname{End} A_n$ yazalım.

13.38. $\varphi : \operatorname{End}\mathbb{Z}_{p^\infty} \longrightarrow \prod_n \operatorname{End} A_n$ fonksiyonu,

$$\varphi(f) = (f_n)_n$$

eşitliğiyle tanımlanmış olsun. φ'nin bir grup homomorfisi olduğunu, yani her $f, g \in \operatorname{End}\mathbb{Z}_{p^\infty}$ için $\varphi(f+g) = \varphi(f) + \varphi(g)$ eşitliğini kanıtlayın.

13.39. $\mathbb{Z}_{p^\infty}$ ve A_n abel grupları olduklarından, $\operatorname{End}\mathbb{Z}_{p^\infty}$ ve $\operatorname{End} A_n$ grupları, toplama altında kapalı oldukları gibi, bileşke işlemi altında kapalıdır. $(f_n)_n$, $(g_n)_n \in \prod_n \operatorname{End} A_n$ için

$$(f_n)_n \circ (g_n)_n = (f_n \circ g_n)_n$$

tanımını yapalım. Her $f, g \in \operatorname{End}\mathbb{Z}_{p^\infty}$ için $\varphi(f \circ g) = \varphi(f) \circ \varphi(g)$ eşitliğini kanıtlayın.

13.40. $f \in \operatorname{End}\mathbb{Z}_{p^\infty}$ için, $\psi(f) = (f_n(1))_n \in \prod_n \mathbb{Z}/p^n\mathbb{Z}$ olsun. ψ'nin $\operatorname{End}\mathbb{Z}_{p^\infty}$ grubundan $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ grubuna giden bir homomorfi olduğunu ve ayrıca $\psi(f \circ g) = \psi(f) \cdot \psi(g)$ eşitliğinin sağlandığını kanıtlayın. ($\prod_n \mathbb{Z}/p^n\mathbb{Z}$ grubunda çarpma, aynen toplama gibi, koordinat koordinat, yani terim terim yapılır.)

13.41. $f_{n+1}(1) \equiv f_n(1) \bmod p^n$ denkliğini kanıtlayın.

13.42. $f_n(1)$ sayılarını 0 ile $p^n - 1$ arasında bir tamsayı olarak görelim. $f_n(1)$'i p tabanında yazalım: $a_0,\, a_1,\, a_2, \ldots, a_{n-1} \in \{0, 1, 2, \ldots, p-1\}$ için,

$$f_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}.$$

Bir önceki alıştırmadan, bir $a_n \in \{0,\, 1,\, 2,\, \ldots,\, p-1\}$ için,

$$f_{n+1} = f_n + a_n p^n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} + a_n p^n$$

eşitliğini kanıtlayın.

13.43. Bir önceki alıştırmadan, bir $f \in \operatorname{End}\mathbb{Z}_{p^\infty}$ andomorfisinin $a_i \in \{0, 1, 2, \ldots, p-1\}$ için,

$$\sum_{i=0}^{\infty} a_i p^i$$

biçiminde gösterilebileceğini kanıtlayın. Bu tür toplamlara ***p*-sel sayı** adı verilir.

13.44. Eğer f, $g \in \operatorname{End}\mathbb{Z}_{p^\infty}$ elemanları bir önceki alıştırmadaki gibi

$$\sum_{i=0}^{\infty} a_i p^i \text{ ve } \sum_{i=0}^{\infty} b_i p^i$$

p-sel sayılarına karşılık geliyorlarsa, $f+g$ ve $f \circ g$ andomorfileri hangi p-sel sayıya karşılık gelirler?

13.5.2 Bölünür Abel Gruplarının Sınıflandırılması

Bu altbölümde, yapacağımız her şeyin temelini teşkil edecek olan şu teoremi kanıtlayacağız.

Teorem 13.23. *Bölünür bir G abel grubu $\mathbb{Q}$ ve asal p sayıları için $\mathbb{Z}_{p^\infty}$ gruplarının direkt toplamına izomorftur; yani I_0 ve $(I_p)_{p \text{ asal}}$ kümeleri (ya da kardinalleri) için*

$$G \simeq \mathbb{Q}^{(I_0)} \oplus \left(\bigoplus_{p \text{ asal}} \mathbb{Z}_{p^\infty}^{(I_p)} \right)$$

olur. Ayrıca $|I_0|$ ve $|I_p|$ kardinalleri G'nin izomorfi tipini belirlerler, yani değişmezleridir.

Kanıt altbölümün sonuna kadar sürecek.

İlk teoremimiz çok yararlı olacak:

Teorem 13.24. *Bir abel grubunun bölünür bir altgrubunun tümleyeni vardır.*

Kanıt: Abel grubuna G, bölünür altgruba da D diyelim. $\mathcal{Z}$ kümesini şöyle tanımlayalım:

$$\mathcal{Z} = \{B \leq G : B \cap D = 1\}.$$

1 altgrubu $\mathcal{Z}$'de olduğundan, $\mathcal{Z} \neq \emptyset$ olur. $\mathcal{Z}$'yi altgrup olma ilişkisiyle sıralayalım, her zamanki gibi altgruplar küçük, üstgruplar büyük olsun. Eğer $\mathcal{C} \subseteq \mathcal{Z}$ bir zincirse, elbette $\bigcup \mathcal{Z} \in \mathcal{Z}$ olur. Demek ki $\mathcal{Z}$ yarısıralı kümesine Zorn Önsavı'nı uygulayabiliriz. Demek ki $B \cap D = 1$ eşitliğini sağlayan maksimal bir B altgrubu vardır. Eğer $G = DB$ ise, o zaman $G = D \oplus B$ olur ve teorem kanıtlanır. Bundan böyle $DB < G$ varsayımını yapalım. $D \cap \langle B, g \rangle = 1$ eşitliğini sağlayan bir $g \notin B$ bularak bir çelişki elde edeceğiz.

Önce rastgele bir $g \in G \setminus DB$ elemanı seçelim. g'yi yavaş yavaş değiştirip tam istediğimiz biçimde bir elemana dönüştüreceğiz.

$B < \langle B, g\rangle$ olduğundan,

$$D \cap \langle B, g\rangle \neq 1$$

olur. Bu kesişimde 1'e eşit olmayan bir eleman seçelim: Diyelim $d \in D$, $b \in B$ ve $n \in \mathbb{Z}$ için,

$$1 \neq d = bg^n \in D \cap \langle B, g\rangle.$$

$n \neq 0$ olmalı, çünkü aksi halde $d = b \in D \cap B = 1$ olur. Gerekirse, yukarıdaki eşitlikte tarafların terslerini alarak $n > 0$ varsayımını yapabiliriz. (g'yi ilk kez değiştirdik.)

Yukarıdaki eşitlikten

$$g^n = db^{-1} \in DB$$

çıkar. Şimdi n'yi asalların çarpımı olarak yazalım: $n = p_1 p_2 \cdots p_k$. Böylece

$$g,\ g^{p_1},\ g^{p_1 p_2},\ \ldots,\ g^{p_1 p_2 \cdots p_k} = g^n \in DB$$

dizisi elde ederiz. Bu dizinin birinci terimi DB'de değil, ama sonuncu terimi DB'de. Diziyi soldan sağa tarayarak DB'ye düşmeyen ilk terimi alalım. Yukarıdaki notasyonu değiştirerek, g'yi bu eleman olarak alabiliriz. Böylece $g \notin DB$, ama bir p asalı için $g^p \in DB$ varsayımını yapabiliriz. (g'yi ikinci kez değiştirdik.)

Şimdi yukarıdaki d ve b elemanlarını unutup, $d \in D$ ve $b \in B$ için

$$g^p = db$$

yazalım. $d_1 \in D$ elemanı $d_1^p = d$ eşitliğini sağlasın. O zaman

$$g^p = db = d_1^p b$$

ve

$$(d_1^{-1} g)^p = b \in B$$

elde ederiz. Şimdi g yerine $d_1^{-1} g$ elemanını bulursak,

$$g \in G \setminus DB, \text{ ve } g^p \in B$$

içindeliklerini buluruz. (g'yi üçüncü kez değiştirdik.)

Gene yukarıdaki d ve b elemanlarını unutalım ve ta en baştan başlayalım. $B < \langle B, g\rangle$ olduğundan,

$$D \cap \langle B, g\rangle \neq 1$$

olur. Bu kesişimde 1'e eşit olmayan bir eleman seçelim: Diyelim $d \in D$, $b \in B$ ve $n \in \mathbb{Z}$ için,

$$1 \neq d = bg^n \in D \cap \langle B, g\rangle.$$

Demek ki $g^n \in DB$. Ama ayrıca $g^p \in B \leq DB$. Eğer n ve p aralarında asalsa, bunlardan $g \in DB$ çıkar (bkz. Alıştırma 5.31), ki bu bir çelişkidir. Demek ki p, n'yi böler. Ama bundan da $g^n \in B$ çıkar. Demek ki,

$$1 \neq d = bg^n \in D \cap B = 1,$$

gene bir çelişki. □

Sonuç 13.25. *Her G abel grubunun maksimum bir bölünür altgrubu vardır. Bu maksimum bölünür altgrup tüm bölünür altgrupları içerir. Eğer bu altgruba D dersek, bir $B \leq G$ için $G = D \oplus B$ olur. B altgrubunun 1'den farklı bölünür bir altgrubu yoktur.*

Kanıt: Bölünür altgrupların ürettiği altgrup bölünür olduğundan, D'yi tüm bölünür altgrupların ürettiği altgrup olarak alalım. Geri kalan her şey Teorem 13.24'den çıkar. □

Demek ki abel gruplarını sınıflandırmak için, 1'den farklı bölünür altgrubu olmayan abel gruplarını sınıflandırmak yeterlidir.

Aşağıdaki önsav sayesinde bölünür grupların analizini burulmalı ve burulmasız bölünür gruplar olarak ikiye ayırabileceğiz.

Sonuç 13.26. *G bölünür bir grup olsun. T, G'nin burulmalı elemanlarından oluşan bir altgrup olsun. O zaman bir $D \leq G$ için $G = T \oplus D$ olur. Ayrıca T ve D bölünürdür ve D burulmasız bir gruptur.*

Kanıt: $t \in T$ ve $n > 0$ bir tamsayı olsun. G bölünür olduğundan $x^n = t$ denkleminin G'de bir çözümü vardır. Eğer g bir çözümse, elbette $g^{n \deg t} = t^{\deg t} = 1$ olur, yani $g \in T$ olur. Demek ki T bölünür bir gruptur. Teorem 13.24'e göre T'nin G'de bir tümleyeni vardır, diyelim D. Demek ki $G = T \oplus D$. Bundan da D'nin bölünür olduğu çıkar. Ayrıca D'nin burulmalı elemanları T'de olmak zorunda olduğundan, D burulmasızdır. □

Sonuç 12.9'a göre yukarıdaki sonuçtaki T grubu, asal p ve

$$T[p^\infty] = \{t \in T : \text{bir } i \in \mathbb{N} \text{ için } t^{p^i} = 1\}$$

altgruplarının direkt toplamına izomorftur:

$$T \simeq \bigoplus_{p \text{ asal}} T[p^\infty].$$

Buradan şu sonucu elde ederiz:

Sonuç 13.27. *G bölünür bir grup olsun. Asal p için,*

$$G[p^\infty] = \{g \in G : \textit{bir } i \in \mathbb{N} \textit{ için } g^{p^i} = 1\}$$

olsun. O zaman $G[p^\infty] \leq G$ bölünür bir p-gruptur. Ayrıca burulmasız ve bölünür bir D altgrubu için, $G = \left(\bigoplus_{p \text{ asal}} G[p^\infty]^{(I_p)}\right) \oplus D$ olur. □

Demek ki bölünür grupları sınıflandırmak için bölünür p-gruplarını ve bölünür burulmasız grupları sınıflandırmamız lazım. Bunu da şimdi yapıyoruz.

Teorem 13.28. *Burulmasız ve bölünür bir grup $\mathbb{Q}$ gruplarının direkt toplamıdır.*

Kanıt: Gruba A diyelim ve grubun işlemini toplamsal olarak yazalım. Eğer $m \neq 0$ bir tamsayı ve $a \in A$ ise, $a = mx$ denkleminin A'da bir çözümü vardır, çünkü A bölünür bir grup; ama ayrıca, A burulmasız olduğundan bu çözüm biriciktir, nitekim eğer $a = mx$ ve $a = my$ olsaydı, $m(x-y) = 0$ ve dolayısıyla $x - y = 0$ ve $x = y$ olurdu. Bundan böyle bu çözümü

$$\frac{1}{m}\, a$$

olarak gösterelim. Demek ki

$$x = \frac{1}{m}\, a \Leftrightarrow mx = a.$$

Şimdi herhangi bir q kesirli sayısını alalım. Amacımız A'nın rastgele bir elemanını q kesirli sayısıyla çarpmak. Önce q sayısını n, $m \in \mathbb{Z}$ için n/m olarak yazalım ve bir $a \in A$ için qa elemanını

$$qa = \frac{n}{m}\, a = \frac{na}{m}$$

olarak tanımlayalım. Yani,

$$x = qa \Leftrightarrow mx = na$$

önermesi doğru olsun. Bu tanımın q sayısının n/m olarak gösteriminden bağımsız olduğunu göstermek zorundayız. Nitekim eğer $n/m = n'/m'$, $mx = na$ ve $m'y = n'a$ ise, sırasıyla $nm' = n'm$,

$$n'mx = n'na = nn'a = nm'y = n'my$$

ve A burulmasız olduğundan $x = y$ olur. Demek ki qa çarpımının tanımında bir sorun yok. Bu çarpım çeşitli özdeşlikler sağlar. Örneğin,

$$q(a + a') = qa + qa',\ (q + q')a = qa + q'a,\ q'(qa) = (q'q)a,\ 0a = 0.$$

Ayrıca $q \in \mathbb{Z}$ olduğunda, qa'nın bu tanımı eski tanıma eşittir[10]. Demek ki artık, $a \in A$ için

$$\mathbb{Q}a = \{qa : q \in \mathbb{Q}\}$$

[10]Biraz lineer cebir bilen bir okur, A abel grubunun bu tanım sayesinde $\mathbb{Q}$ cismi üzerine bir vektör uzayı olduğunu görecektir.

anlamlı ve A'nın bir altgrubu. Ayrıca bir $X \subset \mathbb{Q}$ için

$$\left\langle \bigcup_{x\in X} \mathbb{Q}x \right\rangle = \sum_{x\in X} \mathbb{Q}\, x$$

olur ve bu altgrup elbette bölünür bir gruptur.

Hepsi 0'a eşit olmayan $q_1, \ldots, q_n \in \mathbb{Q}$ kesirli sayıları ve birbirinden farklı $x_1, \ldots, x_n \in A$ elemanları için,

$$q_1 a_1 + \cdots + q_n a_n = 0$$

türünden bir eşitliğe ***doğrusal bağımlılık*** denir. $X \subseteq A$ olsun. Eğer X'in elemanları arasında doğrusal bağımlılık yoksa, X kümesine ***doğrusal bağımsız küme*** diyelim. Demek ki $X \subseteq A$ kümesinin doğrusal bağımsız olması için birbirinden farklı $x_1, \ldots, x_n \in X$ elemanları için,

$$q_1 x_1 + \cdots + q_n x_n = 0$$

eşitliği ancak

$$q_1 = \ldots = q_n = 0$$

ise doğru olabilmeli. Bundan da şu çıkar: Eğer $X \subseteq A$ doğrusal bağımsızsa, o zaman,

$$\sum_{x\in X} \mathbb{Q}x = \bigoplus_{x\in X} \mathbb{Q}x$$

olur. Amacımız, doğrusal bir $X \subseteq A$ için $\sum_{x\in X} \mathbb{Q}x = A$ eşitliğinin doğru olduğu. $q \mapsto qx$ kuralı $\mathbb{Q}$ grubuyla $\mathbb{Q}x$ altgrubu arasında bir izomorfi olduğundan, böylece teoremimiz kanıtlanmış olacak. X'i maksimal doğrusal bağımsız bir küme olarak seçeceğiz. Önce maksimal doğrusal bağımsız kümenin varlığını kanıtlayalım.

Sav 1. *A'nın maksimal bir doğrusal bağımsız altkümesi vardır.*

Sav 1'in Kanıtı. $\mathcal{Z}$, elemanları A'nın doğrusal bağımsız altkümelerinden oluşan küme olsun. $\emptyset \in \mathcal{Z}$ olduğundan (neden?), $\mathcal{Z}$ boşküme değildir. $\mathcal{Z}$'yi altküme olma ilişkisi altında küçükten büyüğe yarısıralayalım. $\mathcal{C} \subseteq \mathcal{Z}$ bir zincir olsun. $\bigcup \mathcal{C} \in \mathcal{Z}$ olduğunu, yani $\bigcup \mathcal{C}$ kümesinin doğrusal bağımsız olduğunu savlıyorum ve hemen kanıtına geçiyorum. $x_1, \ldots, x_n \in \mathcal{C}$ birbirinden farklı elemanlar olsun. Diyelim, $C_1, \ldots, C_n \in \mathcal{C}$ için $x_i \in C_i$. Ama $\mathcal{C}$ bir zincir olduğundan, bu C_i'lerden biri diğerlerini kapsar. Diyelim C_k diğerlerini kapsıyor. O zaman $x_1, \ldots, x_n \in C_k$ olur, ki C_k doğrusal bağımsız olduğundan bu bariz bir çelişkidir. Demek ki $\mathcal{Z}$ tümevarımsal bir küme. Zorn Önsavı'na göre A'da maksimal bir doğrusal küme vardır. Sav 1 kanıtlanmıştır. □

Sav 2. *Eğer $X \subseteq A$, maksimal doğrusal bağımsız bir altkümesiyse, $A = \sum_{x\in X} \mathbb{Q}x$ olur.*

Sav 2'nin Kanıtı. Diyelim $\sum_{x\in X}\mathbb{Q}x < A$. O zaman $A \setminus \sum_{x\in X}\mathbb{Q}x$ kümesinden herhangi bir y elemanı alalım. $X \cup \{y\}$ kümesinin doğrusal bağımsız olduğunu kanıtlayacağız ve böylece X'in maksimalliğiyle çelişeceğiz. Nitekim eğer, birbirinden farklı $x_1, \ldots, x_n \in X$ ve y elemanları arasında doğrusal bir bağımlılık olsaydı, o zaman hepsi 0 olmayan $q_1, \ldots, q_n$, $q \in \mathbb{Q}$ sayıları için,

$$q_1x_1 + \cdots + q_nx_n + qy = 0$$

olurdu. Eğer $q = 0$ ise, X'in doğrusal bağımsız $x_1, \ldots, x_n$ elemanları arasında

$$q_1x_1 + \cdots + q_nx_n = 0$$

bağıntısı olurdu ve bu da $q_1 = \ldots = q_n = 0$ eşitliklerini gerektirirdi, ki bu da $q_1, \ldots, q_n$, $q \in \mathbb{Q}$ sayılarının hepsinin 0 olmamasıyla çelişir. Demek ki $q \neq 0$. Ama bu durumda da y'yi x_i'ler cinsinden yazabiliriz:

$$y = \frac{-q_1}{q}\, x_1 + \cdots + \frac{-q_n}{q}\, x_n,$$

ki bu da y'nin seçimiyle çelişir. Sav 2 de kanıtlanmıştır. □

Bu iki sav teoremi tamamen kanıtlar. □

Teorem 13.29. *Bölünür bir p-grubu Prüfer p-gruplarının direkt toplamıdır.*

Kanıt: G bölünür bir p-grup olsun. X, G'nin bir altgrup kümesi olsun; yani X'in her elemanı G'nin bir altgrubu olsun. Eğer X'in her altgrubu $\mathbb{Z}_{p^\infty}$ grubuna izomorf ise ve

$$\langle A : A \in X\rangle = \bigoplus_{A\in X} A$$

oluyorsa, X'e bu kanıtlık güzel küme diyelim. Elbette $\emptyset$ güzel bir kümedir. $\mathcal{Z}$ kümesi güzel kümelerden oluşsun. $\mathcal{Z}$'yi kapsama ilişkisiyle küçükten büyüğe doğru yarısıralayalım. Böylece yarısıralanmış $\mathcal{Z}$ kümesine Zorn Önsavı'nı uygulayacağız, ama önce $\mathcal{Z}$ kümesinin tümevarımsal olduğunu göstermeliyiz. Bu amaçla bir $\mathcal{C} \subseteq \mathcal{Z}$ zinciri seçelim. $\bigcup\mathcal{C}$'nin elemanları elbette G'nin $\mathbb{Z}_{p^\infty}$ grubuna izomorf altgruplarıdır. Teorem 12.8'ye göre

$$\left\langle A : A \in \bigcup\mathcal{C}\right\rangle = \bigoplus_{A\in\bigcup\mathcal{C}} A$$

olur. Demek ki $\bigcup\mathcal{C} \in \mathcal{Z}$. Demek ki Zorn Önsavı'na göre $\mathcal{Z}$'nin maksimal bir elemanı vardır. Bu elemana $\mathcal{M}$ ve ürettiği guruba H diyelim.

H, bölünür $\mathbb{Z}_{p^\infty}$ gruplarının direkt toplamı olduğu için bölünür bir altgruptur. Dolayısıyla Teorem 13.24'e göre bir $K \leq H$ için $G = H \oplus K$ olur. Eğer

$K \neq 1$ ise, Önsav 13.22'ye göre K'nın $\mathbb{Z}_{p^\infty}$ grubuna izomorf bir altgrup vardır, ki bu da $\mathcal{M}$'nin maksimalliğiyle çelişir. Demek ki $K = 1$ olmalı. □

Böylece Sonuç 13.27, Teorem 13.29 ve Teorem 13.28 sayesinde, bölünür grupları Teorem 13.23'te söylendiği gibi sınıflandırmış olduk. Tek eksiğimiz, teoremdeki kardinallerin biricikliği. Onu da şimdi üç aşamada kanıtlıyoruz.

Önsav 13.30. *p bir asal olsun. $\mathbb{Z}_{p^\infty}^{(I)} \simeq \mathbb{Z}_{p^\infty}^{(J)}$ ise $|I| = |J|$ olur.*

Kanıt: $\mathbb{Z}_{p^\infty}$ sayılabilir olduğundan, gruplardan biri sayılamaz sonsuzluktaysa,

$$|I| = \left|\mathbb{Z}_{p^\infty}^{(I)}\right| = \left|\mathbb{Z}_{p^\infty}^{(J)}\right| = |J|$$

olur. Bundan böyle grupların sayılabilir sonsuzlukta olduklarını varsayalım. Demek ki I ve J (sonlu ya da sonsuz) sayılabilir kümeler.

G ve H varsayımdaki izomorfik gruplar olsun. G_p ve H_p, derecesi $\leq p$ olan elemanlardan oluşan altgruplar olsun. O zaman,

$$(\mathbb{Z}/p\mathbb{Z})^{(I)} \simeq G_p \simeq H_p \simeq (\mathbb{Z}/p\mathbb{Z})^{(J)}$$

olur. Eğer G_p ya da H_p gruplarından biri sonluysa, ikisi de sonlu olmak zorunda, hatta eleman sayıları $p^{|I|}$ ve $p^{|J|}$ olmalı. Demek ki $|I| = |J|$. Eğer Eğer G_p ya da H_p gruplarından biri sonsuzsa, $|I| = \omega = |J|$ olmalı. □

Önsav 13.31. *$\mathbb{Q}^{(I)} \simeq \mathbb{Q}^{(J)}$ ise $|I| = |J|$ olur*[11].

Kanıt: Eğer gruplardan biri sayılamaz sonsuzluktaysa, önsav, aynen bir önceki önsav gibi kanıtlanır. Bundan böyle her iki grubun da sayılabilir sonsuzlukta olduklarını varsayalım. Demek ki I ve J sayılabilir kümeler. Eğer hem I hem J sonsuzsa, sorun yok, $|I| = \omega = |J|$ olur. İkisinden en az birinin sonlu olduğunu varsayalım, diyelim $|I| = n < \infty$. Diyelim $|I| \neq |J|$. Gerekirse I yerine J, J yerine I alarak, $|J|$ sonlu da olsa sonsuz da olsa $|I| < |J|$ varsayımını yapabiliriz.

$A = \mathbb{Q}^{(I)} = \bigoplus_{i=1}^{m} \mathbb{Q}$ ve $B = \mathbb{Q}^{(J)}$ olsun. $\varphi : B \longrightarrow A$ bir izomorfi olsun. B'den $n+1$ tane doğrusal bağımsız eleman alalım: $b_1, \ldots, b_{n+1}$. Bu elemanlar, B'nin $\mathbb{Z}^{n+1}$ grubuna izomorfik bir altgrup üretirler. φ birebir olduğundan, bu elemanların φ-imgeleri de doğrusal bağımsızdırlar ve bunlar da A'nın $\mathbb{Z}^{n+1}$ grubuna izomorfik bir altgrubunu üretirler, diyelim A_1. Teorem 10.24'e göre, A_1'in her i'inci izdüşümü ya 0 ya da $\mathbb{Z}$'ye izomorf. Bu izdüşüme A_{1i} diyelim. Demek ki, eğer tam k tane $A_{1i} \neq 0$ ise,

$$\mathbb{Z}^{n+1} \simeq A_1 \leq \oplus_{i=1}^{n} A_{1i} \simeq \mathbb{Z}^k$$

olur. Ama $k \leq n < n+1$ olduğundan, bu Teorem 13.6 ile çelişir. □

[11] Lineer cebir bilen bir okur için bu önsav çok kolay, ne de olsa gruplar $\mathbb{Q}$ üzerine birer vektör uzayıdır ve boyutları sırasıyla $|I|$ ve $|J|$'dir. Vereceğimiz kanıt da aslında lineer cebirin bu teoremini kanıtlayacak.

Teorem 13.32. *Eğer*

$$\mathbb{Q}^{(I_0)} \oplus \left(\bigoplus_{p \ asal} \mathbb{Z}_{p^\infty}^{(I_p)} \right) \simeq \mathbb{Q}^{(J_0)} \oplus \left(\bigoplus_{p \ asal} \mathbb{Z}_{p^\infty}^{(J_p)} \right)$$

ise $|I_0| = |J_0|$ *ve her* p *asalı için* $|I_p| = |J_p|$ *olur.*

Kanıt: G ve H varsayımdaki izomorfik gruplar olsun. $T(G)$ ve $T(H)$ derecesi sonlu olan elemanlardan oluşan altgrup olsun. Elbette $T(G) \simeq T(H)$ olur. Buradan da

$$\mathbb{Q}^{(I_0)} \simeq G/T(G) \simeq G/T(H) \simeq \mathbb{Q}^{(J_0)}$$

ve Önsav 13.31'den $|I_0| = |J_0|$ çıkar. Asal bir p için, $T(G)_p$ ve $T(H)_p$, grupların p-elemanlarından oluşan altgruplar olsun. $T(G) \simeq T(H)$ izomorfisinden, $T(G)_p \simeq T(H)_p$ çıkar. Demek ki

$$\mathbb{Z}_{p^\infty}^{(I_p)} \simeq T(G) \simeq T(H) \simeq \mathbb{Z}_{p^\infty}^{(J_p)}.$$

Önsav 13.30'dan $|I_p| = |J_p|$ çıkar. □

Teorem 13.23'ün kanıtı tamamlanmıştır.

Teoremdeki $|I_0|$ ve $|I_p|$ kardinal sayılarına grubun ***Ulm değişmezleri*** adı verilir.

13.6 Abel Gruplarının Saf Altgrupları

G bir abel grubu ve $H \leq G$ olsun. H'nin bir elemanının G'de n'inci kökü olabilir ama H'de olmayabilir. Örneğin $G = \mathbb{Z}$, $H = 2\mathbb{Z}$ ise, H'nin 2 elemanının G'de "karekökü" vardır: 1, ama aynı elemanın H'de karekökü yoktur. Eğer her $h \in H$ elemanı ve $n > 0$ tamsayısı için $x^n = h$ eşitliğinin G'de bir çözümü olduğunda, bu denklemin H'de de bir çözümü varsa, H'ye G'nin ***saf altgrubu*** adı verilir. Eğer işlemi toplama altında yazarsak, saf altgrup demek, her $n > 0$ tamsayısı için $nG \cap H = nH$ demektir.

Bu altbölümde her grup bir abel grubu olacak.

Notlar ve Örnekler

13.45. Tümleyeni olan algruplar saf altgruplardır.

13.46. Saf bir altgrubun saf altgrubu saf altgruptur.

13.47. Bölünebilir altgruplar saf altgruplardır.

13.48. G/H burulmasızsa, H saf bir altgruptur.

13.49. Eğer $\operatorname{Tor} G$, G'nin burulmalı elemanlarından oluşan altgrupsa, $\operatorname{Tor} G$ saf bir altgruptur.

13.50. Saf altgruplar zincirinin bileşimi saf bir altgruptur.

13.51. Önsav 13.17'deki H altgrubu saf bir altgruptur. Dolayısıyla aşağıdaki teorem aslında o sonucun bir genellemesidir.

13.52. p bir asal, G bir p-grup ve $H \leq G$ olsun. Bu durumda H'nin G'de saf olması için her $k \geq 0$ için $p^kG \cap H = p^kH$ eşitliği gerek ve yeter koşuldur. Bunun kanıtı oldukça kolaydır: Eğer $n > 0$ ise, p'ye asal bir m ve bir $k \in \mathbb{N}$ için $n = p^km$ yazılabilir. Bu durumda $nG \cap H = p^kmG \cap H = p^kmG \cap mH = m(p^kG \cap H) = mp^kH = nH$ olur. (Üçüncü eşitlik m ile çarpmanın birebir bir fonksiyon olmasından kaynaklanmaktadır.)

Alıştırmalar

13.53. $H \leq G$ ve $P(H) = \{g \in G : \text{bir } n > 0 \text{ doğal sayısı için } ng \in H\}$ olsun. $P(H)$'nin bir saf altgrup olduğunu kanıtlayın.

13.54. $\operatorname{Tor} G$, G'nin burulmalı elemanlarından oluşan altgrup olsun. $P(0) = \operatorname{Tor} G$ eşitliğini kanıtlayın.

13.55. $\operatorname{Tor} G \leq P(H)$ olduğunu kanıtlayın.

13.56. $G/P(H)$'nin burulmasız bir grup olduğunu kanıtlayın.

13.57. $\operatorname{Tor}(G/H) = P(H)/H$ eşitliğini kanıtlayın.

13.58. $P(H)$'nin H'yi ve $\operatorname{Tor} G$'yi içeren en küçük saf altgrup olduğunu kanıtlayın.

13.59. G burulmasız bir grup ve $H \leq G$ olsun. H'nin saf olması için "G/H burulmasızdır" koşulunun yeter ve gerek olduğunu kanıtlayın.

13.60. $G = \mathbb{Z} \times \mathbb{Z}$, $H = (3,2)\mathbb{Z}$, $K = (1,2)\mathbb{Z}$ olsun. G/H ve G/K gruplarının burulmasız olduğunu kanıtlayın. Bir önceki alıştırmayı kullanarak H ve K'nın saf altgruplar olduklarını gösterin. $L = \langle G, H\rangle = (3,2)\mathbb{Z} + (1,2)\mathbb{Z}$ olsun. $(2,0) \in L$ ama $(1,0) \notin L$ olduğunu gösterin. Bunu kullanarak L'nin saf bir altgrup olmadığını gösterin.

13.61. $G = \mathbb{Z}/n\mathbb{Z}$, $H = \langle \overline{m} \rangle$ olsun. $d = \operatorname{obeb}(n,m)$ ve $e = n/d$ olsun. H'nin G'de saf olması için $\operatorname{obeb}(d,e) = 1$ eşitliğinin yeter ve gerek olduğunu kanıtlayın.

Aşağıdaki saf altgruplarla ilgili önemli teorem, Önsav 13.17'yi genelleştirmektedir.

Teorem 13.33. *G bir abel grubu ve H, G'nin bir saf altgrubu olsun. Eğer H'nin eksponenti sonluysa H'nin G'de bir tümleyeni vardır.*

Kanıt: G'yi çarpımsal yazacağız. H'nin eksponentlerini bölen farklı asallar $p_1, \ldots, p_k$ olsun. Önce teoremi $k = 1$ durumunda kanıtlamanın yeterli olduğunu, gerisinin k üzerine tümevarımla kolaylıkla kanıtlanacağını gösterelim. Teoremin $k = 1$ durumda kanıtlandığını varsayalım. Bir p asalı için,

$$H_p = \{h \in H : \text{ bir } n > 0 \text{ tamsayısı için } h^{p^n} = 1\}$$

olsun. O zaman $H_p \leq H$ ve

$$H = H_{p_1} \oplus \ldots \oplus H_{p_k}$$

olur. H'de ayrıştıkları için, H_{p_i}'lerin her biri H'de saftır. H de G'de saf olduğundan, H_{p_i}'leri her biri G'de saftır. $k = 1$ durumunda teoremi kanıtladığımızı varsaydığımız için, bir $K \leq G$ için

$$G = H_{p_1} \oplus K$$

olur. $i \geq 2$ için p_i ve p_1 iki farklı asal olduğundan

$$H_{p_i} \leq K$$

olur; ayrıca H_{p_i}, K'da saftır. Tümevarımla, bir $L \leq K$ için,

$$K = (H_{p_2} \oplus \ldots \oplus H_{p_k}) \oplus L$$

olur. Demek ki,

$$\begin{aligned} G &= H_{p_1} \oplus K = H_{p_1} \oplus ((H_{p_2} \oplus \ldots \oplus H_{p_k}) \oplus L) \\ &= (H_{p_1} \oplus H_{p_2} \oplus \ldots \oplus H_{p_k}) \oplus L = H \oplus L \end{aligned}$$

olur. Demek ki teoremi $k = 1$ için kanıtlamak yeterli.

Bundan böyle $p = p_1$, $H = H_p$ ve $\exp H = p^n$ olsun. Teorem 13.19'a göre $I_1, \ldots, I_n$ kümeleri için

$$H = \bigoplus_{k=1}^{n} \left(\bigoplus_{I_k} \mathbb{Z}/p^k\mathbb{Z} \right) \tag{1}$$

olur.

$$H_k = \bigoplus_{I_k} \mathbb{Z}/p^k\mathbb{Z}$$

olsun. H/H_n, G/H_n grubunun saf bir altgrubudur ve $\exp H/H_n \leq p^{n-1}$'dir. Demek ki tümevarımla H/H_n altgrubunun G/H_n altgrubunda bir tümleyeni vardır. Demek ki bir $H_n \leq K \leq G$ için,

$$G/H_n = H/H_n \oplus K/H_n$$

olur, yani

$$G = HK \text{ ve } H \cap K = H_n$$

olur.

Bu arada H_n'nin K'da saf olduğunu görelim: Eğer $k \in K$ ve $m \in \mathbb{N}$ için $k^m \in H_n \leq H$ oluyorsa, bir $h \in H$ için $k^m = h^m$ olur; ama (1)'den dolayı $h \in H$ elemanını H_n'de seçebiliriz.

Eğer

$$K = H_n \oplus L$$

eşitliğini sağlayan bir $L \leq K$ bulabilirsek, o zaman işimiz iş, çünkü o zaman

$$G = HK = HH_nL = HL$$

ve

$$H \cap L \leq H \cap (K \cap L) \leq (H \cap K) \cap L = H_n \cap L = 1$$

olur, yani $G = H \oplus L$ olur.

Bundan böyle $G = K$ ve $H = H_n \simeq \bigoplus_{I_n} \mathbb{Z}/p^n\mathbb{Z}$ olsun. Teoremi bu durumda kanıtlamanın yeterli olduğunu gördük. Kanıtı ufak bir değişiklikle Önsav 13.17'nin kanıtı gibi olacak. Akıcılığı bozmamak için o önsavın kanıtını çok ufak değişikliklerle tekrarlıyoruz.

Önce $G^{p^n} = \{g^{p^n} : g \in G\}$ altgrubuyla H'nin kesişmediğini görelim: Eğer $g^{p^n} \in H$ ise, bir $h \in H$ için $g^{p^n} = h^{p^n}$ olur. Ama $\exp H = p^n$ olduğundan, buradan $g^{p^n} = h^{p^n} = 1$ çıkar. Bu şöyle de daha kolay biçimde anlaşılır: $G^{p^n} \cap H = H^{p^n} = 1$. Demek ki $G^{p^n} \cap H = 1$.

$$\mathcal{Z} = \{K \leq G : K \cap H = 1 \text{ ve } G^{p^n} \leq K\}$$

olsun. $G^{p^n} \in \mathcal{Z}$ olduğundan $\mathcal{Z} \neq \emptyset$ olur. $\mathcal{Z}$'yi altgrup (ya da altküme) olma ilişkisiyle sıralayalım, altgruplar üstgruplardan küçük olsun. Eğer $(K_i)_i$, $\mathcal{Z}$'nin bir zinciriyse, $\bigcup_i K_i \in \mathcal{Z}$ olur. Dolayısıyla, Zorn Önsavı'na göre $\mathcal{Z}$'nin maksimal bir elemanı vardır. Bu altgruba K diyelim. Demek ki

$$\langle H, K\rangle = HK = H \oplus K \leq G.$$

$HK = G$ eşitliğini kanıtlayacağız. Diyelim eşitlik yok ve $HK < G$. Amacımız $\langle K, g\rangle \cap H = 1$ eşitliğinin doğru olduğu bir $g \in G \setminus K$ elemanının varlığını kanıtlamak; böylece $K < \langle K, g\rangle$ olacak ve K'nın maksimalliğiyle çelişeceğiz.

Önce rastgele bir $g \in G \setminus HK$ alalım. Bu elemanı istediğimizi sağlaması için yavaş yavaş değiştireceğiz. İlk olarak

$$g,\ g^p,\ g^{p^2},\ \ldots,\ g^{p^n} = 1$$

dizisine bakalım. İlk terim, g yani, HK'da değil. Ama son terim, g^{p^n} elemanı yani, HK'da çünkü $g^{p^n} \in G^{p^n} \leq K \leq HK$. Bu dizinin elemanlarını soldan sağa doğru tararken, bir $i = 0, 1, \ldots, n-1$ için

$$g^{p^i} \notin HK \text{ ama } g^{p^{i+1}} \in HK$$

olmalı. g yerine bu g^{p^i} elemanını alarak,

$$g \notin HK \text{ ama } g^p \in HK$$

varsayımını yapabiliriz; öyle yapalım. Şimdi, $h \in H$ ve $k \in K$ için

$$g^p = hk$$

olur. H'nin eksponenti p^n olduğundan

$$g^{p^n} = (g^p)^{p^{n-1}} = (hk)^{p^{n-1}} = h^{p^{n-1}} k^{p^{n-1}}$$

olur. Ama $g^{p^n} \in G^{p^n} \leq K$ olduğundan, buradan $h^{p^{n-1}} \in H \cap K = 1$ ve

$$h^{p^{n-1}} = 1$$

elde ederiz.

Şimdi H grubunda hangi elemanların p^{n-1}'inci kuvvetinin 1'e eşit olduğunu görelim. Teoremin hipotezine göre $H \simeq (\mathbb{Z}/p^n\mathbb{Z})^{(I)}$. Ama

$$\{x \in \mathbb{Z}/p^n\mathbb{Z} : p^{n-1}x = 0\} = p\mathbb{Z}/p^n\mathbb{Z}$$

eşitliğini Örnek 9.53'te kanıtlamıştık; demek ki aynı şey $(\mathbb{Z}/p^n\mathbb{Z})^{(I)}$ grubunda da doğru:

$$\{x \in (\mathbb{Z}/p^n\mathbb{Z})^{(I)} : p^{n-1}x = 0\} = (p\mathbb{Z}/p^n\mathbb{Z})^{(I)} = p \cdot (\mathbb{Z}/p^n\mathbb{Z})^{(I)}.$$

Sonuç olarak benzer önerme (çarpımsal bir grup olan) H için de geçerlidir ve $h^{p^{n-1}} = 1$ olduğundan, bir $h_1 \in H$ için $h = h_1^p$ eşitliğinin doğru olduğunu görürüz. Böylece $g^p = hk = h_1^p k$ ve $(h_1^{-1}g)^p = k \in K$ elde ederiz. $h_1^{-1}g \in G \setminus HK$ olduğundan (aksi halde $g = h_1(h_1^{-1}g) \in H(HK) = HK$ olurdu), g yerine $h_1^{-1}g$ elemanını alıp,

$$g \in G \setminus HK \text{ ve } g^p \in K$$

varsayımını yapabiliriz.

Bu aşamada $\langle K, g\rangle$ altgrubuna bakalım. Bu altgrubun elemanları bir $k \in K$ ve $m \in \mathbb{Z}$ için kg^m biçimindedir (daha önceki k'yı artık unutun). K'nın seçiminden dolayı, $\langle K, g\rangle \cap H \neq 1$ olmalı. Kesişimden 1'e eşit olmayan bir eleman seçelim:

$$1 \neq kg^m \in H$$

olsun. Demek ki $g^m \in HK$. Eğer p asalı n'yi bölmezse, g^p de HK'da olduğundan,

$$g = g^1 = g^{\text{obeb}(n,p)} \in HK$$

olur (bkz. Alıştırma 5.31), ki bu da g'nin seçimiyle çelişir. Demek ki $p|m$, diyelim $ps = m$. Bu durumda, $g^p \in K$ olduğundan,

$$kg^m = kg^{ps} = k(g^p)^s \in K$$

olur. Ama aynı zamanda $kg^m \in H$. Demek ki $kg^m \in H \cap K = 1$, çelişki. □

14. Grup Etkisi

Bu bölümde grup teorisinin uygulamaya en elverişli, dolayısıyla en önemli konusuyla tanışacağız. Grupları doğada bulundukları haliyle göreceğiz.

Gruplar doğada tek başlarına görünmezler, mutlaka grupların yanında etkidikleri bir küme vardır. Ötelemeler ve döndürüler düzleme etkir, Sym n grubu $\{1, 2, \ldots, n\}$ kümesine etkir, Aut G grubu G grubuna etkir vs. Biraz daha somut bir örnek: $\{1, x\} \simeq \mathbb{Z}/2\mathbb{Z}$ grubu masaya konmuş bir bozuk paraya etkir: 1 elemanı parada herhangi bir değişiklik yapmazken x elemanı parayı ters yüz eder, yazıysa tura, turaysa yazı yapar; görüldüğü üzere x'i iki defa paraya uygulamak hiçbir şey yapmamak, yani 1 elemanıyla etkimek demektir. Grubu olası tüm rüzgar esintileri, kümeyi de rüzgardan etkilenecek toz zerreleri olarak görmek çok yanlış olmayan benzetme olabilir.

Grup etkisinin daha derin ve ilginç bir incelemesini daha sonraki ciltlerde, biraz lineer cebir gördükten sonra yapacağız.

14.1 Tanım ve Örnekler

G bir grup, X de bir küme olsun. X'in elemanlarına "nokta" demeyi tercih edeceğiz. $G \times X$'ten X'e giden bir α fonksiyonu ele alalım. Bu fonksiyonun (g, x) ikilisini götürdüğü noktayı $g \cdot x$ olarak gösterelim, yani $\alpha(g, x)$ yerine $g \cdot x$ yazalım; çünkü α'yı bir fonksiyondan ziyade bir tür işlem olarak algılamak istiyoruz. G'nin elemanlarıyla X'in noktalarını çarpıyoruz ve sonuç X'in bir noktası çıkıyor: $g \in G$ elemanı $x \in X$ noktasına etkiyor ve sonuç $g \cdot x$ çıkıyor. Demek ki her $g \in G$ ve $x \in X$ için bir biçimde $g \cdot x \in X$ noktası verilmiş. Bu "çarpma" şu özellikleri sağlasın:

A1. Her $x \in X$ için $1 \cdot x = x$.

A2. Her g, $h \in G$ ve $x \in X$ için $g \cdot (h \cdot x) = (gh) \cdot x$.

Bir başka deyişle çarpma işlemi grubun işlemiyle uyumlu olsun. Bu durumda (G, X, α) üçlüsüne ***grup etkisi*** denir. Bazen de "G grubu X kümesine α vasıtasıyla etkiyor" denir. Bazen de X'e ***G-küme*** adı verilir.

Çoğu zaman α yazılmaz (çünkü ya önemli değildir ya da ne olduğu çok barizdir) ve grup etkisi (G, X) ikilisi olarak gösterilir. Ayrıca çoğu zaman $g \cdot x$

yerine gx yazılır, ancak $G \times X \longrightarrow X$ çarpmasıyla G grubundaki $G \times G \longrightarrow G$ çarpmasının karışma ihtimali varsa $g \cdot x$ yazılımına geri dönülmelidir.

Birazdan birçok örnek vereceğiz. Ama önce aynı kavramı bir başka biçimde tanımlayalım. Her iki tanım da önemlidir, birini bilip diğerini bilmemek sonuçları olabilecek bir eksikliktir.

Bir (G, X, α) grup etkisinde $gx = gy$ ise, o zaman her iki tarafı da g^{-1} ile çarparak $x = y$ elde ederiz. Bunu daha ayrıntılı gösterelim:

$$x = 1x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}(gy) = (g^{-1}g)y = 1y = y.$$

Dolayısıyla X'in elemanlarını (soldan tabii ki) sabit bir $g \in G$ elemanıyla çarpmak X'ten X'e giden birebir bir fonksiyondur. Bu fonksiyon ayrıca örtendir de, çünkü her $y \in X$ için

$$g(g^{-1}y) = y$$

olur. Demek ki $x \mapsto gx$ kuralıyla tanımlanmış fonksiyon X'in bir eşleşmesidir, yani $\operatorname{Sym} X$'in bir elemanıdır. Bu fonksiyonu φ_g olarak gösterelim. Demek ki her $g \in G$ için,

$$\varphi_g : X \longrightarrow X$$

fonksiyonu

$$\varphi_g(x) = gx$$

olarak tanımlandı; ve bu fonksiyon $\operatorname{Sym} X$'in bir elemanı. Ayrıca

$$\varphi_g \circ \varphi_h = \varphi_{gh}$$

olur, çünkü her $x \in X$ için,

$$(\varphi_g \circ \varphi_h)(x) = \varphi_g(\varphi_h(x)) = \varphi_g(hx) = g(hx) = (gh)x = \varphi_{gh}(x)$$

olur. Bundan da

$$\varphi(g) = \varphi_g$$

olarak tanımlanmış

$$\varphi : G \longrightarrow \operatorname{Sym} X$$

fonksiyonunun bir grup homomorfisi olduğu çıkar. Böylece her (G, X, α) grup etkisinin bir $\varphi : G \longrightarrow \operatorname{Sym} X$ grup homomorfisi verdiğini gördük.

Şimdi tam tersine bir

$$\varphi : G \longrightarrow \operatorname{Sym} X$$

grup homomorfisi verilmiş olsun. Eğer $g \in G$ ise, tamamen estetik nedenlerden dolayı $\varphi(g)$ yerine φ_g yazalım. Böylece $g \in G$ ve $x \in X$ için $(\varphi(g))(x)$ yerine $\varphi_g(x)$ yazarak yüklü bir yazılımdan kurtulmuş oluruz.

$$g \cdot x = \varphi_g(x)$$

tanımını yapalım. Böylece $G \times X$'ten X'e giden bir fonksiyon tanımlamış oluruz. Yukarıdaki A1 ve A2 önermelerin sağlandığını kanıtlayalım. φ fonksiyonu G'den $\operatorname{Sym} X$'e giden bir homomorfi olduğundan, φ, G'nin 1 elemanını $\operatorname{Sym} X$'in birim elemanı olan Id_X fonksiyonuna götürür; demek ki

$$1 \cdot x = \varphi_1(x) = \mathrm{Id}_X(x) = x$$

olur. Böylece A1'in doğru olduğunu gördük. Şimdi A2'ye bakalım:

$$g \cdot (h \cdot x) = \varphi_g(\varphi_h(x)) = (\varphi_g \circ \varphi_h)(x) = \varphi_{gh}(x) = (gh) \cdot x.$$

Böylece bir grup etkisi elde ettik.

Eğer yukarıdaki iki prosedürü ardarda uygularsak başladığımız yere döneriz. Bir başka deyişle, bir (G, X, α) grup etkisiyle bir $\varphi : G \longrightarrow \operatorname{Sym} X$ homomorfisi arasında bir fark yoktur.

Grup etkisi grup kavramının somutlaşmış halidir; soyut bir grubu fiziksel olarak gerçekleştirmek olarak algılanabilir.

Notlar ve Örnekler

14.1. G herhangi bir grup ve X herhangi bir küme olsun. $g \in G$ ve $x \in X$ için $g \cdot x = x$ tanımını yapalım; yani ikinci tanıma göre, her $g \in G$ için $\varphi_g = \mathrm{Id}_X$ olsun, yani φ fonksiyonu sabit Id_X fonksiyonu olsun. Bu bir grup etkisidir. Tahm,n edi,leceği üzere en ilginç grup etkisi değildir, ne de olsa G'nin elemanları X'in elemanlarını yerlerinden oynatmıyorlar. Bu etkiye ***trişkadan etki*** adını verebiliriz[1].

14.2. $\operatorname{Sym} X$'in her altgrubu X üzerine doğal olarak etkir.

14.3. $\mathbb{R}^2$ düzleminin $(0,0)$ merkezli döndürüleri kümesi (ki bir gruptur) düzleme etkir.

14.4. $\mathbb{R}^2$ düzleminin ötelemeleri kümesi (ki bir gruptur) düzleme etkir.

14.5. Eğer G, X grubu üzerine etkiyorsa ve $H \leq G$ ise, H grubu da X üzerine etkir. Daha matematiksel bir dille: Eğer (G, X, α) bir grup etkisiyse ve $H \leq G$ ise, $(H, X, \alpha_{|H})$ üçlüsü de bir grup etkisidir.

14.6. Son iki örneğin özel bir durumu olarak: Eğer G bir grupsa, $\operatorname{Aut} G$ grubu, hatta $\operatorname{Aut} G$ grubunun herhangi bir altgrubu G kümesi üzerine doğal olarak etkir.

14.7. Eğer G grubu X kümesi üzerine etkiyorsa ve $Y \subseteq X$ altkümesi $GY \subseteq Y$ içindeliğini sağlıyorsa (ki bu durumda eşitlik olmalıdır), o zaman G grubu Y kümesi üzerine etkir. Herhangi bir $A \subseteq X$ altkümesi için

$$Y = GA = \{ga : a \in A\}$$

olursa, elbette $GY \subseteq Y$ olur ve G grubu Y kümesi üzerine etkir. Bu arada

$$GA = \bigcup_{a \in A} Ga$$

eşitliğini görelim. Ga kümesine a'nın ***G-yörüngesi*** adı verilir. Çok önemli olan bu kavrama tekrar değineceğiz ve sık sık kullanacağız. G elbette Ga yörüngesini etkir.

[1] İngilizcesi *trivial action*.

14.8. G herhangi bir grup olsun. $X = G$ olsun. O zaman $g \in G$ ve $x \in X$ için

$$g \cdot x = gx$$

tanımı bize G'nin X (yani kendisi!) üzerine etkidiğini gösterir. G'nin bu etkisine ***standart etki*** diyelim[2].

14.9. G herhangi bir grup olsun. $X = G$ olsun. O zaman $g \in G$ ve $x \in X$ için

$$g \cdot x = xg^{-1}$$

tanımı bize G'nin X (yani kendisi!) üzerine etkidiğini gösterir. G'nin bu etkisine ***sağdan standart etki*** diyelim.

14.10. G herhangi bir grup olsun. $X = G$ olsun. O zaman $(g, h) \in G \times G$ ve $x \in X$ için

$$(g, h) \cdot x = gxh^{-1}$$

tanımı bize $G \times G$ grubunun G üzerine etkidiğini gösterir.

14.11. G herhangi bir grup olsun. $X = G$ olsun. O zaman $g \in G$ ve $x \in X$ için

$$g \cdot x = gxg^{-1}$$

tanımı G grubunun kendisi üzerine bir grup etkisini verir.

14.12. G herhangi bir grup ve $H \lhd G$ olsun. $X = H$ alalım. O zaman $g \in G$ ve $x \in X$ için

$$g \cdot x = gxg^{-1}$$

tanımı G grubunun H üzerine bir grup etkisini verir.

14.13. G herhangi bir grup ve H, $K \leq G$ olsun. $H \leq N_G(K)$ varsayımını yapalım. O zaman $k \in K$ ve $h \in H$ için

$$h \cdot k = hkh^{-1}$$

tanımı H grubunun K üzerine bir grup etkisini verir.

14.14. G bir grup ve X, G'nin altgruplarından oluşan küme olsun. $g \cdot H = H^g$ tanımıyla G grubu X kümesini etkir.

14.15. Yukarıdaki etkide X kümesini daha küçük alabiliriz. $K \leq G$ olsun. $Y = \{K^g : g \in G\}$ olsun. Bir önceki alıştırmadaki tanımla G grubu Y üzerine etkir.

14.16. Yukarıdaki etkide G grubunu bir altgrup olarak da alabiliriz. K, $H \leq G$ olsun. $Y = \{K^g : g \in G\}$ olsun. H grubu Y üzerine etkir.

14.17. Bölüm 6'daki örneklerdeki her geometrik nesneye nesnenin simetrileri etkiyordu. Örneğin D_8 grubu kareye etkir, $\mathrm{Sym}\,4$ grubu üçgen tabanlı piramide etkir.

14.18. $G = \mathbb{R}^n$ olsun. $X = \mathbb{R}^n$ olsun. $g \in G$ ve $x \in G$ için $g \cdot x = x + g$ olarak tanımlansın. Grup toplamsal yazıldığından, A1 ve A2 koşullarını toplama diline çevirmeliyiz: $0 \cdot x = x + 0 = 0$ ve g, $h \in G$ için

$$(g \cdot (h \cdot x)) = g \cdot (x + h) = (x + h) + g = x + (h + g) = (h + g) \cdot x$$

olur. Bu örneğin Örnek 14.8'deki örneğin özel bir durumu olduğuna dikkatinizi çekeriz.

14.19. Eğer (G, X) bir grup etkisiyse, G'yi doğal olarak $\wp(X)$ üzerine (yani X'in altkümelerinden oluşan küme üzerine) etkiyebiliriz; $(G, \wp(X))$ de bir grup etkisidir. Bu örneğin varyasyonları yapılabilir, örneğin $\wp(X)$'i alacağımıza X'in sonlu altkümelerinden oluşan kümeyi alabiliriz.

Örnekleri çoğaltacağız. Ama önce önemli birkaç temel kavram tanımlayalım ve bu kavramlar üzerine birkaç temel teorem kanıtlayalım.

[2]İngilizcesi *regular action* ya da *standard regular action*.

14.2 Kavramlar ve Temel Teoremler

Bu altbölümde grup etkileriyle ilgili bazı önemli kavramlar tanımlayacağız. Bu altbölüm boyunca bir (G, X) grup etkisi sabitlenmiş olsun.

Çekirdek. Örnek 14.1'de her $g \in G$ ve her $x \in X$ için $g \cdot x = x$ örneğini vermiş ve bu etkiyi "trişkadan etki" olarak adlandırmıştık. G'nin belki her elemanı değil ama bazı elemanları X üzerine birim fonksiyon olarak etkiyebilirler, yani bazı $g \in G$ elemanları her $x \in X$ için $gx = x$ eşiliğini sağlayabilirler.

$$\operatorname{Ker}(G, X) = \{g \in G : \text{her } x \in X \text{ için } gx = gx\}$$

tanımını yapalım. Bu bir altgruptur ve adına etkinin ***çekirdeği*** adı verilir[3]. Eğer etkiyi $\varphi : G \longrightarrow \operatorname{Sym} X$ homomorfisi olarak gösterirsek,

$$\operatorname{Ker}(G, X) = \operatorname{Ker} \varphi$$

olur. Dolayısıyla $\operatorname{Ker}(G, X) \lhd G$ olur. Eğer etkinin ne olduğu konunun gelişinden belliyse, $\operatorname{Ker}(G, X)$ yerine sadece Ker yazmakla yetineceğiz.

Bir etkinin çekirdeği 1 ise, etkiye ***sadık etki*** adı verilir[4]. Etkinin sadık olması demek $\varphi : G \longrightarrow \operatorname{Sym} X$ homomorfisinin birebir olması demektir; ya da daha somut olarak, her $1 \neq g \in G$ elemanının X'in en az bir noktasını yerinden oynatıyor demektir.

Eğer bir etki sadık değilse, etkim sadık değil diye üzülmeyin, grupta küçük bir değişiklikle etkiyi sadık hale getirebiliriz. Nitekim,

$$\overline{\varphi}_{\overline{g}}(x) = gx$$

formülüyle tanımlanmış

$$\overline{\varphi} : G/\operatorname{Ker} \varphi \longrightarrow \operatorname{Sym} X$$

homomorfisi (çekirdeğe bölündüğünden) birebirdir, dolayısıyla sadık bir etki tanımlar. Bu etki daha somut olarak şu formülle tanımlanır: $\overline{g}x = gx$.

