SAKARYA ÜNİVERSİTESİ

Yayın No: 6

CEBİR

Prof. Dr. Fethi ÇALLIALP

ADAPAZARI - 1994

SAKARYA ÜNİVERSİTESİ
Yayın No : 6

CEBİR

Prof. Dr. Fethi ÇALLIALP

Fen - Edebiyat Fakültesi
Öğretim Üyesi

Sakarya Üniversitesi Matbaası
Adapazarı - 1994

ÖNSÖZ

Bu kitap, Üniversitelerimizin Matematik Bölümlerinde okutulmakta olan, **Cebir** veya **Soyut Cebir** dersleri için ders kitabı olarak hazırlanmıştır. Artık Üniversitelerimizde, **Cebir** dersleri farklı kapsamlarda da verilse, içerdiği temel konular belirli olup, belli bir standarda da kavuşmaktadır.

Cebir dersleri, Lineer Cebir dersleri ile paralel veya daha sonra, haftada dört saat civarında iki yarıyılda verildiği planlanarak hazırlanan bu kitabın, öğrencilerimize rehber olacağını ümit ediyorum. Genellikle liseden gelen bir alışkanlıkla, ispat metodlarına alışık olmayan ve soyut kavramlara alışmamış öğrencilerimizin **Cebir** Derslerinde zorlandıkları ve kaynak sıkıntısı çektikleri bir gerçektir. Bu bakımdan, hazırlanan bu kitabın ve baskısı bitmiş olup yeniden düzenlemeye başladığım **Çözümlü Soyut Cebir Problemleri** kitabının bu alanda büyük bir ihtiyaca cevap vereceğine inanıyorum.

Daha önceki denemelerimi takdir ederek, beni böyle bir esere teşvik eden ve her türlü yardımı esirgemeyen meslekdaşlarıma, yazımını büyük bir sabırla gerçekleştiren Melek Öztürk Hanım'a, eserin Sakarya Üniversitesi Yayınları arasında çıkmasına izin veren Sakarya Üniversitesi'nin tüm yetkili kurullarına ve emeği geçen matbaa personeline teşekkür ederim.

FETHİ ÇALLIALP
Mart-1994-Adapazarı

İÇİNDEKİLER

BÖLÜM 1

TEMEL BİLGİLER

1.1 KÜMELER

Bu kesimde, aksiyomatik olarak kümeler teorisinin kuruluşu üzerinde değil, ilerdeki konularda gerekli olan temel kavramlar ve gösterimler üzerinde duracağız.

Küme bir takım nesneler topluluğudur. Kümenin içindeki nesnelere de o kümenin elemanları denir. A bir küme, a da bu kümenin bir elemanı ise $a \in A$ şeklinde yazılır ve "a, A kümesine aittir" diye okunur. Aksine a, A kümesine ait değil ise $a \notin A$ yazılır.

Kümeleri belirtmede iki yol izlenir. Birincisi, liste metodu ile, kümeyi bütün elemanları ile parantez içinde yazmaktır. Örneğin, mutlak değeri 3 den küçük tamsayılar kümesi, $\{-2,-1,0,1,2\}$ ile gösterilir. İkinci metot ise, kümeyi kümenin elemanlarını karakterize eden özellikle belirtmektir. Örneğin yukarıdaki küme, $\{x \in \mathcal{Z} : |x| \leq 3\}$ ile gösterilebilir. Burada $\mathcal{Z}$, tamsayılar kümesini göstermekte ve : dan sonra kümenin elemanlarının sağladığı özellik belirtilmektedir.

Tanım 1.1.1 Elemanları aynı olan iki kümeye **eşit kümeler** denir.

Tanım 1.1.2 Hiçbir elemanı olmayan kümeye **boş küme** denir ve $\emptyset$ ile gösterilir.

Tanım 1.1.3 A ve B iki küme olsunlar. B nin her elemanı, A nın da bir elemanı ise B ye, A nın bir **alt kümesi** denir ve $B \subset A$ ile

gösterilir.

Her kümenin kendisinin bir alt kümesi ve boş kümenin de her kümenin bir alt kümesi olduğu açıktır.

Tanım 1.1.4 Bir kümenin, kendisinden ve boş kümeden farklı her alt kümesine bir **öz alt kümesi** veya **has alt kümesi** denir.

Önerme 1.1.1 A ve B iki küme olsun.

$$A = B \iff A \subset B \text{ ve } B \subset A$$

olmasıdır.

İspat: $\Longrightarrow$: $A = B$ ise eşitlik tanımından, A nın her elemanı B de ve B nin her elemanı A da olacağından $A \subset B$ ve $B \subset A$ bulunur.

$\Longleftarrow$: $A \subset B$ ve $B \subset A$ olsun. Şu halde birinci kapsamadan, A nın her elemanı B de ve ikinci kapsamadan, B nin her elemanı da A da olduğu görülür. Sonuç olarak, A ve B kümeleri eşit bulunur.

Tanım 1.1.5 A ve B kümelerinin her ikisinde ortak olan elemanların oluşturduğu kümeye A ile B nin **arakesiti** veya **kesişimi** denir ve $A \cap B$ ile gösterilir.

Şu halde,

$$A \cap B = \{x : x \in A \text{ ve } x \in B\}$$

dir. Arakesit tanımından, $A \cap B \subset A$ ve $A \cap B \subset B$ olduğu hemen anlaşılır.

Örnek 1:. $A = \{x \in \mathcal{Z} : |x| < 3\}$ ve $B = \{x \in \mathcal{Z} : x > 0\}$ için $A \cap B = \{1, 2\}$ dır.

Tanım 1.1.6 Arakesitleri boş olan kümelere **ayrık kümeler** denir.

Tanım 1.1.7 A ve B kümelerinden en az birine ait olan elemanların oluşturduğu kümeye A ile B nin **birleşimi** denir ve $A \cup B$ ile gösterilir.

Şu halde,

$$A \cup B = \{x : x \in A \text{ veya } x \in B\}$$

dir.

Birleşim tanımından, $A \subset A \cup B$ ve $B \subset A \cup B$ olduğu hemen anlaşılır.

Örnek 2: $A = \{x \in \mathcal{Z} : |x| < 3\}$ ve $B = \{x \in \mathcal{Z} : x > 0\}$ için $A \cup B = \{-2, -1, 0, 1, 2, 3, ...\}$ dir.

Şimdi birleşim ve kesişimin bazı özelliklerini inceliyelim:

Önerme 1.1.2

(i) $A \subset B \Rightarrow A \cap B = A$,

(ii) $A \subset B \Rightarrow A \cup B = B$ dir.

İspat: (i) İki kümenin eşit olduğunu göstermek için Önerme 1.1.1 i kullanalım. $A \cap B \subset A$ olduğu açıktır. Ters kapsamayı göstermek için, $a \in A$ alalım. Arakesit tanımından $a \in A \cap B$ bulunur. Şu halde $A \subset A \cap B$ elde edilir.

(ii) aynı şekilde gösterilir. $B \subset A \cup B$ olduğu açıktır. Ters kapsamayı göstermek için, $a \in A \cup B$ alalım. Birleşim tanımına göre $a \in A$ veya $a \in B$ dir. $A \subset B$ kabul ettiğimiz için her iki halde de $a \in B$ olur. Şu halde $A \cup B \subset B$ dir. Her iki kapsamadan $B = A \cup B$ elde edilir.

Önerme 1.1.3

(i) $A \cup A = A$, $A \cap A = A$ (tek kuvvet özelliği)

(ii) $A \cup B = B \cup A$, $A \cap B = B \cap A$ (simetri özelliği)

(iii) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ (birleşme özelliği) sağlanır.

İspat: Yukarıdaki eşitlikleri birleşim için ispatlıyalım. Arakesitler için de benzer ispat yapılabilir.

(i) $A \subset A \cup A$ olduğu açıktır. $a \in A \cup A$ ise $a \in A$ olacağından $A \cup A \subset A$ da sağlanır. Şu halde her iki kapsamadan eşitlik bulunur.

(ii) $A \cup B$ ve $B \cup A$ kümelerinin her ikisi de A da veya B de olan elemanlardan oluştuğundan eşittirler.

(iii)

$$\begin{aligned} x \in A \cup (B \cup C) &\iff x \in A \text{ veya } (x \in B \cup C) \\ &\iff x \in A \text{ veya } (x \in B \text{ veya } x \in C) \\ &\iff (x \in A \text{ veya } x \in B) \text{ veya } x \in C \\ &\iff x \in (A \cup B) \cup C \end{aligned}$$

denkliklerinden, istenen eşitlik elde edilir.

Önerme 1.1.4
(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (birleşimin kesişim üzerine)
(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (kesişimin birleşim üzerine dağılma özellikleri) sağlanır.

İspat: (i)

$$\begin{aligned} x \in A \cup (B \cap C) &\iff x \in A \text{ veya } (x \in B \cap C) \\ &\iff x \in A \text{ veya } (x \in B \text{ ve } x \in C) \\ &\iff (x \in A \text{ veya } x \in B) \text{ ve } (x \in A \text{ veya } x \in C) \\ &\iff (x \in A \cup B) \text{ ve } (x \in A \cup C) \\ &\iff x \in (A \cup B) \cap (A \cup C) \end{aligned}$$

denkliklerinden istenen elde edilir.

(ii) Benzer şekilde ispatlanır.

I bir indis kümesi olmak üzere, $(A_i)_{i \in I}$ bir kümeler ailesi olsun. I sonlu veya sonsuz herhangi bir küme olabilir. Bu ailenin birleşim ve kesişimi de;

$$\bigcap_{i \in I} A_i = \{x \ : \ \forall i \in I, \ x \in A_i\}$$

$$\bigcup_{i \in I} A_i = \{x \ : \ \exists i \in I, \ x \in A_i\}$$

ile tanımlanır.

Örnek 3: $\mathcal{Z}$ tam sayılar kümesi olmak üzere $n \in \mathcal{Z}$ için $A_n = \{x \in \mathcal{Z} \ : \ x \geq n\}$ olsun.

$$\bigcap_{n \in \mathcal{Z}} A_n = \emptyset \text{ ve } \bigcup_{n \in \mathcal{Z}} A_n = \mathcal{Z}$$

dır.

Tanım 1.1.8 A ve B iki küme olsun. B ye ait, fakat A ya ait olmayan elemanların oluşturduğu kümeye B nin A ile **fark kümesi** denir ve $B \backslash A$ ile gösterilir:

$$B \backslash A = \{x \in B : x \notin A\}.$$

Eğer $A \subset B$ ise fark küme $B - A$ ile de gösterilebilir.

Tanım 1.1.9 A bir küme ve $\forall_i \in I$ için A_i kümeleri, A nın alt kümeleri olsunlar.
(i) $\forall i \in I$ için $A_i \neq \emptyset$,
(ii) $(A_i)_{i\in I}$ ailesi ikişer ikişer ayrık ve
(iii) $A = \bigcup_{i\in I} A_i$ ise $(A_i)_{i\in I}$ ailesine A nın bir **ayrışımı** denir.

Örnek 4: $A = \{1,2,3,4,5\}$ kümesinin bir ayrışımı olarak;
$A_1 = \{1\}$, $A_2 = \{2,3\}$, $A_3 = \{4,5\}$ olmak üzere, $\{A_1, A_2, A_3\}$ alınabilir.

Tanım 1.1.10 A ve B herhangi iki küme olsun. $a \in A$ ve $b \in B$ olmak üzere (a,b) sıralı ikililerinin oluşturduğu kümeye A ile B nin **dik çarpımı** veya **kartezyen çarpımı** denir ve $A \times B$ ile gösterilir:

$$A \times B = \{(a,b) \ : \ a \in A.\ b \in B\}.$$

Tanım 1.1.11 İkililerin eşitliği;

$$(a,b) = (a',b') \Longleftrightarrow a = a' \ \text{ve} \ b = b'$$

ile tanımlanır.

Örnek 5: $A = \{a,b,c\}$, $B = \{1,2\}$ ise

$$\begin{aligned} A \times B &= \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}, \\ B \times A &= \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\} \end{aligned}$$

dir. İkiden çok sayıda kümenin dik çarpımı da benzer şekilde tanımlanabilir.

Önerme 1.1.5 $A \times (B \cup C) = (A \times B) \cup (A \times C)$ dir.
İspat:

$$\begin{aligned} (a,b) \in A \times (B \cup C) &\Longleftrightarrow a \in A \ ve \ b \in B \cup C \\ &\Longleftrightarrow a \in A \ \ ve \ \ (b \in B \ \ veya \ \ b \in C) \\ &\Longleftrightarrow (a \in A \ ve \ b \in B) \ veya \ (a \in A \ ve \ b \in C) \\ &\Longleftrightarrow (a,b) \in A \times B \ \ veya \ \ (a,b) \in A \times C \\ &\Longleftrightarrow (a,b) \in (A \times B) \cup (A \times C) \end{aligned}$$

denkliklerinden, istenen eşitlik elde edilir.

1.1 ALIŞTIRMALAR

1-) A ve B bir S kümesinin alt kümeleri olsunlar. $S - A = A'$ kümesine A nın (S içindeki) **tümleyeni** denir. De Morgan kuralları olarak bilinen aşağıdaki özellikleri gösteriniz.

(i) $(A \cap B)' = A' \cup B'$,

(ii) $(A \cup B)' = A' \cap B'$.

2-) $B \subset A$ ise her C kümesi için,

(i) $B \cup C \subset A \cup C$ ve

(ii) $B \cap C \subset A \cap C$ olduğunu gösteriniz.

3-) (i) $A - (A \cap B) = A \backslash B$ ve

(ii) $A - (A \backslash B) = A \cap B$ olduğunu gösteriniz.

4-) $A \times (B \backslash C) = (A \times B) \backslash (A \times C)$ olduğunu gösteriniz.

5-) $\bigcup_{a \in \mathbb{R}} (a, \infty) = \mathbb{R}$ olduğunu gösteriniz.

6-) $A \triangle B = (A \backslash B) \cup (B \backslash A)$ kümesine A ile B nin **simetrik farkı** denir. $A \triangle B = (A \cup B) \backslash (A \cap B)$ olduğunu gösteriniz.

7-) $(A \cup B) \backslash C = (A \backslash C) \cup (B \backslash C)$ olduğunu gösteriniz.

8-) $A \backslash (A \backslash B) = A \cap B$ olduğunu gösteriniz.

9-) $A \cup B = A$ ise $B \subset A$ olduğunu gösteriniz. .

10-) n elemanlı bir kümenin 2^n alt kümesi olduğunu gösteriniz.

11-) $A \times (B \cap C) = (A \times B) \cap (A \times C)$ olduğunu gösteriniz.

12-) $A \times (B \cup C) = (A \times B) \cup (A \times C)$ olduğunu gösterin.

13-) $A \cup B = (A \triangle B) \cup (A \cap B)$ olduğunu gösreriniz.

14-) $(A \times B) \cup (B \times A) = C \times C$ ise $A = B = C$ olduğunu gösteriniz.

15-) $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$ olduğunu gösteriniz.

16-) $(A \times C) \cup (B \times D) \subset (A \cup B) \times (C \cup D)$ olduğunu gösteriniz. Eşitliğin sağlanmadığı bir örnek bulunuz.

1.2 BAĞINTILAR

Tanım 1.2.1 $A \times B$ nin boş olmayan her alt kümesine A dan B ye bir **bağıntı** denir. $A = B$ ise bağıntıya A da bir **bağıntı** denir.

R, A da bir bağıntı olsun. $(a, b) \in R$ ise a, b ye R ile **bağlıdır** denir ve aRb ile gösterilir.

Şimdi matematiğin birçok dalında önemli bir rol oynayan ve eşitliğin bir genellemesi olarak düşünebileceğimiz denklik bağıntısını tanımlayalım.

Tanım 1.2.2 R, A da bir bağıntı olsun.
i) $\forall a \in A$ için aRa, (yansıma özelliği)
ii) $aRb \Longrightarrow bRa$, (simetri özelliği)
(iii) aRb ve $bRc \Longrightarrow aRc$ (geçişme özelliği)
ise R ye A da bir **denklik bağıntısı** denir.

Örnek 1: Her doğruyu kendisine paralel kabul edersek, doğrular arasındaki paralellik bağıntısı bir denklik bağıntısıdır.

Örnek 2: A düzlemdeki noktalar kümesi olsun. Orjinden aynı uzaklıktaki noktaları denk noktalar diye tanımlarsak bu bir denklik bağıntısıdır.

Örnek 3: $\mathcal{Z}$ tam sayılar kümesi üzerinde, farkları $n > o$ tam sayısı ile bölünebilen tam sayıları denk olarak tanımlarsak bu bir denklik bağıntısıdır. Gerçekten;

i) $\forall a \in \mathcal{Z}$ için $a - a = o$ ve n ile bölünebildiğinden, $a \sim a$ yani bağıntı yansıyandır.

ii) $a, b \in \mathcal{Z}$ denk olsunlar. $a \sim b \Longleftrightarrow n \mid a - b$ (n, a-b yi böler). n, $b - a = -(a - b)$ yi de böleceğinden $b \sim a$, yani bağıntı simetriktir.

iii) $a, b, c \in \mathcal{Z}$ için $a \sim b$ ve $a \sim c$ olsun. Şu halde $n|a - b$ ve $n|b - c$ olacağından, $n|(a - b) + (b - c) = a - c$ yani $a \sim c$ geçişme özelliği sağlanır.

Tanım 1.2.3 R, A da bir denklik bağıntısı olsun. Bir $a \in A$ nın **denklik sınıfı** $\bar{a} = \{b \in A : bRa\}$ ile tanımlanır. Bütün denklik sınıfları kümesi A/R ile gösterilir ve **Bölüm kümesi** olarak adlandırılır.

A daki R denklik bağıntısına göre, yansıma özelliği göz önünde tutularak, $\forall a \in A$ için aRa, yani $a \in \bar{a}$ olduğu ve $\bar{a} \neq \emptyset$ olduğu görülür.

Örnek 4: Örnek 1 deki denklik bağıntısına göre, bu doğrunun denklik sınıfı, bu doğruya göre paralel olan tüm doğrulardan oluşur.

Örnek 5: Örnek 2 deki denklik bağıntısına göre, düzlemdeki bir noktanın denklik sınıfı, merkezi orjin ve bu noktadan geçen çember üzerindeki tüm noktalardır.

Örnek 6: Örnek 3 deki denklik bağıntısına göre, bir $a \in \mathcal{Z}$ nın denklik sınıfı $\bar{a}$, n ye bölündüğünde a ile aynı kalanı bırakan tüm sayılardan oluşur. (Neden ?) Şu halde, farklı n tane denklik sınıfı bulunur. Bu denklik sınıflarının oluşturduğu küme $\mathcal{Z}_n$ ile gösterilir ve **modn kalan sınıfları** veya **denklik sınıfları** kümesi denir.

Önerme 1.2.1 R, A da bir denklik bağıntısı ise R nin belirttiği denklik sınıfları A nın bir ayrışımını belirtir. Tersine, A nın bir ayrışımı verilirse ayrışım kümelerini denklik sınıfları kabul eden A da bir denklik bağıntısı tanımlanabilir.

İspat: R, A da bir denklik bağıntısı olsun.
(i) Denklik sınıflarının boş küme olmıyacağını yukarıda söylemiştik.

(ii) Farklı denklik sınıfları ikişer ikişer ayrıktırlar. Gerçekten, $\bar{a} \cap \bar{b} \neq \emptyset$ olsa, $\exists c \in A$ için $c \in \bar{a}$ ve $c \in \bar{b}$ olur. R nin simetri ve geçişme özellikleri kullanılarak, $(a, c) \in R$ ve $(c, b) \in R$ olacağından $(a, b) \in R$ ile birlikte düşünerek, $(a, b) \in R$ bulunur. Şu halde $\bar{a} \subset \bar{b}$ dir. $\bar{a}$ ile $\bar{b}$ nin rolleri simetrik olduğundan, $\bar{b} \subset \bar{a}$ de gösterilebilir. Sonuç olarak, iki sınıf ayrık değilse aynı sınıf oldukları görülür.

(iii) $\forall a \in A$ için $a \in \bar{a}$ olduğundan, $A = \cup \bar{a}$, yani bütün denklik sınıfları kümesinin birleşiminin A yı verdiği görülür.

Tersine, $(A_i)_{i \in I}$ ailesi A nın bir ayrışımı olsun. A da bir R bağıntısını şöyle tanımlayalım:

$$a, b \in A \text{ için } aRb \iff \exists i \in I \text{ için, } a, b \in A_i$$

Böyle tanımlanan R nin bir denklik bağıntısı olduğunu gösterelim:

(i) Yansıma: $\forall a \in A$ için aRa olduğu açıktır.

(ii) Simetri: $aRb \Longrightarrow \exists i \in I$ için $a, b \in A_i$ olduğundan, a ve b aynı ayrışım kümesinde, yani bRa bulunur.

(iii) Geçişme: aRb ve bRc olsun. Şu halde Rnin tanımına göre a ile b ve b ile c aynı ayrışım sınıfında, yani a, b, c elemanlarının üçü de aynı ayrışım kümesinde olurlar. Buradan aRc bulunur.

Ayrıca bir $a \in A$ ile denk olan elemanların, yani $\overline{a}$ denklik sınıfının a nın içine düştüğü ayrışım sınıfı olduğu da hemen görülür.

Tanım 1.2.4 R, A da bir bağıntı olsun.
i) $\forall a \in A$ için, aRa (yansıma)
ii) aRb ve $bRa \Longrightarrow a = b$ (ters simetri)
iii) aRb ve $bRc \Longrightarrow aRc$ (geçişme) özellikleri varsa R ye A da bir **sıralama bağıntısı** denir.

Örnek 7: $\mathcal{Z}$ tamsayılar kümesinde,

$$a, b \in \mathcal{Z} \text{ için } aRb \Longleftrightarrow a \leq b$$

ile tanımlı R bağıntısı bir sıralama bağıntısıdır.

Örnek 8: A bir küme ve A nın bütün alt kümelerinden oluşan aile, $P(A)$ (kuvvet kümesi) olsun.

$$A_1, A_2 \in P(A) \text{ için, } A_1 \leq A_2 \Longleftrightarrow A_1 \subset A_2$$

ile tanımlansın. $\leq$, $P(A)$ da bir sıralama bağıntısıdır.

R, A da bir sıralama bağıntısı ise $\forall a, b \in A$ için aRb veya bRa olması, yani her iki elemanın karşılaştırılması mümkün olmayabilir.

Tanım 1.2.5 Bir sıralama bağıntısı için herhangi iki eleman karşılaştırılabiliyorsa bu sıralama bağıntısına bir **tam sıralama** denir.

R, A da bir tam sıralama bağıntısı ise ters simetri özelliğinden, $\forall a, b \in A$ ve $a \neq b$ için; aRb veya bRa dan biri ve yalnız biri doğrudur.

Örnek 9: $A = \{2, 3, ..., 9, 10\}$ kümesinde, R bağıntısı

$$aRb \Longleftrightarrow a|b$$

ile tanımlansın. R bağıntısı bir sıralama bağıntısıdır.

Bu bağıntının bir tam sıralama olmadığı gözükmektedir. Örneğin 6 ve 8 karşılaştırılamaz. A nın $\{2,4,8\}$ alt kümesi ise tam sıralıdır.

Tanım 1.2.6 Sıralı bir kümenin, tam sıralı bir alt kümesine bir **zincir** denir.

Tanım 1.2.7 $\leq$, A da bir sıralama bağıntısı olsun.

i) $a_0 \in A$ olsun. A da a_0 dan büyük hiçbir eleman yoksa, yani

$$a_0 \leq x \Longrightarrow x = a_0$$

ise a_0 elemanına A nın bir **büyük elemanı** veya bir **maksimal elemanı** denir.

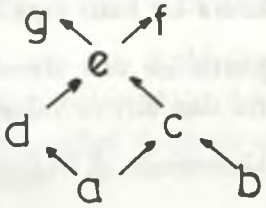
ii) $\forall a \in A$ için $a \leq c$ olacak şekilde $\exists c \in A$ varsa c ye A nın **son elemanı** veya **en büyük elemanı** denir.

iii) $X \subset A$ ve $a \in A$ olsun. $\forall x \in X$ için, $a \leq x$ ise a ya X alt kümesinin bir **alt sınırı** ve tüm alt sınırlar kümesinin en büyük elemanına da X alt kümesinin **infumumu** veya **en büyük alt sınırı** denir ve inf X=a yazılır.

Benzer şekilde küçük eleman, minimal eleman, üst sınır ve en küçük üst sınır (supremum) da tanımlanabilir.

Tanım 1.2.8 $X \subset A$ alt kümesinin bir alt ve bir üst sınırı varsa X alt kümesine **sınırlı** bir alt küme denir.

Örnek 10 $A = \{a,\ b,\ c,\ d,\ e, f,\ g\}$ ve $B = \{c,\ d,\ e\}$ ise şekildeki sıralamaya göre;



i) A nın minimal elemanları a, b;

ii) A nın maksimal elemanları g ve f;

iii) B nin tek alt sınırı a ve üst sınırları da g, e, f dirler.

iv) sup B=e, inf B=a dır.

Örnek 11: $A = \{x \in \mathbb{R} : 0 < x < 1\}$ olduğuna göre, A nın en küçük ve en büyük elemanı yoktur. Fakat, A sınırlı bir kümedir ve $supA = 1$ ve $infA = 0$ dır.

Teorem 1.2.1 (Zorn Lemma) X boş olmayan ve her tam sıralı alt kümesi bir üst sınıra sahip olan sıralı bir küme ise X in bir maksimal elemanı vardır.

1.2 ALIŞTIRMALAR

1-) R bağıntısı reel sayılar kümesi üzerinde,

$$xRy \iff \exists n \in \mathcal{Z}, x, y \in [n, n+1]$$

ile tanımlanıyor. R nin grafiğini çiziniz.

2-) R bağıntısı reel sayılar kümesi üzerinde,

$$xRy \iff 0 \leq x - y \leq 1$$

ile tanımlanıyor. R^{-1} bağıntısını bulunuz.

3-) İyi sıralı bir kümenin, her alt kümesinin de iyi sıralı olduğunu gösteriniz.

4-) İyi sıralı bir kümenin tam sıralı olacağını gösteriniz. Tersi doğru mudur, bir örnekle açıklayınız.

5-) $A = \{\frac{1}{n} : n \in \mathbb{N}\}$ kümesinin sınırlı olup olmadığını araştırınız. Sup A ve inf A yı bulunuz.

6-) 3 elemanlı bir küme üzerindeki bütün sıralama bağıntılarını bulunuz.

7-) R, X kümesi üzerinde bir bağıntı olsun.

$$R^{-1} = \{(x, y) : (y, x) \in R\}$$

de X üzerinde bir bağıntıdır. R^{-1} bağıntısına R nin **ters bağıntısı** denir. R denklik bağıntısı ise R^{-1} in de bir denklik bağıntısı olduğunu gösteriniz.

8-) R bağıntısı $\mathbb{N} \times \mathbb{N}$ kümesi üzerinde,

$$(x,y)R(x',y') \Longleftrightarrow xy' = yx'$$

ile tanımlanıyor. R nin bir denklik bağıntısı olduğunu gösteriniz.

9-) R bağıntısı reel sayılar kümesi üzerinde,

$$xRy \Longleftrightarrow x - y \in \mathcal{Z}$$

ile tanımlanıyor.R nin bir denklik bağıntısı olduğunu gösteriniz.

1.3 FONKSİYONLAR

Fonksiyon (dönüşüm veya tasvir) özel bir bağıntıdır.

Tanım 1.3.1 f, A dan B ye bir bağıntı olsun. $\forall a \in A$ için, a ya f ile bağlı B de bir ve yalnız bir eleman bulunabilirse, f ye A dan B içine bir **fonksiyon veya (dönüşüm)** denir ve $f : A \longrightarrow B$ ile gösterilir. A ya f nin **tanım kümesi**, B ye de **değer kümesi** denir. a ya f fonksiyonu ile karşılık gelen ve tek türlü olarak belirli olan b elemanı $f(a) = b$ ile gösterilir ve b ye f altında a nın **görüntüsü** (veya a ya f altında b nin **orjinali**) denir.

$f : A \longrightarrow B$ bir fonksiyon ise $A \times B$ nin

$$\{(a, f(a)) : a \in A\}$$

alt kümesine f nin **grafiği** denir.

Örnek 1: $I_A : A \longrightarrow A, \forall a \in A$ için $I_A(a) = a$ ile tanımlı fonksiyona, A nın **özdeşlik** veya **birim fonksiyonu** denir.

Örnek 2: $f : \mathcal{Z} \longrightarrow \mathcal{Z}, \forall m \in \mathcal{Z}$ için $f(m) = m^2$ ile tanımlı fonksiyonun, görüntü kümesi $\{m^2 : m \in \mathcal{Z}\}$, kare tam sayılar kümesidir.

Tanım 1.3.2 f ve g, A dan B içine iki fonksiyon ve $\forall a \in A$ için $f(a) = g(a)$ ise f ve g ye eşit fonksiyonlar denir ve $f = g$ ile gösterilir.

Tanım 1.3.3 $f : A \longrightarrow B$ bir fonksiyon ve $f(A) = \{f(a) : a \in A\}$ görüntüler kümesi B ye eşit ise f ye **örten bir fonksiyon** denir.

Şu halde f örten ise $\forall b \in B$ için $f(a) = b$ olacak şekilde $\exists a \in A$ bulunabilir, yani B deki her eleman A daki en az bir elemanın görüntüsüdür.

Örnek 3: Birim fonksiyon örtendir.

Örnek 4: Örnek 2 deki fonksiyon örten değildir. Örneğin $3 \in \mathcal{Z}$, bir tam sayının karesi olmadığından, görüntü değildir.

Tanım 1.3.4 $f : A \longrightarrow B$ bir fonksiyon olsun. $\forall a, b \in A$ için

$$f(a) = f(b) \Longrightarrow a = b$$

ise f ye **bire-bir fonksiyon** denir ve 1-1 yazılır.

Yukarıdaki tanımı şöyle ifade etmek de mümkündür:

$$\forall a, b \in A \text{ ve a} \neq \text{b} \Longrightarrow \text{f(a)} \neq \text{f(b)}.$$

Örnek 5: Birim fonksiyon 1-1 dir. Fakat Örnek 2 deki fonksiyon 1-1 değildir. Çünkü 1 ve -1 elemanlarının görüntüsü aynı olup +1 dir.

Tanım 1.3.5 $f : A \longrightarrow B$ bir fonksiyon ve $X \subset A$ olsun. $\forall x \in X$ için $g(x) = f(x)$ ile tanımlı, $g : X \longrightarrow B$ fonksiyonuna f nin X alt kümesine **kısıtlanışı (daraltılmışı)** denir ve $f|_X$ ile gösterilir. f, 1-1 ise her alt kümesine kısıtlanışının da 1-1 olacağı açıktır.

Örnek 6: $g : \mathbb{R} \longrightarrow \mathbb{R}, g(x) = [|x|]$ ile tanımlı fonksiyonun (0, 1) açık aralığına kısıtlanışı, 0 değerini alan sabit bir fonksiyondur.

Tanım 1.3.6 $f : A \longrightarrow B, g : B \longrightarrow C$ iki fonksiyon olsun. $\forall a \in A$ için $h(a) = g(f(a))$ ile tanımlı, $h : A \longrightarrow C$ fonksiyonuna f ile g nin **bileşke fonksiyonu denir ve $h = gof$ ile gösterilir.**

Örnek 7: $g : \mathbb{R} \longrightarrow \mathcal{Z}, g(x) = [|x|]$ **ve** $f : \mathcal{Z} \longrightarrow \mathcal{Z}, f(x) = x^2$ **ile tanımlı olduğuna göre** fog **fonksiyonunu bulalım.** $fog : \mathbb{R} \longrightarrow \mathcal{Z}$ **fonksiyonu,** $\forall x \in \mathbb{R}$ **için;**

$$(fog)(x) = f(g(x)) = f([|x|]) = [|x|]^2$$

ile tanımlıdır.

Önerme 1.3.1 $f : A \longrightarrow B, g : B \longrightarrow C, h : C \longrightarrow D$ üç fonksiyon ise $ho(gof) = (hog)of$ dir. (Bileşkenin birleşme özelliği)

İspat: $\forall a \in A$ için, bileşke tanımı kullanılarak;

$$[ho(gof)](a) = h(gof)(a) = h(g(f(a)))$$

ve

$$[(hog)of](a) = (hog)(f(a)) = h(g(f(a)))$$

bulunur. Fonksiyonların eşitlik tanımından istenen elde edilir.

Tanım 1.3.7 $f : A \longrightarrow B$ bir fonksiyon ve $Y \subset B$ ise A nın

$$f^{-1}(Y) = \{a \in A : f(a) \in Y\}$$

alt kümesine Y nin f altındaki **ters görüntüsü** denir.

Özel olarak, $Y = \{b\}$ ise $f^{-1}(b) = \{a \in A : f(a) = b\}$ dir. f örten ise $\forall b \in B$ için $f^{-1}(b) \neq \emptyset$ ve f, 1-1 ise $f^{-1}(b)$ de tek elemanlı bir küme olur.

Tanım 1.3.8 $f : A \longrightarrow B$ 1-1 ve örten bir fonksiyon ise $\forall b \in B$ elemanına $f(a) = b$ olacak şekilde (tek türlü belirli olan) bir $a \in A$ elemanı karşılık getirerek, B den A ya tanımlanan fonksiyona f nin **ters fonksiyonu** denir ve $f^{-1} : B \longrightarrow A$ ile gösterilir.

Şu halde f 1-1 ve örten ise $f(a) = b \Longleftrightarrow f^{-1}(b) = a$ dır. Bileşke tanımı göz önüne alınarak;

$$f^{-1}of = I_A \text{ ve } fof^{-1} = I_B$$

olduğu görülür.

Önerme 1.3.2 $f : A \longrightarrow B$ ve $g : B \longrightarrow C$ fonksiyonları verilsin.

(i) f ve g örten ise gof de örten,
(ii) f ve g 1-1 ise gof de 1-1 dir.

İspat: (i) $gof : A \longrightarrow C$ bileşke fonksiyonunun örten olduğunu göstermek için, C deki her elemanın gof bileşkesi altında A daki bir elemanın görüntüsü olduğunu göstermek gerekir.

$c \in C$ olsun. g örten olduğundan, $g(b) = c$ olacak şekilde $\exists b \in B$ vardır. f de örten olduğundan $f(a) = b$ olacak şekilde $\exists a \in A$ vardır. Şu halde $c = g(b) = g(f(a)) = (gof)(a)$ elde edilir.

(ii) $a_1, a_2, \in A$ için $(gof)(a_1) = (gof)(a_2)$ olsun. Bileşke tanımından ve g ile f nin 1-1 oluşlarından

$$g(f(a_1)) = g(f(a_2)) \Longrightarrow f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$$

elde edilir. Şu halde gof de 1-1 dir.

Önerme 1.3.3 A kümesinin kendi üzerine 1-1 ve örten bütün fonksiyonlar kümesi $S(A)$ olsun.

i) f ve $g \in S(A)$ ise $gof \in S(A)$ ve
ii) $f, g, h \in S(A)$ ise $fo(goh) = (fog)oh$ dir.
iii) I_A birim fonksiyon olmak üzere, $\forall f \in S(A)$ için $I_A of = foI_A = f$ dir.
iv) $\forall f \in S(A)$ için $fof^{-1} = f^{-1}of = I_A$ olacak şekilde bir $f^{-1} \in S(A)$ bulunabilir.

İspat: (i) Önerme 1.3.2 den görülür.

(ii) Önerme 1.3.1 den görülür.

(iii) $\forall a \in A$ için, $(I_A of)(a) = I_A(f(a)) = f(a)$ ve

$(foI_A)(a) = f(I_A(a)) = f(a)$ eşitliklerinden istenen görülür.

(iv) $f \in S(A)$ olduğundan, f 1-1 ve örten olur. Şu halde f nin ters fonksiyonu f^{-1} mevcut ve

$$fof^{-1} = f^{-1}of = I_A$$

eşitlikleri sağlanır.

Not: Eğer A, n elemanlı bir küme ise $S(A) = S_n$ ile gösterilir.

Örnek 8: $A = \{1, 2, 3\}$ olsun. $f(1) = 2, f(2) = 3, f(3) = 1$ ve $g(1) = 1, g(2) = 3, g(3) = 2$ ile $f, g \in S_3$ tanımlayalım.

$(gof)(1) = g(f(1)) = g(2) = 3$
$(gof)(2) = g(f(2)) = g(3) = 2$

$(gof)(3) = g(f(3)) = g(1) = 1$

$(fog)(1) = f(g(1)) = f(1) = 2$
$(fog)(2) = f(g(2)) = f(3) = 1$
$(fog)(3) = f(g(3)) = f(2) = 3$

olduğundan, $fog \neq gof$ olduğu görülmektedir.

1.3 ALIŞTIRMALAR

1-) $\mathbb{N}$ den $\mathbb{N}$ ye öyle f ve g fonksiyonları bulunuz ki $gof = I_{\mathbb{N}}$, fakat $fog \neq I_{\mathbb{N}}$ olsun.

2-) $f : A \longrightarrow B$ bir örten fonksiyon ise $\{f^{-1}(b)\}_{b \in B}$ ailesinin, A nın bir ayrışımı olduğunu gösteriniz.

3-) İki küme arasında 1-1 ve örten bir fonksiyon varsa bu iki kümeye **denk** veya **aynı kuvvette** kümeler denir. Kümeler arasında denk olmanın bir denklik bağıntısı olduğunu gösteriniz.

4-) Bir öz alt kümesi ile denk olan kümeye **sonsuz küme** denir. $\mathbb{Z}$ ve $\mathbb{R}$ nin birer sonsuz küme olduğunu gösteriniz.

5-) $\mathbb{N}$ ile denk olan kümelere **sayılabilir sonsuz kümeler** denir. $\mathbb{Q}$ rasyonel sayılar kümesinin, sayılabilir sonsuz bir küme olduğunu gösteriniz.

6-) $\mathbb{R}$ reel sayılar kümesinin, sayılabilir sonsuz bir küme olmadığını gösteriniz.

7-) $f : A \longrightarrow B$ bir fonksiyon ve $P, S \subset B$ olsun.
a) $f^{-1}(P \cup S) = f^{-1}(P) \cup f^{-1}(S)$ ve
b) $f^{-1}(P \cap S) = f^{-1}(P) \cap f^{-1}(S)$ olduğunu gösteriniz.

8-) $f : A \longrightarrow B$ bir fonksiyon ve $X \subset A$ olsun. $f^{-1}(f(X)) \subset X$ olduğunu gösteriniz. Her X alt kümesi için eşitliğin olması için gerek ve yeter koşul f nin 1-1 olmasıdır, gösteriniz.

9-) $f : A \longrightarrow B$ bir fonksiyon ve $P \subset B$ olsun. $f(f^{-1}(P)) \subset P$ olduğunu gösteriniz. Her P alt kümesi için eşitliğin sağlanması için gerek ve yeter koşul f nin örten olmasıdır, gösteriniz.

10-) f ve g örten ve 1-1 iseler $(gof)^{-1} = f^{-1}og^{-1}$ olduğunu gösteriniz.

11-) n elemanlı bir kümenin kendisi üzerine 1-1 fonksiyonlarının (permutasyon) sayısı kaçtır?

12-) n elemanlı bir kümenin, $(m > n)$ m elemanlı bir küme içine 1-1 fonksiyonlarının sayısı kaç tanedir.

13-) n elemanlı bir kümenin, n elemanlı bir küme içine bütün fonksiyonları kaç tanedir?

14-) Negatif olmayan reel sayılar kümesi $\mathbb{R}_+$ üzerinde, $f(x) = x^2$ ile tanımlı $f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$ fonksiyonunun 1-1, örten olup olmadığını araştırınız.

15-) A bir küme ve $P(A)$ nın kuvvet kümesi olsun.
$f(a) = A - \{a\}$ ile tanımlı, $f : A \longrightarrow P(A)$ fonksiyonunun 1-1 örten olup olmadığını araştırınız.

16-) A sonlu bir küme ve $f : A \longrightarrow A$ bir fonksiyon olsun.
a) f örten ise 1-1,
b) f 1-1 ise örten olduğunu gösteriniz.

17-) A sonsuz bir küme ise önceki problemin yanlış olacağını gösteriniz.

18-) $f : A \longrightarrow B$ bir fonksiyon olsun. $a, b \in A$ için
$a \sim b \iff f(a) = f(b)$ ile tanımlı $\sim$ bağıntısının, A da bir denklik bağıntısı olduğunu gösteriniz ve denklik sınıflarını bulunuz.

19-) R, A da bir denklik bağıntısı ve denklik sınıfları kümesi (Bölüm Kümesi) A/R ise, $\pi : A \longrightarrow A/R, \pi(a) = \bar{a}$ ile tanımlı fonksiyonun örten ve $\pi^{-1}(\{\bar{a}\}) = \bar{a}$ olduğunu gösteriniz.

20-) $f : A \longrightarrow B$ fonksiyonunun 1-1 olabilmesi için gerek ve yeter koşul, $gof = I_A$ olacak şekilde $\exists g : B \longrightarrow A$ fonksiyonunun bulunabilmesidir, gösteriniz.

21-) $f : A \longrightarrow B$ fonksiyonunun örten olması için gerek ve yeter koşul, $fog = I_B$ olacak şekilde $\exists g : A \longrightarrow A$ fonksiyonunun bulunabilmesidir, gösteriniz.

22-) A ve B boş olmayan kümeler ise $A \times B$ ve $B \times A$ nın denk (ikisi arasında 1-1 örten bir fonksiyon var) olduğunu gösteriniz.

23-) $f : A \longrightarrow B$ olan bir fonksiyon ve $X, Y \subset A$ olsun.
a) $f(X \cup Y) = f(x) \cup f(Y)$ ve
b) $f(X \cap Y) \subset f(X) \cap f(Y)$ olduğunu gösteriniz.
c) Önceki kapsamında her X ve Y alt kümesi için gerek ve yeter koşul f nin 1-1 olmasıdır, gösteriniz.

1.4 İKİLİ İŞLEMLER

Tanım 1.4.1 $A \times A$ dan A ya bir fonksiyona A da bir **ikili işlem** denir.
$*, A$ da bir ikili işlem ve $a, b \in A$ olsun. (a, b) nin $*$ işlemi altındaki görüntüsünü $a * b$ ile gösterelim. Fonksiyon olma özelliklerinden
i) $\forall a, b \in A$ için A da bir $a * b$ elemanı var ve
ii) bu eleman tek türlü belirlidir.
Bu özelliklerden birincisine işlemin **kapalılığı**, ikincisine de **iyi tanımlılığı** denir.

Tanım 1.4.2 Üzerinde en az bir ikili işlem tanımlı boş olmayan bir kümeye bir **cebirsel yapı** denir. A kümesi üzerinde bir $*$ ikili işlemi tanımlı ise bu cebirsel yapı $(A, *)$ ile gösterilir.

Örnek 1: $\mathbb{N}$ doğal sayılar kümesi üzerinde $(a, b) \longrightarrow a + b$ ve $(a, b) \longrightarrow ab$ ile tanımlı $+$ ve $\cdot$ fonksiyonları birer ikili işlemdirler.

Tanım 1.4.3 $*, A$ da bir ikili işlem olsun.
i) $\forall a, b \in A$ için $a * b = b * a$ ise $*$ işlemi **değişmelidir.**
ii) $\forall a, b, c \in A$ için $a * (b * c) = (a * b) * c$ ise $*$ işlemi **birleşmelidir.**

Örnek 2: $\mathbb{N}$ de tanımlı $+$ ve $\cdot$ işlemleri değişme ve birleşme özelliklerine sahiptir.

Tanım 1.4.4 A da $*$ ve o ikili işlem olsun. $\forall a, b, c \in A$ için;
i) $a * (boc) = (a * b)o(a * c)$ ise $*$ işleminin o işlemi üzerine **soldan dağılma** özelliği vardır.

ii) $((aob)*c) = (a*c)o(b*c)$ ise $*$ işleminin o işlemi üzerine **sağdan dağılma** özelliği vardır.

Not: $*$ işleminin değişme özelliği varsa dağılmanın soldan veya sağdan oluşu fark etmez.

Tanım 1.4.5 $*$, A da bir ikili işlem olsun. $\forall a \in A$ için $a*e = e*a = a$ olacak şekilde bir $e \in A$ varsa e ye $*$ işlemi için **etkisiz (birim) eleman** denir.

Tanım 1.4.6 $*$, A da bir ikili işlem ve $e \in A$ birim elemanı olsun. Bir $a \in A$ elemanı için, $a * a' = a' * a = e$ eşitliğini sağlayan bir $a' \in A$ varsa a' ye a nın **tersi** denir ve $a' = a^{-1}$ veya $a' = -a$ ile gösterilir.

Örnek 3: Doğal sayılarda çarpma işleminin etkisiz elemanı 1 ve 1 in tersi 1 olup, diğer doğal sayıların çarpma işlemine göre tersleri yoktur.

Önerme 1.4.1 $*$, A da bir ikili işlem olsun. A da $*$ işleminin etkisiz elemanı varsa tektir.

İspat: Kabul edelim ki e ve e' iki etkisiz eleman olsun.e bir etkisiz eleman olduğundan, $\forall a \in A$ için $a * e = e * a = a$ ve özel olarak $a = e'$ alınırsa, $e' * e = e * e' = e'$ bulunur. Aynı şekilde e' bir etkisiz eleman olduğundan, $\forall a \in A$ için $a * e' = e' * a = a$ ve özel olarak $a = e$ alınırsa, $e * e' = e' * e = e$ bulunur. Elde edilen eşitlikler karşılaştırılırsa $e = e'$ olduğu görülür.

Önerme 1.4.2 $*$, A da birleşmeli bir ikili işlem ve etkisiz eleman e olsun. Bu takdirde $a \in A$ nın tersi varsa tektir.

İspat: Kabul edelim ki a nın tersi iki tane, a_1 ve a_2 olsun. Şu halde

$$a * a_1 = a_1 * a = e \quad \text{ve} \quad a * a_2 = a_2 * a = e$$

eşitlikleri sağlanır. İkinci eşitlikleri soldan a_1 ile işleme sokarsak,birinci yan

$$a_1 * (a * a_2) = (a_1 * a) * a_2 = e * a_2 = a_2$$

ve ikinci yan da,

$$a_1 * e = a_1$$

bulunur. Şu halde $a_1 = a_2$ dir.

1.4 ALIŞTIRMALAR

1-) $*$ işleminin A da birleşme özelliği varsa $a_1, a_2, a_3 \in A$ için;

$$a_1 * a_2 * a_3 = (a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$$

olarak tanımlanır. $\forall m, n \in \mathbb{N}$ için;

$$a_1 * a_2 * \ldots * a_{m+n} = (a_1 * \ldots * a_m) * (a_{m+1} * \ldots * a_n)$$

olduğunu gösteriniz. (Genel birleşme özelliği)

2-) 5 elemanlı bir küme üzerinde, farklı
a) kaç işlem,
b) kaç değişmeli işlem tanımlanabilir?

3-) $\mathbb{Z}$ de $a * b = a + b - ab$ ile tanımlı $*$ işleminin özelliklerini araştırınız. Adi çarpma işleminin, $*$ işlemi üzerine dağılma özelliği olup olmadığını araştırınız.

4-) Pozitif reel sayılar kümesi üzerinde tanımlanan, $x * y = x^y$ işleminin özelliklerini araştırınız.

5-) A kümesinin, kendi içine mümkün tüm fonksiyonları kümesi $F(A)$ üzerinde tanımlı bileşke işleminin özelliklerini araştırınız.

6-) $\mathbb{Z}$ tam sayılar kümesinde $a * b = max\{a, b\}$ ile tanımlı işlemin özelliklerini inceleyiniz.

7-) $*$ işlemine göre $a \in A$ nın tersi a^{-1} ise a^{-1} in de tersinin varlığını gösteriniz.

8-) 4 elemanlı bir küme üzerinde, kaç tane farklı işlem tanımlanabilir?

9-) 4 elemanlı bir küme üzerinde, kaç tane değişme özelliğine sahip, farklı işlem tanımlanabilir?

10-) $\mathbb{Z}$ de, $a * b = a + b + ab$ ile tanımlı $*$ işleminin varsa birim elemanını bulunuz. Tersi bulunamayan tam sayıları bulunuz.

BÖLÜM 2

TAM VE RASYONEL SAYILAR

2.1 TAM SAYILAR

Bu bölümde liseden de iyi bilinen tam sayılar kümesinin temel özelliklerini sıralıyarak bir incelemesini yapacağız.

Doğal sayılar veya pozitif tam sayılar kümesini $\mathbb{N} = \{1, 2, 3, \ldots\}$ ile, tam sayılar kümesini $\mathcal{Z}$ ile gösterelim.

$\mathcal{Z}$ de iki ikili işlem; toplama ve çarpma liseden alışık olduğumuz gibi tanımlanabilir. Ayrıca, çıkarma işlemini de $x, y \in \mathcal{Z}$ için;

$$x - y = x + (-y)$$

toplama işlemi yardımı ile tanımlamak mümkündür. Fakat bu işlemi, toplamadan farklı bir işlem olarak düşünmeyebiliriz.

Toplama ve çarpmanın şu özellikleri vardır.

Z1: Birleşme Kuralı; $(x + y) + z = x + (y + z), \quad (xy)z = x(yz)$

Z2: Değişme Kuralı; $x + y = y + x, \quad xy = yx$

Z3: Etkisiz Eleman; $x + 0 = x, \quad x1 = x$

Z4: Toplamsal Ters Eleman; $x + (-x) = 0$

Her tam sayının toplamsal tersi veya ters işaretlisi vardır. Fakat çarpımsal tersi olmayabilir. Çarpımsal terslerinin olması için rasyonel sayılar inşa edilir.

Z5: Dağılma Kuralı; $x(y+z) = xy + xz$

Yukarıdaki özelliklerle $(\mathcal{Z}, +, .)$ nın bir değişmeli, birimli bir halka olduğunu 4.Bölümde göreceğiz.

Birleşme özelliği nedeni ile, parantezlerin yeri önemli olmadığından n tane tam sayının toplamı ve çarpımı da tanımlanabilir ve bunlar kısaca $\sum_{i=1}^{n} a_i$ ve $\prod_{i=1}^{n} a_i$ ile de gösterilir.

Ayrıca dağılma özelliği genelleştirilerek;

$$(a_1 + \ldots + a_m)(b_1 + \ldots + b_n) = a_1b_1 + a_1b_2 + \ldots a_rb_s$$

yazılabilir.

Z6: $\forall a, b \in \mathcal{Z}, \quad ab \neq 0 \Longrightarrow a \neq 0, b \neq 0$ dır.

Bu özellik, tam sayılar kümesinde **sıfır bölen** yoktur, şeklinde ifade edilir. Bunun sonucu olarak, kısaltma özelliği sağlanır:

$$a, b, c \in \mathcal{Z}, c \neq 0 \quad \text{ve} \quad ac = bc \Longrightarrow a = b$$

$\mathcal{Z}$ üzerindeki toplama ve çarpma işlemlerine ek olarak, bir de sıralama bağıntısı vardır. $x, y \in \mathcal{Z}$ için, $y = x + a$ olacak şekilde bir a pozitif tam sayısı varsa $y > x$ ile gösterilir. $y = x$ veya $y > x$ ise $y \geq x$ de yazılabilir. $\geq, \mathcal{Z}$ de bir tam sıralamadır ve aşağıdaki özellikleri de sağlar.

Z7: $x_1 \leq x_2$ ve $y_1 \leq y_2 \Longrightarrow x_1 + y_1 \leq x_2 + y_2$ dir.

Z8: $x \leq y$ ve $z > 0$ ise $xz \leq yz$ dir.

$x + (-x) = 0$ olduğundan $Z7$ özelliği kullanılarak, $x < 0$ ise $0 < -x$ bulunur. Ayrıca, $x = 0, \quad x > 0, \quad x < 0$ dan bir ve yalnız biri doğru olduğundan, $x = 0, \quad x > 0, \quad -x > 0$ dan da bir ve yalnız biri doğudur.

Aşağıdaki özellik, ispatlarda sık sık kullanacağımız tümevarımla ispat metodunun temelini teşkil eder.

1. Tümevarım Prensibi: $S \subset \mathbb{N}$ ve $1 \in S$ olsun. $n \in S \Longrightarrow n + 1 \in S$ gerektirmesi doğru ise $S = \mathbb{N}$ dir.

Pozitif tam sayılar hakkında bir $P(n)$ önermesi göz önüne alalım.

i) $n = 1$ için $P(1)$ önermesi doğru ise,

ii) Önermenin n için doğruluğu, $n + 1$ için de doğruluğunu gerektiriyorsa $\forall n \in \mathbb{N}$ için $P(n)$ önermesi doğrudur.

Gerçekten, önermeyi doğru kılan pozitif tam sayılar kümesini S ile gösterirsek, $1 \in S$ ve $n \in S \Longrightarrow n+1 \in S$ gerektirmesi nedeni ile Tümevarım Prensibine göre $S = \mathbb{N}$, yani önerme her pozitif tam sayı için doğru olur.

Teorem 2.1.1 Aşağıdaki ifadeler bir birine denktirler.

i) Tümevarım Prensibi,

ii) $S \subset \mathbb{N}, 1 \in S$ olsun. $\forall m < n, m \in S$ için $n \in S$ ise $S = \mathbb{N}$ dir. (2.Tümevarım Prensibi)

iii) Pozitif tam sayılar kümesinin boş olmayan her alt kümesinin en küçük elemanı vardır. (İyi sıralılık)

İspat: (i) $\Longrightarrow$ (ii): $S \subset \mathbb{N}$, $1 \in S$ ve $\forall m < n, m \in S$ için $n \in S$ olsun.

$$T = \{x \in \mathbb{N} \ : \ \forall y \leq x;\ y \in S\}$$

diyelim. $T \subset S$ ve $1 \in S$ olduğundan, $1 \in T$ olduğu açıktır.

$$n \in T \Longrightarrow \forall y \leq n \ ; \ y \in S \Longrightarrow n+1 \in T$$

olacağından Tümevarım Prensibine göre $T = \mathbb{N}$ bulunur.

(ii) $\Longrightarrow$(iii): $\emptyset \neq S \subset \mathbb{N}$ ve S nin en küçük elemanı bulunmasın. S nin $\mathbb{N}$ deki tamlayanı S^c nin, $\mathbb{N}$ ye eşit olduğunu gösterelim. S nin en küçük elemanı olmadığından $1 \notin S$ ve $1 \in S^c$ dir. $\forall m < n$ için $m \in S^c$ ise $n \in S^c$ olur. Çünkü aksi halde n, S nin en küçük elemanı olurdu. Şu halde (ii) ye göre, $S^c = \mathbb{N}$ yani $S = \emptyset$ bulunur.

(iii) $\Longrightarrow$(i): $1 \in S \subset \mathbb{N}$ ve $n \in S \Longrightarrow n+1 \in S$ olsun. S nin $\mathbb{N}$ deki tamlayanı S^c nin en küçük elemanı yoktur. Çünkü, $n \in S^c$ ise $n-1 \in S^c$ ve $1 \notin S^c$ dir. Şu halde (iii) ye göre, $S^c = \emptyset$ yani $S = \mathbb{N}$ bulunur.

$\mathbb{Z}$ tam sayılar kümesi üzerinde, mutlak değer de tanımlanabilir. Yani, $\mathbb{Z}$ değerlendirilmiş bir halkadır.

Tanım 2.1.1 Bir a tam sayısının **mutlak değeri** $|a|$ ile gösterilir ve

$$|a| = \begin{cases} a \ ; \ a \geq 0 \ \text{ise} \\ -a \ ; \ a < 0 \ \text{ise} \end{cases}$$

ile tanımlanır.

Mutlak değerin şu özellikleri vardır:

M1: $\forall a \in \mathcal{Z}$ için, $|a| \geq 0$,

M2: $|a| = 0 \Longleftrightarrow a = 0$,

M3: $\forall a, b \in \mathcal{Z}$ için, $|ab| \leq |a| + |b|$, (**üçgen eşitsizliği**) sağlanır.

2.1 ALIŞTIRMALAR

1-) Tümevarımla,

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

olduğunu gösteriniz.

2-) Tümevarımla, $0 \leq k \leq n$ için,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

olmak üzere;

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

olduğunu gösteriniz.

3-) $\forall a \in \mathcal{Z}$ için, $-|a| \leq a \leq |a|$ olduğunu gösteriniz.

4-) $\forall a, b \in \mathcal{Z}$ için, $||a| - |b|| \leq |a| + |b|$ olduğunu gösteriniz.

5-) $\mathcal{Z}$ de $|x - 2| \geq 3$ eşitsizliğini çözünüz.

6-) $\mathcal{Z}$ de $1 < |x - 1| \leq 3$ eşitsizliğini çözünüz.

2.2 TAM SAYILARDA ARİTMETİK

Tanım 2.2.1 $a, b \in \mathcal{Z}$ için, $b = ac$ olacak şekilde $\exists c \in \mathcal{Z}$ bulunabilirse a; b **yi böler** denir ve $a|b$ ile gösterilir.

0 ın her katı 0 oluğundan, $0|0$ olduğu ve $0|a$ ise $a = 0$ olacağını görmek kolaydır.

$\mathcal{Z}$ de bölünebilmenin şu özellikleri sağlanır;

B1: $c|b$ ve $b|a \Longrightarrow c|a$,

B2: $\forall a \in \mathcal{Z}$ için $a|a$,

B3: $a|b$ ve $b|a \Longrightarrow a = \mp b$,

B4: $c|a$ ve $c|b \Longrightarrow \forall x, y \in \mathcal{Z};\ b|xa + yb$.

İlk 3 özellikten, pozitif tam sayılar kümesi üzerinde bölünebilmenin bir sıralama bağıntısı olduğu görülür. Bu sıralama bağıntısı tam sıralama değildir.

Tanım 2.2.2 $a, b \in \mathcal{Z}$ için, $b|a$ ise a ile b ye **ilgili tam sayılar** denir.

B3 özelliğinden, sıfırdan farklı her tam sayı tam bir pozitif tam sayı ile ilgilidir. İlgililik bağıntısının bir denklik bağıntısı olduğu kolayca görülebilir. Sıfır tam sayısının denklik sınıfından ibaret tek elemanlı küme, sıfırdan farklı bir tam sayının denklik sınıfı da, kendisi ile ters işaretlisinden oluşan iki elemanlı bir kümedir.

Bölünebilme söz konusu olduğunda, pozitif tam sayıları düşünmek yeterlidir. Çünkü;

$$a|b \Longrightarrow \mp a| \mp b$$

dır.

Tanım 2.2.3 Pozitif bölenleri, yalnız 1 ve kendisi olan 1 den büyük tam sayılara **asal tam sayılar** denir.

En küçük asal sayının 2 olduğu besbellidir.

Önerme 2.2.1 Her $a > 1$ tam sayısının en az bir asal böleni vardır.

İspat: $S = \{d \in \mathcal{Z} : d > 1 \text{ ve } d|a\}$ diyelim. $a|a$ olduğundan $a \in S$, dolayısı ile $S \neq \emptyset$ olur. Pozitif tam sayılar kümesinin iyi sıralı olmasından, S nin en küçük elemanı mevcuttur, buna p diyelim. p nin asal olduğunu gösterirsek önerme ispatlanmış olur.

p asal olmasaydı, $p = qr$ ve $1 < q < p$ olacak şekilde $\exists q, r \in \mathcal{Z}$ bulunabilirdi.

$$q|p \text{ ve } p|a \Longrightarrow q|a$$

olacağından, $q \in S$ olur ve p nin en küçük eleman oluşu ile çelişki elde edilirdi. Şuhalde p asaldır.

Şimdi sonsuz asal sayının varlığını gösterelim:

Önerme 2.2.2 Sonsuz asal sayı vardır.

İspat: İspatı olmayana ergi metodu ile yapalım. Kabul edelim ki asal sayılar kümesi sonlu ve $P = \{p_1, p_2, \ldots, p_n\}$ olsun.

$a = p_1 p_2 \ldots p_n + 1$ tam sayısı 1 den büyük olduğundan, en az bir p asal böleni vardır. Bütün asal sayılar kümesini P ile gösterdiğimizden, $p \in P$ olur. Şu halde $p|p_1 p_2 \ldots p_n$ ve $p|a - p_1 p_2 \ldots p_n = 1$ yani, $p = \mp 1$ bulunur. Bu ise p nin asal oluşu ile çelişir.

Teorem 2.2.1 Her $a > 1$ tam sayısı, bir takım (sonlu sayıda) asal sayıların çarpımı olarak yazılabilir.

İspat: İspatı olmayana ergi metodu ile yapalım. Asal çarpanlara ayrılamıyan bir tam sayı $a > 1$ olsun. Bunların arasında en küçük olanı da c ile gösterelim. $c > 1$ ve c asal olmayacağından, Önerme 2.2.1 e göre $1 < c_1, c_2 < c$ olmak üzere $c = c_1 c_2$ olur. Fakat c yi asal çarpanlara ayrılamayan en küçük pozitif tam sayı olarak aldığımızdan, c_1 ile c_2 asal çarpamlara ayrılabilir, dolayısı ile c de asal çarpanlara ayrılmış olur. Böylece çelişki elde edilir.

Daha sonra, bir tam sayının asal çarpanlara ayrılışının sıra düşünmeksizin tek türlü olduğunu ifade eden Aritmetiğin Temel Teoremini ispatlayacağız. Önce $\mathcal{Z}$ de **kalanlı bölme** veya **bölme algoritması** olarak bilinen şu teoremi ispatlayalım:

Teorem 2.2.2 Pozitif m ve n tam sayıları verildiğinde, tek türlü olarak belirli öyle bir q, r tam sayıları vardır ki $n = qm + r$ ve $0 \leq r < m$ olur.

İspat: İspatı 2. tümevarım prensibini uygulayarak yapalım.$n = 1$ olsun. Eğer $m = 1$ ise $q = 1$, $r = 0$ ve $m > 1$ ise $q = 0$, $r = 1$ alınarak $n = 1$ için iddianın doğruluğu görülür.

$n < m$ ise $q = 0$, $r = n$ alınabilir. $m \leq n$ ise $0 \leq n - m < n$ olur ve $n - m = q_1 m + r$ ve $0 \leq r < m$ olacak şekilde $\exists q_1, r \in \mathcal{Z}$ varsa, $n = m + q_1 m + r = (1 + q_1)m + r$ olacağından, n için de iddianın doğruluğu gösterilmiş olur.

Şimdi q ve r nin tekliğini görelim. Kabul edelim ki;

$$n = q_1 m + r_1, \quad 0 \leq r_1 < m$$
$$n = q_2 m + r_2, \quad 0 \leq r_2 < m$$

ve $r_1 \neq r_2$ olsun. Genelliği bozmadan, $r_2 > r_1$ kabul edebiliriz. $q_1 m + r_1 = q_2 m + r_2 \Longrightarrow (q_1 - q_2)m = r_2 - r_1$ bulunur. $0 < r_2 - r_1 < m$ olduğundan, $0 < (q_1 - q_2)m < m$ dir. Fakat,

$$1 \leq (q_1 - q_2) \Longrightarrow m \leq (q_1 - q_2)m$$

olacağından, $r_1 \neq r_2$ olmasının bizi bir çelişkiye götürdüğü anlaşılır. Şu halde $r_1 = r_2$ ve dolayısı ile $q_1 = q_2$ olmalıdır.

Pozitif tam sayılar için ispatlanan yukarıdaki teoremi daha genel olarak ifade etmek mümkündür:

Teorem 2.2.3 $m \neq 0$ ve $m, n \in \mathcal{Z}$ olsun. Tek türlü olarak belirli öyle $q, r \in \mathcal{Z}$ bulunur ki $n = qm + r$ ve $0 \leq r < |m|$ olur.

Tanım 2.2.4 $n = qm + r$, $0 \leq r < |m|$ ise q ye **bölüm**, r ye de kalan denir. Verilen m ve n tam sayıları için q ve r yi bulmaya da n yi m ile **kalanlı bölme** denir.

Tanım 2.2.5 m ve n sıfırdan farklı bir tam sayı olsunlar.

i) $d|m$ ve $d|n$ olacak şekilde $d > 0$ tam sayısı varsa d ye m ile n nin bir **ortak böleni** denir.

ii) d, m ile n nin ortak böleni olsun. Eğer m ile n nin her e ortak böleni için $e|d$ ise d ye m ile n nin **en büyük ortak böleni** (e.b.o.b) denir ve (m,n)=d ile gösterilir.

a ile b nin iki en büyük ortak böleni c_1 ve c_2 ise $c_1|c_2$ ve $c_2|c_1$, dolayısı ile $c_1 = c_2$ olacağı anlaşılır. Şu halde iki tam sayı verildiğinde en büyük ortak bölenleri tektir.

Teorem 2.2.3 Sıfırdan farklı herhangi iki sayının en büyük ortak böleni vardır ve $d = (m, n)$ ise $d = xm + yn$ olacak şekilde $\exists x, y \in \mathcal{Z}$ bulunabilir.

İspat: $S = \{xm + yn \ : \ xm + yn > 0, x, y \in \mathcal{Z}\}$ diyelim. $x = m$ ve $y = n$ için $m^2 + n^2 > 0$ olduğundan $m^2 + n^2 \in S$ ve $S \neq \emptyset$ olur. Pozitif tam sayıların iyi sıralı olma özelliğinden, S nin bir d gibi en küçük elemanı vardır. Şimdi $d = (m, n)$ olduğunu gösterelim.

m yi d ile kalanlı olarak bölelim. $m = qd + r$ ve $0 \leq r < d$ olacak şekilde $\exists q, r \in \mathcal{Z}$ bulunabilir. $d = xm + yn$ şeklinde olduğundan,

$$m = q(xm + yn) + r \Longrightarrow r = m(1 - qx) + n(-qy)$$

dir. Bu durumda $r \neq 0$ ise $r \in S$ olur ki, $r < d$ olduğu için $d \in S$ nin en küçük oluşu ile çelişir. Şu halde $r = 0$, yani $d|m$ olmalıdır.

m ve n simetrik rol oynadıkları için, benzer şekilde $d|n$ olduğu da gösterilebilir. Böylece d nin m ile n in bir ortak böleni olduğu anlaşılır.

$e \in Z$, $e|m$ ve $e|n$ olsun. $m = eu$ ve $n = ev$ olacak şekilde, $\exists u, v \in \mathcal{Z}$ bulunabilir.

$$d = xm + yn = x(eu) + y(ev) = e(xu + yv),$$

olduğundan $e|d$ dir. Sonuç olarak $d = (m, n)$ ve $d \in S$ olduğundan $\exists x, y \in \mathcal{Z}$ için $d = xm + yn$ olur.

Not: Yukarıdaki teoremin ispatından anlaşıldığı gibi, sıfırdan farklı m ve n tam sayılarının en büyük ortak bölenleri, $x, y \in \mathcal{Z}$ olmak üzere $xm + yn$ şeklindeki en küçük pozitif tam sayıdır.

Tanım 2.2.6 İki tam sayının en büyük ortak bölenleri 1 ise bu iki sayıya **aralarında asal sayılar** denir.

Önerme 2.2.3 p asal ve $0 \neq a \in \mathcal{Z}$ olsun.

$$(a,p) = 1 \iff p \not| a$$

olmasıdır.

İspat: p asal ise pozitif bölenleri, 1 ve p dir. Şu halde $(a,p) = 1$ ise $p \not| a$ dır.

Tersine, $p \not| a$ ise p ile a nın ortak bölenleri ancak 1 olabilir, yani $(a,p) = 1$ dir.

Yukarıdaki özellikten, farklı iki asal sayı aralarında asaldırlar.

Not: $d = xm + yn$ olacak şekilde $\exists x, y \in \mathcal{Z}$ bulunabilirse $d = (m,n)$ olmayabilir. Fakat, yukarıdaki nota göre, $xm + yn$ şeklindeki toplamların en küçüğünün d olması halinde $d = (m,n)$ dir. Özel olarak, $\exists x, y \in \mathcal{Z}$ için, $1 = xm + yn$ ise $(m,n) = 1$ olur.

Şimdi iki tam sayının en küçük ortak bölenlerini bulmak için bir metot verelim. Genelliği bozmadan pozitif tam sayıların en büyük ortak bölenini bulabiliriz. m ve n pozitif tam sayılar olsun. Ard arda aşağıdaki kalanlı bölmeleri yapalım:

$$\begin{array}{lll}
n = q_1 m + r_1 \text{ ve} & 0 \leq r_1 < m & (1) \\
m = q_2 r_1 + r_2 \text{ ve} & 0 \leq r_2 < r_1 & (2) \\
r_1 = q_3 r_2 + r_3 \text{ ve} & 0 \leq r_3 < r_2 & (3) \\
\ldots \quad \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots \\
r_{k-1} = q_{k+1} r_k + r_{k+1} \text{ ve} & 0 \leq r_{k+1} < r_k & (k+1) \\
r_k = q_{k+2} r_{k+1} + 0 & \ldots\ldots\ldots & (k+2)
\end{array}$$

şeklinde kalan 0 oluncaya kadar devam edelim. Kalanların gittikçe küçüldüğüne, $m > r_1 > r_2 > \ldots$ olduğuna dikkat edersek, sonlu bir adım sonra 0 kalanını bulacağımız aşikardır.

Teorem 2.2.4 (Euclid Algoritması) Yukarıda ardarda yapılan kalanlı bölmeler arasında sıfırdan farklı en son kalan m ile n nin en büyük ortak bölenidir, yani $r_{k+1} = (m,n)$ dir.

İspat: Önce r_k nın m ile n nin bir ortak böleni olduğunu gösterelim. Kalanlı bölmelerdeki son eşitlikten, $r_{k+1} | r_k$ ve sondan bir önceki eşitlikten,

$$r_{k+1} | q_{k+1} r_k + r_{k+1} = r_{k-1}$$

ve bu şekilde devam ederek;

$$r_{k+1} | r_k,\ r_{k-1} \ldots,\ r_1,\ m,\ n$$

elde edilir.

Şimdi $e \in \mathcal{Z}$, $e|m$ ve $e|n$ ise $e|r_{k+1}$ olacağını gösterelim.

$$\begin{aligned} e|n \text{ ve } e|m &\Longrightarrow e|n - q_1 m = r_1, \\ e|m \text{ ve } e|r_1 &\Longrightarrow e|m - q_2 r_1 = r_2, \\ e|r_1 \text{ ve } e|r_2 &\Longrightarrow e|r_1 - q_3 r_2 = r_3 \end{aligned}$$

ve böyle devam ederek, $e|r_{k+1}$ bulunur.

Örnek 1: 357 ile 122 nin en büyük ortak bölenini bulalım.

$$\begin{aligned} 357 &= 2.122 + 113 \\ 122 &= 1.113 + 9 \\ 113 &= 12.9 + 5 \\ 9 &= 1.5 + 4 \\ 5 &= 1.4 + 1 \\ 4 &= 4.1 \end{aligned}$$

olduğundan yukarıdaki teoreme göre (375,122)=1 dir.

Yukarıdaki metotla en büyük ortak bölen bulunduktan sonra, $d = (m, n)$ ise $d = xm + yn$ olacak şekilde $x, y \in \mathcal{Z}$ tam sayıları da bulunabilir. Gerçekten, Euclid Algoritmasındaki (1). bölmeden, $r_1 = n - q_1 m$ ve (2). bölmeden; $r_2 = m - q_2 r_1 = m - q_2(n - q_1 m) = -q_2 n + (1 - q_2 q_1)m$ bulunur. Böyle devam edilirse, sıfırdan farklı son kalan yani $r_{k+1} = (m, n) = xm + yn$ şeklinde yazılmış olur. Aynı şey, r_{k+1} in değeri, bir önceki eşitlikte yerine koya koya birinci eşitliğe kadar devam edilerek de elde edilebilir.