Notlar ve Örnekler

14.20. Eğer (G, X) bir grup etkisiyse ve $|X| = n < \infty$ ise, $G/\operatorname{Ker}(G, X)$ grubunun eleman sayısı $n!$ sayısını bölmek zorundadır. Dolayısıyla (G, X) sadıksa ve X sonluysa, G de sonlu olmak zorundadır.

14.21. G bir grup ve $X \subseteq G$ olsun. $H = \{g \in G : X^g = X\}$ olsun. $H \leq G$ olur. (H, X) bir grup etkisidir. $\operatorname{Ker}(H, X) = C_G(X)$ olur. Demek ki $C_G(X) \lhd H$ ve eğer $|X| = n < \infty$ ise $[H : C_G(X)]$ sayısı $n!$ sayısını böler.

14.22. Yukarıdaki alıştırmadan şu çıkar: Eğer $A \lhd G$ sonlu ve normal bir altgrupsa, $C_G(A)$, G'nin sonlu endisli normal bir altgrubudur, endis $|A|!$ sayısını böler.

[3] İngilizcesi *kernel*.

[4] İngilizcesi *faithful*.

14.23. G bir grup, $H \leq G$ olsun. $X = \{xH : x \in G\}$, sol ötelemeler kümesi olsun. $g \in G$ ve $xH \in X$ için $g \cdot xH = gxH$ tanımını yapalım. (G, X) ikilisinin bir grup etkisi olduğunu kontrol etmek çok zor değil; okura bırakıyoruz. Bu etki çok önemlidir, sadık grup etkileri daha sonraki ciltlerde açıklayacağımız bir anlamda bu etkiye denktirler. Çekirdeği bulalım:

$$\begin{aligned}
\operatorname{Ker}(G,X) &= \{g \in G : \text{ her } x \in G \text{ için } g \cdot xH = xH\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } gxH = xH\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } x^{-1}gxH = H\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } x^{-1}gx \in H\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } g \in xHx^{-1}\} \\
&= \textstyle\bigcap_{x\in G} xHx^{-1}.
\end{aligned}$$

Örnek 9.12 ve 10.125'de $\bigcap_{x\in G} xHx^{-1}$ grubuna H'nin G'deki göbeği adını vermiş ve H'nin göbeğini $\operatorname{Core}_G H$ olarak göstermişik: $\operatorname{Core}_G H = \bigcap_{x\in G} xHx^{-1}$. Bu grup H'nin içindeki en büyük G-normal altgruptur.

14.24. G bir grup, $H \leq G$ olsun. $X = \{H^x : x \in G\}$, H'nin eşleniklerinden oluşan kümesi olsun. $g \in G$ ve $H^x \in X$ için $g \cdot H^x = H^{xg^{-1}}$ tanımını yapalım. (G, X) ikilisinin bir grup etkisi olduğunu kontrol etmek çok zor değil; okura bırakıyoruz. Çekirdeği bulalım:

$$\begin{aligned}
\operatorname{Ker}(G,X) &= \{g \in G : \text{ her } x \in G \text{ için } g \cdot H^x = H^x\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } H^{xg^{-1}} = H^x\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } H = H^{xgx^{-1}}\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } xgx^{-1} \in N_G(H)\} \\
&= \{g \in G : \text{ her } x \in G \text{ için } g \in x^{-1}N_G(H)x\} \\
&= \textstyle\bigcap_{x\in G} x^{-1}N_G(H)x = \operatorname{Core} N_G(H).
\end{aligned}$$

Bu arada $x^{-1}N_G(H)x = N_G(x^{-1}Hx)$ eşitliğine dikkatinizi çekeriz.

Sabitleyici. Eğer $x \in X$ ise

$$G_x = \{c \in G : cx = x\}$$

tanımını yapalım. Bu bir altgruptur ve adına x'in ***sabitleyicisi*** adı verilir[5]. Elbette

$$\operatorname{Ker}(G,X) = \bigcap_{x\in X} G_x$$

olur. $g \in G$ için G_{gx} ile G_x arasında yakın bir ilişki vardır:

$$\begin{aligned}
G_{gx} &= \{c \in G : c(gx) = gx\} = \{c \in G : g^{-1}cgx = x\} \\
&= \{c \in G : g^{-1}cg \in G_x\} = \{c \in G : c \in gG_xg^{-1}\} \\
&= gG_xg^{-1} = G_x^{g^{-1}},
\end{aligned}$$

yani

$$G_{gx} = G_x^{g^{-1}} \tag{1}$$

[5]İngilizcesi *stabilizer*.

olur.

Eğer $Y \subseteq X$ ise

$$G_Y = \bigcap_{y \in Y} G_y = \{g \in G : \text{her } y \in Y \text{ için } gy = y\}$$

tanımını yapalım. Bu da bir altgruptur elbette. Adına Y'nin ***noktasal sabitleyicisi*** adı verilir[6]. Eğer $GY \subseteq Y$ ise, $G_Y \lhd G$ olur; bu dediğimiz $G_{gx} = G_x^{g^{-1}}$ eşitliğinden kolaylıkla çıkar ve okura bırakılmıştır.

Elbette $\mathrm{Ker}(G, X) = G_X$ olur.

Buna benzer bir başka tanım daha verilebilir. Y'i küme olarak sabileyen elemanları ele alalım:

$$\{g \in G : gY = Y\}.$$

Burada, Y'nin her elemanını sabitleyen $g \in G$ elemanları değil, Y'yi küme olarak sabitleyen $g \in G$ elemanları ele alınıyor. Bu grubu $G_{\{Y\}}$ olarak yazabiliriz. $G_{\{Y\}}$ grubu Y kümesi üzerine etkir ve bu etkinin çekirdeği G_Y altgrubudur. Elbette eğer $|Y| = 1$ ise $G_Y = G_{\{Y\}}$ olur.

Alıştırmalar

14.25. (G, X) bir grup etkisi olsun. Eğer $\overline{G} = G/\mathrm{Ker}$ ve $x \in X$ ise $\overline{G}_x = \overline{G_x}$ eşitliğini kanıtlayın.

Bundan sonraki alıştırmalarda (G, X) bir grup etkisi ve $Y \subseteq X$.

14.26. Eğer $GY \subseteq Y$ ise, $GY = Y$ olduğunu kanıtlayın. Ama $gY \subseteq Y$ ise eşitlik olmak zorunda değil, örneğin eğer $i > 0$ için $g^i y \neq y$ ise ve $Y = \{g^i y : i \in \mathbb{N}\}$ ise aynen bu olur. Öte yandan eğer g'nin derecesi sonluysa, ya da her $y \in Y$ için $\langle g \rangle y$ sonluysa, $gY \subseteq Y$ içindeliği eşitliği gerektirir.

14.27. $G_Y \lhd G_{\{Y\}}$ olduğunu kanıtlayın.

14.28. $|Y| = n$ olsun. $[G_{\{Y\}} : G_Y]$ sayısının $n!$ sayısını böldüğünü kanıtlayın.

14.29. $|Y| = n$ ve $y \in Y$ olsun. $[G_{\{Y\}} : G_y \cap G_{\{Y\}}] \leq n$ olduğunu kanıtlayın.

14.30. $|Y| = n$ ve $y \in Y$ olsun. Eğer $G_{\{Y\}} y = Y$ ise $[G_{\{Y\}} : G_y \cap G_{\{Y\}}] = n$ olduğunu kanıtlayın.

14.31. Eğer $GY \subseteq Y$ ise, $G_Y \lhd G$ olduğunu kanıtlayın.

Yörünge. $x \in X$ ise,

$$Gx = \{gx : g \in G\}$$

kümesine x'in ***yörüngesi***[7], ya da daha dikkatli olmak istiyorsak x'in ***G-yörüngesi*** adı verilir. Elbette $x \in Gx$ olur. Eğer $Gx = X$ ise, (G, X) grup etkisine ***geçişli grup etkisi*** adı verilir[8]. Her $x \in X$ için, (G, Gx) geçişli bir grup etkisidir. Geçişli grup etkilerinde her $x \in X$ için $\mathrm{Ker} = G_X = \bigcap_{y \in X} G_y = \bigcap_{y \in Gx} G_y = \bigcap_{g \in G} G_{gx} = \bigcap_{g \in G} G_x^{g^{-1}} = \bigcap_{g \in G} G_x^g = \mathrm{Core}_G\, G_x$ olur.

[6] İngilizcesi *pointwise stabilizer*.

[7] İngilizcesi *orbit*.

[8] İngilizcesi *transitive group action*.

Notlar ve Örnekler

14.32. $\operatorname{Sym} X$ grubu X kümesine geçişli etkir.

14.33. $\mathbb{R}^2$ düzleminin $(0,0)$ merkezli döndürülerinden oluşan grup düzleme etkir ama bu etki geçişli değildir. Her yörünge $(0,0)$ merkezli çemberdir.

14.34. $\mathbb{R}^2$ düzleminin ötelemelerinden oluşan grup düzleme geçişli etkir. Bu (ve bir önceki örnek), daha genel olarak $\mathbb{R}^n$ için de geçerlidir.

14.35. Bir grubun sağ ve sol standart etkileri geçişli etkilerdir.

14.36. Örnek 14.23 ve 14.24'teki etkiler geçişli etkilerdir.

14.37. 1 elemanı yüzünden, eğer $G \neq 1$ ise $\operatorname{Aut} G$ grubu G üzerine geçişli etkiyemez.

14.38. $1 \neq G$ sonlu bir grupsa ve $\operatorname{Aut} G$ grubu $G^\sharp = G \setminus \{1\}$ üzerine geçişli etkiyorsa, o zaman grubun 1 dışında tüm elemanlarının derecesi aynı olmalıdır. Cauchy teoreminden dolayı bu ortak derece ancak bir p asalı olabilir. Demek ki grup bir p-gruptur. Sonlu p-gruplarının merkezi olduğundan (yani $Z(G) \neq 1$ olduğundan), geçişli etki yüzünden, grup abel grubu olmak zorundadır. Demek ki bir $n > 0$ için $G = \oplus_n \mathbb{Z}/p\mathbb{Z}$. Bu grupların otomorfi gruplarının $G^\sharp$ üzerine geçişli etkidiği biraz lineer cebirle kolaylıkla kanıtlanabilir (ama bu kitapta okurun lineer cebir bildiğini varsaymıyoruz).

İlk olarak yörüngelerin eşit ya da birbirinden ayrık olduklarını kanıtlayalım.

Önsav 14.1. *İki yörünge ya eşittir ya da ayrık.*

Kanıt: $x, y \in X$ olsun. $Gx \cap Gy \neq \emptyset$ varsayımını yazpalım. Kesişimden bir eleman alalım, diyelim $g_0 x = g_1 y$. O zaman her $g \in G$ için,

$$gx = gg_0^{-1} g_0 x = gg_0^{-1} g_1 y \in Gy$$

olur. Demek ki $Gx \subseteq Gy$. Simetriden dolayı $Gy \subseteq Gx$ içindeliği de doğrudur. □

Demek ki yörüngeler X kümesini ayrık parçalara böler. Her yörüngeden bir temsilci seçersek ve bu temsilciler kümesine T dersek,

$$X = \bigsqcup_{t \in T} Gt$$

olur.

Bazen de Gx tek bir elemandan oluşur, o eleman da x'ten başkası olamaz tabii. Bu durum her $g \in G$ için $gx = x$ olduğunda, yani $G_x = G$ olduğunda vuku bulur. G_x ne kadar büyükse, G'nin o kadar çok elemanı x'i sabitler (yerinden kımıldatmaz) ve dolayısıyla x'in yörüngesi Gx o kadar küçük olur. Bir başka deyişle G_x ile Gx birbirine ters orantılıdır:

Önsav 14.2. *$G/G_x = \{gG_x : g \in G\}$ sol ötelemeler kümesi olsun. O zaman*

$$gG_x \mapsto gx$$

kuralı G/G_x ile Gx yörüngesi arasında bir eşleme verir. Dolayısıyla

$$|G/G_x| = |Gx|$$

yani

$$|G| = |G_x||Gx|$$

olur ve eğer G sonluysa, Gx yörüngesinin eleman sayısı $|G|$ sayısını böler.

Kanıt: Aşağıdaki önermelerin birbirine eşdeğer oldukları bariz:

$$\begin{aligned} &gx = hx, \\ &h^{-1}gx = x, \\ &h^{-1}g \in G_x, \\ &g \in hG_x, \\ &gG_x = hG_x. \end{aligned}$$

Böylece $gG_x \mapsto gx$ kuralının iyi tanımlı olduğunu ve G/G_x'ten Gx'e giden birebir fonksiyon tanımladığını kanıtlamış olduk. Fonksiyonun örten olduğu bariz. Diğer önermeler de bu kanıtladığımızın doğrudan bir sonucu. □

Notlar ve Örnekler

14.39. G bir grup olsun. X'i de G'ye eşit alalım. $g \in G$ ve $x \in G$ için daha önce Örnek 14.8'de $g \cdot x = gx$ tanımını (standart etki) ve Örnek 14.9'da $g \cdot x = xg^{-1}$ tanımını yapmıştık. Burada $g \cdot x = gxg^{-1} = x^{g^{-1}}$ tanımını yapacağız. Tanımlanan bu grup etkisi için,

$$G_x = C_G(x),\ Gx = x^G,\ \text{Ker} = Z(G)$$

olur. Önsav 14.1'e göre yörüngeler, yani x^G eşleniklik sınıfları ya eşittir ya da ayrık. Eğer $G = \operatorname{Sym} n$ ise, eşleniklik sınıfları aynı tipte olan elemanlar kümesidir (bkz. sayfa 51). Önsav 14.2'ye göre $G/C_G(x)$ (sol ötelemeler kümesi) ile x^G arasında $gC_G(x) \mapsto x^{g^{-1}}$ tarafından verilen bir eşleme vardır. Bu eşlemeyi sağ ötelemeler kümesinden de başlatabiliriz: $C_G(x)g \mapsto x^g$. Bunu zaten Alıştırma 8.33'ten biliyoruz. Demek ki

$$|G| = |x^G||C_G(x)|$$

olur.

14.40. Yukarıdaki örneği alalım. 1'in yörüngesi sadece kendisinden oluşur çünkü $g\cdot 1 = g1g^{-1} = 1$ olur. Bu grup etkisinde ne zaman tam iki yörünge olabileceğini bulmaya çalışalım. Diyelim tam iki yörünge var. O zaman herhangi bir $x \in G^\sharp = G \setminus \{1\}$ için,

$$G = \{1\} \sqcup x^G$$

olur. Demek ki grubun 1 dışındaki elemanlarının dereceleri eşittir. Eğer grupta derecesi sonlu olan 1'den farklı bir eleman varsa, o zaman grupta derecesi bir p asalı olan bir eleman vardır; dolayısıyla grubun tüm elemanlarının derecesi p'dir. Eğer $p = 2$ ise grup abel olmak zorunda ve buradan da $G = \{1\} \sqcup x^G = \{1, x\} \simeq \mathbb{Z}/2\mathbb{Z}$ çıkar. Şimdi p asalının 2 olmadığını varsayalım. O zaman grubun her elemanı ve her altgrubu 2-bölünürdür. $x \in G^\sharp$ olsun. $gxg^{-1} = x^{-1}$ eşitliğini sağlayan bir g alalım. $g \in C_G(x)$ olsaydı, x'in derecesi 2 olurdu, bir çelişki. Demek ki $g \notin C_G(x)$.

$$g^2xg^{-2} = g(gxg^{-1})g^{-1} = gx{-}1g^{-1} = (gxg^{-1})^{-1} = (x^{-1})^{-1} = x$$

eşitliklerinden dolayı $g^2 \in C_G(x)$ ve dolayısıyla $g^2 \in C_G(x, g)$ olur. Ama $C_G(x, g)$ grubu 2-bölünür. Dolayısıyla bir $c \in C_G(x, g)$ için $g^2 = c^2$ olur. Bundan da $(gc^{-1})^2 = 1$ çıkar.

$g \neq c$ olduğundan (aksi halde $g \in C_G(c, g)$), derecesi 2 olan bir eleman buluruz; bir çelişki.

Sadece iki eşleniklik sınıfı olan burulmasız gruplar vardır. Ama bu gruplar bölünür olmak zorundadır. Öte yandan bu gruplarda $C_G(x, g)$ gibi altgrupların hepsi bölünür olamazlar; olsaydı yukarıdaki gibi akıl yürütüp grubun sadece 2 elemanı olduğunu kanıtlayabilirdik.

14.41. $H \leq G$ olsun. X, G'nin altgruplarından oluşan küme olsun. H grubu X kümesi üzerine $h \cdot L = L^h$ kuralıyla etkir. L'nin H-yörüngesi,

$$L^H = \{L^h : h \in H\}$$

olur. L'nin H'deki sabitleyicisi ise,

$$H_L = \{h \in H : L^h = L\} = N_H(L)$$

olur. Dolayısıyla,

$$\left|L^H\right| = |H/H_L| = |H/N_H(L)|$$

olur. Buradan da

$$\left|L^H\right| = 1 \Leftrightarrow N_H(L) = H \Leftrightarrow H,\ L\text{'yi normalize eder}$$

eşdeğerlikleri çıkar.

14.42. **Alterne Grup Alt *n*.** $G = \operatorname{Sym} n$ olsun. G'nin, adına makas dediğimiz $(i\ j)$ türünden elemanlarla üretildiğini biliyoruz (sayfa 44). Örnek 8.38'ten,

$$\operatorname{Alt} n = \langle (i\ j)(k\ \ell) : i,\ j,\ k,\ \ell \in \{1, \ldots, n\}\rangle$$

grubunun indeksinin en fazla 2 olduğunu biliyoruz. Örnek 9.22'den bu altgrubun normal olduğunu biliyoruz. Demek ki ya $\operatorname{Sym} n = \operatorname{Alt} n$ ya da $[\operatorname{Sym} n : \operatorname{Alt} n] = 2$. Teorem 3.2'te İndeksin tam 2 olduğunu kanıtlamıştık. Burada farklı bir kanıt sunacağız.

G grubunu n değişkenli ve tamsayı katsayılı polinomlardan oluşan $\mathbb{Z}[T_1, \ldots, T_n]$ kümesi üzerine etkiyebiliriz:

$$\sigma \cdot f(T_1, \ldots, T_n) = f(T_{\sigma(1)}, \ldots, T_{\sigma(n)})$$

olsun. Bunun bir grup etkisi olduğunu görmek çok kolay, okura bırakıyoruz. Her $\sigma \in G$ ve her $f,\ g \in \mathbb{Z}[T_1, \ldots, T_n]$ için

$$\sigma(fg) = \sigma f \pm \sigma g \text{ ve } \sigma(f \pm g) = \sigma f\, \sigma g$$

olur. Özel bir $f \in \mathbb{Z}[T_1, \ldots, T_n]$ elemanı alalım:

$$f = \prod_{i>j} (X_i - X_j)$$

olsun. Her $\sigma \in G$ için, $\sigma(X_i - X_j) = \pm(X_i - X_j)$ olduğundan,

$$\sigma f = \pm f$$

olur. Demek ki G grubu $\{f, -f\}$ kümesi üzerine de etkir. Bundan böyle $n \geq 2$ olsun.

$$(1\ 2)f = -f$$

eşitliğini kanıtlamak kolay. Dolayısıyla her $i \neq j$ için de

$$(i\ j)f = -f$$

olur. Bundan da, her $\sigma \in \operatorname{Alt} n$ için,

$$\sigma f = f$$

bulunur. Bir başka deyişle,

$$\operatorname{Alt} n \leq G_f \leq G \tag{1}$$

olur. $(1\ 2)f = -f$ eşitliğinden, G'nin $\{f, -f\}$ kümesine geçişli etkidiği çıkar. Dolayısıyla

$$2 = |Gf| = |G/G_f|$$

olur. $[G : \operatorname{Alt} n] \leq 2$ olduğundan, bu eşitlikten ve (1)'den, $[\operatorname{Sym} n : \operatorname{Alt} n] = 2$ çıkar. Şu teoremin birinci önermesini kanıtladık[9], ikinci önerme de hemen bundan çıkar.

Teorem 14.3. *Eğer $n \geq 2$ ise, $\operatorname{Alt} n = \langle (i\ j)(k\ \ell) : i, j, k, \ell \in \{1, \ldots, n\}\rangle$ grubu $\operatorname{Sym} n$ grubunun indeksi 2 olan normal bir altgrubudur. Eğer $\alpha \in \operatorname{Sym} n \setminus \operatorname{Alt} n$ derecesi 2 olan herhangi bir elemansa (mesela $(1\ 2)$ makasıysa), $\operatorname{Sym} n = \operatorname{Alt} n \rtimes \langle \alpha \rangle$ olur.* □

$\operatorname{Alt} n$'nin elemanları çift sayıda makasın çarpımı olan elemanlar kümesi olduğuna dikkatinizi çekeriz. Geri kalanlar da tek sayıda makasın çarpımıdır elbette. Demek ki tek sayıda makasın çarpımı, çift sayıda makasın çarpımına eşit olamaz. Bir başka deyişle, tek sayıda makasın çarpımı Id_n olamaz.

Eğer $\alpha \in \operatorname{Sym} n$ elemanı aynı zamanda hem k tane hem de ℓ tane makasın çarpımıysa, diyelim $\alpha = t_1 \cdots t_k = s_1 \cdots s_\ell$ ise,

$$t_1 \cdots t_k s_\ell \cdots s_1 = 1$$

olur, dolayısıyla k ve s ya ikisi birden tektir ya da ikisi birden çifttir. Demek ki $\operatorname{sg} \alpha = (-1)^k = \pm 1$ tanımını yapabiliriz. Bu sayıya α'nın ***işareti*** adı verilir. $\operatorname{Alt} n$'nin elemanlarının işareti 1, diğerlerinin işareti -1'dir.

$$\alpha \mapsto \operatorname{sg} \alpha$$

fonksiyonunun bir $\operatorname{sg} : \operatorname{Sym} n \longrightarrow \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$ grup homomorfisi verdiğini kontrol etmek çok kolay. Buna ***işaret homomorfisi*** adı verilir. Çekirdeği elbette $\operatorname{Alt} n$ olur.

14.43. n bir tek sayı olmak üzere $|G| = 2n$ olsun. G'nin indeksi 2 olan bir altgrubu olduğunu kanıtlayacağız. $\varphi : G \longrightarrow \operatorname{Sym} G$ homomorfisi $g, x \in G$ için $\varphi_g(x) = gx$ olarak tanımlansın (standart etki, bkz. Örnek 14.8). Eğer $g \in G$ derecesi 2 olan bir elemansa, $\varphi_g \in \operatorname{Sym} G$ permütasyonu tam n tane, yani tek sayıda makasın çarpımıdır, dolayısıyla işareti -1'dir, yani $\operatorname{sg}(\varphi_g) = -1$ olur. Demek ki $\operatorname{sg} \circ \varphi : G \longrightarrow \{-1, 1\}$ homomorfisi örtendir. Dolayısıyla $K = \operatorname{Ker} \operatorname{sg} \circ \varphi$ normal bir altgruptur ve indeksi 2'dir. Eğer $g \in G$, derecesi 2 olan herhangi bir elemansa, elbette $G = K \rtimes \langle g \rangle$ olur.

14.44. (Reineke [R]) G eksponenti asal bir p olan bir grup olsun. $g, x \in G \setminus \{1\}$ için $g^x = g^i$ oluyorsa, O zaman $H = \langle x \rangle \simeq \mathbb{Z}/p\mathbb{Z}$ grubu $p-1$ elemanlı $X = \langle g \rangle \setminus \{1\}$ kümesine eşleniklikle etkir. Önsav 14.2'ye göre, g^H kümesinin eleman sayısı ya 1 ya da p olmak zorundadır. p olamayacağından, 1 olur, yani $g^x = g$ olmak zorundadır. Demek ki eksponenti p olan bir grubun en az p tane eşleniklik sınıfı vardır. Dolayısıyla sadece 2 eşleniklik sınıfı olan bir grup, Alıştırma 14.38'e göre sadece 2 elemanı olabilir, yani $\mathbb{Z}/2\mathbb{Z}$'ye izomorftur.

14.45. $\operatorname{Fix}_X G = \{x \in X : \text{her } g \in G \text{ için } gx = x\}$ olsun. $\operatorname{Fix}_X G$'nin elemanları, yörüngesi tek bir elemandan oluşan elemanlardır. Şu eşdeğerlilikler vardır:

$$x \in \operatorname{Fix}_X G \Leftrightarrow |Gx| = 1 \Leftrightarrow Gx = \{x\} \Leftrightarrow G_x = G \Leftrightarrow |G/G_x| = 1.$$

[9] Kanıt [La]'dan alınmıştır. Birçok kitapta bu teoremin ya çok karmaşık ya da yanlış kanıtı yayımlanmıştır. Verdiğimiz kanıta benzemeyen her kanıt, Örneğin Teorem 3.2'nin kanıtı (!) kuşkuyla karşılanmalıdır.

Şimdi (1) eşitliğini ele alalım. Elbette $\operatorname{Fix}_X G \subseteq T$ olur, ne de olsa $\operatorname{Fix}_X G$ kümesinin bir elemanının yörüngesi sadece o elemandan oluşur ve dolayısıyla bu eleman T'de olmak zorundadır. (1) eşitliğini şöyle yazalım:

$$\begin{aligned} X &= \bigsqcup_{t\in T} Gt = \Big(\bigsqcup_{t\in T\setminus \operatorname{Fix}_X G} Gt\Big) \sqcup \Big(\bigsqcup_{t\in \operatorname{Fix}_X G} Gt\Big) \\ &= \Big(\bigsqcup_{t\in T\setminus \operatorname{Fix}_X G} Gt\Big) \sqcup \Big(\bigsqcup_{t\in \operatorname{Fix}_X G} \{t\}\Big) \\ &= \Big(\bigsqcup_{t\in T\setminus \operatorname{Fix}_X G} Gt\Big) \sqcup \operatorname{Fix}_X G. \end{aligned}$$

Şimdi X'in sonlu olduğunu varsayıp, yukarıdaki eşitliği kümelerin eleman sayısı cinsinden yazalım:

$$|X| = \left(\sum_{t\in T\setminus \operatorname{Fix}_X G} |Gt|\right) + |\operatorname{Fix}_X G|. \tag{2}$$

Ama Önsav 14.2'ye göre $t \in T \setminus \operatorname{Fix}_X G$ için $|Gt| = |G/G_t| = |G|/|G_t| \neq 1$ olur. Demek ki,

$$|X| = \left(\sum_{t\in T\setminus \operatorname{Fix}_X G} \frac{|G|}{|G_t|}\right) + |\operatorname{Fix}_X G|. \tag{3}$$

Eğer bir p asalı ve bir $n > 0$ sayısı için $|G| = p^n$ ise, $t \in T \setminus \operatorname{Fix}_X G$ için $|Gt|$ sayısı p'ye bölünür; dolayısıyla (3)'ten dolayı $|\operatorname{Fix}_X G|$ sayısı da p'ye bölünür. Şu sonucu kanıtladık:

Önsav 14.4. *(G, X) bir grup etkisi olsun. Eğer G ve X sonluysa,*

$$|X| = \left(\sum_{t\in T\setminus \operatorname{Fix}_X G} \frac{|G|}{|G_t|}\right) + |\operatorname{Fix}_X G|$$

olur. Eğer ayrıca bir p asalı için $G \neq 1$ bir p-grupsa, $|X| \equiv |\operatorname{Fix}_X G| \mod p$ olur. Dolayısıyla eğer X'in eleman sayısı p'ye bölünmüyorsa, X'te G'nin her elemanı tarafından sabitlenen en az bir nokta vardır. □

14.46. Önsav 14.4'te $X = G$ olsun ve G, X üzerine eşleniklikle etkisin, yani $g \cdot x = x^g$ olsun. O zaman $\operatorname{Fix}_X G = Z(G)$ ve $G_x = C_G(x)$ olur. (3)'ten şu çıkar:

$$|G| = |Z(G)| + \sum_{x\in U} \frac{|G|}{|C_G(x)|} = |Z(G)| + \sum_{x\in U} |x^G|.$$

Formüldeki U, merkezde olmayan eşleniklik sınıfından bir ve bir tek eleman barındırır. Örneğin eğer $G = \operatorname{Sym} 4$ ise, $Z(G) = 1$ olur. $U = \{(1\ 2),\ (1\ 2\ 3),\ (1\ 2)(3\ 4),\ (1\ 2\ 3\ 4)\}$ olarak alabiliriz. Eşleniklik sınıflarının eleman sayıları

$$\begin{aligned} |(1\ 2)^G| &= \tbinom{4}{2} = 6 \\ |(1\ 2\ 3)^G| &= \tbinom{4}{3} \times 2 = 8 \\ |(1\ 2)(3\ 4)^G| &= \tbinom{4}{2}/2 = 3 \\ |(1\ 2\ 3\ 4)^G| &= 3! = 6 \end{aligned}$$

olur. Denklem bize

$$4! = 1 + 6 + 8 + 3 + 6$$

verir.

14.47. **[Matsuyama, H.]** *G sonlu bir p-grup ve $H \leq G$ olsun. Ya $H \lhd G$ olur ya da $H^x \leq N_G(H)$ içindeliğini sağlayan bir $x \in G \setminus N_G(H)$ vardır.*

Kanıt: $X = \{H^x : x \in G\}$ olsun. $|H| = |G/N_G(H)|$, dolayısıyla p'nin bir kuvveti olduğunu biliyoruz. Diyelim H normal değil. O zaman $|X| > 1$ olur. $Y = X \setminus \{H\}$ olsun. H grubu Y üzerine eşleniklikle etkir: $h \cdot H^x = H^{xh^{-1}}$. Şimdi Önsav 14.4'ü uygularsak H'nin sabitlediği, yani normalize ettiği bir $H^x \in Y$ noktasının varlığını görürüz. Hatta bunlardan en az $p-1$ tane vardır. □

14.48. Önsav 14.4'ün önemli bir sonucunu daha bulalım.

Teorem 14.5. *$H \leq \operatorname{Aut} G$ olsun. Bir p asalı için G ve H'nin sonlu p-grupları olduklarını varsayalım. O zaman $1 < \operatorname{Fix}_G H = \{g \in G : \text{her } \varphi \in H \text{ için } \varphi(g) = g\} \leq G$ olur.*

Kanıt: (H, G) bir grup etkisidir (Örnek 14.6). $\operatorname{Fix}_G H$ elbette G'nin bir altgrubudur. Önsav 14.4'ü uygularsak p asalının $\operatorname{Fix}_G H$ altgrubunun eleman saysını böldüğü çıkar. Etkisiz elemanın varlığından dolayı $0 < |\operatorname{Fix}_G H|$ olur. □

Aslında bu teoremde H'nin illa sonlu olduğunu varsaymak gerekmez, önemli olan G'ye sadık etkiyen $H/\operatorname{Ker}(H, G)$ grubunun sonlu bir p-grubu olmasıdır, ki G sonlu olduğundan bu grup da mutlaka sonlu olmalıdır.

14.49. Teorem 14.5'i kullanarak Teorem 8.10'u bir kez daha kanıtlayabiliriz:

Teorem 14.6. *Sonlu bir p-grubunun merkezi 1'den farklıdır.*

Kanıt: Cauchy teoreminden dolayı sonlu bir p-grubunun eleman sayısı p'nin bir kuvvetidir. Bir önceki teoremde H yerine $\operatorname{Inn} G$ alalım. $\operatorname{Inn} G \simeq G/Z(G)$ olduğundan, $\operatorname{Inn} G$'de bir p-grubudur. Dolayısıyla $\operatorname{Fix}_G(\operatorname{Inn} G) \neq 1$. Ama tabii ki

$$\operatorname{Fix}_G(\operatorname{Inn} G) = \{x \in G : \text{Her } g \in G \text{ için } \operatorname{Inn}_g(x) = x\} = Z(G).$$

Teorem kanıtlanmıştır. □

Dikkatli okur, bu kanıtın Teorem 8.10'un kanıtından farklı olmadığını, sadece aynı kanıtı bir başka dile çevirdiğimizin farkına varacaktır.

14.50. Burnside eşitliği olarak anılan son derece ilginç ve şaşırtıcı bir eşitlik kanıtlayacağız. $g \in G$ için,

$$\operatorname{Fix}_X g = \{x \in X : gx = x\}$$

tanımını yapalım. $\operatorname{Fix}_X g$, g'nin sabitlediği noktalar kümesidir. Mesela $\operatorname{Fix}_X 1 = X$ olur.

Teorem 14.7 (Burnside)**.** *G ve X sonluysa, G'nin bir elemanının sabitlediği ortalama nokta sayısı yörünge sayısı kadardır. Yani eğer yörünge sayısı t ise,*

$$\frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_X g| = t$$

olur.

Kanıt: Aşağıdaki kümeyi iki farklı biçimde sayacağız:

$$A = \{(g, x) \in G \times X : gx = x\}.$$

Önce şu hesabı yapalım:

$$|A| = \sum_{g \in G} |\{x \in X : gx = x\}| = \sum_{g \in G} |\operatorname{Fix}_X g|.$$

Bir de şu hesabı:

$$|A| = \sum_{x \in X} |\{g \in G : gx = x\}| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|Gx|}.$$

Ama aynı yörüngede olan x noktaları için $|Gx|$ sabittir. Dolayısıyla eğer $T \subseteq X$ kümesi her yörüngeden bir ve bir tane nokta barındırıyorsa, $t \in T$ için,

$$\sum_{x \in Gt} \frac{|G|}{|Gx|} = \sum_{x \in Gt} \frac{|G|}{|Gt|} = |G|$$

olur. Bunu göz önüne alarak bir önceki eşitlik dizisini kaldığımız yerden devam ettirelim:

$$|A| = \sum_{x \in X} \frac{|G|}{|Gx|} = \sum_{t \in T} \left(\sum_{x \in Gt} \frac{|G|}{|Gx|} \right) = \sum_{t \in T} |G| = |T||G|$$

elde ederiz. İlk eşitliğimizle birlikte,

$$\sum_{g \in G} |\operatorname{Fix}_X g| = |A| = |T||G|$$

elde ederiz. □

14.51. Şimdi IMO 1987 yarışmasında sorulan ve Alıştırma 3.37'te sorduğumuz soruyu yanıtlayabiliriz:

$$P_n(k) = \{f \in \operatorname{Sym} n : f \text{ tam } k \text{ eleman sabitliyor}\}$$

olsun.

$$\sum_{k=0}^{n} k|P_n(k)| = n!$$

eşitliğini kanıtlayın.

Kanıt: Biraz önce kanıtlanan Burnside eşitliğini uygulayalım:

$$1 = t = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_X g| = \frac{1}{n!} \sum_{k=0}^{\infty} \sum_{g \in P_n(k)} |\operatorname{Fix}_X g| = \frac{1}{n!} \sum_{k=0}^{\infty} \sum_{g \in P_n(k)} k = \frac{1}{n!} \sum_{k=0}^{\infty} |P_n(k)|k.$$

İstediğimiz eşitlik kanıtlanmışır. Lise öğrencilerinin bu cevabu bulabilmeleri için, Burnside'ın teoreminde olduğu gibi

$$A = \{(g, x) \in \operatorname{Sym} n \times \{1, \ldots, n\} : gx = x\}$$

kümesini iki farklı biçimde saymaları gerekiyordu herhalde. □

Alıştırmalar

14.52. $(\operatorname{Sym} n)' \leq \operatorname{Alt} n$ olduğunu kanıtlayın.

14.53. $\operatorname{Sym} n$'nin tek elemanlı her altgrubunun $\operatorname{Alt} n$'nin bir altgrubu olduğunu kanıtlayın.

14.54. $\operatorname{Sym} n$'nin $\operatorname{Alt} n$'nin altgrubu olmayan her altgrubunun indeksi 2 olan normal bir altgrubu olduğunu kanıtlayın.

14.55. (G, X) bir grup etkisi olsun. A, $B \subseteq G$ ve Y, $Z \subseteq X$ olsun.

$$F(A) = \operatorname{Fix}_X A = \{x \in X : \text{ her } a \in A \text{ için } ax = x\} = \bigcap_{a \in A} \operatorname{Fix}_X a$$

olsun. Aşağıdaki önermeleri kanıtlayın:

a. $A \subseteq G_{F(A)}$.

b. $Y \subseteq F(G_Y)$.

c. Eğer $A \subseteq B$ ise $F(B) \subseteq F(A)$.

d. Eğer $Y \subseteq Z$ ise $G_Z \leq G_Y$.

e. $F(G_{F(A)}) = F(A)$.

f. $G_{F(G_Y)} = G_Y$.

15. Sıfırkuvvetli ve Çözülür Gruplar

Bu bölümde illa abel grubu olmak zorunda olmayan ama abel gruplarına oldukça benzeyen gruplar üzerinde duracağız: sıfırkuvvetli ve çözülür gruplar. Dileyen okur bu (son derece önemli) bölümü daha sonraya bırakarak bir sonraki bölüme geçebilir.

15.1 Komütatör Altgrupları

G bir grup ve H, $K \leq G$ olsun. H ve K'nın ***komütatör grubu*** adı verilen $[H, K]$ altgrubu şöyle tanımlanır:

$$[H, K] = \langle [h, k] : h \in H,\ k \in K \rangle.$$

Buradaki $[h, k]$ elemanı $[h, k] = h^{-1}k^{-1}hk$ olarak tanımlanmıştır. Bu tür elemanlara ***komütatör*** adı verilir. Demek ki $[H, K]$ altgrubunun elemanları, $h \in H$ ve $k \in K$ için $[h, k]$ ya da $[h, k]^{-1}$ biçiminde yazılan sonlu sayıda elemanın çarpımıdır; çarpılacak komütatör ve tersi sayısının bir üstsınırı olmayabileceği gibi, bazı durumlarda sadece bir tek çarpım yetebilir; en uç örnek $[H, K] = 1$ durumu, bu durumda $[H, K]$ altgrubunun her elemanı 0 tane komütatörün çarpımıdır.

Biraz hesapla kolayca kanıtlanacağı üzere $[k, h] = [h, k]^{-1}$ olduğundan, $[H, K] = [K, H]$ olur.

Eğer H altgrubu K'yı normalize ediyorsa, her $h \in H$ ve $k \in K$ için

$$[h, k] = h^{-1}k^{-1}hk = (h^{-1}k^{-1}h)k \in KK \subseteq K,$$

dolayısıyla $[H, K] \leq K$ olur. Eğer H ve K birbirlerini normalize ediyorlarsa (mesela her ikisi de G'de normalse), $[H, K] \leq H \cap K$ olur. Bir de ayrıca $H \cap K = 1$ ise, her $h \in H$ ve $k \in K$ için $hk = kh$ olur.

$[h, k]^g = [h^g, k^g]$ eşitliğinden, eğer bir g elemanı H ve K altgruplarını normalize ediyorsa, o zaman g'nin $[H, K]$ altgrubunu da normalize ettiği çıkar.

Dolayısıyla eğer $H,\ K \lhd G$ ise, $[H,K] \lhd G$ çıkar. Bu bulduğumuz sonuç şaşırtıcı olmayabilir, ama bir sonraki paragrafta normallik konusunda beklenmedik bir sonuç kanıtlayacağız.

Basit bir hesapla hemen çıkan

$$[xy,z] = [x,z]^y[y,z] \text{ ve } [x,yz] = [x,z][x,y]^z \tag{1}$$

eşitliklerinden, daha doğrusu bunların doğrudan bir sonucu olan

$$[x,z]^y = [xy,z][y,z]^{-1} \text{ ve } [x,y]^z = [x,z]^{-1}[x,yz]$$

eşitliklerinden kolaylıkla (ve sırasıyla) H ve K altgruplarının $[H,K]$ altgrubunu normalize ettiği anlaşılır, yani $\langle H,K\rangle \leq N_G([H,K])$ olur. Bunun özel bir durumu olarak her $H \leq G$ için $[G,H] \lhd G$ elde ederiz.

Eğer $\varphi : G \longrightarrow G_1$ bir grup homomorfisiyse, elbette

$$\varphi([H,K]) = [\varphi(H),\varphi(K)]$$

olur. Eğer $A \lhd G$ ise, bundan,

$$[HA/A, KA/A] = [H,K]A/A$$

çıkar.

Bu bulduklarımızı ileride referans verebilmek amacıyla bir önsavda toparlayalım:

Önsav 15.1. *G bir grup ve $H,\ K \leq G$ olsun.*

i. *$[H,K] = [K,H]$ olur.*

ii. *Eğer $H,\ K \lhd G$ ise $[H,K] \lhd G$ olur.*

iii. *Eğer H altgrubu K'yı normalize ediyorsa, $[H,K] \leq K$ olur. Dolayısıyla eğer H ve K birbirlerini normalize ediyorlarsa (örneğin G'de normallerse) $[H,K] \leq H \cap K$ olur; ve eğer bir de ayrıca $H \cap K = 1$ ise, her $h \in H$ ve $k \in K$ için $hk = kh$ olur.*

iv. *H ve K altgrupları $[H,K]$ altgrubunu normalize eder.*

v. *$[G,H] \lhd G$ olur.*

vi. *Eğer $\varphi : G \longrightarrow G_1$ bir grup homomorfisiyse, her $H,\ K \leq G$ için,*

$$\varphi([H,K]) = [\varphi(H),\varphi(K)]$$

olur.

vii. *Eğer $A \lhd G$ ise $[HA/A, KA/A] = [H,K]A/A$ olur.* □

Notlar ve Örnekler

15.1. [**Transfer**[1]] G bir grup ve $H \leq G$, indeksi $n < \infty$ olan bir altgrup olsun. G/H sol ötelemeler kümesinin temsilcilerini seçelim, diyelim $x_1, \ldots, x_n$ elemanlarını seçtik. Demek ki

$$G = \bigsqcup_{i=1}^{n} x_i H.$$

Şimdi $g \in G$ olsun. Her $i = 1, \ldots, n$ için, öyle bir $j = 1, \ldots, n$ ve $h \in H$ var ki

$$g x_i = x_j h$$

olur. Buradaki j ve h elbette i'ye g'ye göre değişir. Bir

$$\alpha_g : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$$

fonksiyonu ve $f_i(g) \in H$ elemanı için

$$g x_i = x_{\sigma_g(i)} f_i(g)$$

yazalım. Ardından H/H' grubunun şu elemanını ele alalım:

$$\tau(g) = \prod_{i=1}^{n} \overline{f_i(g)} \in H/H'.$$

Çarpım sırasının önemi yoktur çünkü H/H' bir abel grubudur. (H/H' grubu yerine $H' \leq A \leq H$ için H/A türünden bir grup da alabilirdik.)
Şimdi birkaç (oldukça şaşırtıcı) şey kanıtlayalım.
a. *Her $g \in G$ için $\sigma_g \in \operatorname{Sym} n$ olur.*
Kanıt: α_g'nin birebir olduğunu kanıtlamak yeterli. Diyelim $\sigma_g(i) = \sigma_g(j)$. O zaman

$$g x_i,\ g x_j \in x_{\sigma_g(i)} H = x_{\sigma_g(j)} H$$

olur, ve dolayısıyla

$$x_j^{-1} x_i = ((g x_j)^{-1})(g x_i) \in H$$

olur, ki bundan da $x_i = x_j$, yani $i = j$ çıkar.
b. *$\tau(g)$ elemanı x_i'lerin seçiminden bağımsızdır.*
Kanıt: Bir başka temsilciler kümesi seçelim: $h_i \in H$ için $y_i = x_i h_i$ olsun. $g \in G$ olsun. O zaman

$$g y_i = g x_i h_i = x_{\sigma_g(i)} f_i(g) h_i = y_{\sigma_g(i)} h_i^{-1} f_i(g) h_i \in y_{\sigma_g(i)} H$$

olur. Demek ki f_i'ye tekabül eden f_i' fonksiyonu

$$f_i'(g) = h_i^{-1} f_i(g) h_i$$

olarak tanımlanmıştır. Bu eleman H/H' grubunda hesaplandığında

$$\overline{f_i(g)} = \overline{f_i'(g)}$$

çıkar. Demek ki $\tau(g)$ değeri de değişmez. (Bu arada σ_g permütasyonunun da x_i'lerin seçiminden bağımsız olduğunu gösterdik.)
c. *τ bir homomorfidir.*
Kanıt: $a, b \in G$ olsun.

$$(ab) x_i = a(b x_i) = a(x_{\sigma_b(i)} f_i(b)) = (a x_{\sigma_b(i)}) f_i(b) = x_{\sigma_a(\sigma_b(i))} f_{\sigma_b(i)}(a) f_i(b)$$

[1] Issai Schur ve Emil Artin tarafından bağımsız bulunan transfer kavramı, sonlu grup teoride ve cebirsel sayılar kuramında önemlidir, ama bu notlarda bir daha kullanılmayacaktır.

ve

$$(ab)x_i = x_{\sigma_{ab}(i)} f_i(ab)$$

hesaplarından,

$$f_i(ab) = f_{\sigma_b(i)}(a) f_i(b)$$

çıkar. Demek ki

$$\begin{array}{rcl} \tau(ab) & = & \prod_i \overline{f_i(ab)} = \prod_i \left(\overline{f_{\sigma_b(i)}(a)}\, \overline{f_i(b)} \right) \\ & = & \prod_i \overline{f_{\sigma_b(i)}(a)} \prod_i \overline{f_i(b)} = \prod_i \overline{f_i(a)} \prod_i \overline{f_i(b)} \\ & = & \tau(a)\tau(b). \end{array}$$

(Sondan bir önceki eşitlik σ_b'nin bir permütasyon olmasından çıkar.) Bu arada $\sigma_{ab} = \sigma(a) \circ \sigma(b)$ eşitliğini de kanıtladık, ama bunu çok daha önceden de biliyorduk: Bkz örnek 8.28.

d. $G' \leq \operatorname{Ker} \tau$ *olur, bu sayede* $\overline{\tau}(\overline{g}) = \tau(g)$ *fonksiyonu* G/G' *grubundan* H/H' *grubuna giden bir homomorfi tanımlar.*

Kanıt: H/H' bir abel grubu olduğundan, $G' \leq \operatorname{Ker} \tau$ olur. Gerisi kolay. □

15.2. $n \geq 2$, $G = \operatorname{Sym} n$, $H = \langle (1\ 2) \rangle = \{\mathrm{Id}_n, (1\ 2)\} \simeq \mathbb{Z}/2\mathbb{Z}$ olsun. $\tau : \operatorname{Sym} n \longrightarrow H$ transfer fonksiyonunu hesaplayalım. Teorem 14.3'e göre

$$\operatorname{Sym} n = \operatorname{Alt} n \sqcup \operatorname{Alt} n (1\ 2) = \operatorname{Alt} n\ H.$$

Demek ki sol temsilciler kümesi olarak $\operatorname{Alt} n$ grubunu alabiliriz. α, $\beta \in \operatorname{Alt} n$ için, $\alpha\beta = \gamma h$ eşitliğini sağlayan $\gamma \in \operatorname{Alt} n$ ve $h \in H$ vardır. Ama $\operatorname{Alt} n$ bir grup olduğu için $h = \mathrm{Id}_n$ olmak zorundadır. Demek ki τ fonksiyonu $\operatorname{Alt} n$ üzerinde sabit 1 (ya da Id_n) değerini alıyor. Öte yandan $(1\ 2)\beta = ((1\ 2)\beta(1\ 2)^{-1})(1\ 2)$, ve $(1\ 2)\beta(1\ 2)^{-1} \in \operatorname{Alt} n$ ve $(1\ 2) \in H$ olduğundan, $\tau(1\ 2) = (1\ 2)^{|\operatorname{Alt} n|} = (1\ 2)^{n!/2}$ olur. Demek ki $n \geq 4$ ise τ, sabit Id_n fonksiyonudur. Eğer $n = 3$ ise τ fonksiyonu $\operatorname{Alt} n$ üzerinde Id_n, geri kalan elemanlar üzerine $(1\ 2)$ değerini alır, yani işaret fonksiyonunun yaptığını yapar aşağı yukarı.

15.3. $G = \langle x \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ ve n'yi bölen bir k doğal sayısı için, $H = \langle x^k \rangle$ olsun. O zaman $X = \{1, x, x^2, \ldots, x^{k-1}\}$ kümesi H'nin bir temsilciler kümesidir. (Bkz. Örnek 8.2.) $\tau : G \longrightarrow H$ transfer homomorfisini bulalım. G döngüsel olduğundan, $\tau(x)$ değerini bulmak yeterli. $i = 0, 1, 2, \ldots, k-2$ için $xx^i = x^{i+1} \in X$ olduğundan ve $xx^{k-1} = x^k \in H$ olduğundan, $\tau(x) = x^k$ olur. Demek ki τ homomorfisi elemanların k'ıncı kuvvetlerini alır: Her $g \in G$ için $\tau(g) = g^k$ olur.

Alıştırmalar

15.4. Herhangi bir G grubunda, her x, $y \in G$ ve her n doğal sayısı için

$$[x, y^n] = [x, y][x, y]^y \cdots [x, y]^{y^{n-1}}$$

eşitliğini kanıtlayın. İpucu: (1) ve tümevarım. Ayrıca ($n = 0$ için) "hiç tane" komütatörün çarpımı tanım gereği 1'dir.

15.5. Herhangi bir G grubunda, her x, $y \in G$ ve her n, m doğal sayısı için $[x^m, y^n]$ elemanının $[x, y]^{x^i y^j}$ türünden elemanların çarpımı olduğunu kanıtlayın.

15.6. A, B, $C \lhd G$ olsun. $[A, BC] = [A, B][A, C]$ ve $[AB, C] = [A, C][B, C]$ eşitliklerini gösterin.

15.7. $A = \langle X \rangle$ ve $B = \langle Y \rangle$ olsun. Her $g \in G$ için $X^g \subseteq X$ ve $Y^g \subseteq Y$ varsayımını yapalım. $[A, B] = \langle [x, y] : x \in X,\ y \in Y \rangle$ eşitliğini gösterin.

15.8. G bir grup ve $A \lhd G$ bir abel altgrubu olsun. Bir $g \in G$ alalım. Alıştırma 9.32.b'ye göre $\operatorname{ad}(g) : A \longrightarrow A$ bir grup homomorfisidir. $[G', A] = 1$ varsayımını yapalım. Şunları gösterin:

a. $C_A(g) \lhd G$.
b. $[g, A] = \mathrm{ad}(g)(A)$.
c. $[g, A] \lhd G$.

15.9. $g \in G$ ve $H \leq G$ olsun. $[g, H] \subseteq Z$ varsayımını yapalım. $\mathrm{ad}(g)(h) = [g, h]$ ile tanımlanmış $\mathrm{ad}(g) : H \longrightarrow Z$ fonksiyonunun bir grup homomorfisi olduğunu gösterin. Her $h \in H$, $n \in Z$ için $[g, h]^n = [g^n, h] = [g, h^n]$ eşitliğini gösterin.

15.10. Eğer $z \in Z_2(G)$ elemanı $z^n \in Z$ içindeliğini sağlıyorsa, $[z, G]$ altgrubunun eksponentinin sonlu olduğunu ve n'yi böldüğünü kanıtlayın.

15.11. $G = D_6 \simeq \mathrm{Sym}\,3$ ve $\mathbb{Z}/3\mathbb{Z} \simeq H = G' \leq G$, derecesi üç olan bir eleman tarafından üretilen altgrup olsun. $\tau : G \longrightarrow H$ transfer homomorfisinin sabit 1 fonksiyonu olduğunu kanıtlayın.

15.12. $G = D_6$ ve $t \in G \simeq \mathrm{Sym}\,3$, derecesi iki olan bir eleman ve $H = \langle t \rangle = \{1, t\}$ olsun. $\tau : G \longrightarrow H$ transfer homomorfisini bulun. (Bu sefer sabit 1 fonksiyonu olmaz).

15.2 Azalan Merkezî Seriler, Türev Serileri

Bu altbölümde bir G grubunun çok özel ve çok önemli altgruplarını tanımlayacağız.

$$G^0 = G^{(0)} = G$$

olsun. i üzerine tümevarımla,

$$G^{i+1} = [G, G^i]$$

ve

$$G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

tanımlarını yapalım.

$$G^1 = G^{(1)} = [G, G]$$

eşitliğine dikkatinizi çekerim. Adına G'nin ***türevi*** denen bu altgrup daha ziyade G' olarak yazılır ve çok önemlidir. Başat özellikleri aşağıda:

Önsav 15.2. *G' altgrubu G/H'nin bir abel altgrubu olduğu G'nin en küçük altgrubudur; bir başka deyişle G/G' bir abel grubudur ve eğer $H \lhd G$ için G/H bir abel grubuysa $G' \leq H$ olur. Ayrıca eğer $G' \leq H \leq G$ ise, $H \lhd G$ olur ve G/H grubu abeldir.*

Kanıt: Her x, $y \in G$ için, G/G' grubunda çalışarak,

$$\overline{x}^{-1}\overline{y}^{-1}\overline{xy} = \overline{x^{-1}y^{-1}xy} = \overline{[x, y]} = \overline{1}$$

yani,

$$\overline{xy} = \overline{yx}$$

buluruz. Demek ki G/G' bir abel grubudur.

Şimdi $H \lhd G$ olsun ve G/H grubunun abel olduğunu varsayalım. O zaman G/H grubunda hesap yaparak, her $x, y \in G$ için,

$$\overline{x^{-1}y^{-1}xy} = \overline{x}^{-1}\overline{y}^{-1}\overline{xy} = 1,$$

yani

$$x^{-1}y^{-1}xy \in H$$

buluruz. G' grubunun elemanları bu tür elemanların ve terslerinin çarpımı olduğundan, bu bulduğumuzdan $G' \leq H$ çıkar.

Son olarak G' altgrubunu içeren bir $H \leq G$ alalım. O zaman her $h \in H$ ve $g \in G$ için,

$$h^g = g^{-1}hg = hh^{-1}g^{-1}hg = h[h, g] \in HG' \subseteq H$$

olur. Demek ki $H \lhd G$ olur.

Bu son sonucun bir başka kanıtını verelim: G/G' grubu abel olduğundan her altgrubu normaldir. Şimdi sonuç, Teorem 11.1'in son cümlesinden çıkar. □

Eğer $H \leq G$ ise H' altgrubundan da sözedebiliriz: $H' = [H, H]$. Örneğin, tanıma göre,

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] = (G^{(i)})' \leq G^{(i)}$$

olur. Demek ki $G^{(i)}/G^{(i+1)}$ bir abel grubudur.

G^i ve $G^{(i)}$ altgruplarının daha başka temel özelliklerini görelim.

Önsav 15.1.v'e göre her $G^i \lhd G$ olur. (Bunu kanıtlamak için tümevarıma bile gerek yok.) Önsav 15.1.ii'ye göre tümevarımla her i için $G^{(i)} \lhd G$ olur.

Tanımdan hemen $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq G^{(i)}$ içindeliği çıkar. $G^n \lhd G$ olduğundan, Önsav 15.1.iii'ün ikinci cümlesinden, her i için $G^{i+1} = [G, G^i] \leq G^i$ olduğu görülür. Aynı olgu tümevarımla da kanıtlanabilir: $G^{i+1} = [G, G^i] \leq [G, G^{i-1}] = G^i$. Demek ki hem $(G^i)_i$ hem de $(G^{(i)})_i$ altgrup dizisi azalandır. $(G^n)_n$ dizisine ***azalan merkezî seri*** adı verilir. $(G^{(n)})_n$ dizisine de ***azalan türev serisi*** denir[2].

Bu dizilerin iki ardışık teriminde eşitlik elde edersek, eşitlik sonsuza dek sürer: Eğer $G^i = G^{i+1}$ ise $G^{i+2} = [G, G^{i+1}] = [G, G^i] = G^{i+1}$ olur; aynı şekilde eğer $G^{(i)} = G^{(i+1)}$ ise $G^{(i+2)} = [G^{(i+1)}, G^{(i+1)}] = [G^{(i)}, G^{(i)}] = G^{(i+1)}$ olur[3].

$G^{(i)} \leq G^i$ içindeliği kolaylıkla tümevarımla kanıtlanabilir:

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [G, G^i] = G^{i+1}.$$

Ama birazdan bundan çok daha iyisini kanıtlayacağız.

$(G^{(i)})^{(j)} = G^{(i+j)}$ eşitliği j üzerine tümevarımla kolaylıkla kanıtlanabilir.

Bu bulduklarımızı da not edelim:

[2] Aslında bir seriden değil, bir diziden sözetmek gerekir ama gelenek bu yöndedir.

[3] $G^\omega = \bigcap_{i\in\mathbb{N}} G^i$ ve $G^{(\omega)} = \bigcap_{i\in\mathbb{N}} G^{(i)}$ tanımları yapılıp aynı prosedürle dizi devam ettirilebilir. Bir α ordinali için G^α ve $G^{(\alpha)}$ altgrupları tahmin edilen yöntemle tanımlanabilir; ama biz böyle bir uğraşa girişmeyeceğiz.

Önsav 15.3. *Her $i, j \in \mathbb{N}$ için aşağıdakiler doğrudur:*
i. G^i, $G^{(i)} \lhd G$.
ii. $G^{i+1} \leq G^i$ *ve* $G^{(i+1)} \leq G^{(i)}$.
iii. $G^{(i)} \leq G^i$.
iv. $G^{(i)}/G^{(i+1)}$ *bir abel grubudur.*
v. $(G^{(i)})^{(j)} = G^{(i+j)}$ *olur.* □

Eğer $H \leq G$ ise, tümevarımla kolaylıkla $H^i \leq G^i$ ve $H^{(i)} \leq G^{(i)}$ olduğu gösterilebilir. Ayrıca, gene tümevarımla, eğer $H \lhd G$ ise, Önsav 15.1.vii kullanılarak $(G/H)^i = G^iH/H$ ve $(G/H)^{(i)} = G^{(i)}H/H$ olduğunu göstermek işten bile değildir.

Önsav 15.4. *Eğer $H \leq G$ ise $H^i \leq G^i$ ve $H^{(i)} \leq G^{(i)}$ olur. Ayrıca, eğer $H \lhd G$ ise $(G/H)^i = G^iH/H$ ve $(G/H)^{(i)} = G^{(i)}H/H$ olur.* □

Alıştırmalar

15.13. G^i/G^{i+1} bölüm grubunun bir abel grubu olduğunu kanıtlayın.

15.14. $G = D_{2n}$ grubu için G^i ve $G^{(i)}$ altgruplarını hesaplayın.

15.15. $(\operatorname{Sym} n)' \leq \operatorname{Alt} n$ olduğunu kanıtlayın.

15.16. $(\operatorname{Sym} n)' = \operatorname{Alt} n$ eşitliğini kanıtlayın. İpucu: Eğer $n = 3$ ise $\operatorname{Alt} n$'nin her elemanı bir komütatördür. Eğer $n \geq 4$ ise, her ayrık $(i\ j)$ ve $(k\ \ell)$ makasları için $(i\ j)(k\ \ell)$ permütasyonu 2 komütatörün çarpımıdır.

15.17. Eğer $n \geq 5$ ise $(\operatorname{Alt} n)' = \operatorname{Alt} n$ eşitliğini (bir biçimde!) kanıtlayın.

15.18. Önsav 15.3'ü dikkatlice kanıtlayın. (Basit fakat önemli bir alıştırmadır.)

15.19. Önsav 15.4'ü dikkatlice kanıtlayın. (Basit fakat önemli bir alıştırmadır.)

15.20. G^n grubunun $[x_1, [x_2, \ldots, [x_n, x_{n+1}] \ldots]]$ türünden elemanlar tarafından üretildiğini kanıtlayın. Benzer bir önermeyi $G^{(n)}$ grupları için bulup kanıtlayın.

Önsav 15.3.iii'ten çok daha iyisini yapabiliriz:

Önsav 15.5. *G bir grup olsun.*
i. *Her $x, y, z \in G$ için $[[x, y^{-1}], z]^y [[y, z^{-1}], x]^z [[z, x^{-1}], y]^x = 1$ olur.*
ii. *Eğer $H, K \leq G$ altgrupları $[[H, K], K] = 1$ eşitliğini sağlıyorlarsa $[H, K'] = 1$ olur.*
iii. P. Hall'un Üç Altgrup Önsavı. *$H, K, L \lhd G$ olsun. O zaman*

$$[[H, K], L] \leq [[K, L], H][[L, H], K]$$

olur.
iv. *Her i ve j doğal sayıları için $[G^i, G^j] \leq G^{i+j+1}$ olur.*
v. *Her i için $G^{(i)} \leq G^{2^i - 1}$ olur.*

Kanıt: i. Tamamen hesaba dayalı. Okura bırakıyoruz.

ii. Eğer birinci kısımda $x \in H$ ve $y, z \in K$ alırsak, $[[y, z^{-1}], x] = 1$ elde ederiz. Bu da istediğimizi verir.

iii. Bu da birinci kısımdan kolayca çıkar.

iv. Önermenin her i ve j için doğru olduğunu j üzerine tümevarımla kanıtlayacağız. Eğer $j = 0$ ise tanımdan istediğimiz çıkar. Eğer önerme sabit bir j ama her i için doğruysa, bir önceki kısımdan

$$\begin{aligned}
[G^i, G^{j+1}] &= [G^i, [G^j, G]] \leq [G^j, [G, G^i]][G, [G^i, G^j]] \\
&= [G^{i+1}, G^j][G, [G^i, G^j]] \leq [G^{i+1}, G^j][G, G^{i+j+1}] \\
&\leq G^{i+1+j+1}[G, G^{i+j+1}] = G^{i+1+j+1}G^{i+j+1+1} \\
&= G^{i+j+2}
\end{aligned}$$

çıkar. İstediğimiz kanıtlanmıştır.

v. Eğer $i = 0$ ise kanıtlayacak bir şey yok. Eğer önerme i için doğruysa,

$$\begin{aligned}
G^{(i+1)} &= [G^{(i)}, G^{(i)}] \leq [G^{2^i-1}, G^{2^i-1}] \\
&\leq G^{(2^i-1)+(2^i-1)+1} = G^{2^i+2^i-1} = G^{2^{i+1}-1}.
\end{aligned}$$

olur. İstediğimiz kanıtlanmıştır. □

15.3 Çözülür Gruplar

Abel gruplarını geçmişte incelemiştik ve her ne kadar sınıflandıramasak da en azından sonlu eleman tarafından üretilenleri (dolayısıyla sonlu olanlarını) sınıflandırmıştık. Bu ve daha birçok nedenden (tam olarak doğru olmasa da) abel grupları anlaşılması kolay gruplar olarak addedilebilir. Eğer bir G grubunun normal bir $1 \neq A < G$ abel altgrubu varsa ve ayrıca G/A bölüm grubu abelse, o zaman G'nin abel gruplarından biraz daha komplike bir grup olduğu ama anlaşılması çok da zor olmayan bir grup olduğuna hükmedebiliriz. Bu tür gruplara bazen ***metabel grupları*** dendiği olur. Bu gruplar bir anlamda "yarım abeldirler". Eğer bir G grubunun normal bir abel A grubu varsa ve G/A metabelse, o zaman bu grup metabel grupları kadar olmasa da gene de bir nebze kolay bir grup olduğuna hükmedebiliriz; bu gruplar da "üçte bir abel" olarak addedilebilir. Bunu devam ettirebiliriz. İşte bu bölümde bir grubun abel-bölü-abel-bölü-abel-...-bölü-abel olmasını kavramlaştıracağız.

G bir grup olsun ve diyelim G'nin öyle

$$1 = A_n \leq A_{n-1} \leq \ldots \leq A_1 \leq G = A_0 \qquad \text{(Ç)}$$

normal altgrupları var ki her $i = 0, 1, \ldots, n-1$ için A_i/A_{i+1} bir abel grubu oluyor. Bu durumda G'ye ***çözülür grup*** denir. Çözülür grup kavramı, katsayılarının köklerini alarak ve toplama çarpma gibi temel aritmetik işlemleriyle polinomiyal denklemlerin köklerin bulunmasına dayanır ve ta Evariste Galois'ya kadar gider. Eğer n bu özelliği sağlayan en küçük doğal sayıysa, G'ye

n'inci dereceden çözülür grup ve n'ye G'nin ***çözülürlük sınıfı*** adı verilir. Demek ki 1 grubu 0'ıncı dereceden çözülür gruptur, 1 olmayan bir abel grubu 1'inci dereceden çözülür gruptur, abel olmayan bir metabel grup 2'inci dereceden çözülür gruptur vs.

Bu kavram çok yararlıdır çünkü çözülürlük sınıfı üzerine tümevarım yapılıp kimileyin abel grupları için doğru olan olgular çözülür gruplar için genelleştirilebilir.

Bu arada, A_i/A_{i+1} grubunun abel olmasının $A_i' \leq A_{i+1}$ önermesine denk olduğunu anımsayalım. Bu gözlemden, eğer G grubunun (Ç)'deki gibi bir normal altgrup dizisi varsa o zaman her i için $G^{(i)} \leq A_i$ olduğu çıkar; nitekim $i = 0$ ise kanıtlanacak bir şey yok ve eğer $G^{(i)} \leq A_i$ ise, $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [A_i, A_i] \leq A_{i+1}$ olur. Dolayısıyla $G^{(n)} = 1$ olur. Demek ki eğer G en fazla n'inci dereceden çözülürse o zaman $G^{(n)} = 1$ olur.

Tersine, diyelim $G^{(n)} = 1$. O zaman Önsav 15.3.iv'e göre, G çözülür bir gruptur ve (tanıma göre) çözülürlük sınıfı en fazla n'dir. Bir teorem elde ettik.

Teorem 15.6. *G'nin en fazla n'inci dereceden çözülür olması için yeter ve gerek koşul $G^{(n)} = 1$ eşitliğidir. Eğer $G^{(n)} = 1$ ama $G^{(n-1)} \neq 1$ ise G grubu n'inci dereceden çözülür olur.* □

Demek ki bir grup n'inci dereceden çözülürse ve $n > 0$ ise, o zaman $1 \neq G^{(n-1)} \lhd G$ normal altgrubu abel olur. Her grubun 1'den farklı normal bir abel altgrubu yoktur ve bu bir ayrıcalık sayılabilir.

Bir grubun çözülür olması için (Ç)'deki A_{i+1} altgruplarının illa G'de normal olmalarına gerek yok, A_i'de normal olmaları yeter. (Ama A_i/A_{i+1} grubunun abel olması koşulu hâlâ daha geçerli.) Bazen gerekli olabilecek bu sonucu kanıtlayalım.

Önsav 15.7. *Eğer G grubunun, her i için A_i/A_{i+1} bölüm grubunun abel olduğu bir*

$$1 = A_n \lhd A_{n-1} \lhd \ldots \lhd A_1 \lhd A_0 = G$$

altgrup dizisi varsa o zaman G çözülür olur ve çözülürlük sınıfı $\leq n$'dir.

Kanıt: $B_i = A_1^{(i-1)}$ olsun. $B_1 = A_1 \lhd G$ olur. $B_{i+1} = B_i'$ olduğundan, Önsav 15.1.iv'e göre tümevarımla her i için $B_i \lhd G$ olur. Ve elbette $B_{i+1} \leq B_i$ olur. $B_i' = B_{i+1}$ olduğundan, B_i/B_{i+1} bir abel grubudur. □

Bir grubun çözülür olduğu şöyle de anlaşılır, özellikle grup sonluysa:

Önsav 15.8. *G bir grup ve $A \lhd G$ olsun.*
i. *Eğer G, n'inci dereceden çözülürse, A ve G/A en fazla n'inci dereceden çözülür olur.*
ii. *Eğer A ve G/A çözülür gruplarsa o zaman G çözülür bir gruptur. Ayrıca G'nin çözülürlük sınıfı, A ve G/A'nın çözülürlük sınıflarının toplamından küçükeşittir.*

iii. *Eğer G, n'inci dereceden çözülürse ve $0 \leq i \leq n$ ise, o zaman $G^{(i)}$ altgrubu $(n-i)$'inci dereceden çözülürdür.*

Kanıt: Birinci önerme tamamen Önsav 15.4'ten çıkar. İkinci önermeyi kanıtlayalım. Diyelim $A^{(i)} = 1$ ve $(G/A)^{(j)} = 1$. Bu son eşitlikten ve Önsav 15.4'ten $G^{(j)} \leq A$ çıkar. Bundan ve Önsav 15.3.v'ten $G^{(i+j)} = (G^{(j)})^{(i)} \leq A^{(i)} = 1$ çıkar. Son önerme Önsav 15.3.v'ten çıkar. İstediğimiz kanıtlanmıştır. □

Notlar ve Örnekler

15.21. *Birbirini normalize eden iki çözülür altgrubun ürettiği altgrup da çözülürdür.*
Kanıt: A ve B birbirini normalize eden iki altgrup olsun. AB grubunun çözülür olduğunu kantlamak istiyoruz. Önsav 15.8.ii'ye göre AB/A grubunun çözülür olduğunu kanıtlamak yeterli. Ama $AB/A \simeq B/(A \cap B)$ (Örnek 10.4.113) ve Önsav 15.8.i'e göre $B/(A \cap B)$ grubu çözülürdür. □

15.22. *Sonlu bir G grubunun bir tane maksimal normal ve çözülür altgrubu vardır. Eğer bu altgruba $R(G)$ dersek, $G/R(G)$ grubunun $\{\overline{1}\}$'den başka çözülür normal altgrubu yoktur.*
Kanıt: İki normal ve çözülür altgrup tarafından üretilmiş bir grubun normal ve çözülür olduğunu kanıtlamak yeterli çünkü o zaman $R(G)$'yi tüm normal çözülür altgruplar tarafından üretilmiş grup olarak almak yeterli. Normallik bariz. Çözülürlük de Örnek 15.21'dan çıkıyor. Son önerme bariz. □
$R(G)$ altgrubuna grubun ***çözülürlük radikali*** adı verilir. Sonsuz gruplarda da $R(G)$, normal ve çözülür altgruplar tarafından üretilen altgrup olarak tanımlanabilir; bu durumda $R(G)$ yerel çözülür olur(yani sonlu sayıda eleman tarafından üretilen altgrupları çözülür olur) ama çözülür olmak zorunda değildir.

Alıştırmalar

15.23. D_{2n} grubunun çözülür olduğunu ve çözülürlük sınıfının en fazla 2 olduğunu gösterin. Bu grup ne zaman abeldir?

15.24. Eğer $n \geq 5$ ise Sym n ve Alt n çözülür değildirler. Öte yandan Sym 4 çözülür bir gruptur. Gösterin.

15.25. $\langle x, y | [x, y] = y^n \rangle$ grubunun çözülür olduğunu kanıtlayın. Eğer $n \neq 0$ ise bu grubun metabel olduğunu kanıtlayın.

15.26. Eğer G_i gruplarının her biri en fazla n'inci dereceden çözülürse, $\prod_I G_i$ ve $\bigoplus_I G_i$ grubunun en fazla n'inci dereceden çözülür olduğunu kanıtlayın.

15.27. Aut$(\mathbb{Z} \times \mathbb{Z})$ çözülür bir grup değildir. (Kanıtı kolay olmayabilir.)

15.28. **(Lineer cebir ve matris halkalarını bilenlere.)** Herhangi bir K cismi üzerine (mesela $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ya da $\mathbb{Z}/p\mathbb{Z}$ olabilir), $i < j$ için (i, j)'inci girdisi 0 olan tersinir (yani çaprazında 0 bulunmayan) matrisler kümesi, matris çarpımı altında bir gruptur ve çözülür bir gruptur.

15.29. Sonlu eleman tarafından üretilmiş çözülür ve burulmalı bir grubun sonlu olduğunu kanıtlayın. İpucu: Alıştırma 15.20.

15.30. Her sonlu sayıda elemanın sonlu altgrup ürettiği gruplara ***yerel sonlu grup*** denir. Bir önceki alıştırmadan hareketle çözülür bir grubun yerel sonlu olması için burulmalı olmasının yeter ve gerek olduğunu gösterin.

15.4 Artan Merkezî Seri

G bir grup olsun. Her $i \leq 0$ için $Z_i(G) = 1$ tanımını yapıp $i \geq 0$ için G'nin ***i'inci merkezini*** tümevarımla şöyle tanımlayalım:

$$Z_{i+1}(G) = \{z \in G : [z, G] \subseteq Z_i(G)\}.$$

Elbette

$$Z_1(G) = Z(G),$$

yani $Z_1(G)$ grubun merkezi olur. Eğer G konunun gelişinden belliyse $Z_i(G)$ yerine bazen Z_i yazacağız.

Tümevarımla $Z_i(G) \lhd G$ olgusunu kanıtlamak zor değildir. Aslında (gene tümevarımla) daha güçlü bir ifade kanıtlanabilir: Her $\varphi : G \longrightarrow H$ homomorfisi için, kolayca görüleceği üzere

$$\varphi(Z_i(G)) \leq Z_i(\varphi(G))$$

olur. Ama eşitliğin doğru olmadığı durumlar olabilir, örneğin $Z_2(G) > Z(G)$ ise ve $\varphi : G \longrightarrow G/Z(G)$ doğal izdüşüm ise, $\varphi(Z_1(G)) = \overline{1} < Z_2(G)/Z(G) = Z(\varphi(G))$ olur. Öte yandan eğer φ birebirse, kolayca görüleceği üzere

$$\varphi(Z_i(G)) = Z_i(\varphi(G))$$

olur. Buradan da (φ'yi $\varphi_g : x \mapsto x^g$ iç otomorfileri olarak alarak) $Z_i(G) \lhd G$ olduğu görülür. Hemen ardından da $Z_i(G) \leq Z_{i+1}(G)$ olduğu ve $G/Z_i(G)$ grubundan sözedebileceğimiz çıkar. Tanımdan hemen, $i \geq 0$ için

$$Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G)$$

eşitliğinin doğru olduğu anlaşılır. Demek ki $Z_{i+1}(G)/Z_i(G)$ bir abel grubudur.

$$1 = Z_0(G) \leq Z_1(G) \leq \ldots \leq Z_i(G) \leq Z_{i+1}(G) \leq \ldots$$

dizisine ***artan merkezî seri*** adı verilir[4]. Serinin ardışık iki terimi bir defa eşitlendi mi ondan sonra hep eşitlenir. Ama seri sürekli de artabilir[5].

Bulduklarımızı yazalım:

Önsav 15.9. *Her i için $Z_{i-1}(G) \leq Z_i(G) \lhd G$ olur. Eğer $\varphi : G \longrightarrow H$ bir grup homomorfisiyse $\varphi(Z_i(G)) \leq Z_i(\varphi(G))$ olur. Homomorfi birebirse eşitlik olur.* □

[4] Aslında bir seriden değil, bir diziden sözetmek gerekir ama gelenek bu yöndedir.

[5] Eğer α bir ordinalse $Z_{\alpha+1}$ tahmin edildiği üzere $Z(G/Z_\alpha(G)) = Z_{\alpha+1}(G)/Z_\alpha(G)$ olacak biçimde ve eğer α bir limit ordinalse $Z_\alpha(G) = \bigcup_{\beta<\alpha} Z_\beta(G)$ olarak tanımlanabilir. Ama bu kavramlara bu kitapta ihtiyacımız olmayacak.

Artan merkezî seriyle azalan merkezî seri arasında bir ilişki vardır:

Önsav 15.10. *Her j ve her $i \geq 0$ için*

$$[G^i, Z_j(G)] \leq Z_{j-i-1}(G) \text{ ve } [G^i, Z_{i+1}(G)] = 1$$

olur.

Kanıt: Birinci önermeyi kanıtlayalım. Eğer $i = 0$ ise sorun yok. Geri kalanı i üzerine tümevarımla kanıtlayacağız. Önermenin i ve her j için doğru olduğunu varsayalım. Önsav 15.5.iii'te normal altgruplar için kanıtlanan

$$[[H, K], L] \leq [[K, L], H][[L, H], K]$$

içindeliğini kullanacağız. Buna göre,

$$\begin{aligned} [G^{i+1}, Z_j] &= [[G^i, G], Z_j] \leq [[G, Z_j], G^i]\,[[Z_j, G^i], G] \\ &\leq [Z_{j-1}, G^i]\,[[Z_j, G^i], G] \leq [Z_{j-1}, G^i]\,[Z_{j-i-1}, G] \\ &\leq [Z_{j-1}, G^i]\,Z_{j-i-2} \leq Z_{j-1-i-1}\,Z_{j-i-2} = Z_{j-(i+1)-1} \end{aligned}$$

olur. Eğer $j = i + 1$ alırsak ikinci önerme bundan hemen çıkar. □

Alıştırmalar

15.31. Her $z \in Z_2(G)$ için $g \mapsto [g, z]$ kuralıyla tanımlanmış $\operatorname{ad} z : G \longrightarrow Z(G)$ fonksiyonunun bir grup homomorfisi olduğunu ve $[g, z]^n = [g, z^n] = [g^n, z]$ eşitliklerini kanıtlayın. Buradan, eğer g ya da z'den biri p-elemansa, $[g, z]$'nin de bir p-eleman olduğunu kanıtlayın. Eğer $p \neq q$ asalları için g ve z elemanlarının biri p-eleman, diğeri q-elemansa $gz = zg$ eşitliğini kanıtlayın. Bu son dediğimiz $Z_n(G)$ altgrubunun tüm elemanları için doğrudur ve yakın gelecekte kanıtlanacaktır. Şimdilik sonucu elemanlardan biri ikinci merkezdeyse kanıtladık.

15.32. $z \in Z_2(G)$ elemanı, bir p asalı ve bir $n \in \mathbb{N}$ doğal sayısı için $z^{p^n} \in Z(G)$ içindeliğini sağlasın. (Yani $\overline{z} \in Z_2(G)/Z(G)$ elemanı bir p-eleman olsun.) Her $g \in G$ için $[g, z]$'nin de bir p-eleman olduğunu kanıtlayın.

15.33. (I. Schur). $G/Z(G)$ grubunun sonlu olduğunu varsayalım. G' altgrubunun sonlu olduğunu göstereceğiz. $|G/Z(G)| = n$ olsun.

a. $G'/(G' \cap Z(G))$ grubunun sonlu olduğunu kanıtlayın. Demek ki istediğimizi kanıtlamak için $G' \cap Z(G)$ grubunun sonlu olduğunu göstermek yetecek.

b. $X = \{[g, h] : g,\, h \in G\}$ kümesinin en fazla n^2 elemanı olduğunu gösterin.

c. $X = \{x_1, \ldots, x_k\}$ olsun. $G' \cap Z(G)$ grubunun her elemanının $m_1, \ldots, m_k \in \mathbb{N}$ için $x_1^{m_1} \cdots x_k^{m_k}$ biçiminde yazılacağını gösterin.

d. Her $g,\, h \in G$,

$$[g, h]^{n+1} = g^{-1}[g, h]^n g[g, h] = g^{-1}[g, h]^{n-1}[g^2, h]^{g^{-1}} g$$

eşitliklerini gösterin.

e. (c) ve (d)'den $G' \cap Z(G)$ grubunun her elemanının X'in en fazla n^3 elemanının çarpımı olarak yazıldığını gösterin. Demek ki $G' \cap Z(G)$ sonlu bir gruptur.

Bunu bir teorem olarak yazalım:

Teorem 15.11 (I. Schur)**.** *$G/Z(G)$ grubu sonluysa G' grubu sonludur.* □

15.34. [R. Baer, bkz. [Ro]]. A ve B, G grubunun birbirini normalleyen iki altgrubu olsun.

$$X = \{[a, b] : a \in A,\ b \in B\}$$

kümesinin sonlu olduğunu varsayalım. $[A, B]$ altgrubunun sonlu olduğunu göstereceğiz. G yerine AB altgrubunu alarak, $G = AB$ eşitliğini varsayabiliriz. Bu varsayımla A ve B, G'nin normal altgrupları olurlar. $U = [A, B] = \langle X \rangle \leq A \cap B$ tanımını yapalım. Elbette $U \lhd G$ olur.

G grubu X kümesi üzerine eşleniklik etkisiyle etkir. X sonlu olduğundan, bu etkinin çekirdeği olan $C_G(X)$ altgrubunun G'deki indeksi sonludur. Elbette $C_G(X) = C_G(U)$ olur (bkz. Alıştırma 7.10), dolayısıyla $C_U(X) = Z(U)$ olur.

$$U/Z(U) = U/C_U(X) = U/(C_G(X) \cap U) \simeq C_G(X)U/C_G(X) \leq G/C_G(X)$$

olduğundan, $[U : Z(U)] \leq [G : C_G(X)] < \infty$ olur ve Örnek 15.33'ten U' altgrubunun sonlu olduğu çıkar. Böylece bütün altgrupların G/U' grubunda imgesini alarak $U' = 1$ varsayımını yapabiliriz. (G grubu yerine G/U' grubunu, A altgrubu yerine A/U' altgrubunu vs. alalım.) Elbette X'in $\{[a, u] : a \in A,\ u \in U\}$ altkümesi sonludur ve, $U' = 1$ olduğundan, elemanları birbiriyle değişir.

Show that $[a, u]^2 = [a, u^2]$. Conclude that $[A, U]$ is finite. Show that, without loss of generality, we may assume that $[A, U] = 1$. Conclude that, without loss of generality U is central in G.

e. Show that X is closed under the squaring map $x \mapsto x^2$. Conclude that $[A, B]$ is finite.
xxxxxxxxxxxxxxxxxxxxxxx

15.5 Sıfırkuvvetli Gruplar

Eğer bir n doğal sayısı için $Z_n(G) = G$ oluyorsa G'ye ***sıfırkuvvetli grup*** ya da ***nilpotent grup*** adı verilir. Eğer n, bu eşitliği sağlayan en küçük doğal sayıysa, G'ye ***n'inci dereceden sıfırkuvvetli grup*** ya da ***n-sıfırkuvvetli grup*** denir. Bu durumda $c(G) = n$ yazacağız ve n'ye G'nin ***sıfırkuvvet derecesi*** adını vereceğiz. Eğer $c(G) = n$ ise, G'ye bazen ***n-sıfırkuvvetli*** diyeceğiz.

Sıfırkuvvetli grupların çözülür olduğu Önsav 15.7'den hemen çıkıyor, ne de olsa Z_i/Z_{i+1} grupları abel gruplarıdır. Hatta aynı önsavdan, eğer sıfırkuvvet edercesi n ise, çözülürlük derceesinin $\leq n$ olduğu çıkıyor. Ama birazdan bundan çok daha iyisini yapacağız (bkz. Teorem 15.15).

Sıfırkuvvetlik sınıfı üzerine tümevarım yapılıp kimileyin abel grupları için doğru olan olgular sıfırkuvvetli gruplar için genelleştirilebileceğinden önemli ve yararlı bir kavramdır.

Önsav 15.12. *i bir doğal sayı olsun. G'nin sıfırkuvvetli olması için yeter ve gerek koşul G/Z_i grubunun sıfırkuvvetli olmasıdır. Eğer $Z_i \neq G$ ise, $c(G) = c(G/Z_i) + i$ olur.*

Kanıt: Tanıma bakılırsa $c(G/Z_i) = c(G) - i$ olduğu hemen anlaşılır. □

Sıfırkuvvetli olmanın bir başka eşdeğer tanımı daha vardır. Merkezî serilerden biri artan, biri azalandır. $(G^i)_i$ azalır, $(Z_i(G))_i$ artar. Eğer G sıfırkuvvetliyse, $Z_i(G)$ altgruplarının G grubuna ulaşma hızı, G^i altgruplarının 1 altgrubuna ulaşma hızına eşittir. Şimdi bunu kanıtlacağız.

Teorem 15.13. **i.** *Eğer $G^n = 1$ ise, her i için $G^{n-i} \leq Z_i(G)$ olur. Dolayısıyla $Z_n(G) = G$ olur.*

ii. *Eğer $Z_n(G) = G$ ise $G^i \leq Z_{n-i}(G)$ olur. Dolayısıyla $G^n = 1$ olur.*

iii. *Eğer $G^n = 1$ ise G en fazla n'inci dereceden sıfırkuvvetlidir. Eğer n, bu eşitliğini sağlayan en küçük doğal sayıysa G tam n'inci dereceden sıfırkuvvetlidir.*

Kanıt: i. Eğer $i = 0$ ise, istediğimiz içindelik hipotezden çıkar. Önermeyi i için kabul edip $i+1$ için kanıtlayalım. $[G^{(n+1)-i}, G] = [G^{n+1-i}, G] = G^{n-i} \leq Z_i(G)$ olduğundan, tanıma göre $G^{(n+1)-i} \leq Z_{i+1}(G)$ olur.

ii. Eğer $i = 0$ ise, istediğimiz içindelik hipotezden çıkar. Önermeyi i için kabul edip $i+1$ için kanıtlayalım: $G_{i+1} = [G^i, G] \leq [Z_{n-i}(G), G] = Z_{n-i-1}(G) = Z_{n-(i+1)}(G)$.

iii. Yukarıda kanıtlananlardan çıkar. □

Sonuç 15.14. *$Z_i(G)$ en fazla i'inci dereceden sıfırkuvvetlidir.*

Kanıt: $[G, Z_j(G)] \leq Z_{j-1}(G)$ olduğundan, $[Z_i(G), Z_j(G)] \leq Z_{j-1}(G)$ olur. Bunu tekrar tekrar kullanarak $Z_i(G)^i = 1$ buluruz. □

Teorem 15.15. *Sıfırkuvvetli gruplar çözülür gruplardır. Sıfırkuvvet derecesi n ise, grubun çözülürlük derecesi $n \leq 2^m - 1$ eşitsizliğini sağlayan en küçük m doğal sayısından küçükeşittir, yani çözülürlük derecesi $\leq \lceil \log_2(n+1) \rceil$ olur*[6]*.*

Kanıt: Önsav 15.5.v'i kullanacağız: $G^{(m)} \leq G^{2^m-1} \leq G^n = 1$. □

Öte yandan çözülür gruplar sıfırkuvvetli olmak zorunda değildirler, hatta çözülür grupların merkezleri 1 olabilir; Örnek 5.44'teki grup böyle bir gruptur.

Asal bir p sayısı için sonlu p-gruplarının sıfırkuvvetli olması çok önemlidir, bir sonraki bölümde bunu kullanacağız:

Teorem 15.16. *Asal bir p sayısı için sonlu p-grupları sıfırkuvvetlidir. Ayrıca grubun eleman sayısı $n \geq 2$ için p^n ise sıfırkuvvet sınıfı en fazla $n-1$'dir*

Kanıt: Grubun eleman sayısı üzerine tümevarım yapacağız. Eğer grubun p elemanı varsa, grup abel grubudur, dolayısıyla 1'inci dereceden sıfırkuvvetlidir. En genel durumda: Gruba G adını verirsek, Teorem 8.10'a ya da 14.6'ya göre $Z(G) \neq 1$ olur. $G/Z(G)$ tümevarımla sıfırkuvvetli olduğundan, Önsav 15.12'e göre G sıfırkuvvetlidir.

Şimdi $|G| = p^n$ varsayımını yapalım. Eğer $n = 2$ ise grubun abel grubu olduğunu, dolayısıyla birinci sınıf sıfırkuvvetli olduğunu biliyoruz. Şimdi $n > 2$ varsayımını yapalım. O zaman $|G/Z(G)| \leq p^{n-1}$ olur. Tümevarımla, $G/Z(G)$ grubunun sıfırkuvvet derecesi en fazla $n-2$'dir. Önsav 15.12'ye göre G'nın sıfırkuvvet derecesi en fazla $n-1$'dir. □

Notlar ve Örnekler

[6] $\lceil x \rceil$ sayısı x'ten büyükeşit en küçük tamsayıdır.

15.35. Bu notta, asal bir $p > 2$ için p^3 elemanlı grupları sınıflandıracağız. Eğer grup abelse üç seçeneğimiz olduğunu biliyoruz:

$$(\mathbb{Z}/p\mathbb{Z})^3,\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z},\ \mathbb{Z}/p^3\mathbb{Z}.$$

Bundan böyle p^3 elemanlı G grubunun abel olmadığını varsayalım. Teorem 15.16'ya göre G'nin 2-sıfırkuvvetli olduğunu biliyoruz. Ama bunu ve çok daha fazlasını şöyle de kanıtlayabiliriz: $1 < Z(G) < G$ olduğunu biliyoruz. Demek ki ya $|Z(G)| = p$ ya da $|Z(G)| = p^2$. Ama ikinci şıkta $|G/Z(G)| = p$ ve dolayısıyla $G/Z(G)$ döngüsel ve o zaman da G abel grubu olur (Örnek 9.66), çelişki. Demek ki $|Z(G)| = p$ ve derecesi p olan bir z elemanı için $Z(G) = \langle z \rangle$. Burada z merkezin 1'den farklı herhangi bir elemanı olabilir, dolayısıyla her an için z'yi değiştirebiliriz. Ayrıca $|G/Z(G)| = p^2$ olduğundan, $G/Z(G)$ bir abel grubudur (Sonuç 8.11), dolayısıyla $G' \leq Z(G)$ olur. $G' \neq 1$ olduğundan $G' = Z(G)$ olmalı. Aynı zamanda, p^2 elemanlı bir grup olan $G/Z(G)$ döngüsel olamayacağından (aksi halde G bir abel grubu olurdu, Örnek 9.66), $G/Z(G) \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ olur. Grubun yapısı bayağı ortaya çıktı ama daha fazlasını bulacağız. Diyelim $G/Z(G) = \langle \overline{x}, \overline{y} \rangle$. O zaman

$$G = \langle x, y, z \rangle = \{x^a y^b z^c : a, b, c \in \{0, 1, \ldots, p-1\}\}$$

olur. (x ve y seçimimizi de değiştirebiliriz.) Daha çarpım tablosunu, yani

$$(x^a y^b z^c)(x^{a'} y^{b'} z^{c'})$$

çarpımını bulmamız lazım. Bu çarpımı

$$(x^a y^b z^c)(x^{a'} y^{b'} z^{c'}) = x^{a''} y^{b''} z^{c''}$$

olarak yazabilmemiz lazım. $z \in Z(G)$ olduğundan

$$(x^a y^b z^c)(x^{a'} y^{b'} z^{c'}) = x^a y^b x^{a'} y^{b'} z^{c+c'}$$

olur. Demek ki, önemli olan $y^b x^{a'}$ elemanını

$$y^b x^{a'} = x^{a_1} y^{b_1} z^{c_1}$$

olarak yazabilmek; bir de $\deg x$ ve $\deg y$ derecelerini bulmak gerekiyor. Bu derecelerin ya p ya da p^2 olmaları gerektiğini biliyoruz. Ama her durumda $x^p,\ y^p \in Z(G)$ olmalı. Her ikisinin de derecesinin p^2 olduğunu varsayalım. O zaman bir $i = 1, \ldots, p-1$ için $y^p = (x^p)^i = x^{ip}$ olur. Alıştırma 1.23'te her grupta her a ve b elemanı ve her $n \in \mathbb{N}$ için

$$(ab)^n = a^n b^n [b, a^{n-1}]^{b^{n-1}} [b, a^{n-2}]^{b^{n-2}} \cdots [b, a]^b$$

eşitliğini kanıtlamıştık. Örneğimizde $[b, a] \in G' = Z(G)$ olduğundan, eşitlik,

$$(ab)^n = a^n b^n [b, a^{n-1}][b, a^{n-2}] \cdots [b, a]$$

eşitliğine dönüşür. Grubun sıfırkuvvet derecesi 2 olduğundan, bundan

$$(ab)^n = a^n b^n [b, a^{1+2+\cdots+(n-1)}] = a^n b^n [b, a]^{n(n-1)/2}$$

elde ederiz. Şimdi $n = p$ alalım ve $p > 2$ varsayımını yapalım. O zaman, $[b, a] \in Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$ olduğundan

$$(ab)^p = a^p b^p = a^p b^p [b, a]^{p(p-1)/2} = a^p b^p$$

olur. Son olarak, a yerine x^{-i}, b yerine y alalım:

$$(x^{-i} y)^p = x^{-ip} y^p = 1$$

elde ederiz. Demek ki y yerine $x^{-i}y$ elemanını alırsak, $y^p = 1$ varsayımını yapabiliriz. Böylece, eğer $p > 2$ ise en azından y'yi derecesi p olan bir eleman olarak alabileceğimizi gösterdik. Bundan böyle $\deg y = p$ varsayımını yapabileceğiz.
Eğer $\deg x = p^2$ ise, $Z(G) = G' < \langle x\rangle \lhd G$ olur. Demek ki,

$$G = \langle x\rangle \rtimes \langle y\rangle \simeq \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}.$$

Örnek 12.24'te x ve y'den birinin derecesinin p^2, diğerinin derecesinin p olduğu örnekler vermiştik. Bunların bu tür tüm grupları verdiğini göstermek zor değil.
Bundan böyle $\deg x = p$ varsayımını yapalım. $z \in Z(G) \setminus \{1\}$ elemanını $[x, y]$ elemanına eşit seçebiliriz. O zaman

$$xy = yx[x, y] = yxz$$

olur ve böylece grubun yapısı tamamen ortaya çıkar:

$$G = \langle x, y, z \,|\, x^p = y^p = z^p = [x, z] = [y, z] = 1,\ [x, y] = z\rangle.$$

Bulduğumuz gruba ***Heisenberg p-grubu*** adı verilir.

Heisenberg grubu resmi gelecek

Eksponenti p'dir (çünkü $p > 2$ varsayımını yaptık, $p = 2$ ise Heisenberg grubunun eksponenti 4'tür; zaten 2 olsaydı G abel grubu olurdu). Matrisleri bilenler için Heisenberg grubu şöyle tasvir edilebilir:

$$\left\{ x^i y^j z^k = \begin{pmatrix} 1 & i & k \\ 0 & 1 & j \\ 0 & 0 & 1 \end{pmatrix} : i,\ j,\ k \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

Alıştırmalar

15.36. Örnek 5.44'teki grubun ikinci dereceden çözülür olduğunu, ama merkezinin 1 olduğunu, dolayısıyla sıfırkuvvetli olamayacağını kanıtlayın.

15.37. Eğer n bir tek sayıysa, D_{2n} grubunun merkezinin 1 olduğunu dolayısıyla sıfırkuvvetli olmadığını kanıtlayın. Bu grubun ikinci dereceden çözülür olduğunu daha önce görmüştük.

15.38. Eğer $n > 2$ bir çift sayıysa, D_{2n} grubunun merkezinin 2 elemanlı olduğunu kanıtlayın. $D_{2n}/Z(D_{2n}) \simeq D_n$ olduğunu kanıtlayın. $n = 2$ ise $D_{2n} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ olur.

15.39. Önceki iki alıştırmadan hareketle, eğer n, 2'nin bir kuvveti değilse D_{2n} grubunun sıfırkuvvetli olmadığını kanıtlayın. (Bkz. Teorem 15.16.) Eğer bir $k > 1$ tek sayısı için $n = 2^m k$ ise, her $i \le k$ için $Z_i(D_{2n}) \simeq \mathbb{Z}/2^i\mathbb{Z}$ olduğunu, ama $i \ge m$ için $Z_{i+1}(D_{2n}) = Z_i(D_{2n})$ olduğunu kanıtlayın.

15.40. $\langle x, y \mid [[x, y], x], [[x, y], y]\rangle$ grubunun 2-sıfırkuvvetli olduğunu kanıtlayın.

15.41. $G = \langle a, b \mid a^{12}, b^2, baba^5\rangle$ grubunun sıfırkuvvetli olduğunu gösterin. İpucu: $G \simeq \langle a\rangle \rtimes \langle b\rangle$ ve eğer $u = a^3$ ve $v = a^4$ ise $\langle a\rangle \simeq \langle u\rangle \oplus \langle v\rangle$ olur. Ayrıca $u^b = u^{-1}$, $v^b = v$. Şimdi $G \simeq (\langle u\rangle \rtimes \langle b\rangle) \times \langle v\rangle \simeq D_8 \times \mathbb{Z}/3\mathbb{Z}$ olduğunu gösterin.

15.42. Eğer G_i gruplarının her biri en fazla n'inci dereceden sıfırkuvvetliyse, $\prod_I G_i$ ve $\bigoplus_I G_i$ grubunun en fazla n'inci dereceden sıfırkuvvetli olduğunu kanıtlayın.

15.43. 2-sıfırkuvvetli bir grupta $(xy)^n = x^n y^n [y, x]^{n(n-1)/2}$ olduğunu kanıtlayın.

15.44. Teorem 15.16 sonsuz p-grupları için doğru değildir, örneğin eğer $\sigma = (1\ 2 \ldots p) \in \operatorname{Sym} p$ ise, Örnek 12.22'de tanımlanan $G = \mathbb{Z}^p_{p^\infty} \rtimes \langle\sigma\rangle$ bir p-gruptur ancak sıfırkuvvetli değildir. Kanıtlayın.

15.45. **(Lineer cebir ve matris halkalarını bilenlere.)** Herhangi bir K cismi üzerine (mesela $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ya da $\mathbb{Z}/p\mathbb{Z}$ olabilir), $i < j$ için (i, j)'inci girdisi 0 ve (i, i)'inci girdisi 1 olan matrisler kümesi, matris çarpımı altında bir gruptur ve sıfırkuvvetli bir gruptur.

15.46. **(Lineer cebir ve matris halkalarını bilenlere.)** Herhangi bir K cismi üzerine (mesela $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ya da $\mathbb{Z}/p\mathbb{Z}$ olabilir), $i < j$ için (i, j)'inci girdisi 0 olan tersinir (yani çaprazında 0 bulunmayan) matrisler kümesi, matris çarpımı altında bir gruptur. Bu grup çözülürdür (bkz. Alıştırma 15.28.) ama eğer $|K| > 2$ ise sıfırkuvvetli değildir.

15.47. p bir asal olsun. Sıfırkuvvetli bir p-grubun yerel sonlu olduğunu kanıtlayın. İpucu: Alıştırma 15.30.

Notlar ve Örnekler

15.48. *Eğer sıfırkuvvetli bir grubun* 1*'den farklı bir* p*-elemanı varsa* (p *bundan böyle hep bir asal olacak*)*, o zaman grubun merkezinde* 1*'den farklı bir* p*-eleman vardır.*

Kanıt: Sonucu sıfırkuvvet derecesi üzerine tümevarımla kanıtlayalım. Gruba G diyelim. Grup abelse sorun yok. Bundan böyle grubun abel olmadığını varsayalım. Diyelim $Z(G)$'de 1'den farklı bir p-eleman yok. O zaman $G/Z(G)$ grubunda 1'den farklı bir p-eleman vardır. Önsav 15.12'ye göre, tümevarımla, $Z(G/Z(G)) = Z_2(G)/Z(G)$ grubunda 1'den farklı bir p-eleman vardır, diyelim $\overline{z}$. Demek ki $z \in Z_2(G) \setminus Z(G)$ ve bir $n > 0$ için $z^{p^n} \in Z(G)$ olur. z merkezde olmadığından, $C_G(z) < G$ olur. Bir $g \in G \setminus C_G(z)$ seçelim. O zaman Alıştırma 15.32'ye göre, $1 \neq [g, z] \in Z(G)$ bir p-elemandır. □

15.49. *G sıfırkuvvetli bir grup olsun. $G/Z(G)$'de* 1*'den farklı bir p-elemanı varsa, o zaman $Z(G) \cap G'$ altgrubunda* 1*'den farklı bir p-eleman vardır.*

Kanıt: Örnek 15.48'e göre $Z(G/Z(G)) = Z_2(G)/Z(G)$ grubunda 1'den farklı bir p-eleman vardır. $z \in Z_2(G) \setminus Z(G)$ elemanı $z^p \in Z(G)$ içindeliğini sağlasın. Eğer $g \in G \setminus C_G(z)$ ise, $1 \neq [g, z] \in Z(G) \cap G'$ olur. Ayrıca $[g, z]^p = [g, z^p] = 1$ olur. □

15.50. *G sıfırkuvvetli bir grup ve $i > 0$ olsun. Eğer $G/Z_i(G)$'de* 1*'den farklı bir p-elemanı varsa, o zaman $Z(G) \cap G'$ altgrubunda* 1*'den farklı bir p-eleman vardır.*

Kanıt: i üzerine tümevarımla kanıtlayacağız. $i = 1$ durumu Örnek 15.49'da halledildi.

$$G/Z_i \simeq (G/Z_{i-1})/(Z_i/Z_{i-1}) = (G/Z_{i-1})/Z(G/Z_{i-1})$$

olduğundan, $(G/Z_{i-1})/Z(G/Z_{i-1})$ grubunda 1'den farklı bir p-eleman vardır. Örnek 15.48'e göre G/Z_{i-1} grubunda 1'den farklı bir p-eleman vardır. Tümevarımla istenen sonuç kanıtlanır. □

15.51. *G sıfırkuvvetli bir group ve $D \leq G$, p-bölünür bir altgrup olsun. O zaman D'nin elemanları G'nin tüm p-elemanlarıyla değişir. Hatta D'nin elemanları $G/Z(G)$ grubunun tüm p-elemanlarıyla değişir.*

Kanıt: İkinci önermeyi kanıtlamak yeterli. $g \in G$ elemanı bir $n \in \mathbb{N}$ için $g^{p^n} \in Z(G)$ içindeliğini sağlasın. Sıfırkuvvet derecesi üzerine tümevarımla $\overline{G} = G/Z(G)$ grubunda $[\overline{D}, \overline{g}] = \overline{1}$, yani $[D, g] \leq Z(G)$ olur. Rastgele bir $d \in D$ alalım ve $e^{p^n} = d$ eşitliğini sağlayan bir $e \in D$ elemanı bulalım. Örnek 15.9'a göre $[d, g] = [e^{p^n}, g] = [e, g^{p^n}] = 1$ olur. □

15.52. *p-bölünür ve sıfırkuvvetli bir p-grup abel grubu olmak zorundadır.*

Kanıt: Bir öncekinden çıkar. □

15.53. Sıfırkuvvetli grupların şu özelliği de çok önemlidir:

Teorem 15.17. Normalleme Koşulu. *Eğer G sıfırkuvvetli bir grupsa ve $H < G$ ise $H < N_G(H)$ olur.*

Kanıt: Kanıtı grubun sıfırkuvvetlilik sınıfı üzerine tümevarımla yapacağız. Grup abel olduğunda, sorun yok. Bundan böyle grubun abel olmadığını varsayalım. Eğer $Z(G) \not\leq H$ ise, $H < HZ(G) \leq N_G(H)$ olduğundan, önermenin doğruluğu bariz. Bundan böyle $Z(G) \leq H$ varsayımını yapalım. Önsav 15.12'ye göre $c(G/Z(G)) = c(G) - 1 < c(G)$ olduğundan, eğer $\overline{G} = G/Z(G)$ ve $\overline{H} = H/Z(G) < \overline{G}$ ise, tümevarımla, $H/Z(G) = \overline{H} <$

$N_{\overline{G}}(\overline{H})$ elde ederiz. Ama Örnek 11.1'e göre $N_{\overline{G}}(\overline{H}) = N_G(H)/Z(G)$. Demek ki

$$H/Z(G) < N_G(H)/Z(G),$$

dolayısıyla $H < N_G(H)$. □

İkinci Kanıt: Elbette $Z(G) \leq N_G(H)$ olur. $H_0 = H$ ve $H_{i+1} = N_G(H_i)$ tanımlarını yapalım. Tümevarımla $Z_i(G) \leq H_i$ olduğunu kanıtlamak zor değil: $[Z_{i+1}(G), H_i] \leq Z_i(G) \leq H_i$ olduğundan, bundan kolaylıkla $Z_{i+1}(G)$'nin H_i'yi normalleştirdiği, yani $Z_{i+1}(G) \leq H_{i+1}$ çıkar. Dolayısıyla $H_n = G$ olur. Buradan da $N_G(H) < H$ çıkar (aksi halde normalleyicilerle G'ye kadar çıkamazdık). □

Üçüncü Kanıt: Öyle bir j vardır ki $G^{j+1} \leq H$ ama $G^j \not\leq H$. Elbette $H/G^{j+1} \lhd G^j/G^{j+1}$ olur, çünkü G^j/G^{j+1} bir abel grubudur. Teorem 11.1'e göre $H \lhd G^j$ olmalı. Bundan da $H \lhd HG^j$ çıkar. Ama $H < HG^j$ olduğundan, istediğimiz kanıtlanmıştır. □

15.54. *Sıfırkuvvetli bir G grubunun maksimal bir altgrubu normaldir ve indeksi bir asaldır. Dolayısıyla maksimal altgrup G' altgrubunu içermek zorundadır.* (Eğer maksimal bir altgrup varsa tabii; olmayabilir de.)

Kanıt: Grup G, maksimal altgrup da M olsun. $M < N_G(M)$ olduğundan, $N_G(M) = G$, yani $M \lhd G$ olur. Demek ki M ile G arasında başka bir altgrup yoktur, yani G/M'nin sadece iki altgrubu vardır. Bu da bir p asalı için $G/M \simeq \mathbb{Z}/p\mathbb{Z}$ demektir. G/M abel grubu olduğundan, $G' \leq M$ olur. □

15.55. Aşağıdaki teoremin iki farklı kanıtını sunacağız. İlk kanıtımız (eğer grup sonsuzsa) Zorn Önsavı'nı kullanacak ve standart argüman tiplerinden şaşmayacak. İkinci kanıtımız Zorn Önsavı'nı kullanmayacak.

Teorem 15.18. *Eğer G sıfırkuvvetli bir grupsa ve p bir asalsa, G'nin p-elemanları (mecburen karakteristik) bir altgrup oluşturur. Dolayısıyla sıfırkuvvetli ve burulmalı bir grup, asal p sayıları için maksimal p-altgruplarının direkt toplamıdır.*

Birinci Kanıt: Bunun bir kanıtı şöyle yapılabilir: Zorn Önsavı'nı kullanarak G'nin maksimal bir p altgrubunu bulabiliriz. (Eğer grup sonluysa maksimal p altgrubu bulmak için Zorn Önsavı'na gerek yok.) Bu p-altgruba P adını verelim. Eğer P'nin G-normal olduğunu kanıtlarsak, Teorem 12.7'ye göre istediğimiz kanıtlanmış olur. Diyelim P, G-normal değil. O zaman Teorem 15.17'ye göre, $P \leq N_G(P) < N_G(N_G(P))$ olur. Teorem 10.12'e göre P, $N_G(P)$ altgrubunun p-elemanlarının kümesidir, dolayısıyla $N_G(P)$'nin bir otomorfisi altında değişmez, yani $N_G(P)$'nin karakteristik altgrubudur. Ama eğer $g \in N_G(N_G(P))$ ise, $x \mapsto x^g$ fonksiyonu $N_G(P)$'nin bir otomorfisidir, dolayısıyla $P^g = P$ ve $g \in N_G(P)$ olur; buradan da $N_G(N_G(P)) = N_G(P)$ çıkar, çelişki. Birinci önerme kanıtlanmıştır. İkinci önerme bundan ve Teorem 4.10'dan çıkar. □

Yukarıdaki teoremi kanıtlamak için maksimal p-altgrupların varlığına ihtiyacımız vardı ve bu altgrupların varlığını kanıtlamnak için Zorn Önsavı'nı kullandık. Ama kanıtın sonunda bu maksimal p-altgruptan tek bir tane olduğunu gördük (p-elemanlar kümesi). Dolayısıyla bu önsav Zorn Önsavı kullanılmadan da kanıtlanabilmeli, çünkü varlığı Zorn Önsavı'yla kanıtlanan bir nesneden bir tane olmamalı, hatta ne olduğu anlaşılamamalı bile; oysa biz maksimal p-altgrubun p-elemanlar kümesi olduğunu kanıtladık.

Şimdi aynı teoremi Zorn Önsavı'nı kullanmadan kanıtlamaya koyulacağız.

İkinci Kanıt: Bu sefer Zorn Önsavı'nı kullanmayacağız. P, G'nin p-elemanlarından oluşan altküme olsun. Eğer G bir abel grubuysa, P elbette bir altgruptur. Gerisini grubun sıfırkuvvet derecesine göre tümevarımla kanıtlayacağız. Tümevarımla $P_1 = P \cap G' \leq G$ olur. Elbette $P \cap G' \lhd G$, hatta bu altgrup G'de karakteristiktir. Şimdi P_1'in sıfırkuvvet sınıfı üzerinden tümevarım yapacağız. Önce $P_1 = 1$ durumunu, yani $P \cap G' = 1$ durumunu ele alalım. P'nin merkezî olduğunu göstereceğiz, bu da istediğimizi kanıtlamış olacak. Örnek 15.49'a göre $G/Z(G)$'de 1'den farklı bir p-eleman yoktur. Demek ki

$P \subseteq Z(G)$. Şimdilik tümevarım adımını yapalım. Elbette $P/Z(P_1)$, $G/Z(P_1)$ grubunun p-elemanlarından oluşan kümedir ve

$$\begin{aligned}(G/Z(P_1))' \cap P/Z(P_1) &= G'Z(P_1)/Z(P_1) \cap P/Z(P_1) = G'/Z(P_1) \cap P/Z(P_1) \\ &= (G' \cap P)/Z(P_1) = P_1/Z(P_1)\end{aligned}$$

olur. Dolayısıyla tümevarım varsayımımızı $G/Z(P_1)$ grubuna uygulayabiliriz: $P/Z(P_1) \leq G/Z(P_1)$ olur. Ama $Z(P_1) \subseteq P$ olduğundan, bundan $P \leq G$ çıkar. Böylece tümevarım adımı da tamamlanmış oldu. □

Sonuç 15.19. *Sıfırkuvvetli bir grupta burulmalı elemanlar bir altgrup oluşturur ve bu altgrup (maksimal) p-altgruplarının direkt toplamıdır.* □

Sonuç 15.20. *p ve q iki farklı asal olsun. Sıfırkuvvetli bir grupta p-elamanların çarpımları ve komütatörleri de p elemanlardır. Ayrıca p-elemanlarla q-elemanlar birbirleriyle değişirler.* □

Sonuç 15.21. *Burulmalı bir sıfırkuvvetli grup maksimal p-altgruplarının direkt toplamıdır, dolayısıyla yerel sonludur.*

Sonuç 15.22. *Sıfırkuvvetli ve burulmalı bir grupta bölünür altgruplar merkezîdir.*

Kanıt: Örnek 15.51'den ve yukarıdaki sonuçlardan çıkar. □

15.56. (Chernikov [Ch1, Ch2]) *G sıfırkuvvetli ve p-bölünür bir grup olsun. O zaman grubun merkezi Z, grubun tüm p-elemanlarını içerir ve p-bölünürdür. $i \geq 1$ için G/Z_i ve Z_{i+1}/Z_i grupları p-bölünürdür ve etkisiz elemandan başka p-elemanları yoktur.*
Kanıt: Örnek 15.51'e göre, grubun p-elemanları merkezîdir. Aynı örneğe göre G/Z grubunun etkisiz elemandan başka p-elemanı yoktur. Buradan Z altgrubunun p-bölünür olduğu çıkar. $G/Z_i(G)$ grupları elbette p-bölünürdür. Biraz önce kanıtladığımız üzere bu grupların merkezi olan Z_{i+1}/Z_i grupları da p-bölünürdür. Ve gene biraz önce kanıtladığımız üzere, $i \geq 0$ için

$$(G/Z_i)/Z(G/Z_i) = (G/Z_i)/(Z_{i+1}/Z_i) \simeq G/Z_{i+1}$$

grubunun etkisiz elemandan başka p-elemanı yoktur. Dolayısıyla, G/Z_{i+1} grubunun bir altgrubu olan Z_{i+1}/Z_i grubunun da etkisiz elemandan başka p-elemanı yoktur. □

15.57. *Eğer $A \leq Z(G)$ ise ve G/A grubu n'inci dereceden sıfırkuvvetliyse, G ya n ya da $(n+1)$'inci dereceden sıfırkuvvetlidir.*
Kanıt: Önsav 15.4'e göre

$$\overline{1} = (G/A)^n = G^n A/A$$

ve dolayısıyla $G^n \leq A \leq Z(G)$ olur. Buradan da $G^{n+1} = [G, G^n] \leq [G, Z(G)] = 1$ çıkar. Teorem 15.13'e göre G en fazla $(n+1)$'inci dereceden sıfırkuvvetlidir. G'nin sıfırkuvvet sınıfının n'den küçük olamayacağını zaten biliyoruz. □

15.58. *G bir grup ve H, $K \leq G$, birbirini normalize eden iki nilpotent altgrup olsun. O zaman HK de nilpotent bir altgruptur.*
Kanıt: G yerine $\langle H, K\rangle$ alarak, H ve K'nın G'de normal olduklarını varsayabiliriz. Eğer G bir abel grubuysa, sonuç bariz. Gerisini G'nin sıfırkuvvet derecesi üzerine tümevarımla yapalım. Tümevarım varsayımına göre

$$\langle HZ(G)/Z(G), KZ(G)/Z(G)\rangle = HKZ(G)/Z(G) \simeq HK/(HK \cap Z(G))$$

nilpotent bir gruptur. $HK \cap Z(G) \leq Z(HK)$ olduğundan, sonuç Örnek 15.57'den çıkar. □

15.59. *Sonlu bir grubun normal sıfırkuvvetli altgruplarının maksimali vardır ve bu altgrup biriciktir.*

Kanıt: Örnek 15.58'e göre tüm normal sıfırkuvvetli altgruplar tarafından üretilmiş altgrup maksimal sıfırkuvvetli normal altgruptur. □

$F(G)$ olarak yazılan bu altgrup ***Fitting altgrubu*** olarak bilinir. Sonlu grup teorisinde çok önemlidir.