Örnek 2: (357, 122) =1= x. 357 +y. 122 olacak şekilde $\exists x, y \in \mathcal{Z}$ bulalım. Örnek 1 deki eşitlikler göz önüne alınırsa,

$$\begin{aligned} 1 &= 5 - 4 = 5 - (9 - 5) = 2.5 - 9 \\ &= 2.(113 - 12.9) - 9 = 2.113 - 25.9 \\ &= 2.113 - 25(122 - 113) = 27.113 - 25.122 \\ &= 27.(357 - 2.122) - 25.122 = 27.357 - 79.122 \end{aligned}$$

bulunur. $x = 27$, $y = 79$ alınabilir. Başka x ve y tam sayıları bulunabilir mi?

Teorem 2.2.5 m ve n sıfırdan farklı ve c herhangi bir tam sayı olsun.

$$(m,n) = 1 \text{ ve } m|nc \Longrightarrow m|c$$

dir.

İspat: $(m,n) = 1$ olduğundan, $\exists x, y \in \mathcal{Z}$ için $1 = xm + yn$ olur. Son eşitliğin her iki yanını c ile çarparak, $c = x(mc) + y(nc)$ bulunur.

$$m|mc \text{ ve } m|nc \Longrightarrow m|x(mc) + y(nc) = c$$

elde edilir.

Sonuç 1: p asal ve $p|mn \Longrightarrow p|m$ veya $p|n$ dir.

İspat: p asal olduğundan, $p|m$ veya $(p,m) = 1$ dir. (Önerme 2.2.3) Teoreme göre $p|mn$ ve $(p,m) = 1$ ise $p|n$ elde edilir.

Sonuç 2: p asal ve $a_1, a_2, \ldots a_n \in \mathcal{Z}$ olsun.

$$p|a_1a_2 \ldots a_n \Longrightarrow \exists i = 1,2,\ldots,n, \quad p|a_i$$

dir.

İspat: n üzerine tümevarımla, sonuç 1 den elde edilir.

$\mathcal{Z}$ de asal çarpanlara ayrılışın varlığını Teorem 2.2.1 de görmüştük.

Aritmetiğin Temel Teoremi 2.2.6 Her $a > 1$ tam sayısının asal çarpanlara ayrılışı, sıra düşünmeksizin tek türlüdür.

İspat: $a > 1$ tam sayısı $a = p_1p_2 \ldots p_m = q_1q_2 \ldots q_n$ şeklinde iki türlü asal çarpanlara ayrılmış olsun. $m = n$, ve p_i ile q_j asallarının da aynı olduğunu gösterelim.

$$p_1p_2 \ldots p_m = q_1q_2 \ldots q_n \Longrightarrow p_1|q_1q_2 \ldots q_n$$

olduğundan, Sonuç 2 ye göre $\exists j = 1,2,\ldots,n$ için, $p_1 = q_j$ olur. Sıra düşünülmediğinden, $p_1 = q_1$ alabiliriz. Yukarıdaki eşitlikte, her iki

yandan p_1 ile kısaltma yaparak,

$$p_2p_3\dots p_m = q_2q_3\dots q_n \Longrightarrow p_2|q_2q_3\dots q_n$$

bulunur. Benzer düşünce ile $p_2 = q_2$ alınabilir. Bu şekilde devam ederek her p_i nin q_j lerden birine eşit olacağı anlaşılır. p ve q lerin rolü simetrik olduğundan, her q de p_i lerden birisidir. Böylece iddia ispatlanmış olur.

Bölünebilme özellikleri göz önünde tutularak, pozitif tam sayıların tek türlü asal çarpanlara ayrılışı, sıfırdan farklı tüm tam sayılar için de ifade edilebilir.

Teorem 2.2.7 Sıfırdan farklı her $a \in \mathcal{Z}$, $a = (\mp 1)p_1p_2\dots p_n$ şeklinde, farklı olmaları gerekmeyen bir takım asal sayıların (n=0 olabilir) çarpımı olarak yazılabilir ve bu yazılış sıra düşünmeksizin tek türlüdür.

Aynı asal sayıların çarpımını üslü şekilde yazarak;

$$a = (\mp 1)p_1^{m_1}p_2^{m_2}\dots p_t^{m_t}, \quad (p_i \text{ ler asal}, \quad m_i > 0)$$

şeklinde yazılabilir.

Örnek 3: $300 = 2^2.3.5^2$, $500 = 2^2.5^3, 81 = 3^4$.

En büyük ortak bölene benzer şekilde en küçük ortak kat da tanımlanabilir.

Tanım 2.2.7 m ve n sıfırdan farklı iki tamsayı olsun.

i) $m|k$ ve $n|k$ olacak şekilde bir $k > 0$ tam sayısı varsa k ya m ile n nin bir **ortak katı** denir.

ii) k, m ile $n$nin bir ortak katı olsun. Eğer m ile n nin her ortak katı için $k|t$ ise k ya m ile n nin **en küçük ortak katı** denir ve $k = [m, n]$ ile gösterilir.

En büyük ortak bölen ve en küçük ortak kat, asal çarpanlara ayrılış yardımı ile de bulunabilir. Bunun için verilen iki sayı, $p^0 = 1$ yazarak, aynı asalların çarpımı olarak yazılır.

$$a = p_1^{m_1}p_2^{m_2}\dots p_r^{m_r} \quad \text{ve} \quad b = p_1^{n_1}p_2^{n_2}\dots p_r^{n_r}$$

$(p_i \text{ ler asal}, \quad m_i, n_i \geq 0)$ olsun.

$$c = p_1^{c_1}p_2^{c_2}\dots p_r^{c_r}|a = p_1^{m_1}p_2^{m_2}\dots p_r^{m_r} \Longleftrightarrow c_i \leq m_i, i = 1, 2, \dots, r$$

olduğu göz önüne alınarak;

$$(a,b) = p_1^{max(m_1,n_1)} p_2^{max(m_2,n_2)} \dots p_r^{max(m_r,n_r)}$$
$$[a,b] = p_1^{min(m_1,n_1)} p_2^{min(m_2,n_2)} \dots p_r^{min(m_r,n_r)}$$

elde edilir.

Önerme 2.2.4 a ve b pozitif tam sayılar olsun.

$$(a,b)[a,b] = ab$$

dir.

İspat: Asal çarpanlara ayrılış kullanılarak;

$$(a,b)[a,b] = p_1^{max(m_1,n_1)+min(m_2,n_2)} \dots p_r^{max(m_r,n_r)+min(m_r,n_r)}$$

ve $max(m_i,n_i) + min(m_i,n_i) = m_i + n_i$ olduğu göz önüne alınarak,

$$(a,b)[a,b] = p_1^{m_1+n_1} \dots p_r^{m_r+n_r} = (p_1^{m_1} \dots p_r^{m_r})(p_1^{n_1} \dots p_r^{n_r}) = ab$$

elde edilir.

Tanım 2.2.8 Pozitif n tam sayısı için $1 \leq a \leq n$ ve $(a,n) = 1$ olan a tam sayılarının sayısı $\phi(n)$ ile gösterilir ve **Euler Fonksiyonu** denir.

Euler Fonksiyonunun şu özellikleri vardır:

E1: p asal ise $\phi(p) = p - 1 = p(1 - \frac{1}{p})$ dir.

E2: p asal ve $a \in \mathbb{N}$ ise $\phi(p^a) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$ dir.

E3: $(m,n) = 1$ ise $\phi(mn) = \phi(m)\phi(n)$ dir.

E4: $m = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ ise;

$$\begin{aligned}\phi(m) &= \phi(p_1^{a_1})\phi(p_2^{a_1}) \dots \phi(p_r^{a_r}) \\ &= p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \dots (1 - \tfrac{1}{p_r})\end{aligned}$$

dir.

Örnek 4: $\phi(2^4) = 2^4(1 - \frac{1}{2}) = 2^3 = 8,$

$\phi(2^4.3^2) = \phi(2^4)\phi(3^2) = 2^3.3.2 = 48.$

2.2 ALIŞTIRMALAR

1-) $\forall m, n \in \mathcal{Z}, m \neq 0$ için $n = qm + r$ ve $|r| \leq \frac{|m|}{2}$ olacak şekilde $\exists q, r \in \mathcal{Z}$ bulunabileceğini gösteriniz. Bu yazılışın tek türlü olup olmadığını araştırınız.

2-) $(a, mn) = 1 \iff (a, m) = (a, n) = 1$ olduğunu gösteriniz.

3-) $\forall i = 1, 2, \ldots, n$ için $(a, b_i) = 1$ ise $(a, b_1, b_2, \ldots, b_n) = 1$ olduğunu gösteriniz.

4-) $(a, b) = 1$ ise $\forall n \in \mathbb{N}$ için $(a^n, b^n) = 1$ olduğunu gösteriniz.

5-) $a, b \in \mathcal{Z}$ için $xa + yb = 1$ olacak şekilde $\exists x, y \in \mathcal{Z}$ bulunabilir ise $(a, b) = 1$ olduğunu gösteriniz.

6-) $(m, n) = 1, m|a$ ve $n|a \Longrightarrow mn|a$ olduğunu gösteriniz.

7-) $(m, n) = 1$ ise $(m + n, m - n) = 1$ veya 2 olduğunu gösteriniz.

8-) $(m, n) = 1$ ise $(m + n, mn) = 1$ olduğunu gösteriniz.

9-) $(3425, 273) = d$ yi bulunuz ve $d = 3425x + 273y$ olacak şekilde $\exists x, y \in \mathcal{Z}$ bulunuz.

10-) $(m, n) = 1$ ise $\phi(mn) = \phi(m)\phi(n)$ olduğunu gösteriniz.

11-) n çift ise $\phi(2n) = 2\phi(n)$ olduğunu gösteriniz.

12-) n tek ise $\phi(2n) = \phi(n)$ olduğunu gösteriniz.

13-) p asal ve $p|a^n \Longrightarrow p^n|a^n$ olduğunu gösteriniz.

14-) 100! ün sonunda kaç sıfır vardır?

15-) $2^m - 1$ asal ise m nin asal olacağını gösteriniz.

16-) $2^m + 1$ bir asal sayı ise m nin 2 nin bir kuvveti olacağını gösteriniz. (Fermat asal sayısı)

2.3 MODÜLER ARİTMETİK

Bu kesimde, cebirsel yapıları daha iyi kavrayabilmek için, tam sayıların bazı aritmetik özellikleri üzerinde duracağız.

Tanım 2.3.1 m sıfırdan farklı bir tamsayı olsun. $a, b \in \mathcal{Z}$ için;

$$a \equiv b(mod\ m) \implies m|a-b$$

ile tanımlanır ve a ile b mod m denktirler denir.

$m|a-b \implies -m|a-b$ olduğundan, $m > 0$ kabul edilebilir.

Önerme 2.3.1 Yukarıda tanımlanan $\equiv$ bağıntısı $\mathcal{Z}$ de bir denklik bağintısıdır.

İspat: i) Yansıma: $\forall a \in \mathcal{Z}$ için; $m|0 = a - a$ olduğundan, $a \equiv a(mod\ m)$ dir.

ii) Simetri: $a, b \in \mathcal{Z}$ için; $a \equiv b(mod\ m)$ olsun. Şu halde, $m|a-b$ ve $m|b-a = -(a-b)$ olduğundan, $b \equiv a(mod\ m)$ dir.

iii) Geçişme: $a, b, c \in \mathcal{Z}$ için, $a \equiv b(mod\ m)$ ve $b \equiv c(mod\ m)$ olsun.

$$m|a-b \text{ ve } m|b-c \implies m|a-b \text{ ve } m|b-c \implies m|a-c = (a-b)+(b-c)$$

olduğundan, $a \equiv c(mod\ m)$ dir.

Tanım 2.3.2 $\mathcal{Z}$ deki $\equiv$ denklik bağıntısının belirttiği denklik sınıflarına, m modülüne göre (mod m) kalan sınıfları denir ve tüm kalan sınıfları kümesi $\mathcal{Z}_m$ ile gösterilir.

$a \in \mathcal{Z}$ nın denklik sınıfı, $\bar{a} = \{x \in \mathcal{Z} : m|a-x\}$ dir.

Önerme 2.3.2 $a \equiv b(mod\ m) \iff$ a ve b nin m ile bölümünden elde edilen kalanın aynı olmasıdır.

İspat: $\implies$: $a \equiv b(mod\ m)$ olsun. a ve b yi m ile kalanlı olarak bölelim. $a = qm + r$, $b = q'm + r'$ ve $0 \leq r,\ r' < m$ olacak şekilde

$\exists q, r, q', r', \in \mathcal{Z}$ bulalım.

$$\begin{aligned} a \equiv b(mod\ m) &\Longrightarrow m|a-b \Longrightarrow a = b + km, \exists k \in \mathcal{Z} \\ &\Longrightarrow a = b + km = qm + r,\ 0 \leq r < m \\ &\Longrightarrow b = (q-k)m + r,\ 0 \leq r < m \end{aligned}$$

olduğundan, kalanlı bölmenin tekliğinden $q' = q - k$ ve $r = r'$ elde edilir.

$\Longleftarrow$: a ve b nin, m ile bölümünden elde edilen kalanlar aynı olsunlar. Yani, $a = qm + r$, $b = q'm + r'$ ve $0 \leq r, r' < m$ olsun. Bu takdirde,

$$a - b = (q - q')m \Longrightarrow m|a-b \Longrightarrow a \equiv b(mod\ m)$$

elde edilir.

Not: Bir $a \in \mathcal{Z}$ nin $m > 0$ ile bölümünden elde edilen kalanlar; $0, 1, \ldots, m-1$ olacağından,$\bar{a}$ sınıfı; $\bar{0}, \bar{1}, \ldots, \overline{m-1}$ sınıflarından biridir. Şu halde $\mathcal{Z}_m$, m elemanlı bir kümedir.

Örnek 1: $\mathcal{Z}_6 = \{\bar{0}, \bar{1}, \ldots, \bar{5}\}$ dir. Örneğin, $14 \equiv 2(mod\ 6)$ ve $23 \equiv 5(mod\ 6)$ olduğundan, $14 \in \bar{2}$ ve $23 \in \bar{5}$ dir.

Önerme 2.3.3 $a \equiv a_1(mod\ m)$ ve $b \equiv b_1(mod\ m)$ ise $a + b \equiv a_1 + b_1(mod\ m)$ dir.

İspat:

$$\begin{aligned} a \equiv a_1(mod\ m),\ b \equiv b_1(mod\ m) &\Longrightarrow m|a-a_1,\ m|b-b_1 \\ &\Longrightarrow m|(a+b)-(a_1+b_1) \\ &\Longrightarrow a+b \equiv a_1+b_1(mod\ m) \end{aligned}$$

elde edilir.

Tanım 2.3.3 $\bar{a}$, $\bar{b} \in \mathcal{Z}_m$ için, $\bar{a} \oplus \bar{b} = \overline{a+b}$ ile tanımlanır.

Yukarıdaki önermeden, $\bar{a}$ ve $\bar{b}$ sınıflarının toplamının sınıflardan alınan temsilcilere bağlı olmadığı, yani $\oplus$ nın iyi tanımlı olduğu anlaşılır.

Önerme 2.3.4 $a \equiv a_1(mod\ m)$ ve $b \equiv b_1(mod\ m)$ ise $ab \equiv a_1 b_1(mod\ m)$ dir.

İspat:

$$a \equiv a_1 (mod\ m)\ ve\quad b \equiv b_1 (mod\ m) \Longrightarrow m|a - a_1 \text{ ve } m|b - b_1$$
$$\Longrightarrow m|a_1(b - b_1) + b(a - a_1) = a\,b - a_1\,b_1$$
$$\Longrightarrow ab \equiv a_1 b_1 (mod\ m)$$

elde edilir.

Tanım 2.3.4 $\bar{a}$, $\bar{b} \in \mathcal{Z}_m$ için, $\bar{a} \odot \bar{b} = \overline{a + b}$ ile tanımlanır.

Yukarıdaki önermeden, $\bar{a}$ ve $\bar{b}$ sınıflarının çarpımının sınıflardan alınan temsilcilere bağlı olmadığı, yani $\odot$ nın iyi tanımlı olduğu anlaşılır.

Örnek 2: $\mathcal{Z}_6$ da $\bar{2} \oplus \bar{5} = \bar{7} = \bar{1}$, $\bar{2} \odot \bar{5} = \bar{10} = \bar{4}$ dir.

Önerme 2.3.5 $\mathcal{Z}_m$ de $\oplus$ işleminin şu özellikleri vardır. $\forall \bar{a}, \bar{b}, \bar{c}, \in \mathcal{Z}_m$ için,

i) $\bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a}$ dir. (Değişme özelliği)

ii) $\bar{a} \oplus (\bar{b} \oplus \bar{c}) = (\bar{a} \oplus \bar{b}) \oplus \bar{c}$ dir. (Birleşme özelliği)

iii) $\bar{a} \oplus \bar{0} = \bar{a}$ dır. ($\bar{0}$ etkisiz (sıfır) eleman)

iv) $\bar{a} \oplus \bar{x} = \bar{0}$ olacak şekilde $\exists \bar{x} \in \mathcal{Z}_m$ bulunabilir. (Ters eleman)

İspat: i) $\mathcal{Z}_m$ de $\oplus$ tanımına göre,

$$\bar{a} \oplus (\bar{b} \oplus \bar{c}) = \bar{a} \oplus \overline{b + c} = \overline{a + (b + c)}$$

ve

$$(\bar{a} \oplus \bar{b}) \oplus \bar{c} = \overline{a + b} \oplus \bar{c} = \overline{(a + b) + c}$$

dir. $\mathcal{Z}$ de $+$ nın birleşme özelliğinden dolayı istenen eşitlik elde edilir.

ii) $\forall a, b \in \mathcal{Z}$ için, $a + b = b + a$ olduğundan;
$\bar{a} \oplus \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} \oplus \bar{a}$ elde edilir.

iii) $\bar{a} \oplus \bar{0} = \overline{a + 0} = \bar{a}$ olduğu açıktır.

iv) $\forall a \in \mathcal{Z}$ için, a nın ters işaretlisi $-a$ ile gösterilirse $a + (-a) = 0$ dır. Buradan $\bar{a} \oplus \overline{(-a)} = \overline{a + (-a)} = \bar{0}$ bulunur. Şu halde $\bar{a}$ nın tersi, $\overline{-a}$ sınıfıdır.

Önerme 2.3.6 $\mathcal{Z}_m$ de $\odot$ nın şu özellikleri vardır.
$\forall \bar{a}, \bar{b}, \bar{c}, \in \mathcal{Z}_m$ için;
i) $\bar{a} \odot (\bar{b} \odot \bar{c}) = (\bar{a} \odot \bar{b}) \odot \bar{c}$ dır. (Birleşme özelliği)
ii) $\bar{a} \odot \bar{b} = \bar{b} \odot \bar{a}$ dır. (Değişme özelliği)
iii) $\bar{a} \odot \bar{1} = \bar{a}$ ($\bar{1}$ birim eleman)
iv) $\bar{a} \odot \bar{0} = \bar{0}$ ($\bar{0}$ yutan eleman)

İspat: $\odot$ nın tanımı kullanılarak, önceki önermede olduğu gibi ispatlanır.

Önerme 2.3.7 $\forall \bar{a}, \bar{b}, \bar{c} \in \mathcal{Z}_m$ için,

$$\bar{a} \odot (\bar{b} \oplus \bar{c}) = (\bar{a} \odot \bar{b}) \oplus (\bar{a} \odot \bar{c})$$

dir. ($\odot$ nın $\oplus$ üzerine dağılma özelliği)

İspat:

$$\bar{a} \odot (\bar{b} \oplus \bar{c}) = \bar{a} \oplus \overline{b+c} = \overline{a(b+c)}$$

ve

$$(\bar{a} \odot \bar{b}) \oplus (\bar{a} \odot \bar{c}) = \overline{ab} \oplus \overline{ac} = \overline{ab+ac}$$

dir. $\mathcal{Z}$ de; çarpmanın toplama üzerine dağılma özelliğinden istenen eşitlik elde edilir.

Örnek 3: $\mathcal{Z}_6$ da $\bar{2} \odot (\bar{3} \oplus \bar{4}) = \bar{2} \odot \bar{1} = \bar{2}$ ve $(\bar{2} \odot \bar{3}) \oplus (\bar{2} \odot \bar{4}) = \bar{0} \oplus \bar{2} = \bar{2}$ dir.

$\mathcal{Z}_6$ da $\bar{2} \odot \bar{3} = \bar{0}$ eşitliğinde olduğu gibi sıfır olmayan iki sınıfın çarpımı, $\bar{0}$ olabilir. $\mathcal{Z}$ de ise bu mümkün değildir.

Tanım 2.3.5 $\mathcal{Z}_m$ de kendileri $\bar{0}$ den farklı olduğu halde çarpımları $\bar{0}$ olan sınıflara **sıfır bölen sınıflar** denir.

Örnek 4: $\mathcal{Z}_6$ da sıfır bölenleri; $\bar{2}, \bar{3}, \bar{4}$ dirler.
$\mathcal{Z}_{10}$ da sıfır bölenler; $\bar{2}, \bar{4}, \bar{5}, \bar{6}, \bar{8}$ dirler.

Önerme 2.3.8 $a \equiv b(mod\ m) \Longrightarrow (a, m) = (b, m)$ dir.

İspat: $a \equiv b(mod\ m) \Longrightarrow m|a-b \Longrightarrow a = b + mk$, $\exists k \in \mathcal{Z}$ dır. $(a, m) = d$ olsun. $d|a$ ve $d|m$ olduğundan, $d|b = a - mk$ dır. Şu halde

d, b ile m nin bir ortak bölenidir. Eğer t herhangi bir ortak bölen ise $t|b$ ve $t|m \Longrightarrow t|a = b + mk$ olacağından, $t|d = (a,m)$ bulunur. Şu halde $d = (b,m)$ dir.

Not: Yukarıdaki önermeye göre bir kalan sınıfındaki tüm sayıların modül ile ebob leri aynıdır. Şu tanım yapılabilir.

Tanım 2.3.6 $\bar{a} \in \mathcal{Z}$ sınıfı için, $(a,m) = 1$ ise $\bar{a}$ sınıfına bir **asal kalan sınıfı** denir. $\mathcal{Z}_m$ nin bütün asal kalan sınıfları $\mathcal{Z}_m^*$ ile gösterilir.

$\mathcal{Z}_m^*$ eleman sayısının $\phi(m)$ Euler fonksiyonu ile verildiğine dikkat edelim. Ayrıca m modülü asal ise $\mathcal{Z}_m^* = \mathcal{Z}_m - \{\bar{0}\}$ olduğu açıktır.

Önerme 2.3.9 İki asal kalan sınıfının çarpımı da bir asal kalan sınıfıdır.

İspat: $\bar{a}, \bar{b} \in \mathcal{Z}_m^*$ olsun. $(a,m) = (b,m) = 1$ olduğundan, $xa + ym = 1$ olacak şekilde $\exists x, y \in \mathcal{Z}$ bulunabilir. Bu eşitliğin her iki yanını b ile çarparsak,

$b = xab + ymb$ elde edilir. $(ab,m) = t$ dersek, $t|ab$ ve $t|m$ bulunur. $(m,b) = 1$ kabul ettiğimiz için, m ve b nin bir ortak böleni olan $t = 1$ olmalıdır. Şu halde $\overline{ab} = \bar{a} \odot \bar{b}$ de bir asal kalan sınıfıdır.

Önerme 2.3.10 $\mathcal{Z}_m$ deki $\bar{0}$ dan farklı bir kalan sınıfının sıfır bölen olması için gerek ve yeter koşul kalan sınıfı olmamasıdır.

İspat: $\Longrightarrow$: $\bar{0} \neq \bar{a} \mathcal{Z}_m$ bir sıfır bölen olsun. Şu halde $\bar{a}\bar{b} = \bar{0}$ olacak şekilde bir $\bar{b} \in \mathcal{Z}_m$ bulunabilir.

$\bar{a}$ nın bir asal kalan sınıfı olduğunu kabul edelim. Yani $(a,m) = 1$ olsun. $\bar{a}\bar{b} = \overline{ab} = \bar{0} \Longrightarrow m|ab$ ve $(a,m) = 1$ olduğundan, $m|b$ yani $\bar{b} = \bar{0}$ çelişkisi elde edilir. Şu halde $\bar{a}$ bir asal kalan sınıfı değildir.

$\Longleftarrow$: $\bar{0} \neq \bar{a}$ bir asal kalan sınıfı olmasın. Şu halde $(a,m) = d > 1$ dir. $\bar{a} \neq \bar{0}$ olduğundan, $m \nmid a$ dır. Buradan, $d \neq m$ bulunur.

$(a,m) = d \Longrightarrow m = dm', a = da'$ ve $(a',m') = 1$, $\exists a', m' \in \mathcal{Z}$ bulunabilir. $am' = da'm' = a'm$ eşitliğinden, $\bar{a}\overline{m'} = \bar{0}$ bulunur. $\overline{m'} \neq \bar{0}$ olduğundan, sonuç olarak $\bar{a}$ nin bir sıfır bölen olduğu anlaşılır.

Tanım 2.3.7 $\bar{a} \in \mathcal{Z}_m$ olsun. $\bar{a}\bar{c} = \bar{1}$ olacak şekilde $\exists \bar{c} \in \mathcal{Z}_m$ varsa $\bar{c}$

ye $\bar{a}$ nın tersi denir.

$\mathcal{Z}_m$ de hangi sınıfların tersinin olduğunu aşağıdaki önerme gösterir.

Önerme 2.3.11 $\mathcal{Z}_m$ deki bir kalan sınıfının tersinin olması için gerek ve yeter koşul bir asal kalan sınıfı olmasıdır.

İspat: $\Longrightarrow$: $\bar{a} \in \mathcal{Z}_m$ nin tersi mevcut olsun. Yani $\bar{a}\,\bar{c} = \bar{1}$ olacak şekilde $\exists \bar{c} \in \mathcal{Z}_m$ bulunabilsin. $\bar{a}$ nin bir sıfır bölen olmadığını gösterirsek Önerme 2.3.10'a göre bir asal kalan sınıfı olur.

Bir $\bar{0} \neq \bar{b} \in \mathcal{Z}_m$ için, $\bar{a}\bar{b} = \bar{0}$ olduğunu kabul edelim. Bu eşitliğin her iki yanını $\bar{a}$ nin tersi $\bar{c}$ ile çarparsak,

$$\bar{c}(\bar{a}\bar{b}) = (\bar{c}\bar{a})\bar{b} = \bar{b} = \bar{0}$$

çelişkisi elde edilir. Şu halde $\bar{a}$ bir sıfır bölen değildir.

$\Longleftarrow$: $\bar{a}$ bir asal kalan sınıfı olsun. Bu takdirde, $(a, m) = 1$ ve $xa + ym = 1$ olacak şekilde $\exists x, y \in \mathcal{Z}$ bulunabilir. Buradan, $xa \equiv 1(mod\ m)$ veya $\bar{x}\,\bar{a} = 1$ elde edilir. Şu halde $\bar{a}$ nın tersi mevcuttur.

Sonuç: m asal tam sayı ise $\mathcal{Z}_m$ deki sıfırdan farklı her kalan sınıfının tersi mevcuttur.

Örnek 5: $\mathcal{Z}_{10}$ daki asal kalan sınıfları veya tersi mevcut sınıflar $\phi(10) = \phi(5) = 4$ tane olup, bunlar; $\bar{1}, \bar{3}, \bar{7}, \bar{9}$ durlar. $\mathcal{Z}_{10}$ daki sıfır bölenler de; $\bar{2}, \bar{4}, \bar{5}, \bar{6}, \bar{8}$ dirler.

Euler Teoremi 2.3.1 $m \in \mathcal{Z}$ olsun. $(a, m) = 1$ olan $\forall a \in \mathcal{Z}$ için $a^{\phi(m)} \equiv 1(mod\ m)$ veya $\bar{a}^{\phi(m)} = \bar{1}$ dir.

İspat: $\mathcal{Z}_m^*$ asal kalan sınıflar kümesini düşünelim. $\bar{a} \in \mathcal{Z}_m^*$ sabit bir asal kalan sınıfını alalım. $\forall \bar{b} \in \mathcal{Z}_m^*$ için, $f(\bar{b}) = \bar{a}\bar{b}$ ile
$f : \mathcal{Z}_m^* \longrightarrow \mathcal{Z}_m^*$ fonksiyonu tanımlayalım. Önceki önermeye göre $\bar{a}\bar{b} \in \mathcal{Z}_m^*$ olduğu açıktır.

f nin 1-1 olduğunu gösterelim.

$$f(\bar{b}) = f(\bar{c}) \Longrightarrow \bar{a}\,\bar{b} = \bar{a}\,\bar{c} \Longrightarrow \bar{b} = \bar{c}$$

($\bar{a}$ nın tersi olduğundan) elde edilir.

$\mathcal{Z}_m^* = \{\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{\phi(m)}\}$ sonlu elemanlı bir küme olduğundan, f nin 1-1 olması örten olmasını da gerektirir.

Şu halde f, $\mathcal{Z}_m^*$ ın elemanlarını aralarında değiştireceğinden,

$$\bar{a}_1\bar{a}_2\cdots\bar{a}_{\phi(m)} = f(\bar{a}_1)f(\bar{a}_2)\cdots f(\bar{a}_{\phi(m)}) = \bar{a}^{\phi(m)}\bar{a}_1\bar{a}_2\cdots\bar{a}_{\phi(m)}$$

dir. $\bar{a}_1\bar{a}_2\cdots\bar{a}_{\phi(m)}$ asal kalan sınıfı ile kısaltarak, $\bar{a}^{\phi(m)} = \bar{1}$ bulunur.

Sonuç: (**Fermat Teoremi**) Özel olarak $m = p$ asal tamsayı ise $p \nmid a$ olan $\forall a \in \mathcal{Z}$ için, $a^{p-1} \equiv 1(mod\ p)$ dir.

Örnek 6: 3^{27} nin 5 ile bölümünden elde edilen kalanı bulalım. Fermat teoremine göre $\phi(5) = 4$ ve

$$3^4 \equiv 1(mod\ 5) \Longrightarrow (3^4)^6 = 3^{24} \equiv 1(mod\ 5)$$

olduğundan, $3^{27} \equiv 3^3 \equiv 2(mod\ 5)$ elde edilir.

Tanım 2.3.8 $ax \equiv b(mod\ m)$ şeklindeki bir denkleme **bir bilinmeyenli lineer kongrüans** denir. Bu denklemi sağlayan x tam sayılarının kümesine de kongrüansın **çözüm kümesi** denir.

Önerme 2.3.12 $ax \equiv b(mod\ m)$ nin bir çözümü $x_0 \in \mathcal{Z}$ ise $\bar{x}_0 \in \mathcal{Z}_m$ sınıfındaki tüm sayılar da bir çözümdür.

İspat: $\forall x \in \bar{x}_0$ için, $x \equiv x(mod\ m) \Longrightarrow ax \equiv ax_0 \equiv b(mod\ m)$ olduğundan, istenen elde edilir.

Önerme 2.3.13 $(a, m) = 1$ ise $ax \equiv b(mod\ m)$ nin çözümü var ve $mod\ m$ tek bir sınıftır.

İspat: $(a, m) = 1$ olduğundan, $\bar{a}\bar{c} = \bar{1}$ olacak şekilde $\exists \bar{c} \in \mathcal{Z}_m$ vardır. $ax \equiv b(mod\ m)$ kongrüansının her iki yanını, $\bar{c} = (\bar{a})^{-1}$ ile çarparak, $x \equiv bc(mod\ m)$ bulunur. $\bar{x} = \overline{bc} \in \mathcal{Z}_m$ bir çözümdür.

Şimdi çözümün, $mod\ m$ tek bir sınıftan ibaret olduğunu gösterelim. $\bar{x}_1$ ve $\bar{x}_2$ iki çözüm olsun.

$$\bar{a}\bar{x}_1 = \bar{a}\bar{x}_2 \Longrightarrow \bar{x}_1 = \bar{x}_2$$

dir. Çünkü, $\bar{a}$ bir asal kalan sınıfı olup tersi mevcuttur.

Şimdi lineer kongrüansın çözümü için bir kriter verelim.

Önerme 2.3.14 $ax \equiv b(mod\ m)$ nin bir çözümünün olması için gerek ve yeter koşul $(a,m)|b$ olmasıdır.

İspat: $\Longrightarrow$: $ax \equiv b(mod\ m)$ nin bir çözümü x_0 olsun. Şu halde $ax_0 \equiv b(mod\ m) \Longrightarrow m|ax_0 - b$ olduğundan, $ax_0 - b = km$ olacak şekilde $\exists k \in \mathcal{Z}$ bulunabilir.

$$(a,m)|a \text{ ve } (a,m)|m \Longrightarrow (a,m)|b = ax_0 - km$$

elde edilir.

$\Longleftarrow$: $(a,m)|b$ olsun. $(a,m) = d$ diyelim. $a = da'$ ve $m = dm'$ olacak şekilde $\exists a', m' \in \mathcal{Z}$ bulunabilir ve $(a',m') = 1$ dir. $d|b$ kabul ettiğimizden, $b = db'$ olacak şekilde $\exists b' \in \mathcal{Z}$ bulunabilir.

$$ax \equiv b(mod\ m) \Longleftrightarrow ax - by = m, \exists x, y \in \mathcal{Z}$$

denktirler. $x, y \in \mathcal{Z}$ olmak üzere $ax - by = m$ denklemine bir **Diophant denklemi** denir.

Diophant denkleminin her iki yanını d ile kısaltarak;

$$a'x - b'y = m' \Longleftrightarrow a'x \equiv b'(mod\ m')$$

elde edilir. Önerme 2.3.13'e göre son kongrüansın çözümü var ve $mod\ m'$ tek sınıftır. $\bar{a}$ nün $mod\ m'$ tersi $\bar{c}$ ise bu çözüm, $x = cb' + qm'$ $(q \in \mathcal{Z})$ dir.

Sonuç: $ax \equiv b(mod\ m)$ kongrüansı verilsin. $d = (a,m)|b$ ise bu kongrüansın çözümleri $mod\ m$, d sınıftır.

İspat: $a = da'$, $b = db'$ ve $m = dm'$ ise yukarıdaki önermeye göre;

$$ax \equiv b(mod\ m) \Longleftrightarrow a'n \equiv b'(mod\ m)$$

ve son kapsamın çözümü $mod\ m'$ tek sınıftır. Bu çözüm, $\bar{c}$ sınıfı $\bar{a}'$ nün $mod\ m'$ tersi olmak üzere, $x = cb' + qm'$, $(q \in \mathcal{Z})$ ile verilir. Eğer q tam sayısı olarak, $q = dk + r$, $0 \leq r < d$, $(k \in \mathcal{Z})$ koyarsak bütün çözümler $x = cb' + rm' + km$, $(k \in \mathcal{Z})$ olur. $mod\ m$ kalan sınıfları

olarak düşünülürse, $r = 0, 1, \ldots, d-1$ alınarak bu sınıfların sayısının d tane olduğu görülür.

Örnek 7: $6x \equiv 3(mod\ 15)$ kongrüansının çözümlerini *mod* 15 kalan sınıfları ile bulalım. $(6, 15) = 3|3$ olduğundan çözüm var ve *mod* 15, 3 sınıf çözümdür.

$$6x \equiv 3(mod\ 15) \Longleftrightarrow 2x \equiv 1(mod\ 4)$$

$\bar{2}$ nın *mod* 5 tersi $\bar{3}$ olduğundan, son kongrüansın çözümü $x \equiv 3(mod\ 5)$ dir. Bu çözümleri $x = 3 + 5q, (q \in \mathcal{Z})$ olarak yazalım ve sırası ile $q = 3k + r$ ve $r = 0,\ 1,\ 2$ koyalım.

$$\begin{cases} r = 0 & \Longrightarrow \quad x = 3 + 15k \\ r = 1 & \Longrightarrow \quad x = 8 + 15k \\ r = 2 & \Longrightarrow \quad x = 11 + 15k \end{cases}$$

yani *mod* m çözümler $\bar{3}$, $\bar{8}$ ve $\bar{11}$ olarak bulunur.

Özetliyecek olursak, bir lineer kongrüansın çözümlerini bulma; $(a, m) = 1, ax \equiv b(mod\ m)$ kongreansının çözümlerini bulmaya indirgenir ve bunun için 3 yol izlenebilir.