15.60. *G sıfırkuvvetli bir grup ve $i \geq 1$ bir doğal sayı olsun. Eğer G/G^i grubu p-bölünürse G/G^{i+1} grubu da p-bölünürdür. Demek ki G/G' grubu p-bölünürse G de p-bölünür.*

Kanıt: $G/G^i \simeq (G/G^{i+1})/(G^i/G^{i+1})$ olduğu için, G yerine G/G^{i+1} grubunu alarak $G^{i+1} = 1$ varsayımını yapabiliriz. O zaman $G^i \leq Z(G)$ ve $G^{i-1} \leq Z_2(G)$ olur. Demek ki G^i bir abel grubu olur. Diyelim G^i grubunun p-bölünür olduğunu kanıtladık. Bir $g \in G$ alalım. Hipoteze göre öyle bir $h \in G$ vardır ki G/G^i grubunda $\overline{g} = \overline{h}^p$ olur, yani $gh^{-p} \in G^i$ olur. Ama G^i'nin p-bölünür olduğunu varsaymıştık. Demek ki bir $k \in G^i \leq Z(G)$ için $gh^{-p} = k^p$ ve dolayısıyla $g = (kh)^p$ olur ve böylece istediğimiz kanıtlanır. Demek ki G^i altgrubunun p-bölünür olduğunu kanıtlamak yeterli. G^i bir abel grubu olduğu için, üreteçlerinin p-bölünür olduğunu kanıtlamalıyız. Demek ki $g \in G$ ve $h \in G^{i-1} \leq Z_2(G)$ için G^i'nin rastgele bir üreteci olan $[g,h]$ elemanının p-bölünür olduğunu kanıtlamalıyız. G/G^i grubunda $\overline{g} = \overline{x}^p$ eşitliğini sağlayan bir $x \in G$ alalım. Bir $y \in G^i \leq Z(G)$ için $gx^{-p} = y$ olur. Bu durumda, Örnek 15.31'e göre, $[g,h] = [x^p y, h] = [x^p, h] = [x,h]^p$ olur. İstediğimiz kanıtlanmıştır. □

15.61. *Sıfırkuvvetli grupların yegâne en büyük p-bölünür altgrupları vardır. Bu altgrup biricik olduğundan normal, hatta karakteristiktir.*

Kanıt: Gruba G diyelim. $\mathcal{D}$, G'nin p-bölünür altgruplarından oluşan küme olsun. $\mathcal{D}$'nin elemanları tarafından üretilen altgrup da D olsun. Örnek 15.60'a göre, D/D' grubunun p-bölünür olduğunu kanıtlamak yeterli. Kolayca gösterilebileceği üzere, D/D' abel grubu, $\{HD'/D' : H \in \mathcal{D}\}$ kümesinin elemanları tarafından üretilmiştir (bkz. Alıştırma 10.34). Ama bu kümenin elemanları D/D' grubunun p-bölünür altgruplarıdır, dolayısıyla D/D' grubu p-bölünürdür. □

15.62. *G sıfırkuvvetli bir grup olsun. Eğer bir $D \lhd G$ için, D ve G/D grupları p-bölünürse, G grubu da p-bölünür.*

Kanıt: Örnek 15.60'a göre, G/G' grubunun p-bölünür olduğunu kanıtlamak yeterli.
$(G/D)/(G/D)' = (G/D)/(G'D/D) \simeq G/G'D$ grubunun p-bölünür olduğunu biliyoruz. Ayrıca D/D' grubu p-bölünür olduğundan, $(D/D')/((G' \cap D)/D') \simeq D/(G' \cap D)$ grubunun p-bölünür olduğunu biliyoruz. Ama $G'D/G' \simeq D/(G' \cap D)$ olduğundan, bundan $G'D/G'$ grubu da p-bölünür olduğu çıkar.
$G/G'D$ ve $G'D/G'$ gruplarının p-bölünür olduğunu kanıtladık. G/G' bir abel grubu olduğundan, bundan kolaylıkla G/G' grubunun p-bölünür olduğu çıkar.

15.63. *G, sıfırkuvvet derecesi $n \geq 2$ olan bir grup olsun. Her $g \in G$ için $\langle G', g\rangle$ altgrubunun sıfırkuvvet derecesi en fazla $n-1$'dir.*

Kanıt: Eğer $n = 2$ ise, o zaman $G' \leq Z(G)$, dolayısıyla $\langle G', g\rangle \leq \langle Z(G), g\rangle$ olur. Ama $\langle Z(G), g\rangle$ elbette bir abel grubudur. Demek ki $\langle G', g\rangle$ grubu da abeldir, yani en fazla 1'inci dereceden sıfırkuvvetlidir. Şimdi $n > 2$ durumunu tümevarımla ele alalım. $H = \langle G', g\rangle$ olsun. $G/Z(G)$ grubu $(n-1)$'inci dereceden sıfırkuvvetlidir. Ayrıca $(G/Z(G))' = G'Z(G)/(G)$ olduğunu biliyoruz (Önsav 15.4). Böylece, tümevarımla

$$\langle (G/Z(G))', \overline{g}\rangle = \langle G'Z(G)/Z(G), \overline{g}\rangle = \langle G', g\rangle Z(G)/Z(G) = HZ(G)/Z(G)$$

grubunun sıfırkuvvet derecesinin en fazla $n-2$ olduğunu anlamış oluruz. Elbette $Z(G) \leq Z(HZ(G))$ olur. Örnek 15.57'ye göre $HZ(G)$ grubunun sıfırkuvvet derecesi en fazla $n-1$ olur. H bu grubun bir altgrubu olduğundan, onun da sıfırkuvvet derecesi en fazla $n-1$ olur. □

15.64. *G sıfırkuvvetli bir grup olsun. Eğer G/G' döngüsel bir grupsa G de döngüsel bir gruptur.*

Kanıt: G'nin abel olmadığını varsayalım. O zaman sıfırkuvvet derecesi $n \geq 2$ olur. $\overline{g}$

elemanı G/G' grubunun bir üreteci olsun. Demek ki $G = \langle G', g\rangle$ olur. Örnek 15.63'e göre G'nın sıfırkuvvet derecesi $n-1$ olur. Bir çelişki. Demek ki G bir abel grubu ve $G' = 1$. □

15.65. Aşağıdaki teorem de sıfırkuvvetli gruplarda önemlidir. Teorem, sıfırkuvvetli grupların merkezinin her normal altgrupla kesiştiğini, yani merkezin bayağı büyük olduğunu söylüyor.

Teorem 15.23 (Hirsch)**.** *Eğer G sıfırkuvvetliyse ve $1 \neq A \lhd G$ ise, $A \cap Z(G) \neq 1$ olur.*

Kanıt: Sıfırkuvvet derecesi üzerine tümevarım yapacağız. Eğer G bir abel grubuysa önerme bariz. Genel durumu ele alalım. Tümevarımla $AZ(G)/Z(G) \cap Z(G/Z(G)) \neq \overline{1}$, yani $AZ(G)/Z(G) \cap Z_2(G)/Z(G) \neq 1$, yani $Z(G) < AZ(G) \cap Z_2(G)$ (bkz. Alıştırma 9.69), yani $A \cap Z_2(G) \not\leq Z(G)$ (bkz. Alıştırma 9.23). Madem öyle, bir $z \in A \cap Z_2(G) \setminus Z(G)$ elemanı alalım. Bir de z ile değişmeyen bir $g \in G$ elemanı alalım. O zaman $z \in Z_2(G)$ olduğundan, $[z,g] \in Z(G)$ olur ve $z \in A \lhd G$ olduğundan, $[z,g] \in A$ olur. Demek ki $1 \neq [z,g] \in A \cap Z(G)$. □

Bunun sonucu olarak, sıfırkuvvetli grupların minimal normal altgrupları merkezî olmak zorundadır.

Alıştırmalar

15.66. G sıfırkuvvetli bir grup ve $A \leq G$ minimal normalse $A \leq Z(G)$ ve $A \simeq \mathbb{Z}/p\mathbb{Z}$ olduğunu kanıtlayın.

15.67. p bir asal olsun. Eleman sayısı p^n olan bir grubun her $i = 0, 1, \ldots, n$ için p^i elemanlı normal bir altgrubu olduğunu kanıtlayın. Bu normal altgrupların birbirini kapsayacak biçimde seçebileceğimizi kanıtlayın.

15.68. G sıfırkuvvetli bir grup olsun. Bir $N \lhd G$ için $G = G'N$ ise $N = G$ eşitliğini kanıtlayın. İpucu: i üzerine tümevarımla $G^i \leq G^{i+1}N$ içindeliğini kanıtlayın.

15.69. (Dixmier [D], see [Wa, Corollary 3.2]). G sıfırkuvvetli bir grup olsun. $\exp(G/G') = n$ varsayımını yapalım.

a. Her i için $\exp(G^i/G^{i+1}) | n$ olduğunu gösterin.

b. c, grubun sıfırkuvvet derecesiyse, $\exp(G) | n^c$ olduğunu gösterin.

16. Sylow Teoremleri

G sonlu bir grup olsun. Diyelim $|G| = n$. Ayrıca bir p asalı seçelim. G'nin p-altgrupları vardır, mesela 1 altgrubu. Ama G sonlu olduğundan G'nin maksimal p-altgrupları da vardır, yani kendisinden daha büyük bir p-altgrup olmayan p-altgrupları vardır[1]. Tabii eğer p asalı n'yi bölmüyorsa, bu maksimal p-altgrup 1 altgrubu olmak zorundadır; ama tam tersine bölüyorsa, o zaman Cauchy teoremine göre G'nin maksimal p-altgrupları 1'den farklı olurlar.

Norveçli matematikçi (ve aslında bir lise öğretmeni olan) Sylow, G'nin maksimal p-altgrupları hakkında çok önemli sonuçlar bulmuştur. Bu bölüm bu teorem ve uygulamaları hakkında. Birinci bölümde teoremi kanıtlayacağız. İkinci bölümde teoremi kullanarak bazı küçük grupları sınıflandıracağız.

16.1 Sylow Teoremleri

G, n ve p girişteki gibi olsun. Bu altbölümün içerik kazanması açısından p'nin n'yi böldüğünü varsayalım. p'nin n'yi bölen en büyük kuvveti p^k olsun. Diyelim $n = p^k m$. Tabii m sayısı p asalına bölünmez. G'nin maksimal p-altgruplarına ***Sylow p-altgrupları*** adı verilir. Elbette her p-altgrup bir Sylow p-grubunun içindedir.

Sylow p-altgruplarıyla ilgili şu harika önermeler doğrudur.

Teorem 16.1 (Sylow Teoremleri)**.** *G sonlu bir grup, $|G| = n$, p bir asal ve* $\text{obeb}(n, m) = 1$ *olmak üzere, bir $k \in \mathbb{N}$ için $n = p^k m$ olsun.*

i. *G'nin Sylow p-altgruplarının eleman sayısı p^k'dır.*

ii. *Bu altgrupların sayısı s_p ise s_p, m'yi böler ve $s_p \equiv 1 \bmod p$ olur.*

iii. *G'nin Sylow p-altgrupları birbirine eşleniktirler.*

Kanıt: X, G'nin Sylow p-altgrupları kümesi olsun. Kanıt boyunca G'yi ve G'nin altgruplarını, X'in ve X'in altkümeleri üzerine eşleniklik etkisiyle etki-

[1] Her grubun maksimal bir p-altgrubu olduğu Zorn Önsavı kullanılarak kolaylıkla kanıtlanabilir (bkz. Alıştırma 5.29). Ancak sonlu grupların maksimal p-altgrupları olduğunu kanıtlamak için (elbette) Zorn Önsavı'na ihtiyaç yok, ve ayrıca bu bölümde kanıtlayacağımız teoremler sonsuz gruplar için her zaman doğru değil.

yeceğiz, yani Altbölüm 14.1'in yazılımıyla, $g \in G$ ve $P \in X$ için $g \cdot P = P^{g^{-1}}$ olacak.

Sav 1. *Eğer bir Sylow p-altgrubu P bir p-eleman tarafından normalize ediliyorsa, o zaman bu p-eleman Sylow p-altgrubunda olmak zorundadır. Dolayısıyla P grubu $N_G(P)$'nin p-elemanlarından oluşur ve $N_G(P)/P$ grubunun 1'den başka p-elemanı yoktur.*

Sav 1'in Kanıtı: Diyelim Sylow p-altgrubu P, bir p-eleman olan g tarafından normalize ediliyor. O zaman Teorem 10.12'e göre $P\langle g\rangle$ bir p-gruptur. Ama P maksimal bir p-altgrubu. Demek ki $P = P\langle g\rangle$ ve $g \in P$. Birinci önerme kanıtlandı. Son iki önerme birincisinin sonucudur. □

Sav 2. *P, $Q \in X$ ise $P^Q = \{P^q : q \in Q\}$ kümesinin eleman sayısı p'nin bir kuvvetidir. Eğer $P = Q$ ise bu kümenin tek bir elemanı vardır elbette, o da P'dir, ama eğer $P \neq Q$ ise kümenin eleman sayısı p'ye bölünür.*

Sav 2'nin Kanıtı: $\left|P^Q\right| = |Q/N_Q(P)|$ olduğunu biliyoruz (Bkz. Örnek 14.41). Eğer $N_Q(P) = Q$ ise, yani Q, P'yi normalize ediyorsa, bir önceki sava göre $Q \leq P$, yani $Q = P$ olur. Demek ki $Q \neq P$ ise, $N_Q(P) < Q$ olur, yani $\left|P^Q\right| = |Q/N_Q(P)|$ sayısı p'ye bölünür. □

Kanıta devam edelim. P bir Sylow p-altgrubu ve

$$Y = P^G = \{P^g : g \in G\} \subseteq X$$

olsun. Önce P grubunu Y üzerine etkiyelim. Sav 2'ye göre biri dışında tüm P-yörüngelerin eleman sayısı p'ye bölünür ve p'ye bölünmeyen yegâne yörünge P'nin P-yörüngesidir, çünkü tek elemanlıdır. Böylece $|Y| \equiv 1 \bmod p$ çıkar. Şimdi, eğer varsa, $X \setminus Y$'den bir Q elemanı alalım ve Q grubunu Y üzerine etkiyelim. Bu sefer, gene Sav 2'ye göre, tüm Q-yörüngeler p'ye bölünür; dolayısıyla $|Y| \equiv 0 \bmod p$ olur, ki bu da biraz önce bulduğumuzla çelişir. Demek ki $X = Y$ ve $|X| \equiv 1 \bmod p$. (iii) ve (ii)'nin ikinci yarısı kanıtlandı.

Yukarıda kanıtladığımız $X = P^G$ eşitliğinden, $|X| = |G/N_G(P)|$ çıkar. Demek ki $|G/N_G(P)|$ sayısı p'ye asal. Sav 1'den dolayı $|N_G(P)/P|$ de p'ye asal. Demek ki $|G/P| = |G/N_G(P)|\,|N_G(P)/P|$ de p'ye asal. Buradan $|P| = p^k$ çıkar. (i) kanıtlandı.

$m = |G/P| = |G/N_G(P)|\,|N_G(P)/P| = |X||N_G(P)/P|$ eşitliklerinden dolayı $|X|$, m'yi böler. Bu da (ii)'nin ilk yarısını kanıtlar. □

G sonlu bir grup olsun. $\mathrm{Syl}_p G$, G grubunun Sylow p-altgrupları kümesini simgeler. G grubunun $\mathrm{Syl}_p G$ kümesi üzerine eşleniklik etkisi bize bir $G \longrightarrow \mathrm{Sym}\,\mathrm{Syl}_p G$ homomorfizması verir. G grubu $\mathrm{Syl}_p G$ üzerine geçişli etkidiğinden, bu homomorfi oldukça zengindir. Aşağıda bu zenginliğe (oldukça basit) örnekler vereceğiz.

$s_p(G)$, G grubunun Sylow p-altgrubu sayısını temsil edecek, yani $s_p(G) = |\,\mathrm{Syl}_p G|$. Grup belliyse $s_p(G)$ yerine sadece s_p yazacağız. Eğer $s_p = 1$ ise, Sylow teoremine göre grubun Sylow p-altgrubu normaldir.

Notlar ve Örnekler

16.1. $G = \operatorname{Sym} 3$ olsun. $|G| = 3! = 6 = 2 \times 3$ olur.
Önce $p = 2$ durumunu ele alalım. $s_2 \equiv 1 \bmod 2$ ve $s_2|3$ olduğundan s_2 ya 1 ya 3 olur. Nitekim $s_2 = 3$'tür:

$$G_3 = \langle (1\ 2) \rangle,\ G_2 = \langle (1\ 3) \rangle,\ G_1 \langle (2\ 3) \rangle$$

altgrupları Sylow 2-altgruplarıdır. Bu altgruplar Sylow teoreminin de söylediği gibi birbirlerine eşleniktirler: Eğer $g = (1\ 2\ 3)$ ise, $G_3^g = G_2$ ve $G_2^g = G_1$ olur.
Eğer $X = \{G_1, G_2, G_3\}$ ise, G, eşleniklikle X kümesi üzerine etkir: Her $g \in G$ için $\tilde{g}(G_i) = gG_ig^{-1}$ ise, $g \mapsto \tilde{g}$ kuralı bize bir $\tilde{} : G \longrightarrow \operatorname{Sym} X \simeq \operatorname{Sym} 3$ homomorfisini verir. Bu homomorfinin örten olduğunu, dolayısıyla bir izomorfizma olduğunu göstermek zor değil. Bu yaptığımızı şöyle ifade edebiliriz: $\operatorname{Sym} 3$ grubu, $\{1, 2, 3\}$ kümesini bilmese de, yani kendisinin $\operatorname{Sym} 3$ olduğunu bilmese de, $\operatorname{Sym} 3$'e izomorf olduğunu biliyor.
Şimdi $p = 3$ durumuna bakalım. $s_3 \equiv 1 \bmod 3$ ve $s_3|2$ olduğundan $s_3 = 1$ olmalı, yani tek bir Sylow 3-altgrubu olmalı; nitekim,

$$A = \langle (1\ 2\ 3) \rangle = \{\mathrm{Id}_3, (1\ 2\ 3), (1\ 3\ 2)\}$$

altgrubu $\operatorname{Sym} 3$'ün yegâne Sylow 3-altgrubudur. Böylece $\operatorname{Sym} 3 = A \rtimes G_1$ olduğu, dolayısıyla $\operatorname{Sym} 3$'ün çözülür bir grup olduğu anlaşılır.

16.2. $G = \operatorname{Sym} 4$ olsun. Demek ki $|G| = 4! = 24 = 2^3 3$.
Önce $p = 2$ durumunu ele alalım. Bir Sylow 2-altgrubunun $2^3 = 8$ tane elemanı vardır ve $s_2 \equiv 1 \bmod 2$ ve $s_2|3$ olduğundan bunların sayısı ya 1 ya 3'tür. Nitekim $s_2 = 3$'tür. Sylow 2-altgruplarından biri

$$H_2 = \langle (1\ 2),\ (3\ 4) \rangle \rtimes \langle (1\ 3)(2\ 4) \rangle = \langle (1\ 3\ 2\ 4) \rangle \rtimes \langle (1\ 2) \rangle \simeq D_8$$

altgrubudur. Diğerleri

$$H_3 = \langle (1\ 3),\ (2\ 4) \rangle \rtimes \langle (1\ 2)(3\ 4) \rangle$$

ve

$$H_4 = \langle (1\ 4),\ (2\ 3) \rangle \rtimes \langle (1\ 2)(3\ 4) \rangle$$

altgruplarıdır. Bütün bu Sylow 2-altgrupları, G'nin normal bir altgrubu olan

$$A = \{\mathrm{Id}_4,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

altgrubunda kesişirler.
H_1, H_2 ve H_3 altgrupları Sylow teoreminin de söylediği gibi birbirlerine eşleniktirler. Ancak A altgrubu hepsini normalize eder. Bunu şöyle de açıklayabiliriz: Eğer $X = \{H_1, H_2, H_3\}$ ise, G, eşleniklikle X kümesi üzerine etkir: Her $g \in G$ için $\tilde{g}(H_i) = gH_ig^{-1}$ ise, $g \mapsto \tilde{g}$ kuralı bize bir $\tilde{} : G \longrightarrow \operatorname{Sym} X \simeq \operatorname{Sym} 3$ homomorfisini verir. Bu homomorfinin örten olduğu, çekirdeğinin de A olduğu kolaylıkla kontrol edilebilir. Dolayısıyla $G/A \simeq \operatorname{Sym} 3$ olur. Daha da fazlası doğru: Eğer G_4, $G = \operatorname{Sym} 4$ grubunun 4'ü sabitleyen elemanlarından oluşan $\operatorname{Sym} 3$'e izomorf altgrupsa, $G = A \rtimes G_4 \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \operatorname{Sym} 3$ olur, dolayısıyla $G = \operatorname{Sym} 4$ de çözülür bir gruptur.
Şimdi $p = 3$ durumuna bakalım. $s_3 \equiv 1 \bmod 3$ ve $s_3|8$ olduğundan s_3 ya 1 ya 4 olmalı. Nitekim $s_3 = 4$'tür. Sylow 3-altgruplarından biri

$$B_4 = \langle (1\ 2\ 3) \rangle \leq G_4$$

olur. B_1, B_2 ve B_3 altgruplarının ne olduklarını okur anlamıştır.
Eğer $X = \{B_1, B_2, B_3, B_4\}$ ise, G, eşleniklikle X kümesi üzerine etkir: Her $g \in G$ için $\tilde{g}(H_i) = gH_ig^{-1}$ ise, $g \mapsto \tilde{g}$ kuralı bize bir $\tilde{} : G \longrightarrow \operatorname{Sym} X \simeq \operatorname{Sym} 4$ homomorfisini verir. Bu homomorfinin örten olduğu, dolayısıyla birebir, yani bir izomorfi olduğu kolaylıkla kontrol edilebilir. Demek ki $\operatorname{Sym} 4$ grubu da kendisinin $\operatorname{Sym} 4$'e izomorf olduğunun farkında.

16.3. Sıra $\operatorname{Sym} 5$'e geldi, ama bir $\operatorname{Sym} 5$ yerine bir p asalı için $\operatorname{Sym} p$ grubunun Sylow p-altgruplarını sayalım. Sylow p-altgruplarının eleman sayısı p'dir, dolayısıyla döngüseldirler ve 1 dışında elemanlarının derecesi p'dir ve ayrıca iki farklı Sylow p-altgrubu 1'de kesişirler. Bu bilgileri kullanarak s_p'yi hesaplayalım. $\operatorname{Sym} p$'nin derecesi p olan elemanları p uzunluğunda döngülerdir, bunlardan da $(p-1)!$ tane vardır. Bu $(p-1)!$ tane p dereceli elemanın $p-1$ tanesi aynı Sylow p-altgrubundadır. Demek ki

$$s_p = \frac{(p-1)!}{p-1} = (p-2)!$$

Sylow teoreminden dolayı bu sayı $\equiv 1 \bmod p$ olmalıdır. Wilson teoremini kanıtladık:

Sonuç 16.2 (Wilson Teoremi)**.** *Eğer p bir asalsa $(p-2)! \equiv 1 \bmod p$, dolayısıyla $(p-1)! \equiv -1 \bmod p$ olur.*

16.4. Genel olarak $\operatorname{Sym} n$ grubunun bir Sylow p-altgrubunu bulmak çok zor değildir. p bir asal olsun. p'nin $n!$ sayısını bölen en büyük üssü

$$\operatorname{val}_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

sayısıdır; yani $p^{\operatorname{val}_p n!}$ sayısı $n!$ sayısını böler ama $p^{\operatorname{val}_p n!}$ sayısı $n!$ sayısını bölmez. Burada $[x]$, x'in tamkısmı anlamına gelmektedir. Bunun kanıtı kolaydır ve aritmetikle ilgili hemen hemen her kitapta bulunur, mesela [N2]'de. Bu toplam sonlu bir toplamdır elbette.

$\operatorname{Sym} n$'nin bir Sylow p-altgrubu bulma yöntemini bir örnekle gösterelim. $n = 1000$, $p = 3$ olsun. Sylow 3 grubunun eleman sayısını hesaplayalım.

$$\left[\frac{1000}{3}\right] + \left[\frac{1000}{9}\right] + \left[\frac{1000}{27}\right] + \cdots$$

sayısı

$$333 + 111 + 37 + 12 + 4 + 1 = 498$$

olduğundan Sylow 3-altgrubunun 3^{498} tane elemanı vardır. Bu grubu üreten 498 elemanı yazacağız.

Sylow 3-altgrubunun üreteçlerini sıralayacağız. Önce şu üreteçleri alalım:

$$(1\ 2\ 3),\ (4\ 5\ 6),\ (7\ 8\ 9),\ \ldots\ (997\ 998\ 999).$$

Bu elemanlar $H_1 \simeq (\mathbb{Z}/3\mathbb{Z})^{333}$ grubunu üretirler. Ama Sylow 3-altgrubunun çok daha fazla elemanı vardır. Şimdi H_1 grubunun bu üreteçlerini eşleniklik etkisiyle üçer üçer karan şu elemanlara bakalım:

$$(1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9),\ \ldots,\ (991\ 994\ 997)(992\ 995\ 998)(993\ 996\ 999).$$

Bu elemanlardan 111 tane vardır. Bu 111 eleman tarafından üretilen gruba H_2 dersek, $H_2 \simeq (\mathbb{Z}/3\mathbb{Z})^{111}$ olur. H_2, H_1'in üreteçlerini kardığından, H_2, H_1'i normalize eder, dolayısıyla

$$\langle H_1, H_2 \rangle = H_1 \rtimes H_2$$

olur ve bu grup da $\operatorname{Sym} 1000$'in bir 3-altgrubu olur. Böylece $3^{333}3^{111} = 3^{333+111}$ elemanlı bir 3-altgrubu elde etmiş oluruz. Şimdi H_1'in ve H_2'nün üreteçlerini ayrı ayrı karan 3-elemanlar bulacağız. Bunun için H_2'nin ilk üç üretecini yazalım:

$$(1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9),\ (10\ 13\ 16)(11\ 14\ 17)(12\ 15\ 18),\ (19\ 22\ 25)(20\ 23\ 26)(21\ 24\ 27)$$

ve şu elemana bakalım:

$$(1\ 10\ 19)(4\ 13\ 22)(7\ 16\ 25)(2\ 11\ 20)(5\ 14\ 23)(8\ 17\ 26)(3\ 12\ 21)(6\ 15\ 24)(9\ 18\ 27).$$

Bu eleman H_1 ve H_2'nin yukarıda ortaya çıkardığımız üreteçlerini karar. Bunun gibi daha 37 tane vardır. Bu elemanlar tarafından üretilen gruba H_3 diyelim. $H_3 \simeq (\mathbb{Z}/3\mathbb{Z})^{37}$ olur ve $H_1 \rtimes H_3$ altgrubunu normalize eder.

$$\langle H_1, H_2, H_3 \rangle = (H_1 \rtimes H_2) \rtimes H_3$$

olur. Bu grubun tam $3^{333}3^{111}3^{37} = 3^{333+111+37}$ tane elemanı vardır. Okur herhalde devamını kendi getirebilir.

Bu bölümü uzatarak yukarıdaki güzel kanıtın büyüsünü bozmayalım.

16.2 Sylow Teoremlerinin Sonuçları ve Uygulamaları

Bu bölümde p hep bir asal olacak.

Sonuç 16.3. *p ve q iki asal, n bir doğal sayı olsun. Eğer $q \not\equiv 1 \bmod p$ ise $p^n q$ elemanlı bir grupta bir tane Sylow p-altgrubu vardır, dolayısıyla grup çözülürdür.*

Kanıt: Teoreme göre $s_p \equiv 1 \bmod p$ ve $s_p | q$ olur. Demek ki ya $s_p = 1$ ya da $s_p = q$. Hipotez ikinci olasılığı yasaklıyor. Demek ki $s_p = 1$ ve Sylow p-altgrubu normal. Eğer gruba G, Sylow p-altgrubuna da P dersek, $P \lhd G$ ve $|G/P| = q$ olur. Dolayısıyla G/P döngüsel bir gruptur, dolayısıyla abeldir. P ise p-grup olduğundan sıfırkuvvetlidir (Teorem 15.16), dolayısıyla o da çözülürdür (Teorem 15.15). G/P ve P çözülür olduğundan, G de çözülürdür (Önsav 15.8.ii). □

Eğer $p > q$ ise yukarıdaki sonucun hipotezi doğru olur. Ama bu durumda teoremin doğruluğunu Sonuç 10.17'dan da biliyoruz.

Sonuç 16.4. *p ve q iki asal olsun. pq elemanlı bir grup ele alalım. Grup çözülürdür. Eğer $p < q$ ise grubun normal bir Sylow q-altgrubu vardır. Eğer $p < q$ ise ve ayrıca $q \not\equiv 1 \bmod p$ ise grup döngüseldir.*

Kanıt: Eğer $p = q$ ise, p^2 elemanlı bir grubun abel grubu olduğunu biliyoruz. Eğer $p \neq q$ ise ya $p > q$ ya da $q > p$ olur ve sonuç önceki sonuçtan çıkar.

Şimdi ikinci önermeye geçelim. $s_q \equiv 1 \bmod q$ denkliğini sağlayan s_q sayısı p'yi bölmek zorunda olduğundan, $q > p$ varsayımından dolayı, $s_q = 1$ olur. Demek ki Sylow q-altgrubu da normaldir; ayrıca döngüseldir de.

Üçüncü önerme: Sonuç 16.3'e göre (p elemanlı, dolayısıyla döngüsel olan) Sylow p-altgrubu normaldir. Eğer A ve B, G'nin Sylow p ve q-altgruplarıysa, bütün bunlardan $G = A \oplus B \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$ çıkar. □

Sonuç 16.5. *p ve q iki asal olsun. $p^2 q$ elemanlı bir grup çözülürdür. Eğer $p < q$ ve $q \not\equiv 1 \bmod p$ ise $p^2 q$ elemanlı bir grup abel grubudur.*

Kanıt: Gruba G diyelim. Eğer $p = q$ ise, grup bir p-grubu olur, dolayısıyla sıfırkuvvetlidir. Eğer $p > q$ ise Sonuç 16.3'ten dolayı G çözülürdür. Şimdi $q > p$ varsayımını yapalım. Eğer Sylow altgruplarından biri normalse (hatta grubun 1'den farklı normal bir özaltgrubu varsa), istediğimizi elde etmiş oluruz. Bundan böyle Sylow altgruplarının normal olmadıklarını varsayalım. Demek ki $s_q = p$ ya da p^2. Ama $s_q \equiv 1 \bmod q$ ve $q > p$ olduğundan $s_q \neq p$. Demek ki $s_q = p^2$. Sylow q-altgruplarının eleman sayısı q (bir asal) olduğundan, birbirinden farklı iki Sylow q-grubu ancak 1'de kesişebilirler. Demek ki q-eleman sayısı $p^2(q-1) = |G| - p^2$ olur. Böylece G'nin tam p^2 tane p-elemanı olduğu görülür. Sylow p-altgrubunun eleman sayısı p^2 olduğundan, bu p-elemanlar Sylow p-altgrubunu teşkil ederler. Demek ki grubun tek bir Sylow p-altgrubu vardır ve bu Sylow p-altgrubu mecburen normaldir. Birinci önerme kanıtlanmıştır.

Şimdi ikinci önermeyi kanıtlayalım. $s_p | q$ olduğundan $s_p = 1$ ya da q olmalı. Ayrıca $s_p \equiv 1 \bmod q$ olduğundan, $s_p \neq q$ olur. Demek ki $s_p = 1$ ve p^2 elemanlı (dolayısıyla bir abel grubu olan) Sylow p-altgrubu normal.

$s_q | p^2$ olduğundan $s_q = 1, p, p^2$ olur. Ayrıca $s_q \equiv 1 \bmod q$ olmalı. $q > p$ olduğundan, $s_q \neq p$ olmalı. Eğer $s_q = p^2$ ise, q asalı $p^2 - 1 = (p-1)(p+1)$ sayısını böler, dolayısıyla q asalı $p-1$ ve $p+1$ sayılarından birini böler. Birinci şıkkın mümkün olmadığını $q > p$ eşitsizliğinden biliyoruz. Demek ki q asalı $p+1$'i böler; ama $q > p$ olduğundan bundan da $q = p+1$ çıkar, ki bu da $q \neq 1 \bmod p$ koşuluyla çelişir. Demek ki $s_q = 1$ ve q elemanlı (dolayısıyla bir abel grubu olan) Sylow q-altgrubu da normal.

Eğer A ve B, G'nin Sylow p ve q-altgruplarıysa, bütün bunlardan $G = A \oplus B$ çıkar. □

Notlar ve Örnekler

16.5. 15 elemanlı bir grup $\mathbb{Z}/15\mathbb{Z}$ grubuna izomorf olmak zorundadır çünkü Sonuç 16.3'e göre Sylow 3 ve 5-altgrupları normal olmak zorundadır. Kesişimleri 1 olduğundan elemanları birbirleriyle değişirler.

16.6. Aynı nedenden 35 elemanlı bir grup $\mathbb{Z}/35\mathbb{Z}$ grubuna izomorf olmak zorundadır.

16.7. $|G| = 12 = 2^2 \times 3$ ise, bu durum Sonuç 16.5'in kapsamına girmiyor ama gene de üstesinden gelebiliriz. $s_3 \equiv 1 \bmod 3$ ve $s_3 | 4$ olur. Demek ki $s_3 = 1$ ya da $s_3 = 4$. Eğer $s_3 = 4$ ise, her biri 3 elemanlı olan Sylow 3-altgrupları ikişer ikişer 1'de kesişirler ve böylece derecesi 3 olan toplam $4 \times (3-1) = 8$ tane eleman olur. Geri kalan $12 - 8 = 4$ eleman normal bir Sylow 2-altgrubu oluşturmak zorundadır. Demek ki 12 elemanlı bir grupta Sylow altgruplarından biri normal olmak zorundadır.

16.8. $|G| = 28 = 2^2 \times 7$ ise, $s_7 \equiv 1 \bmod 7$ ve $s_7 | 4$ olur. Demek ki $s_7 = 1$ olur.

16.9. $|G| = 2^3 \times 7 = 56$ ise, $s_7 \equiv 1 \bmod 7$ ve $s_7 | 8$ olur. Demek ki $s_7 = 1$ ya da 8 olmalı. Eğer $s_7 = 8$ ise G'nin $8 \times (7-1) = 48$ tane derecesi 7 olan elemanı verdır. Geri kalan 8 eleman normal bir Sylow 2-altgrubu oluşturmak zorunda kalır.

16.10. $|G| = 2^3 \times 5^m$ ise, $s_5 \equiv 1 \bmod 5$ ve $s_5 | 8$ olur. Demek ki $s_5 = 1$ olur.

16.11. $|G| = 2^4 \times 5 = 80$ ise, derecesi 5 olan elemanları sayarak, eğer $s_5 \neq 1$ ise $s_2 = 1$ olduğu gösterilebilir. Öte yandan aynı beceri aynı yöntemle $|G| = 2^4 \times 5^2 = 400$ için gösterilemez. Kanıtlaması oldukça zor bir teorem, $p^n q^m$ eleman sayılı grupların çözülür olduğunu söyler (Burnside teoremi). Kanıtlaması çok çok daha zor bir teorem, eleman

sayısı 2'ye bölünmeyen sonlu grupların çözülür olduğunu söyler (Feit-Thompson teoremi, [FT]).

16.12. Yukarıdaki örnek ve teoremlerde Sylow p-altgruplarından biri hep normal oluyordu ama bu her zaman böyle olmak zorunda değil. Örneğin Örnek 16.2'de ele aldığımız ve çözülür olduğunu kanıtladığımız $\operatorname{Sym} 4$ grubunun eleman sayısı $2^3 \times 3$'tür ama ne Sylow 2-altgrupları ne de Sylow 3-altgrupları normaldir.

16.13. $p \neq 2$ için $\operatorname{Sym} n$'nin Sylow p-altgrupları $\operatorname{Alt} n$'nin içindedir. Hatta $\operatorname{Sym} n$'nin tek elemanlı her altgrubu $\operatorname{Alt} n$'nin bir altgrubudur. Bu dediğimiz elbette Sylow 2-altgrupları için geçerli değildir.

16.14. Döngüsel grupların Sylow p-altgrupları (döngüsel grupların her altgrubu gibi) döngüseldir. Ama bunun tersi doğru değildir: n bir tek sayıysa, D_{2n}'nin her Sylow p-altgrubu döngüseldir ama D_{2n}, bırakın döngüsel olmayı, abel grubu bile değildir.

16.15. $|G| = 30$ olsun. Örnek 14.43'e göre G'nin 15 elemanlı normal bir H altgrubu vardır. Örnek 16.5'e göre H bir abel grubudur ve 3 ve 5-Sylow altgruplarının çarpımıdır. Bu altgruplar H'nin karakteristik altgrupları olduklarından, G'de normaldirler. Demek ki 30 elemanlı gruplarda $s_3 = s_5 = 1$ olur. Daha fazlasını yapabiliriz: Örnek 14.43'e göre $G \simeq (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$. Buradan G'nin aşağıdaki gruplardan birine izomorf olduğu kolaylıkla çıkar:

$$\mathbb{Z}/30\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \times D_{10},\ \mathbb{Z}/5\mathbb{Z} \times D_6,\ D_{30}.$$

16.16. $|G| = 105$ olsun. Önce $s_5 = s_7 = 1$ olduğunu kanıtlayacağız, daha sonra 105 elemanlı grupları sınıflandıracağız. Sylow teoremlerinden hemen,

$$s_3 = 1,\ 7,\ s_5 = 1,\ 21,\ s_7 = 1,\ 15$$

çıkar.

Önce s_5 ya da s_7'nin 1 olduğunu gösterelim. Eğer ikisinden biri 1'e eşit olmasaydı, derecesi 5 olan $21(5-1) = 84$, derecesi 7 olan $15(7-1) = 90$ eleman olurdu ve böylece grubun eleman sayısı 105'i çok aşardı.

$S_p \leq G$, bir Sylow p-altgrup olsun. O zaman, S_5 ya da S_7'den biri normal olduğundan, S_5S_7, G'nin 35 elemanlı bir altgrubu olur. Indeksi 3 olduğundan, Teorem 10.17'ya göre $S_5S_7 \lhd G$ olur. Ama Örnek 16.6'ya göre $S_5S_7 \simeq \mathbb{Z}/35\mathbb{Z}$ olur. Dolayısıyla S_5 ve S_7 bu altgrubun karakteristik altgruplarıdır. Bundan da S_5 ve S_7'nin G'de normal oldukları çıkar. Demek ki,

$$G \simeq (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$$

olur. Grup hakkında daha fazla bilgi elde edebiliriz: $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ altgrubu 15 elemanlı olduğundan bir abel grubudur. Demek ki $\mathbb{Z}/5\mathbb{Z} \leq Z(G)$ olur. Öte yandan $\mathbb{Z}/7\mathbb{Z}$ grubunun derecesi 3 olan iki otomorfisi vardır: elemanları 2 ve 4 ile çarpmak. Demek ki 105 elemanlı en az iki, en fazla üç izomorf olmayan grup vardır. Ama 2 ile ya da 4 ile çarpmanın yol açtığı gruplar izomorfturlar. Demek ki 105 elemanlı sadece 2 grup vardır.

16.17. $p > 2$ bir asal olsun. $2p$ elemanlı bir grubun ya döngüsel ya da D_{2p}'ye izomorf olduğunu kanıtlayın.

Alıştırmalar

16.18. 20 ve 100 elemanlı gruplarda Sylow 5-altgrubunun normal olduğunu kanıtlayın.

16.19. $p \neq q$ iki asal olsun. Eğer $s_p(G) = s_q(G) = 1$ ise Sylow p-altgrubun elemanlarıyla Sylow q-grubunun elemanları değişirler.

16.20. Sonlu bir grubun sıfırkuvvetli olması için her Sylow p-altgrubunun normal olması yeter ve gerek koşuldur. (Bkz. Teorem 15.18.)

16.21. D_{2n}'nin Sylow p-altgruplarının izomorfi tipini ve eleman sayısını bulun.

16.22. $\mathrm{Sym}\,5$ ve $\mathrm{Alt}\,5$ gruplarında $s_3 = 10$ ve $s_5 = 6$ olduğunu kanıtlayın.

16.23. 45 elemanlı grupların abel olduklarını kanıtlayın.

16.24. 99 ve 175 elemanlı grupların abel olduklarını kanıtlayın. (Bkz. Sonuç 16.5.)

16.25. Sonlu bir grupta Sylow p-altgruplarının kesişiminin normal (hatta karakteristik) bir altgrup olduğunu kanıtlayın. Eğer $G = \mathrm{Sym}\,4$ ve $p = 2$ ise bu kesişimi bulun.

16.26. $\mathrm{Sym}\,5$'in 15 ya da 30 elemanlı altgrubu olmadığını kanıtlayın.

Aşağıdaki sonucun sadece kendisi değil, kanıt yöntemi de önemlidir. Benzer kanıt yöntemleri başka kapsamlarda da işe yarayabilir. Zaten bu yüzden "Frattini Teoremi" değil "Frattini argümanı" ya da "akıl yürütmesi" adı verilir.

Sonuç 16.6 (Frattini Akıl Yürütmesi)**.** *G bir grup, $H \lhd G$ ve $P \in \mathrm{Syl}_p H$ olsun. O zaman $G = HN_G(P)$ olur.*

Kanıt: $g \in G$ olsun. $P^g \leq H^g = H$ olur. Demek ki $P^g \in \mathrm{Syl}_p H$. Sylow teoremine göre bir $h \in H$ için $P^g = P^h$, yani $gh^{-1} \in N_G(P)$ olur. Buradan $g \in N_G(P)H$ çıkar. □

Notlar ve Örnekler

16.27. *G sonlu bir grup ve $P \in \mathrm{Syl}_p G$ olsun. Eğer $N_G(P) \leq H \leq G$ ise $N_G(H) = H$ ve $|G/H| \equiv 1 \bmod p$ olur. Bunun özel bir durumu olarak $N_G(N_G(P)) = N_G(P)$ elde ederiz.*
Kanıt: $P \in \mathrm{Syl}_p H$ ve $H \lhd N_G(H)$ olduğundan, Frattini akıl yürütmesine göre (Sonuç 16.6'da G yerine $N_G(H)$ alın), $N_G(H) = HN_{N_G(H)}(P) \leq HN_G(P) = H$ olur. Demek ki $N_G(H) = H$.
$N_G(P) \leq H$ olduğundan, $N_G(P) = N_H(P)$ olur. Sylow teoremine göre,

$$|G/N_G(P)| = s_p(G) \equiv 1 \bmod p$$

olur. Aynı teoremi H'ye uygularsak

$$|H/N_G(P)| = |H/N_H(P)| = s_p(H) \equiv 1 \bmod p$$

buluruz.

$$|G/N_G(P)| = |G/H||H/N_G(P)|$$

olduğundan, basit modüler aritmetik gereği $|G/H| \equiv 1 \bmod p$ buluruz.
Son önerme için $H = N_G(P)$ almak yeterli. □

16.28. *120 elemanlı bir grup basit olamaz.*
Kanıt: G eleman sayısı 120 olan basit bir grup olsun. G'nin 6 tane Sylow 5-altgrubu var. Dolayısıyla G'yi $\mathrm{Sym}\,6$'nın içine gömebiliriz. G'nin normal altgrubu olmadığı için G, $\mathrm{Alt}\,6$'nın içine gömülür. Bundan böyle $G \leq \mathrm{Alt}\,6$ varsayımını yapalım. $P \leq G \leq \mathrm{Alt}\,6$ bir Sylow 5-altgrubu olsun. $|N_G(P)| = 20$ ama basit bir hesapla görülebileceği üzere $|N_{\mathrm{Alt}\,6}(P)| = 10$. Çelişki. Bkz. `https://crazyproject.wordpress.com/2010/07/18/there-are-no-finite-simple-groups-of-even-order-less-than-500-except-for-the-orders-2-60-168-and-360/`

Alıştırmalar

16.29. $N \lhd G$ ve P, N'nin bir Sylow p-altgrubu olsun. Eğer $P \lhd N$ ise $P \lhd G$ olduğunu kanıtlayın.

16.30. $|G| = 24$ olsun. G'nin 4 ya da 8 elemanlı normal bir altgrubu olduğunu kanıtlayacağız. $P \in \mathrm{Syl}_2\, G$ olsun. $|P| = 8$ olur. $G \longrightarrow \mathrm{Sym}\, G/P \simeq \mathrm{Sym}\, 3$, homomorfisi G'nin G/P sol ötelemeler kümesine standart etkisi olsun. K, bu homomorfinin etkisi olsun. $K \leq P$ olduğundan, $|K|$ sayısı 8'i böler. Öte yandan $24/|K| = |G/K|$ sayısı $|\mathrm{Sym}\, 3| = 3! = 6$ sayısını böler, demek ki $|K| = 4$ ya da 8 olmalı. Ayrıntıları kontrol edin.

Seminer Konuları

A. Öklid Düzleminin Simetrileri

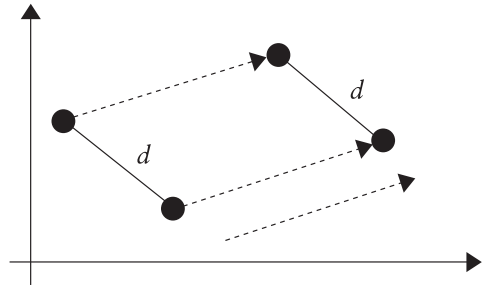
Çocukluğumuzdan beri aşina olduğumuz Öklid düzleminde mesafe, paralellik, açı, doğrusal olmak gibi kavramlar ve ilişkiler vardır. Bu kavramlara saygı duyan dönüşümler, mesela mesafeyi değiştirmeyen, paralelliği bozmayan, açıyı değiştirmeyen, doğrusallığı koruyan dönüşümler illa ki önemli olmalı, en azından haritacılıkta, denizcilikte, havacılıkta! Bu bölümde bu kavramlardan bazılarını koruyan dönüşümlerle ilgileneceğiz[1].

A.1 İzometriler

Düzlemde iki noktanın uzaklığını değiştirmeyen dönüşümler (fonksiyonlar) vardır. Bunlara ***izometri*** adı verilir. Birazdan bunların hepsini bulacağız.

Bu tür dönüşümlere birkaç örnek verelim:

1. Öteleme. Noktaları belli bir doğrultuda ve belli bir uzaklıkta ötelediğimizde, noktaların aralarındaki mesafe değişmez. Bu tür dönüşümlere ***öteleme*** denir.

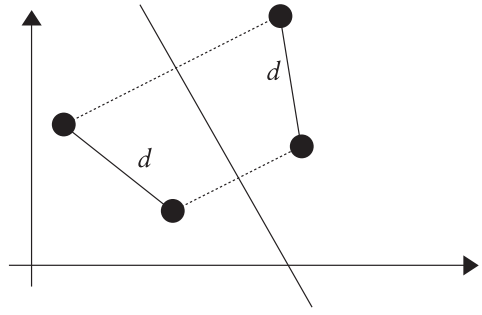


Bir vektör doğrultusunda öteleme noktaların birbirlerine olan uzaklığını değiştirmez.

2. Simetri. İki noktanın herhangi bir doğruya göre simetriğini aldığınızda, o iki nokta arasındaki mesafe değişmez.

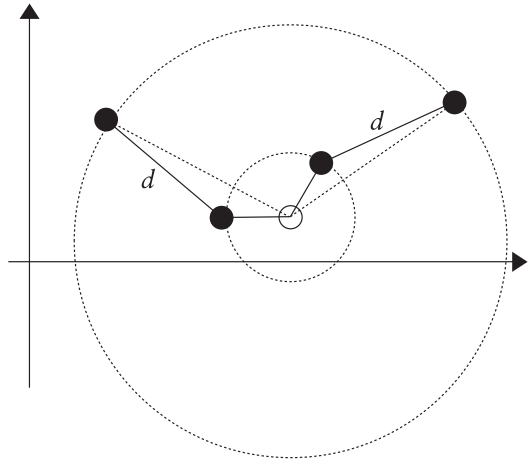
[1] Bu ek Seyfi Türkelli'yle birlikte yazılmıştır.

3. Döndürü. Düzlemi belli bir nokta etrafında belli bir derece döndürmek noktalar arasındaki mesafeyi bozmaz.



Bir doğruya göre alınan simetri noktaların birbirlerine olan uzaklığını değiştirmez.

Bu dönüşümlere ***rotasyon*** ya da ***döndürü*** denir.



Düzlemi bir noktanın etrafında döndürmek noktalar arasındaki mesafeyi değiştimez.

Yukardaki dönüşümlerin bileşkeleri de noktalar arasındaki mesafeleri değiştirmezler. Bu yazıda, bunların birbirleriyle bileşkeleri dışında, düzlemin mesafe değiştirmeyen dönüşümü olmadığını kanıtlayacağız. Buna benzer bir sonucu önce gerçel sayılar kümesi $\mathbb{R}$ için kanıtlayalım, daha kolay olacak.

A.1.1 $\mathbb{R}$'nin İzometrileri

Gerçel sayılarda x ve y arasındaki mesafe, herkesin bildiği üzere, $|x-y|$ olarak tanımlanır. Demek ki,

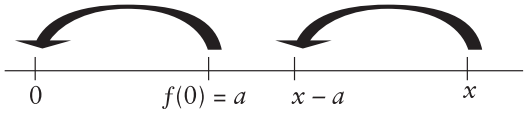
$$|x-y| = |f(x) - f(y)|$$

eşitliğini sağlayan tüm $f : \mathbb{R} \to \mathbb{R}$ dönüşümlerini (fonksiyonlarını) bulmak istiyoruz.

f böyle bir dönüşüm olsun. Aşağıda, f'yi adım adım değiştirerek en sonunda $\mathrm{Id}_{\mathbb{R}}$ (yani birim fonksiyonu, yani hiçbir noktanın yerini değiştirmeyen fonksiyon) yapacağız. Birinci adımda f'yi $f(0) = 0$ eşitliğini sağlayan bir dönüşümle değiştireceğiz. İkinci adımda f'yi $f(0) = 0$ ve $f(1) = 1$ eşitliğini sağlayan bir dönüşümle değiştireceğiz. Üçüncü adımda böyle bir dönüşümüm hiçbir noktanın yerini değiştirmediğini kanıtlayacağız. İlk iki adımda yaptığımız değişimleri bildiğimizden, üçüncü adım bize mesafeleri değiştirmeyen tüm dönüşümleri verecek.

Birinci Adım. İlk olarak 0'ı tekrar 0'a geri getireceğiz. Şöyle yapalım: Diyelim 0 noktası f altında a noktasına gitti, yani $f(0) = a$. Tüm x noktalarını $x - a$ noktalarına gönderen dönüşüme t_{-a} diyelim ve $t_{-a} \circ f$ dönüşümüne bakalım. Bu dönüşüm hâlâ daha mesafeleri korur (çünkü hem f hem de t_{-a} dönüşümü mesafeleri korur). Dahası, bu dönüşüm 0 noktasını 0 noktasına yollar:

$$(t_{-a} \circ f)(0) = t_{-a}(f(0)) = t_{-a}(a) = a - a = 0.$$

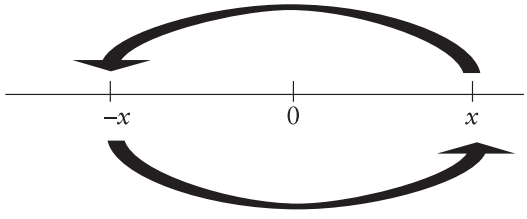


t_{-a} dönüşümü

İkinci Adım. Yukarda 0 noktasını 0 noktasına geri götürdük. Bu ikinci adımda f'nin ayrıca bu özelliği olduğunu varsayalım. Demek ki f dönüşümü

a. Noktalar arasındaki mesafeyi koruyor, ve

b. $f(0) = 0$.



r_{-1} dönüşümü, 180 derecelik döndürücü...

Şimdi, yukardaki iki özelliği bozmadan 1 noktasını 1 noktasına yollattıracağız. Aşağıdaki eşitliklere bakalım: $1 = |1 - 0| = |f(1) - f(0)| = |f(1) - 0| = |f(1)|$, yani $|f(1)| = 1$. Demek ki $f(1)$ ya 1'e ya da -1'e eşit. $f(1) = \epsilon = \pm 1$ olsun.

Şimdi $r_\epsilon(x) = \epsilon x$ dönüşümüne bakalım[2]. Bu dönüşüm noktalar arasındaki mesafeyi bozmaz ve bu da, f gibi, 0 noktasını 0 noktasına gönderir.

[2]Her $x \in \mathbb{N}$ için, $r_1(x) = x$ ve $r_{-1}(x) = -x$.

Şimdi $r_\epsilon \circ f$ dönüşümünü ele alalım. Bu $r_\epsilon \circ f$ dönüşümü hâlâ daha noktalar arasındaki mesafeyi korur, ayrıca 0'ı 0'a ve 1'i 1'e gönderir:

$$(r_\epsilon \circ f)(0) = r_\epsilon(f(0)) = r_\epsilon(0) = \epsilon 0 = 0.$$
$$(r_\epsilon \circ f)(1) = r_\epsilon(f(1)) = r_\epsilon(\epsilon) = \epsilon^2 = 1.$$

Demek ki, eğer $f, 0$ noktasını 0 gönderiyorsa, $r_\epsilon \circ f$ dönüşümü noktalar arasındaki mesafeyi korur, ayrıca 0'ı 0'a ve 1'i 1'e gönderir.

Üçüncü Adım. Yukarda 1 noktasını tekrar 1 noktasına geri götürdük, ayrıca 0 da 0'a gidiyor. Şimdi dönüşümümüzün bu iki özelliği sağladığını varsayalım. Demek ki f dönüşümü,

a. Noktalar arasındaki mesafeyi koruyor,

b. $f(0) = 0$,

c. $f(1) = 1$.

Bu üç özelliği sağlayan bir dönüşümün hiçbir noktanın yerini değiştirmeyeceğini, yani özdeşlik fonksiyonu olduğunu kanıtlayacağım şimdi.

Herhangi bir x noktası (sayısı) alalım. İki küçük hesap yapalım:

$$|x| = |x - 0| = |f(x) - f(0)| = |f(x)|,$$
$$|x - 1| = |f(x) - f(1)| = |f(x) - 1|.$$

Birinci hesaptan $f(x) = \pm x$ çıkar. Diyelim $f(x) = -x$. Bundan ve ikinci hesaptan $\pm(x - 1) = -x - 1$ çıkar. Bunun tek bir çözümü vardır: $x = 0$. Demek ki $f(x) = -x$ ise, $x = 0$ ve $f(x) = x$.

İstediğimizi kanıtladık, yani böyle bir f, birim fonksiyonu olmak zorunda.

Özetleyin. Noktalar arasındaki mesafeyi değiştirmeyen herhangi bir $f : \mathbb{R} \to \mathbb{R}$ dönüşümü aldık. Birinci adımda $t_{-a} \circ f$ dönüşümünü alarak 0'ı 0'a yolladık (Burada $a = f(0)$.) İkinci adımda, belli bir $\epsilon = \pm 1$ için, $r_\epsilon \circ t_{-a} \circ f$ dönüşümünün 0'ı 0'a ve 1'i 1'e yolladığını kanıtladık. (Burada $\epsilon = (t_{-a} \circ f)(1) = t_{-a}(f(1)) = f(1) - a = f(1) - f(0)$.) Üçüncü adımda böyle bir dönüşümün $\mathrm{Id}_\mathbb{R}$ olduğunu kanıtladık, yani

$$r_\epsilon \circ t_{-a} \circ f = \mathrm{Id}_\mathbb{R}\text{, yani } f = t_a \circ r_\epsilon.$$

Teorem A.1. *Gerçel sayıların mesafeyi değiştirmeyen dönüşümleri kümesi*

$$\{t_a \circ r_\epsilon : a \in \mathbb{R}, \epsilon = \pm 1\}$$

kümesidir. Eğer f mesafeleri değiştirmeyen bir dönüşümse, f,

$$f(x) = (f(1) - f(0))x + f(0)$$

olarak tanımlanan dönüşümüdür. Burada $f(1) - f(0) = \pm 1$ olmak zorundadır[3].

[3]Uzmanın dilinde yukardaki sonuç $\mathrm{Isom}(\mathbb{R}) \approx \mathbb{R} \times \mathbb{Z}/2\mathbb{Z}$ olarak okunur.

A.1.2 $\mathbb{R}^2$'nin İzometrileri

Şimdi $f : \mathbb{R}^2 \to \mathbb{R}^2$, mesafeleri değiştirmeyen bir dönüşüm olsun. Yukardaki gibi f'yi yavaş yavaş birim fonksiyonuna dönüştüreceğiz.

Birinci Adım. Yukardaki gibi, önce $(0,0)$ noktasını gittiği yerden geri getirelim. Şöyle yapalım: $f(0,0) = (a,b)$ ise, noktalarımızı $(-a,-b)$ yönüne doğru öteleyelim, ki (a,b) noktasına giden $(0,0)$ noktası tekrar $(0,0)$ noktasına geri dönsün. Bir başka deyişle, $t_{(-a,-b)}$ dönüşümü,

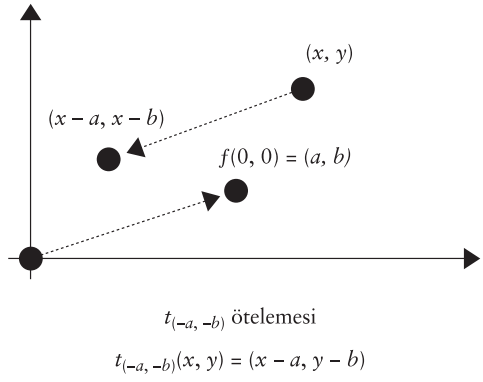
$$t_{(-a,-b)}(x,y) = (x-a, y-b)$$

olarak tanımlanmış ötelemeyse, f yerine

$$t_{(-a,-b)} \circ f$$

dönüşümüne bakalım. Bu dönüşüm noktaların mesafesini bozmadığı gibi, ayrıca $(0,0)$ noktasının yerini de değiştirmez:

$$(t_{(-a,-b)} \circ f)(0,0) = t_{(-a,-b)}(f(0,0)) = t_{(-a,-b)}(a,b) = (a-a, b-b) = (0,0).$$

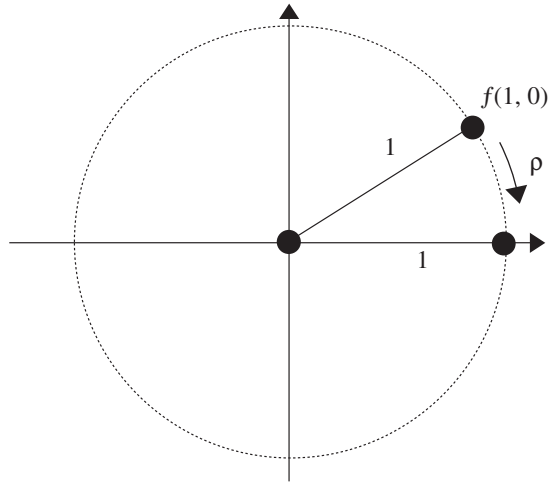


İkinci Adım. Şimdi f, noktaların aralarındaki mesafeyi değiştirmeyen ve $f(0,0) = (0,0)$ eşitliğini sağlayan bir dönüşüm olsun. f'yi değiştirerek, f'ye $(1,0)$ noktasını da sabitlettireceğiz. $(1,0)$ noktasının $(0,0)$ noktasına uzaklığı 1. Bu yüzden, f, $(0,0)$ noktasını sabitlediğine göre, mesafeleri de değiştirmediğine göre ve $f, (1,0)$ noktasını $(0,0)$'dan uzaklığı gene 1 olan bir başka noktaya yollar. $(0,0)$ merkezli bir döndürüyle bu noktayı tekrar $(1,0)$ noktasına geri götürebiliriz: Öyle bir ρ döndürüsü vardır ki, $\rho \circ f$ dönüşümü,

a. Noktalar arasındaki mesafeyi korur,

b. $(0,0)$'ın yerini değiştirmez,

c. $(1,0)$'ın yerini değiştirmez.



Üçüncü Adım. Şimdi f'nin yukardaki üç özelliği sağladığını varsayalım. Bu sefer $(0,1)$ noktasını tekrar $(0,1)$ noktasına geri götüreceğiz. $(0,1)$ noktasının $(0,0)$ noktasından uzaklığı 1, $(1,0)$ noktasından uzaklığı $\sqrt{2}$'dir. Dolayısıyla $(0,1)$ noktasının gittiği yer de bu iki özelliği sağlamalı. Yani $(0,1)$ noktası ya gene $(0,1)$ noktasına ya da $(0,-1)$ noktasına gitmeli. Bir başka deyişle, belli bir $\epsilon = \pm 1$ için $f(0,1) = (0,\epsilon)$ eşitliği geçerlidir. Şimdi $r_\epsilon(x,y) = (x,\epsilon\gamma)$ dönüşümüne bakalım. Bu dönüşüm, eğer $\epsilon = 1$ ise birim dönüşümdür, eğer $\epsilon = -1$ ise x eksenine göre simetridir. Dolayısıyla r_ϵ dönüşümü - aynen f gibi - noktalar arasındaki mesafeyi değiştirmez ve $(0,0)$ ve $(1,0)$ noktalarını sabitler. Dolayısıyla $r_\epsilon \circ f$ dönüşümü de aynı özellikleri sağlar. Ayrıca $r_\epsilon \circ f$ dönüşümü $(0,1)$ noktasını gene $(0,1)$ noktasına yollar:

$$(r_\epsilon \circ f)(0,1) = r_\epsilon(f(0,1)) = r_\epsilon(0,\epsilon) = (0,\epsilon^2) = (0,1).$$

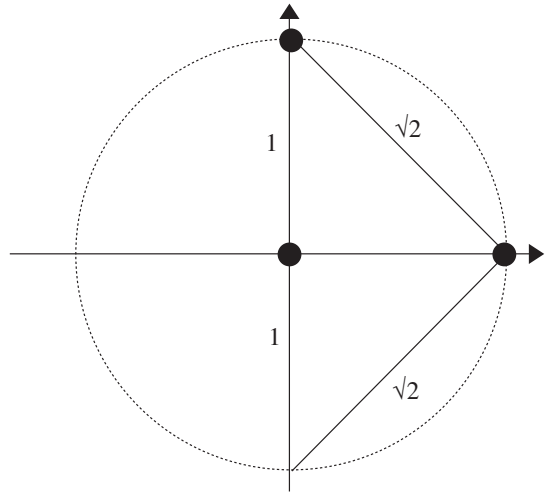
Demek ki $r_\epsilon \circ f$ dönüşümü,

a. Noktalar arasındaki mesafeyi korur,

b. $(0,0)$'ın yerini değiştirmez,

c. $(1,0)$'ın yerini değiştirmez,

d. $(0,1)$'ın yerini değiştirmez.



Dördüncü Adım. Şimdi f'nin yukardaki dört özelliği sağladığını varsayalım. Bu durumda f'nin birim fonksiyon olduğunu kanıtlamak oldukça kolaydır. Ayrıntıları okura bırakıyoruz.

Özetleyin. Noktalar arasındaki mesafeyi değiştirmeyen bir f dönüşümüyle başladık işe. Birinci adımda f yerine, belli bir t ötelemesi için, $t \circ f$ alarak $(0,0)$ noktasının sabitlendiğini varsayabildik. İkinci adım sayesinde, $t \circ f$ yerine, $(0,0)$ merkezli belli bir ρ döndürüsü için, $\rho \circ t \circ f$ dönüşümünü alarak sadece $(0,0)$ noktasının değil, ayrıca $(1,0)$ noktasının da sabitlendiğini varsayabiliriz. Üçüncü adım sayesinde, $\rho \circ t \circ f$ yerine, x eksenli bir r_ϵ simetrisi için, $r_\epsilon \circ \rho \circ t \circ f$ dönüşümünü alarak sadece $(0,0)$ ve $(1,0)$ noktalarının değil, ayrıca $(0,1)$ noktasının da sabitlendiğini varsayabiliriz. Dördüncü adımda böyle bir dönüşümün birim fonksiyon olması gerektiğini söyledik (kanıtını okura bıraktık.) Demek ki, belli bir t ötelemesi, $(0,0)$ merkezli belli bir ρ döndürüsü ve x eksenli bir r_ϵ simetrisi için, $r_\epsilon \circ \rho \circ t \circ f = \mathrm{Id}$. Aşağıdaki teoremi kanıtladık:

Teorem A.2. *$f : \mathbb{R}^2 \to \mathbb{R}^2$, noktaların arasındaki mesafeyi değiştirmeyen bir dönüşüm olsun. O zaman, belli bir t ötelemesi, $(0,0)$ merkezli belli bir ρ döndürüsü ve x eksenli bir r_ϵ simetrisi için, $f = t \circ \rho \circ r_\epsilon$ olur*[4].

A.2 Doğruları Doğrulara Götüren Dönüşümler

Bir önceki bölümde $\mathbb{R}^2$ düzleminin uzaklığı değiştirmeyen dönüşümlerini bulduk. O yazıdaki teoreme (ikincisine) bakıldığında, bu dönüşümlerin doğruları doğrulara yolladığı anlaşılır, çünkü ötelemeler, simetriler ve döndürüler doğruları doğrulara yollarlar.

[4]Uzman dilinde bu teorem, $\mathrm{Isom}(\mathbb{R}^2) \approx (\mathbb{R}^2 \times \mathbb{R}/\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ olarak okunur.

Bu yazıda $\mathbb{R}^2$ düzleminin doğruları doğrulara yollayan birebir dönüşümlerini, yani her ℓ doğrusu için, $f(\ell) = \ell'$ ilişkisini sağlayan sağlayan bir ℓ' doğrusunun bulunduğu dönüşümleri sınıflandıracağız (ℓ' doğrusu her ℓ için değişir, yoksa f birebir olamaz.)

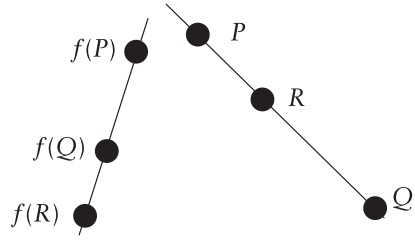
Yukardaki özelliği olan bir f dönüşümü paralel doğruları paralel doğrulara götürmek zorundadır. Nitekim, eğer ℓ ve m paralel doğrularsa ve $f(\ell) = \ell'$ ve $f(m) = m'$ ise ve $P \in \ell' \cap m'$ ise, o zaman, belli bir $\mathcal{Q} \in \ell$ ve $R \in m$ için $f(\mathcal{Q}) = P = f(R)$ olmak zorunda; ve f birebir olduğundan $\mathcal{Q} = R \in m \cap \ell$, çelişki.

Bu yüzden (paralel doğruları paralel doğrulara götürdüğünden) bu dönüşümler, $\mathbb{R}^2$ Öklid geometrisinin özyapı dönüşümleri olarak düşünülebilir.

Heyecanı kaybetmemek için sonucu şimdiden söylemeyeceğiz.

$f : \mathbb{R}^2 \to \mathbb{R}^2$ yukardaki gibi bir dönüşüm olsun. Demek ki her $P, \mathcal{Q} \in \mathbb{R}^2$ için, $f, P\mathcal{Q}$ doğrusunu $f(P)$ ve $f(Q)$'dan geçen doğruya yolluyor, yani

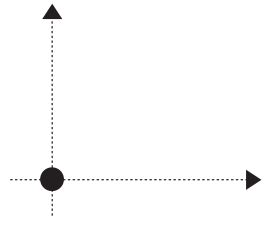
$$f(P\mathcal{Q}) = f(P)f(\mathcal{Q}).$$



Birinci Adım. Bir önceki yazıdaki gibi f'nin bir ötelemeyle bileşkesini alıp, f'nin $(0,0)$ noktasını gene $(0,0)$ noktasına götürdüğünü varsayabiliriz. Şöyle yaparız: $f(0,0) = (a,b)$ ise ve $t : \mathbb{R}^2 \to \mathbb{R}^2$ fonksiyonu (ötelemesi)

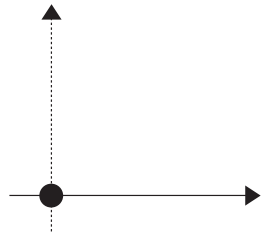
$$f(x,y) = (x-a, y-a)$$

olarak tanımlanmışsa, f yerine $t \circ f$ dönüşümünü alıp, f'nin doğruları doğrulara götürdüğünü, ayrıca (0, 0) noktasını yerinden kımıldatmadığını varsayabiliriz.



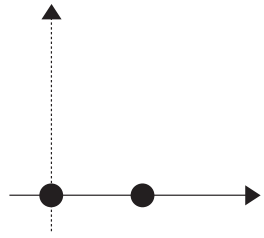
İkinci Adım. $f : \mathbb{R}^2 \to \mathbb{R}^2$ doğruları doğrulara götüren ve $(0,0)$ noktasını kımıldatmayan bir dönüşüm olsun. O zaman $(0,0)$'dan geçen doğrular f altında

gene $(0,0)$'dan geçen doğrulara giderler. $(0,0)$ merkezli bir döndürüyle x eksenini gittiği yerden aynen geri getirebiliriz, yani öyle bir r döndürüsü bulabiliriz ki, $r \circ f$ dönüşümü doğruları doğrulara götürür, $(0,0)$ noktasını sabit tutar ve ayrıca x eksenini gene x eksenine yollar[5].



Görüldüğü gibi f dönüşümünü yavaş yavaş özdeşliğe benzetiyoruz.

Üçüncü Adım. $f : \mathbb{R}^2 \to \mathbb{R}^2$, doğruları doğrulara götüren, $(0,0)$ noktasını kımıldatmayan ve x eksenini x eksenine götüren bir dönüşüm olsun. $(1,0)$ noktası, belli bir $a \in \mathbb{R} \setminus \{0\}$ için, $(a,0)$ noktasına gider. $r_a : \mathbb{R}^2 \to \mathbb{R}^2$ fonksiyonu $r_a(x,y) = (a^{-1}x, y)$ olarak tanımlansın. r_a fonksiyonu, aynen f gibi, doğruları doğrulara götürür, $(0,0)$ noktasını $(0,0)$ noktasına götürür, x eksenini gene x eksenine götürür. Şimdi $r_a \circ f$ dönüşümüne bakalım. Bu dönüşüm de doğruları doğrulara götürür, $(0,0)$ noktasını $(0,0)$ noktasına götürür, x eksenini gene x eksenine götürür, ama ayrıca $(1,0)$ noktasını gene $(1,0)$ noktasına götürür.



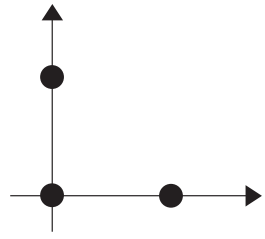
Dördüncü Adım. $f : \mathbb{R}^2 \to \mathbb{R}^2$ fonksiyonu, doğruları doğrulara götürsün ve $(0,0)$ ve $(1,0)$ noktalarını sabitlesin. (O zaman x eksenini x eksenine götürmek zorundadır. Dolayısıyla, paralel doğruları paralel doğrulara götürdüğünden yatay doğruları yatay doğrulara götürmek zorundadır.) Şimdi $(0,1)$ noktasını tekrar $(0,1)$ noktasına götürmek istiyoruz. Nasıl yapacağız? Bu, biraz daha zor.

$f(0,1) = (c,d)$ olsun. Şimdi $g : \mathbb{R}^2 \to \mathbb{R}^2$ dönüşümünü

$$g(x,y) = (x - d^{-1}cy, d^{-1}y)$$

[5]Uzmana Not: Eğer $\mathbb{R}$ yerine başka bir cisim alırsak, bu adımda döndürü kullanamayız, ama doğrusal bir dönüşümle x eksenini x eksenine götürebiliriz.

kuralıyla tanımlayalım. g dönüşümü doğruları doğrulara götürür ve $(0,0)$ ve $(0,1)$ noktalarını sabitler. Ayrıca (c,d) noktasını $(0,1)$ noktasına götürür. Demek ki $g \circ f$ dönüşümü doğruları doğrulara götürür ve $(0,0),(1,0)$ ve $(0,1)$ noktalarını sabitler (dolayısıyla x ye y eksenlerini de kendilerine götürür.)



İkinci, Üçüncü ve Dördüncü Adımlar Üzerine Bir Not. İki, üç ve dördüncü adımları doğrusal bir dönüşümle tek hamlede yapabilirdik.

$$f(1,0) = (a,b) \text{ ise } f(0,1) = (c,d)$$

ise,

$$g(x,y) = \left(\frac{dx - cy}{ad - bc}, \frac{-bx + ay}{ad - bc} \right)$$

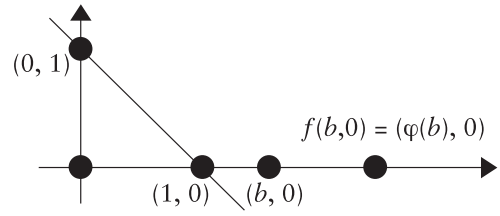
kuralıyla tanımlanmış olsun. Şimdi $g \circ f$ dönüşümü doğruları doğrulara götürür ve $(0,0),(1,0)$ ve $(0,1)$ noktalarını sabitler. (Tabii bunu yapmadan önce $ad - bc \neq 0$ eşitsizliğini kanıtlamak lazım.)

Beşinci Adım. $f : \mathbb{R}^2 \to \mathbb{R}^2$ fonksiyonu, doğruları doğrulara götürsün ve $(0,0),(1,0)$ ve $(0,1)$ noktalarını sabitlesin. O zaman f dönüşümü bu noktalardan geçen üç doğruyu gene kendilerine götürür, yani x eksenini x eksenine, y eksenini y eksenine ve $y = -x + 1$ doğrusunu gene kendine götürmek zorundadır. Ayrıca f'nin paralel doğruları paralel doğrulara götürdüğünü biliyoruz. Dolayısıyla yatay doğruları yatay doğrulara, dikey doğruları dikey doğrulara götürür. Ayrıca eğimi -1 olan doğruları gene eğimi -1 olan doğrulara götürür. Bayağı şey biliyoruz. Bütün bunlardan f'nin her noktayı sabitlediğini kanıtlayacağız.

Şimdi $x \in \mathbb{R}$ olsun. $(x,0)$ noktası x ekseninde olduğundan,

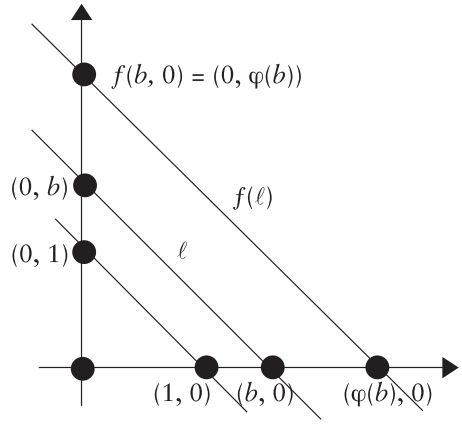
$$f(x,0) = (\varphi(x),0)$$

türünden yazılabilir. Böylece bir $\varphi : \mathbb{R} \to \mathbb{R}$ fonksiyonu elde ediyoruz. f dönüşümü $(0,0)$ ve $(1,0)$ noktalarını sabitlediğinden $\varphi(0) = 0$ ve $\varphi(1) = 1$. Yakın gelecekte, her $x \in \mathbb{R}$ için, $\varphi(x) = x$ eşitliğini kanıtlayacağız.



Bundan böyle $f : \mathbb{R}^2 \to \mathbb{R}^2$ ve $\varphi : \mathbb{R} \to \mathbb{R}$ bu paragrafta tanımlandığı gibi olsunlar.

Altıncı Adım. Bu adımda, her $x \in \mathbb{R}$ için $f(0,x) = (0,\varphi(x))$ eşitliğini kanıtlayacağız. Herhangi bir $b \in \mathbb{R}$ alalım. f dönüşümü y eksenini gene y eksenine götürdüğünden, $f(0,b)$ noktası y ekseni üstündedir, yani birinci koordinatı 0'dır. İkinci koordinatın $\varphi(b)$ olduğunu kanıtlayacağız.



Şimdi $(b,0)$ ve $(0,b)$ noktalarından geçen ℓ doğrusunu ele alalım ve yukarıdaki şekilden izleyelim. Eğimi -1 olan ℓ doğrusu f tarafından kendisine paralel bir doğruya yollanır. Ama $(b,0) \in \ell$ olduğundan, $(\varphi(b),0) = f(b,0) \in f(\ell)$. Demek ki $f(0,b) = (0,\varphi(b))$.

Yedinci Adım. Şimdi şunu iddia ediyoruz: Her $(x,y) \in \mathbb{R}^2$ için

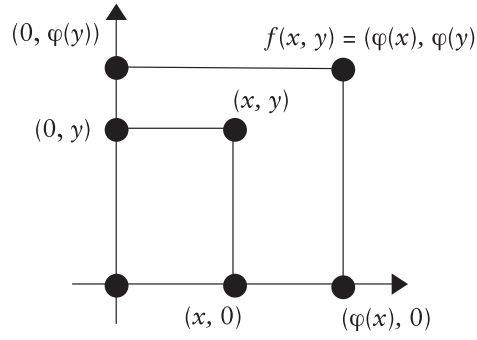
$$f(x,y) = (\varphi(x),\varphi(y))$$

eşitliği doğrudur.

Herhangi bir (x,y) noktası alalım. $(x,0)$'dan geçen dikey doğru

$$f(x,0) = (\varphi(x),0)$$

'dan geçen dikey doğruya gitmek zorunda. Aynı zamanda $(0,y)$'den geçen yatay doğru $f(0,y) = (0,\varphi(y))$'den geçen yatay doğruya gitmek zorunda. Dolayısıyla (x,y) noktası $(\varphi(x),\varphi(y))$ noktasına gitmek zorunda.

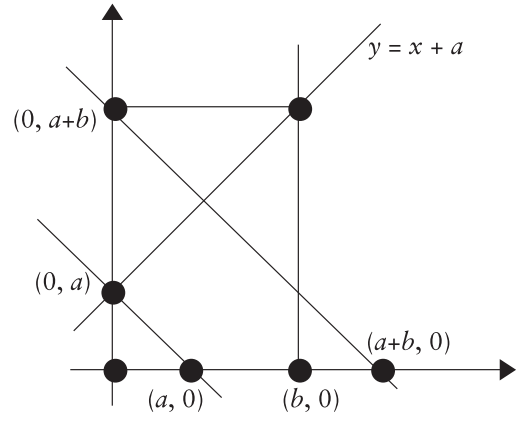


Bir Sonuç. Yukardaki adıma göre, $(1,1)$ noktası f altında

$$f(1,1) = (\varphi(1), \varphi(1)) = (1,1)$$

noktasına, yani kendine gitmek zorunda. Dolayısıyla $(0,0)$ ve $(1,1)$ noktalarından geçen doğru da kendine gider. Demek ki eğimi 1 olan bir doğru gene eğimi 1 olan bir doğruya gider. Eğimi -1 olan bir doğrunun gene eğimi -1 olan bir doğruya gittiğini zaten biliyoruz.

Sekizinci Adım. Bu paragrafta, φ'nin toplamaya saygı duyduğunu, yani her $x, y \in \mathbb{R}$ için, $\varphi(x+y) = \varphi(x) + \varphi(y)$ eşitliğini kanıtlayacağız.



Yukarıdaki şekilden de görüleceği üzere, $(a,0)$ ve $(b,0)$ noktası verilmişse,

$$(a+b, 0)$$

noktasını dikey, yatay ve eğimi 1 ve -1 olan doğruların kesişimlerinden elde edebiliriz. Şimdi, $(a+b,0)$ noktasını bulmak için kullandığımız bu yedi doğruya ve yedi noktaya f'yi uygulayalım. Aynen bu şekle benzeyen bir durum elde ederiz. x ve y eksenler ve $(0,0)$ noktası yerlerinden kımıldamaz. Böylece

$$f(a,0) = (\varphi(a), 0)$$

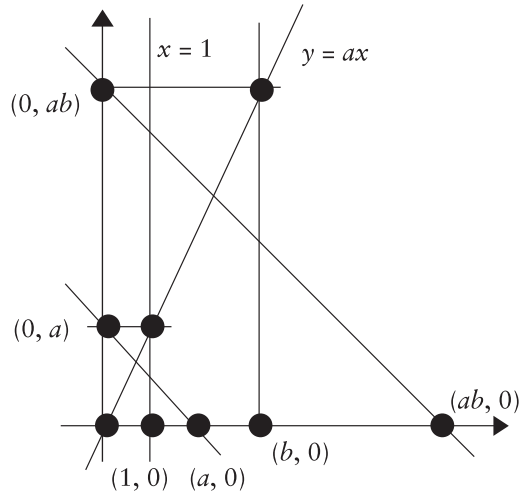
ve $f(b,0) = (\varphi(b),0)$ noktalarından hareket ederek ve aynı yöntemle

$$(\varphi(a) + \varphi(b), 0)$$

noktasını elde ederiz. Öte yandan bu nokta aynı zamanda $f(a+b,0)$, yani $(\varphi(a+b),0)$ noktasıdır da. Demek ki $\varphi(a+b) = \varphi(a) + \varphi(b)$.

Dokuzuncu Adım. Bu paragrafta, φ'nin çarpmayla uyumlu olduğunu, yani her $x, y \in \mathbb{R}$ için, $\varphi(xy) = \varphi(x)\varphi(y)$ eşitliğini kanıtlayacağız.

Aşağıdaki şekilden de görüleceği üzere, $(a,0)$ ve $(b,0)$ noktası verilmişse, $(ab,0)$ noktasını verilmiş noktalardan geçen doğrularla elde edebiliriz. Şimdi, $(ab,0)$ noktasını bulmak için kullandığımız bu dokuz doğru ve dokuz noktaya f'yi uygulayalım. Aynen bu şekle benzeyen bir durum elde ederiz. Üç doğru (x ve y eksenleri ve $x = 1$ doğrusu) ve iki nokta ($(0,0)$ ve $(1,0)$ noktaları) yerlerinden kımıldamaz.



Böylece $f(a,0) = (\varphi(a),0)$ ve $f(b,0) = (\varphi(b),0)$ noktalarından hareket ederek aynı yöntemle $(\varphi(a)\varphi(b),0)$ noktasını elde ederiz. Öte yandan bu nokta aynı zamanda $f(ab,0)$, yani $(\varphi(ab),0)$ noktasıdır da. Demek ki $\varphi(ab) = \varphi(a)\varphi(b)$.

Onuncu Adım. Adım adım yolun sonuna geldik. Şimdi önümüzde, her $x, y \in \mathbb{R}$ için, $\varphi(x+y) = \varphi(x) + \varphi(y)$ ve $\varphi(xy) = \varphi(x)\varphi(y)$ eşitliklerini sağlayan bir fonksiyon var. Böyle bir φ fonksiyonunun birim fonksiyon olduğunu göstermek zor değildir. Demek ki dördüncü adımda bulduğumuz dönüşüm birim fonksiyonuymuş.

Özetleyin. Doğruları doğrulara gönderen birebir bir $f : \mathbb{R} \to \mathbb{R}$ fonksiyonuyla yola koyulduk.

Birinci adımda, bir t ötelemesi için, $t \circ f$ dönüşümünün doğruları doğruları götürdüğünü, ayrıca $(0,0)$ noktasının yerini değiştirmediğini gördük.

İkinci adımda, bir ρ döndürüsü için, $\rho \circ t \circ f$ dönüşümünün doğruları doğruları götürdüğünü, $(0,0)$ noktasının yerini değiştirmediğini, ayrıca x eksenini x eksenine götürdüğünü gördük.

Üçüncü adımda, belli bir a için,

$$r(x,y) = (a^{-1}x, y)$$

kuralıyla tanımlanan bir r fonksiyonu için,

$$r \circ \rho \circ t \circ f$$

dönüşümünün doğruları doğruları götürdüğünü, $(0,0)$ noktasının yerini değiştirmediğini, x eksenini x eksenine götürdüğünü ve ayrıca $(1,0)$ noktasını $(1,0)$ noktasına götürdüğünü gördük.

Dördüncü adımda, belli bir $u, v \in \mathbb{R}$ için ve $g(x,y) = (x - uy, vy)$ kuralıyla tanımlanan g fonksiyonu için, $g \circ r \circ \rho \circ t \circ f$ dönüşümünün doğruları doğruları götürdüğünü, $(0,0)$ noktasının yerini değiştirmediğini, x eksenini x eksenine götürdüğünü, $(1,0)$ noktasını $(1,0)$ noktasına götürdüğünü ve ayrıca $(0,1)$ noktasını $(0,1)$ noktasına götürdüğünü gördük.

Beşinci ve sonraki adımlarda, yukardaki özelliğe sahip bir fonksiyonun birim fonksiyon olması gerektiğini gördük, yani $g \circ r \circ \rho \circ t \circ f = \mathrm{Id}_{\mathbb{R}}$. Bundan da kolaylıkla şu sonuç çıkar:

Teorem A.3. *$f : \mathbb{R}^2 \to \mathbb{R}^2$ doğruları doğrulara götüren birebir bir fonksiyon olsun. O zaman, öyle bir t ötelemesi, öyle bir ρ döndürüsü ve öyle bir*

$$g(x,y) = (ax + by, cy)$$

fonksiyonu vardır ki, $f = t \circ \rho \circ g$ eşitliği sağlanır[6]*.*

Alıştırmalar

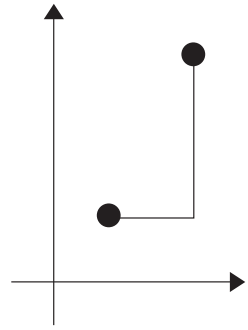
A.1. $\mathbb{R}^n$ uzayının mesafe değiştirmeyen dönüşümlerini bulun. (Not: $\mathbb{R}^n$ uzayında $(x_1, \ldots, x_n)$ ve $(y_1, \ldots, y_n)$ arasındaki mesafe

$$\sqrt[2]{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}$$

olarak tanımlanır.)

A.2. "Mesafe" kavramı bulunduğumuz coğrafyaya göre değişebilir. Örneğin, bir şehrin sokaklarındaysanız, bir noktadan bir diğer noktaya gitmek için düz doğruyu seçemeyebilirsiniz, karşınıza evler, hanlar, konaklar çıkar, özellikle bu iş için tasarlanmış sokaklardan yürümek zorundasınız.

[6] Uzmana Not: Bu teoremin kanıtından şunlar çıkar: 1. K bir cisim olsun. K^2'nin doğruları doğrulara götüren eşlemeleri $(K^2 \times \mathrm{GL}_2(K)) \times \mathrm{Aut}(K)$ grubuna izomorfiktir. 2. Eğer $B_2(\mathbb{R})$ üst-üçgen matrislerse (yani standard Borel altgrubu), $\mathrm{GL}_2(\mathbb{R}) = SO_2(\mathbb{R})B_2(\mathbb{R})$. (Ama bu iki altgrubun hiçbiri normal değil, ayrıca ikisi de çözülebilir.)



Örneğin New York'ta, bir noktadan bir başka bir noktaya ancak kuzey, doğu, güney ve batı yönlerine doğru giderek gidebilirsiniz. New York sokaklarındaki (x, y) ve (z, t) noktaları arasındaki (en kısa) mesafe

$$d((x, y), (z, t)) = |x - z| + |y - t|$$

olarak tanımlanmalı. $\mathbb{R}^2$ düzleminin bu mesafe kavramını değiştirmeyen dönüşümlerini bulun, yani her $x, y, z, t \in \mathbb{R}$ için,

$$d((x, y), (z, t)) = d(f(x, y), f(z, t))$$

eşitliğini sağlayan tüm $f : \mathbb{R}^2 \to \mathbb{R}^2$ dönüşümlerini bulun.

B. Kartezyen Çarpım Serbest Abel Grubu Olmayabilir

$\bigoplus_{\mathbb{N}} \mathbb{Z}$ grubu, tanım gereği, serbest abel grubudur. Acaba, $\prod_{\mathbb{N}} \mathbb{Z}$ grubu da serbest mi? Bu ekte[1] $\prod_{\mathbb{N}} \mathbb{Z}$ grubunun serbest abel grup olmadığını, yani bir I kümesi için $\oplus_I \mathbb{Z}$ grubuna izomorf olmadığını kanıtlayacağız[2].

Teorem B.1. *$P = \prod_{\mathbb{N}} \mathbb{Z}$ grubu serbest abel grubu değildir.*

Kanıtın Anafikri: Herhangi bir I için $\oplus_I \mathbb{Z}$ serbest abel grubunda 2'ye bölünen, yani 2'nin katı olan elemanlar kümesi $\oplus_I 2\mathbb{Z}$ altgrubudur. 3'e bölünen elemanlar kümesi ise $\oplus_I 3\mathbb{Z}$ altgrubudur. Genel olarak, n'ye bölünen elemanlar kümesi $\oplus_I n\mathbb{Z}$ altgrubudur. Bunların hepsinin kesişimi de 0 altgrubudur. Yani $\oplus_I \mathbb{Z}$ serbest abel grubunda tüm doğal sayılara bölünen 0'dan farklı bir eleman yoktur. Bir başka deyişle, verilmiş herhangi bir $a \neq 0$ elemanı için, $a = nx$ denkleminin çözümünün olmadığı bir $n > 0$ doğal sayısı vardır. Yani

$$\exists a \neq 0 \, \forall n > 0 \, \exists x \; a = nx \tag{2}$$

önermesi $\oplus_I \mathbb{Z}$ serbest abel grubunda ve her serbest abel grubunda yanlıştır. Bunu aklımızda tutalım.

Aynı önerme aynı nedenden P grubunda da yanlıştır. Ama bu önermenin P'de doğru olmasına ramak kalmıştır. Bu muğlak cümleyi açıklayalım.

$$A = \bigoplus_{\mathbb{N}} \mathbb{Z} \leq \prod_{\mathbb{N}} \mathbb{Z} = P$$

olsun.

$$p = (n!)_n = (1, 1, 2, 6, 24, 120, \ldots, n!, \ldots) \in \prod_{\mathbb{N}} \mathbb{Z}$$

[1] Bu ek Halime Ömrüuzun ile birlikte yazılmıştır.

[2] Lineer Cebir bilenlere not: Eğer K bir cisimse, $\prod_{\mathbb{N}} K$ bir vektör uzayı olduğundan, vektör uzayı olarak (dolayısıyla bir grup olarak da) $\oplus_I K$ vektör uzayına izomorftur. Bu nedenden dolayı benzer sonucun $\prod_{\mathbb{N}} \mathbb{Z}$ grubu için doğru olmaması oldukça şaşırtıcı bulunabilir.

olsun. P grubunda $p = 2x$ denkleminin çözümü yoktur çünkü p'nin ilk iki koordinatı 2'ye bölünmez. Benzer nedenden $p = 3x$ ya da $p = 4x$ denkleminin de çözümleri yoktur. Ama sonlu sayıdaki ilk birkaç koordinatı yok sayarsak, yani biraz hata payıyla $p = nx$ denklemini P grubunda çözebiliriz. Mesela

$$x = (0, 0, 0, 2, 8, 40, \ldots, n!/3, \ldots)$$

ise

$$3x = (0, 0, 0, 6, 24, 120, \ldots, n!, \ldots)$$

olur ve

$$p - 3x = (1, 1, 2, 0, 0, \ldots, 0, \ldots) \in A$$

olur. Bir başka deyişle, P grubunda,

$$p = nx$$

denklemini, bırakın her n için çözmeyi, tek bir $n > 1$ için bile çözemeyiz belki ama,

$$\overline{p} = n\overline{x}$$

denklemini her $n > 0$ için P/A bölüm grubunda çözebiliriz. Sonuç olarak (2) önermesi P/A bölüm grubunda doğrudur.

(2) önermesi P/A bölüm grubunda doğru olduğu gibi, elbette, $A \leq H < P$ içindeliklerini sağlayan her H altgrubu için P/H bölüm grubunda da doğrudur. Dolayısıyla eğer H'yi, (1) eşitliğini kullanarak,

a. $A \leq H < P$,

b. P/H serbest

olacak biçimde seçebilirsek, o zaman bir çelişki elde ederiz ve böylece (1) eşitliğinin doğru olamayacağı çıkar.

Planımız tam böyle yürümeyecek. p'yi yukarıdaki verildiği şekilde seçmeyeceğiz. Ama her pozitif doğal sayıya olmasa da, giderek artan doğal sayılara bölünen bir p elemanının ve yukarıdaki gibi bir H altgrubunun varlığını gösterebileceğiz, bunlar da bize yetecek.

Kanıt: Tam tersine P'nin bir serbest abel grubu olduğunu varsayalım. O zaman P'nin bir tabanı vardır, diyelim $(e_i)_{i \in I}$:

$$P = \prod_{\mathbb{N}} \mathbb{Z} = \bigoplus_{I} \mathbb{Z}e_i. \tag{1}$$

i. P sayılamaz sonsuzlukta olduğundan, I da sayılamaz sonsuzluktadır. (Hatta her ikisinin de kardinalitesi $\mathbb{R}$'nin kardinalitesi kadardır.)

ii. $f_n \in P$ elemanı, n'inci koordinatı 1, diğer tüm koordinatları 0 olan eleman olsun. Bunlardan sayılabilir sonsuzlukta vardır ve A altgrubunu üretirler. f_n'yi e_i'lerin lineer kombinasyonu olarak yazalım:

$$f_n = \sum_{i \in I} \alpha_{ni} e_i.$$

Verilmiş bir n için bu toplamda sadece sonlu sayıda 0'dan farklı α_{ni} vardır. J, yukarıdaki eşitliklerde gerçekten kullanılan göstergeç kümesi olsun, yani

$$J = \{i \in I : \text{ bir } n \in \mathbb{N} \text{ için } \alpha_{ni} \neq 0\}$$

olsun. J kümesi sayılabilir sonsuzluktadır. Böylece,

$$f_n = \sum_{i \in J} \alpha_{ni} e_i \tag{3}$$

yazabiliriz.

iii. Bu paragrafta söz verdiğimiz H altgrubunu bulacağız.

$$H = \langle e_i : i \in J \rangle = \bigoplus_{i \in J} \mathbb{Z} e_i$$

olsun. J sayılabilir sonsuzlukta olduğundan, H de sayılabilir sonsuzluktadır. Ayrıca, (3)'ten dolayı, her n için $f_n \in H$ olduğundan,

$$A = \langle f_n : n \in I \rangle \leq H$$

olur. Ayrıca elbette,

$$P = \bigoplus_{I} \mathbb{Z} e_i = H \oplus \left(\bigoplus_{I \setminus J} \mathbb{Z} e_i \right)$$

ve dolayısıyla

$$P/H \simeq \bigoplus_{I \setminus J} \mathbb{Z} e_i$$

olur. Yani P/H serbest abeldir. Dolayısıyla (2) önermesi P/H grubunda doğru olamaz.

iv. Eğer bir $p = (p_n)_n \in P$ elemanının tüm koordinatları 0'dan değişikse ve her n için $p_n < p_{n+1}$ ise ve p_n koordinatı p_{n+1} koordinatını bölüyorsa, p elemanına ***üstel artan eleman*** diyelim. Üstel artan elemanlar kümesi sayılamaz sonsuzluktadır çünkü üstel bir eleman elde etmek için her koordinattan bir sonraki koordinatı elde etmek için o koordinatı 2'yle **ya da** 3'le çarpabiliriz.

v. H sayılabilir sonsuzlukta, üstel artan elemanlar sayılamaz sonsuzlukta olduğundan olduğundan, H'de olmayan bir üstel artan eleman vardır. Bu elemanlardan birine $p = (p_n)_n$ diyelim. P/H grubunda, her n için

$$\overline{p} = p_n \overline{x}$$

denkleminin bir çözümü vardır. Nitekim eğer

$$x = (0, 0, \ldots, 0, 1, p_{n+1}/p_n, p_{n+2}/p_n, \ldots) \in P$$

ise

$$p - p_n x = (p_0, p_1, \ldots, p_{n-1}, 0, 0, \ldots) \in A \leq H,$$

ve P/H grubunda,

$$\overline{p} = p_n \overline{x}$$

olur. Demek ki (2) önermesi P/H'de doğru. Bu da bir önceki paragrafla çelişir. Hedeflediğimiz teorem kanıtlanmıştır. □

C. Hemen Hemen Her Sonlu Çizge Asimetriktir

Eğer bir çizgenin özdeşlik, yani Id fonksiyonundan başka otomorfizması yoksa, bu çizgeye ***asimetrik*** denir. İşte birden fazla noktası olan en küçük asimetrik çizge:

Resim gelecek, otomorfizmasız çizge

Asimetrik çizge bulmak hiç kolay değildir. Ama bu zorluk anlaşılan, asimetrik çizgelerin enderliğinden değil, beynimizin simetrisiz düşünmede zorlanmasından kaynaklanmaktadır. Nitekim hemen hemen her sonlu çizge asimetriktir. Bir başka deyişle, büyük bir n doğal sayısı için n noktalı rastgele bir çizge seçseniz, bu çizge çok büyük bir olasılıkla asimetrik olacaktır. Bu yazıda bunu kanıtlayacağız. Tam olarak neyi kanıtlayacağımızı açıklayalım.

n elemanlı bir V kümesi alalım. $V = \{1, 2, \ldots, n\}$ olabilir mesela. Noktalar kümesi V olan çizgelerden oluşan kümeye Ω diyelim. Ω'nın tam

$$2^{\binom{n}{2}}$$

tane elemanı vardır. Nitekim noktalar kümesi V olan bir X çizgesi bağıntılarıyla, yani $E(X)$ olarak simgelenen bağıntılar kümesiyle belirlenir ve $E(X)$ de, V'nin 2 elemanlı altkümeler kümesi olan $\wp_2(V)$'nin bir altkümesidir. Demek ki

$$|\Omega| = |\wp(\wp_2(V))| = 2^{|\wp_2(V)|} = 2^{\binom{n}{2}}.$$

Bu bölümde Ω kümesiyle $\wp(\wp_2(V))$ kümesini özdeşleştireceğiz. (Ω'daki çizgelerin noktaları V'nin elemanları olarak belirlenmiş olduğundan, Ω'daki çizgeler bağıntılar kümesi tarafından tamamen belirlenir.)

Ω kümesindeki asimetrik çizge sayısı a_n olsun.

$$\mu_n = \frac{a_n}{2^{\binom{n}{2}}}$$

sayısı, asimetrik çizgelerin Ω kümesindeki oranıdır. Bu yazıda bu oranın 1'e yakınsadığını, yani

$$\lim_{n\longrightarrow\infty} \mu_n = 1$$

eşitliğini kanıtlayacağız. Böylece büyük n doğal sayıları için asimetrik çizge sayısının hemen hemen toplam çizge sayısı kadar olduğu anlaşılacak.

Kanıtımızın iskeletini oluşturacak olan basit bir önsavla başlayalım.

Önsav C.1 (Burnside[1])**.** *Sonlu G grubu sonlu bir V kümesine etkisin. O zaman V'deki yörünge sayısı G'nin elemanlarının sabitlediği ortalama eleman sayısına, yani*

$$\frac{1}{|G|}\sum_{g\in G} |\operatorname{Fix}_V(g)|$$

sayısına eşittir.

Kanıt: $A = \{(g,x) \in G \times V : gx = x\}$ kümesini iki değişik biçimde sayalım. Eğer saymayı $g \in G$ üzerine toplayarak yaparsak,

$$|A| = \sum_{g\in G} |\operatorname{Fix}_V(g)| \tag{1}$$

buluruz. Şimdi de saymayı $x \in X$ üzerine yapalım. Okurun

$$Gx = \{gx : g \in G\} = x\text{'in } G\text{-yörüngesi}$$

ve

$$G_x = \{g \in G : gx = x\} = x\text{'in } G\text{'deki sabitleyicisi} \leq G$$

tanımlarıyla,

$$|G| = |Gx||G_x|$$

eşitliğini bildiğini varsayıyoruz[2]. Her yörüngeden bir eleman (temsilci) seçelim ve bu temsilcilerden oluşan kümeye Y diyelim. Bu durumda,

$$|A| = \sum_{x\in X} |G_x| = \sum_{x\in X} \frac{|G|}{|Gx|} = \sum_{y\in Y} |Gy| \frac{|G|}{|Gy|} = \sum_{y\in Y} |G| = |G|\,|Y| \tag{2}$$

olur. (1) ve (2) eşitliklerinden istediğimiz çıkar. □

$G = \operatorname{Sym}(V)$ olsun. G, Ω üzerine doğal olarak etkir. Bu etkimeyi şöyle görebiliriz: G, elbette V üzerine etkir; dolayısıyla $\wp_2(V)$ üzerine de etkir; dolayısıyla $\wp(\wp_2(V)) = \Omega$ üzerine de etkir.

[1]Halk arasında Burnside Önsavı olarak bilinen bu önsav aslında Burnside'dan daha eskidir, Frobenius'a, hatta Cauchy'ye kadar uzanır.

[2]Nitekim, kolayca kanıtlanabileceği üzere, $gG_x \mapsto gx$ fonksiyonu G/G_x sol ötelemeler kümesinden Gx yörüngesine giden bir eşlemedir.

$X \in \Omega$ için, X'in G-yörüngesi GX, elbette X'e izomorf olan çizgelerden oluşur; ne de olsa g, X ile gX arasındaki izomorfizmadır. $G_X = \mathrm{Aut}(X)$ eşitliği de bariz biçimde doğrudur. Demek ki X'e izomorf çizge sayısı,

$$|GX| = \frac{|G|}{|G_X|} = \frac{|G|}{|\,\mathrm{Aut}(X)|} = \frac{n!}{|\,\mathrm{Aut}(X)|}$$

dir.

Şimdi, yukardaki önsavdaki A kümesinin analogu olan,

$$\{(g, X) : gX = X\} = \{(g, X) : g \in \mathrm{Aut}(X)\}$$

kümesinin elemanlarını $g \in G$ üzerine toplayarak hesaplayalım. $g \in G$ olsun. $g \in \mathrm{Aut}(X)$ ise X'in bağıntılar kümesi, X'in her bağıntısı için, bu bağıntının $\langle g\rangle$-yörüngesini de içerir; yani $E(X)$ kümesi $\wp_2(V)$'nin $\langle g\rangle$-yörüngelerinden oluşur. Ve bu koşul sadece gerek değil, ayrıca yeterdir de: Eğer $E(X)$ kümesi $\wp_2(V)$'nin $\langle g\rangle$-yörüngelerinden oluşuyorsa o zaman $g \in \mathrm{Aut}(X)$ olur. Dolayısıyla eğer $\wp_2(V)$'deki $\langle g\rangle$-yörünge sayısı r ise, g tam tamına 2^r tane farklı çizgenin otomorfizmasıdır. Bu r sayısını $y(g)$ olarak gösterelim:

$$y(g) = \wp_2(V)\text{'nin } \langle g\rangle\text{-yörünge sayısı.}$$

Demek ki

$$|A| = \sum_{g\in G} 2^{y(g)}$$

olur. Burnside Önsavı'na göre, Ω'nın G-yörüngesi sayısı, yani birbirine izomorf olmayan çizge sayısı,

$$\frac{1}{n!}\sum_{g\in G} 2^{y(g)}$$

dir. Şimdi bu sayı hakkında genel bir bilgi edinelim:

Önsav C.2. *Ω'nın izomorf olmayan çizge sayısı, yani G-yörüngesi sayısı $\lim_{n\to\infty} o(n) = 0$ eşitliğini sağlayan bir o fonksiyonu için*

$$(1 + o(n))\frac{2^{\binom{n}{2}}}{n!}$$

dir.

Kanıt: Bir $g \in G$ elemanının **desteği**, g'nin sabitlemediği, yani yerinden oynattığı elemanlar kümesidir. Bir g elemanı ne kadar fazla eleman sabitliyorsa, yani desteği ne kadar küçükse, V ve $\wp_2(V)$ kümelerindeki yörüngeleri o kadar küçük, dolayısıyla yörünge sayıları da o kadar büyük olur. Örneğin $\mathrm{Id}_V \in G$ elemanının her yörüngesi tek bir elemandan oluşur, dolayısıyla $\wp_2(V)$

kümesindeki yörünge sayısı (maksimal sayı olan) $\binom{n}{2}$ dir. Eğer $a \neq b \in V$ için $g = (a\,b) \in G$ ikili döngüsüyse, g-yörüngelerin ya 1 ya da 2 elemanı vardır. Nitekim bu durumda g-yörüngeler şunlardır:

1. $\{\{a, b\}\}$,
2. Her $x \in V \setminus \{a, b\}$ için $\{\{a, x\}, \{b, x\}\}$,
3. Her $x, y \in V \setminus \{a, b\}$ için $\{\{x, y\}\}$

Demek ki g-yörüngesi sayısı

$$1 + (n-2) + \binom{n-2}{2}$$

dir. Bu ısınma hareketlerinden sonra ciddi hesaplara geçelim.

$g^n = 1$ ise, bir $\langle g \rangle$-yörüngesinde en fazla n tane eleman vardır, o elemanlar da $X, gX, g^2X, \ldots, g^{n-1}X$ biçiminde yazılan çizgelerdir. (Ama bunlardan bazıları birbirine eşit olabilir.) Ve yörüngelerde ne kadar az eleman varsa, toplam yörünge sayısı o kadar artar. Dolayısıyla, eğer Id_V elemanını saymazsak en fazla yörüngeyi derecesi 2 olan elemanlar verir, çünkü bu elemanların yörüngelerinde ya 1 ya da 2 çizge vardır. Bunlar arasından da en fazla yörünge yukarda ele aldığımız $(a\,b)$ ikili döngüleri tarafından verilir.

Yukarda söylediklerimizden şu çıkar: Desteğinin eleman sayısı $2r$ olan $g \in G$ elemanları arasında yörünge sayısı en büyük olanlar, r tane ikili ayrık döngüden oluşan g'lerdir. Şimdi bu tür bir elemanın yörünge sayısını hesaplayalım. İki elemanlı yörüngeleri teker teker sıralayalım:

1. g'nin desteğinde olan ama aynı döngüde bulunmayan $x \neq y \in V$ için $\{\{x, y\}, \{gx, gy\}\}$ kümesi iki elemanlı bir yörüngedir ve bunlardan

   $$r(r-1)$$

   tane vardır.

2. g'nin desteğinde olan bir x ve g'nin desteğinde olmayan bir y için

   $$\{\{x, y\}, \{gx, y\}\}$$

   kümesi iki elemanlı bir yörüngedir ve bunlardan

   $$r(n-2r)$$

   tane vardır.

Demek ki 2 elemanlı yörünge sayısı

$$r(r-1) + r(n-2r) = r(n-r-1)$$

dır. Tek elemanlı yörünge sayısı da bunların dışında kalanlardır ve onlardan da

$$\binom{n}{2} - 2r(n-r-1)$$

tane vardır. Dolayısıyla toplam g-yörünge sayısı

$$r(n-r-1) + \left(\binom{n}{2} - 2r(n-r-1)\right) = \binom{n}{2} - r(n-r-1)$$

olur.

Şimdi $m \leq n-2$ herhangi bir doğal sayı olsun. m'nin değerini daha sonra işimize geldiği gibi belirleyeceğiz. G'nin elemanlarını üç kümeye ayıralım:

- $\mathcal{C}_1$ sınıfı: Sadece Id_V elemanı. Bu sınıfta 1 tane eleman vardır.
- $\mathcal{C}_2$ sınıfı: Desteği en fazla m elemanlı olan ve Id_V'den değişik elemanlar. Bu sınıfta en fazla

  $$\binom{n}{m} m! < \frac{n!}{(n-m)!} < n^m$$

  tane eleman vardır.
- $\mathcal{C}_3$ sınıfı: Geri kalanlar. Bu sınıfta en fazla

  $$n! < n^n$$

  tane eleman vardır.

Her bir sınıfın elemanlarının yörünge sayısının üstsınırını bulacağız.
$\mathcal{C}_1$ sınıfı için: Id_V'in yörünge sayısı tam tamına

$$2^{\binom{n}{2}}$$

dir.

$\mathcal{C}_2$ sınıfı için: $\mathcal{C}_2$'nin elemanları arasından maksimum yörünge sayısı, bir tek ikili döngüden oluşan elemanlar tarafından elde edilir. Bunların yörünge sayısını yukarda belirlemiştik:

$$\binom{n}{2} - (n-2).$$

$\mathcal{C}_3$ sınıfı için: $\mathcal{C}_3$'ün elemanları arasından maksimum yörünge sayısı, $m/2$ tane ikili döngülerden oluşan elemanlar tarafından elde edilir. Bunların yörünge sayısını da yukarda belirlemiştik:

$$\binom{n}{2} - \frac{m}{2}\left(n - \frac{m}{2} - 1\right) < \binom{n}{2} - \frac{nm}{4}.$$

Demek ki,

$$\begin{aligned}\sum_{g\in G} 2^{y(g)} &< 2^{\binom{n}{2}} + n^m 2^{\binom{n}{2}-(n-2)} + n^n 2^{\binom{n}{2}-nm/4} \\ &= 2^{\binom{n}{2}} \left(1 + n^m 2^{-n+2} + n^n 2^{-nm/4}\right).\end{aligned}$$

Bundan da önsavın kanıtını bitirmek için,

$$n^m 2^{-n+2} + n^n 2^{-nm/4}$$

dizisinin ya da

$$n^m 2^{-n} + n^n 2^{-nm/4}$$

dizisinin limitinin 0 olduğunu kanıtlamanın yeterli olduğu anlaşılıyor. Bu iki ifadenin her birinin limitinin ayrı ayrı 0 olduğunu göstermeliyiz. Bunun için özel bir m seçeceğiz. $c > 4$ ve 2'lik tabanda log fonksiyonu için,

$$m = [c \log n]$$

olsun. Önce birinci terimin 0'a gittiğini kanıtlayalım: $2^{\log n} = n$ eşitliğini kullanarak ve yeterince büyük n alarak,

$$n^m 2^{-n} = \frac{n^m}{2^n} \leq \frac{n^{c \log n}}{2^n} = \frac{2^{c \log^2 n}}{2^n} = 2^{c \log^2 n - n} < 2^{c \log n - n}$$

buluruz. $\lim_{n\to\infty}(c \log n - n) = -\infty$ olduğundan, birinci terimin 0'a gittiği anlaşılır. İkinci terime bakalım şimdi:

$$n^n 2^{-nm/4} = \frac{n^n}{2^{nm/4}} = \frac{n^n}{2^{n(c/4)\log n}} = \frac{n^n}{n^{nc/4}} = n^{n(1-c/4)}$$

ve $1 - c/4 < 0$ olduğundan, ikinci terim de 0'a gider. □

Şimdi artık asimetrik çizgelerin tüm çizgelere oranının, nokta sayısı n sonsuza gittiğinde 1'e gittiğini kanıtayabiliriz.

Girişten μ_n oranını anımsayınız. Bu sayı asimetrik çizgelerin tüm çizgelere oranı olarak tanımlanmıştı. Asimetrik olmayan bir X çizgesinin yörüngesinin eleman sayısı

$$|GX| = \frac{n!}{|\operatorname{Aut} X|} \leq \frac{n!}{2}$$

olduğundan, asimetrik olanların yörüngesinde de tam $n!$ tane eleman bulunduğundan, bir yörüngenin ortalama eleman sayısı,

$$\frac{1}{2^{\binom{n}{2}}} \sum_{X\in\Omega} |GX| \leq \frac{1}{2^{\binom{n}{2}}} \left(\mu_n 2^{\binom{n}{2}} n! + (1-\mu_n) 2^{\binom{n}{2}} \frac{n!}{2}\right) = n! \frac{1+\mu_n}{2}$$

olur. Yörünge sayısı da bir önceki önsav tarafından verildi. Demek ki

$$\left(n!\frac{1+\mu_n}{2}\right)\left((1+o(n))\frac{2^{\binom{n}{2}}}{n!}\right)$$

çarpımı çizge sayısından, yani $2^{\binom{n}{2}}$ sayısından büyüktür:

$$\left(n!\frac{1+\mu_n}{2}\right)\left((1+o(n))\frac{2^{\binom{n}{2}}}{n!}\right) > 2^{\binom{n}{2}}.$$

Bundan,

$$\frac{1+\mu_n}{2}(1+o(n)) > 1$$

çıkar. Çarpmayı ve bariz sadeleştirmeleri yapalım:

$$\mu_n + o(n) + \mu_n o(n) > 1.$$

Ama ayrıca $\lim o(n) = 0$ ve $0 \leq \mu_n \leq 1$ olduğundan, $\lim \mu_n o(n) = 0$ olur. Son iki satırdan,

$$\lim \mu_n \geq 1,$$

yani

$$\lim \mu_n = 1$$

çıkar. Demek ki sonlu çizgelerin çok büyük bir çoğunluğu, hatta tamamına yakını asimetrikmiş. □

Kaynakça

Chris Godsil ve Gordon Royle, **Algebraic Graph Theory**, Springer, Graduate Text in Mathematics 207, 2001.

D. Direkt ve Ters Limit

X herhangi bir küme olsun. X'in bazı altkümelerinden oluşan bir aile alalım: $(X_i)_i$. Bu altkümelerin bileşimini alıp X'in bir başka altkümesini bulabiliriz elbet: $\bigcup_i X_i$. Bu bölümde yapacaklarımız işte bu "bileşim alma" işlemini genelleştirecek.

D.1 Özdeşleştirme

Matematikte, her şeyi daha basit ve daha kullanışlı kılan "özdeşleştirmek" diye bir şey vardır. Sık sık başvurulur özdeşleştirmeye. Bir A kümesi, bir başka kümenin A'ya çok benzeyen bir altkümesiyle "özdeşleştirildiği", böylece eşit olamayan elemanlara eşit muamelesi çekildiği olur. Yapılan özdeşleştirme genellikle o kadar doğaldır ki, ortalama bir vatandaş farkına varmaz bile.