1) $\bar{a}$ nın *mod* m tersi kolaylıkla bulunabilirse ve tersi $\bar{c}$ ise çözüm $x \equiv bc(mod\ m)$ dir.

2) Verilen kongrüans diophant denklemine çevrilir.

$$ax \equiv b(mod\ m) \Longleftrightarrow ax - my = b, \quad \exists x, y \in \mathcal{Z}$$

a ve m tam sayılarına ardarda kalanlı bölmeler uygulayarak, $1 = ax' - my'$ olacak şekilde $\exists x', y' \in \mathcal{Z}$ bulup, her iki yanı b ile çarpılarak bir x çözümü, dolayısı ile kongrüansın *mod* m, $\bar{x}$ çözüm sınıfı bulunmuş olur.

3) Verilen kongrüans denk kongrüanslara dönüştürülerek modül küçültülür.

Şimdi bir örnek üzerinde bu yolları açıklayalım.

Örnek 8: $38x \equiv 16\ (mod\ 111)$ kongrüansını çözelim. $(38, 111) = 1$ olduğundan çözüm var ve *mod* 111 tek sınıftır.

1.yol: $\overline{38}$ nin *mod* 111 tersini bulmak kolay değildir. Onun için bu yolla yapmayalım.

2.yol: $38x \equiv 16 mod\ 111 \iff 38x - 111y = 16$ dır. $(38, 111) = 1$ olup,

$111 = 2.38 + 35$
$38 = 1.35 + 3$
$35 = 11.3 + 2$
$3 = 1.2 + 1$

ve son eşitlikden 1'i çekip, başa doğru yerine koya koya 1' i 111 ve 38 cinsinden hesaplarsak;

$1 = 3 - 2 = 3 - (35 - 11.3) = 12.3 - 35$
$= 12.(38 - 35) - 35 = 12.38 - 13.35$
$= 12.38 - 13.(111 - 2.38) = 38.38 - 13.111$ bulunur.

$1 = 38.38 - 13.111$ eşitliğinin her iki yanını 16 ile çarparak, $16 = (16.38).38 - (16.13).111$ ve diophant denkleminin bir çözümü de $x = 16.38 = 608$ ve $y = 16.13 = 208$ olarak elde edilir.

Şu halde verilen kongrüansın *mod* 111 tek çözüm sınıfı $\overline{x} = \overline{608} = \overline{53}$ bulunur.

3.yol: Modül küçülterek verilen kongrüansı çözelim:

$$\begin{aligned} 38x \equiv 16(mod\ 111) &\iff 38x - 111y = 16 \\ &\iff -111y \equiv 3y \equiv 16(mod\ 38) \\ &\iff 3y - 38z = 16 \\ &\iff -38z \equiv z \equiv 16 \equiv 1(mod\ 3) \end{aligned}$$

denkliklerini kullanarak bir çözüm bulalım. z=1 alınırsa, $3y = 38 + 16 = 54 \Longrightarrow y = 18$,

$$38x = 111.18 + 16 = 2014 \Longrightarrow x = 53$$

bulunur. Şu halde *mod* 111, 53 ün sınıfı $\overline{53}$ tek çözümdür.

Şimdi birden çok sayıda verilen kongrüans sistemlerinin çözümünü inceliyelim. Aşağıdaki teorem **Çinlilerin Kalan Teoremi** olarak bilinir.

Önerme 2.3.14 $m, n \in \mathcal{Z}$ ve $d = (m, n)$ olsun.

$$\begin{cases} x \equiv a(mod\ m) \\ x \equiv b(mod\ n) \end{cases}$$

denklik sisteminin çözümünün bulunabilmesi için gerek ve yeter koşul $a \equiv b(mod\ d)$ olmasıdır. Bu takdirde çözüm, $mod\ [m, n]$ tek bir sınıftır.

İspat: $\Longrightarrow$: Verilen denklem sisteminin bir çözümünün varlığını kabul edelim. Birinci denklemden, $x = a + tm$ olacak şekilde $\exists t \in \mathcal{Z}$ bulunabilir. Bunu ikinci denklemde yerine yazarsak,

$$x = a + tm \equiv b(mod\ n) \Longrightarrow tm \equiv b - a(mod\ n)$$

elde edilir. Önerme 2.3.13 gereğince, çözümün varlığından $(m, n) = d | b - a$, yani $a \equiv b(mod\ d)$ elde edilir.

$\Longleftarrow$: $a \equiv b(mod\ d)$ olsun. $x \equiv a(mod\ m) \Longleftrightarrow x = a + tm$ ve bunu ikinci denklemde yerine yazarsak,

$$a + tm \equiv b(mod\ n) \Longleftrightarrow tm \equiv b - a(mod\ n)$$

bulunur. $(m, n) = d \mid b - a$ kabul ettiğimizden, Önerme 2.3.13 gereğince son kongrüansın bir çözümünün mevcut olduğu anlaşılır.

$$tm \equiv b - a(mod\ n) \Longleftrightarrow t\frac{m}{d} \equiv \frac{b-a}{d}(mod\ \frac{n}{d})$$

ve $(\frac{m}{d}, \frac{n}{d}) = 1$ olduğundan, Önerme 2.3.13 gereğince istenilen şekilde bir t tam sayısı mevcut ve $mod\ \frac{n}{d}$ teklikle belirli olduğu anlaşılır. Bu çözüm t_0 ise ve $t = t_0 + u\frac{n}{d}$, $(u \in \mathcal{Z})$ koyarsak,

$$x = a + (t_0 + u\frac{n}{d})m = a + t_0 m + u\frac{mn}{d}$$

bulunur. $(m, n) = d$ ve $(m, n)[m, n] = mn$ olduğu göz önünde tutulursa, $a_0 = a + t_0 m$ için $x \equiv a_0(mod\ [m, n])$ elde edilir.

Şimdi sistemin çözümünün $mod\ [m, n]$ teklikle belirli olduğunu gösterelim. x ve y iki çözüm olsunlar.

$$\begin{cases} x \equiv a(mod\ m) \\ x \equiv b(mod\ n) \end{cases}$$

ve

$$\begin{cases} y \equiv a(mod\ m) \\ y \equiv b(mod\ n) \end{cases}$$

kongrüanslarından, $m|x-y$ ve $n|x-y$ bulunur. Şu halde ekok tanımından, $[m,n]|x-y$ yani,
$x \equiv y(mod\ [m,n])$ elde edilir.

Sonuç: $(m,n)=1$ ise $\begin{cases} x \equiv a(mod\ m) \\ x \equiv b(mod\ n) \end{cases}$
denklem sisteminin çözümü var ve $mod\ mn$ tektir.

Örnek 9: $(6,8)=2|4-2$ olduğundan,

$$\begin{cases} x \equiv 2(mod\ 6) \\ x \equiv 4(mod\ 8) \end{cases}$$

sisteminin; çözümü var ve mod 24 tek sınıf çözümdür.

$x \equiv 2(mod\ 6) \Longrightarrow x = 2+6t$, ikinci denklemde yerine konursa;

$$\begin{aligned} 2+6t \equiv 4(mod\ 8) &\Longleftrightarrow 6t \equiv 2(mod\ 8) \\ &\Longleftrightarrow 3t \equiv 1(mod\ 4) \\ &\Longleftrightarrow t \equiv 3(mod\ 4) \end{aligned}$$

bulunur. $t = 3+4u$, $(u \in \mathcal{Z})$ dersek,

$$x = 2+6t = 2+6(3+4u) = 20+24u$$

yani $\bar{x} = \overline{20}$ tek çözümdür.

Örnek 10: $(3,5,7)=1$ olduğu için,

$$\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 3(mod\ 5) \\ x \equiv 4(mod\ 7) \end{cases}$$

sisteminin çözümü var ve mod 3.5.7 tek sınıf çözümdür.

$$x \equiv 2(mod\ 3) \Longrightarrow x = 2+3t, \quad (t \in \mathcal{Z})$$

$$\begin{aligned} x = 2+3t \equiv 3(mod\ 5) &\Longrightarrow 3t \equiv 1(mod\ 5) \\ &\Longrightarrow t \equiv 2(mod\ 5) \\ &\Longrightarrow t = 2+5k, \quad (k \in \mathcal{Z}) \end{aligned}$$

$x = 2 + 3(2 + 5k) = 8 + 15k \equiv 5(mod\ 7) \Longrightarrow$
$15k \equiv k \equiv -3 \equiv 4(mod\ 7) \Longrightarrow k = 4 + 7t, \quad (t \in \mathcal{Z})$
bulunur. Şu halde $n = 8+15(4+7t) = 68+105t$, yani $\overline{x} = \overline{68}$ çözümdür.

2.3 ALIŞTIRMALAR

1-) $\mathcal{Z}_9$ da $\bar{3}\bar{x} + \bar{2} = \bar{6}$ denklemini çözünüz.

2-) $\mathcal{Z}_{11}$ de $\bar{3}\bar{x} + \bar{2} = \bar{6}$ denklemini çözünüz.

3-) $(m, n) = 1$ ve $an \equiv bn(mod\ m)$ ise $a \equiv b(mod\ m)$ olduğunu, fakat $(m, n) \neq 1$ ise eşitliğin yanlış olabileceğini gösteriniz.

4-) $an \equiv bn(mod\ m) \Longleftrightarrow a \equiv b(mod\ \frac{m}{(m,n)})$ olduğunu gösteriniz.

5-) Her a tek tam sayısı için, $a^2 \equiv 1(mod\ 8)$ olduğunu gösteriniz.

6-) $p \neq 2$ asal bir tam sayı ise $x^2 \equiv 1(mod\ p)$ kongrüansının $\mathcal{Z}_p$ de tam iki çözümü olduğunu gösteriniz.

7-) $5x + 11y = 33$ diophant denklemini çözünüz.

8-) $14x \equiv 21(mod\ 28)$ kongrüansının çözümlerini $mod\ 28$ kalan sınıfları olarak bulunuz.

9-) Bir sepetteki yumurtalar 9 ar 9 ar sayıldığından 5, 20 şer 20 şer sayıldığında 8 artmaktadır. Sepetteki yumurtaların sayısı 1000 ile 1300 arasında olduğu bilindiğine göre kaç yumurta vardır, bulunuz.

10-) Aşağıdaki sistemleri çözünüz.

a) $\begin{cases} x \equiv 7(mod\ 10) \\ x \equiv 5(mod\ 27) \end{cases}$

b) $\begin{cases} x \equiv 6(mod\ 10) \\ x \equiv 8(mod\ 18) \end{cases}$

c) $\begin{cases} x \equiv 2(mod\ 9) \\ x \equiv 3(mod\ 12) \end{cases}$

11-) $28x \equiv 15(mod\ 107)$ kongrüansını çözünüz.

12-) $a^{10} \equiv 10(mod\ 26)$ olduğuna göre $(a, 26)$ kaçtır?

13-) $(a, 15) = 1$ ise $a^4 \equiv 1(mod\ 15)$ olduğunu gösteriniz.

14-) $2x \equiv 1(mod\ 63)$ kongrüansını sağlayan en küçük doğal sayıyı bulunuz.

15-) 7^{9999} sayısının son üç basamağını bulunuz.

BÖLÜM 3

GRUPLAR

Bu bölümde tek işlemli cebirsel yapılardan olan grup üzerinde duracağız.

3.1 GRUP AKSİYOMLARI

Tanım 3.1.1 G boş olmayan bir küme ve $*, G$ de bir ikili işlem olsun. $(G,*)$ cebirsel yapısı aşağıdaki aksiyomları sağlıyorsa bir **grup** denir.

$G1$: $*, G$ de bir ikili işlemdir.

$G2$: $*$ işleminin G de birleşme özelliği vardır. Yani, $\forall a,b,c \in G$ için, $a*(b*c) = (a*b)*c$ dir.

$G3$: $*$ işleminin, G de birim elemanı vardır. Yani, $\forall a \in G$ için, $a*e = e*a = a$ olacak şekilde $\exists e \in G$ vardır.

$G4$: $*$ işlemine göre, G deki her elemanın bir tersi vardır. Yani $a \in G$ için, $a*a^{-1} = a^{-1}*a = e$ olacak şekilde $\exists a^{-1} \in G$ bulunabilir.

Not: Önerme 1.4.1 ve Önerme 1.4.2 ye göre, birim elemanın ve ters elemanın teklikle belirli olduğu görülür.

Tanım 3.1.2 $(G,*)$ bir grup ve $\forall a,b \in G$ için $a*b = b*a$ değişme özelliği de sağlanıyorsa gruba, **değişmeli grup** veya **Abel grubu** denir.

Tanım 3.1.3 G sonlu bir küme ise $(G, *)$ grubuna bir **sonlu grup** denir ve eleman sayısına da **grubun mertebesi** denir.

Not: Değişmeli gruplarda işlem $+$ ise **toplamsal grup** denir. Grubun işlemi . ise **çarpımsal grup** denir. Çarpımsal grup, değişmeli olmayabilir.

Örnek 1: $\mathcal{Z}$ tam sayılar kümesi, adi toplama işlemine göre bir toplamsal gruptur.

Örnek 2: $\mathcal{Q}$ rasyonel sayılar kümesi ve $\mathbb{R}$ reel sayılar kümesi, adi toplama işlemine göre birer toplamsal grupturlar.

Örnek 3: $\mathcal{Q} - \{0\}$ ve $\mathbb{R} - \{0\}$ kümeleri, adiçarpma işlemine göre birer değişmeli, çarpımsal grupturlar.

Örnek 4: $G = \{1, -1\}$ kümesi, çarpma işlemine göre mertebesi 2 olan bir değişmeli gruptur.

Örnek 5: $G = \{1, -1, i, -i\}$ kümesi çarpma işlemine göre mertebesi 4 olan bir değişmeli gruptur.

Örnek 6: $A \neq \emptyset$ kümesi için, $S(A)$ ile A nın, kendi üzerine 1-1 bütün fonksiyonları kümesini gösterelim. Önerme 1.3.3 ye göre, $S(A)$ bileşke işlemi altında değişmeli olmayabilen bir gruptur.

Tanım 3.1.4 $A \neq \emptyset$ sonlu bir küme ise A nın kendi üzerine 1-1 fonksiyonlarına bir **permütasyon** denir ve A, n elemanlı ise A nın permütasyonları kümesi, $S(A) = S_n$ ile gösterilir ve **simetrik grup (permutasyon grubu)** denir.

S_n, $n!$ elemanlı bir gruptur.

Önerme 3.1.1. (Kısaltma özelliği) $(G, *)$ bir grup ise $\forall a, b, c \in G$ için;

i) $a * b = a * c \Longrightarrow b = c$ ve

ii) $a * c = b * c \Longrightarrow a = b$ kısaltma özellikleri sağlanır.

İspat: (i) $(G, *)$ bir grup olduğundan, her elemanın tersi vardır.

Eşitliğin her iki yanı sodan a^{-1} ile çarpılarak;

$$\begin{aligned} a*b=a*c &\Longrightarrow a^{-1}*(a*b)=a^{-1}*(a*c) \\ &\Longrightarrow (a^{-1}*a)*b=(a^{-1}*a)*c \\ &\Longrightarrow b=c \end{aligned}$$

elde edilir.

ii) Benzer şekilde ispatlanır.

Önerme 3.1.2 $(G,*)$ bir grup ise $\forall a,b\in G$ için;

i) $a*x=b$ ve

ii) $y*a=b$ olacak şekilde $\exists x,y\in G$ var ve teklikle belirlidir.

İspat: (i) $(G,*)$ bir grup olduğundan, her elemanın tersi vardır. Eşitliğin her iki yanını soldan a^{-1} ile çarparak;

$$a*x=b\Longrightarrow a^{-1}*(a*x)=a^{-1}*b\Longrightarrow (a^{-1}*a)*x=a^{-1}*b\Longrightarrow x=a^{-1}*b$$

bulunur. Şu halde $x=a^{-1}*b\in G$ aranan elemandır.

Şimdi, varlığını gösterdiğimiz x elemanının tekliğini gösterelim. Eşitliği sağlayan iki $x_1,x_2\in G$ olsa idi, kısaltma özelliğini gösteren, önceki önerme kullanılarak;

$$a*x_1=a*x_2\Longrightarrow x_1=x_2$$

bulunurdu.

(ii) Benzer şekilde ispatlanır.

Not: $(G,*)$ grubunda birleşme özelliği sağlandığından, herhangi üç eleman için;

$$(a*b)*c=a*(b*c)$$

yerine $a*b*c$ yazılabilir. Tümevarımla, $\forall k\in\mathbb{N}$ için de $a_1*a_2*\ldots*a_k$ tanımlanabilir ve genel birleşme kuralı (Bak 1.4 Alıştırma 1) sağlanır.

Şimdi çarpımsal bir grupta bir elemanın kuvvetini tanımlayalım.

Tanım 3.1.5 G bir grup ve $a\in G$ olsun. $n\in Z$ için,

$$a^n=\begin{cases} a.a\ldots a \ (n \text{ defa}) \ ; & \text{eğer } n>0 \text{ ise,} \\ 1 \ ; & \text{eğer } n=0 \text{ ise,} \\ a^{-1}.a^{-1}\ldots a^{-1} \ (-n \text{ defa}) \ ; & \text{eğer } n<0 \text{ ise,} \end{cases}$$

ile tanımlanır.

Önerme 3.1.3 G bir grup ve $a, b \in G$ olsun. $\forall m, n \in \mathbb{N}$ için
(i) $a^m.a^n = a^{m+n}$ ise,
(ii) $(a^m)^n = a^{mn}$ dir.
(iii) G değişmeli grup ise $(a.b)^n = a^n.b^n$ dir.

İspat: (i) $a^m.a^n = a^{m+n}$ olduğunu, n üzerine tümevarım uygulayarak ispatlıyalım. $n = 1$ için, $a^m.a = a^{m+1}$ olduğu, tanımdan kolayca görülür. n için kabul edip, $n + 1$ için eşitliği ıspatlıyalım:

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

(ii) ve (iii) nin ispatları okuyucuya bırakılmıştır.

Not: $m, n \in \mathbb{N}$ için, $(a^m)^{-1} = (a^{-1})^m = a^{-m}$ olduğu gösterilerek, yukarıdaki önermenin $\forall m, n \in Z$ için doğru olduğu da gösterilebilir.

Toplamsal grupta da kuvvet yerine kat tanımlanabilir.

Tanım 3.1.6 $(G, +)$ bir grup ve $a \in G$olsun. $n \in Z$ için

$$na = \begin{cases} a + a + \ldots + a \ \ (n \text{ defa}); & \text{eğer } n > 0 \text{ ise,} \\ 0 \ ; & \text{eğer } n = 0 \text{ ise,} \\ (-a) + (-a) + \ldots + (-a) \ \ (-n \text{ defa}); & \text{eğer } n < 0 \text{ ise} \end{cases}$$

ile tanımlanır.

Önerme 3.1.4 $(G, +)$ bir grup ve $a, b \in G$ olsun. $\forall m, n \in Z$ için
i) $ma + na = (m + n)a$,
ii) $m(na) = (mn)a$ ve
iii) $n(a + b) = na + nb$ dir.

İspat: Önceki önerme gibi ispatlanır.

Önerme 3.1.5 $G \neq \emptyset$ bir küme ve $*, G$ de bir ikili işlem olsun. $*$ işlemi, $G1$ (kapalılık) ve $G2$ (birleşme) aksiyomları ile aşağıdaki koşulları sağlasın:

A) $\forall a \in G$ için, $e * a = a$ olacak şekilde bir $e \in G$ (sol birim) ve

B) G de alınan herhangi bir a elemanı için, $a^* * a = e$ olacak şekilde bir $a^* \in G$ (a nın sol tersi) bulunabilsin.

Bu takdirde, $G1$, $G2$, A, B koşulları grup aksiyomlarına denktirler.

İspat: $G1, G2, A$ ve B özellikleri varsa, $(G, *)$ ın bir grup olacağını, yani $G3$ ve $G4$ aksiyomlarının da sağlandığını gösterelim.

$G4$: Önce $\forall a \in G$ nın sol tersi varsa a^{-1} tersinin de varlığını, yani

$$a^* * a = e \ \ ise \ \ a^* * a = a * a^* = e \Longrightarrow a^* = a^{-1}$$

olduğunu gösterelim.

(B) den $a^* * a = e$ olduğundan, $(a^* * a) * a^* = e * a^*$ ve (A) dan $e * a^* = a^*$ olduğundan, $a^* * (a * a^*) = (a^* * a) * a^* = a^*$ bulunur. Tekrar (B) yi kullanarak, $(a^*)^* * a^* = e$ olacak şekilde bir $(a^*)^* \in G$ bulunabileceğinden, önceki eşitliğin her iki yanını soldan $(a^*)^*$ ile çarparak;

$$[(a^*)^* * a^*] * (a * a^*) = a * a^* = (a^*)^* * a^* = e$$

bulunur. Şu halde $a^* = a^{-1}$ dir.

$G3$: Şimdi de sol birimin, G de $*$ işlemine göre birim olduğunu, yani, $\forall a \in G$ için $e * a = a * e = a$ eşitliğini gösterelim:

(B) den, $\forall a \in G$ için $a^* * a = e$ olacak şekilde $\exists a^* \in G$ bulunabildiğinden,

$$a * e = a * (a^* * a) = (a * a^*) * a$$

ve $G4$ ün ispatında görüldüğü gibi, $a * a^* = e$ olduğundan son eşitlikten, $a * e = e * a = a$ elde edilir.

Tersine olarak, $(G, *)$ bir grup ise (A) ve (B) nin sağlanacağı besbellidir.

Önerme 3.1.6 $G \neq \emptyset$ bir küme ve $*, G$ de bir ikili işlem olsun. $*$ işleminin, $G1$ (kapalılık) ve $G2$ (birleşme) özellikleri ile

I) $\forall a, b \in G$ için $a * x = b$ ve $y * a = b$ olacak şekilde $\exists x, y \in G$ bulunabilsin.

Bu takdirde, $G1, G2, I$ koşulları grup aksiyomlarına denktirler.

İspat: $(G,*)$ bir grupsa, $G1$ ve $G2$ grup aksiyomları ile birlikte (I) koşulunun, yani soldan ve sağdan bölmenin mümkün olduğunu görmek kolaydır. Gerçekten $x = a^{-1} * b$ ve $y = b * a^{-1}$ olarak alınabilir.

Tersine, $G1$ ve $G2$ ile birlikte (I) koşulu sağlanırsa $(G,*)$ ın bir grup olacağını gösterelim. Bunun için, önceki probleme göre, G de bir sol birim ve G deki her elemanın bir sol tersinin varlığını göstermek yeter.

$b \in G$ alalım. (I) ya göre, $y * b = b$ olacak şekilde bir $y = e \in G$ nin varlığı bilinmektedir. Şimdi bu e için, $\forall a \in G$ elemanının $e * a = a$ eşitliğinin sağlandığını yani, e nin bir sol birim olduğunu gösterelim.

(I) ya göre, $b * f = a$ olacak şekilde bir $f \in G$ vardır.

$$e * a = e * (b * f) = (e * b) * f = b * f = a$$

olacağından, istenen elde edilir. Şimdi $\forall a \in G$ nin bir sol tersinin varlığını gösterelim.

(I) ya göre, $y * a = e$ olacak şekilde $\exists y = a^* \in G$ var ve bu a nın sol tersidir.

Önerme 3.1.7 $G \neq \emptyset$ sonlu bir küme ve $*$, G de bir ikili işlem olsun. $*$ işleminin, $G1$ (kapalılık), $G2$ (birleşme) ve sağdan, soldan kısaltma özellikleri varsa $(G,*)$ bir gruptur.

İspat: $G \neq \emptyset$ sonlu bir küme ve $a \in G$ olsun. $f_a : G \longrightarrow G$ fonksiyonunu, $\forall x \in G$ için $f_a(x) = a * x$ ile tanımlayalım. Soldan kısaltma özelliği sağlandığından,

$$f_a(x) = f_a(y) \Longrightarrow a * x = a * y \Longrightarrow x = y,$$

yani f_a nın 1-1 olduğu görülür. G sonlu bir küme olduğundan, f_a aynı zamanda örten de olur. Şu halde $\forall a, b \in G$ için, $f_a(x) = a * x = b$ olacak şekilde bir $x \in G$ vardır.

Benzer şekilde, $\forall y \in G$ için $g_a(y) = y * a$ ile tanımlı, $g_a : G \longrightarrow G$ fonksiyonu da, sağdan kısaltma özelliği sebebi ile 1-1 ve dolayısı ile örten olur. Şu halde $\forall a, b \in G$ için, $g_a(y) = y * a = b$ olacak şekilde bir $y \in G$ vardır. Önceki önermeye göre $(G,*)$ bir grup olur.

Önerme 3.1.8 $(G_1,*)$ ve (G_2,o) iki grup olsun.

$\forall(a_1,b_1),(a_2,b_2) \in G_1 \times G_2$ için, $(a_1,b_1).(a_2,b_2) = (a_1 * a_2, b_1 o b_2)$ ile tanımlanan . işlemine göre, $G_1 \times G_2$ nin bir grup olduğunu gösteriniz. Bu gruba, G_1 ile G_2 nin **direkt çarpımı** denir.

İspat: $\forall(a_1,b_1),(a_2,b_2) \in G_1 \times G_2$ için $(a_1 * a_2, b_1 o b_2) \in G_1 \times G_2$ olduğundan, $G1$ (kapalılık) aksiyomu sağlanır.

$G2$: $\forall(a_1,b_1),(a_2,b_2),(a_3,b_3) \in G_1 \times G_2$ için;

$$\begin{aligned}[(a_1,b_1).(a_2,b_2)].(a_3,b_3) &= (a_1 * a_2, b_1 o b_2).(a_3,b_3) \\ &= ((a_2 * a_2) * a_3, (b_1 o b_2) o b_3),\end{aligned}$$

$$\begin{aligned}(a_1,b_1).[(a_2,b_2).(a_3,b_3)] &= (a_1,b_1).(a_2 * a_3, b_2 o b_3) \\ &= (a_1 * (a_2 * a_3), b_1 o (b_2 o b_3))\end{aligned}$$

bulunur. G_1 grubunda $*$ işleminin ve G_2 grubunda o işleminin birleşme özelliklerinden, . işleminin birleşme özelliği elde edilir.

$G3$: e_1 ve e_2, sırası ile G_1 ve G_2 gruplarının birim elemanları iseler, $(e_1,e_2) \in G_1 \times G_2$ de . işlemine göre birimdir. Gerçekten, $\forall(a,b) \in G_1 \times G_2$ için

$$(a,b).(e_1,e_2) = (a * e_1, b o e_2),$$

$$(e_1,e_2).(a,b) = (e_1 * a, e_2 o b)$$

bulunur. e_1 ile e_2 nin birim eleman olmalarından, istenen elde edilir.

3.1 ALIŞTIRMALAR

1-) $f_1(x) = x_1, f_2(x) = \frac{1}{x}, f_3(x) = -x$ ve $f_4(x) = -\frac{1}{x}$ ile tanımlı $f_i : \mathbb{R} \longrightarrow \mathbb{R}$ (i=1, 2, 3, 4) fonksiyonları için, $G = \{f_1, f_2, f_3, f_4\}$ kümesinin bileşke işlemi altında bir grup oluşturduğunu gösteriniz.

2-) $G = \{a \in \mathbb{R} : -1 < a < 1\}$ ve $\forall a,b \in G$ için $a * b = \frac{a+b}{1+ab}$ ile bir $*$ işlemi tanımlansın. $(G,*)$ ın bir değişmeli grup olduğunu gösteriniz.

3-) $G = \{2^n : n \in Z\}$ nin adi çarpma işlemine göre bir değişmeli grup olduğunu gösteriniz.

4-) Modülü 1 olan bütün kompleks sayıların çarpma işlemine göre bir değişmeli grup olduğunu gösteriniz.

5-) Her $a \in G$ için, $a^2 = e$ olan grubun değişmeli olduğunu gösteriniz.

6-) Her $a, b \in G$ için $(ab)^2 = a^2b^2$ olan grubun değişmeli olduğunu gösteriniz.

7-) $Z_2 \times Z_4$ direkt çarpımını bulunuz ve bu grupta her elemanın 4 katının sıfır olduğunu gösteriniz.

8-) Asal kalan sınıflar kümesi, Z_m^* in çarpımsal bir grup olduğunu gösteriniz.

9-) $G = \{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}\}$ kümesinin, çarpma işlemine göre bir grup olduğunu gösteriniz.

10-) $(G, *)$ bir grup ve $S \neq \emptyset$ bir küme olsun.

$$M(S,G) = \{f : S \longrightarrow G \quad \text{fonksiyon}\}$$

kümesi üzerinde,

$\forall f, g \in M(S,G)$ için, $x \in S$ olmak üzere, $(fog)(x) = f(x) * g(x)$ ile o işlemi tanımlanıyor. $(M(S,G), o)$ nun bir grup olduğunu gösteriniz.

11-) $m \times n$ reel matrislerin, toplama işlemine göre bir grup olduğunu gösteriniz.

12-) $n!$ mertebeden regüler matrislerin, çarpma işlemine göre bir grup olduğunu gösteriniz.

13-) $G = \{e, a\}$ bir grup ve e birim elemanı ise grubun işlem tablosunu yapınız ve grubun değişmeli olduğunu gösteriniz.

14-) $G = \{e, a, b\}$ bir grup ve e birim elemanı ise grubun işlem tablosunu yapınız ve grubun değişmeli olduğunu gösteriniz.

15-) 4 elemanlı bir grubun değişmeli olduğunu gösteriniz.

16-) Eleman sayısı çift olan bir grupta, tersi kendine eşit olan birimden farklı bir eleman daha bulunduğunu gösteriniz.

17-) Değişmeli iki grubun direkt çarpımının da değişmeli olduğunu gösteriniz.

3.2 ALT GRUPLAR

Tanım 3.2.1 G bir grup ve H, G nin boş olmayan bir alt kümesi olsun. Eğer H, G deki işleme göre kendi başına bir grup ise H ye, G nin bir **alt grubu** denir ve $H < G$ ile gösterilir.

$H < G$ ise G nin biriminin H de olacağı açıktır. e, G nin birimi ise G ve $\{e\}$, G nin her zaman alt gruplarıdırlar.

Tanım 3.2.1 Bir grubun, kendinden ve birimden farklı bir alt grubuna **öz alt grup** denir.

Şimdi, G nin boş olmayan bir alt kümesi verildiğinde ve zaman bir alt grup olacağını gösteren bir kriter gösterelim.

Önerme 3.2.1 G bir grup ve $\emptyset \neq H \subset G$ olsun. H nin bir alt grup olması için gerek ve yeter koşul

i) $\forall a, b \in H$ için, $ab \in H$ ve

ii) $\forall a \in H$ için, $a^{-1} \in H$ olmasıdır.

İspat: $\Longrightarrow$: $H < G$ olsun. H kendi başına bir grup olduğundan, grup aksiyomlarının hepsini sağlar. (i) ve (ii) koşulları, grup aksiyomlarından $G1$ ve $G4$ olduğundan, gereklilik ispatlanmış olur.

$\Longleftarrow$: Verilen H alt kümesi için (i) ve (ii) koşulları sağlansın. Şu halde grup aksiyomlarından, $G1$ ve $G4$ sağlanmış demektir. Şimdi diğer aksiyomlarında sağlandığını görelim. G deki tüm elemanlar için, birleşme özelliği sağlandığından, H alt kümesindeki elemanlar için de sağlanır. Şu halde H, $G2$ aksiyomunu da sağlar.

Bir $a \in H$ alalım. (ii) koşuluna göre $a^{-1} \in H$ ve $a, a^{-1} \in H$ olmasından, (i) koşuluna göre $aa^{-1} = e \in H$ olduğundan, $G3$ aksiyomu da sağlanır.

Yukarıdaki önermenin koşullarını birleştirerek, kriteri şöyle de ifade etmek mümkündür.

Önerme 3.2.2 G grubunun, boş olmayan bir alt kümesinin, alt grup olması için gerek ve yeter koşul $\forall a, b \in H$ için, $ab^{-1} \in H$ (veya $a^{-1}b \in H$) olmasıdır.

İspat: $\Longrightarrow$: $H < G$ ise $\forall b \in H$ için $b^{-1} \in H$ ve $\forall a, b \in H$ için $ab^{-1} \in H$ olacağı açıktır.

$\Longleftarrow$: $\forall a, b \in H$ için, $ab^{-1} \in H$ olsun. $H \neq \emptyset$ olduğundan, $\exists a \in H$ var ve $a = b$ için kabul edilen koşul gereğince $aa^{-1} = e \in H$ bulunur. $e, b \in H$ için koşulu yazarsak, $eb^{-1} = b^{-1} \in H$ olur. Şu halde önceki önermenin (ii) koşulu sağlanır.

$\forall a, b \in H$ için $b^{-1} \in H$ ve $(b^{-1})^{-1} = b$ göz önünde tutularak, $\forall a, b \in H$ için $a(b^{-1})^{-1} = ab \in H$ bulunur. Şu halde önceki önermenin (i) koşulu da sağlanır ve $H < G$ bulunur.

Eğer H alt kümesinin sonlu sayıda elemanı varsa alt grup olma kriteri daha da basitleşir.

Önerme 3.2.3 H, bir G grubunun boş olmayan sonlu bir alt kümesi ve G deki işleme göre kapalı ise $H < G$ dir.

İspat: Önerme 3.2.1 in (i) kapalılık koşulu sağlandığından, (ii) koşulunun sağlandığını da gösterirsek, ispat tamamlanmış olur.

Bir $a \in H$ alalım. Eğer $a = e$ ise $a^{-1} = e \in H$ dır. $a \neq e$ olsun. H da işlem kapalı olduğundan, a nın tüm pozitif kuvvetleri de H dadır. Fakat, H sonlu bir küme olduğundan; a, a^2, ..., a^m, ... elemanlarının hepsi farklı olamazlar. Şu halde, $r > s > 0$ tam sayılar için $a^r = a^s$ olur. Grupta kısaltma özelliği kullanılarak, $a^{r-s} = e$ ve $a \neq e$ kabul ettiğimizden, $r - s > 1$, yani $r - s - 1 > 0$ olup, $a^{r-s-1} = a^{-1} \in H$ bulunur.

Önerme 3.2.4 Bir grubun bir takım alt gruplarının ara kesiti de bir alt gruptur.

İspat: $\{H_i\}_{i \in I}$ ailesi, G grubunun bir takım alt grupları olsunlar. $H = \bigcap_{i \in I} H_i$ diyelim. Önerme 3.2.2 ye göre, $\forall a, b \in H$ için, $ab^{-1} \in H$ olduğunu gösterirsek, $H < G$ olduğu anlaşılır.

$$\begin{aligned} a, b \in H &\Longrightarrow \forall i \in I, \ a, b \in H_i \\ &\Longrightarrow \forall a \in I, \ ab^{-1} \in H_i \quad (H_i < G) \\ &\Longrightarrow ab^{-1} \in H = \bigcap_{i \in I} H_i \end{aligned}$$

gerektirmelerinden istenen elde edilir.

Tanım 3.2.3 G bir grup ve a, B iki alt kümesi olsunlar. $AB = \{ab : a \in A, b \in B\}$ ye A ile B kümelerinin **çarpımı** denir. Özel olarak, $A = \{a\}$ ise $\{a\}B = aB$ ile gösterilir. Benzer tanım, toplamsal grup için de yapılabilir.

Önerme 3.2.5 $H, K < G$ olsun. $HK < G \iff HK = KH$ olmasıdır.

İspat: $\Longrightarrow$: $HK < G$ olsun. $\forall h \in H, \forall k \in K$ için $h^{-1} \in H, k^{-1} \in K$ olduğu göz önünde tutularak $h^{-1}k^{-1} \in HK$ ve $kh = (h^{-1}k^{-1})^{-1} \in HK$ bulunur. Şu halde $KH \subset HK$ olur.

Tersine, $x \in HK$ alalım. HK alt grup olduğundan, $x^{-1} = hk \in HK$ dır. Şu halde $x = (hk)^{-1} = k^{-1}h^{-1} \in KH$, yani $HK \subset KH$ olur.