Örneğin bir n tamsayısı, $n/1$ kesirli sayısıyla özdeşleştirilir ve böylece her tamsayıyı bir kesirli sayı olarak görebiliriz. Oysa tamsayılar kümesiyle kesirli sayılar kümesi, başlangıçta birbirinden ayrık kümeler olarak inşa edilir, özdeşleştirmeden sonra doğal sayılar kümesi kesirli sayılar kümesinin altkümesi olarak görülür.

Bir başka örnek: Her gerçel sayı hemen hemen her zaman sabit bir polinomla özdeşleştirilir. Sabit polinomlarla gerçel sayılar arasında bir ayrım gözetilmez, ki aslında gözetilmesi gerekir, ne de olsa gerçel sayı gerçel sayıdır, polinom da polinom.

Liselerde her polinom (en azından katsayıları gerçel sayılar kümesindeyse) bir fonksiyon olarak görülür. Burada da aslında (matematikçiler arasında her zaman pek rağbet görmeyen) bir özdeşleştirme sözkonusudur. Bir polinom asla bir fonksiyon değildir. Ama her polinom bir fonksiyon yaratır ve kimi zaman polinomu yarattığı fonksiyon olarak görmekte bir sakınca yoktur.

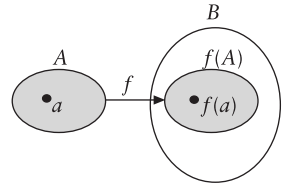
Bir lise matematik kitabında $\mathbb{R}$'nin $\mathbb{R} \times \mathbb{R}$ kümesinin altkümesi olduğu yazıyordu. Bu tamamen yanlıştır. Yazarın yaptığı yanlışı anlamak zor değil, yazar muhtemelen gençliğinde karmaşık sayılara biraz fazla odaklanmış (gerçekten de r gerçel sayısı $r + 0i$ karmaşık sayısıyla özdeşleştirilir) ve kimseye haber vermeden, $\mathbb{R}$ ile $\mathbb{R} \times \mathbb{R}$'nin $\mathbb{R} \times \{0\}$ altkümesini özdeşleştirmiş. Oysa $\mathbb{R}$

ile, örneğin,

$$\{(x, x) : x \in \mathbb{R}\}$$

altkümesini de özdeşleştirebilirdi... Dolayısıyla yazarın hiç de bariz olmayan bir özel özdeşleştirmeyi yaptığını söylemesi gerekiyordu.

Özdeşleştirmek şöyle bir şeydir: A ve B iki küme olsun ve f, A'dan B'ye giden birebir bir fonksiyon olsun. f, elbette A ile $f(A)$ kümeleri arasında bir eşleme tetikler. Bu eşleme kimi zaman öylesine doğal olabilir ki, A'nın bir a elemanıyla B'nin $f(a)$ elemanı arasında bir ayrım yapmak içimizden gelmez,



tam tersine ayrım yapmak nerdeyse günah kategorisine girer. Bu durumda, B kümesi yerine

$$(B \setminus f(A)) \cup A$$

kümesi alınır, yani B'den $f(A)$ koparılıp yerine A yapıştırılır. Eskiden $f(a)$ elemanının B'de gördüğü görevi, bu yeni kümede a elemanı görür. Bu işlem, $f(A)$'yı kesip yerine A'yı dikmek olarak ya da $f(A)$'daki elemanların adlarını değiştirmek olarak görülebilir, hatta bu son yorum daha kullanışlıdır. İşin püf noktası şu: Eski B unutulur ve artık B yerine

$$(B \setminus f(A)) \cup A$$

kümesiyle çalışılır, hem de sanki B eski B imişçesine... Biraz saçma olacak ama, sanki

$$f(a) = a \text{ ve } B = (B \setminus f(A)) \cup A$$

eşitlikleri geçerliymiş gibi davranılır.

Bu yapılana, "A ile $f(A)$ kümelerini f eşlemesi kullanarak özdeşleştirmek" denir (oysa aslında altkümelerden öte elemanlar özdeşleştiriliyordur).

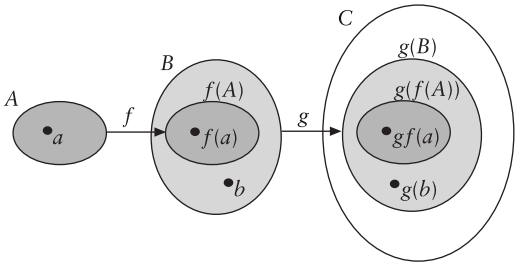
Şimdi bir adım daha gidelim. Aşağıdaki şekilden izleyin. Sadece A ve B kümeleri ve

$$f : A \to B$$

birebir fonksiyonu değil, bir de ayrıca C kümesi ve

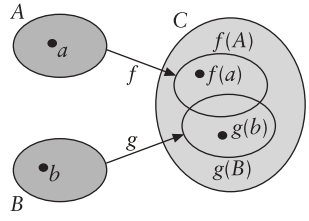
$$g : B \to C$$

birebir fonksiyonu verilmiş olsun. A'yı $f(A)$ ile özdeşleştirip elde edilen yeni B'yi $g(B)$ ile özdeşleştirmek işten bile değildir. Yukarda yaptığımızı iki defa yapmak yeterlidir. Böylece C'nin $g(f(a))$ elemanı a elemanıyla özdeşleşir ve $g(B) \setminus g(f(A))$'nın bir $g(b)$ elemanı b ile özdeşleşir.

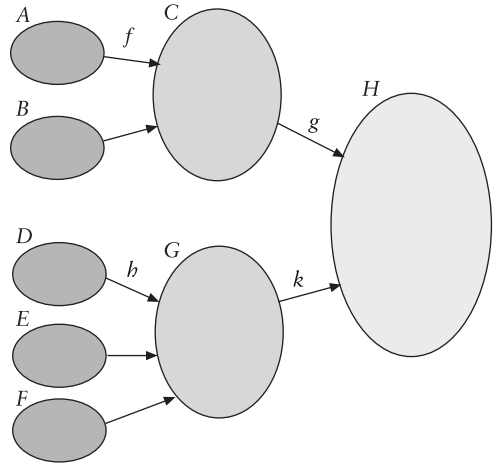


Eğer üç yerine dört küme olursa, işler belki biraz daha zorlaşır ama her seferinde zorlukla kolayca başa çıkabiliriz.

Daha karmaşık özdeşleştirmeler de olabilir. Diyelim A, B ve C diye adlandırılmış üç kümemiz ve $f : A \to C$ ve $g : B \to C$ birebir fonksiyonlarımız var. f'yi kullanarak A ve $f(A)$ kümelerini özdeşleştirebiliriz. g'yi kullanarak B ve $g(B)$ kümelerini de özdeşleştirebiliriz. Ama $f(A) \cap g(B)$'nin elemanlarına ne olacak? Bu elemanlar A'nın mı yoksa B'nin mi elemanıyla özdeşleşecekler? Yanıt: Her ikisiyle birden özdeşleşecekler.



Aşağıdaki şekildeki gibi çok daha karmaşık durumlar da olabilir. Aşağıdaki durumda, imgeleri bir zaman sonra eşit olan elemanlar özdeşleştirilirler.



Örneğin $a \in A$ ile $d \in D$ elemanları

$$g(f(a)) = k(h(d))$$

eşitliğini sağlıyorsa, A'nın a elemanıyla D'nin d elemanı eşleştirilmek istenebilir.

Aslında özdeşleştirmenin gerçekleşmesi için fonksiyonların birebir olmalarına gerek yok. Fonksiyonlar birebir olmasalar da özdeşleştirmeleri yapabiliriz. Hatta kümelerin birbirinden değişik olmalarına da gerek yok, kümelerin hepsi aynı bile olabilirler.

Yapmak istediğimiz şu: Bazı kümeler ve bu kümeler arasında bazı fonksiyonlar verilmiş. Verilen tüm kümelerin bileşimini almak istiyoruz, ancak görüntüleri bir zaman sonra aynı olan elemanları bileşim kümesinde sanki tek bir elemanmış gibi görmek, yani matematikte yaygın olarak kullanılan deyimle, bu elemanları birbirleriyle özdeşleştirmek istiyoruz. Özdeşleştirmek yerine büzüştürmek de diyebilirdik.

Ama dikkat, gereğinden fazla eleman özdeşleştirmek istemiyoruz. Örneğin, abartıp, tüm kümelerdeki tüm elemanları tek bir elemana büzüştürebilirdik... Özdeşleşmesi gereken elemanlar özdeşmeli ama özdeşleşmemesi gereken elemanlar da özdeşmemeli. Yani kıvamı tutturmalıyız.

İki örnek alalım. Birincisi uydurma bir örnek, ikincisiyse klasik.

Örnekler

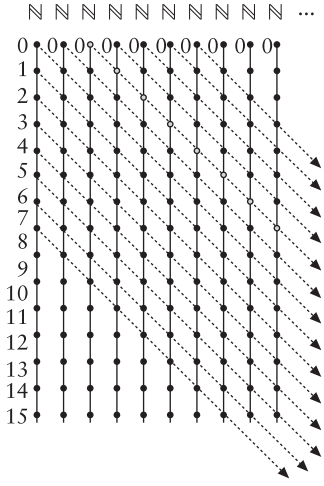
D.1. $I = \mathbb{N}$ olsun ve bildiğimiz sıralamayla sıralanmış olsun. Her $i \in I$ için, $X_i = \mathbb{N}$ ve

$$\varphi_i : X_i \to X_{i+1}$$

fonksiyonu

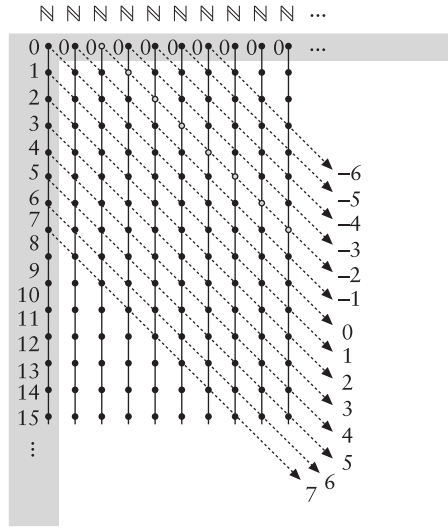
$$\varphi_i(x) = x + 1$$

formülüyle tanımlanmış olsun. Kümelerin ve fonksiyonların resimleri aşağıda:



X_0'ın 0 elemanıyla X_1'in 1 elemanı ve X_2'nin 2 elemanı ve X_3'ün 3 elemanı ve genel olarak X_n'in n elemanı özdeşleştirilecekler çünkü φ_0, X_0'ın 0 elemanını X_1'in 1 elemanına götürüyor, φ_1, X_1'ın 1 elemanını X_2'nin 2 elemanına götürüyor vs.

Bunun gibi X_1'in 0 elemanıyla X_2'nin 1 elemanı, X_3'ün 2 elemanı, X_4'ün 3 elemanı ve genel olarak X_n'in $n-1$ elemanı özdeşleşecekler.
Şekillerdeki her okun üstünden geçtiği noktalar birbirleriyle özdeşleşip nihai kümede (bir tür bileşim kümesinde) tek bir eleman olacaklar. Yani nihai kümede her ok için ayrı bir eleman olacak.



Elde edilecek nihai küme, "artı 1" fonksiyonlarını da kale alınca, belli ki $\mathbb{Z}$'ye benzeyecek. X_0'daki (yani ilk $\mathbb{N}$ kümesindeki) her eleman için nihai kümede bir eleman gerekiyor, çünkü bu elemanlar birbirleriyle özdeşleşemezler. Bir de nihai kümede, her $i > 0$ için, $0 \in X_i$ elemanının özdeşleşeceği ayrı bir eleman gerekiyor, çünkü bunlar ne aralarında ne de daha öncekilerle özdeşleşebilirler. Resmi yukarda.

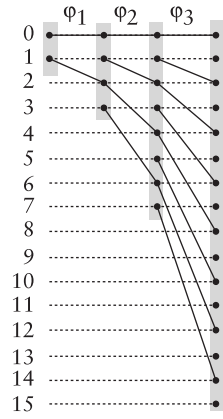
D.2. **Prüfer p-Grubu.** Teoriye girişmeden önce çok basit olmayan bir örnek verelim. Her $k > 0$ doğal sayısı ve her x tamsayısı için

$$\varphi_k([x]_k) = [px]_{k+1}$$

formülüyle tanımlanmış olan

$$\varphi_k : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^{k+1}\mathbb{Z}$$

fonksiyonunu ele alalım. Burada $[x]_k$, x'in $\mathbb{Z}/p^k\mathbb{Z}$ kümesindeki imgesini temsil etmektedir. φ_k fonksiyonlarının birebir olduklarını kanıtlamak zor değildir.



Yukarıdaki şekilde $p = 2$ ve $k = 1, 2, 3$ için φ_k fonksiyonlarını göstermeye çalıştık. Amacımız, örneğin,

$\mathbb{Z}/2\mathbb{Z}$'nin [1] elemanını
$\mathbb{Z}/4\mathbb{Z}$'nin [2] elemanını
$\mathbb{Z}/8\mathbb{Z}$'nin [4] elemanını

birbirleriyle özdeşleştirmek. (Gereksiz göstergeçleri attık.) Bunun gibi,

$\mathbb{Z}/4\mathbb{Z}$'nin [3] elemanını
$\mathbb{Z}/8\mathbb{Z}$'nin [6] elemanını
$\mathbb{Z}/16\mathbb{Z}$'nin [12] elemanını
...

birbirleriyle özdeşleştirmek istiyoruz. Bir başka deyişle, $\mathbb{Z}/2^k\mathbb{Z}$ kümelerinin tüm k'lar için bileşimini alıp, bu bileşimdeki her $[a]_k \in \mathbb{Z}/2^k\mathbb{Z}$ elemanını $[2a]_{k+1} \in \mathbb{Z}/2^{k+1}\mathbb{Z}$ elemanıyla özdeşleştirmek istiyoruz. Her maksimum ok silsilesini tek bir eleman olarak görmek de diyebiliriz yapmak istediğimiz şeye; böylece bileşimdeki her eleman, içinde bulunduğu (yegâne) ok silsilesiyle özdeşleştirebiliriz. Örneğin,

$$[24]_6 \in \mathbb{Z}/2^6\mathbb{Z}$$

elemanını

$$[3]_2 \to [6]_4 \to [12]_5 \to [24]_6 \to [48]_7 \to \cdots$$

maksimal ok silsilesiyle özdeşleştirebiliriz. (Tam bunu yapmayacağız ama yapabilirdik; buna çok benzer bir şey yapacağız.)

Tam ne yapacağımızı çıtlatalım: $0 \leq a < 2^k$ için, $\mathbb{Z}/2^k\mathbb{Z}$ kümesinin $[a]_k$ elemanını $a/2^k$ kesirli sayısıyla özdeleştireceğiz.

Başlıyoruz: $\mathbb{Z}_{2^\infty}$, $[0, 1)$ aralığındaki, paydası 2'nin bir kuvveti olarak yazılabilen kesirli sayılar kümesi olsun. Bir başka deyişle

$$\mathbb{Z}_{2^\infty} = \{a/2^k : k \in \mathbb{N} \setminus \{0\} \text{ ve } a = 0, 1, \ldots, 2^k - 1\}$$

olsun. Şimdi her k ve her $a = 0, 1, 2, \ldots, 2^k - 1$ için $\mathbb{Z}/2^k\mathbb{Z}$ kümesinin $[a]_k$ elemanını $\mathbb{Z}_{2^\infty}$ kümesinin $a/2^k$ elemanıyla özdeşleştirelim. Söylediklerimiz daha iyi anlaşılsın diye,

$$\psi_k : \mathbb{Z}/2^k\mathbb{Z} \to \mathbb{Z}_{2^\infty}$$

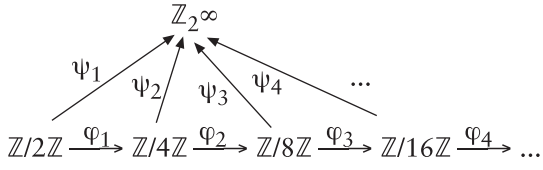
fonksiyonunu

$$\psi_k([a]_k) = a/2^k$$

kuralıyla tanımlayalım ve $\mathbb{Z}/2^k\mathbb{Z}$ kümesinin bir $[a]_k$ elemanını $\mathbb{Z}_{2^\infty}$ kümesinin

$$\psi_k([a]_k) = a/2^k$$

elemanıyla özdeşleştirelim.



$\mathbb{Z}_{2^\infty}, \mathbb{Z}/2^k\mathbb{Z}$ kümelerinin bir anlamda bileşimidir;
φ_k fonksiyonlarıyla birbirlerine bağlantılanmış elemanlar,
$\mathbb{Z}_{2^\infty}$ kümesinde tek bir elemanmış gibi gösterilmişlerdir
ψ'ler özdeşleştirme fonksiyonlarıdır.
Her k için $\psi_{k+1} \circ \varphi_k = \psi_{k+1}$ eşitliği sağlanır.

şekildeki artı eksi bileşke olacak xxxxx

Böylece istediğimiz olur çünkü (yukardaki şekilden yaptıklarımızı takip edebilirsiniz),
1. Hem $\mathbb{Z}/2^k\mathbb{Z}$ kümesinin $[a]_k$ elemanı, hem de $\mathbb{Z}/2^{k+1}\mathbb{Z}$ kümesinin $[2a]_{k+1}$ elemanı, $\mathbb{Z}_{2^\infty}$ kümesinin aynı elemanıyla, $a/2^k$ elemanıyla özdeşleştirilmiştir.
2. $\mathbb{Z}_{2^\infty}, \psi_k(\mathbb{Z}/2^k\mathbb{Z})$ kümelerinin bileşimidir.
Bu yaptıklarımızı 2'den herhangi bir p asalına genelleştirmek işten bile değildir. Hatta p'nin asal olmasına bile gerek yoktur. (Ama uygulamada p hep bir asaldır.)

Birazdan bütün bunları kuramsal olarak yapacağız. Sayfanın en altındaki şekildeki gibi bir durum sözkonusu olacak ve şeklin en sağındaki soru işaretli kümeyi bulmaya çalışacağız. Şekilde aynı küme birçok kez belirebilir, her kümenin değişik olmasına neden yok.

"Özdeşleştirmek" diyen aslında "denklik ilişkisi" der, çünkü a ile b elemanlarının özdeşleştirildiğini $a \equiv b$ simgesiyle gösterirsek, belli ki şu önermeler doğru olur (ya da olmalı):

$$a \equiv a,$$
$$a \equiv b \text{ ise } b \equiv a,$$
$$a \equiv b \text{ ve } b \equiv c \text{ ise } a \equiv c,$$

ki bunlar da bir denklik ilişkisinin tanmının koşullarıdır.

Okura yeterince sezgi kazandırdığımızı düşünerek artık matematiğe geçelim. Elde edeceğimiz nihai kümeye kümeler ve fonksiyonlar sisteminin ***direkt*** ya da ***tümevarımsal limit*** adı verilir.

D.2 Direkt Limit

Önce verilerimizi toparlayalım.

I yarısıralı bir küme olsun, yani I üstünde, her $i, j, k \in I$ için,

$$\begin{aligned} &i \leq i, \\ &i \leq j \text{ ve } j \leq i \Rightarrow i = j, \\ &i \leq j \text{ ve } j \leq k \Rightarrow i \leq k \end{aligned}$$

özelliklerini sağlayan bir $\leq$ ikili ilişkisi olsun. (Yukarda verdiğimiz örnekte $I = \mathbb{N}$ ve sıralama da bildiğimiz sıralamaydı.) Bir de ayrıca I'nın $\leq$ yarısıralamasının ***yönlendirilmiş*** olduğunu, yani her $i, j \in I$ için, $i \leq k$ ve $j \leq k$ eşitsizliklerini sağlayan bir $k \in I$ olduğunu varsayalım. Bu I kümesi göstergeç kümemiz olacak. Şimdi de kümelerimizi ve aralarındaki fonksiyonları belirleyelim.

$(X_i)_{i \in I}$ herhangi bir küme ailesi olsun. Her $i \leq j$ göstergeçi için,

$$\varphi_{ij} : X_i \to X_j$$

bir fonksiyon olsun. Ve bu $(\varphi_{ij})_{ij}$ fonksiyon kümesi üzerine şu varsayımı yapalım: Her $i < j < k$ göstergeci için,

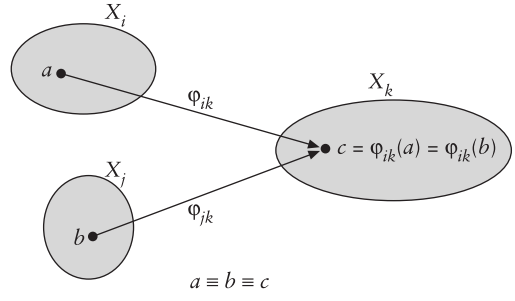
$$\varphi_{ii} = \mathrm{Id}_{X_i} \text{ ve } \varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}.$$

Tüm bu veri,

$$(X_i, \varphi_{ij})_{i<j \in I}$$

olarak simgelenir ve adına ***direkt sistem*** denir.

Amacımız bu X_i kümelerinin bileşimini almak ama φ_{ij} fonksiyonları altında aynı elemana giden elemanlar arasında bir ayrım gözetmemek, yani bunları birbirleriyle özdeşleştirmek.



Değişik i'ler için X_i kümeleri kesişebilirler, hatta Örnek 1'de olduğu gibi X_i kümelerinin bazıları aynı küme olabilirler. Bunu engellemek için X_i yerine $X_i \times \{i\}$ kümesini alıp bu ayrık kümelerin bileşimini alalım.

$$X = \bigcup_{i \in I} (X_i \times \{i\})$$

olsun. (Özdeşleştirmek yerine ayrıştırdığımızın farkındayız, özdeşleştirmeye birazdan geçeceğiz. Amacımız değişik göstergeçlerle ifade edilmiş X_i kümelerinde bulunan aynı elemanları özdeşleştirmek değil, bunu yapmak oldukça kolaydır, bunun için X_i'lerin bileşimini almak yeterdir; amacımız φ fonksiyonları altında imgesi aynı olan, ya da imgesi bir zaman sonra aynı olan elemanları özdeşleştirmek.) X kümesi üzerine şu ikili ilişkiyi tanımlayalım:

$$(x,i) \equiv (y,j)$$

ancak ve ancak i ve j'den büyükeşit bir k için,

$$\varphi_{ik}(x) = \varphi_{jk}(y)$$

ise. Eğer $i \leq j$ ise ($\equiv$ ilişkisinin tanımında $k = j$ alın),

$$(x,i) \equiv (\varphi_{ij}(x), j)$$

ilişkisinin doğru olduğunu dikkatlerinize sunarız.

Tanımladığımız bu ilişki bir denklik ilişkisidir. Nitekim:

- Her $i \in I$ için $\varphi_{ii}(x) = \mathrm{Id}_{X_i}(x) = x$ olduğundan, her $x \in X_i$ için $(x,i) \equiv (x,i)$ olur.
- Eğer $(x,i) \equiv (y,j)$ ise ve $k \geq i$ ve $k \geq j$ eşitsizliklerini sağlayan bir k göstergeci için $\varphi_{ik}(x) = \varphi_{jk}(y)$ oluyorsa, aynı k göstergeci $(y,j) \equiv (x,i)$ denkliğini göstermek için de kullanılabilir.
- $(x,i) \equiv (y,j)$ ve $(y,j) \equiv (z,k)$ olsun. u ve v göstergeçleri

$$\varphi_{iu}(x) = \varphi_{ju}(y) \text{ ve } \varphi_{jv}(y) = \varphi_{kv}(z)$$

eşitliklerini sağlasın. $w \in I$, hem u hem de v'den büyük bir göstergeç olsun. O zaman,

$$\begin{aligned}\varphi_{iw}(x) &= (\varphi_{uw} \circ \varphi_{iu})(x) = \varphi_{uw}(\varphi_{iu}(x)) = \varphi_{uw}(\varphi_{ju}(y)) = (\varphi_{uw} \circ \varphi_{ju})(y) \\ &= \varphi_{jw}(y) = (\varphi_{vw} \circ \varphi_{jv})(y) = \varphi_{vw}(\varphi_{jv}(y)) = \varphi_{vw}(\varphi_{kv}(z)) = \varphi_{kw}(z)\end{aligned}$$

olur, dolayısıyla $(x,i) \equiv (z,k)$ olur.

Böylece $\equiv$ ilişkisinin bir denklik ilişkisi olduğu kanıtlandı.

$(x,i) \in X_i \times \{i\}$ elemanının denklik sınıfını $[x,i]$ olarak gösterelim:

$$[x,i] = \{(y,j) : y \in X_j \text{ ve } (x,i) \equiv (y,j)\}.$$

Demek ki her $i \leq j$ için,

$$[x,i] = [\varphi_{ij}(x), j]$$

olur.

Son olarak $X/\equiv$ kümesini alalım:

$$X/\equiv = \{[x,i] : i \in I, x \in X_i\}$$

İşte bu, tam istediğimiz kümedir! Bu bölümün devamında okuru buna ikna etmeye çalışacağız.

X_i kümesinin bir x elemanını, $X/\equiv$ kümesindeki $[x,i]$ elemanıyla özdeşleştireceğiz. Bu özdeşleştirmeyi matematiksel olarak ifade edebilmek amacıyla,

$$\Psi_i : X_i \to X/\equiv$$

fonksiyonunu

$$\Psi_i(x) = [x,i]$$

formülüyle tanımlayalım. X_i'nin x elemanının $X/\equiv$ kümesinin $\Psi_i(x)$ elemanıyla özdeşleştirilmiş olduğunu hayal edin.

İşte bu $X/\equiv$ kümesi aradığımız kümedir.

Yazının başında amaçladığımız hedefe ulaştığımızı göstermek için iki şey kanıtlamalıyız:

A1. *Eğer φ_{ij} fonksiyonları birebirse, Ψ_i fonksiyonu da birebirdir.*

Nitekim $x, y \in X_j$ için $\Psi_i(x) = \Psi_i(y)$ olsun. O zaman $[x,i] = [y,i]$, yani $(x,i) \equiv (y,i)$, yani bir $k \geq i$ için $\varphi_{ik}(x) = \varphi_{ik}(y)$ olur. Ama φ_{ik} birebir olduğundan, bundan $x = y$ çıkar.

A2. *$X/\equiv$ kümesi (X_i'lerin olmasa da) $\Psi_i(X_i)$'lerin bileşimidir. Yani*

$$X/\equiv = \bigcup_{i \in I} \Psi_i(X_i)$$

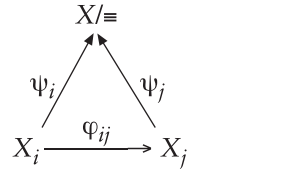
eşitliği geçerlidir.

Bunun doğruluğu tanımlardan hemen çıkıyor:

$$X/\equiv = \{[x,i] : i \in I, x \in X_i\} = \{\Psi_i(x) : i \in I, x \in X_i\} = \bigcup_{i \in I} \Psi_i(X_i).$$

Önemli bir özellik daha:

A3. *Her $i \leq j \in I$ için, $\Psi_j \circ \varphi_{ij} = \Psi_i$.*



Her $i \leq j$ için $\psi_j \circ \varphi_{ij} = \psi_j$ eşitliği sağlanır.

± yerine ∘ olacak xxxxx

Nitekim her $x \in X_i$ için,

$$(\Psi_j \circ \varphi_{ij})(x) = \Psi_j\left(\varphi_{ij}(x)\right) = [\varphi_{ij}(x), j] = [x, i] = \Psi_i(x)$$

olur.

Bu son özellikten şu çıkar: $x \in X_i$ elemanıyla $\varphi_{ij}(x) \in X_j$ elemanı, $X/\equiv$ kümesinin aynı elemanıyla, $\Psi_i(x)$ elemanıyla özdeşleştirilmiştir.

$X/\equiv$ kümesine $(X_i, \varphi_{ij})_{i<j\in I}$ direkt sisteminin ***direkt*** ya da ***tümevarımsal limiti*** adı verilir ve $X/\equiv$ yerine

$$\varinjlim (X_i, \varphi_{ij})_{i<j\in I}$$

yazılır. Eğer kolaylık karışıklığa neden olmayacaksa $\varinjlim (X_i, \varphi_{ij})_{i<j\in I}$ yerine

$$\varinjlim X_i$$

yazılır. Biz bir süre (gerçek tanımı verinceye dek) $X/\equiv$ yazılımını kullanacağız. Ψ_j fonksiyonlarına ***özdeşleştirme fonksiyonları*** adı verilebilir.

Yazının en son bölümünde direkt limitin tanımını hafifçe değiştireceğiz ve yukardaki $X/\equiv$ kümesi direkt limitlerden sadece biri olacak.

Okur, umarız, direkt limitin tanımının ne kadar doğal olduğunu görmüştür. Nerdeyse bileşim kadar doğal. O kadar doğal ki tanım başka türlü yapılamazdı!.. Bu kadar doğal bir tanımın bazı olağanüstü sonuçları olmalı.

D.3 Direkt Limitin Evrensel Özelliği

Yukardaki gibi bir

$$(X_i, \varphi_{ij})_{i<j\in I}$$

direkt sistemi verilmiş olsun. $X/\equiv$ kümesi ve $\Psi_i : X_i \to X/\equiv$ fonksiyonları da bir önceki bölümde tanımlandıkları gibi olsun. Her $i \leq j \in I$ için, bir önceki bölümde kanıtladığımız

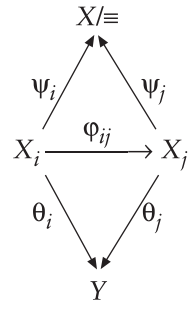
$$\Psi_j \circ \varphi_{ij} = \Psi_i$$

eşitliğini anımsayın.

Bütün bunların dışında herhangi bir Y kümesi ve her $i \leq j \in I$ için

$$\theta_j \circ \varphi_{ij} = \theta_i$$

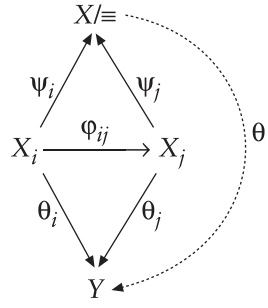
eşitliklerini sağlayan $\theta_i : X_i \to Y$ fonksiyonları verilmiş olsun. (Bkz. aşağıdaki şekil.)



Öyle bir $\theta : X/\equiv \to Y$ fonksiyonu bulacağız ki, her $i \in I$ için

$$\theta \circ \Psi_i = \theta_i$$

eşitliği sağlanacak. (Bkz. aşağıdaki şekil.)



Bu özellik, direkt limitin ***evrensel özelliği*** olarak bilinir.

Sağlanmasını istediğimiz $\theta \circ \Psi_i = \theta_i$ eşitliği bize aslında $\theta : X/\equiv \to Y$ fonksiyonunun tek bir biçimde tanımlanması gerektiğini söylüyor. Nitekim, madem ki $\theta \circ \Psi_i = \theta_i$ eşitliği sağlanmalı, o zaman her $x \in X_i$ için

$$\theta_i(x) = (\theta \circ \Psi_i)(x) = \theta(\Psi_i(x)) = \theta([x, i])$$

olmalı, yani $\theta : X/\equiv \to Y$ fonksiyonu

$$\theta([x, i]) = \theta_i(x)$$

formülüyle tanımlanmalı. Bunun gerçekten bir tanım olduğunu gösterelim. $x \in X_i$ ve $y \in X_j$ için

$$[x, i] = [y, j]$$

olsun. O zaman

$$(x, i) \equiv (y, j)$$

olur ve tanıma göre i ve j'den büyükeşit bir $k \in I$ için

$$\varphi_{ik}(x) = \varphi_{jk}(y)$$

olur. Demek ki,

$$\theta_i(x) = (\theta_k \circ \varphi_{ik})(x) = \theta_k(\varphi_{ik}(x)) = \theta_k(\varphi_{jk}(y)) = (\theta_k \circ \varphi_{jk})(y) = \theta_j(y),$$

yani

$$\theta_i(x) = \theta_j(y).$$

Sonuç olarak,

$$[x,i] = [y,j] \Rightarrow \theta_i(x) = \theta_j(y)$$

önermesini kanıtladık. Bundan da,

$$\theta([x,i]) = \theta_i(x)$$

formülünü yazmaya hakkımız olduğu çıkar. Böylece tanımlanan $\theta : X/\equiv \to Y$ fonksiyonu elbette her $i \in I$ için

$$\theta \circ \Psi_i = \theta_i$$

eşitliğini sağlar.

Direkt limitin dördüncü özelliğini kanıtladık:

A4. *Eğer bir Y kümesi ve $\theta_j \circ \varphi_{ij} = \theta_i$ eşitliklerini sağlayan $\theta_i : X_i \to Y$ fonksiyonları verilmişse, o zaman her $i \in I$ için $\theta \circ \Psi_i = \theta_i$ eşitliğini sağlayan bir ve bir tane $\theta : X/\equiv \to Y$ fonksiyonu vardır.*

Örnekler

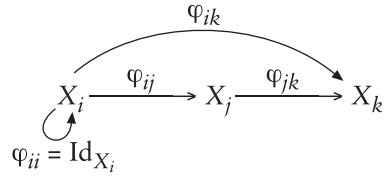
D.3. Bölümün ta başında verdiğimiz en basit örneğe geri dönelim. X herhangi bir küme olsun. X'in bazı altkümelerinden oluşan bir aile alalım: $(X_i)_i$. Eğer her $i \leq j$ için $X_i \subseteq X_j$ ise, $\varphi_{ij} : X_i \to X_j$ fonksiyonu

$$\varphi_{ij}(x) = x$$

olarak tanımlansın. O zaman $\varinjlim X_i$ aynen X_i kümelerinin bileşimidir ve $\Psi_i(x) = x$ olarak tanımlanır.

D.4. Eğer I'nın en büyük elemanı varsa ve bu elemana m dersek, yukarda bulunan $\varinjlim X_i$ kümesinin bu X_m'den pek bir farkı yoktur ve $\Psi_i = \varphi_{im}$ olarak alınabilir.

Teorem D.1 (Ana Teorem)**. i.** *Bir $(X_i, \varphi_{ij})_{i<j\in I}$ direkt sistemi verilmiş olsun.*

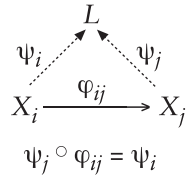


Veri : $\varphi_{ii} = \mathrm{Id}_{X_i}$ ve $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$

Öyle bir L kümesi ve her $i \leq j \in I$ için

$$\Psi_j \circ \varphi_{ij} = \Psi_i$$

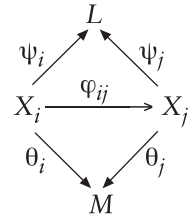
eşitliklerini sağlayan öyle $\Psi_i : X_i \to L$ fonksiyonları vardır ki,



her M kümesi ve

$$\theta_j \circ \varphi_{ij} = \theta_i$$

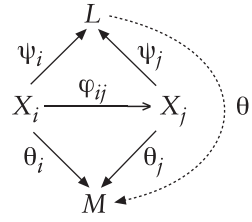
eşitliklerini sağlayan her $(\theta_i : X_i \to M)_i$ fonksiyon ailesi için,



xxxx $\pm$ işreti $\circ$ olacak.

$$\theta \circ \Psi_i = \theta_i$$

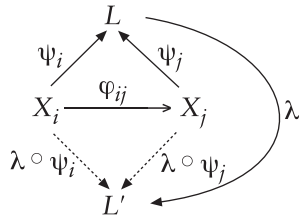
eşitliklerini sağlayan bir ve bir tane $\theta : L \to M$ fonksiyonu vardır. [Evrensel özellik]



ii. *Eğer $(L, \Psi_i : X_i \to L)_i$ ailesi yukardaki evrensel özelliği sağlıyorsa ve $\lambda : L \to L'$ herhangi bir eşlemeyse, o zaman*

$$\left(L', \lambda \circ \Psi_i : X_i \to L'\right)_i$$

ailesi de evrensel özelliği sağlar.

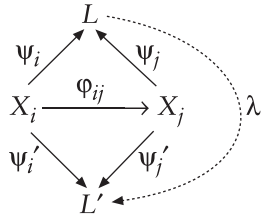


xxxx ± işreti ∘ olacak.

iii. *Eğer* $(L, \Psi_i : X_i \to L)_i$ *ailesinin sağladığı bu evrensel özelliği bir de ayrıca* $(L', \Psi_i' : X_i \to L')_i$ *ailesi de sağlıyorsa, o zaman öyle bir* $\lambda : L \to L'$ *eşlemesi vardır ki, her* $i \in I$ *için,*

$$\Psi_i' = \lambda \circ \Psi_i$$

olur.



Kanıt: i. Teoremin birinci kısmını zaten kanıtlamıştık: L kümesi $X/\equiv$ olsun ve $\Psi_i : X_i \to L$ fonksiyonlarını daha önce tanımladığımız gibi alın.
ii. $(L, \Psi_i : X_i \to L)_i$ ailesi evrensel özelliği sağlasın ve $\lambda : L \to L'$ bir eşleme olsun.

$$\big(L', \lambda \circ \Psi_i : X_i \to L'\big)_i$$

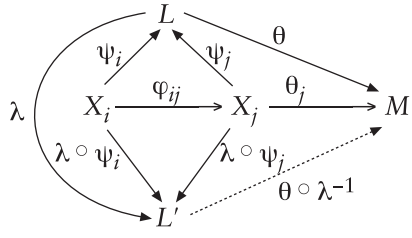
ailesinin de evrensel özelliği sağladığını kanıtlamak istiyoruz. Elbette,

$$(\lambda \circ \Psi_i) \circ \varphi_{ij} = \lambda \circ (\Psi_i \circ \varphi_{ij}) = \lambda \circ \Psi_j$$

eşitliği sağlanır. Şimdi M bir küme ve $\theta_i : X_i \to M$ fonksiyonları

$$\theta_j \circ \varphi_{ij} = \theta_i$$

eşitliklerini sağlasın.



xxxx ± işreti ∘ olacak.

Yukardaki şekilden takip edin. $\theta \circ \lambda^{-1} : L' \to M$ fonksiyonuna bakalım. Her i için,

$$\left(\theta \circ \lambda^{-1}\right) \circ (\lambda \circ \Psi_i) = \theta \circ \Psi_i = \theta_i$$

olur. İstediğimiz kanıtlanmıştır.

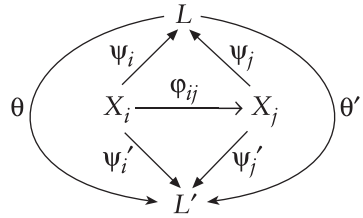
iii. Şimdi de hem $(L, \Psi_i : X_i \to L)_i$ ailesinin hem de $(L', \Psi'_i : X_i \to L')_i$ ailesinin evrensel özelliği sağladığını varsayalım. Birinci sistem evrensel özelliği sağladığından, evrensel özelliğin tanımında $M = L'$ ve $\theta_i = \Psi'_i$ alarak,

$$\theta \circ \Psi_i = \Psi'_i$$

eşitliklerini sağlayan bir $\theta : L \to L'$ fonksiyonunun olduğunu buluruz. İkinci sistem de evrensel özelliği sağladığından, evrensel özelliğin tanımında bu sefer $M = L$ ve $\theta_i = \Psi_i$ alarak,

$$\theta' \circ \Psi'_i = \Psi_i$$

eşitliklerini sağlayan bir $\theta' : L' \to L$ fonksiyonunun olduğunu buluruz.



Şimdi $\theta' \circ \theta : L \to L$ fonksiyonu, her i için,

$$\left(\theta' \circ \theta\right) \circ \Psi_i = \theta' \circ (\theta \circ \Psi_i) = \theta' \circ \Psi'_i = \Psi_i,$$

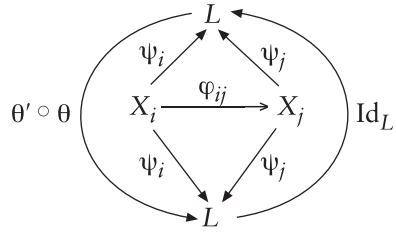
yani

$$\left(\theta' \circ \theta\right) \circ \Psi_i = \Psi_i$$

eşitliğini sağlar. Ayrıca $\mathrm{Id}_L : L \to L$ fonksiyonu da, her i için,

$$\mathrm{Id}_L \circ \Psi_i = \Psi_i$$

eşitliğini sağlar.



∘ işareti yanlış. xxx uniicode'da olacak, daha küçük olmalı.

Ama evrensel özelliğe göre (tanımda $M = L$ ve $\theta_i = \Psi_i$ alın) bu tür eşitlikleri sağlayan fonksiyon biriciktir. Demek ki $\theta' \circ \theta = \mathrm{Id}_L$ olmalı. Aynı nedenden $\theta \circ \theta' = \mathrm{Id}_{L'}$ olur. Demek ki θ ve θ' birbirinin tersi eşlemelerdir. $\lambda = \theta$ alalım. İstenen $\Psi'_i = \lambda \circ \Psi_i$ eşitliği elbette sağlanır. □

Verilmiş bir $(X_i, \varphi_{ij})_{i<j\in I}$ direkt sistemi için, bu özelliği sağlayan bir

$$(L, \Psi_i : X_i \to L)_i$$

ailesi ana teoremde görüldüğü gibi çok güçlü bir anlamda biriciktir. Böyle bir aileye $(X_i, \varphi_{ij})_{i<j\in I}$ direkt sisteminin ***direkt limiti*** adı verilir. Direkt limiti

$$\varinjlim (X_i, \varphi_{ij})_{i<j\in I}$$

olarak yazacağız (direkt limitlerden herhangi biri anlamında). Eğer kolaylık olacaksa ve karışıklığa neden olmayacaksa $\varinjlim (X_i, \varphi_{ij})_{i<j\in I}$ yerine

$$\varinjlim X_i$$

yazılır.

Sonuç D.2. *Yukardaki varsayım ve yazılımlarla,*
i. $L = \cup_{i\in I}\Psi_i(X_i)$ *eşitliği geçerlidir.*
ii. *Eğer* φ_{ij} *fonksiyonları birebirse,* Ψ_i *fonksiyonları da birebirdir.*
iii. $a \in X_i$ *ve* $b \in X_j$ *olsun.* $\Psi_i(a) = \Psi_j(b)$ *eşitliği için yeter ve gerek koşul, hem* i*'den hem de* j*'den büyükeşit bir* k *için* $\varphi_{ik}(a) = \varphi_{jk}(b)$ *eşitliğinin geçerli olmasıdır.*

Kanıt: Tüm söylenenler $L = X/\equiv$ ve $\Psi_i(x) = [x, i]$ fonksiyonları için geçerlidir. Dolayısıyla Ana Teorem'den dolayı aynı özellikler herhangi bir direkt limit için de geçerlidir. Bu kanıtın ayrıntılarını okura bırakıyoruz.
(i)'in bir başka kanıtı: X_i'lerin en az birinin boşküme olmadığını ve L'de 1'den fazla eleman olduğunu varsayabiliriz. $L' = \cup_{i\in I}\Psi_i(X_i)$ ve $\Psi'_i : X_i \to L'$ fonksiyonu

$$\Psi'_i(x) = \Psi_i(x)$$

eşitliğiyle verilmiş olsun. Evrensel özelliğe göre, $\theta \circ \Psi_i = \Psi'_i$ eşitliğini sağlayan bir ve bir tane $\theta : L \to L'$ vardır. Eğer $L' \subset L$ olsaydı, o zaman bir $u \in L \setminus L'$ için, diğer değerlere dokunmadan, $\theta(u)$ tanımını değişik biçimlerde yapabilirdik ve $\theta \circ \Psi_i = \Psi'_i$ eşitliği bozulmazdı; ki bu da θ'nın biricikliğiyle çelişir. □

Dileyen okur, direkt limitin kümesini en başta tanımladığımız gibi $X/\equiv$ olarak alabilir; tabii o zaman $\Psi_i(x) = [x, i]$ olarak tanımlanmak zorundadır. Aşağıda direkt limiti $X/\equiv$ olarak almayacağız, bunun yerine Sonuç D.2'ye başvuracağız. Doğrusu direkt limiti $X/\equiv$ olarak alsaydık kanıtlarımız birazcık daha somut ve anlaşılır olurdu.

D.4 Cebirsel Yapılarda Direkt Limit

Eğer her X_i kümesi üzerinde grup, halka, cisim, R-modül, R-cebiri gibi cebirsel bir yapı varsa ve X_i'ler arasındaki φ_{ij} fonksiyonları söz konusu olan yapıya göre birer homomorfiyse, o zaman $\varinjlim X_i$ direkt limiti üzerine "olabilecek en doğal biçimde" aynı cebirsel yapı tanımlanabilir ve bu yapıya göre bir önceki bölümde bulunan Ψ_i fonksiyonları birer homomorfi olur. Ayrıca geçen altbölümde sözünü ettiğimiz evrensel özellik bu kapsama da uyum sağlar. Bir başka deyişle, Ana Teorem'deki "küme" yerine "grup, halka, modül" gibi uygun olan cebirsel yapıyı yazarsak ve "fonksiyon" yerine uygun cebirsel yapının morfizmasını yazarsak, teorem geçerliliğini korur. Bu sonucu sadece gruplar için yazıp kanıtlayacağız. Diğer yapılar için kanıt çok benzerdir ve okura bırakılacaktır.

Örnek D.2'deki $\mathbb{Z}_{p^\infty}$ (ki aslında bir gruptur, ***Prüfer p-grubu*** olarak bilinir) aslında yapacaklarımıza verilebilecek en standart örnektir.

Teorem D.3. *$(X_i, \varphi_{ij})_{i<j\in I}$ bir direkt sistem olsun. Ayrıca her X_i'nin bir grup olduğunu ve her $\varphi_{ij} : X_i \to X_j$ fonksiyonunun bir grup homomorfizması olduğunu varsayalım.*

$$(L, \Psi_i : X_i \to L)_i$$

ailesi bu sistemin bir direkt limiti olsun. O zaman L üzerine öyle bir ve bir tek grup yapısı konulabilir ki $\Psi_i : X_i \to L$ fonksiyonları grup morfizmaları olur. Ayrıca her M grubu ve

$$\theta_j \circ \varphi_{ij} = \theta_i$$

eşitliklerini sağlayan her $(\theta_i : X_i \to M)_i$ grup morfizması ailesi için öyle bir ve bir tane $\theta : L \to M$ grup morfizması vardır ki her $i \in I$ için

$$\theta \circ \Psi_i = \theta_i$$

olur. Ayrıca eğer $(L', \Psi'_i : X_i \to L')_i$ bu özelliği sağlayan bir başka sistemse, Ana Teorem iii'te bulunan λ bir grup izomorfizması olur.

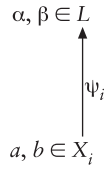
Kanıt: L üzerinde bir grup yapısı tanımlayacağız ve daha sonra Ψ_i'lerin bir grup homomorfizması olduklarını göstereceğiz. Grup yapısı tanımlamak biraz zaman alacak.

$\alpha, \beta \in L$ olsun. $\alpha\beta$ diye bir eleman tanımlamak istiyoruz, ki L üzerine bir grup yapısından bahsedebilelim. Önce bir sav:

Sav 1. *$\alpha, \beta \in L$ ise öyle bir $i \in I$ göstergeci ve $a, b \in X_i$ elemanları vardır ki,*

$$\Psi_i(a) = \alpha \text{ ve } \Psi_i(b) = \beta$$

olur.



xxx Resim neden küçük?

Kanıt: $L = \cup_{i\in I}\Psi_i(X_i)$ eşitliğini anımsayalım (A2 özelliği). Bu eşitlikten dolayı öyle $i, j \in I$ ve $a_i \in X_i, b_j \in X_j$ vardır ki,

$$\Psi_i(a_i) = \alpha \text{ ve } \Psi_j(b_j) = \beta$$

olur. Eğer $i = j$ olsaydı ve kanıtımız biterdi, ama öyle olmayabilir. Hem i'den hem de j'den büyük bir $k \in I$ bulalım. O zaman,

$$\Psi_k\left(\varphi_{ik}(a_i)\right) = \Psi_i\left(a_i\right) = \alpha$$

ve

$$\Psi_k\left(\varphi_{jk}(b_j)\right) = \Psi_j\left(b_j\right) = \beta$$

olur. Şimdi $\varphi_{ik}\left(a_i\right), \varphi_{jk}\left(b_j\right) \in X_k$ ve bu elemanların Ψ_k imgeleri sırasıyla α ve β'ya eşit. Demek ki,

$$\Psi_k(a) = \alpha \text{ ve } \Psi_k(b) = \beta$$

eşitliklerini sağlayan

$$a = \varphi_{ik}\left(a_i\right) \in X_k \text{ ve } b = \varphi_{jk}\left(b_j\right) \in X_k$$

elemanları bulduk. Savımız kanıtlanmıştır. □

Sav'ın Kanıtına Dair Not: Burada önemli olan a ve b'nin aynı X_k kümesinde seçilmiş olmaları. (Daha önceki a_i ve b_j'nin biri X_i'de öbürü X_j'deydi.)

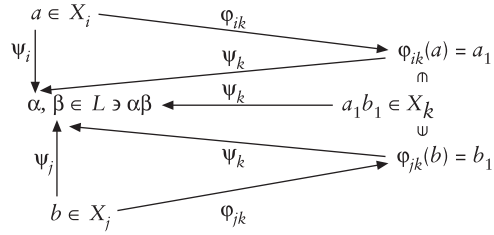
Sav 1'in varsayımlarından devam edelim.

X_i bir grup olduğundan, a ve b elemanlarını çarpıp gene X_i grubunda bir eleman elde edebiliriz ve bu çarpımın Ψ_i imgesini alarak L'den bir eleman bulabiliriz.

Niyetimiz

$$\alpha\beta = \Psi_i(ab)$$

tanımını yapmak ama önce böyle bir tanıma hak kazandığımızı kanıtlamalıyız, $\Psi_i(ab)$'nin sadece α ve β'ya göre değiştiğini, seçilen a, b ve i'den bağımsız olduğunu kanıtlamalıyız.



$\alpha, \beta \in L$ olsun. $a \in X_i$ ve $b \in X_j$ elemanları
$\psi_i(a) = \alpha$ ve $\psi_j(b) = \beta$ eşitliklerini sağlasın. $k \geq i, j$ olsun.
$a_1 = \varphi_{ik}(a)$ ve $b_1 = \varphi_{jk}(b)$ olsun.
O zaman $\psi_k(a_1) = \alpha$ ve $\psi_k(b_1) = \beta$ olur.
$\alpha\beta$ çarpımını $\psi_k(a_1 b_1)$ olarak tanımlamak istiyoruz.

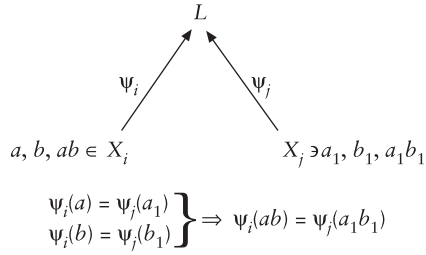
Sav 2. *$a, b \in X_i$ ve $a_1, b_1 \in X_j$ elemanları,*

$$\Psi_i(a) = \Psi_j(a_1), \Psi_i(b) = \Psi_j(b_1)$$

eşitliklerini sağlasınlar. O zaman

$$\Psi_i(ab) = \Psi_j(a_1 b_1)$$

olur.



Kanıt: $\Psi_i(a) = \Psi_j(a_1)$ olduğundan, Sonuç 2.iii'e göre, bir $k \geq i, j$ göstergeci için,

$$\varphi_{ik}(a) = \varphi_{jk}(a_1)$$

olur. Aynı nedenden, bir $\ell \geq i, j$ göstergeci için,

$$\varphi_{i\ell}(b) = \varphi_{j\ell}(b_1)$$

olur. Şimdi $m \geq k, \ell$ olsun. Yukardaki iki eşitlikteki terimlerin sırasıyla φ_{km} ve $\varphi_{\ell m}$ morfizmaları altında imgelerini alalım. Örneğin birincisinden,

$$\varphi_{im}(a) = \varphi_{km}(\varphi_{ik}(a)) = \varphi_{km}(\varphi_{jk}(a_1)) = \varphi_{jm}(a_1)$$

elde ederiz. Benzer şekilde, ikinci eşitlik bize

$$\varphi_{im}(b) = \varphi_{jm}(b_1)$$

verir. Şimdi, $\varphi_{im}(a), \varphi_{jm}(a_1), \varphi_{im}(b), \varphi_{jm}(b_1)$ elemanlarının hepsi X_m grubunda. Dolayısıyla

$$\varphi_{im}(ab) = \varphi_{im}(a)\varphi_{im}(b) = \varphi_{jm}(a_1)\varphi_{jm}(b_1) = \varphi_{im}(a_1 b_1)$$

bulunur. Bundan da - Sonuç D.2.iii'e göre

$$\Psi_i(ab) = \Psi_j(a_1 b_1)$$

çıkar. Savımız kanıtlanmıştır. □

Şimdi $\alpha, \beta \in L$ için, Sav D.4'e göre

$$\Psi_i(a) = \alpha \text{ ve } \Psi_i(b) = \beta$$

eşitliklerini sağlayan herhangi bir $i \in I$ göstergeci ve $a, b \in X_i$ elemanları seçelim ve $\alpha\beta$ çarpımını

$$\alpha\beta = \Psi_i(ab)$$

olarak tanımlayalım. Sav D.4'e göre tanım i'nin ve a ve b'nin seçimlerinden bağımsızdır.

Bu işlemin L üzerine bir grup yapısı tanımladığı çok belli. Ayrıca çarpımın tanımından dolayı

$$\Psi_i(a)\Psi_i(a) = \alpha\beta = \Psi_i(ab)$$

olur, yani $\Psi_i : X_i \to L$ fonksiyonları artık birer grup homomorfizması olurlar.

Böylece teoremin birinci kısmı kanıtlandı. Gelelim ikinci kısmına. M bir grup ve $\theta_i : X_i \to M$ grup morfizmaları ve her $i \leq j \in I$ için

$$\theta_j \circ \varphi_{ij} = \theta_i$$

eşitliklerini sağlasınlar. Öyle bir $\theta : L \to M$ grup morfizması bulacağız ki her $i \in I$ için

$$\theta \circ \Psi_i = \theta_i$$

olacak. $\theta \circ \Psi_i = \theta_i$ koşulundan dolayı, eğer θ, varsa, her $x \in X_i$ için

$$\theta \circ \Psi_i(x) = \theta_i(x),$$

yani

$$\theta(\Psi_i(x)) = \theta_i(x)$$

eşitliğini sağlamalı. Dolayısıyla, Sonuç'a göre, θ'yı tanımlamanın tek bir yolu vardır: Verilmiş bir $\alpha \in L$ için önce

$$\alpha = \Psi_i(x)$$

eşitliğini sağlayan bir $x \in X_i$ seçilir; sonra

$$\theta(\alpha) = \theta_i(x)$$

olarak alınır. Demek ki, θ varsa ancak böyle tanımlanabilir. Şimdi yukardaki tanımın caiz olduğunu, $\Psi_i(x) = \Psi_j(y)$ için $\theta_i(x) = \theta_j(y)$ olduğunu kanıtlayalım. Nitekim,

$$\Psi_i(x) = \Psi_j(y)$$

olduğundan, Sonuç'a göre, i ve j'den büyük bir k için

$$\varphi_{ik}(x) = \varphi_{jk}(y)$$

olur. Her iki tarafa da θ_k uygulayalım:

$$\theta_k\left(\varphi_{ik}(x)\right) = \theta_k\left(\varphi_{jk}(x)\right)$$

buluruz. θ_j'ler üzerine yapılan varsayımdan dolayı, bundan da

$$\theta_i(x) = \theta_j(y)$$

çıkar. Teorem tamamen kanıtlanmıştır. □

Yukardakinin nerdeyse aynısının tıpkısı hemen hemen her türlü cebirsel yapıda yapılabilir: Halkalarda, cisimlerde, modüllerde (aynı halka üzerine)... Direkt limit de doğal olarak aynı yapıya sahiptir. Hatta nesnelerimiz sıralı kümeler, morfizmalarımız da sıralamayı koruyan fonksiyonlar olabilir. Birinci örneğimiz bu türden zaten. Dikkat ederseniz, o örnekte sıralı bir küme olan $\mathbb{Z}$'yi elde ettik.

Alıştırmalar

D.1. Her i doğal sayısı için $X_i = \mathbb{R}^{\geq 0}$ olsun. Her $i < j$ için, $f_{ij}(x) = x^{2^{j-i}}$ olsun. Bu verilerin bir direkt sistem tanımladığını kanıtlayın. Direkt limiti bulun. Direkt limit üzerine Ana Teorem'de kanıtlanan doğal grup yapısı nedir? Direkt limit üzerine bir sıralama bulun. Göstergeçleri $\mathbb{N}$ yerine $\mathbb{Z}$'de alsaydık ne değişirdi?