$\Longleftarrow$: $HK = KH$ olsun. $\forall x, y \in HK$ için, $x = h_1k_1$ ve $y = h_2k_2$ olacak şekilde $\exists h_1, h_2 \in H$ ve $\exists k_1, k_2 \in K$ vardır.

$$xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$$

dir. $k_1k_2^{-1} \in K$ ve $h_2^{-1} \in H$ olduğundan, $(k_1k_2^{-1})h_2^{-1} \in KH = HK$ ve $(k_1k_2^{-1})h_2^{-1} = hk$ olacak şekilde $\exists h \in H$ ile $\exists k \in K$ bulunabilir. Şu halde, $xy^{-1} = h_1(k_1k_2^{-1})h_2^{-1} = (h_1h)k \in HK$ elde edilir. Önerme 3.2.2 ye göre $HK < G$ bulunur.

3.2. ALIŞTIRMALAR

1-) $H = \{\begin{bmatrix} 1 & d \\ o & 1 \end{bmatrix} : d \in \mathbb{R}\}$ kümesinin, 2x2 regüler, reel matrislerin çarpımsal grubunun bir alt grubu olduğunu gösteriniz.

2-) A kümesinin kendi üzerine, 1-1 bütün fonksyonlar kümesi $S(A)$ nın bileşke işlemine göre oluşturduğu grup içinde, bir $a \in A$ elemanını sabit bırakan tüm fonksiyonların bir alt grup oluşturduğunu gösteriniz.

3-) $H_1 < G_1$ ve $H_2 < G_2$ ise $H_1 \times H_2 < G_1 \times G_2$ olduğunu gösteriniz.

4-) $\{2^n : n \in \mathbb{Z}\}$ kümesinin, reel sayıların çarpımsal grubunun bir alt grubu olduğunu gösteriniz.

5-) Tam sayıların toplamsal grubunun bütün alt gruplarını belirleyiniz.

6-) G grubunun tüm elemanları ile değişmeli olan elemanlarının bir alt grup oluşturduğunu gösteriniz.(**Merkez**)

3.3 DEVİRLİ ALT GRUPLAR

Tanım 3.3.1 M , bir G grubunun bir alt kümesi olsun. M yi kapsayan, G nin bütün alt gruplarının arakesitine M **nin ürettiği (doğurduğu) alt grup** denir ve $< M >$ ile gösterilir. M nin elemanlarına da $< M >$ grubunun **üreteçleri (doğurayları)** denir.

$K < G$ ve $M \subset H$ ise tanımdan $< M > \subset H$ olduğu hemen anlaşılır. Şu halde $< M >$, M alt kümesini kapsayan "en küçük" alt grup olarak da tanımlanabilir.

Önerme 3.3.1 $M \subset G$ olsun. M nin ürettiği alt grup;

$$< M >= \{a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} \ : \ a_i \in M,\ r \in \mathbb{N},\ n_i \in \mathcal{Z},\ i = 1, 2, \dots, r\}$$

dir.

İspat:

$$H = \{a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} \ : \ a_i \in M,\ r \in \mathbb{N},\ n_i \in \mathcal{Z},\ i = 1, 2, \dots, r\}$$

kümesinin G nin bir alt grubu olduğunu gösterelim.

$$a = a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} \quad ve \quad b = b_1^{m_1} b_2^{m_2} \dots b_s^{m_s}$$

olmak üzere, $a, b \in H$ için,

$$ab^{-1} = a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} b_s^{-m_s} \dots b_2^{-m_2} b_1^{-m_1} \in H$$

olduğundan, $H < G$ dir.

$m \in M$ alalım. m yi kendinin bir kuvvet çarpımı olarak düşünerek, yani H nın tanımında, $r = 1$ ve $n_1 = 1$ alarak $m \in H$ bulunur. Şu halde $M \subset H$ dır. $H < G$ olduğundan, $< M > \subset H$ elde edilir.

Tersine olarak, $H \subset < M >$ kapsamasını gösterelim. $a = a_1^{n_1} a_2^{n_2} \ldots a_{n_r}^{n_r} \in H$ alalım. $a_1, a_2, \ldots, a_r \in M \subset < M >$ ve $< M >$ bir grup olduğundan, bu elemanların kuvvetleri ve bunların çarpımları da $< M >$ de kalır. Şu halde $a = a_1^{n_1} a_2^{n_2} \ldots a_r^{n_r} \in < M >$, yani $H \subset < M >$ elde edilir. Her iki kapsamadan da eşitlik bulunur.

Tanım 3.3.2 Bir G grubu için, $G =< M >$ olacak şekilde bir $M \subset G$ alt kümesi bulunabiliyorsa, G ye M ile **üretilmiş grup** denir. Eğer M sonlu bir küme ise G ye **sonlu üretilmiş grup** ve $M = \{a\}$ tek elemanlı bir küme ise G ye a ile üretilmiş **devirli grup** denir ve $G =< a >$ yazılır.

Önerme 3.3.1 e göre, çarpımsal grup için, $< a >= \{a^n : n \in \mathcal{Z}\}$ dir. G toplamsal grup olarak alınırsa, a nın ürettiği devirli grup $< a >= \{na : n \in \mathcal{Z}\}$ dır.

Örnek 1: $\mathcal{Z}$, 1 ile üretilmiş sonsuz bir devirli gruptur.

Örnek 2: $G = \{1, i, -1, -i\}$ grubu i ile üretilmiş 4.mertebeden bir (sonlu) devirli gruptur.

Örnek 3: $\mathcal{Z}_m$, $\bar{1}$ ile üretilmiş m. mertebeden bir devirli gruptur.

$G =< a >$ olsun. a nın bütün pozitif kuvvetlerini aldığımızda, iki hal söz konusudur.

1) a nın bütün kuvvetleri birbirinden farklıdır. Bu durumda, G sonsuz devirli grup olur.

2) a nın bazı kuvvetleri aynıdır. Eğer $r > s$ tam sayıları için $a^r = a^s$ ise kısaltma özelliği kullanılarak, $a^{r-s} = e$ bulunur. Pozitif tam sayıların iyi sıralı oluşundan, $a^m = e$ olan en küçük bir pozitif tam sayı bulunabilir. Bu en küçük pozitif tam sayı t ise

$$G = \{a, a^2, \ldots a^t = e\}$$

olur. Gerçekten, $n \in \mathcal{Z}$ olmak üzere $a^n \in G =< a >$ alalım. n yi t ile kalanlı bölerek, $n = qk + r, 0 \leq r < t, \exists q, r \in \mathcal{Z}$ şeklinde yazalım.

$$a^n = a^{qt} a^r = (a^t)^q a^r = e a^r = a^r$$

olduğundan, $a^n \in \{a, a^2, \ldots a^t = e\}$ yani $G \subset \{a, a^2, \ldots a^t = e\}$ bulunur. $a \in G$ olduğundan ters kapsama da doğrudur.

Önerme 3.3.2 Devirli bir grubun her alt grubu da devirlidir.

İspat: $G =< a >$ ve $H < G$ olsun. Eğer $H = \{e\}$ ise H nın e ile üretilen bir devirli grup olduğu açıktır.

$H \neq \{e\}$ ve $n \neq 0$ tam sayısı için, $a^n \in H$ olsun. $H < G$ olduğundan, $(a^n)^{-1} = a^{-n} \in H$ dır. Şu halde genelliği bozmadan, $n > 0$ olmak üzere $a^n \in H$ kabul edebiliriz. Pozitif tam sayıların iyi sıralı oluşundan, $a^s \in H$ olacak şekilde en küçük pozitif tam sayı s olsun. Bu durumda $H =< a^s >$ olacağını gösterelim. İlk önce $a^s \in H$ ve $H < G$ olduğundan, $< a^s > \subset H$ dır.

Tersine, bir $a^n \in H$ alalım. y yi n ile kalanlı bölerek, $n = qs + r$, $0 \leq r < s$, $\exists q, r \in \mathcal{Z}$ şeklinde yazalım. Buradan,

$$a^n = (a^s)^q a^r \Longrightarrow a^r = a^n (a^s)^{-q} \in H$$

bulunur. Fakat $0 < r < s$ ve $a^r \in H$ olması s nin seçimi ile gelişir. Şu halde $r = 0, n = qs$ olmalıdır. Buradan $a^n = (a^s)^q \in < a^s >$, yani $H \subset < a^s >$ bulunur. Her iki kapsamadan istenen eşitlik elde edilir.

Önerme 3.3.3 (i) $< a >$ bir sonsuz devirli grup ise alt grubu da bir sonsuz devirli gruptur.

(ii) $< a >, t.$ meretebeden bir devirli grup ise her alt grubunun mertebesi t yi böler ve t nin her pozitif q böleni için mertebesi q olan bir ve yalnız bir tane alt grubu vardır. Eğer $t = sq$ ise bu alt grup, $< a^s >$ dir.

İspat: (i) Önceki önermeye göre devirli bir grubun her alt grubu da devirlidir. Şimdi sonsuz bir devirli grubun her alt grubunun da sonsuz olacağını gösterelim. $H < < a >$ olsun. Önceki önermenin ispatında, $a^s \in H$ olan en küçük pozitif tam sayı s ise $H =< a^s >$ olduğunu göstermiştik $< a >$ sonsuz bir devirli grup olduğundan, a nın bütün kuvvetleri, dolayısı ile a^s nin bütün kuvvetleri birbirinden farklıdır. Şu halde $H =< a^s >$ de bir sonsuz devirli grup olur.

(ii) $< a >= \{a, a^2 \ldots a^t = e\}$, $t.$ mertebeden bir devirli grup ve H bir alt grubu olsun. $a^s \in H$ koşulunu sağlayan en küçük pozitif tam

sayı s ise, Önerme 3.3.2 ye göre $H =< a^s >$ dir. Şimdi $s|t$ olduğunu gösterelim. t yi s ile kalanlı olarak bölelim. $t = ks + r$, $0 \leq r < s$ olacak şekilde $\exists r \in \mathcal{Z}$ bulunabilir.

$$e = a^t = (a^s)^k.a^r \Longrightarrow a^r = (a^s)^{-k} \in H$$

dir. $0 < r < s$ ise $a^r \in H$ olması s nin yukarıdaki seçimi ile çelişir. Şu halde $r = 0$, yani $s|t$ olmalıdır. Eğer $t = sq$ $(q \in \mathcal{Z})$ ise $H =< a^s >$ nin mertebesi $q = \frac{t}{s}$ olur, çünkü $t = sq$ sayısı $a^t = e$ eşitliğini sağlayan en küçük pozitif tam sayı olduğundan, $(a^s)^q = e$ eşitliğini sağlayan en küçük pozitif tam sayı da q olur. Şu halde H alt grubunun mertebesi q olup, $q|t$ dir.

Şimdi t nin her q bölenine karşılık bir ve yalnız bir tane alt grup olacağını gösterelim.

$q|t$ ise $t = qs$ olacak şekilde s tam sayısı teklikle belirlidir. Yukarıda gösterildiği gibi $< a^s >$ alt grubunun mertebesi de q olur ve q. mertebeden alt grup da tektir. Çünkü q. mertebeden bir alt grup, $t = qs$ olmak üzere $< a^s >$ dir.

Tanım 3.3.3 G bir grup ve $a \in G$ olsun. a nın ürettiği $< a >$ devirli grubunun mertebesine a elemanının **mertebesi** denir ve $o(a)$ ile gösterilir.

Şu halde $o(a)$, $a^n = e$ koşulunu sağlayan $n > 0$ tam sayıları arasında en küçük olanıdır.

Önerme 3.3.4 G bir grup, $a \in G$ ve $o(a) = n$ olsun.

$$a^m = e \Longleftrightarrow n|m$$

dir.

İspat: $\Longrightarrow$: $a^m = e$ olsun. m yi n ile kalanlı bölerek, $m = kn + r$ ve $0 \leq r < n$ olacak şekilde $k, r \in \mathcal{Z}$ bulunabilir. $o(a) = n$ olduğundan, $a^n = e$ ve $e = a^m = (a^n)^k.a^r = a^r$ bulunur. Fakat, $0 < r < n$ ise $a^r = e$ olması n nin bu koşulu sağlayan en küçük pozitif tam sayı olması ile çelişir. Şu halde $r = 0$, yani $n|m$ olmalıdır.

$\Longleftarrow$: $n|m$ olsun. $m = nk$, $k \in \mathcal{Z}$ ise $a^m = (a^n)^k = e^k = e$ olur.

Önerme 3.3.5 $G =< a >, n$. mertebeden bir devirli grup olsun. a^s nin G nin bir üreteci olması için gerek ve yeter koşul $(s,n) = 1$ olmasıdır.

İspat: $\Longrightarrow$: a^s, G nin bir üreteci ise $G =< a >=< a^s >$ dir. $a \in < a^s > \Longrightarrow a = (a^s)^t, \exists t \in \mathbb{N}$ olur. Kısaltma özelliği kullanılarak, $a^{st-1} = e$ ve bir önceki önermeye göre, $n|st - 1$ bulunur. Şu halde $\exists y \in \mathcal{Z}$ için, $st - 1 = ny$ veya $st - ny = 1$ olacağından, $(s,n) = 1$ elde edilir.

$\Longleftarrow$: $(s,n) = 1$ olsun. $\exists x, y \in \mathcal{Z}$ için, $xs + yn = 1$ ve

$$a = (a^s)^x.(a^n)^y = a^{sx}.e = (a^s)^x$$

dir. Şu halde, $a \in < a^s >$ olacağından, $G =< a > \subset < a^s >$ dir. $a^s \in < a >$ olduğundan, $< a^s > \subset < a >= G$ olduğu da açıktır. Her iki kapsamadan istenen eşitlik elde edilir.

Önerme 3.3.6 $G =< a >$ bir sonsuz devirli grup ise üreteçleri a ve a^{-1} dir.

İspat: a^s, $G =< a >$ nın bir üreteci ise $(a^s)^x = a$ olacak şekilde $\exists x \in \mathcal{Z}$ bulunabilirdi. Buradan da $< a >$ nın sonsuz devirli grup olması nedeni ile $sx = 1$, yani $s = \mp 1$ bulunurdu.

Bir A kümesinin kendi üzerine 1-1 bütün fonksiyonları kümesi $S(A)$ nın bileşke işlemi altında bir grup oluşturduğunu biliyoruz. $S(A)$ nın bir alt grubuna bir **dönüşüm grubu** denir. Özel olarak, düzgün bir n-gen düşünelim ve köşelerini $A_1, A_2, A_3, ...A_n$ ile gösterelim. Bu düzgün n-genin, uzunluğu koruyan ve köşelerini birbirine dönüştüren bir fonksiyona *izometri* veya *simetri* denir. Şu halde f bir simetri ise $|A_1 - A_2| = |f(A_1) - f(A_2)|$ olacağından, A_1 ve A_2 komşu köşeler ise $f(A_1)$ ve $f(A_2)$ de komşudurlar. Düzgün n-genin 2n simetrisi var ve bunlar bileşke işlemi altında bir grup oluştururlar. Bu gruba **Dihedral** grup denir ve D_n ile gösterilir.

Örnek 4: Eşkenar üçgenin simetri grubunu bulalım. Bu grup 6 elemanlı olup, eşkenar üçgenin merkezi etrafında $0, \frac{2\pi}{3}, \frac{4\pi}{3}$ derecelik dönmeleri ile kenar orta dikmelerine göre simetrilerden oluşur. Bu dönüşümler sırası ile

$$I=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, D=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, D^2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$

$$T_1=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, T_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, T_3=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

dirler. Şu halde eşkenar üçgenin simetri grubunun işlem tablosu aşağıdaki gibidir.

o	I	D	D^2	T_1	T_2	T_3
I	I	D	D^2	T_1	T_2	T_3
D	D	D^2	D^3	T_2	T_3	T_1
D^2	D^2	I	D	T_3	T_1	T_2
T_1	T_1	T_3	T_2	I	D^2	D
T_2	T_2	T_1	T_3	D	I	D^2
T_3	T_3	T_2	T_1	D^2	D	I

$T_1D=T_3$, $T_1D^2=T_2$ olduğu göz önüne alınarak;

$$D_3=\{I,\ D,\ D^2,\ T_1,\ T_1D,\ T_1D^2\}$$

yazılabilir. Burada $D^3=T_1^2=I$ ve $DT_1=T_1D^2$ eşitlikleri sağlanır. Şu halde eşkenar üçgenin simetri grubu, yukarıdaki eşitlikleri sağlayan D ve T_1 dönüşümleri ile üretilmiştir. Genel olarak, D_n dihedral grubu, aralarında belli bir bağıntı sağlayan iki üreteçli bir gruptur.

Örnek 5: $D_n=<x,y\ :\ x^n=y^2=e$ ve $xy=yx^{n-1}>$ ise

$$D_n=\{e,x,x^2,\ldots,x^{n-1},y,yx,yx^2,\ldots,yx^{x-1}\}$$

dir. Gerçekten,

$$xy=yx^{n-1}\Longrightarrow x^2y=x(xy)=(xy)x^{n-1}=yx^{2(n-1)}$$

olduğu düşünülerek, $\forall i=1,2,\ldots,n-1$ için $x^iy=yx^{i(n-1)}$ bulunur. $x^n=e$ olduğundan, $i(n-1)\equiv j(mod\ n)$, $(0\leq j\leq n-1)$ ise $x^iy=yx^j$ bulunur. x ile y nin ürettiği grup, bu iki elemanın değişik sırada bütün kuvvetlerinin çarpımı olacağından istenen elde edilir.

3.3 ALIŞTIRMALAR

1-) Devirli bir grubun değişmeli olduğunu gösteriniz.

2-) $\mathcal{Z}$ de 5 in ürettiği devirli alt grubu bulunuz.

3-) $\mathcal{Q} - \{0\}$kümesinin çarpma işlemine göre bir devirli grup olup olmadığını araştırınız. $\frac{1}{5}$ in ürettiği alt grubu bulunuz.

4-) $(\mathcal{Q}, +)$ nın bir devirli grup olup olmadığını araştırınız. $\frac{1}{5}$ in ürettiği alt grubu bulunuz.

5-) $\mathcal{Z}_{10}^*$ ın bir devirli grup olduğunu gösteriniz.

6-) $\mathcal{Z}_{15}^*$ ın bir devirli grup olmadığını gösteriniz.

7-) p asal ise $\mathcal{Z}_{p^2}$ nin bir devirli grup olduğunu gösteriniz ve üreteçlerini bulunuz.

8-) $\mathcal{Z}_2 \times \mathcal{Z}_8$ direkt çarpımının bir devirli grup olmadığını gösteriniz.

9-) G değişmeli bir grup ise G nin sonlu mertebeden bütün elemanlarının bir grup oluşturduğunu gösteriniz. Bu gruba G nin "burulma (torsion)" alt grubu denir.

10-) G sonlu bir grupsa her $a \in G$ için $a^n = e$ olacak şekilde bir n tam sayısının varlığını gösteriniz.

11-) Bir G grubunun, elemanlarının mertebelerinin en küçük üst sınırına grubun **üssü** denir. G grubu üssü g olan bir çarpımsal değişmeli grup ise $\forall a \in G$ için $o(a)|g$ olduğunu gösteriniz.

12-) p asal tam sayı ise $\mathcal{Z}_p^*$ ın devirli grup olduğunu gösteriniz.

13-) G bir grup ve $a \in G$ ise $o(a) = o(a^{-1})$ olduğunu gösteriniz.

14-) G bir grup ve $a, b \in G$ ise $o(a) = o(bab^{-1})$ olduğunu gösteriniz.

15-) G bir grup ve $a, b \in G$ olsun. $o(a) = n$ ise $a^r = a^s$ olması için gerek ve yeter koşul $r \equiv s(mod\ n)$ olmasıdır, gösteriniz.

16-) G değişmeli bir grup ve $a, b \in G$ olsun. $o(a) = m$, $o(b) = n$ ve $(m, n) = 1$ ise $o(ab) = mn$ olduğunu gösteriniz.

17-) G bir grup, $a \in G$ ve $o(a) = n$ olsun. $o(a^m) = \frac{n}{(m,n)}$ olduğunu gösteriniz.

18-) $G =< a >$, 20. mertebeden bir devirli grup ise bütün üreteçlerini ve alt gruplarını bulunuz.

19-) 20. mertebeden bir devirli grubun mertebesi 5 olan kaç elemanı vardır?

20-) a ve b bir G grubunun mertebesi sonlu iki elemanı ise ab nin mertebesinin sonlu olmayabileceğini bir örnekle gösteriniz.

21-) $G =< a >$, mn. mertebeden bir devirli grup olsun. a^n nin mertebesinin m olduğunu gösteriniz.

22-) G bir grup ve $a, b \in G$ olsun. $o(a) = 5, aba^{-1} = b^2$ ise $o(b)$ yi bulunuz.

23-) G bir grup, H ve K da iki alt grup olsunlar. $HK < G$ ise HK nın $H \cup K$ ile üretilen alt grup olduğunu gösteriniz.

24-) $G =< a >$, n. mertebeden bir devirli grup ve $m|n$ ise $x^m = e$ denklemini sağlayan $x \in G$ lerin sayısının tam m tane olduğunu gösteriniz.

25-) $G =< a >$, n. mertebeden bir devirli grup ve $(m, n) = d$ ise $x^m = e$ denklemini sağlayan $x \in G$ lerin sayısının tam d tane olduğunu gösteriniz.

26-) $x^{13} \equiv 1(mod\ 29)$ kongrüansının tek çözümünün $x \equiv 1(mod\ 29)$ olduğunu gösteriniz.

27-) p asal tam sayı ve $d|p-1$ ise $x^d \equiv 1(mod\ p)$ kongrüansının $\mathcal{Z}_p$ de tam d çözümü olduğunu gösteriniz.

28-) $\mathcal{Z}_p^*$ ın üreteçlerinin sayısını bulunuz.

29-) p asal tam sayı olsun. $x^2 \equiv -1(mod\ p)$ kongrüansının, $p = 2$ veya $p \equiv 1(mod\ 4)$ ise çözümünün varlığını, eğer $p \equiv 3(mod\ 4)$ ise çözümünün olmadığını gösteriniz.

30-) Karenin simetri grubunu bulunuz. Dönmelerin bir devirli alt grup oluşturduğunu gösteriniz.

31-) Karenin simetriler grubunun üreteçlerini bulunuz.

3.4 NORMAL ALT GRUPLAR

Gruplar teorisinde normal alt gruplar önemli bir rol oynarlar.

Tanım 3.4.1 G bir grup ve $H < G$ olsun. G de $\equiv$ bağıntısını,

$$a \equiv b \ (mod\ H) \iff ab^{-1} \in H$$

ile tanımlayalım.

Önerme 3.4.1 $H < G$ alt grubuna göre yukarıda tanımlanan $\equiv$ bağıntısı bir denklik bağıntısıdır.

İspat: (i) Yansıma : $\forall a \in G$ için, $aa^{-1} = e \in H$ olduğundan, $a \equiv a(mod\ H)$ dır.

(ii) Simetri: $a, b \in G$ için, $a \equiv b(mod\ H)$ ise tanıma göre $ab^{-1} \in H$ ve $H < G$ olduğundan, $(ab^{-1})^{-1} = ba^{-1} \in H$ olur. Şu halde, $b \equiv a\ (mod\ H)$ dır.

(iii) Geçişme: $a, b, c \in G$ için, $a \equiv b(modH)$ ve $b \equiv c(mod\ H)$ ise tanıma göre $ab^{-1} \in H$ ve $bc^{-1} \in H$ olduğundan, $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$ olur. Şu halde, $a \equiv c(mod\ H)$ dır.

Önerme 3.4.2 Yukarıdaki denklik bağıntısına göre $a \in G$ elemanının sınıfı $\bar{a} = Ha = \{ha : h \in H\}$ alt kümesidir. Ha ya H alt grubuna göre a nın sağ denklik sınıfı denir.

İspat: Denklik sınıfı tanımına göre, $\bar{a} = \{b \in G : b \equiv a(mod\ H)\}$ dır. $b \equiv a(mod\ H) \iff ba^{-1} \in H \iff b \in Ha$ denkliklerinden $\bar{a} = Ha$ bulunur.

Benzer şekilde sol denklik sınıfları da tanımlanabilir.

Önerme 3.4.3 G bir grup ve $H < G$ olsun.

$$a \equiv b(mod\ H) \iff a^{-1}b \in H$$

ile tanımlı $\equiv$ bağıntısı G de bir denklik bağıntısıdır. Bu denklik bağıntısına göre, $a \in G$ elemanının sınıfı $aH = \{ah : h \in H\}$ alt kümesidir. aH ya H alt grubuna göre a nın sol denklik sınıfı denir.

Lagrange Teoremi 3.4.1 Sonlu bir grubun her alt grubunun mertebesi grubun mertebesini böler.

İspat: G sonlu bir grup, $o(G) = n$ olsun. $H < G$ ve $o(H) = m$ diyelim. Önce bütün sol denklik sınıflarında aynı sayıda eleman bulunduğunu gösterelim.

$a, b \in G$ olmak üzere, herhengi iki aH ve bH sol denklik sınıfı alalım. $f(ah) = bh$ ile tanımlanan, $f : aH \longrightarrow bH$ fonksiyonunun örten olduğu kolayca görülür.

$$f(ah) = f(ah') \Longrightarrow bh = bh' \Longrightarrow h = h'$$

den f nin 1-1 olduğu da görülür.

G sonlu olduğundan, sol denklik sınıflarının sayısı da sonlu olur. Sol denklik sınıflarının sayısı r olsun. $eH = H$ olduğundan, H alt grubunu da bir sol denklik sınıf olarak düşünebiliriz. Şu halde bütün sol denklik sınıflarında da $o(H) = m$ eleman olur.

Denklik sınıfları G nin bir ayrışımını belirttiğinden, $o(G) = m.r$, yani $m = o(H) | o(G) = n$ elde edilir.

Sonuç 1: $H < G$ alt grubuna göre sağ ve sol denklik sınıflarının sayısı aynıdır. Bu sayıya H alt grubunun G içindeki indeksi denir ve $(G : H)$ ile gösterilir.

İspat: Teoremin ispatında olduğu gibi, H ye göre sağ denklik sınıflarında aynı sayıda eleman olduğu ve $He = H$ nın da bir sağ denklik sınıfı olduğu göz önüne alınarak, sağ denklik sınıfları sayısının da $\frac{o(G)}{o(H)}$ olduğu görülür. Şu halde;

$$(G : H) = \frac{o(G)}{o(H)}.$$

Sonuç 2: $o(G) = n$ ise $\forall a \in G$ için, $a^n = e$ dir. Şu halde $o(a) | o(G) = n$ dir.

İspat: $H =< a >< G$ alalım. Lagrange teoremine göre, $m = o(H) = o(a)|o(G) = n$ dir. $n = mt, (t \in Z)$ ise $a^n = (a^m)^t = e$ bulunur.

Sonuç 3: (Euler Teoremi) $\forall a \in \mathcal{Z}, (a, m) = 1$ için,

$$a^{\phi(m)} \equiv 1(mod\ m)$$

dir.

İspat: Z_m^* asal kalan sınıflar kümesi, $\phi(m)$ elemanlı bir grup olduğundan, Sonuç 2' ye göre $\forall \bar{a} \in Z_m^*$ için, $\bar{a}^{\phi(m)} = \bar{1}$ yani,

$$a^{\phi(m)} \equiv 1(mod\ m)$$

bulunur.

Teorem 3.4.2 $N < G$ olsun. Aşağıdaki ifadeler birbirine denktir.

(i) $\forall a \in G, \forall x \in N$ için $axa^{-1} \in N$ dir.
(ii) $\forall a \in G$ için $aNa^{-1} \subset N$ dir.
(iii) $\forall a \in G$ için $aNa^{-1} = N$ dir.
(iv) $\forall a \in G$ için $aN = Na$ dır.

İspat: $(i) \Longrightarrow (ii) : aNa^{-1} = \{axa^{-1} : x \in N\}$ olduğundan, (i) ye göre $\forall a \in G, \forall x \in N$ için $axa^{-1} \in N$ olur. Şu halde $aNa^{-1} \subset N$ dir.

(ii) $\Longrightarrow$(iii) : $\forall a \in G$ için $aNa^{-1} \subset N$ olsun. $a^{-1} \in G$ için de $a^{-1}Na \subset N \Longrightarrow N \subset aNa^{-1}$ olacağından, $aNa^{-1} = N$ elde edilir.

(iii) $\Longrightarrow$ (iv) : $\forall a \in G$ için $aNa^{-1} = N$ ise $aN = Na$ olacağı açıktır.

(iv) $\Longrightarrow$ (i) : $\forall a \in G$ için $aN = Na$ olsun. Şu halde $\forall a \in G$ için, $aNa^{-1} = N$ yani $\forall x \in N$ için de $axa^{-1} \in N$ bulunur.

Tanım 3.4.2 Teoremin denk koşullarından birini sağlayan G nin bir N alt grubuna **normal alt grup** denir ve $N \triangleleft G$ ile gösterilir.

Not: G değişmeli bir grup ise her alt grup normaldir.
Şu halde $N \triangleleft G$ ise N ye göre tanımlanan sağ ve sol denklik sınıfları aynıdır.

Tanım 3.4.3 $N \triangleleft G$ olsun. G nin N ye göre sağ (veya sol) denklik sınıfları kümesi G/N ile gösterilir.

Önerme 3.4.4 $N \triangleleft G$ ise G/N de çarpma işlemini $\forall aN, bN \in G/N$ için,

$$(aN).(bN) = (ab)N$$

ile tanımlayalım. Bu çarpım, kalan sınıflarından alınan a, b temsilcilerinden bağımsızdır.

İspat: $N \triangleleft G$ olduğundan, $\forall a \in G$ için $aN = Na$ dır. $(aN).(bN)$ nin herhangi bir elemanı, $x_1, x_2 \in N$ olmak üzere $(ax_1).(bx_2) = a(x_1b)x_2$ şeklindedir. $x_1b \in Nb = bN$ olduğundan, $x_1b = bx$ olacak şekilde $\exists x \in N$ bulunabilir. Şu halde

$$(ax_1)(bx_2) = a(x_1b)x_2 = a(bx)x_2 = (ab)xx_2 \in (ab)N$$

bulunur. Buradan $(aN).(bN) \subset (ab)N$ elde edilir.

Ters kapsamayı göstermek için, herhangi bir $(ab)x \in (ab)N, (x \in N)$ alalım. $\forall y \in N$ için,

$$(ab)x = a(yy^{-1})bx = (ay)(y^{-1}b)xvey^{-1}b \in Nb = bN$$

olduğundan, $y^{-1}b = bx_1, (x_1 \in N)$ yazarsak

$$(ab)x = (ay)(bx_1)x = (ay)(bx_1x) \in (aN).(bN)$$

yani, $(ab)N \subset (aN).(bN)$ kapsaması elde edilir. Her iki kapsamadan istenen eşitlik elde edilir.

Şimdi de sol denklik sınıfları çarpımının temsilciye bağlı olmadığını gösterelim.

$$\begin{aligned} aN = a_1N \ \ ve \ \ bN = b_1N &\Longrightarrow a_1^{-1}a = x \in N \ \ ve \ \ b_1^{-1}b = x_1 \in N \\ &\Longrightarrow a = a_1x \ \ ve \ \ b = b_1x_1 \\ &\Longrightarrow ab = (a_1x)(b_1x_1) = a_1(xb_1)x_1 \end{aligned}$$

bulunur. $N \triangleleft G$ olduğundan, $xb_1 \in Nb_1 = b_1N \Longrightarrow xb_1 = b_1x_2$, $\exists x_2 \in N$ olur. Şu halde, $ab = a_1(b_1x_2)x_1 = (a_1b_1)x_2x_1 \in (a_1b_1)N$ olduğundan $(ab)N = (a_1b_1)N$ elde edilir.

Teorem 3.4.3 $N \triangleleft G$ ise G/N bir gruptur.

İspat: Önceki önermede $\forall aN,\ bN \in G/N$ için $(aN).(bN) = (ab)N \in G/N$ olduğunu gördük. Şu halde $G1$ aksiyomu sağlanır. $G2$ birleşme aksiyomunun sağladığını göstermeyi okuyucuya bırakıyoruz.

$G3$: $\forall aN \in G/N$ için, $(aN).(eN) = (ae)N = aN$ olduğundan $eN = N$ birimdir.

$G4$: $\forall aN \in G/N$ için $(aN).(a^{-1}N) = eN = N$ olduğundan, $(aN)^{-1} = a^{-1}N$ bulunur. Şu halde G/N bir gruptur.

Tanım 3.4.4 $N \triangleleft G$ ise G/N grubuna, G nin N ye göre bölüm grubu denir.

Teorem 3.4.4 G sonlu bir grup ve $N \triangleleft G$ ise G/N de sonlu bir grup ve

$$o(G/N) = \frac{o(G)}{o(N)}$$

dir.

İspat: G sonlu bir grup ise N ye göre sol (veya sağ) denklik sınıfları sayısı da sonlu ve Lagrange Teoreminin 1. Sonucuna göre;

$$o(G/N) = \frac{o(G)}{o(N)}$$

olur.

Not: G toplamsal bir grup ise değişmeli olacağından her alt grubu normal olur. Şu halde her alt grubuna göre bölüm grubu tanımlanabilir. $N < G$ ve $a \in G$ ise a nın denklik sınıfı $a + N = \{a + x : x \in N\}$ dir.

Örnek 1: $N =< 4 >= 4\mathcal{Z}$ alt grubuna göre $\mathcal{Z}/N$ bölüm grubu $\{N, 1 + N, 2 + N, 3 + N\}$ dir. Çünkü herhangi bir $n \in Z$ alındığında, $n = 4q + r$, $0 \leq r < 4$ olacak şekilde $\exists q, r \in \mathcal{Z}$ bulunabilir. Böylece n tam sayısı bu 4 sınıftan birine ait olur. Şu halde $\mathcal{Z}/N = \mathcal{Z}_4$ dür.

Teorem 3.4.5 Bir grubun indeksi 2 olan bir alt grubu normaldir.

İspat: $N < G$ ve $(G : N) = 2$ olsun. Bu takdirde iki sağ ve sol denklik sınıfları vardır. N hem sağ hem de sol denklik sınıfı olarak düşünülebilir. $a \notin N$ ise sağ denklik sınıfları N, aN ve sol denklik sınıfları N, Na olur. Ayrık birleşim olarak $G = N \cup aN = N \cup Na$ olmasından, $aN = Na = G - N$ olacağından sol ve sağ denklik sınıflarının aynı olduğu görülür. Şu halde $N \triangleleft G$ dir.

Teorem 3.4.6 $N \triangleleft G$ ve $N < K < G$ ise $N \triangleleft K$ ve $K/N < G/N$ dir. Eğer ayrıca $N < K \triangleleft G$ ise $K/N \triangleleft G/N$ dir. Tersine G/N nin alt grupları $N < K < G$ olmak üzezr K/N şeklinde ve normal alt grupları da $N < K \triangleleft G$ olmak üzere K/N şeklindedir.

İspat: $N \triangleleft G$ ve $N < K < G$ olsun. $N \triangleleft K$ olacağı açıktır. $\forall k \in K$ için $kN \in K/N$ sınıfı, $k \in G$ olarak düşünülebileceğinden G/N nin de bir elelmanı olur. Şu halde $K/N < G/N$ dir. Eğer $K \triangleleft G$ ise $\forall g \in G, \forall k \in K$ için $gkg^{-1} \in K$ olur. $\forall gN \in G/N$ için,

$$(gN)(kN)(gN)^{-1} = (gkg^{-1})N \in K/N$$

olacağından, $K/N \triangleleft G/N$ bulunur.

Tersine, $\bar{K} < G/N$ alalım. $K = \{g \in G : gN \in \bar{K}\}$ diyelim. $\forall k_1, k_2 \in K$ için $k_1, N, k_2, N \in \bar{K}$ ve $\bar{K} < G/N$ olduğundan,

$$(k_1N)(k_2N)^{-1} = k_1k_2^{-1}N \in \bar{K}$$

ve K nın tanımından, $k_1, k_2^{-1} \in K$ bulunur. Şu halde $K < G$ dir. $\forall x \in N$ için $xN = N$ ve N, G/N nin birimi olduğundan $\bar{K}$ dedir. Buradan $N < K$ bulunur. Eğer $\bar{K} \triangleleft G/N$ ise $K \triangleleft G$ dir. Çünkü $\forall g \in G$ ve $\forall k \in K$ için,

$$(gkg^{-1})N = (gN)(kN)(gN)^{-1} \in \bar{K}$$

dir.

Tanım 3.4.5 G bir grup ve $a, b \in G$ olsun. $aba^{-1}b^{-1}$ elemanına a ve b nin komütatörü denir ve $[a, b]$ ile gösterilir.

$ab = [a, b]ba$ olduğundan, $[a, b]$ ye ab ile ba nın değişme ölçüsü olarak bakılabilir.

Önerme 3.4.5 G grubunun değişmeli olması için gerek ve yeter koşul $\forall a, b \in G$ için, $[a, b] = e$ olmasıdır.

İspat : $\Longrightarrow$: G değişmeli bir grup ise $\forall a, b \in G$ için, $ab = ba$ ve $[a, b] = aba^{-1}b^{-1} = e$ dir.

$\Longleftarrow$: $\forall a, b \in G$ için $[a, b] = aba^{-1}b^{-1} = e$ ise $ab = ba$ olacağı açıktır.

Tanım 3.4.6 Bir grubun bütün komütatörlerinin ürettiği alt gruba **komütatör alt grup** denir ve $[G,\ G]$ ile gösterilir.

$$[G,\ G] = \{c_1c_2 \ldots c_m \ :\ c_i \text{ komütatör},\ i = 1, 2, ., m,\ \ m \in \mathbb{N}\}$$

dir.

Önerme 3.4.6 $[G,\ G]$, G nin bir normal alt grubudur.

İspat : $\forall c \in [G,\ G]$ ve $\forall a \in G$ için, $aca^{-1} = aca^{-1}c^{-1}c = [a, c]c$ dir. $[a, c]$ ve c iki komütatör olduğundan, çarpımları $[G,\ G]$ komütatatör alt grubunda olur. Şu halde $[G,\ G] \lhd G$ dir.

Teorem 3.4.7 G bir grup ve $N \lhd G$ olsun. G/N bölüm grubunun değişmeli olması için gerek ve yeter koşul $[G,\ G] \subset N$ olmasıdır.

İspat: Önerme 3.4.5 e göre bir grubun değişmeli olması için gerek ve yeter koşul tüm komütatörlerinin birim olmasıdır. Şu halde G/N nin değişmeli olması için gerek ve yeter koşul $\forall aN, bN \in G/N$ için,

$$\begin{aligned} N = [aN,\ bN] &= (aN)(bN)(aN)^{-1})(bN)^{-1} \\ &= (aba^{-1}b^{-1})N = [a, b]N \end{aligned}$$

olmasıdır. $N = [a, b]N \Longleftrightarrow [a, b] \in N$ olduğundan, G/N değişmeli $\Longleftrightarrow [G,\ G] \subset N$ bulunur.

Sonuç: $N = [G,\ G]$ alınırsa $G/[G,\ G]$ değişmeli gruptur. Ayrıca, $[G,\ G]$ bu özellikte en küçük alt gruptur.

Tanım 3.4.7 Bir G grubunun has, hiçbir normal alt grubu yoksa G ye **basit grup** denir.

Örnek 2: Mertebesi asal olan grup basittir. Gerçekten, $o(G) = p$ ve $H < G$ ise Lagrange teoremine göre $o(H)|o(G) = p$ olduğundan,

$o(H) = 1$ veya p olabilir. Buradan $H = \{e\}$ veya $H = G$ bulunur. Şuhalde G nin has hiçbir alt grubu, dolayısı ile has hiçbir normal alt grubu olamaz.

Tanım 3.4.8 G bir grup ve $M \triangleleft G$ olsun. M yi kapsayan, M ve G den başka hiçbir normal alt grubu yoksa, M ye G nin bir maksimal normal alt grubu denir.

Teorem 3.4.8 $M \triangleleft G$ maksimal $\iff G/M$ basit olmasıdır.

İspat: $\Longrightarrow$: $M \triangleleft G$ maksimal olsun. Teorem 3.4.6' ya göre, $\bar{K} \triangleleft G/M$ ise G nin öyle bir $K \triangleleft G$ normal alt grubu vardır ki $M \triangleleft K$ ve $\bar{K} = K/M$ dir. Fakat M maksimal olduğundan, $M = K$ veya $K = G$ dir. Bu durumda $\bar{K}, G/M$ nin has olmayan bir normal alt grubudur, yani G/M basittir.

$\Longleftarrow$: G/M basit olsun. Teorem 3.4.6 ya göre G nin, M yi kapsayan M ve G den başka hiçbir normal alt grubu olamaz, yani $M \triangleleft G$ maksimaldir.

3.4 ALIŞTIRMALAR

1) Bir grubun bir takım normal alt gruplarının kesişiminin de bir normal alt grup olduğunu gösteriniz.

2) H ve K, bir G grubunun iki normal alt grubu ve $H \cap K = \{e\}$ ise $\forall h \in H$ ve $\forall k \in K$ için $hk = kh$ olduğunu gösteriniz.

3) $H < G, K \triangleleft G$ ise $HK < G$ olduğunu gösteriniz.

4) $H \triangleleft G, K \triangleleft G$ ise $HK \triangleleft G$ olduğunu gösteriniz.

5) $N \triangleleft G$ ve $a \in G$ olsun. $o(a)$ sonlu ise $o(aN) | o(a)$ olduğunu gösteriniz.

6) G sonlu bir grup ve $N \triangleleft G$ olsun. $r = (G : N)$ ve $(r, o(N)) = 1$ ise $x^{o(N)} = e$ eşitliğini sağlayan her $x \in G$ nin N normal alt grubunda olacağını gösteriniz.

7) G değişmeli bir grup ve H da G nin torsion alt grubu (mertebesi

sonlu elemanlarının kümesi) olsun.

a) $H \triangleleft G$ ve

b) G/H nın birimden farklı her elemanın mertebesinin sonsuz olduğunu gösteriniz.

8) $Z \triangleleft Q$ olduğunu gösteriniz ve Q/Z nin, her elemanının mertebesi sonlu olan sonsuz bir grup olduğunu gösteriniz.

9) G sonlu bir grup ve $N \triangleleft G$ olsun. $r = (G : N)$ ise $\forall a \in G$ için $a^r \in N$ olduğunu gösteriniz.

10) Değişmeli grubun her normal alt gruba göre bölüm grubunun da değişmeli olduğunu gösteriniz.

11) G bir grup ve $H \subset G$ olsun.

a) $M(H) = \{a \in G : aHa^{-1} = H\} < G$,

b) $H < G$ ise $H \triangleleft M(H)$ ve

c) $H, K < G, H \triangleleft K$ ise $K \subset M(H)$ olduğunu gösteriniz.

12) $H \triangleleft G \iff G = M(H)$ olduğunu gösteriniz.

13) $H \triangleleft K \triangleleft G$ ise $H \triangleleft G$ olmayabileceğini bir örnekle gösteriniz.

14) K bir G grubunun devirli ve normal bir altgrubu ise K nın her H alt grubu için $H \triangleleft G$ olacağını gösteriniz.

15) G sonlu bir grup ve indeksi 2 olan bir alt grubu varsa G nin basit olmayacağını gösteriniz.

16) Sonlu bir grubun verilen mertebeden tek bir alt grubu varsa bu alt grubun normal olacağını gösteriniz.

17) G grubunun merkezi M ve G/M devirli ise G nin değişmeli olacağını gösteriniz.

18) $H, K < G$ ve $a \in G$ olsun. $M_K(H) = \{k \in K : kHk^{-1} = H\}$ ile tanımlansın.

a) $M_K(H) < G$ ve

b) $H \triangleleft M_K(H)$ olduğunu gösteriniz.

19) 10.mertebeden bir devirli grubun, 2.mertebeden alt grubuna göre bölüm grubunu bulunuz.

20) D_4 dihedral grubunun alt gruplarını ve bölüm gruplarını bulunuz.

21) $H, K, L < G$ ve $H \subset L$ ise $HK \cap L = H(K \cap L)$ eşitliğini gösteriniz.

22) $G = Z_2 \times Z_4$ grubunda $H =< (\bar{0}, \bar{2}) >$ alt grubu veriliyor.
a) $(G : H)$ yı,
b) $(\bar{1}, \bar{2})H$ nın mertebesini bulunuz.

23) G bir grup, $N \triangleleft G$ ve $A \subset G$ olsun. $G =< A >$ ve $\overline{A} = \{x + N : x \in A\}$ ise $G/N =< \overline{A} >$ olduğunu gösteriniz.

3.5 HOMOMORFİZMALAR

Bu kısımda, bir gruptan diğerine grupların cebirsel yapısını koruyan fonksiyonlar üzerinde duracağız.

Tanım 3.5.1 $(G, .)$ ve $(H, *)$ iki grup ve $f : G \longrightarrow H$ bir fonksiyon olsun. $\forall a, b \in G$ için $f(a.b) = f(a) * f(b)$ ise f ye G den H ye bir **homomorfizma** denir.

Örnek 1: $f : G \longrightarrow H, \forall a \in G$ için $f(a) = e_H$ ise f, G den H ye bir homomorfizmadır. Bu homomorfizmaya **aşikar homomorfizma** denir.

Örnek 2: G reel sayıların toplamsal grubu ve H sıfırden farklı reel sayıların çarpımsal grubu olsun. $f(x) = 2^x$ ile tanımlı f fonksiyonu, $\forall x, y \in \mathbb{R}$ için $f(x + y) = 2^{x+y} = 2^x.2^y = f(x)f(y)$ eşitliğini sağladığından bir homomorfizmadır.

Örnek 3: $D_3 = \{e, x, x^2, y, yx, yx^2\}$ ve $H = \{e, y\}$ gruplarını alalım. $f(y^i x^j) = y^i$ $(i = 0, 1,\ j = 0, 1, 2)$ ile tanımlı $f : D_3 \longrightarrow H$ fonksiyonu bir homomorfizmadır. Gerçekten;

$$f(y^i x^j y^k x^t) = f(y^i x^j) f(y^k x^t)$$

olduğunu gösterelim. $k = 0$ ise eşitliğin doğruluğu açıktır. $k = 1$ ise

$$y^i x^j y x^t = y^i (x^j y) x^t = y^i (y x^{j(n-1)}) x^t = y^{i+1} x^{j(n-1)+t}$$

($x^j y = y x^{j(n-1)}$,bak.3.3 Örnek 5) olduğundan eşitlik doğrudur.

Örnek 4: $x \in Z$ için $f(x) = \bar{x}$ ile x in *mod* n kalan sınıfını gösterelim. $f : Z \longrightarrow Z_n$ bir homomorfizmadır. Çünkü, $\forall x, y \in Z$ için,

$$f(x+y) = \overline{x+y} = \bar{x} + \bar{y}$$

dir.

Önerme 3.5.1 $f : G \longrightarrow H$ bir homomorfizma olsun.
(i) $f(e_G) = e_H$ ve
(ii) $\forall a \in G$ için, $f(a^{-1}) = f(a)^{-1}$ dir.

İspat: (i) $a \in G$ ise $f(a) = f(ae_G) = f(a)f(e_G)$ ve H bir grup olduğundan, $f(a)^{-1}$ ile soldan çarparak, $f(e_G) = e_H$ elde edilir.

(ii) $\forall a \in G$ için,

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H$$

olduğundan, her iki yanı $f(a)^{-1}$ ile çarparak, $f(a^{-1}) = f(a)^{-1}$ elde edilir.

Önerme 3.5.2 $f : G \longrightarrow H$ bir homomorfizma olsun.
(i) G nin her alt grubunun f altındaki görüntüsü H nin bu alt grubudur.
(ii) H nın her alt grubunun f altındaki ters görüntüsü G nin bir alt grubudur.

İspat: (i) $N < G$ olsun. $f(N) = \{f(a) \in H \ : \ a \in N\} < H$ olduğunu gösterelim.

$a, b \in N$ olmak üzere, $f(N)$ nin herhangi iki elemanı $f(a)$ ve $f(b)$ olsun. Önceki önermeyi kullanarak,

$$f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$$

bulunur. $N < G$ ve $a, b \in N$ aldığımızdan, $ab^{-1} \in N$ olduğu göz önünde tutularak, $f(a)f(b^{-1}) \in f(N)$ elde edilir.

(ii) $K < H$ olsun. $f^{-1}(K) = \{a \in G \ : \ f(a) \in K\} < G$ olduğunu gösterelim.

$\forall a, b \in f^{-1}(K)$ için, $f(a), f(b) \in K$ ve $K < H$ olduğundan, $f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in K$ olur. Şu halde $f^{-1}(K)$ nın tanımına göre, $ab^{-1} \in f^{-1}(K)$ elde edilir.

Benzer teorem normal alt gruplar için de ispatlanabilir.

Önerme 3.5.3 $f : G \longrightarrow H$ bir homomorfizma olsun.

(i) f örten ise G nin her normal alt grubunun f altındaki görüntüsü H nın bir normal alt grubudur.

(ii) H nın her normal alt grubunun f altındaki ters görüntüsü G nin bir normal alt grubudur.

İspat: (i) f örten ve $N \triangleleft G$ olsun. Önceki önermeye göre $f(N) < H$ dır. Şimdi normal alt grup olduğunu gösterelim.

$\forall h \in H$, $\forall f(a) \in f(N)$ $(a \in N)$ alalım. f örten olduğundan, $h = f(b)$ olacak şekilde $\exists b \in G$ ve

$$hf(a)h^{-1} = f(b)f(a)f(b)^{-1} = f(b)f(a)f(b^{-1}) = f(bab^{-1})$$

olur. $N \triangleleft G$ olduğundan, $bab^{-1} \in N$ ve $hf(a)h^{-1} \in f(N)$ elde edilir.

(ii) $K \triangleleft H$ olsun. $f^{-1}(K) < G$ olduğunu önceki önermede gördük. Şimdi normal alt grup olduğunu gösterelim.

$\forall a \in G$, $\forall b \in f^{-1}(K)$ için,

$$f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)f(b)f(a)^{-1}$$

ve $f(b) \in K$, $K \triangleleft H$ olduğundan, $f(aba^{-1}) \in K$ yani, $aba^{-1} \in f^{-1}(K)$ elde edilir.

Tanım 3.5.2 $f : G \longrightarrow H$ bir homomorfizma ise

$$f^{-1}(e_H) = \{a \in G \ : \ f(a) = e_H\}$$

kümesine f homomorfizmasının **çekirdeği** denir ve Çek f ile gösterilir.

Önerme 3.5.1 den $e_G \in$ Çek f olduğu açıktır.

Önerme 3.5.4 $f : G \longrightarrow H$ homomorfizmasının 1-1 olması için gerek ve yeter koşul Çek $f = \{e_G\}$ olmasıdır.

İspat: $\Longrightarrow$: f 1-1 olsun. Önerme 3.5.1 ye göre,

$$a \in Çek\ f \Longrightarrow f(a) = e_H = f(e_G) \Longrightarrow a = e_G$$

bulunur. Şu halde $Çek\ f = \{e_G\}$ dir.

$\Longleftarrow$: $Çek\ f = \{e_G\}$ olsun. $a, b \in G$ için,

$$\begin{aligned} f(a) = f(b) &\Longrightarrow f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) = e_H \\ &\Longrightarrow ab^{-1} \in Çek\ f \Longrightarrow ab^{-1} = e_G \Longrightarrow a = b \end{aligned}$$

olduğundan, f 1-1 dir.

Tanım 3.5.3 Örten, 1-1 bir homomorfizmaya bir **izomorfizma** denir. Eğer G ve H grupları arasında bir izomorfizma varsa bu gruplara izomorf gruplar denir ve $G \cong H$ yazılır.

İzomorf gruplar arasında 1-1 eşleme var ve grup yapıları da bu eşleme altında bozulmadığı için izomorfizma bir eşitlik gibi düşünülebilir.

Önerme 3.5.5 G bir grup ve $N \triangleleft G$ ise $\forall x \in G$ için, $\varphi(x) = Nx$ ile tanımlı $\varphi : G \longrightarrow G/N$ bir örten, homomorfizmadır ve $Çek\ \varphi = N$ dir.

İspat: $\forall x \in G$ elemanının $N \triangleleft G$ normal alt grubuna göre (sağ) denklik sınıfı teklikle belirli olduğundan $\varphi : G \longrightarrow G/N$ bir fonksiyon ve G/N deki her sınıf, boş kümeden farklı olması sebebi ile $\exists x \in G$ nin sınıfı olacağından, φ örtendir.

$\forall x, y \in G$ için,

$$\varphi(xy) = N(xy) = (Nx)(Ny) = \varphi(x)\varphi(y)$$

olduğundan φ bir homomorfizmadır.

$$x \in Çek\ \varphi \Longleftrightarrow \varphi(x) = Nx = N \Longleftrightarrow x \in N$$

olduğundan, $Çek\ \varphi = N$ bulunur.

Not: G bir grup ve $N \triangleleft G$ ise çekirdeği N olan bir homomorfizma vardır. Gerçekten yukarıda tanımlanan $\varphi : G \longrightarrow G/N$ homomorfizması alınabilir.

Homomorfizma Teoremi 3.5.1 $f : G \longrightarrow H$ bir homomorfizma olsun.

(i) $\text{Çek}\, f = N \triangleleft G$

(ii) $h \in H$ ve bir $a \in G$ için $f(a) = h$ ise $f^{-1}(h) = aN$ dir.

(iii) $G/N \cong f(G)$ dir.

İspat: (i) $\{e_H\} \triangleleft H$ olduğundan, Önerme 3.5.3 (ii) ye göre, $f^{-1}(e_H) = \text{Çek}\, f \triangleleft G$ dir.

(ii) $h \in H$ ve bir $a \in G$ için $f(a) = h$ olsun.

$$\begin{aligned} x \in f^{-1} &\iff f(x) = h = f(a) \\ &\iff f(x)f(a)^{-1} = f(x)f(a^{-1}) = f(xa^{-1}) = e_H \\ &\iff xa^{-1} \in \text{Çek}\, f = N \iff x \in Na = aN \end{aligned}$$

denkliklerinden istenen elde edilir.

(iii) $\forall aN \in G/N$ için $\bar{f}(aN) = f(a)$ ile $\bar{f} : G/N \longrightarrow f(G)$ fonksiyonu tanımlayalım. Önce $\bar{f}$ nin, aN sınıfından alınan temsilciye bağlı olmadığını gösterelim. Yani, $aN = bN$ ise $\bar{f}(aN) = \bar{f}(bn)$ olduğunu gösterelim. $ab^{-1} \in N = \text{Çek}\, f$ ve

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_H \Longrightarrow f(a) = f(b)$$

bulunur. Şu halde $\bar{f}$ iyi tanımlıdır.

$\forall a,\ b \in G$ için, $\bar{f}(aN.bN) = \bar{f}(abN) = f(ab)$
ve f homomorfizma olduğu göz önüne alınırsa,

$$\bar{f}(aN.bN) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$$

elde edilir. Şu halde $\bar{f}$ bir homomorfizmadır.

$$\begin{aligned} \bar{f}(aN) = \bar{f}(bN) &\Longrightarrow f(a) = f(b) \\ &\Longrightarrow f(a)f(b)^{-1} = f(ab^{-1} = e_H \\ &\Longrightarrow ab^{-1} \in \text{Çek}\, f = N \Longrightarrow aN = bN \end{aligned}$$

olduğundan, $\bar{f}$ 1-1 dir.

Son olarak $\bar{f}$ nin örten olduğunu gösterelim.

$f(G)$ nin herhangi bir elemanı $a \in G$ olmak üzere, $f(a)$ şeklinde olduğundan, $aN \in G/N$ için $\bar{f}(aN) = f(a)$ olur. Böylece $\bar{f} : G/N \longrightarrow f(G)$ nin bir izomorfizma olduğu görülür.

Sonuç: $f : G \longrightarrow H$ bir örten homomorfizma ise Önerme 3.5.5 de tanımlı $\varphi : G \longrightarrow G/N(N = Çekf)$ ve $\bar{f} : G/N \longrightarrow f(G) = H$ fonksiyonları için $f = \bar{f}o\varphi$ dir. φ örten homomorfizmasına **doğal homomorfizma** ve f nin böyle yazımına da **doğal ayrışım** denir.

Eğer $f : G \longrightarrow H$ homomorfizması örten değil ise $\mathbf{i}(f(g)) = f(g)$, $\mathbf{i} : f(G) \longrightarrow H$ ile tanımlı gömme fonksiyonu alınarak, $f = \mathbf{i}o\bar{f}o\varphi$ şeklinde yazılabilir.

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle\varphi}\downarrow & & \uparrow{\scriptstyle i} \\ G/Çek\ f & \xrightarrow{\bar{f}} & f(G) \end{array}$$

1.İzomorfizma Teoremi 3.5.2 $f : G \longrightarrow \bar{G}$ örten bir homomorfizma, $Çek\ f = K$, $\bar{N} \lhd \bar{G}$ ve $N = f^{-1}(\bar{N})$ olsun. Bu takdirde, $G/N \cong \bar{G}/\bar{N} \cong (G/K)/(N/K)$ dır.

İspat: $\forall g \in G$ için, $\psi(g) = f(g)N$ ile $\psi : G \longrightarrow \bar{G}/\bar{N}$ dönüşümü tanımlayalım. f örten olduğundan, $\forall \bar{g} \in \bar{G}$ için, $f(g) = \bar{g}$ olacak şekilde $\exists g \in G$ bulunabilir. Şu halde $\bar{G}/\bar{N}$ nin herhangi bir elemanı $\bar{g}\bar{N} = f(g)\bar{N} = \psi(g)$ olduğundan ψ örtendir.

f nin homomorfizma olduğu ve sınıf çarpımı göz önünde tutularak, $\forall a, b \in G$ için

$$\psi(ab) = f(ab)\bar{N} = f(a)f(b)\bar{N} = (f(a)\bar{N})(f(b)\bar{N}) = \psi(a)\psi(b)$$

yani ψ nin bir homomorfizma olduğu görülür.

Şimdi $Çek\ \psi$ yi bulalım. Bir $g \in G$ nin $Çek\ \psi$de olması için gerek ve yeter koşul $\psi(g) = f(g)\bar{N} = \bar{N}$ olmasıdır. Bu da $f(g) \in \bar{N}$ olması ile aynı şeydir. $N = f^{-1}(\bar{N})$ olduğundan, $f(g) \in \bar{N} \iff g \in N$ bulunur. Buradan, $Çek\ \psi = N$ elde edilir. $\psi : G \longrightarrow \bar{G}/\bar{N}$ çekirdeği N olan örten bir homomorfizma olduğundan Homomorfizma Teoreminden $G/N \cong \bar{G}/\bar{N}$ bulunur. Aynı teorem gereğince, $\bar{G} = G/K$ ve $\bar{N} = N/K$ olduğundan istenen elde edilir.

2.İzomorfizma Teoremi 3.5.3 G bir grup, $H < G$ ve $K \lhd G$ olsun. Bu takdirde, $HK = KH < G$ ve $H \cap K \lhd H$ olup $HK/K \cong H/H \cap K$ dır.

İspat: $K \lhd G$ olduğundan, $\forall h \in H$ için $hK = Kh$ dır. $HK = \cup hK = \cup Kh = KH$ olduğundan, $HK = KH < G$ bulunur. $K \subset$

$HK \subset G$ olduğundan, $K \lhd HK$ olduğu açıktır. Şu halde HK/K tanımlıdır.

$H \cap K \lhd H$ olduğunu görmek de kolaydır. Şu halde $H/H \cap K$ da tanımlıdır.

$\forall h \in H$ için, $\psi(h) = hK$ ile $\psi : H \longrightarrow HK/K$ fonksiyonu tanımlayalım.

ψ örtendir. Çünkü $hk \in HK$ olmak üzere $(hk)K = hK = \psi(h)$ dır.

ψ bir homomorfizmadır. Çünkü $\forall h_1, h_2 \in H$ için,

$$\psi(h_1h_2) = (h_1h_2)K = (h_1K)(h_2K) = \psi(h_1)\psi(h_2)$$

dir.

Şimdi Çek ψ yi bulalım. Bir $h \in H$ için,

$$h \in \text{Çek } \psi \Longleftrightarrow \psi(h) = hK = K \Longleftrightarrow h \in H \cap K$$

olduğundan, Çek $\psi = H \cap K$ dır.

Homomorfizma Teoreminden $H/H \cap K \cong HK/K$ elde edilir.

A nın kendi üzerine 1-1 bütün fonksiyonları kümesini $S(A)$ ile göstermiş ve bunun bileşke işlemi altında bir grup olduğunu görmüştük. $S(A)$ nın alt gruplarına bir **dönüşüm grubu** denir. Şimdi her grubun bir dönüşüm grubu olarak düşünülebileceğini gösterelim.

Cayley Teoremi 3.5.4 Her grup bir dönüşüm grubuna izomorftur.

İspat: G bir grup ve $a \in G$ olsun. $\forall x \in G$ için, $T_a(x) = ax$ ile $T_a : G \longrightarrow G$ fonksiyonu tanımlayalım.

G bir grup olduğundan kısaltma özelliği sağlanır ve

$$T_a(x) = T_a(y) \Longrightarrow ax = ay \Longrightarrow x = y$$

bulunur. Şu halde T_a fonksiyonu 1-1 dir.

$\forall y \in G$ için, $Ta(x) = ax = y$ olacak şekilde $\exists x \in G$ bulunabilir. Gerçekten, $x = a^{-1}y \in G$ alınabilir. Buradan T_a nın örten olduğu da görülür. Sonuç olarak $T_a \in S(G)$ dir.

Şimdi, $\forall a \in G$ için $\psi(a) = T_a$ ile $\psi : G \longrightarrow S(G)$ fonksiyonu tanımlayalım.

ψ bir homomorfizmadır: $\forall a, b, x \in G$ için,

$$\begin{aligned} T_{ab}(x) &= (ab)x = a(bx) = aT_b(x) = T_a(T_b(x)) \\ &= (T_a o T_b)(x) \end{aligned}$$

olduğundan, $T_{ab} = T_a o T_b$ yani, $\psi(ab) = \psi(a) o \psi(b)$ dir.

ψ 1-1 dir: $a, b \in G$ için:

$$\psi(a) = \psi(b) \Longrightarrow T_a = T_b \Longrightarrow T_a(e) = T_b(e) \Longrightarrow a = b$$

dir.

Şu halde Homomorfizma Teoremine göre, $G \cong \psi(G)$ ve $\psi(G) < S(G)$ olduğundan istenen elde edilir.

Sonuç: G n. mertebeden bir grup ise $S(G) = S_n$ olduğundan, G grubu S_n nin bir alt grubuna izomorftur.

Yukarıdaki teorem nedeni ile simetrik grupların önemi oldukça çoktur. 3.6. kesimde simetrik grupları daha ayrıntılı olarak inceleyeceğiz.

Tanım 3.5.4 Bir G grubunun kendi üzerine bir izomorfizmasına bir **otomorfizma** denir. G nin bütün otomorfizmaları kümesi $O(G)$ ile gösterilir.

Önerme 3.5.6 G nin bütün otomorfizmaları kümesi $O(G)$ bileşke işlemi altında bir gruptur.

İspat: Okuyucuya bırakılmıştır.

Önerme 3.5.7 G bir grup ve $a \in G$ olsun. $\forall x \in G$ için,

$$\varphi_a(x) = axa^{-1}$$

ile tanımlı $\varphi_a : G \longrightarrow G$, G nin bir otomorfizmasıdır. φ_a ya G nin bir **iç otomorfizması** denir.

İspat: $\forall x, y \in G$ için,

$$\varphi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y)$$

olduğundan, φ_a bir homomorfizmadır.

$$\varphi_a(x) = \varphi_a(y) \Longrightarrow axa^{-1} = aya^{-1} \Longrightarrow x = y$$

olduğundan, φ_a 1-1 dir.

$\forall y \in G$ için $\varphi_a(x) = axa^{-1} = y$ olacak şekilde $\exists x \in G$ bulunabileceğinden, φ_a örten de olur. Şu halde $\varphi_a \in O(G)$ dir.

Önerme 3.5.8 Bir G grubunun bütün iç otomorfizmaları, $O(G)$ otomorfizmalar grubunun bir alt grubudur.

İspat: G nin bütün iç otomorfizmalar kümesini $I(G)$ ile gösterelim. Önceki önermede alınan her $a \in G$ için bir $\varphi_a \in I_G$ bulunabildiğini gördük. Şu halde $\emptyset \neq I(G) \subset O(G)$ dir.

$I(G)$ nin bir alt grup olduğunu göstermek için, $a, b \in G$ olmak üzere alınan $\forall \varphi_a, \varphi_b \in I(G)$ için, $\varphi_a o \varphi_b \in I(G)$ ve $\varphi_a^{-1} \in I(G)$ olduğunu göstermek yeter.

$$\begin{aligned} \forall x \in G,\ (\varphi_a o \varphi_b)(x) &= \varphi_a(\varphi_b(x)) = a(bxb^{-1})a^{-1} \\ &= (ab)x(ab)^{-1} = \varphi_{ab}(x) \end{aligned}$$

olduğundan, $\varphi_a o \varphi_b = \varphi_{ab} \in I(G)$ dir. Buna göre,

$\varphi_a o \varphi_{a^{-1}} = \varphi_{aa^{-1}} = \varphi_e$ ve $\varphi_{a^{-1}} o \varphi_a = \varphi_{a^{-1}a} = \varphi_e$ dir. Ayrıca, $\forall x \in G$ için $\varphi_e(x) = exe^{-1} = x = I_G(x)$ olduğundan φ_e nin $O(G)$ de birim eleman olduğu görülür. Önceki eşitlikler göz önüne alınırsa, $\varphi_{a^{-1}} = \varphi_a^{-1}$ elde edilir.

Önerme 3.5.9 $\forall a \in G$ için, $\psi(a) = \varphi_a$ ile tanımlı, $\psi : G \longrightarrow I(G)$ fonksiyonu bir homomorfizma ve Çek $\psi = M$ (G nin merkezi) olup, $G/M \cong I(G)$ dir.

İspat: İç otomorfizma tanımından, ψ nin örten olduğu anlaşılır. Önerme 3.5.8 de $\forall a, b \in G$ için $\varphi_a o \varphi_b = \varphi_{ab}$ olduğunu gösterdiğimiz için $\psi(ab) = \varphi_{ab} = \varphi_a o \varphi_b = \psi(a) o \psi(b)$ yani, ψ nin bir homomorfizma olduğu görülür.

Şimdi Çek ψ yi hesaplayalım:

$$\begin{aligned} a \in \text{Çek } \psi \iff \psi(a) = \varphi_a = \varphi_e &\iff \forall x \in G, \varphi_a(x) = \varphi_e(x) \\ &\iff \forall x \in G, axa^{-1} = exe^{-1} = x \\ &\iff \forall x \in G ax = xa \\ &\iff a \in M \ \text{(merkez)} \end{aligned}$$

olduğundan, Çek $\psi = M$ bulunur.

Homomorfizma teoreminden $G/M \cong I(G)$ elde edilir.

Tanım 3.5.5 G bir grup ve $a, b \in G$ olsun. $b = xax^{-1}$ olacak şekilde bir $x \in G$ varsa b ye a nın (x ile) bir **eşleniği** denir ve $a \approx b$ ile gösterilir.

Önerme 3.5.10 " $\approx$ " eşlenik olma bağıntısı G de bir denklik bağıntısıdır.

İspat: Yansıma: $\forall a \in G$ için $a = eae^{-1}$ olduğundan, $a \approx a$ dır.

Simetri:

$$a \approx b \implies \exists x \in G, b = xax^{-1}$$
$$\implies \exists x \in G, a = x^{-1}bx \implies b \approx a$$

dır.

Geçişme: $a \approx b$ ve $b \approx c$ olsun.
$\exists x, y \in G, b = xax^{-1}$ ve $c = yby^{-1} \implies c = y(xax^{-1})y^{-1}$

$$\implies c = (yx)a(yx)^{-1} \implies a \approx c$$

Tanım 3.5.6 G de $\approx$ denklik bağıntısının belirttiği denklik sınıflarına **eşlenik sınıfları** denir. $a \in G$ nın belirttiği eşlenik sınıfı $C(a) = \{x \in G : a \approx x\}$ ile gösterilir.

Not: Denklik sınıfları, kümesinin ayrışımını belirttiğinden, G sonlu bir grup ise grubun mertebesi, eşlenik sınıflarındaki elemanların sayıları toplamıdır. $C(a)$ eşlenik sınıfının eleman sayısı c_a ile gösterilir. c_a, a ile eşlenik olan elemanların sayısıdır.

$$G = C(a_1) \cup C(a_2) \cup \cdots \cup C(a_k)$$

G nin eşlenik sınıflarına ayrılışı ise $o(G) = c_{a_1} + c_{a_2} + \cdots + c_{a_k}$ olur. Şimdi c_a ların nasıl hesaplanacağını görelim.

Teorem 3.5.5 G sonlu bir grup ve $a \in G$ olsun. a nın merkezleştiricisi $M(a) = \{x \in G : ax = xa\}$, G nin bir alt grubudur ve $c_a = (G : M(a))$ dır. Şu halde $G = C(a_1) \cup C(a_2) \cup \cdots \cup C(a_k)$ ise

$$o(G) = \sum_{i=1}^{k} (G : M(a_i)) = \sum_{i=1}^{k} \frac{o(G)}{o(M(a_i))}$$

dir.

İspat: $\forall x, y \in M(a)$ için $xa = ax$ ve $ya = ay$ olduğundan,

$$(xy^{-1})a = x(y^{-1}a) = x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$$

yani $xy^{-1} \in M(a)$ bulunur. Buradan, $M(a) < G$ elde edilir.

Şimdi $c_a = (G : M(a))$ olduğunu gösterelim. $(G : M(a)) = r$ diyelim ve G nin $M(a)$ alt grubuna sol denklik sınıflarına ayrılışı,

$$G = M(a) \cup b_1 M(a) \cup \ldots \cup b_{r-1} M(a)$$

olsun.

a nın, $M(a)$ daki tüm elemanlarla eşlenikleri a elemanını verir. Gerçekten, $x \in M(a)$ ise $ax = xa$ ve $xax^{-1} = a$ olur.

a nın, $b_i M(a)$ sınıfındaki tüm elemanlarla eşlenikleri de a nın b_i ile eşleniğini, yani $b_i a b_i^{-1}$ elemanını verir. Gerçekten, $x \in M(a)$ olmak üzere $y = b_i x \in b_i M(a)$ alalım.

$$yay^{-1} = (b_i x)a(b_i x)^{-1} = b_i(xax^{-1})b_i^{-1} = b_i a b_i^{-1}$$

dir. Çünkü $x \in M(a)$ olduğundan, $xax^{-1} = a$ dır.

Son olarak, a nın $b_1, b_2, \ldots b_{r-1}$ ile eşleniklerinin birbirinden ve a dan farklı olduğunu gösterirsek, a nın farklı tüm eşleniklerinin sayısının r, yani $c_a = (G : M(a)) = r$ olduğu anlaşılır.

$i \neq j$ olmak üzere, a nın b_i ve b_j ile eşlenikleri aynı olsa;

$$\begin{aligned} b_i a b_i^{-1} = b_j a b_j^{-1} &\Longrightarrow (b_j^{-1} b_i)a = a(b_j^{-1} b_i) \\ &\Longrightarrow b_j^{-1} b_i \in M(a) \end{aligned}$$

bulunur. Bu ise b_i ve b_j nin $M(a)$ alt grubuna göre, aynı sol denklik sınıfında olması demektir. Halbuki b_i ve b_j farklı sınıflardan alınmış temsilciler olduğundan bu bir çelişkidir.

Benzer şekilde $b_i a b_i^{-1}$ lerin a dan farklı olduğu da gösterilebilir. Aksi halde,

$$a = b_i a b_i^{-1} \Longrightarrow ab_i = b_i a \Longrightarrow b_i \in M(a)$$

çelişkisi elde edilir.

Teoremin son iddiası, yukarıdaki nottan elde edilir.