D.5 Ters Limit

D.6 Aralarındaki İlişki

E. Serbest Gruplar Üzerine

E.1 Altgrupların Üreteçleri

G bir grup ve $H \leq G$ bir altgrup olsun. Gerekirse Seçim Aksiyomu'nu kullanarak, H'nin G'deki her sol ötelemesinden ***sol temsilci*** ya da kısaca ***temsilci*** adını vereceğimiz bir eleman seçelim ve seçilen bu temsilciler kümesini L ile gösterelim. Demek ki

$$G = \bigsqcup_{\ell \in L} \ell H.$$

Yani $L \subseteq G$ öyle seçilmiş olsun ki, her $g \in G$ için

$$g \in \ell H$$

içindeliğini sağlayan bir ve bir tane $\ell \in L$ olsun. Bu $\ell \in L$ elemanını $\overline{g}$ olarak yazalım. Yani $\overline{g}$ elemanı,

$$\overline{g} \in L \text{ ve } g \in \overline{g}H$$

içindelikleriyle belirlensin. Demek ki

$$\overline{g} = g \Leftrightarrow g \in L.$$

Ayrıca H ötelemesinin temsilcisi olarak hep 1'i seçelim, yani

$$L \cap H = \{1\}$$

olsun.

Her $\ell \in L$ ve $g \in G$ için,

$$g\ell = \overline{g\ell} \cdot \delta(g, \ell)$$

eşitliğini sağlayan bir ve bir tane $\delta(g, \ell) \in H$ vardır. Demek ki,

$$\delta(g, \ell) = \overline{g\ell}^{-1} \cdot g\ell \in H. \tag{1}$$

Kanıtlayacağımız ilk sonuç yazımızın temel direğini oluşturacak:

Teorem E.1. *G, X altkümesi tarafından üretilmiş bir grup olsun. $H \leq G$ bir altgrup ve L, H'nin bir sol temsilcileri kümesi olsun. Ayrıca $L \cap H = \{1\}$ olsun. O zaman, yukardaki yazılımla,*

$$H = \langle \delta(x, \ell) : \ell \in L, x \in X \rangle$$

olur.

Kanıt: $h \in H$ olsun. h'yi X'in elemanları cinsinden yazalım: Öyle bir $n \in \mathbb{N}$ ve $x_1, \ldots, x_n \in X$ ve $\epsilon_1, \ldots, \epsilon_n = \pm 1$ vardır ki,

$$h = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$$

olur. Şimdi hesap yapalım.

Bir $\ell_{n-1} \in L$ için,

$$h = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} = x_1^{\epsilon_1} \cdots x_{n-1}^{\epsilon_{n-1}} (x_n^{\epsilon_n} \cdot 1) = x_1^{\epsilon_1} \cdots x_{n-1}^{\epsilon_{n-1}} \ell_{n-1} \delta(x_n^{\epsilon_n}, 1)$$

olur. Aynı düşünceyi kaldığımız yerden $x_{n-1}^{\epsilon_{n-1}} \ell_{n-1}$ için tekrar ettirelim: Bir $\ell_{n-2} \in L$ için,

$$= x_1^{\epsilon_1} \cdots x_{n-2}^{\epsilon_{n-2}} \ell_{n-2} \delta(x_{n-1}^{\epsilon_{n-1}}, \ell_{n-1}) \delta(x_n^{\epsilon_n}, 1).$$

Bunu böyle devam ettirerek, $\ell, \ell_1, \ldots, \ell_{n-1} \in L$ için

$$h = \ell \cdot \delta(x_1^{\epsilon_1}, \ell_1) \cdots \delta(x_{n-1}^{\epsilon_{n-1}}, \ell_{n-1}) \delta(x_n^{\epsilon_n}, 1)$$

buluruz. δ'lar ve h elemanı H'de olduğundan $\ell \in H \cap L = \{1\}$, yani $\ell = 1$ bulunur. Demek ki $\ell_n = 1 \in L$ tanımıyla

$$h = \delta(x_1^{\epsilon_1}, \ell_1) \cdots \delta(x_{n-1}^{\epsilon_{n-1}}, \ell_{n-1}) \delta(x_n^{\epsilon_n}, \ell_n)$$

bulunur.

Son olarak, $\ell_1 = \overline{x^{-1}\ell}$ ve $\ell_2 = \overline{x\ell_1}$ için,

$$x^{-1}\ell = \ell_1 \delta(x^{-1}, \ell)$$

ve

$$\ell = x\ell_1 \delta(x^{-1}, \ell) = \ell_2 \delta(x, \ell_1) \delta(x^{-1}, \ell)$$

olur, yani

$$\delta(x, \ell_1) \delta(x^{-1}, \ell) = 1$$

ve dolayısıyla

$$\delta(x^{-1}, \ell) = \delta(x, \ell_1)^{-1}$$

olur. Teoremimiz kanıtlanmıştır. □

Sonuç E.2. *Sonlu sayıda eleman tarafından üretilmiş bir grubun sonlu endisli altgrupları da sonlu sayıda eleman tarafından üretilir. Eğer grup n eleman tarafından üretilmiş ve altgrubun endisi m ise, altgrup en fazla nm eleman tarafından üretilmiştir.* □

E.2 Serbest Grupların Altgrupları

Teorem E.3. *Serbest grupların altgrupları da serbesttir.*

Kanıt biraz zaman alacak. F, X altkümesi tarafından serbestçe üretilmiş serbest bir grup olsun.

$H \leq F$ olsun. S, H'nin birimli sol temsilciler kümesi olsun. Her $x_i \in X$ ve $\epsilon_i = \pm 1$ için,

$$s = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \in S$$

olduğunda ve yazılım indirgenemez olduğunda (yani daha kısası yazılamıyorsa, yani ardışık x_i'ler arasında sadeleşme yaşanmıyorsa), her $i = 1, \ldots, n$ için

$$x_i^{\epsilon_i} \cdots x_n^{\epsilon_n} \in S$$

oluyorsa, o zaman S'ye ***Schreier temsilcileri kümesi*** diyeceğiz. Bu

$$x_i^{\epsilon_i} \cdots x_n^{\epsilon_n} \in S$$

elemanlarına s'nin ***son dilimi*** adını vereceğiz.

Önsav E.4. *Schreier temsilcileri kümesi her zaman vardır.*

Kanıt: $f \in F$ için $|f|$, f'nin X'e göre uzunluğu olsun, yani f'nin eşit olduğu indirgenemez kelimenin uzunluğu olsun. fH ötelemesinin uzunluğu $|fH|$ de,

$$|fH| = \min fH = \min\{|fh| : h \in H\}$$

olarak tanımlansın. Schreier temsilcilerini $|fH|$ ötelemesinin uzunluğu üzerine tümevarımla seçeceğiz.

fH ötelemesinden seçilen temsilcinin uzunluğu $|fH|$'ye eşit olacak. Uzunluğu 0 olan H'den 1'i seçelim. $S_0 = \{1\}$ olsun. Tümevarımla öyle

$$S_0 \subseteq S_1 \subseteq \ldots \subseteq S_n \subseteq S_{n+1} \subseteq \ldots$$

altkümeleri bulacağız ki, eğer fH'nin uzunluğu n ise, S_n'de fH kümesinden bir ve bir tane eleman olacak ve ayrıca, S_n'nin elemanlarının son dilimleri gene S_n'de (aslında S_{n-1}'de) olacak. Tahmin edileceği ve kolayca görüleceği üzere, $S = \cup_n S_n$ istediğimiz Schreier temsilcilerini verir.

Diyelim uzunluğu $\leq n$ olan ötelemelerden uygun temsilcileri, yani S_n kümesini seçtik. Uzunluğu $n+1$ olan bir fH ötelemesi alalım. Demek ki fH'nin

$$y_1 y_2 \cdots y_{n+1}$$

indirgenemez yazılımlı bir elemanı için ($y_i \in X \cup X_i^{-1}$),

$$fH = y_1 y_2 \cdots y_{n+1} H$$

olur.

$$m = |y_2 \cdots y_{n+1} H|$$

olsun. Elbette $m \leq |y_2 \cdots y_{n+1}| = n$. Dolayısıyla, tümevarım varsayımına göre, bu ötelemenin S_n'de olan bir temsilcisi vardır; diyelim bu temsilci $z_i \in X \cup X_i^{-1}$ için

$$z_1 \cdots z_m \in y_2 \cdots y_{n+1} H$$

olarak yazılıyor. Şimdi

$$y_1 z_1 \cdots z_m H = y_1(z_1 \cdots z_m H) = y_1(y_2 \cdots y_{n+1} H) = fH$$

olduğundan, $1 + m \geq |y_1 z_1 \cdots z_m| \geq |fH| = n + 1$ ve $m = n$ olur. Demek ki $y_1 z_1 \cdots z_m$ yazılımı indirgenemezdir. Bu elemanı ve bu yöntemle elde edilen tüm elemanları S_n kümesine ekleyelim. Böylece istenen S_{n+1} kümesini elde ederiz. □

Eğer $|gh| = |g| + |h|$ ise, yani g'nin ve h'nin indirgenemez gösterimlerinde g'nin son elemanıyla h'nin ilk elemanı sadeleşmiyorsa, bunu gh yerine $g_\Delta h$ yazarak göstereceğiz. Aksi halde, yani uzunluk kısalıyorsa gh yerine $g_- h$ yazacağız.

Şimdi oldukça teknik ama çok önemli bir önsav.

Önsav E.5. *F, X ve H yukardaki gibi olsun. S bir Schreier sol temsilciler kümesi olsun. $s, t \in S$ ve $x, y \in X$ olsun.*

i. *Eğer $\delta(x,s) \neq 1$ ise $\delta(x,s) = \overline{xs}^{-1} {}_\Delta x_\Delta s$.*

ii. *Eğer $\delta(x,s) = \delta(y,t) \neq 1$ ise $x = y$ ve $s = t$.*

iii. *$h \in H = \langle \delta(x,s) : s \in S, x \in X \rangle$ olsun. Eğer*

$$h = \delta(x_1, s_1)^{\epsilon_1} \cdots \delta(x_n, s_n)^{\epsilon_n}, \tag{2}$$

h elemanının δ'lar cinsinden indirgenemez bir gösterimiyse, yani en kısa yazılımıysa, yani hiçbir $\delta(x_i, s_i)$ elemanı 1'e eşit değilse ve ardışık δ'lar bariz biçimde sadeleşmiyorsa (ki bir önceki maddeye göre bu ancak x'ler ve s'ler eşitse ve işaretleri farklıysa olabilir), o zaman

$$h = \cdots {}_\Delta x_1^{\epsilon_1} {}_\Delta \cdots {}_\Delta x_n^{\epsilon_n} {}_\Delta \cdots$$

olur; bir başka deyişle h'nin X cinsinden indirgenemez gösteriminde (2)'deki $\delta(x_i, s_i)$ ifadesinde beliren x_i üreteci sadeleşmez.

Kanıt: i. Diyelim $xs = x_- s$. O zaman bir $t \in S$ için $s = x^{-1} {}_\Delta t$ olur. (S Schreier olduğundan t gerçekten de S'dedir.) O zaman da

$$\delta(x,s) = \overline{xs}^{-1} \cdot xs = \bar{t}^{-1} t = t^{-1} t = 1,$$

çelişki.

Şimdi diyelim $\overline{xs}^{-1} _ x$, ya da aynı anlama gelen $x^{-1} _ \overline{xs}$. O zaman bir $t \in S$ için $\overline{xs} = xt$ olur. Bu durumda da,

$$\delta(x,s) = \overline{xs}^{-1} \cdot xs = (xt)^{-1}xs = t^{-1}s,$$

yani $t^{-1}s \in H$ ve $sH = tH$ ve $s = t$ ve bir satır yukardaki merkezlenmiş formülden $\delta(x,s) = 1$ olur, çelişki.

ii. $\delta(x,s) = \delta(y,t) \neq 1$ varsayımını yapalım. Demek ki (i)'e göre,

$$\overline{xs}^{-1}{}_{\Delta} x_{\Delta} s = \overline{xs}^{-1}{}_{\Delta} y_{\Delta} t.$$

Eğer $|s| = |t|$ ise $s = t$ olur ve sadeleştirmeden sonra $x = y$ elde ederiz, tam istediğimiz gibi. Eğer $|s| < |t|$ ise, $|xs| \leq |t|$ olur ve yukarda merkezlenen eşitlikten dolayı, bir u için $u_{\Delta} xs = t$ olur. S, Schreier olduğundan, $xs \in S$. Demek ki

$$\overline{xs}^{-1}{}_{\Delta} x_{\Delta} s = (xs)^{-1}xs = 1,$$

çelişki.

iii. $x, y \in X$ ve $s, t \in S$ için, $\delta(x,s)^{\pm 1}\delta(y,t)^{\pm 1}$ ifadesini açarsak dört şıkla karşı karşıya kalırız:

$$\begin{array}{l}
(\overline{xs}^{-1}{}_{\Delta} x_{\Delta} s)\,(\overline{yt}^{-1}{}_{\Delta} y_{\Delta} t) \\
(\overline{xs}^{-1}{}_{\Delta} x_{\Delta} s)\,(t^{-1}{}_{\Delta} y^{-1}{}_{\Delta} \overline{yt}) \\
(s^{-1}{}_{\Delta} x^{-1}{}_{\Delta} \overline{xs})\,(\overline{yt}^{-1}{}_{\Delta} y_{\Delta} t) \\
(s^{-1}{}_{\Delta} x^{-1}{}_{\Delta} \overline{xs})\,(t^{-1}{}_{\Delta} y^{-1}{}_{\Delta} \overline{yt})
\end{array}$$

Birinci durumda sadeleşmenin olması için $s = \overline{yt}^{-1}$ ve $xy = 1$ olmalı, ki bu imkânsız. Aynı nedenden son durum da imkânsız.

İkinci durumda sadeleşmenin olması için $s = t$ ve $x = y$ olmalı, ki bu durum varsayımdan dolayı olamaz.

Üçüncü durumda sadeleşmenin olabilmesi için $\overline{xs} = \overline{yt}$ ve $x = y$ olmalı. Demek ki $xsH = \overline{xs}H = \overline{yt}H = ytH = xtH$ ve $sH = tH$ ve $s = t$. Bu da varsayımdan dolayı mümkün değil.

Demek ki sadeleşme olmuyor. □

Teorem E.3'ün Kanıtı: Yukardaki önsavın ikinci ve üçüncü maddesinden hemen çıkar. Hatta şu daha keskin ifadeyi kanıtladık:

Teorem E.6. *Eğer F serbest grubu X altkümesi tarafından serbestçe üretiliyorsa, $H \leq F$ ise ve S, H'nin bir Schreier temsilcileri kümesiyse, o zaman H altgrubu,*

$$Y = \{\delta(x,s) : x \in X,\ s \in S,\ \delta(x,s)\} \setminus \{1\}$$

altkümesi tarafından serbestçe üretilir. □

Örnekler

E.1. F grubu x ve y tarafından serbestçe üretilmiş olsun. $A = \{1, a\} \simeq \mathbb{Z}/2\mathbb{Z}$ olsun. $\phi : F \longrightarrow A$ homomorfisi $\phi(x) = a$ ve $\phi(y) = 1$ eşitlikleriyle tanımlanmış olsun. $H = \operatorname{Ker}\phi$ olsun. Elbette H, endisi 2 olan normal bir altgruptur. H'yi serbestçe üreten (ve yukardaki teoremin söylediği) elemanları bulalım. Önce Schreier temsilcilerini seçelim:

$$S = \{1, x\}$$

olsun. S elbette Schreier temsilcileri kümesidir.

$$X = \{x, y\}$$

alacağız elbette. Yukardaki teoremdeki Y kümesinin elemanlarını bulalım. Bunun için $\delta(x,1)$, $\delta(x,x)$, $\delta(y,1)$, $\delta(y,x)$ elemanlarını teker teker hesaplamalıyız.
$\delta(x,1)$ hesabı: $x \cdot 1 = x = x \cdot 1 \in xH$. Demek ki $\delta(x,1) = 1 \notin Y$.
$\delta(x,x)$ hesabı: $x \cdot x = x^2 = 1 \cdot x^2 \in H$ çünkü $\phi(x^2) = \phi(x)^2 = a^2 = 1$ ve $x^2 \in H$. Demek ki $\delta(x,x) = x^2 \in Y$.
$\delta(y,1)$ hesabı: $y \cdot 1 = y = 1 \cdot y \in xH$. Demek ki $\delta(y,1) = y \in Y$.
$\delta(y,x)$ hesabı: $y \cdot x = x \cdot x^{-1}yx \in xH$. Demek ki $\delta(y,x) = x^{-1}yx = y^x \in Y$.
Demek ki $Y = \{x^2, y, y^x\}$ ve H bu üç eleman tarafından serbestçe üretiliyor.

Eğer F_n, n eleman tarafından serbestçe üretilmiş serbest grupsa, bu örnekte, $F_3 \simeq H \overset{2}{\lhd} F_2$ ilişkilerini gösterdik.

E.2. F gene yukardaki gibi x ve y tarafından üretilen serbest grup olsun. Bu sefer $H = \langle f^2 : f \in F\rangle$ olsun. Elbette $H \lhd G$ ve

$$G/H = \langle \overline{x}, \overline{y}\rangle = \langle \overline{x}\rangle \times \langle \overline{y}\rangle \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Schreier temsilcilerini seçelim:

$$S = \{1, x, y, xy\}$$

ve teoremdeki Y'yi bulalım, yani δ'ları hesaplayalım.
$\delta(x,1)$ hesabı: $x \cdot 1 = x = x \cdot 1 \in xH$ olduğundan, $\delta(x,1) = 1$.
$\delta(x,x)$ hesabı: $x \cdot x = x^2 \in H$ olduğundan, $\delta(x,1) = x^2$.
$\delta(x,y)$ hesabı: $x \cdot y = xy \in xyH$ olduğundan, $\delta(x,y) = 1$.
$\delta(x,xy)$ hesabı: $x \cdot xy = x^2y = y \cdot y^{-1}x^2y \in yH$ olduğundan, $\delta(x,xy) = y^{-1}x^2y = x^{2y}$.
$\delta(y,1)$ hesabı: $y \cdot 1 = y \in yH$ olduğundan, $\delta(y,1) = 1$.
$\delta(y,x)$ hesabı: $y \cdot x = yx = xy \cdot y^{-1}x^{-1}yx \in xyH$ olduğundan, $\delta(y,x) = y^{-1}x^{-1}yx = [y,x]$.
$\delta(y,y)$ hesabı: $y \cdot y = y^2 \in H$ olduğundan, $\delta(y,y) = y^2$.
$\delta(y,xy)$ hesabı: $y \cdot xy = yxy = x \cdot x^{-1}yxy \in xH$ olduğundan, $\delta(y,xy) = x^{-1}yxy$.
Demek ki H grubu x^2, x^{2y}, $[y,x]$, y^2, $x^{-1}yxy$ elemanları tarafından serbestçe üretilmiştir.

Bu örnekte, $F_5 \simeq H \overset{4}{\lhd} F_2$ ilişkilerini gösterdik.

E.3. F gene yukardaki gibi x ve y tarafından üretilen serbest grup olsun.

$$A = \langle a\rangle \times \langle b\rangle \simeq \mathbb{Z} \times \mathbb{Z}$$

olsun. $\phi : F \longrightarrow A$ homomorfisi $\phi(x) = a$ ve $\phi(y) = b$ eşitlikleriyle tanımlansın. $H = \operatorname{Ker}\phi$ olsun. $F/H \simeq \mathbb{Z} \times \mathbb{Z}$ abelyen bir grup olduğundan $F' \leq H$ olur. Aslında

$$H = \{x^{i_1}y^{j_1} \cdots x^{i_n}y^{j_n} : n \in \mathbb{N},\, i_k, j_k \in \mathbb{Z},\, \sum i_k = \sum j_k = 0\}$$

eşitliğini görmek zor değil. Birazdan $H = F'$ eşitliğinin doğru olduğunu göreceğiz. Önce H'yi serbestçe üreten altkümeyi bulalım.

$$S = \{x^i y^j : i, j \in \mathbb{Z}\}$$

olsun. S elbette bir Schreier temsilcileri kümesidir. H'yi üreten δ'ları hesaplayalım.
$\delta(x, x^i y^j)$ hesabı: $x \cdot x^i y^j = x^{i+1} y^j \in x^{i+1} y^j H$. Demek ki $\delta(x, x^i y^j) = 1$.
$\delta(y, x^i y^j)$ hesabı: $y \cdot x^i y^j = x^i y^{j+1} \cdot y^{-j-1} x^{-i} y x^i y^j \in x^i y^{j+1} H$. Demek ki

$$\delta(x, x^i y^j) = y^{-j-1} x^{-i} y x^i y^j = y^{-1} y^{-j} x^{-i} y x^i y^j = [y, x^i y^j]$$

ve H altgrubu

$$\{[y, x^i y^j] : i \in \mathbb{Z}, j \in \mathbb{Z}, i \neq 0\}$$

kümesi tarafından serbestçe gerilmiştir. Bu altküme de F' altgrubunun bir altkümesi olduğundan, $H \leq F'$, yani $H = F'$ çıkar.
Bu örnekten de görüldüğü gibi iki elemanlı serbest grubun altgrupları her zaman sonlu sayıda eleman tarafından üretilmek zorunda değil, mesela $F_2' \simeq F_\omega$ olur.

Bu arada söz (yukardaki örnekte) açılmışken F grubu X ve Y altkümeleri tarafından serbestçe üretiliyorsa, F/F' grubu, abelyen grup olarak X ve Y tarafından serbestçe üretilir, yani

$$F \simeq \bigoplus_{x \in X} \mathbb{Z}x \simeq \bigoplus_{y \in Y} \mathbb{Z}y$$

olur. Abelyen grup teoriden (ya da tek üreteçli idealler bölgeleri üzerine modüllerin sınıflandırılmasından) biliyoruz ki bu durumda $|X| = |Y|$ olmalı. Demek ki serbest bir grubun serbest üreteçlerinin kümesinin kardinali değişmez ve bir κ kardinali için F_κ notasyonu caizdir.

E.3 Serbest Tümleyen

F, X tarafından serbestçe üretilmiş serbest grup, $X = Y \sqcup Z$, $H = \langle Y \rangle$ ve $K = \langle Z \rangle$ olsun. H ve K'ya birbirinin ***serbest tümleyeni*** diyeceğiz ve bunu göstermek için

$$F = H \star K$$

yazacağız. Bu durumda F'nin her elemanı H ve K'nın elemanlarının alterne eden çarpımları olarak yazılır ve bu yazılım özünde biriciktir; bir başka deyişle F'nin her f elemanı için, öyle bir ve bir tane $n \in \mathbb{N} \setminus \{0\}$, $h_1 \in H$, $h_2, \ldots, h_n \in H \setminus \{1\}$, $k_1, \ldots, k_{n-1} \in K \setminus \{1\}$, $k_n \in K$ elemanları vardır ki

$$f = h_1 k_1 \cdots h_n k_n$$

olur. Bu durum başgösterdiğinde H'ye (ya da K'ya), F'nin ***serbest faktörü*** adı verilir.

Örnekler

E.4. F grubu x ve y elemanları tarafından serbestçe üretilsin. $H = \langle x, x^y\rangle$ ve $K = \langle y\rangle$ olsun. H'nin her $x^{n_1}y^{m_1}\cdots x^{n_k}y^{m_k}$ elemanınında $\sum m_i = 0$ olur ama K'nın sadece 1 elemanında bu durum başgösterir. Dolayısıyla $H \cap K = 1$ ama $\langle H, K\rangle = H \star K$ olmaz çünkü $1 \neq h = x^y \in H$, $1 \neq h_1 = x^{-1} \in H$, $1 \neq k = y^{-1} \in K$, $1 \neq k_1 = y \in K$ için $hkh_1k_1 = x^y y^{-1}x^{-1}y = 1$ olur.

Demek ki eğer $F = \langle H, K\rangle$ serbest bir grupsa ve $H \cap K = 1$ ise, Y, H'yi ve Z, K'yı serbestçe üretse bile, $Y \cup Z$ kümesi F'yi serbestçe germek zorunda değildir.

E.5. F serbest bir grup olsun. Yukardaki örnekten de kolayca anlaşılacağı gibi eğer $N \lhd F$ ve $K \leq F$ ise $\langle N, K\rangle = N \star K$ ancak $K = 1$ için mümkündür. Bunun sonuçlarını bir sonraki altbölümde göreceğiz.

Teorem E.7. *F serbest bir grup ve $H \leq F$ olsun. Eğer H sonlu sayıda eleman tarafından üretiliyorsa, öyle bir $K \leq F$ altgrubu vardır ki, $\langle H, K\rangle \simeq H \star K$ olur ve bu altgrubun F'de endisi sonludur.*

Kanıt: R, H'nin bir Schreier temsilcileri kümesi olsun. Teorem E.6'dan dolayı, H'nin

$$Y := \{\delta(x, r) : x \in X, r \in R, \delta(x, r)\} \setminus \{1\}$$

altkümesi tarafından serbestçe üretildiğini biliyoruz. Ama varsayıma göre H sonlu eleman tarafından üretiliyor. Demek ki Y sonlu. $|Y| = n$ olsun ve

$$Y = \{\delta(x_1, r_1), \ldots, \delta(x_n, r_n)\}$$

olsun.

Öyle bir $Z \supseteq Y$ bulacağız ki, $\langle Z\rangle$ altgrubu Z tarafından serbestçe üretilecek ve bu altgrubun F'deki endisi sonlu olacak. Bunu kanıtlarsak teorem kanıtlanmış olacak çünkü bu durumda $K = \langle Y \setminus Z\rangle$ almak yeterli.

$\delta(x_i, r_i) = \overline{x_i r_i}^{-1} \cdot x_i r_i$ eşitliğini anımsayalım. S kümesini

$$\overline{x_1 r_1},\ r_1\ \ldots,\ \overline{x_n r_n},\ r_n$$

elemanlarının son dilimlerinden oluşan küme olsun. S, R'nin sonlu bir altkümesidir. Ayrıca $1 \in S$ ve S'nin elemanlarının son dilimleri de S'dedir.

İlk olarak F'den $\operatorname{Sym} S$'ye giden bir ϕ homomorfisi bulacağız, yani F grubunun S kümesi üzerine bir etkimesini bulacağız. Bir paragraf önce bulmaya söz verdiğimiz Z üreteç kümesi,

$$\operatorname{Stab}_F(1) = F_1 = \{f \in F : \phi_f(1) = 1\}$$

altgrubunu serbestçe üretecek[1]. $[F : F_1] \leq |S|$ olduğundan bu da teoremi kanıtlayacak. Aslında $[F : F_1] = |S|$ eşitliğini bulacağız.

ϕ homomorfisini bulmak için X'ten $\operatorname{Sym} S$'ye giden bir fonksiyon bulmak yeterli. İstediklerimizin yerine gelmesi için bu fonksiyonu dikkatlice seçeceğiz.

[1] S'nin F_1'in F'de bir Schreier temsilcileri kümesi olduğunu kanıtlayacağız ve Z, Teorem E.6'da X ve S için verilen F_1'in üreteç kümesi olacak.

Her $x \in X$ için,

$$S(x) = \{s \in S : \overline{xs} \in S\}$$

olsun. $S(x)$, elbette S'nin bir altkümesidir (ama boşküme de olabilir). Böylece her $x \in X$ için

$$\phi_x(s) = \overline{xs}$$

kuralıyla tanımlanmış bir

$$\phi_x : S(x) \longrightarrow S$$

fonksiyonu bulmuş olduk. ϕ_x'in birebir olduğunu savlıyoruz. Nitekim, diyelim $\phi_x(s) = \phi_x(t)$, yani $\overline{xs} = \overline{xt}$ o zaman $xsH = xtH$ ve $sH = tH$ olur ve bundan da $s = t$ çıkar. Demek ki ϕ_x birebirmiş.

Şimdi ϕ_x'i rastgele bir biçimde S'den S'ye giden bir eşleşmeye tamamlayalım[2]. Bu genişlemeye de ϕ_x adını verelim. Demek ki $\phi_x \in \operatorname{Sym} S$ ve her $s \in S(x)$ için $\phi_x(s) = \overline{xs}$.

Böylece $\phi(x) = \phi_x$ kuralıyla verilmiş bir

$$\phi : X \longrightarrow \operatorname{Sym} S$$

fonksiyonu bulunur. F, X tarafından serbestçe üretildiğinden, bulduğumuz (ya da seçtiğimiz) bu ϕ fonksiyonunu genişleten bir ve bir tane

$$F \longrightarrow \operatorname{Sym} S$$

homomorfisi vardır. Bu homomorfiyi de ϕ ile gösterelim. Son olarak

$$\operatorname{Stab}_F(1) = F_1 = \{f \in F : \phi_f(1) = 1\}$$

tanımını yapalım.

Şimdi her $t \in S$ için $\phi_t(1) = t$ eşitliğini kanıtlayacağız[3]. Bunun için iki teknik hesap yapacağız:

Birinci teknik hesap: $s \in S$ ve $x \in X$ olsun. $xs \in S$ varsayımını yapalım. Demek ki $\overline{xs} = xs \in S$ ve $s \in S(x)$. Dolayısıyla

$$\phi_x(s) = \overline{xs} = xs. \tag{3}$$

İkinci teknik hesap: $s \in S$ ve $x \in X$ olsun. Ama bu sefer $x^{-1}s \in S$ varsayımını yapalım. Demek ki $\overline{x^{-1}s} = x^{-1}s \in X(s)$ ve dolayısıyla $\phi_x(x^{-1}s) = x(x^{-1}s) = s$. Son eşitlikte ϕ_x'i sol taraftan sağ tarafa geçirirsek, $\phi_{x^{-1}}(s) = x^{-1}s$ buluruz.

[2]Bu seçimi Seçim Aksiyomu kullanmadan yapmak için, $\operatorname{Sym} S$'nin elemanlarını bir biçimde tamsıralamak ve ϕ_x'i genişleten $\operatorname{Sym} S$'nin ilk elemanını seçmek yeterli.

[3]Böylece F serbest grubunun S kümesini geçişli etkidiği kanıtlanmış olacak.

Demek ki $s \in S$, $y \in X \cup X^{-1}$ ve $ys \in S$ ise,

$$\phi_y(s) = ys$$

olur. Bunu temel alarak, $t \in S$ için $\phi_t(1)$'i hesaplayalım. t'yi $X \cup X^{-1}$ kümesinin elemanları cinsinden yazalım: Diyelim $y_1, \ldots, y_k \in X \cup X^{-1}$ için

$$t = y_1 \cdots y_k$$

olsun. S'nin elemanlarının son dilimleri de S'de olduğundan, yukarda yaptıklarımızdan,

$$\begin{aligned} \phi_t(1) &= \phi_{y_1 \cdots y_k}(1) = \phi_{y_1} \cdots \phi_{y_{k-1}} \phi_{y_k}(1) \\ &= \phi_{y_1} \cdots \phi_{y_{k-1}}(y_k) = \phi_{y_1} \cdots \phi_{y_{k-2}}(y_{k-1} y_k) \\ &= \ldots = y_1 \cdots y_k = t \end{aligned}$$

olur. Demek ki her $t \in S$ için

$$\phi_t(1) = t.$$

Bundan da S kümesinin F_1'in F'deki temsilcileri kümesi olduğu çıkar. Nitekim, eğer $f \in F$ ise, $\phi_f(1) = t \in S$ tanımını yaparak, sırasıyla, $\phi_f(1) = \phi_t(1)$, $\phi_{t^{-1}f}(1) = 1$, $t^{-1}f \in F_1$ ve $f \in tF_1$ bulunur. Ayrıca $s, t \in S$ için $sF_1 = tF_1$ ise, sırasıyla, $t^{-1}s \in F_1$ grubu, $\phi_{t^{-1}s}(1) = 1$, $s = \phi_s(1) = \phi_t(1) = t$ olur.

S kümesi bir Schreier temsilcileri kümesi olduğundan, Teorem E.6'ya göre, F_1 altgrubu

$$Z = \{\epsilon(x, s) : x \in X,\ s \in S,\ \epsilon(x, s)\} \setminus \{1\}$$

tarafından serbestçe üretilir. Buradaki $\epsilon(x, s) \in F_1$ elemanı, Teorem E.6'daki F_1 ve S'ye tekabül eden elemanlardır, yani $\epsilon(x, s) \in F_1$ ve $\widehat{xs} \in S$ olmak üzere,

$$\epsilon(x, s) = \widehat{xs}^{-1} \cdot xs$$

olarak tanımlanmıştır.

Son olarak $Y \subseteq Z$ içindeliğini kanıtlayalım. Bunun için her $i = 1, \ldots, n$ için,

$$\overline{x_i r_i} = \widehat{x_i r_i}$$

eşitliğini kanıtlamak yeterli. Bunun için iki küçük olguya ihtiyacımız var:

$f \in F$ olsun. Demek ki bir $t = \widehat{f} \in S$ için $f \in tF_1$. Dolayısıyla

$$\phi_f(1) = \phi_t(1) = t = \widehat{f}.$$

Ayrıca S'nin tanımı gereği $x_i r_i \in S$; ve elbette $r_i \in S$. Yani $r_i \in S(x_i)$. Buradan da (3)'ten dolayı $\phi_{x_i}(r_i) = x_i r_i$ çıkar.

Bunlardan hareketle hesaplayalım:

$$\widehat{x_i r_i} = \phi_{x_i r_i}(1) = \phi_{x_i} \phi_{r_i}(1) = \phi_{x_i}(r_i) = x_i r_i = \overline{x_i r_i}.$$

Böylece $Y \subseteq Z$ içindeliği kanıtlandı. □

E.4 Birkaç Sonuç

Bu bölümde serbest gruplarla ilgili birkaç sonuç kanıtlayacağız. Her biri yukarda yaptıklarımızdan çıkacak.

Sonuç E.8 (Schreier)**.** *Serbest bir grubun sonlu eleman tarafından üretilmiş normal bir altgrubu ya* 1*'dir ya da sonlu endislidir.*

Kanıt: F serbest grup olsun. $H \lhd F$ sonlu eleman tarafından üretilmiş olsun. O zaman Teorem E.7'ye göre, bir $K \leq F$ için $\langle H, K\rangle = H * K$ grubunun F'de endisi sonlu olur. Ama $H \lhd F$ olduğundan $K = 1$ olmalıdır. □

Eğer bir grubun sonlu endisli altgruplarının kesişimi 1 ise, gruba ***kalıntısal sonlu grup*** adı verilir. Bir G grubunun kalıntısal sonlu olması şöyle de ifade edilir: Her $1 \neq g \in G$ için g'yi içermeyen sonlu endisli bir altgrup vardır. Örneğin, sonlu üreteçli abelyen gruplar, döngüsel grupların direkt toplamı olduklarından, kalıntısal sonludurlar.

Teorem E.9 (F.W. Levi)**.** *Serbest gruplar kalıntısal sonludur.*

Kanıt: F serbest bir grup olsun. $1 \neq f \in F$ olsun. Theorem E.7'ye göre, $\langle f, K\rangle = \langle f\rangle * K$ eşitliğini sağlayan sonlu endisli bir K altgrubu vardır. $J = \langle f\rangle * K$ olsun. K, Y altkümesi tarafından serbestçe üretilmiş olsun. Son olarak,

$$L = \langle J', Y, f^2\rangle$$

olsun. Elbette $[J : L] = [J/J' : L/J'] = 2$'dir ve $f \notin L$. □

Bir G grubunun ***hopf grubu*** olması demek, her $1 \neq N \lhd G$ için $G/N \not\cong G$ demektir. Örneğin sonlu gruplar Hopf gruplarıdır, ama Prüfer p-grupları Hopf grupları değildirler, hatta antihopfdurlar diyebiliriz!

Teorem E.10. *Sonlu eleman tarafından üretilmiş serbest gruplar Hopfiyandırlar.*

Bu teorem, Teorem E.9'un ve bir sonrakinin sonucu.

Teorem E.11 (I.A. Mal'cev)**.** *Sonlu eleman tarafından üretilmiş kalıntısal sonlu gruplar hopfiyandırlar.*

Mal'cev'in teoremini kanıtlamak için önce kendi başına önemli bir önsav kanıtlayalım.

Önsav E.12. *$n \in \mathbb{N}$ olsun. Sonlu (diyelim m tane) eleman tarafından üretilmiş bir grubun endisi n olan sonlu sayıda (en fazla $(n!)^m$ tane) altgrubu vardır.*

Kanıt: Gruba G diyelim. G, eleman sayısı m olan X altkümesi tarafından üretilmiş olsun. $H \leq G$, endisi n olan bir altgrup olsun.

$$G/H = \{xH : x \in G\},$$

olsun. G, G/H kümesini soldan bilinen şekilde soldan ötelemeyle etkisin: $g \in G$ ve $xH \in G/H$ için,

$$g \cdot (xH) = gxH$$

olsun. Böylece $\psi(g)(xH) = gxH$ formülüyle verilmiş bir

$$\psi : G \longrightarrow \mathrm{Sym}(G/H)$$

grup homomorfisi buluruz. Elbette,

$$G_H := \{g \in G : gH = H\} = H$$

olur.

$|G/H| = n$ olduğundan G/H ile $\{1, 2, \ldots, n\}$ kümeleri arasında birebir bir eşleme vardır. $f(H) = 1$ eşitliğini sağlayan böyle bir eşleme seçelim. Bu f eşlemesi sayesinde

$$\phi_f(\sigma) = f \circ \sigma \circ f^{-1}$$

formülüyle verilen bir

$$\phi_f : \mathrm{Sym}(G/H) \longrightarrow \mathrm{Sym}\, n$$

grup izomorfisi bulunur ve böylece bir

$$\psi_f := \phi_f \circ \psi : G \longrightarrow \mathrm{Sym}\, n$$

grup homomorfisi elde ederiz. Böylece G grubu $\{1, \ldots, n\}$ kümesini etkiler: $g \star i = (\psi_f(g))(i)$. Bu etkilemeyle,

$$G_1 := \{g \in G : g \star 1 = 1\} = \{g \in G : (\psi_f g)(1) = 1\} = H$$

olur. Demek ki endisi n olan $H \leq G$ sayısı, olası $\psi_f : G \longrightarrow \mathrm{Sym}\, n$ homomorfizma sayısından daha fazla olamaz. Ama G, X tarafından üretildiğinden G'den $\mathrm{Sym}\, n$'ye giden homomorfi sayısı X'ten $\mathrm{Sym}\, n$'ye giden fonksiyon sayısından fazla olamaz. Bundan da en fazla $(n!)^m$ tane vardır[4]. □

[4]Bu kanıtta her $H \leq G$ için bir $f : G/H \longrightarrow \{1, \ldots, n\}$ eşlemesi seçerek, daha sonra sonlu olacağını kanıtlayacağımız G/H kümesi için Seçim Aksiyomu'nu kullanmış olduk! Aslında Seçim Aksiyomunu kullanmak zorunda değildik. Her $H \leq G$ için $f(H) = 1$ eşitliğini sağlayan bir $f : G/H \longrightarrow \{1, \ldots, n\}$ eşlemesi seçeceğimize, bu eşitliği sağlayan tüm f eşlemelerini alalım. Ardından, tüm bu f'ler için tüm ψ_f'leri alalım. Böylece Seçim Aksiyomu'nu kullanmadan aynı sonucu elde ederiz.

Teorem E.11'in Kanıtı. G teoremdeki gibi bir grup olsun. Diyelim bir $N \lhd G$ için $G/N \simeq G$. Herhangi bir $n \in \mathbb{N}$ sabitleyelim. Önsav E.12'ye göre G'nin endisi n olan sonlu sayıda altgrubu olduğundan, G/N'nin de endisi n olan aynı sayıda altgrubu vardır. Ama G/N'nin altgrupları, bir ve bir tane $N \leq H \leq G$ için G/H biçiminde yazılırlar ve $[G/N : H/N] = [G : H]$ olur. Demek ki G'nin endisi n olan tüm altgrupları N'yi içermek zorundadır. n rastgele olduğundan, bundan da G'nin endisi sonlu olan her algrubunun N'yi içerdiği çıkar. Demek ki G'nin sonlu altgruplarının kesişimi N'yi içeriyor. Dolayısıyla $N = 1$. □

Teorem E.13 (J. Nielsen, 1918)**.** *Eğer F grubu n elemanlı X altkümesi tarafından serbestçe üretilmiş bir grupsa ve $Y \subseteq F$, n elemanlı ve F'yi üreten bir altkümeyse, o zaman Y, F'yi serbestçe üretir.*

Kanıt: $f : X \longrightarrow Y$ herhangi bir eşleme olsun. Bu eşleme sayesinde $\phi_f : F \longrightarrow F$ homomorfisi elde ederiz. Y, X'i gerdiğinden, ϕ_f örtendir. Demek ki $F/\operatorname{Ker}\phi_f \simeq F$ olur. Teorem E.10'a göre $\operatorname{Ker}\phi_f = 1$'dir. Demek ki ϕ_f birebirdir. Bu da aynen F'nin Y tarafından serbestçe üretildiği anlamına gelir (Y'nin elemanları tarafından sağlanan herhangi bir eşitlik, $\operatorname{Ker}\phi_f$'te 1 olmayan bir eleman yaratır). □

Kaynakça

Gilbert Baumslag, **Topics in Combinatorial Group Theory**, Birkhäuser, Lectures in Mathematics 1993.

F. Zorn Önsavı

F.1 Problemler

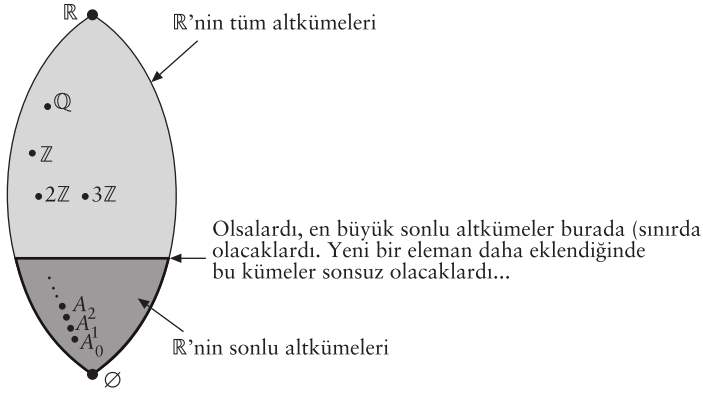
F.1.1 İmkânsız Bir Problem

İmkânsız bir problemle başlayalım: Gerçel sayılar kümesi $\mathbb{R}$'nin **maksimal** bir sonlu altkümesini bulmaya çalışalım...

Doğru anladınız! Dediğimiz gibi imkânsız bir problemi çözmeye çalışacağız... Gerçel sayılardan oluşan öyle bir sonlu küme bulmaya çalışacağız ki, bu kümeden daha fazla gerçel sayı içeren hiçbir gerçel sayı kümesi sonlu olamasın...

Böyle bir küme olamaz elbet. Eğer $\mathbb{R}$'nin bir altkümesinin sonlu sayıda elemanı varsa, bu altkümeye yeni bir gerçel sayı ekleyerek ondan daha büyük ama gene sonlu sayıda elemanı olan bir başka küme elde ederiz.

Biz gene de böyle bir küme bulmaya çalışalım! Maksat komiklik olsun...



Aradığımız, "en büyük" sonlu küme değil, yani tüm sonlu kümeleri altküme olarak içeren sonlu bir küme aramıyoruz. Sadece o sonlu kümeden "daha büyük", yani o sonlu kümeyi özeltküme olarak içeren sonlu bir altküme olmasını istemiyoruz.

$\mathbb{R}$'nin sonlu bir altkümesini alalım. Eğer bu küme $\mathbb{R}$'nin maksimal bir sonlu altkümesiyse işimiz iş. Değilse (ki değildir!) o zaman bu kümeden daha büyük

ama hâlâ sonlu bir küme daha vardır. (Kümelerimiz hep $\mathbb{R}$'nin altkümeleri olsunlar, artık bunu sürekli tekrarlamayalım.) Şimdi eskisinden daha büyük olan bu yeni kümeye bakalım. Bu yeni kümenin maksimal sonlu küme olma olasılığı eski kümeye göre daha yüksek tabii... Eğer bu yeni küme maksimal bir sonlu kümeyse, işimiz iş, istediğimizi elde ettik. Değilse, o zaman bu kümeden daha büyük sonlu bir küme daha vardır (ki var, biliyoruz). Şimdi bu en yeni sonlu kümeye bakalım, acaba bu en yeni sonlu küme maksimal bir sonlu küme mi? Eğer öyleyse maksimal bir sonlu küme bulduk ve sorunumuzu hallettik. Değilse, bu kümeden daha büyük bir sonlu altküme vardır. Şimdi bu sonlu altkümeye bakalım, acaba bu en gıcır sonlu küme maksimal bir sonlu altküme mi?..

Birinci kümemize A_0 diyelim. Eğer A_0, $\mathbb{R}$'nin maksimal bir sonlu altkümesiyse, sorun yok. Diyelim şansımız yaver gitmedi (!) ve A_0, $\mathbb{R}$'nin maksimal bir sonlu altkümesi değil, o zaman ondan daha büyük sonlu bir küme vardır. A_0'dan daha büyük sonlu bir küme alalım ve bu kümeye A_1 diyelim. A_1, maksimal bir sonlu küme değilse, A_1'den daha büyük sonlu bir küme vardır. Bu kümeye de A_2 diyelim. Bunu böylece sürdürebiliriz:

$$A_0 \subset A_1 \subset A_2 \subset A_3 \subset \ldots \subset A_n.$$

Bunların biri maksimal bir sonlu kümeyse imkânsız problemimizi çözdük demektir. Ama değilse işlemi sonsuza kadar sürdürebiliriz. Sürdürelim:

$$A_0 \subset A_1 \subset A_2 \subset A_3 \subset \ldots \subset A_n \subset \ldots$$

Böyle bir diziye ***zincir*** adını verelim.

Yukardaki zincirin A_n "halkaları" sonlu gerçel sayı kümeleri. Herbirinin bir öncekinden daha fazla elemanı var. Dolayısıyla hiçbiri maksimal bir sonlu küme değil. Bunların **herbirinden** daha büyük ama hâlâ sonlu bir gerçel sayı kümesi bulup bu kümenin maksimal bir sonlu küme olup olmadığına bakalım... Bulacağımız bu yeni küme A_n'lerin hepsini (altküme olarak) içermek zorunda olduğundan sonlu olamaz maalesef. Ama olsaydı ne güzel olurdu... Bu, bütün A_n'leri içeren sonlu kümeye A_ω der ve kaldığımız yerden devam ederdik... Durum şöyle olurdu:

$$A_0 \subset A_1 \subset A_2 \subset A_3 \subset \ldots \subset A_n \subset \ldots \subset A_\omega.$$

Eğer A_ω maksimal bir sonlu kümeyse sorunu çözmüş olurduk. Değilse (ki değil, çünkü A_ω sonlu bile değil), o zaman A_ω'dan daha büyük sonlu bir küme bulur ve aynı işlemi maksimal bir sonlu altkümeye toslayana dek sürekli tekrarlardık. Bir zincire geldiğimizde ise zincirin bileşimini içeren sonlu bir küme bulmayı umup gene yolumuza devam ederdik. Bu yöntemi hiç durmadan tekrarlayarak maksimal bir sonlu küme bulmaya çalışabilirdik.

Ama ne yazık ki bunlar hayal, bütün A_n'leri içeren A_ω gibi sonlu bir küme yok evrende.

Bütün bu yaptıklarımızı sonlu altkümeler yerine $\mathbb{R}$'nin sayılabilir altkümeleriyle yapsaydık, gene başarısızlığa uğrardık, çünkü $\mathbb{R}$'nin en büyük sayılabilir altkümesi de yoktur (çünkü sayılabilir bir kümeye bir eleman daha eklersek gene sayılabilir bir küme elde ederiz) ama bu sefer yukardaki yöntemle başarısızlığa uğrayacağımızı gösteremezdik (çünkü sayılabilir sonsuzluktaki sayılabilir kümenin bileşimi gene sayılabilirdir (ama bu sonucu kanıtlamak için Seçim Aksiyomu'na ihtiyaç vardır)).

Gene de yukardaki fikrin başarıya ulaşacağı durumlar olacaktır. Bizi izlemeye devam edin!

F.1.2 Çok Kolay Bir Problem

Gene çok kolay bir problem ele alalım, ama bu sefer lütfen çözümü olsun! Bu sefer $\mathbb{R}$'nin 1'i içermeyen maksimal bir altkümesini bulalım.

Gerçekten çok kolay bir problem bu. Tek bir çözümü var: $\mathbb{R} \setminus \{1\}$. Yani bu sefer sadece maksimal değil, gerçekten de koşulumuzu sağlayan **en büyük** altküme var. Ama biz bu çözümü bilmediğimizi varsayarak yukardaki yöntemi deneyelim.

$\mathbb{R}$'nin 1'i içermeyen herhangi bir altkümesinden başlayalım. Bu altküme boşküme de olabilir, $\{0\}$ ya da $\{\pi\}$ kümesi de olabilir, hatta, şans bu ya, $\mathbb{R} \setminus \{1\}$ kümesi de olabilir; önemli olan 1'i içermemesi. 1'i içermeyen bu ilk kümeye A_0 diyelim. Eğer A_0 kümesi 1'i içermeyen maksimal bir altkümeyse, o zaman keyfimize diyecek yok, problemi çözdük. Ama diyelim A_0 kümesi 1'i içermeyen maksimal bir küme değil. O zaman A_0'ı içeren ve A_0'dan daha fazla elemanı olan ama 1'i içermeyen bir A_1 kümesi vardır. Eğer A_1 kümesi 1'i içermeyen maksimal bir kümeyse, o zaman problemimizi çözdük demektir. Ama diyelim A_1 kümesi 1'i içermeyen maksimal bir küme değil. O zaman A_1'i içeren ve A_1'den daha fazla elemanı olan ama hâlâ daha 1'i içermeyen bir A_2 kümesi vardır. Eğer A_2 kümesi 1'i içermeyen maksimal bir kümeyse, o zaman problemimizi çözdük demektir... Bunu böylece devam ettirelim. Eğer belli bir aşamada, diyelim n'inci aşamada A_n kümesi 1'i içermeyen maksimal bir kümeyse, o zaman problemimizi çözdük demektir... Diyelim hiçbir A_n, 1'i içermeyen maksimal bir küme değil, sürekli daha büyüğünü buluyoruz. Durumu resmedelim:

$$A_0 \subset A_1 \subset A_2 \subset A_3 \subset \ldots \subset A_n \subset \ldots$$

ve özetleyelim: Bunların hepsi gerçel sayı kümeleri ve hiçbiri 1'i içermiyor ve herbirinin bir öncekinden daha fazla elemanı var.

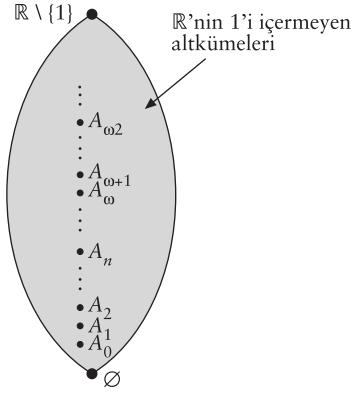
Bunların herbirinden daha büyük ve 1'i içermeyen bir küme bulup bu kümenin 1'i içermeyen maksimal bir küme olup olmadığına bakalım. Bulacağımız bu yeni kümenin A_n'lerin hepsinden daha büyük olmasını istediğimizden, A_n'lerin hepsini altküme olarak içermek zorundadır. Bir önceki örnekte A_n'lerin hepsinden daha büyük ve sonlu bir küme bulamamıştık, yoktu öyle bir küme, bakalım şimdi bulabilecek miyiz? Heyecan son haddinde!

Bütün bu A_n'lerin bileşimini alırsak, A_n'lerin hepsinden daha büyük bir küme buluruz elbet. Ayrıca, A_n'lerin hiçbiri 1'i eleman olarak içermediğinden, A_n'lerin bileşimi de 1'i eleman olarak içermez. Ne güzel!

Demek ki tüm A_n'leri altküme olarak içeren ama 1'i eleman içermeyen en az bir küme vardır. A_ω, bu kümelerden biri olsun. Örneğin

$$A_\omega = \bigcup_{n\in\mathbb{N}} A_n$$

olabilir, ama bundan daha büyük bir küme de olabilir, ne olduğu pek önemli değil, önemli olan A_ω'nın A_n'lerin hepsini altküme olarak içermesi ama 1'i içermemesi.



Kaldığımız yerden A_0 yerine A_ω ile devam edelim. Eğer A_ω kümesi 1'i içermeyen maksimal bir kümeyse, o zaman başarıya ulaştık demektir... Değilse, A_ω'yı altküme olarak içeren ama A_ω'dan daha büyük olan ve 1'i içermeyen bir küme var demektir. Bu kümeye $A_{\omega+1}$ diyelim. Okur tahmin ediyordur bundan sonra ne yapacağımızı. Eğer $A_{\omega+1}$ kümesi 1'i içermeyen maksimal bir kümeyse, o zaman problemimizi çözdük demektir... Değilse, $A_{\omega+1}$'in, $A_{\omega+1}$'den daha büyük ve 1'i içermeyen bir üstkümesi var demektir. Bu kümeye $A_{\omega+2}$ diyelim... Bunu böylece sürdürürüz... Eğer

$$A_\omega \subset A_{\omega+1} \subset A_{\omega+2} \subset \ldots \subset A_{\omega+n} \subset \ldots$$

zincirinin $A_{\omega+n}$ halkalarından hiçbiri 1'i içermeyen maksimal bir küme değilse, bunların bileşimi örneğin, 1'i içermeyen ve yukardakilerin herbirinden daha

büyük bir kümedir. Böyle bir kümeye $A_{\omega 2}$ adını verelim. Eğer $A_{\omega 2}$ kümesi 1'i içermeyen maksimal bir kümeyse, o zaman problemimizi çözdük demektir... Değilse, işlemi devam ettirebiliriz... Eğer belli bir aşamada, 1'i içermeyen maksimal bir altkümeye (yani $\mathbb{R}\setminus\{1\}$'e, ama sonucun bu olduğunu bilmiyormuş gibi davranıyoruz) rastlarsak o zaman gayretlerimiz amacına ulaşmış demektir, duralım. Ama eğer kümeleri hep 1'i içermeyecek biçimde büyütebiliyorsak, bir adım ileri gidelim. Başarıya ulaşmadığımız sürece hep ileri gidebileceğimizi biliyoruz.

$$A_{\omega 2} \subset A_{\omega 2+1} \subset A_{\omega 2+2} \subset \ldots \subset A_{\omega 2+n} \subset \ldots$$

Eğer hep başarısızlığa uğramışsak, bir sonraki aşamada bu kümelerin bileşimini içeren ama 1'i içermeyen herhangi bir küme alıp buna $A_{\omega 3}$ diyelim ve yukardaki gibi devam edelim.

Peki ama bu durmadan ileri gitmenin bir sonu gelecek mi? En sonunda, gerekirse sonsuz hatta çok sonsuz adımı aşıp $\mathbb{R} \setminus \{1\}$ kümesine ulaşabilecek miyiz?

Bu sorunun yanıtı hiç de bariz değil. $\mathbb{R}$ çok büyük bir küme olduğundan (bkz. [SKK]) ulaşmak istediğimiz $\mathbb{R}\setminus\{1\}$ kümesi de bayağı büyüktür, sayılamaz sonsuzluktadır. (Bunun ne demek olduğunu bilmeyen umursamasın.) Yukarıdaki yöntemle zaten bildiğimiz $\mathbb{R} \setminus \{1\}$ çözümüne ulaşıp ulaşamayacağımızdan emin olamayız.

F.1.3 Benzer Bir Problem

Bu sefer $\mathbb{R}$'nin maksimal bir özaltkümesini bulmaya çalışalım. Yani $\mathbb{R}$'nin öyle bir altkümesini bulalım ki, $\mathbb{R}$'nin bu altkümeden daha büyük bir altkümesi $\mathbb{R}$'ye eşit olsun. Yanıtı gene biliyoruz: Eğer a, $\mathbb{R}$'nin herhangi bir elemanıysa, $\mathbb{R} \setminus \{a\}$ kümesi $\mathbb{R}$'nin maksimal bir özaltkümelerinden biridir, $\mathbb{R}$'nin ondan daha büyük bir özaltkümesi yoktur.

Bu sefer birden fazla yanıt var, $\mathbb{R}$'nin her a elemanı için bir çözüm ($\mathbb{R} \setminus \{a\}$ çözümünü) bulabiliriz.

Aynı yöntemi denersek bu sefer de birinci örneğimizdeki zorluğa toslarız: Eğer

$$A_0 \subset A_1 \subset A_2 \subset A_3 \subset \ldots \subset A_n \subset \ldots$$

kümelerinin herbiri $\mathbb{R}$'nin özaltkümesiyse, bunların hepsini birden içeren bir küme $\mathbb{R}$'ye eşit olabilir, yani bunların hepsinin bileşimi $\mathbb{R}$ olabilir. Örneğin, $n \in \mathbb{N}$ için,

$$A_n = (-\infty,\, n)$$

aralığıysa, bu A_n'lerin hepsi özaltkümedir, hiçbiri maksimal bir özaltküme değildir, ama bileşimleri $\mathbb{R}$'dir.