Tanım 3.5.7 G nin eşlenik sınıflarına ayrılışı, $G = C(a_1) \cup \ldots \cup C(a_k)$ ise $o(G) = \sum_{i=1}^{k} (G : M(a))$ denklemine, G nin **eşlenik sınıf denklemi** denir.

Bir eşlenik sınıfının, tek bir elemandan ibaret olması için gerek ve yeter koşul o elemanın grubun merkezinde olmasıdır. Gerçekten;

$$a \in M \iff \forall x \in G; xa = ax \iff \forall x \in G, xax^{-1} = a \iff C(a) = \{a\}$$

dır. Şu halde eşlenik sınıf denklemi,

$$o(G) = o(M) + \sum (G : M(a))$$

şeklinde yazılabilir. Burada toplam, birden fazla eleman bulunduran eşlenik sınıflarından alınan temsilciler üzerinden alınmıştır.

Şimdiye kadar elemanlar için tanımladığımız eşleniklik kavramını, alt gruplar için de tanımlayabiliriz.

Tanım 3.5.8 H, $K < G$ ve $a \in G$ olsun.

i) $aHa^{-1} = \{aha^{-1} \in G : h \in H\}$ kümesine H **alt grubunun** (a ile) **eşleniği** denir.

ii) $M_K(H) = \{k \in K : kHk^{-1} = H\}$ kümesine H alt grubunun K içindeki **merkezleştiricisi** denir.

aHa^{-1} ve $M_K(H)$ ın da G nin alt grupları ve $M_K(H) < K$ olduğunu göstermek kolaydır.

Not: $\forall a \in G$ için $aHa^{-1} = H \iff H \triangleleft G$ olduğundan, normal alt grubun kendinden başka eşleniği yoktur.

Eğer $K = G$ ise $M_G(H)$ yerine $M(H)$ de yazılabilir ve $M(H)$ ya H nın merkezleştirici denir.

Önerme 3.5.11 $H < G$ olsun. $H \triangleleft M(H)$ ve $M(H)$ bu özellikte G nin en büyük alt grubudur.

İspat: $M(H) < G$ ve $H \subset M(H)$ olduğunu göstermek kolaydır.

$H \triangleleft K < G$ olsun. $\forall k \in K$ için $kHk^{-1} = H$ olduğundan, $k \in M(H)$, yani $K \subset M(H)$ bulunur.

Önerme 3.5.12 $H, K < G$ olsun. H nın, K alt grubundaki elemanlarla farklı eşleniklerinin sayısı $(K : M_K(H))$ dır.

İspat: $k_1, k_2 \in K$ alalım.

$$\begin{aligned} k_1 H k_1^{-1} &\iff H = (k_1^{-1}k_2)H(k_1^{-1}k_2)^{-1} \\ &\iff k_1^{-1}k_2 \in M_K(H) \iff k_1 M_K(H) = k_2 M_K(H) \end{aligned}$$

denkliklerinden, H nın K daki elemanlarla farklı eşleniklerinin sayısının, K nın $M_K(H)$ alt grubuna göre sol denklik sınıfları sayısına, yani $(K : M_K(H))$ indeksine eşit olduğu anlaşılır.

Şimdi eşlenik sınıf denkleminin bir uygulaması olarak aşağıdaki teoremi ispatlayalım:

Teorem 3.5.6 Mertebesi bir asal tam sayının kuvveti olan, bir sonlu grubun merkezi birimden farklıdır.

İspat: p asal, $n \geq 1$ ve $o(G) = p^n$ olsun. Teorem 3.5.5 'e göre, $a \in G$ için $M(a) < G$ ve Lagrange teoremine göre, $o(M(a))|o(G) = p^n$ olduğundan, $0 \leq n_a \leq n$ olmak üzere $o(M(a)) = p^{n_a}$ dır.

$$a \in M \iff M(a) = G \iff n_a = n$$

denklikleri göz önünde tutularak, eşlenik sınıf denklemi yazılacak olursa,

$$o(G) = p^n = o(M) + \sum_{n_a < n} \frac{p^n}{p^{n_a}} = o(M) + \sum_{n_a < n} p^{n-n_a}$$

bulunur. Bu eşitlikten $p|o(M)$ elde edilir. Şu halde $o(M) > 1$, yani M merkezinde birimden başka eleman da vardır.

Sonuç: p asal tam sayı olmak üzere, p^2 mertebeli grup değişmelidir.

İspat: G grubu değişmeli $\iff M = G$ olmasıdır. Önceki teoreme göre $o(M) \neq 1$ ve $o(M)|p^2$ olacağından, $o(M) = p$ veya p^2 olur. Eğer $o(M) = p$ olmayacağını gösterirsek, iddia ispatlanmış olur.

$o(M) = p$ olsun. $\exists a \in G - M$ alalım. $M < M(a)$ ve $M \neq M(a)$ olacağından, $o(M(a)) > p$ ve Lagrange teoreminden $o(M(a)) \mid p^2$ yani $o(M(a)) = p^2$ ve $M(a) = G$ bulunur.

$$M(a) = G \Longleftrightarrow a \in M$$

demek olduğundan, bu $a \in G - M$ olması ile çelişir. Şu halde $o(M) = p$ olamaz.

3.5 ALIŞTIRMALAR

1-) İzomorfizma farkı ile mertebesi 1, 2, 3 olan grupların tek olduğunu gösteriniz.

2-) İzomorfizma farkı ile mertebesi 4 olan iki tip grup olduğunu gösteriniz.

3-) Mertebesi n olan bütün devirli grupların $(\mathcal{Z}_n, +)$ grubu ile izomorf olduğunu gösteriniz.

4-) Her sonsuz devirli grubun $(\mathcal{Z}, +)$ grubu ile izomorf olduğunu gösteriniz.

8-) İki homomorfizmanın bileşkesinin de bir homomorfizma olduğunu gösteriniz.

9-) Bir izomorfizmanın tersinin de bir izomorfizma olduğunu gösteriniz.

10-) G, H ve K üç grup olsun.

i) Her grubun kendisi ile izomorf,

ii) $G \cong H \Longrightarrow H \cong G$ ve

iii) $G \cong H$ ve $H \cong K \Longrightarrow G \cong K$ olduğunu gösteriniz.

11-) $f : G \longrightarrow H$ bir izomorfizma ise $\forall a \in G$ için $o(a) = o(f(a))$ olduğunu gösteriniz.

12-) Bir devirli grubun homomorf görüntüsünün de bir devirli grup olduğunu gösteriniz.

13-) $f : G \longrightarrow G$ bir homomorfizma ve $H = \{a \in G : f(a) = a\}$ ise $H < G$ olduğunu gösteriniz.

14-) G bir değişmeli grup ve $f : G \longrightarrow G, f(x) = x^n$ ile tanımlı olsun. f nin bir homomorfizma olduğunu gösteriniz.

15-) $f : G \longrightarrow H$ bir homomorfizma ve G bir basit grup ise f nin 1-1 veya aşikar homomorfizma olacağını gösteriniz.

16-) Sonsuz bir grubun otomorfizmalarını bulunuz.

17-) n. mertebeden bir devirli grubun otomorfizmalar grubunun, *mod* n asal kalan sınıflar grubu $\mathcal{Z}_n^*$ ile izomorf olduğunu gösteriniz.

18-) G değişmeli bir grup ve $o(G) = 2k + 1, (k \geq 1)$ ise $\forall a \in G$ için $a = b^2$ olacak şekilde $\exists b \in G$ bulunabileceğini gösteriniz.

19-) $f : G \longrightarrow H$ bir homomorfizma ve $K < G$ olsun.

$$f^{-1}(f(K)) = K\text{Çek } f$$

olduğunu gösteriniz.

20-) 2×2 reel, regüler matrislerin çarpımsal grubu $M_{2\times 2}$ olsun. $f(A) = det\ (A)$ ile tanımlı $f : M_{2\times 2} \longrightarrow \mathbb{R} - (o)$ fonksiyonunun bir örten homomorfizma olduğunu gösteriniz.

21-) G ve H iki grup ve $f : G \longrightarrow H$ ile $g : H \longrightarrow G$ iki fonksiyon olsunlar.

i) f örten; f ve gof birer homomorfizma iseler, g nin de bir homomorfizma

ii) g 1-1; g ve gof birer homomorfizma iseler, f nin de bir homomorfizma olduğunu gösteriniz.

22-) Bir homomorfizma altında, iki eşlenik alt grubun görüntülerinin de eşlenik alt grup olduklarını gösteriniz.

23-) G_1 ve G_2 gruplarının direkt çarpımı $G_1 \times G_2$ olsun.

$$\forall (a, b) \in G_1 \times G_2; \quad \pi(a, b) = a$$

ile tanımlı, $\pi : G_1 \times G_2 \longrightarrow G_1$ fonksiyonunun bir örten homomorfizma olduğunu gösteriniz.

24-) $(m,n) = 1$ ise $\mathcal{Z}_m \times \mathcal{Z}_n \cong \mathcal{Z}_{mn}$ olduğunu gösteriniz.

25-) $\mathcal{Z}_2 \times \mathcal{Z}_6$ ve $\mathcal{Z}_{24}$ gruplarının izomorf olup olmadıklarını araştırınız.

26-) $\mathcal{Z}_4 \times \mathcal{Z}_6$ nın $(\bar{1}, \bar{1})$ ile üretilen alt grubunu bulunuz.

27-) İç otomorfizmalar grubunun, otomorfizmalar grubunun bir normal alt grubu olduğunu gösteriniz.

28-) $H < G$, $K \triangleleft G$ olsun.

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)}$$

olduğunu gösteriniz.

29-) D_n dihedral grubunun merkezini bulunuz.

30-) D_4 dihedral grubunun eşlenik sınıf denklemini yazınız.

31-) D_4 dihedral grubunun birimden farklı bir otomorfizmasını bulunuz.

32-) $H < G$ ve G nin her f otomorfizması için $f(H) \subset H$ ise H alt grubuna G nin **karakteristik alt grubu** denir. Karakteristik alt grubun normal alt grup olduğunu gösteriniz.

33-) Bir G grubunun, komütatör alt grubunun bir karakteristik alt grup olduğunu gösteriniz.

34-) $N \triangleleft G$ ve H, N nin bir karakteristik alt grubu ise $H \triangleleft G$ olduğunu gösteriniz.

35-) G sonlu bir grup ve f, G nin $x \in G$ için,

$$f(x) = x \iff x = e$$

koşulunu sağlayan bir otomorfizması olsun. $\forall a \in G$ için $a = b^{-1}f(b)$ olacak şekilde $\exists b \in G$ bulunabildiğini gösteriniz.

36-) Cayley Teoremini kullanark $\mathcal{Z}_4$ grubuna izomorf olan dönüşüm grubunu bulunuz.

3.6 SİMETRİK GRUPLAR

n elemanlı bir kümenin kendi üzerine 1-1 bir fonksiyonuna bir n-li **permütasyon** denir. Bütün n-li permütasyonların kümesinin, bileşke işlemi altında bir grup oluşturduğunu biliyoruz. Bu grup S_n ile gösterilir ve **simetrik grup** veya **permütasyon grubu** olarak adlandırılır.

$f \in S_n$ ve $f, \{x_1, x_2, \ldots, x_n\}$ kümesinin kendi üzerine bir 1-1 fonksiyon olsun. $i_1, i_2, \ldots, i_k$; 1, 2, ... ,n nin bir değişik sırada sıralanışı, yani bir permütasyonu olmak üzere, $f(x_k) = x_i$ $(k = 1, 2, \ldots, n)$ ise f fonksiyonunu, her elemanın altına görüntüsünü yazarak;

$$f = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix} = \begin{pmatrix} x_k \\ x_{i_k} \end{pmatrix}$$

ile veya x leri yazmıyarak;

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

ile gösterelim.

Tanım 3.6.1 Bir f permütasyonu, $j_1, j_2, \ldots, j_k$ $(k > 1)$ farklı doğal sayılar olmak üzere;

$$f(j_1) = j_2,\ f(j_2) = j_3,\ \ldots,\ f(j_{k-1}) = j_k,\ f(j_k) = j_1$$

ile tanımlı ise $f = (j_1 j_2 \cdots j_k)$ ile gösterilir ve k uzunluğunda bir **devir** denir. 1 uzunluğundaki bir devir de özdeşlik fonksiyonu olarak alınır.

Bir deviri, saat yönünde yönlendirilmiş çember üzerinde dizilmiş semboller olarak düşünebilir ve herhangi bir j den başlayarak;

$$f = (j_1 j_2 \ldots j_k) = (j_2 j_3 \ldots j_k j_1) = \ldots = (j_k j_1 \ldots j_{k-1})$$

farklı şekillerde yazabiliriz.

Örnek 1: $(1\ 2\ 3\ 5) \in S_5$ deviri açık olarak yazılırsa;

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$$

permütasyonunu verir.

İki permütasyonun bileşkesi değişmeli değildir. Fakat iki devir ortak eleman bulundurmuyorsa, yani ayrık devir iseler bileşkesi değişmelidir. Bundan sonra fog bileşkesi yerine fg yazalım.

Önerme 3.6.1 Ayrık devirlerin çarpımı değişmelidir.

İspat: $f = (i_1, i_2, \ldots i_r)$ ve $g = (j_i, j_2 \ldots j_s)$ iki ayrık devir olsunlar. $n \notin \{i_1, \ldots, i_r, j_1, \ldots, j_s\}$ ise $f(n) = n$ ve $g(n) = n$ dir. $g(f(n)) = g(n) = n$ ve $f(g(n)) = f(n) = n$ bulunur.

Eğer $n \in \{i_1, i_2, \ldots i_r\}$ ise $f(n) \in \{i_1, i_2, \ldots i_n\}$ dir. f ve g ayrık olduklarından, $n, f(n) \notin \{j_i, j_2, \ldots, j_s\}$ bulunur. Şu halde, $g(n) = n$ ve $g(f(n)) = f(n)$ dir. Diğer taraftan da $f(g(n)) = f(n)$ dir. Benzer şekilde, $n \in \{j_i, j_2, \ldots, j_s\}$ için de $f(g(n)) = g(f(n))$ olduğu gösterilebilir. Şu halde $fg = gf$ dir.

Önerme 3.6.2 r uzunluğundaki bir devirin mertebesi r dir.

İspat: $f = \{i_1, i_2, \ldots, i_r\}$ yi r uzunluğunda bir devir kabul edelim. $1 \leq k, j \leq r$ için

$$\begin{aligned} j + k \leq r &\text{ ise } f^k(i_j) = i_{j+k} \\ j + k > r &\text{ ise } f^k(i_j) = i_{j+k-r} \end{aligned}$$

dir. Buradan $f^r = 1$ ve $1 \leq t < r$ için $f^t \neq 1$ olduğu görülür. Şu halde f nin mertebesi r dir.

Önerme 3.6.3 S_n deki her permütasyon sıra gözetmeksizin, ayrık devirlerin çarpımı olarak tek türlü yazılabilir.

İspat: $f \in S_n$ olsun. 1 in f altında ard arda görüntülerini alalım. $1, f(1), f^2(1), \ldots$ dizisi sonlu olduğu için belli bir adımdan sonra tekrar eder. Şu halde $f^k(1) = 1$ olacak şekilde en küçük bir pozitif k tam sayısı var ve $1, f(1), \ldots f^k(1)$ elemanları birbirinden farklıdırlar. Böylece k uzunluğunda bir $(1 f(1) \ldots f^{k-1}(1))$ deviri elde edilir. İşleme, bu devirde gözükmeyen başka bir sayı alarak devam edilirse, elde edilen devirler ayrık ve çarpımları f yi verir. Bu şekilde f yi ayrık devirlere ayırma, sıra gözetilmezse tek türlü olur.

Örnek 2: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix} = (1)(2\ 5)(3\ 4\ 6)$ dır.
1 uzunluğundaki devirler yazılmayabilir.

Önerme 3.6.4 Bir $f \in S_n$ permütasyonunun mertebesi, ayrıldığı ayrık devirlerin uzunluklarının ekok dır.

İspat: f nin ayrık devirlere ayrılışı $f = c_1, c_2, \ldots, c_s$, c_i devirinin uzunluğu t_i ve $ekok(t_1, t_2, \ldots, t_s) = m$ olsun. Ayrık devirlerin çarpımı değişmeli olduğundan, $f^m = c_1^m c_2^m \ldots c_s^m$ dir. Önerme 3.6.2 ye göre, c_i devirinin mertebesi $o(c_i) = t_i$ olduğundan, $c_1^m = c_2^m = \ldots = c_s^m = 1$ dir. Şu halde $f^m = 1$ bulunur.

Diğer taraftan, f nin c_i deki sayılara kısıtlanışı c_i yi verdiğinden, $f^n = 1$ olması her $i = 1, 2, \ldots s$ için $c_i^n = 1$ olmasını gerektirir. Şu halde $t_i | n$ dir. Böylece $f^n = 1$ olan en küçük pozitif tam sayının ekok $(t_1, t_2, \ldots, t_s) = m$ olduğu görülür.

Örnek 3: $f = (3\ 4)(1\ 2\ 5)$ permütasyonu için, $o(f) = ekok(2, 3) = 6$ ve $g = (3\ 4)(1\ 2\ 3\ 5) = (1\ 2\ 3\ 4\ 5)$ olduğundan, $o(g) = 5$ dir.

Önerme 3.6.5 Her devir 2 li devirlerin (transpozisyon) bir çarpımıdır.

İspat: $(i_1\ i_2\ \ldots\ i_r) = (i_1\ i_r)\ldots(i_1\ i_3)(i_1\ i_2)$ olduğundan istenen elde edilir.

Bir devirin 2 li devirlerin çarpımı olarak yazılması tek türlü değildir. Fakat, bir permütasyonun ayrıldığı 2 li devirlerin sayısının teklik ve çiftliği değişmez.

Örnek 4: $f = (1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2) = (1\ 4)(2\ 3)(2\ 3)(1\ 3)(1\ 2)$.

Tanım 3.6.2 Bir permütasyon çift sayıda 2 linin çarpımı ise bu permütasyona **çift**, aksi halde **tek** permütasyon denir.

Önerme 3.6.6 S_n nin $(n \geq 2)$ bütün çift permütasyonları kümesi A_n, S_n nin $n!/2$ elemanlı bir alt grubudur.

İspat: $1 \in A_n$ olduğundan $\emptyset \neq A_n \subset S_n$ dir. $\forall f, g \in A_n$ için f ve g çift sayıda 2 li nin çarpımı olduğundan, fg de çift sayıda 2 linin çarpımı olur, yani $fg \in A_n$ bulunur. Şu halde A_n, sonlu S_n grubunun çarpımsal kapak bir alt kümesi olduğundan, $A_n < S_n$ dir.

$o(S_n) = n!$ dir. S_n de tek ve çift permütasyonların sayısının aynı olduğunu gösterirsek, $o(A_n) = n!/2$ elde edilir. $A_n = \{f_1, f_2, \ldots, f_k\}$ olsun. A_n nin elemanlarını bir (ab) ikilisi ie çarpalım.
$\{(ab)f_1, (ab)f_2, \ldots, (ab)f_k\}$ permütasyonları da tek olurlar ve bunların dışında da tek permütasyon yoktur. Çünkü, g bir tek permütasyon olsa idi $(ab)g \in A_n$ ve $(ab)g = f_i \Longrightarrow g = (ab)f_i$ olurdu.

Sonuç: A_n, S_n nin indeksi 2 olan bir normal alt grubudur.

İspat: $(S_n : A_n) = \frac{n!}{n!/2} = 2$ olduğundan, $A_n \triangleleft S_n$ dir.

Örnek 5: $S_3 = \{(1), (12), (23), (31), (123), (213)\}$ ve
$A_3 = \{(1), (123), (132)\}$ dir.

Şimdi S_n deki bir elemanın eşleniklerini ve S_n nin eşlenik sınıflarına ayrışımını inceliyelim:

Önerme 3.6.7 $\sigma \in S_n$ için,

$$\sigma(i_1,\ i_2,\ \cdots\ i_r)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \ldots\ \sigma(i_r))$$

dir.

İspat: Önce $\sigma(i_1, i_2, \ldots i_r)\sigma^{-1}$ dönüşümü altında bir $1 \leq x \leq n$ sayısının görüntüsünü bulalım. İşlem bileşke işlemi olduğuna göre sondan başlayarak görüntüler bulunur.

Eğer $\sigma^{-1}(x) \notin \{i_1, i_2, \ldots, i_r\} \Longleftrightarrow x \notin \{\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_r)\}$ ise $(i_1, i_2, \ldots, i_r)(\sigma^{-1}(x)) = \sigma^{-1}(x) \Longrightarrow [\sigma(i_1, i_2, \ldots i_r)\sigma^{-1}](x) = x$ elde edilir. Diğer taraftan, $(\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r))(x) = x$ de aynıdır.

$\sigma^{-1}(x) \in \{i_1, i_2, \ldots i_r\}$, $x = \sigma(i_j)$, $(j = 1,\ 2,\ \ldots\ r)$ olsun.

$$[\sigma(i_1,\ i_2,\ \ldots\ i_r)\sigma^{-1}](x) = [\sigma(i_1,\ i_2,\ \ldots\ i_r)\sigma^{-1}](\sigma(i_j))$$

görüntüsü $j < r$ ise $\sigma(i_{j+1})$, $j = r$ ise $\sigma(j_1)$ bulunur. Diğer taraftan, sağ taraftaki permütasyon alınırsa, $(\sigma(i_1)\ \sigma(i_2)\ \ldots\ \sigma(i_r))(\sigma(i_j))$ da aynısıdır. Şu halde,

$$\sigma(i_1, i_2, \ldots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r))$$

elde edilir.

Sonuç: İki devirin eşlenik olmaları için gerek ve yeter koşul aynı uzunlukta olmalarıdır.

Örnek 6: S_4 de $\sigma = (132)$ ise,

$$\sigma(1\ 2\ 4\ 3)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(4)) = (3\ 1\ 2\ 4)$$

dir.

Örnek 7: S_5 de $(1\ 2\ 3)$ ve $(1\ 3\ 4\ 5)$ eşlenik değildirler

Örnek 8: S_5 de $(1\ 2\ 3\ 4)$ ve $(1\ 3\ 4\ 5)$ eşleniktirler. Gerçekten, $\sigma(1\ 2\ 3\ 4)\sigma^{-1} = (1\ 3\ 4\ 5)$ olacak şekilde $\exists\sigma \in S_5$ bulunabilir. Bir σ bulmak istersek,

$$\sigma(1\ 2\ 3\ 4)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)) = (1\ 3\ 4\ 5)$$

olduğundan; $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 5$ yani

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 5 \end{pmatrix} = (2\ 3\ 4\ 5)$$

alınabilir. (Yukarıdaki eşitliği sağlayan tüm $\sigma \in S_5$ ları bulunuz.)

Yukarıdaki önermeye göre bir devirin σ ile eşleniği kolayca bulunur. Herhengi bir $f \in S_n$ permütasyonunun σ ile eşleniğini bulmak için f ayrık devirlere ayrılır ve her bir devirin σ ile eşlenikleri alındıktan sonra hepsinin bileşkesi alınır.

Örnek 9:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \text{ nin } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

ile eşleniğini bulalım.

$f = (1\ 3\ 4)(2\ 5)$ ve $\sigma = (1\ 3)(2\ 4\ 5)$ olduğuna göre;

$$\begin{aligned} \sigma f\sigma^{-1} &= \sigma(1\ 3\ 4)\sigma^{-1} = (\sigma(1\ 3\ 4)\sigma^{-1})(\sigma(2\ 5)\sigma^{-1}) \\ &= (\sigma(1)\ \sigma(3)\ \sigma(4))(\sigma(2)\ \sigma(5)) = (3\ 1\ 5)(4\ 2). \end{aligned}$$

Tanım 3.6.2 $n \in \mathbb{N}$ olsun. $n_1 \leq n_2 \leq \ldots \leq n_r$ ve $n = n_1 + n_2 + \ldots n_r$ koşullarını sağlayan bir $n_1, n_2, \ldots, n_r$ doğal sayılar

dizisine n nin bir ayrışımı denir. n nin tüm ayrışımları sayısı $p(n)$ ile gösterilir.

Örnek 10:

$1 = 1 \implies p(1) = 1;$
$2 = 2, 2 = 1 + 1 \implies p(2) = 2;$
$3 = 3, 3 = 1 + 2, 3 = 1 + 1 + 1 \implies p(3) = 3;$
$4 = 4, 4 = 1 + 3, 4 = 1 + 1 + 2, 4 = 1 + 1 + 1 + 1, 4 = 2 + 2 \implies$ $p(4) = 5$ dir.

Önerme 3.6.8 S_n de eşlenik sınıflarının sayısı $p(n)$ dir.

İspat: Önerme 3.6.7 nin sonucuna göre, iki devirin eşlenik olmaları için gerek ve yeter koşul uzunluklarının aynı olmasıdır. S_n deki her permütasyon, ayrık devirlerin bir çarpımı olarak yazıldığında, ayrık devirlerin uzunlukları $n_1 \leq n_2 \leq \ldots \leq n_r$ olmak üzere $n = n_1 + n_2 + \ldots + n_r$ olacağından, n nin bir ayrışımını belirtir. Şu halde S_n de iki permütasyonun eşlenik olmaları için gerek ve yeter koşul bu permütasyonların n nin aynı ayrışımını vermeleridir. Dolayısı ile S_n deki farklı eşlenik sınıflarının sayısı $p(n)$ olur.

Örnek 11: S_4 de $p(4) = 5$ eşlenik sınıfı vardır. Bunlar;

$C_1 = \{I\}, \quad C_2 = \{(12), (13), (14), (23), (24), (34)\}$
$C_3 = \{(12)(34), (13)(24), (14)(23)\}$
$C_4 = \{(123), (132), (124), (142), (134), (143), (234), (243)\}$
$C_5 = \{(1234), (1243), (1324), (1342), (1423), (1432)\}$

olup, aynı ayrışımı veren permütasyonlardan oluşurlar. Şu halde S_4 ün sınıf denklemi de 24=1+3+6+8 dir.

Önerme 3.6.9 A_n tüm 3 lü devirlerin kümesi ile üretilmiştir.

İspat: S_n nin tüm 3 lü devirlerinin kümesini S ile gösterelim. $n \leq 2$ ise $S = \emptyset$, S yi kapsayan en küçük alt grup, $< S >= \{I\} = A_n$ bulunur. $n \geq 3$ olsun. 3 lü devirler çift olduğundan, $S \subset A_n$ ve dolayısı ile $< S > \subset A_n$ olur.

Şimdi ters kapsamayı gösterelim. A_n, iki tane 2 lilerin çarpımları ile üretildiğinden, $i_1 \neq i_2$ ve $i_1 \neq i_4$ olmak üzere, $(i_1 i_2)(i_3 i_4)$ şeklindeki

çarpımların $< S >$ de olduğunu gösterirsek, $A_n \subset < S >$ elde edilir. Bu durumda 3 hal vardır:

i) i_j $(j = 1,2,3,4)$ lerden sadece ikisi farklıdır: $i_1 = i_3$, $i_2 = i_4$ olsun. Bu durumda, $(i_1\, i_2)(i_3\, i_4) = I \in < S >$ dir.

ii) i_j $(j = 1,2,3,4)$ lerden üçü farklıdır: $i_1 = i_3$ olsun. Bu durumda, $(i_1\, i_2)(i_3\, i_4) = (i_1\, i_4\, i_2) \in < S >$ dir.

iii) i_j $(j = 1,2,3,4)$ lerin hepsi farklıdır: Bu durumda $(i_1\, i_2)(i_3\, i_4) = (i_1\, i_3\, i_2)(i_1\, i_3\, i_4) \in < S >$ olduğu kolayca gösterilebilir.

Önerme 3.6.10 $N \triangleleft A_n, n \geq 5$ olsun. N bir 3 lü devir kapsarsa $N = A_n$ dir.

İspat: $N \triangleleft A_n$ normal alt grubu bir 3 lü devir kapsarsa, bütün 3 lü devirleri kapsayacağını gösterirsek, önceki önermeye göre, $N = A_n$ olduğu anlaşılır.

$(i_1 i_2 i_3) \in N$ olsun. S_n de herhangi bir üçlü devir de $(j_1\, j_2\, j_3)$ olsun.

$$\sigma(i_1) = j_1,\ \sigma(i_2) = j_2,\ \sigma(i_3) = j_3$$

olacak şekilde $\exists \sigma \in S_n$ var ve

$$\sigma(i_1\, i_2\, i_3)\sigma^{-1} = (\sigma(i_1)\, \sigma(i_2)\, \sigma(i_3)) = (j_1\, j_2\, j_3)$$

olur.

Eğer $\sigma \in A_n$ ise $N \triangleleft A_n$ olduğundan, $(j_1\, j_2\, j_3) \in N$ elde edilir.

Eğer $\sigma \notin A_n$ ise $n \geq 5$ kabul ettiğimizden, $\{a,b\}\{j_1, j_2, j_3\} = \emptyset$ olacak şekilde $1 \leq a, b \leq n$ bulunabilir. $\sigma \notin A_n$ olduğundan, $\tau = (ab)\sigma \in A_n$ olur ve

$$\begin{aligned} \rho(i_1\, i_2\, i_3)\rho^{-1} &= (ab)\sigma(i_1\, i_2\, i_3)\sigma^{-1}(ab) = (ab)(j_1\, j_2\, j_3)(ab) \\ &= (j_1\, j_2\, j_3) \in N \end{aligned}$$

elde edilir.

Hiçbir öz normal alt grubu bulunmayan gruplara basit gruplar demiştik. Şimdi gruplar teorisinde önemli bir yeri olan basit gruba bir örnek verelim.

Abel Teoremi 3.6.1 $n \neq 4$ için A_n alterne grubu basittir.

Bu teoremin ispatını vermeyeceğiz. A_4 ün basit grup olmadığını gösterelim.

$$V_4 = \{I,\ (12)(34),\ (13)(24),\ (13)(24)\} < A_4$$

alt grubu aynı zamanda normal alt gruptur. Çünkü $\forall \sigma \in S_4$ ile V_4 deki elemanların eşleniği gene V_4 dedir. Şu halde $V_4 \lhd S_4$ dolayısı ile $V_4 \lhd A_4$ dir. V_4 grubuna **Klein'in 4-lü grubu** denir.

3.6 ALIŞTIRMALAR

1-) Aşağıdaki permütasyonları ayrık devirlerin çarpımı olarak yazınız ve mertebelerini bulunuz.

i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 4 & 6 & 7 & 3 \end{pmatrix}$

ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 5 & 7 & 4 & 6 \end{pmatrix}$

2-) Aşağıdaki permütasyonları ayrık devirlerin çarpımı olarak yazınız ve mertebelerini bulunuz.

i) (1 2 3 4) ii) (1 2 3 4 5 6) (3 4 5 6)

3-) Aşağıdaki σ ve ρ ler için $\sigma\rho\sigma^{-1}$ yi bulunuz.

i) $\sigma = (1\ 2\ 3\ 4)$, $\rho = (1\ 2)(3\ 4)$

ii) $\sigma = (1\ 3)$, $\rho = (1\ 3\ 2)(2\ 4)$

4-) S_n de $r < n$ olmak üzere kaç r li devir vardır?

5-) S_n de, $\sigma = (1\ 2\ \ldots\ n)$ nin eşlenik sınıfını bulunuz.

6-) S_n de $\sigma = (1\ 2\ \ldots\ n)$ nin merkezleştiricisini bulunuz.

7-) A_4 deki her elemanı 3 lü devirlerin çarpımı olarak yazınız.

8-) S_4 ün iç içe bir normal alt gruplar zincirini yazınız.

9-) $\sigma = (1\ 2\ 3\ 4)$ ile değişmeli olan S_4 deki elemanları bulunuz.

10-) $\sigma = (1\ 2\ 3)(4\ 5)$ ile S_5 de merkezleştiricisini bulunuz.

11-) A_4 ün 6. mertebeden bir alt grubun bulunmadığını gösteriniz.

12-) $n \geq 5$ ise A_n nin $\frac{n!}{4}$ mertebeden bir alt grubunun olmadığını gösteriniz.

13-) Lagrange teoreminin karşıtının doğru olmadığını gösteriniz.

14-) S_n nin, $\{(1\ 2),\ (1\ 3),\ \ldots,\ (1\ n)\}$ ikilileri ile üretildiğini gösteriniz.

15-) S_n nin, $\{(1\ 2),\ (1\ 3),\ \ldots\ n)\}$ ile üretildiğini gösteriniz.

16-) p asal tam sayı ise $x^p = I$ eşitliğini sağlayan $x \in S_p$ lerin sayısının $(p-1)! + 1$ olduğunu gösteriniz.

3.7 ABEL GRUPLARI

Bu kısımda direkt çarpım hakkında bazı sonuçlar elde ettikten sonra Abel Grupları veya Değişmeli grupların yapısını inceliyeceğiz. Gruplar teorisinde, verilen mertebeden bütün grupları sınıflandırmak zor bir problemdir. Bu kısımda, yalnız sonlu Abel gruplarının sınıflandırılması yapılacaktır.

Verilen iki grup G_1 ile G_2 nin direkt çarpımını Önerme 3.2.8 de, tanımlamıştık. n grubun direkt çarpımı da benzer şekilde tanımlanır:

$G_1, G_2, \ldots, G_n$ gruplarının direkt çarpımı; $G_1 \times G_2 \times \cdots \times G_n$ kartezyen çarpım kümesi üzerinde bileşen bileşen yapılan grup işlemine göre elde edilen gruptur:

$$(a_1, \ldots, a_n)(a'_1, \ldots, a'_n) = (a_1 a'_1, \ldots, a_n a'_n)$$

Bir G grubu verildiğinde, G nin ne zaman G_1 ve G_2 gibi iki grubun direkt çarpımı olduğunu bilmek oldukça yararlıdır. Çünkü bu takdirde G nin yapısını, G_1 ve G_2 gruplarının yapısı ile belirlemiş oluruz.

Teorem 3.7.1 G bir grup ve H ile K da iki alt grubu olsunlar. Bu takdirde aşağıdaki koşullar denktirler:

i) G, H ile K nın direkt çarpımına izomorftur: $G \cong H \times K$;

ii) H, $K \triangleleft G$, $HK = G$ ve $H \cap K = \{e_G\}$,

iii) $\forall h \in H$ ye $\forall k \in K$ için, $hk = kh$ ve $\forall x \in G$ için, $x = hk$ olacak şekilde, tek türlü belirli $\exists h \in H$ ve $\exists k \in K$ bulunabilir.

İspat: (i) $\Longrightarrow$ (ii): $G \cong H \times K$ olsun. İzomorfizmayı eşitlik gibi düşünebiliriz. $G = H \times K$ nın sırası ile H ve K üzerine **izdüşümlerini**

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

ile gösterelim. (Bak 3.5 Alıştırma 23). Bu izdüşümler (örten) homomorfizmalar olup; $\text{Çek}\ \pi_1 = K$ ve $\text{Çek}\ \pi_2 = H$, G nin normal alt gruplarıdırlar. G nin her (h,k) elemanı da;

$$(h,k) = (h,1)(1,k)$$

şeklinde yazılabildiğinden, $G = HK$ ve

$$(h,k) \in H \cap K \Longleftrightarrow h = k = e_G$$

olduğundan, $H \cap K = \{e_G\}$ elde edilir. Burada H ile $H \times \{e\}$, K ile $K \times \{e\}$ arasında fark gözetilmemiştir.

(ii) $\Longrightarrow$ (iii): $\forall h \in H$ ve $\forall k \in K$ için, $H, K \triangleleft G$ olduğu göz önünde tutularak;

$$hkh^{-1}k^{-1} \in H \cap K = \{e\} \Longrightarrow hk = kh$$

elde edilir.

$G = HK$ da herhangi bir eleman x olsun. $\exists h, h_1 \in H, \exists k, k_1 \in K$ için, $x = hk = h_1k_1$ olsa

$$h_1^{-1}h = k_1k^{-1} \in H \cap K = \{e\} \Longrightarrow h = h_1, k = k_1$$

elde edilir.