Bu zorluğu yenmek için bu problemi bir önceki probleme dönüştürüp belli bir a için ($a = 1$ olabilir), bu belirlenmiş a'yı içermeyen maksimal bir altkümeyi bulmaya çalışmalıyız. Şans bu ya, a'yı içermeyen maksimal bir altküme $\mathbb{R}$'nin maksimal bir özaltkümesidir.

F.1.4 Orta Zorlukta Bir Problem

Şimdi bir başka probleme el atalım. Bu problem daha zor olacak. Kesirli sayılar kümesi $\mathbb{Q}$'nün çıkarma altında kapalı ve 1'i içermeyen maksimal bir altkümesini bulmaya çalışalım. Yani öyle bir $M \subseteq \mathbb{Q}$ kümesi bulmaya çalışalım ki,

1. Her x, $y \in M$ için, $x - y \in M$ olsun.
2. 1 sayısı M'de olmasın.
3. M, $\mathbb{Q}$'nün yukardaki iki koşulu sağlayan maksimal bir altkümesi olsun. Yani $M \subset N \subseteq \mathbb{Q}$ ise, N ya çıkarma altında kapalı olmayacak (yani birinci koşulu sağlamayacak) ya da 1'i içerecek (yani ikinci koşulu sağlamayacak).

"Maksimal" koşulundan vazgeçip ilk iki koşulu sağlayan bir küme bulalım. $\emptyset$ ya da $\{0\}$ bu tür kümelerdendir. Çift sayılar kümesi $2\mathbb{Z}$ de çıkarma altında kapalıdır ve 1'i içermez. Bu iki özelliği sağlayan herhangi bir küme alalım ve bu kümeye A_0 adını verelim. Eğer A_0 ilk iki koşulu sağlayan maksimal bir kümeyse sorun yok, çözüme ulaştık. Değilse, ilk iki koşulu sağlayan ve A_0'dan daha büyük bir $A_1 \subset \mathbb{Q}$ vardır.

Bu işlemi sürdürelim.

$$A_0 \subset A_1 \subset A_2 \subset A_3 \subset \ldots \subset A_n$$

kümelerini elde ederiz. Amacımıza henüz ulaşmamışsak, yani A_n, ilk iki koşulu sağlayan maksimal bir küme değilse devam edelim. Sonlu bir aşamada ilk iki koşulu sağlayan $\mathbb{Q}$'nün maksimal bir altkümesine rastlamamışsak şöyle bir zincir elde ederiz:

$$A_0 \subset A_1 \subset A_2 \subset A_3 \subset \ldots \subset A_n \subset \ldots$$

Bunların her biri $\mathbb{Q}$'nün 1'i içermeyen ve çıkarma altında kapalı altkümeleri, ama hiçbiri en büyüğü değil, yani her biri bir öncekinden daha fazla eleman içeriyor. Bunların bileşimini alalım:

$$A_\omega = \bigcup_{n \in \mathbb{N}} A_n.$$

A_ω da 1'i içermez, çünkü A_n'lerin hiçbiri 1'i içermiyor. (A_ω'nın 1'i içermesi için A_n'lerin en az birinin 1'i içermesi gerekir.) Ayrıca A_ω da çıkarma altında kapalıdır. Bunu kanıtlayalım. A_ω'dan iki eleman alalım, diyelim x ve y. Bu iki eleman A_ω'da olduğundan, herbiri A_n'lerden birindedir, ama ikisi birden aynı

A_n'de olmayabilir, en azından bundan henüz emin değiliz, birazdan olacağız ama... Diyelim,

$$x \in A_n \text{ ve } y \in A_m.$$

Şimdi ya $n \leq m$ ya da $m \leq n$. Durum x ve y açısından simetrik olduğundan, birinin diğerinden farkı yok, dolayısıyla gönül rahatlığıyla $m \leq n$ eşitsizliğini varsayabiliriz. Böylece,

$$y \in A_m \subseteq A_n$$

olur. Demek ki hem x, hem de y sayıları A_n kümesindeler. Ama A_n çıkarma altında kapalı. Buradan $x - y \in A_n$ çıkar. Ama şimdi, $A_n \subseteq A_\omega$ olduğundan, $x - y \in A_\omega$ çıkar. Böylece A_ω kümesinin çıkarma altında kapalı olduğunu kanıtlamış olduk.

Demek ki bir sonraki aşamada A_ω kümesini alabiliriz. Bu küme A_n kümelerinin hepsinden daha büyük ve ayrıca 1'i içeriyor ve de çıkarma altında kapalı. Kaldığımız yerden A_0 yerine A_ω ile devam edelim. Eğer A_ω kümesi, 1'i içermeyen ve çıkarma altında kapalı olan maksimal bir kümeyse, o zaman işimiz bitti, istediğimizi bulduk. Öyle değilse, o zaman, A_ω'yı altküme olarak içeren (yani A_ω'nın üstkümesi olan) ama A_ω'dan daha fazla eleman içeren öte yandan 1'i içermeyen ve gene çıkarma altında kapalı bir küme var demektir. Bu kümeye $A_{\omega+1}$ diyelim. Eğer $A_{\omega+1}$ kümesi 1'i içermeyen ve çıkarma altında kapalı maksimal bir kümeyse, o zaman problemimizi çözdük demektir... Değilse, $A_{\omega+1}$'in, $A_{\omega+1}$'den daha büyük ve 1'i içermeyen ve çıkarma altında kapalı bir üstkümesi var demektir. Bu kümeye $A_{\omega+2}$ diyelim... Bunu böylece sürdürürüz... Eğer

$$A_\omega \subset A_{\omega+1} \subset A_{\omega+2} \subset \ldots \subset A_{\omega+n} \subset \ldots$$

zincirinin $A_{\omega+n}$ halkalarından hiçbiri 1'i içermeyen ve çıkarma altında kapalı maksimal bir küme değilse, bunların bileşimi örneğin, 1'i içermeyen ve çıkarma altında kapalı ve yukardakilerin herbirinden daha büyük bir kümedir. Böyle bir kümeye $A_{\omega 2}$ adını verelim. Eğer $A_{\omega 2}$ kümesi 1'i içermeyen ve çıkarma altında kapalı maksimal bir kümeyse, o zaman problemimizi çözdük demektir... Değilse, işlemi devam ettirebiliriz... Eğer belli bir aşamada, 1'i içermeyen ve çıkarma altında kapalı maksimal bir altkümeye rastlarsak o zaman çabalarımız amacına ulaşmış demektir, duralım. Ama eğer kümeleri hep 1'i içermeyecek ve çıkarma altında kapalı olacak biçimde büyütebiliyorsak, bir adım ileri gidelim. Hep ileri gidebileceğimizi biliyoruz.

$$A_{\omega 2} \subset A_{\omega 2+1} \subset A_{\omega 2+2} \subset \ldots \subset A_{\omega 2+n} \subset \ldots$$

Eğer sürekli başarısızlığa uğramışsak, bir sonraki aşamada bu kümelerin bileşimini içeren ama 1'i içermeyen ve çıkarma altında kapalı herhangi bir küme alıp buna $A_{\omega 3}$ diyelim ve yolumuza devam edelim...

Bir zaman sonra istediğimiz kümeye rastlayacak mıyız? Zor soru...

Çözüm: Yukarıdaki yöntemi terkedelim, belli ki bir yere varamayacak. Aradığımız kümelerden birini ayan beyan yazacağım:

p herhangi bir asal sayı olsun.

$$M = \{pa/b \colon a,\, b \in \mathbb{Z} \text{ ve } p,\, b\text{'yi bölmüyor}\}$$

olsun. M çıkarma altında kapalıdır, bunu görmek kolay. Ayrıca M, 1'i de içermez; çünkü aksi takdirde, p'nin b'yi bölmediği $a,\, b \in \mathbb{Z}$ tamsayıları için $1 = pa/b$ olur, buradan $pa = b$ ve p'nin b'yi böldüğü çıkar ki bunun böyle olmadığını biliyoruz... Demek ki $1 \notin M$.

Şimdi M'nin, $\mathbb{Q}$'nün bu iki özelliği olan maksimal bir altkümesi olduğunu kanıtlayalım. N, M'den daha büyük ve çıkarma altında kapalı herhangi bir kesirli sayılar kümesi olsun. 1'in N'de olduğunu kanıtlayacağız ve böylece istediğimiz kanıtlanmış olacak.

Önce çıkarma altında kapalı kümelerin çok bilinen ve kolay kanıtlanan bir özelliğini verelim:

Önsav F.1. *Eğer N çıkarma altında kapalıysa ve boşküme değilse, o zaman $0 \in N$ ve N toplama altında da kapalıdır. Ayrıca $-N \subseteq N$ olur.*

Kanıt: $N \neq \emptyset$ olduğundan, N'de en az bir eleman vardır. a ve b, (birbirine eşit ya da değil) N'nin herhangi iki elemanı olsun. N çıkarma altında kapalı olduğundan,

$$0 = a - a \in N,$$

$$-a = 0 - a \in N$$

ve

$$a + b = a - (-b) \in N$$

olur. □

Sonuç F.2. *N ve M, $\mathbb{Q}$'nün çıkarma altında kapalı iki altkümesi olsun. Eğer $M \subseteq N$ ve $x \in N$ ise o zaman $M + Zx \subseteq N$ olur.* □

Şimdi biraz önce tanımladığımız,

$$M = \{pa/b \colon a,\, b \in \mathbb{Z} \text{ ve } p,\, b\text{'yi bölmüyor}\}$$

kümesinin, 1'i içermeyen ve çıkarma altında kapalı maksimal kesirli sayı kümesi olduğunu kanıtlayalım.

Teorem F.3. *Yukarıda tanımlanan M kümesi, 1'i içermeyen ve çıkarma altında kapalı bir maksimal kesirli sayı kümesidir.*

Kanıt: N, M'nin çıkarma altında kapalı herhangi bir üstkümesi olsun. Diyelim, N'de olan ama M'de olmayan bir x kesirli sayısı var. a ve b tamsayıları için, $x = a/b$ yazalım. a ve b'nin birbirine asal olduklarını varsayabiliriz. x, M'de olmadığından, p, a'yı bölmez. Demek ki a ve p birbirine asallar. Dolayısıyla $pu + av = 1$ eşitliğini sağlayan u ve v tamsayıları vardır [S]. Dolayısıyla,

$$pu + vbx = pu + vb(a/b) = pu + va = 1.$$

Ama $pu = pu/1 \in M$ ve $vbx \in \mathbb{Z}x$. Dolayısıyla,

$$1 = pu + vbx \in M + \mathbb{Z}x \subseteq N.$$

Böylece, M'nin özaltkümesi olduğu çıkarma altında kapalı her kesirli sayı kümesinin 1'i içermek zorunda olduğunu kanıtladık. Demek ki M, 1'i içermeyen ve çıkarma altında kapalı olan $\mathbb{Q}$'nün bir maksimal altkümesidir. □

F.1.5 Çetin Bir Problem

Son olarak çetin bir problemi ele alacağız. Problemimiz bir önceki problemin benzeri olacak. Yalnız bu sefer $\mathbb{Q}$'nün değil $\mathbb{R}$'nin altkümeleriyle uğraşacağız.

$\mathbb{R}$'nin çıkarma altında kapalı ve 1'i içermeyen maksimal bir altkümesini bulmaya çalışacağız. Yöntemimizi biliyorsunuz, eğer çıkarma altında kapalı ve 1'i içermeyen bir küme maksimalsa, duralım; değilse o kümeden bir büyüğü vardır. Şimdi o büyük kümeden hareket edelim. Bunu böylece sürdürelim. Eğer hiçbir zaman maksimal bir kümeye rastlamazsak, o zaman

$$A_0 \subset A_1 \subset A_2 \subset A_3 \subset \ldots \subset A_n \subset \ldots$$

diye bir dizi elde ederiz. Bu dizideki kümelerin her biri bir öncekinden daha büyüktür. Her biri çıkarma altında kapalıdır. Hiçbirinde 1 yoktur. Şimdi bu kümelerin bileşimini alalım. Bu bileşim de çıkarma altında kapalıdır ve 1'i içermez. Şimdi A_0'la yaptığımızı bu bileşimle yapalım. Ve bunu çıkarma altında kapalı ve 1'i içermeyen maksimal bir kümeye rastlayana dek sürekli sürdürelim.

Bu yöntemle, böyle bir kümeye rastlama şansımız var mı? [Sİ] ders notlarında gördüklerimiz böyle bir maksimal kümeye rastlayacağımız konusunda bize bir güvence veremez.

Peki, bir önceki problemdeki gibi, çıkarma altında kapalı ve 1'i içermeyen maksimal bir kümeyi - sanki gökten inmiş gibi - okurlara sunabilir miyiz? Sunamayız! Sadece biz değil kimse sunamaz.

Böyle bir kümenin varlığı bir sonraki bölümde söz edeceğimiz **Zorn Önsavı** kullanılarak kanıtlanabilir. Zorn Önsavı'nın kanıtı da Seçim Aksiyomu'nu gerektirir, Seçim Aksiyomu olmadan yapılamaz.

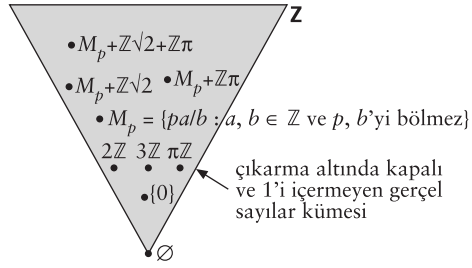
Seçim Aksiyomu'nun yardımıyla kanıtlayacağımız Zorn Önsavı sayesinde, elle, akılla, emek vererek bulamayacağımız matematiksel nesnelerin varlığını kanıtlayabileceğiz. Zorn Önsavı'nı (daha doğrusu Seçim Aksiyomu'nu) matematikçilerin yardımına yetişen tanrısal bir el olarak algılayabilirsiniz: Seçim Aksiyomu sayesinde, olmasını çok arzuladığımız ama geleneksel yöntemlerle varlığı kanıtlanamayan kümeler var olacaklar.

F.2 Zorn Önsavı ve Birkaç Sonucu

F.2.1 Hazırlık

Okurun bir önceki altbölümü okuduğunu ve orada ortaya konulan derin sorunu kavradığını varsayıyoruz. O altbölümde ele aldığımız ama pek başarılı olamadığımız kanıtlama yönteminden, yani bir kümenin belli koşullara sahip maksimal bir altkümesinin varlığını gösterme çabamızdan sözedeceğiz bu altbölümde.

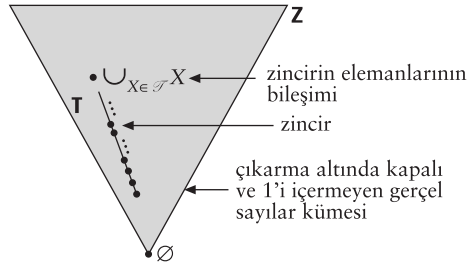
Geçen altbölümde, son örnekte, çıkarma altında kapalı olan ve 1'i içermeyen gerçel sayılar kümelerini ele almıştık. Bu bölümün en azından başında $\mathbb{R}$'nin bu tür altkümelerine yoğunlaşalım. $\mathbb{R}$'nin bu tür altkümelerini eleman olarak içeren kümeye $\mathcal{Z}$ adını verelim. Uzunca bir süre bu örnekle uğraşacağız.



Yukardaki şekilde $\mathcal{Z}$'yi çizdik. Altkümeleri aşağıya, üstkümeleri yukarıya yazdık, yani $\mathcal{Z}$'nin elemanlarının (altküme ilişkisine göre aşağıdan yukarıya doğru) sıralanmasına dikkat ettik: $A \subset B$ ise A'yı alta B'yi yukarıya yazdık. Dolayısıyla boşkümeyi en alta koyduk. Bunun bir üstünde $\mathcal{Z}$'nin tek sonlu sayıda elemanı olan $\{0\}$ kümesi var. Daha yukarda 1 ve -1 dışındaki a sayılarının katlarından oluşan $a\mathbb{Z}$ kümeleri var. Resimde göstermedik ama bir üst katta $\sqrt{2}\mathbb{Z}+\pi\mathbb{Z}$ gibi iki elemanla "üretilen" çıkarma altında kapalı ve 1'i içermeyen $a\mathbb{Z}+b\mathbb{Z}$ kümeleri var. (Soru: $\sqrt{2}\mathbb{Z}+\sqrt{3}\mathbb{Z}$ kümesi $\mathcal{Z}$'de midir?) Resimde bir de M_p diye bir küme var, tanımına bakılırsa 1'i içermiyor ve çıkarma altında kapalı, yani $\mathcal{Z}$'de. Velhasıl, $\mathbb{R}$'nin çıkarma altında kapalı ve 1'i içermeyen her altkümesi $\mathcal{Z}$'nin bir elemanı ve bu altkümeler küçükten büyüğe doğru dizilmişler.

$\mathcal{Z}$ kümesinin ***zincir özelliği*** adı verilen şu özelliği var:

Eğer $\mathcal{T} \subseteq \mathcal{Z}$ ise ve her $X, Y \in \mathcal{T}$ için ya $X \subseteq Y$ ya da $Y \subseteq X$ ise, o zaman $\mathcal{T}$ 'nin elemanlarının bileşimi olan $\cup_{X\in\mathcal{T}} X$ kümesi de $\mathcal{Z}$'dedir.



Bunun kanıtı oldukça kolay. Eğer $\bigcup_{X\in\mathcal{T}} X$ kümesi 1'i içerseydi, $\mathcal{T}$'nin bir X elemanı da 1'i içermek zorunda olurdu ki, bu imkânsız, çünkü

$$X \in \mathcal{T} \subseteq \mathcal{Z}.$$

Demek ki $\bigcup_{X\in\mathcal{T}} X$ kümesi 1'i içeremez. Şimdi $\bigcup_{X\in\mathcal{T}} X$ kümesinin çıkarma altında kapalı olduğunu kanıtlayalım. x ve y, $\bigcup_{X\in\mathcal{T}} X$ kümesinden iki eleman olsun. O zaman, $x \in X$ ve $y \in Y$ ilişkilerinin doğru olduğu $X, Y \in \mathcal{T}$ kümeleri vardır. $\mathcal{T}$'nin zincir özelliğinden dolayı ya $X \subseteq Y$ ya da $Y \subseteq X$ olmalı. x ve y açısından durum simetrik olduğundan, $Y \subseteq X$ ilişkisini kabul etmede bir mahsur yok. O zaman $y \in Y \subseteq X$ ve hem x hem de y, X'in birer elemanı. Ama X çıkarma altında kapalı bir küme. Demek ki $x - y \in X$. Öte yandan, X elbette $\bigcup_{X\in\mathcal{T}} X$ kümesinin bir altkümesi. Sonuç: $x - y \in \bigcup_{X\in\mathcal{T}} X$ ve $\bigcup_{X\in,\mathcal{T}} X$ kümesi çıkarma altında kapalı.

$\mathcal{Z}$'nin, "her $X, Y \in \mathcal{T}$ için ya $X \subseteq Y$ ya da $Y \subseteq X$" özelliğini sağlayan $\mathcal{T}$ altkümelerine zincir diyelim. O zaman yukardaki özellik şöyle okunur:

$\mathcal{Z}$'nin her zincirinin bileşimi gene $\mathcal{Z}$'dedir.

Geçen bölümde, bu özelliği, $\mathcal{Z}$'nin sayılabilir sonsuzlukta elemanı olan zincirleri için kullanmıştık. Birazdan yazacağımız Zorn Önsavı'nda $\mathcal{Z}$'nin sayılabilir ya da sayılamaz sonsuzluktaki tüm zincirlerini ele almamız gerekecek.

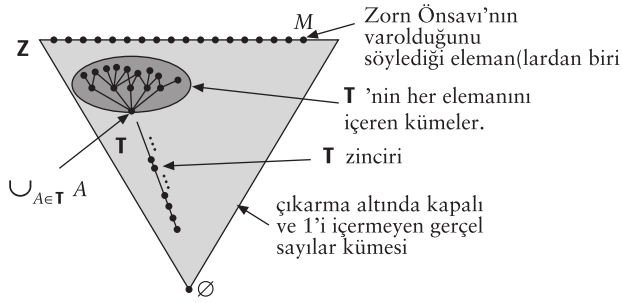
Bu arada, $\bigcup_{X\in\mathcal{T}} X$ kümesinin kimileyin $\bigcup \mathcal{T}$ olarak yazıldığını da anımsatalım. Bu tıkız yazılım, simge sayısında hatırı sayılır bir indirim sağlar.

Birazdan ifade edeceğimiz Zorn Önsavı için "$\mathcal{Z}$'nin her zincirinin bileşimi gene $\mathcal{Z}$'dedir" özelliğinden daha zayıf bir özellik gerekir. İşte o özellik:

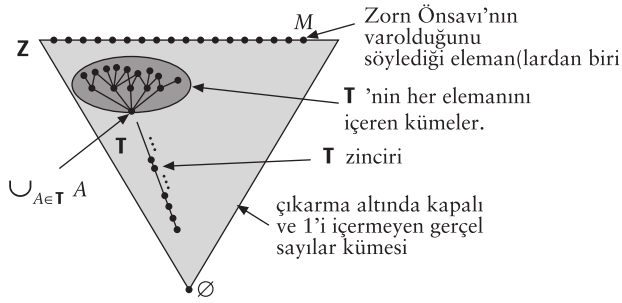
$\mathcal{T}$, $\mathcal{Z}$'nin herhangi bir zinciriyse, $\mathcal{Z}$'de $\mathcal{T}$'nin her elemanından büyükeşit bir eleman vardır.

Yukardaki örnekte, eğer $\mathcal{T} \subseteq \mathcal{Z}$ bir zincirse, $\bigcup \mathcal{T}$, $\mathcal{Z}$'dedir ve $\mathcal{T}$'nin her elemanından büyükeşittir. (Eğer $A \subseteq B$ ise B'nin A'dan ***büyükeşit*** olduğunu

söylüyoruz. Eğer $A \subset B$ ise B'nin A'dan ***büyük*** olduğunu söyleyeceğiz. Aslında, aşağıdaki şekilden de görüleceği üzere, $\bigcup \mathcal{T}$, $\mathcal{Z}$'de bulunan ve $\mathcal{T}$'nin her elemanınından daha büyükeşit olan elemanların en küçüğüdür. Ama bu özelliğin bir önemi olmayacak bizim için.)



Birazdan tanıtacağımız Zorn Önsavı, eğer $\mathcal{Z}$ yukardaki son italik koşulu sağlıyorsa, o zaman $\mathcal{Z}$'nin en az bir maksimal elemanının olduğunu söyler.

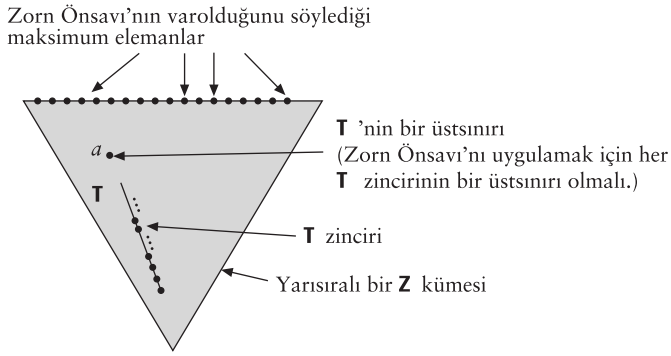


Yani, Zorn Önsavı, $\mathcal{Z}$ üzerine koşulan yukardaki italik koşul doğru olduğunda, öyle bir $M \in \mathcal{Z}$ vardır ki, der, $\mathcal{Z}$'nin hiçbir elemanı M'den daha büyük olamaz, en fazla M'ye eşit olabilir. Ama dikkat: Bu maksimal elemanlardan sonsuz sayıda olabilir (ki çoğu zaman da öyledir).

F.2.2 Zorn Önsavı

Artık Zorn Önsavı'nı anlayacak bilgi birikimine sahibiz:

Önsav F.4. *$(\mathcal{Z}, \leq)$ kısmi sıralı bir küme olsun. Eğer $\mathcal{Z} \neq \emptyset$ ise ve $\mathcal{Z}$'nin her zincirinin bir üstsınırı varsa o zaman $\mathcal{Z}$'nin maksimal bir elemanı vardır.*



Dikkat ederseniz, Zorn Önsavı, geçen bölümde yapmak isteyip de yapamadığımızı herhangi bir zahmete girmeksizin yapıyor. Bir tür sihirbazlık, ya da Tanrı'nın eli diyebilirsiniz.

Zorn Önsavı'nı [N4]'te Seçim Aksiyomu'nu kullanarak kanıtlayacağız. Burada Zorn Önsavı'nı kanıtlamadan kabul edip, önsavı kullanan birkaç basit ama önemli örnek vereceğiz.

İlk olarak, Zorn Önsavı'nı kullanarak, daha önce bulmaya çalışıp bulamadığımız, bu bölümde de konu mankeni olarak kullandığımız kümenin varlığını kanıtlayalım:

Teorem F.5. *Gerçel sayılar kümesi* $\mathbb{R}$*'nin çıkarma altında kapalı ve* 1*'i içermeyen maksimal bir altkümesi vardır.*

Kanıt: Zorn Önsavı'nı kullanacağız.

$$\mathcal{Z} = \{A \subseteq \mathbb{R} : A \text{ çıkarma altında kapalı ve } 1 \notin A\}$$

olsun. $\mathcal{Z}$'yi "altkümesi olmak" ilişkisiyle sıralayalım. Şimdi $(\mathcal{Z}, \subseteq)$ kısmi sıralamasının Zorn Önsavı'nın koşullarını sağladığını gösterelim. $\{0\} \in \mathcal{Z}$ olduğundan $\mathcal{Z} \neq \emptyset$. Şimdi ikinci koşulun sağlandığını kanıtlayalım. $\mathcal{T} \subseteq \mathcal{Z}$ bir zincir olsun. $\bigcup \mathcal{T}$,$\mathcal{T}$'nin her elemanının bir üstkümesi olduğundan, eğer $\bigcup \mathcal{T} \in \mathcal{Z}$ ise, $\bigcup \mathcal{T}$, $\mathcal{T}$'nin bir üstsınırı olur. Dolayısıyla $\bigcup \mathcal{T} \in \mathcal{Z}$ önermesini kanıtlayalım. Bunun için iki şey kanıtlamalıyız:

1. $\bigcup \mathcal{T}$ çıkarma altında kapalı olmalı,
2. $\bigcup \mathcal{T}$, 1'i içermemeli.

Birinciden başlayalım. x, $y \in \bigcup \mathcal{T}$ olsun. Bu iki eleman $\mathcal{T}$'nin elemanlarından birindedir, ama ikisi birden aynı elemanda olmayabilir, en azından bundan henüz emin değiliz, birazdan olacağız ama... Diyelim, A, $B \in \mathcal{T}$ için, $x \in A$ ve $y \in B$. Ama $\mathcal{T}$ bir zincir olduğundan,

$$\text{ya } A \subseteq B \text{ ya da } B \subseteq A.$$

Durum x ve y açısından simetrik olduğundan, birinin diğerinden farkı yok, dolayısıyla gönül rahatlığıyla $A \subseteq B$ ilişkisini varsayabiliriz. Böylece,

$$x \in A \subseteq B$$

olur. Demek ki hem x, hem de y, B'de. Ama B çıkarma altında kapalı. Buradan $x - y \in B$ çıkar. Ama şimdi, $B \subseteq \bigcup \mathcal{T}$ olduğundan, $x - y \in \bigcup \mathcal{T}$ olur. Böylece $\bigcup \mathcal{T}$ kümesinin çıkarma altında kapalı olduğunu kanıtlamış olduk.

Şimdi, $1 \notin \bigcup \mathcal{T}$ önermesini kanıtlayalım. $\bigcup \mathcal{T}$ kümesinin elemanları $\mathcal{T}$'nin elemanlarının elemanlarıdır; dolayısıyla 1, $\bigcup \mathcal{T}$ kümesinde olsaydı, 1, $\mathcal{T}$ kümesinin bir elemanının elemanı olurdu. Ama $\mathcal{T}$'nin hiçbir elemanı 1'i içermez. Dolayısıyla, 1 de $\bigcup \mathcal{T}$ kümesinde olamaz. □

Notlar

1. Zorn Önsavı'nda $\mathcal{Z} \neq \emptyset$ koşulunu kanıtlamak genel olarak kolaydır ama gene de unutulmaması gerekir. Eğer $\mathcal{Z}$ boşkümeyse, $\mathcal{Z}$'nin maksimal bir eleman barındırma şansı yoktur!

2. Uygulamada çoğu zaman $\mathcal{Z}$ bir kümeler kümesidir ve kısmi sıralama da $\subseteq$ tarafından verilmiştir. Bu arada, $\mathcal{Z}$ 'de bir kısmi sıralama tanımlanmamışsa önsavı uygulayamayacağınıza dikkatinizi çekerim.

3. Uygulamada çoğu zaman $\mathcal{Z}$'nin bir $\mathcal{T}$ zincirinin en küçük üstsınırı bulunmaya çalışılır (daha kolaydır çünkü) ama böyle bir zorunluluk yoktur tabii.

4. Zorn Önsavı'nın var olduğunu söylediği maksimal elemanı görebiliyorsanız, yani açık açık tanımını yazabiliyorsanız ya da diğer tüm maksimal elemanlardan ayırdedebiliyorsanız, o zaman Zorn Önsavı'nı gereksiz yere kullanmışsınız demektir, maksimal elemanın varlığını Zorn Önsavı'nı kullanmadan da kanıtlayabilirdiniz.

Örneğin, Zorn Önsavı yardımıyla yukarda varlığı kanıtlanan $\mathbb{R}$'nin çıkarma altında kapalı ve 1'i içermeyen maksimal bir altkümesini açık açık yazamazsınız. Zorn Önsavı doğruysa böyle maksimal bir altküme vardır ama birini bile "işte budur" diye gösteremezsiniz. Öte yandan aynı problemi $\mathbb{Q}$ için sormuş ve Teorem F.3'te açık açık bir çözümünü bulmuştuk. Demek ki $\mathbb{Q}$ için Zorn Önsavı gerekmiyor ama $\mathbb{R}$ için gerekiyor. İlginç...

5. Zorn Önsavı'nı gerekmedikçe kullanmamakta estetik ve matematiksel yarar vardır. Örneğin maksimal elemandan tek bir tane varsa, Zorn Önsavı'nı gereksiz yere kullanmış olmalısınız. Aynı teoremi bu sefer Zorn Önsavı kullanmadan kanıtlamaya çalışmalısınız.

6. Zorn Önsavı'nın varsayımlarını sağlayan $\mathcal{Z}$ kümelerine talihsiz bir şekilde ***tümevarımsal*** küme denir; [N3]'de verdiğimiz tümevarımsal küme tanımıyla karıştırılmamalı.

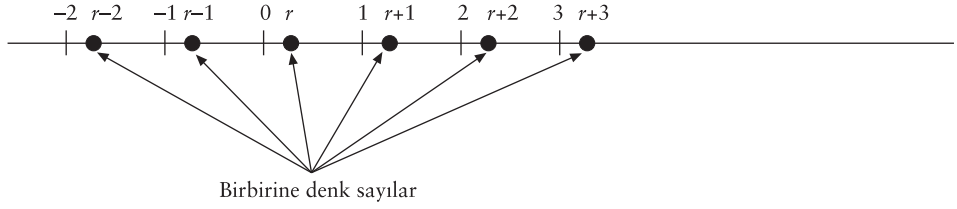
Zorn Önsavı uygulaması olarak bir başka örnek verelim.

Eğer iki r ve s gerçel sayısı arasındaki fark tamsayıysa bu iki gerçel sayıya birbirine ***denk*** diyelim ve bunu $r \equiv s$ olarak gösterelim. Demek ki,

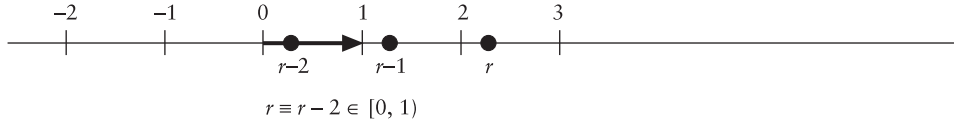
$$r \equiv s \Leftrightarrow r - s \in \mathbb{Z}.$$

Örneğin, π, $\pi+1$, $\pi+2$, $\pi-3$ sayıları birbirine denktir. π'ye denk gerçel sayılar belli bir $n \in \mathbb{Z}$ tamsayısı için $\pi + n$ olarak yazılan sayılardır.

Bu, daha genel olarak doğrudur, her r gerçel sayısı için, r'ye denk gerçel sayılar, belli bir $n \in \mathbb{Z}$ için $r + n$ olarak yazılan sayılardır.



Şimdi amacımız, öyle bir $X \subseteq \mathbb{R}$ kümesi bulmak ki, her $r \in \mathbb{R}$ için, $r \equiv x$ denkliğinin doğru olduğu bir ve bir tek $x \in X$ olsun. Böyle bir X kümesi kolaylıkla bulunabilir, örneğin $X = [0, 1)$ yarı açık aralığı istediğimiz özelliği sağlar.



Nitekim, eğer bir r gerçel sayısı verilmişse, r'ye yeterince 1 ekleyerek ya da r'den yeterince 1 çıkararak, $[0, 1)$ aralığında r'ye denk bir sayıya ulaşırız ve $[0, 1)$ aralığında r'ye denk başka bir sayı da yoktur.

Şu basit teoremi kanıtladık:

Teorem F.6. *Öyle bir $X \subseteq \mathbb{R}$ vardır ki, her $r \in \mathbb{R}$ için $r - x$'in tamsayı olduğu bir ve bir tek $x \in X$ vardır. ($X = [0, 1)$ alınabilir.)*

Yukardaki basit teoremde $\mathbb{Z}$ yerine $\mathbb{Q}$ koyarsak teorem çok daha çetin bir önermeye dönüşür: □

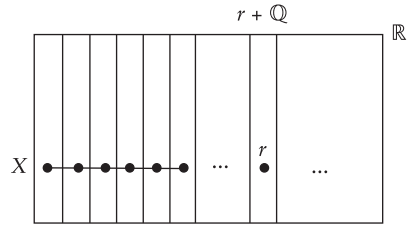
Teorem F.7. *Öyle bir $X \subseteq \mathbb{R}$ vardır ki, her $r \in \mathbb{R}$ için $r - x$ sayısının kesirli bir sayı olduğu bir ve bir tek $x \in X$ vardır.*

Kanıt: $\mathbb{R}$ kümesi üzerine $\equiv$ ilişkisini,

$$r \equiv s \Leftrightarrow r - s \in \mathbb{Q}$$

olarak tanımlayalım. Daha önceki $\mathbb{Z}$ burada $\mathbb{Q}$ oldu. Ama bu sefer, $[0, 1)$ aralığı gibi açık seçik bir yanıtı yok bu sorunun.

Öyle bir $X \subseteq \mathbb{R}$ kümesi bulmak istiyoruz ki, her $r \in \mathbb{R}$ için, $r \equiv x$ denkliğinin doğru olduğu bir ve bir tek $x \in X$ olsun.



Böyle bir X kümesi vardır. Hem de çok vardır. Ama biri bile elle bulunamaz, illa Zorn Önsavı gerekiyor!

X kümesinin varlığını hemen kanıtlayalım. Kanıtta (zorunlu olarak) Zorn Önsavı'nı kullanacağız. (Aslında aynı kanıt Seçim Aksiyomu kullanılarak çok daha basit bir biçimde yapılabilir ama vereceğimiz kanıt Zorn Önsavı'nın kullanıldığı kanıtların tipik özelliklerini taşıdığından, kanıtımızı önemsiyoruz.)

$$\mathcal{Z} = \{X \subseteq \mathbb{R} \colon X\text{'in iki farklı elemanı birbirine denk olamaz}\}$$

olsun. Yani $X \in \mathcal{Z}$ ise, X'in iki farklı elemanının farkı $\mathbb{Q}$'de olamaz. $\mathcal{Z}$'yi "altküme olma" ilişkisiyle sıralandıralım. Bakalım $\mathcal{Z}$, Zorn Önsavı'nın koşullarını sağlıyor mu?

Boşküme ve tek elemanlı her sayı kümesi $\mathcal{Z}$ 'de olduğundan, $\mathcal{Z}$ boşküme değildir. Gözü örneğe doymayan okur, $\{1, \sqrt{2}\}$ kümesinin de $\mathcal{Z}$'de olduğunu kanıtlayabilir.

Şimdi $\mathcal{T} \subseteq \mathcal{Z}$ bir zincir olsun. $\bigcup \mathcal{T}$'nin $\mathcal{Z}$'nin bir elemanı olduğunu kanıtlayacağız. x ve y, $\cup\mathcal{T}$ kümesinden iki değişik sayı olsun. Bu iki eleman $\mathcal{T}$ 'nin elemanlarından birinin elemanıdır. Diyelim, A, $B \in \mathcal{T}$ için, $x \in A$ ve $y \in B$. Ama $\mathcal{T}$ bir zincir olduğundan, ya $A \subseteq B$ ya da $B \subseteq A$. Durum x ve y açısından simetrik olduğundan, birinin diğerinden farkı yok, dolayısıyla gönül rahatlığıyla $A \subseteq B$ ilişkisini varsayabiliriz. Böylece, $x \in A \subseteq B$ olur. Demek ki hem x, hem de y, B'de. B, $\mathcal{Z}$'de olduğundan x ve y denk olamazlar.

Demek ki $\mathcal{Z}$, Zorn Önsavı'nın önkoşullarını sağlıyor. Dolayısıyla Zorn Önsavı'na göre $\mathcal{Z}$'nin bir maksimal elemanı olmalı. Bu elemana X diyelim. Şimdi bu X'in dilediğimiz X olduğunu kanıtlayacağız.

$r \in \mathbb{R}$ olsun. Diyelim r'nin denk olduğu bir $x \in X$ yok. O zaman r, X'te olamaz. Şimdi $X_1 = X \cup \{r\}$ olsun. X_1, X'ten daha büyük olduğundan, X_1, $\mathcal{Z}$ kümesinde olamaz. Ama biz gene de X_1'in $\mathcal{Z}$'de olduğunu kanıtlama başarısında bulunacağız.

Eğer X_1, $\mathcal{Z}$'de olmasaydı, o zaman X_1'de $x \equiv y$ denkliğini sağlayan iki farklı x ve y elemanı olurdu.

$$X_1 = X \cup \{r\} \text{ ve } X \in \mathcal{Z}$$

olduğundan, hem x hem de y, X'te olamaz, demek ki ikisinden biri r'ye eşit olmalı. Diyelim $y = r$. Ama o zaman da $r \equiv x \in X$ olur, oysa biz böyle bir x'in

olmadığını varsaymıştık. Bir çelişki. Demek ki böyle bir $r \in \mathbb{R}$ yok. Dolayısıyla $\mathbb{R}$'nin her elemanı X'in bir elemanına denktir.

Eğer $\mathbb{R}$'nin bir elemanı X'in iki elemanına denk olsaydı, o zaman X'in o iki elemanı birbirine denk olurdu, dolayısıyla $X \in \mathcal{Z}$ olduğundan, bu iki eleman birbirine eşit olurdu. Demek ki $\mathbb{R}$'nin her elemanı X'in bir ve bir tek elemanına denktir. Kanıtımız bitmiştir. □

Kaynakça

[**9**] M. Ashbacher, **Finite Group Theory**, Cambridge University Press, 1986.

[B] Baumslag, Gilbert, **Lecture Notes on Nilpotent Groups**, AMS (Conference Board of the Mathematical Sciences, Regional Conference Series in Mathematics) 1971.

[Ch1] Chernikov, S. N., *Complete groups with ascending central series*, Mat. Sb. 18 (1946) 397–422 (Rusça).

[Ch2] Chernikov, S. N., *On the theory of complete groups*, Mat. Sb. 22 (1948) 319–348, 455–456.

[Co] Conrad, Keith, *Consequences of Sylow Theorems*, http://www.math.uconn.edu/∼kconrad/-blurbs/grouptheory/sylowapp.pdf (son erişim: 27 Ekim 2013) ve daha genel olarak http://www.math.uconn.edu/∼kconrad/blurbs/.

[D] Dixmier, S., *Exposants des quotients des suites centrales descendantes et ascendantes d'un groupe*, C.R. Acad. Sci. Paris 258 (1964) 2751–2753.

[FT] Feit, W. ve Thompson, J. G., *Solvability of groups of odd order*, Pacific J. Math. 13 (1963) 775–1029.

[F] Fuchs, L., **Abelian Groups**, Publishing House of the Academy of Sciences 1958 ya da Pergamon Press 1960.

[G] Griffith, Phillip A., **Infinite Abelian Group Theory**, The University of Chicago Press 1970.

[H] Hall, P., *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. (2) 36 (1933) 29–62.

[Hi] K. Hirsch, *On infinite soluble groups II*, Proc. London Math. Soc (2) 44 (1938) 336–344.

[Kap] Kaplansky, Irving, **Infinite Abelian Groups**, University of Michigan 1954.

[Ku] Kurosh, A. G., **Theory of Groups**, AMS Chelsea Publishing House 1960, İngilizceye çeviren K. A. Hirsch (iki cilt).

[Ro] Rosenlicht, M., *On a result of Baer*, Proc. Amer. Math. Soc. 12 (1961) 984–988.

[La] Lang, Serge, **Algebra**, xxx.

[N1] Nesin, Ali, **Sezgisel Kümeler Kuramı**, 3'üncü basım, Nesin Yayıncılık 2011.

[N2] Nesin, Ali, **Sayma**, Nesin Yayıncılık 2013.

[N3] Nesin, Ali, **Sayıların İnşası**, Nesin Yayıncılık tarafından muhtemelen 2014'te yayımlanacak. Bkz. TÜBA açık ders notları: http://www.acikders.org.tr/course/category.php?id=2.

[N4] Nesin, Ali, **Aksiyomatik Kümeler Kuramı**, Nesin Yayıncılık tarafından yayımlanacak. Bkz. TÜBA açık ders notları: http://www.acikders.org.tr/course/category.php?id=2.

[P] Passman, D., **Permutation Groups**, Mathematics Lecture Series, Benjamin, New York, 1968.

[R] Reineke, J., *Minimale Gruppen*, Z. Math. Logik Grundl. Math. 21 (1975) 357–379.

[Sp] Spitznagel, E. L., *Note on the Alternating Group*, Amer. Math. Monthly 75 (1968), 68-69.

[Su] Suzuki, Michio, **Group Theory I ve II**, Springer-Verlag 1982 ve 1986. (Japonca orijinali 1977 ve 1978.)

[Wa] Warfield, Robert B., Jr., **Nilpotent Groups**, Springer Verlag, Lecture Notes in Mathematics 513, 1976.

[Wi] Wielandt, Helmut, **Finite Permutation Groups**, Academic Press 1964. Almancadan çeviren R. Berkov.

[Z] Zassenhaus, H., **The Theory of Groups**, Chelsea, 1949.

Dizin

$*$, 343
$-g$, 61
$1 + p^k\mathbb{Z}/p^n\mathbb{Z}$, 172
$<$, 69
AA^{-1}, 22
$D(G)$, 222
G', 128, 137
$G[n]$, 183
$G[p^\infty]$, 183
$G^{(I)}$, 18
H^G, 118
H^g, 118
H^x, 77
$[G : H]$, 116
$[H, K]$, 128
$[a, b]$, 21
$\overline{x}$, 132
$\bigoplus_{i\in I} G_i$, 18
$\circ$, 10
$\coprod_I G$, 18
$\coprod_{i\in I} G_i$, 18
$\dim A$, 208
$\dim_{\mathbb{Z}} A$, 208
$\equiv$, 24
$\hookrightarrow$, 161
$\langle X\rangle$, 96
$\langle X, Y\rangle$, 96
$\langle X^G\rangle$, 127
$\langle x_1, \ldots, x_n\rangle$, 96
$\langle\langle X\rangle\rangle$, 127
$\leq$, 23, 69
$\oplus_I G$, 18
$\rtimes_\varphi$, 196
$\overset{n}{\leq}$, 116
$\overset{n}{\lhd}$, 125
$\varinjlim$, 325
$\mathbb{Z}/n\mathbb{Z}$ halkası, 141
$\mathbb{Z}_{p^\infty}$, 138, 179, 187
a^G, 21
a^b, 21
ng, 61

0, 9, 61
1, 20, 57, 72

abel grubu, 10, 13, 137
ad, 144, 258
Alt 4, 85
Alt n, 46, 50, 98, 116, 125, 127, 184, 198, 250
alterne grup, 46, 250
altgrup, 16, 23, 69
aralarında asal, 26
ardışık makas, 44
artan merkezî seri, 265
Artin, Emil, 257
asal sayı, 26
asimetrik çizge, 307
Aut $\mathbb{G}^n$, 151
Aut $\mathbb{Z}$, 150
ayrık döngü, 35
ayrışmak, 197
azalan merkezî seri, 260
azalan türev serisi, 260

Bézout teoremi, 26
Baer, R., 267
bağımsız küme, 205
basit grup, 126
Baumslag, Gilbert, 349
bijeksiyon, 10
bileşke, 10
birbiriyle değişmek, 20
birim fonksiyon, 11
birinci türev, 128, 137
birleşme özelliği, 9, 10, 12
boşkelime, 130
boyut, 208
bölmek, 24
bölü, 24
bölüm grubu, 125
bölüm kümesi, 113
bölünür, 72
bölünür abel grupları, 229–236
bölünür altgrup, 222
bölünür grup, 72, 134, 138, 148, 179, 222
Burnside, 253
Burnside eşitliği, 253
burulmalı elemanlar, 134
burulmalı eleman, 62, 169
burulmalı grup, 62, 136, 148
burulmasız, 62
burulmasız grup, 136

Cauchy Teoremi, 65, 165
cebir, 6

$C_G(C)$, 21
$C_G(c)$, 20
cisim, 6
Core, 127, 166, 246
çekirdek, 160
çekirdek (etkinin), 245
çifte öteleme, 112
Çin Kalan Teoremi, 169
çözülür grup, 262
çözülür gruplar, 262–264
çözülürlük radikali, 264
çözülürlük sınıfı, 263

Δ, 15
$D(G)$, 222
D_{2n}, 86
D_8, 82
dağılma, 143
deg g, 62
değişmeli grup, 10, 13
derece, 134
derece (Sym n'de), 41, 42
derece (çizgede), 86
derece (elemanın), 62, 114
devirli grup, 97
dihedral grup, 82, 86
direkt limit, 325, 331
direkt sistem, 322
direkt toplam, 18, 184
doğal gömme, 143
doğal izdüşüm fonksiyonları, 17, 18
doğal izdüşüm fonksiyonu, 73
doğal taban, 205
doğal üreteçler, 98
doğrusal bağımlılık, 233
doğrusal bağımsız küme, 205, 233
doğrusal kombinasyonu, 204
döndürü, 19, 288
döngü, 34, 35
döngüsel grup, 97, 136, 137, 169, 187
döngüsel gruplar, 187
dört boyutlu küp, 89

e, 20, 57
ebob, 26
ekok, 29
eksponent, 62
en büyük ortak böleni, 25
en küçük ortak kat, 29
End, 149
End $\mathbb{Q}$, 150
End $\mathbb{Z}_{p^\infty}$, 228
End $\mathbb{Z} \times \mathbb{Z}$, 150
End A, 151
endomorfi, 149
eşküme, 105
eşlenik, 21, 118
eşlenik altgrup, 77
eşlenik elemanlar, 51
eşleniklik sınıfı, 21, 51, 118, 249
eşleşme, 10
eşyapı dönüşümü, 143
etkimek, 241
etkisiz eleman, 9, 10, 13
Euler φ fonksiyonu, 142
Euler, L., 142
Euler-Fermat Teoremi, 142
exp fonksiyonu, 150

$F(G)$, 274
f^{-1}, 41
Feit-Thompson teoremi, 283
Fermat'nın Küçük Teoremi, 142
Fitting altgrubu, 274
$\mathrm{Fix}_X\, G$, 251
$\mathrm{Fix}_X\, g$, 253

G', 128
$G^{(I)}$, 18
G-küme, 241
G-yörünge, 243, 247
$G_1 \times \ldots \times G_n$, 18
$G_1 \oplus \ldots \oplus G_n$, 18
Galois, Evariste, 262
geçişli grup etkisi, 247
G^i, 128
$G[n]$, 183
G^n, 17
G-normal, 124
gof, 10
göbek, 127, 246
gömme, 161
gömülmek, 161
$G[p^\infty]$, 183
grup, 6
grup etkisi, 241
grup homomorfisi, 143
G_x, 246
G_Y, 247
$G_{\{Y\}}$, 247

$H \star K$, 343
halka, 5, 142, 151
Hall, P., 128, 261
Heisenberg p-grubu, 270
hiç tane, 258
Hirsch, 275
$[H, K]$, 128
H-K-ötelemesi, 118
$\mathrm{Hom}(G, H)$, 143
$\mathrm{Hom}(G, H_1 \times H_2)$, 144
$\mathrm{Hom}\left(G, \prod_i H_i\right)$, 145
homomorfi, 143
homomorfik imge, 146
homomorfizma, 143
homoteti, 19
$\mathrm{Hom}(\mathbb{Q}, \mathbb{Z})$, 148
$\mathrm{Hom}(\mathbb{Z}, H)$, 147

$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, H)$, 147
$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$, 147
$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$, 148
Hopf grubu, 347

işaret homomorfisi, 251
iç otomorfi, 152
Id_X, 11
i'inci merkez, 265
ikili işlem, 12
indeks, 116
indirgenemez, 25
Inn, 152, 169
Inn_g, 144, 152, 169
işaret, 46, 251
işlem, 12
izdüşüm fonksiyonu, 17, 18, 73, 116, 132, 144
izometri, 287
izomorfi, 149

kaide, 18, 40
kalıntısal sonlu grup, 347
karakteristik altgruplar, 153
kartezyen çarpım, 16, 17
kelime, 129
Ker, 160
$\mathrm{Ker}(G, X)$, 245
kısıtlanmış çarpım, 18
komütatör, 21, 255, 258, 259, 266
komütatör grubu, 255
Korkmaz, Aslı Can, 3
Kronecker δ sembolü, 99
Kronecker delta sembolü, 202
kuvvet (elemanın), 57
küpün simetrileri, 86–89

Lagrange teoremi, 113
Levi, F.W., 347
$\varinjlim X_i$, 331

makas, 43
maksimal altgrup, 74, 77, 179
maksimal p-altgrup, 76, 164, 277
Mal'cev, I.A., 347
matematiksel yapı, 19
Matsuyama, H., 253
merkez, 73, 125, 137, 253
merkezî altgrup, 73
merkezî eleman, 73
merkezlemek, 20
merkezleyici, 20, 21, 73, 118, 137
mertebe, 62
minimal altgrup, 74
mod, 24
modüler sayılar, 6
modül, 6
modülo, 20, 24

n eleman tarafından üretilmek, 98
n'inci dereceden çözülür grup, 263
n'inci dereceden sıfırkuvvetli grup, 267
n-bölünür, 72
n-sıfırkuvvetli, 267
$N_G(X)$, 73
Nielsen, J., 349
nilpotent grup, 267
noktasal çarpımı, 17
noktasal sabitleyicisi, 247
normal altgrup, 123, 124
normalize etmek, 124, 163
normalleme koşulu, 271
normalleyici, 73, 118, 119, 124, 175
n-sıfırkuvvetli grup, 267

obeb, 26
otomorfi, 19, 149
Ömrüuzun, Halime, 3, 303
öteleme, 19, 105
öteleme (geometrik), 287
özaltgrup, 23, 69
özdeşleştirme, 315
özdeşleştirme fonksiyonları, 325
özdeşlik fonksiyonu, 11

$\mathbb{P}$, 155
$\prod_{i=1}^{n} G_i$, 18
p-grup (Sym n'de), 115
p-altgrup, 76, 163
p-bölünür, 77
p-bölünür grup, 72
p-bölünür, 138, 271, 273
p-eleman, 64, 163, 169, 271
p-group, 253
p-grup, 76, 119, 175
p-sel sayı, 229
p^2 elemanlı gruplar, 119
p^3 elemanlı gruplar, 269
parçalanış sayısı, 54
p-bölünebilir, 165
p-eleman, 64
permütasyon, 10, 33
permütasyonun tersi, 41
Philip Hall eşitliği, 21
π-sayı, 72
$\prod_I G$, 17
piramitin simetrileri, 83–86
Prüfer p-grubu, 138, 179, 187, 189, 224–229, 319, 332

$\mathbb{Q}$, 5, 15, 74, 77, 171, 179, 228, 356–359
$\mathbb{Q}$ (altgruplar), 227
$\mathbb{Q}^*$, 10, 15
$\mathbb{Q}/\mathbb{Z}$, 138
$\mathbb{Q}^{>0}$, 15, 155

$\mathbb{R}$, 5, 15
$\mathbb{R}^*$, 9
$\mathbb{R}^*$, 15

$\mathbb{R}^\star$, 9–10
$\mathbb{R}^\star$, 72
$\mathbb{R}^{>0}$, 10, 15, 72
Reineke, J., 251
rotasyon, 288

sağdan etkisiz eleman, 13
sabitleyici, 246
sadık etki, 245
saf altgrup, 236
sağdan standart etki, 244
Schreier temsilcileri kümesi, 339
Schur, I., 266
Schur, Issai, 257
serbest abel grubu, 205
serbest abel grupları, 201
serbest faktör, 343
serbest grup, 129
serbest tümleyen, 343
serbestçe üretilmiş grup, 215
serbestçe üretmek, 205
Seyfi Türkelli, 287
sg, 46, 251
sıfırkuvvet derecesi, 267
sıfırkuvvetli grup, 267–275
sınıf, 105
sınıflandırmak, 74
simetri, 79, 82
simetrik fark, 15
simetrik grup, 33
S_n, 33
sol ötelemeler kümesi, 112
sol temsilci kümesi, 107
soldan etkisiz eleman, 13
son dilim, 339
sonlu eksponantlı grup, 217
sonlu eksponent, 62, 183
sonsuz derece, 62
standart etki, 244
Supp, 18
Süer, Ergin, 3
Süer, Ersin, 3
Sylow p-altgrupları, 277
Sylow teoremleri, 277
Sylow, Peter Ludwig Mejdell, 277
Sym n'nin Sylow p-altgrupları, 280
Sym X, 10–11, 33
Sym n, 11, 33
Şahin, Çiğdem, 3

$T(G)$, 136
taban, 205
temel makas, 43
temsilciler, 107
ters eleman, 14
ters fonksiyon, 11
tersinir elemanlar, 170
Tolgay, Betül, 3
toplamsal grup, 61
Tor G, 134, 236
transfer, 257
transpozisyon, 43
trişkadan altgrup, 69
trişkadan etki, 243
Türkelli, Seyfi, 3
tümevarımsal limit, 325
tümevarımsal, 364
tümleyen, 197
türev, 128, 259
türev altgrubu, 137
Türkelli, Seyfi, 287

Ulm değişmezleri, 236
uyumlu, 143
üç altgrup önsavı, 128, 261
üreteç, 43, 44, 96
üreteç kümesi, 96, 103, 204
üreteç sayısı, 101, 221
üretilmek, 98, 127

val_p, 155
vektör uzayı, 6

Wilson teoremi, 280

x^0, 57
X^g, 73
x^n, 57

yan çarpım, 18
yanküme, 105
yansıma, 80
yarıçarpım, 196
yerel çözülür, 264
yerel sonlu, 273
yerel sonlu grup, 264, 271
yörünge, 243, 247
yutan eleman, 141

$\mathbb{Z}$, 5, 9, 15, 23–31
$\mathbb{Z}$ (altgruplar), 23
$\mathbb{Z}$-bağımsız küme, 205
$\mathbb{Z}/n\mathbb{Z}$, 6, 140
$(\mathbb{Z}/p^n\mathbb{Z})^\star$, 172
$\mathbb{Z}/p^n\mathbb{Z}$, 135, 136, 142
$\mathbb{Z}/p\mathbb{Z}$, 6, 135, 156
$\mathbb{Z}g$, 66
Z_i, 265
$Z_i(G)$, 265
zincir, 352
zincir özelliği, 360
$\mathbb{Z}_{p^\infty}$ (altgruplar), 226
$\mathbb{Z}^n$, 100
$\mathbb{Z}/n\mathbb{Z}$, 141
Zorn Önsavı, 359, 362
Zorn önsavı, 362
$\mathbb{Z}_{p^\infty}$, 332
$\mathbb{Z}_{p^\infty}$, 138, 179, 187
$\mathbb{Z} \times \mathbb{Z}$, 151
$(\mathbb{Z}/n\mathbb{Z})^\star$, 142