(iii) $\Longrightarrow$ (i) $\alpha : H \times K \longrightarrow G, \alpha(h,k) = hk$ fonksiyonu bir homomorfizmadır. Gerçekten, $\forall h, h' \in H$ ve $\forall k, k' \in K$ için;

$$\begin{aligned} \alpha[(h,k)(h',k')] &= \alpha(hh', kk') = (hh')(kk') \\ &= (hk)(h'k') = \alpha(h,k)\alpha(h',k') \end{aligned}$$

(H ve K daki elemanların değişme özelliği kullanılarak) elde edilir.

α nin örten ve 1-1 olduğu (iii) hipotezinden anlaşılır. Şu halde α bir izomorfizmadır ve $G \cong H \times K$ dır.

Sonuç 1: G bir grup ve $G_1, G_2, \ldots, G_r$ alt grupları olsunlar. Bu takdirde aşağıdaki koşullar denktirler:

i) $G \cong G_1 \times G_2 \times \ldots \times G_r$,

ii) $\forall i = 1, 2, \ldots, r$ için $G_i \triangleleft G$, $G = G_1 G_2 \ldots G_r$ ve $G_1 \ldots G_{i-1} \cap G_i = \{e\}$,

iii) $\forall i, j = 1, 2, \ldots, r, i \neq j$ için, G_i ve G_j nin elemanları değişmeli ve G nin her x elemanı, $x_i \in G_i$ olmak üzere, $x = x_1 x_2 \ldots x_r$ şeklinde tek türlü yazılabilir.

Sonuç 2: Değişmeli grup, eğer toplamsal olarak yazılmışsa direkt çarpıma, **direkt toplam** da denir ve $G = H \oplus K$ ile gösterilir.

G değişmeli bir grup ve $\{a_1, a_2, \ldots, a_n\}$ ile üretilmiş ise $\forall x \in G$ nin, $m_1, m_2, \ldots, m_n \in \mathcal{Z}$ olmak üzere;

$$x = a_1^{m_1} a_2^{m_2} \ldots a_n^{m_n}$$

şeklinde olduğunu biliyoruz. (Bak Önerme 3.3.1) Eğer grup toplamsal olarak yazılmışsa, grubun her elemanı;

$$x = m_1 a_1 + m_2 a_2 + \ldots + m_n a_n$$

şeklinde olur. Fakat bu yazılışta m_i katsayıları tek türlü olarak belirli değildir. Örneğin $o(a_i) = t_i$ ise m_i katsayısı yerine $m_i + t_i q, (q \in \mathcal{Z})$ alsak aynı elemanı buluruz.

Eğer grubun her elemanı yukarıdaki şekilde tek türlü olarak yazılışa sahip olacak şekilde bir $\{a_1, a_2, \ldots, a_n\}$ üreteç sistemi varsa buna grubun bir **tabanı** denir ve a_i nin ürettiği devirli grubu A_i ile gösterirsek, bu takdirde G grubu, A_i devirli gruplarının direkt toplamı olur:

$$G = A_1 \oplus A_2 \oplus \ldots \oplus A_n.$$

Tersine, G grubu devirli bir takım alt grupların direkt toplamı ise G nin her elemanı a_i üreteçlerinin toplamı olarak tek türlü yazılabilir ve yazılışta katsayılar, $o(a_i)$ sonlu ise belli bir kısıtlamadan sonra tek türlü olur. Aşağıda her sonlu üretilmiş değişmeli grup için bir taban bulunabileceğini göreceğiz. Bundan sonra değişmel grupları, toplamsal şekilde alacağız.

Önerme 3.7.1 G değişmeli bir grup ise sonlu mertebeden elemanları G nin bir alt grubunu oluşturur. Bu alt gruba G nin **torsion** alt **grubu** denir ve G ile gösterilir.

İspat: Grubun sıfırının mertebesi 1, (sonlu) olduğundan, $0_G \in G^t$ ve $G^t \neq \emptyset$ dur. Alt grup olma kriterini sağlayalım. Yani, $\forall a, b \in G^t$ için, $a - b \in G^t$ olduğunu gösterelim. Eğer $o(a) = r$, $o(b) = s$ ise;

$$ra = sb \Longrightarrow rs(a - b) = 0$$

olduğundan $a - b$ nin mertebesinin sonlu olduğu anlaşılır.

Tanım 3.7.1 G^t nin elemanlarına **torsion elaman** , grubun diğer elemanlarına da **serbest torsion eleman** denir.

Tanım 3.7.2 $G = G^t$ ise gruba **torsion grup** , $G^t = \{0\}$ ise gruba **serbest torsion grup** denir.

Önerme 3.7.2 Sonlu üretilmiş torsion grup sonludur.

İspat: $G =< a_1, a_2, \ldots, a_n >$ ve $o(a_i) = n_i$ olsun. G nin her x elemanı, $0 \leq m_i < n_i$ olmak üzere;

$$x = m_1 a_1 + m_2 a_2 + \ldots + m_n a_n$$

şeklinde yazılabilir. Şu halde G grubunda en çok $m_1 m_2 \ldots m_n$ eleman olabilir.

Tanım 3.7.3 G bir değişmeli grup ve $e_1, e_2, \ldots, e_n$ serbest torsion elemanları olsun. $\forall x \in G$ için,

$$x = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n$$

olacak şekilde tek türlü olarak belirli $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{Z}$ varsa G grubuna; $e_1, e_2, \ldots, e_n$ elemanları üzerinde **serbest değişmeli grup** denir.

Kısaca serbest değişmeli grup, serbest torsion elemanlardan oluşan bir tabanı bulunabilen gruptur. Birçok taban bulunabilir. Fakat tabandaki elemanların sayısı hep aynıdır. Bu sayıya serbest değişmeli grubun **rangı** denir.

Teorem 3.7.2 F_n, $E = \{e_1, e_2, \ldots, e_n\}$ üzerinde bir serbest değişmeli grup olsun. E den A değişmeli grubuna her fonksiyon tek türlü olarak $F_n \longrightarrow A$ bir homomorfizmaya genişletilebilir. Özel olarak, sonlu üretilmiş grup, bir serbest değişmeli grubun homomorf resmidir.

İspat: $f : E \longrightarrow A$ fonksiyonu verilsin. E ye kısıtlanışı f olacak şekilde bir $f' : F_n \longrightarrow A$ homomorfizmasının bulunabildiğini gösterelim.

$f(e_i) = a_i$ ise F_n nin her elemanı tek türlü olarak $\sum \beta_i e_i$ şeklinde olduğundan,

$$f'(\sum \beta_i e_i) = \sum \beta_i a_i$$

ile tanımlı $f' : F_n \longrightarrow A$ nin aranan homomorfizma olduğu kolaylıkla gösterilebilir.

Şimdi $A =< a_1, a_2, \ldots, a_n >$ sonlu üretilmiş kabul edelim. F_n, $E = \{e_1, e_2, \ldots, e_n\}$ üzerinde serbest değişmeli grup ve e_i yi a_i ye götürelim. Yukarıda açıklandığı gibi, bir $F_n \longrightarrow A$ homomorfizması vardır. Görüntü kümesi a_i üreteçlerini kapsadığından, bu homomorfizma örtendir.

Önerme 3.7.3 Sonlu üretilmiş bir değişmeli grubun serbest olması için gerek ve yeter koşul serbest torsion olmasıdır.

İspat: Serbest değişmeli grubun serbest torsion olduğu açıktır. Tersine $A =< a_1, a_2, \ldots, a_n >$ sonlu üretilmiş ve serbest torsion olsun. n üzerine tümevarım uygulayalım.

$n = 1$ ise A devirli grup olur ve iddia doğrudur. $n > 1$ kabul edelim. $A, \{a_1, a_2, \ldots, a_n\}$ üzerinde serbest ise ispatlanacak birşey kalmaz. Aksi

halde aşikar olmayan bir bağıntı

$$\beta_1 a_1 + \ldots + \beta_n a_n = 0$$

bulunur. β tam sayılarının ebob lerinin 1 olduğu kabul edilebilir. Aksi halde ebob leri ile bölünür, çünkü A yı serbest torsion grup kabul ettik.

Eğer $\beta_1 = \mp 1$ ise $a_1 = \mp(\beta_2 a_2 + \cdots + \beta_n a_n)$ olacağından, $A =< a_2, \ldots, a_n >$ olur ve tümevarım hipotezinde iddia doğrudur.

Şimdi $|\beta_1| \geq |\beta_2| > 0$ kabul edelim ve a_2 yerine $a_2' = a_2 + \mu a_1$ alalım. Bu takdirde yukarıdaki bağıntı;

$$(\beta_1 - \mu\beta_2)a_1 + \beta_2 a_2' + \cdots + \beta_n a_n = 0$$

olur. $\mathcal{Z}$ de bölme algoritması gereğince $|\beta_1 - \mu\beta_2| < |\beta_2|$ olacak şekilde μ bulunabileceğinden, bu şekilde devam ederek, katsayılarından biri ∓ 1 olan bir bağıntı elde edilmiş olur. Böylece üreteçlerden biri değerleri cinsinden yazılmış ve tümevarım hipotezine göre iddianın doğruluğu ispatlanmış olur.

Önerme 3.7.4 Her sonlu üretilmiş, değişmeli grup bir sonlu grupla bir serbest grubun direkt toplamıdır.

İspat: A sonlu üretilmiş bir değişmeli grup olsun. A/A^t de sonlu üretilmiş serbest torsion grup (Bak. Alıştırma 5) ve önceki önermeye göre serbest değişmeli gruptur. $e_1, e_2, \ldots, e_n$ le A nın, $mod\ A^t$ sınıfları A/A^t de taban olacak şekilde seçilmiş elemanlar olsunlar. e ler $mod A^t$ aşikar olmayan bir bağıntı sağlamadıklarından dolayı A da da sağlamazlar. Şu halde $F =< e_1, \ldots, e_n >$ serbest değişmeli bir gruptur. $A = F \oplus A^t$ ve A^t nin sonlu olduğunu gösterirsek önerme ispatlanmış olur.

$A/A^t \cong F$ olduğundan, $\forall x \in A$ için, $x = a + \sum \beta_i e_i$ $(a \in A^t)$ şeklinde yazılabilir. $\sum \beta_i e_i \in A^t$ ve mertebesi k olsun.

$k \sum \beta_i e_i = 0 \Longrightarrow k\beta_i = 0$ (e_i ler taban) olduğundan, $\beta_i = 0, i = 1, 2, \ldots, n$ bulunur. Şu halde $A^t \cap F = (0)$ dır. $A = F \oplus A^t$ elde edilir. A^t, A nın homomorf resmi olduğundan sonlu üretilmiştir ve torsion grup olması nedeni ile sonludur.

Şu halde sonlu üretilmiş değişmeli grupları incelemek için sonlu grupları incelemek gerekir.

Tanım 3.7.4 Bütün elemanlarının mertebesi, p asal sayısının bir kuvveti olan gruba **p-grup** denir.

Şimdi sonlu değişmeli gruplar için temel teoremi ifade edelim.

Teorem 3.7.3 Her sonlu değişmeli grup, farklı p asalları için bir takım p-gruplarının direkt toplamı olarak tam bir türlü olarak ifade edilebilir. Daha açık olarak, $o(A)$ yı bölen asllar $p_1, \ldots, p_r$ ve A_p ler mertebesi p nin kuvveti olan A daki elemanlarını oluşturduğu (maksimal) p-grup olmak üzere;

$$A = A_{p_1} \oplus A_{p_2} \oplus \ldots \oplus A_{p_r}$$

dir.

Diğer taraftan her p-grup bir takım devirli grupların direkt toplamıdır. Önerme 3.7.3 ile birlikte yukarıdaki teoremi birleştirirsek şu teoremi elde ederiz.

Abelyen Grupların Temel Teoremi 3.7.4 Her sonlu üretilmiş değişmeli grup, bir takım devirli grupların direkt toplamıdır. Buradaki gruplar ya sonsuz devirli gruplar, ya da asal kuvvet mertebeli devirli grupturlar. Bu asal sayılar teklikle belirlidir.

Örnek 1: $2^3 = 8$. mertebeden izomorf olmayan bütün değişmeli grupları belirleyelim. 2^3 ün bölenleri; $2, 2^2, 2^3$ olduğundan, bu gruplar; $\mathcal{Z}_8$, $\mathcal{Z}_2 \oplus \mathcal{Z}_{2^2}$, $\mathcal{Z}_2 \oplus \mathcal{Z}_2 \oplus \mathcal{Z}_2$ dirler.

Daha genel olarak p^m mertebeden değişmeli gruplar, m nin ayrışım sayısı $p(m)$ ise, izomorfizma farkı ile $p(m)$ tanedir.

Örnek 2: $G = \mathcal{Z}_{15} \oplus \mathcal{Z}_{50}$ grubun p-grupları direkt çarpımı olarak yazalım.

$$\mathcal{Z}_{15} \cong \mathcal{Z}_3 \oplus \mathcal{Z}_5 \quad \text{ve} \quad \mathcal{Z}_{50} \cong \mathcal{Z}_2 \oplus \mathcal{Z}_{5^2}$$

olduğundan,

$$G \cong \mathcal{Z}_2 \oplus \mathcal{Z}_3 \oplus \mathcal{Z}_5 \oplus \mathcal{Z}_{5^2}$$

dir.

3.7 ALIŞTIRMALAR

1-) $G = H \times K$ ve $H_1 \triangleleft H, K_1 \triangleleft K$ ise $H_1 \times K_1 \triangleleft G$ ve $G/H_1K_1 \cong H/H_1 \times K/K_1$ olduğunu gösteriniz.

2-) $H, K \triangleleft G$ ve $H \cap K = \{e\}$ ise G nin $G/H \times G/K$ nın bir alt grubuna izomorf olduğunu gösteriniz.

3-) H ve K gruplarının merkezi C ve D ise $H \times K$ nın merkezinin $C \times D$ olduğunu gösteriniz.

4-) p ve q farklı asal tam sayılar ise $\mathcal{Z}_p \oplus \mathcal{Z}_q = \mathcal{Z}_{pq}$ olduğunu gösteriniz.

5-) G^t, G nin torsion alt grubu ise G/G^t nin serbest torsion grup olduğunu gösteriniz.

6-) A bir değişmeli grup ve p asal olsun.

$$A_p = \{a \in A \ : \ \exists r \geq 0, p^r a = 0\}$$

kümesinin, A nın maksimal bir p-grubu olduğunu gösteriniz.

7-) $\mathcal{Z}_5 \oplus \mathcal{Z}_5$ ile $\mathcal{Z}_{25}$ in izomorf olmadığını gösteriniz.

8-) 100. mertebeden değişmeli grupları belirtiniz.

9-) G sonlu değişmeli bir grup olsun. $d_1|d_2|\ldots|d_n$ ve $o(G_i) = d_i$ olmak üzere,

$$G \cong G_1 \oplus G_2 \oplus \ldots \oplus G_n$$

şeklinde, G_i devirli gruplarının bulunabileceğini gösteriniz.

10-) 30. mertebeden değişmeli grupları belirleyiniz. Grupta her mertebeden kaç eleman bulunduğunu hesaplayınız.

11-) $\mathcal{Q}$ rasyonel sayılarının toplamsal grubunun serbest torsion grup, fakat serbest değişmeli grup olmadığını gösteriniz.

12-) p_i ler farklı asal sayılar olmak üzere, mertebesi $p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$ olan değişmeli grupların izomorf olmayanlarının sayısının, $p(n_1)p(n_2)\ldots p(n_r)$ olduğunu gösteriniz.

3.8 SYLOW TEOREMLERİ

Lagrange Teoremine göre, bu sonlu grubun her alt grubunun mertebesinin grubun mertebesini böldüğünü biliyoruz. Ayrıca G bir grup ise $o(G)$ nin her pozitif bölenine karşılık bir ve yalnız bir bir alt grubu bulunduğunu da biliyoruz. Fakat herhangi bir G sonlu grubu için bu doğru değildir. Yani, Lagrange teoreminin karşıtı doğru olmayabilir. Buna iki örnek verebiliriz:

Abel Teoremine göre, $n \geq 5$ ise A_n alterne grubu basit olup, $o(A_n) = \frac{n!}{2}$ nin bir böleni, örneğin $\frac{n!}{4}$. mertebeden A_n nin bir alt grubu bulunmamaktır. Çünkü böyle bir alt grubu olsa idi, A_n içindeki indeksi 2 olacağından A_n nin bir normal alt grubu olacak ve A_n nin basit grup olması ile çelişecektir.

İkinci örnek olarak, A_4 alterne grubunu alabiliriz. Bu grubun mertebesi 12 dir ve 6. mertebeden bir alt grubu yoktur.

$n|o(G)$ ise G nin n. mertebeden ne zaman alt grubunun bulunduğuna dair İsveçli matematikçi Sylow bazı teoremler ispatladı.(1872).Bu kesimde Sylow Teoremleri olarak bilinen bu sonuçları inceleyeceğiz. Önce değişmeli gruplar için **Cauchy Teoremini** görelim.

Teorem 3.8.1 G değişmeli ve sonlu bir grup olsun. p asal ve $p|o(G)$ ise G de mertebesi p olan bir eleman, dolayısı ile G nin p. mertebeden bir alt grubu vardır.

İspat: Grubun mertebesi üzereine 2. tümevarım prensibini uygulayalım. $o(G) = 1$ ise iddia doğrudur. Mertebesi $o(G)$ den küçük gruplar için iddianın doğruluğunu kabul edelim.

$a \in G$ ve $a \neq e$ olsun. Eğer $p|o(a) = r$ ve $r = pr'$ ise $a_1 = a^{r'}$ nin mertebesi p olur ve teorem ispatlanmış olur.

Eğer $p \not| o(a) = r$ ise $p|o(G)$ aldığımızdan,

$$p \mid \frac{o(G)}{r} = o(G/ < a >)$$

bulunur. Fakat,

$$o(G/ < a >) < o(G)$$

olduğundan, tümevarım hipotezine göre iddia doğru, yani $G/ < e >$ nın mertebesi p olan bir elemanı mevcuttur. Bu eleman $b < a >$ olsun. $o(b < a >) = p$ dır. $o(b) = s$ diyelim.

$$(b < a >)^s = b^s < a >=< a > \Longrightarrow p|s = o(b)$$

dir. Şu halde $b \in G$ için, $p|o(b)$ olduğundan ilk durumda gösterildiği gibi G de mertebesi p olan bir elemanın varlığı gösterilmiş olur.

Mertebesi p olan elemanın ürettiği alt grup da p. mertebeden olur.

1.Sylow Teoremi 3.8.2 p bir asal sayı ve $k \geq 0$, $p^k \mid o(G)$ ise G grubunun, p^k mertebeden bir alt grubu vardır.

İspat: G grubunun mertebesi üzerine 2.tümevarım prensibini uygulayalım. $o(G) = 1$ ise iddia doğrudur. Mertebesi $o(G)$ den küçük gruplar için iddianın doğruluğunu kabul edelim.

G nin sınıf denklemi;

$$o(G) = o(M) + \sum_{M(a_j) \neq M} (G : M(a_j)$$

ni düşünelim. Eğer $p \not| o(M)$ ise $\exists j$ için,
$p \not| (G : M(a_j))$ olmalıdır. Şu halde $p^k \mid M(a_j)$ olacak şekilde bir $a_j \notin M$ bulunabilir. $o(M(a_j)) < o(G)$ olduğundan, tümevarım hipotezine göre, $M(a_j)$ nin dolayısı ile G nin p^k mertebeden bir alt grubu bulunmuş olur.

Eğer $p \mid o(M)$ ise M değişmeli grup olduğundan, önceki teoreme göre M de mertebesi p olan bir $c \in M$ var ve $< c >$ nin mertebesi p dir. Ayrıca, $< c > \triangleleft G$ olur. (Neden?).

$$o(G/ < c >) = \frac{o(G)}{p},$$

p^{k-1} ile bölünebildiğinden, tümevarım hipotezine göre $G/ < c >$ grubunun, p^{k-1} mertebeden bir alt grubu bulunabilir. Bu alt grup, $< c >$

H sağlayan bir $H < G$ için, $H/ < c >$ şeklindedir. Böylece;

$$o(H) = (H :< c >)o(c) = p^{k-1}.p = p^k$$

elde edilir.

Tanım 3.8.1 $o(G) = mp^k$, p asal ve $p \nmid m$ ise p^k mertebeden alt gruba G nin **p-Sylow alt grubu** denir.

p-Sylow alt grubunun varlığı 1.Sylow Teoreminden anlaşılır. Bir grubun birden çok p-sylow alt grubu olabilir.

Örnek 1: S_3 ün 3 tane 2-sylow alt grubu vardır. Bunlar:

$$\{1,(12)\},\ \{1,(13)\},\ \{1,(23)\}.$$

Şimdi 2-sylow teoremi için bir yardımcı teorem ispatlayalım:

Önerme 3.8.1 P, G nin bir p-sylow alt grubu, $a \in G$ ve $o(a)$, p asal sayısının bir kuvveti olsun. Bu takdirde $aPa^{-1} = P$ ise $a \in P$ dir.

İspat: $aPa^{-1} = P \iff a \in M(P)$ demektir. Şu halde teoremi ispatlamak için $M(P) - P$ de, mertebesi p nin kuvveti olan bir elemanın bulunmadığını göstermeliyiz.

Kabul edelim ki, böyle bir eleman var ve bu eleman a olsun. $P \lhd M(P)$ olduğundan, Önerme 3.5.11, $M(P)/P$ grubunu ve aP sınıfını düşünebiliriz. $o(aP) \mid o(a)$ olduğundan, $o(aP)$ de p nin bir kuvvetidir. Buradan, $< aP >$ nin, $M(P)/P$ nin p kuvvet mertebesi bir devirli grubu olduğu anlaşılır. Şu halde $M(P)$ nin, P yi kapsayan ve $K/P =< aP >$ olan bir K alt grubu vardır. $a \notin P$ asal kabul ettiğimizden, $K \neq P$ dir. $< aP >$ ve P bir p-grup olduklarından, K da bir p-grup olur. Buradan P nin en büyük p kuvvet mertebeden oluşunun, $P \subset K$ ve $P \neq K$ ile çeliştiği görülür.

Şu halde $M(P) - P$ de, p kuvvet mertebeli eleman olamaz.

2.Sylow Teoremi 3.8.3 G sonlu bir grup, p bir asal sayı olsun. G nin p-sylow alt gruplarının sayısı *mod* p 1'e denktir ve bu sayı, $o(G)$ nin bir bölenidir. Ayrıca G nin tüm p-Sylow alt grupları eşleniktirler.

İspat: P, G nin bir p-Sylow alt grubu olsun. Eşlenik alt grupların mertebeleri aynı olduğundan, P nin tüm eşlenikleri de birer p-Sylow alt grupturlar.

Önce P nin farklı eşlenik alt gruplarının sayısını araştıralım:
Eğer $P \lhd G$ ise tüm eşlenikleri kendine eşit ve bu sayı 1 olur.

P nin kendinden farklı bir eşleniği P_1 olsun. P_1 in eşlenikleri P nin de eşlenikleri olduğundan, önce P_1 in P nin elemanları ile farklı eşleniklerini düşünelim. Önerme 3.8.1 göz önünde tutularak;

$$M_P(P_1) = \{a \in P \ : \ aP_1a^{-1} = P_1\} = P \cap P_1$$

ve $P \cap P_1$ de bir p-grup olduğundan, $o(P \cap P_1)$ de p nin bir kuvvetidir. P_1 in P nin elemanları ile farklı eşlenikleri sayısı, Önerme 3.5.12 ye göre;

$$(P : M_P(P_1)) = \frac{o(P)}{o(P \cap P_1)} = p^{k_1}$$

bulunur.

$k_1 = 0$ ise

$$P = P_1 \cap P \Longrightarrow P \subset P_1$$

çelişkisi çıkacağından, $k_1 > 0$ dır. Ayrıca P_1 in, P nin elemanları ile eşlenikleri arasında P nin kendisinin bulunmadığını görebiliriz. Gerçekten: bir $a \in P$ için $aP_1a^{-1} = P$ olsa, $P_1 = a^{-1}Pa \subset P$ çelişkisi bulunurdu.

P nin yukarıda bulduğumuz p^{k_1} tane eşleniğinden başka bir eşleniği P_2 ise aynı işlemleri P_1 yerine P_2 alarak tekrarlarız, böylece $k_2 > 0$ olmak üzere P nin elemanları ile P_2 nin (dolayısı ile P nin) p^{k_2} tane eşleniği daha bulunur. Bulunan P_1 ve P_2 nin, P nin elemanları ile eşlenikleri farklıdırlar. Gerçekten, $a, b \in P$ için;

$$aP_1a^{-1} = bP_1b^{-1} \Longrightarrow (b^{-1}a)P_1(b^{-1}a)^{-1} = P_2$$

olacağından, P_2 nin P_1 in $b^{-1}a \in P$ elemanı ile eşleniği olduğu bulunur ki, bu P_2 nin seçimi ile çelişir. Bu şekilde devam ederek, G sonlu grup olduğundan ve fazla sonlu adım sonra P nin tüm eşlenikleri bulunmuş olur. Bunlar, P nin kendisi; P_1 in P deki elemanlarla bulunan p^{k_1}

eşleniği; P_2 nin P deki elemanlarla bulunan p^{k_2} eşleniği; vs. dir. Bu eşleniklerin sayısı, $k_i > 0$ olmak üzere;

$$1 + p^{k_1} + \cdots + p^{k_i} \equiv 1(mod\ p)$$

sağlanır.

Şimdi tüm p-sylow alt gruplarının birbirine eşlenik olduklarını gösterelim. Böylece teoremin birinci kısmı tamamlanmış olur.

R, P Sylow p-alt grubuna eşlenik olmayan başka bir p-sylow alt grubu olsun. R nin, P deki elemanlarla eşleniklerinin sayısı yukarıda görüldüğü gibi, $j_1 > 0$ olmak üzere;

$$\frac{o(P)}{o(R \cap P)} = p^{j_1}$$

dir. ($j_1 = 0$ olsa $R = P$ olur.) Bu eşlenik alt gruplar içinde, $e \in P$ için $eRe^{-1} = R$ olduğundan, R nin kendisi de vardır. Yukarıdaki gibi düşünerek, R nin tüm eşleniklerinin sayısı $j_i > 0$ olmak üzere;

$$p^{j_1} + \ldots + p^{j_i} \equiv 0(mod\ p)$$

olduğu gösterilebilir. Burada önemli olan nokta tüm j_i lerin pozitif olmasıdır. (Çünkü $j_i = 0$ olması R nin P ile eşlenik olması demektir.) Halbuki bir sayı $mod\ p$ ya 0 ya da 1'e denk olacağından bir çelişki elde edilmiş olur.

Son olarak tüm p-sylow alt gruplarının sayısının $o(G)$ yi böldüğünü gösterelim:

p-Sylow P alt gruplarının tüm eşleniklerinin sayısı;

$$(G : M(P)) = \frac{o(G)}{o(M(P))}$$

olduğundan, $(G : M(P)) \mid o(G)$ bulunur.

Sylow teoremlerinin bir uygulaması olarak iki örnek verelim:

Örnek 2: $o(G) = 20$ ise G basit olamaz. 20 nin asal bölenleri 2 ve 5 olduğundan, G nin 2-Sylow ve 5-Sylow alt grupları vardır. 5-Sylow

alt gruplarının sayısı 2-Sylow teoremine göre, 20 yi böler ve $\equiv 1(mod\ 5)$ dir. 20 nin bölenleri; 1, 2, 4, 5, 10 ve 20 arasında bu özellikteki sayı ancak 1 olabilir. Şu halde bir tek 5-Sylow alt grup var ve tek olması nedeni ile normal alt gruptur. Şu halde bu grup basit olamaz.

Örnek 3: Mertebesi 15 olan grup basit olamaz. 15 in asal bölenleri 3 ve 5 olup, 3-Sylow ve 5-Sylow alt grupları vardır. 15 in bölenleri; 1, 3, 5 ve 15 içinde $\equiv 1 mod\ 3$ ve $\equiv 1(mod\ 5)$ olan sayılar sadece 1 olduğu için, 3-Sylow ve 5-Sylow alt gruplar birer tanedir. Şu halde bu alt gruplar normal ve grup basit değildir.

3.8 ALIŞTIRMALAR

1-) Mertebesi 30 olan bir grubun basit olmadığını gösteriniz.

2-) Mertebesi 42 olan bir grubun, 7-Sylow alt grubunun normal alt grup olduğunu gösteriniz.

3-) Mertebesi 28 olan bir grubun, 7 mertebeden bir normel alt grubun varlığını gösteriniz.

4-) p ve q asal sayılar, $p < q$ olsun. $q \not\equiv 1(mod\ p)$ ve $o(G) = pq$ ise $G \cong \mathcal{Z}_p \oplus \mathcal{Z}_q$ ve G nin bir devirli grup olduğunu gösteriniz.

5-) $p > 2$ asal sayı ve $o(G) = 2p$ ise G nin devirli grup veya bir dihedral grup olduğunu gösteriniz.

BÖLÜM 4

HALKALAR

Bu bölümde iki işlemli cebirsel yapılardan, halka ve cisim üzerinde duracağız.

4.1 HALKALAR

$\mathcal{Z}$ tam sayılar kümesinin sağladığı aritmetiğin temel işlemlerinin özellikleri başka cebirsel yapılar için de sağlanır. Onun için genel tanım yapmak yararlı olacaktır.

Tanım 4.1.1 $R \neq \emptyset$ kümesi üzerinde tanımlı iki ikili işlem $+$ ve $\cdot$ olsun. Aşağıdaki aksiyomları sağlayan $(R, +, \cdot)$ cebirsel yapısına bir halka denir.

H1: $(R, +)$ bir değişmeli gruptur.

H2: $\cdot$ işleminin R de birleşme özelliği vardır.

H3: $\cdot$ işleminin $+$ işlemi üzerine sağdan ve soldan dağılma özellikleri vardır:

$\forall a, b, c \in R$ için, $a(b + c) = ab + ac$ ve $(a + b)c = ac + bc$.

Halkanın $+$ işlemine göre etkisiz elemanına halkanın **sıfır elemanı** denir ve O_R ile gösterilir. Halkanın $\cdot$ işlemine göre etkisiz elemanı olmayabilir. Eğer ikinci işleme göre de etkisiz eleman varsa böyle bir halkaya **birimli halka** denir ve bu etkisiz elemana da halkanın **birim**

elemanı denir ve 1_R ile gösterilir.

Halka, ikinci işleme göre değişme özelliğine sahip ise halkaya değişmeli **halka** denir.

Gruplarda olduğu gibi, iki eleman için tanımlı $+$ ve $\cdot$ işlemleri, sonlu sayıda eleman için de tümevarımla tanımlanabilir. Bu durumda genel birleşme ve genel dağılma özellikleri de sağlanır:

$$(\sum_{i=1}^{k} a_i) + (\sum_{i=k}^{n} a_i) = \sum_{i=1}^{n} a_i, \quad (\prod_{i=1}^{k} a_i)(\prod_{i=k}^{n} a_i) = \prod_{i=1}^{n} a_i$$

$$(\sum_{i=1}^{m} a_i)(\sum_{j=1}^{n} b_j) = \sum_{i=1}^{m}(\sum_{j=1}^{n} a_i b_j).$$

Önerme 4.1.5 R bir halka olsun. $\forall a, b \in R$ için,
i) $a0_R = 0_R a = 0_R$,
ii) $a(-b) = (-a)b = -(ab)$,
iii) $(-a)(-b) = ab$ dir.

İspat: i) Sıfır elemanın tanımı ve soldan dağılma özelliği kullanılarak, $\forall a \in R$ için;

$$a0_R = a(0_R + 0_R) = a0_R + a0_R$$

bulunur. R nin $+$ işlemine göre bir grup olduğu göz önüne alınırsa, son eşitlikten $a0_R = 0_R$ elde edilir.

Benzer düşünce ile $0_R a = 0_R$ olduğu da gösterilebilir.

ii) $\forall a, b \in R$ için;

$$0_R = a0_R = a(b + (-b)) = ab + a(-b)$$

bulunur. Ters eleman tanımı göz önünde tutularak, son eşitlikten $a(-b) = -(ab)$ elde edilir.

Benzer düşünce ile $(-a)b = -(ab)$ olduğu da gösterilebilir.

iii) Önceki özellik kullanılarak, $\forall a, b \in R$ için;

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$$

bulunur.

Sonuç: R birimli bir halka ise $\forall a \in R$ için;
i) $(-1_R)a = -a$ ve
ii) $(-1_R)(-1_R) = 1_R$ dir.

Örnek 1: $R = \{0\}$ tek elmanlı bir halkadır. Buna **sıfır halka** (veya **asikar halka**) denir. Genel olarak halkayı sıfır halkadan farklı kabul edeceğiz.

Önerme 4.1.2 Birimli bir halkada birim ve sıfır elemanlar birbirinden farklıdır.

İspat: R birimli bir halka olsun. Halkaya sıfır halkadan farklı kabul ettiğimiz için $\exists 0_R \neq a \in R$ bulunabilir ve $a1_R = a \neq 0 = 0_R a$ olduğundan, $1_R \neq 0_R$ dir.

Bir halkada, sıfırın her elemanla çarpımı sıfırdır. Fakat sıfırdan farklı iki elemanın çarpımı da sıfır olabilir.

Tanım 4.1.2 R halkasında, $0_R \neq a \in R$ elemanı için;
$ab = 0_R$ (veya $ba = 0_R$) olacak şekilde $\exists 0_R \neq b \in R$ bulunabilirse a ya, halkanın bir **sıfır böleni**, böyle bir b yoksa **sıfır böleni değildir** denir.

Tanımdan 0_R, ne sıfır bölen, ne de sıfır bölen olamayan elemandır.

Örnek 2: $\mathcal{Z}$ tam sayılar halkası birimli, değişmeli bir halka ve sıfır bölensizdir.

Örnek 3: $\mathcal{Z}_m$, *mod* m kalan sınıflar kümesi Bölüm 2 de tanımlı $\ominus$ ve $\odot$ işlemlerine göre bir birimli ve değişmeli halkadır. Bu halkada sıfır bölenler olabilir. Örneğin $\bar{2}, \bar{3} \in \mathcal{Z}$ için, $\bar{2} \odot \bar{3} = \bar{0}$ olduğundan $\bar{2}$ ve $\bar{3}$ sıfır bölendirler. $\mathcal{Z}_6$ nın sıfır bölenleri, $\{\bar{2}, \bar{3}, \bar{4}\}$ asal kalan sınıfı olmayan sınıflardır. Eğer $m = p$ asal ise $\mathcal{Z}_p$ halkası birimli, değişmeli ve sıfır bölensiz olur.

Örnek 4: 2×2 tam sayı bileşenli matrisler kümesinin, matrisler arasındaki toplama ve çarpma işlemine göre, birimli fakat değişmeli olmayan ve sıfır bölenli bir halka olduğu gösterilebilir.

Tanım 4.1.3 Sıfır bölensiz bir halkaya **tam halka** denir. Birimli, değişmeli ve sıfır bölensiz (tam) halkaya da bir **tamlık bölgesi** denir.

Önerme 4.1.3 R bir halka ve $c \in R$ sıfır bölen olmayan bir eleman olsun. $\forall a, b \in R$ için,

$$ac = bc \ \ (\text{veya} \ \ ca = cb) \Longrightarrow a = b$$

sağdan (veya soldan) **kısaltma özelliği** sağlanır.

İspat: $ac = bc \Longrightarrow ac - bc = 0_R \Longrightarrow (a-b)c = 0_R$ olur. c sıfır bölen olmadığından, $a - b = 0_R$ yani $a = b$ bulunur. $ca = cb$ ise benzer şekilde gösterilir.

Sonuç 1: R tam halka $\Longleftrightarrow \forall 0_R \neq c \in R$ ile sağdan ve soldan kısaltma özelliği sağlanır.

Sonuç 2: R bir tam halka ise, $a \neq 0_R$ için $ax = b$ olacak şekilde $\exists x \in R$ varsa teklikle belirlidir. Fakat böyle bir x elemanı bulunmayabilir.

Tanım 4.1.4 R birimli ve değişmeli bir halka ve $R - \{0_R\} = R^*$, ikinci işlem $\cdot$ ye göre bir grup ise R ye bir **cisim** denir.

Tanıma ve Sonuç 2 ye göre, bir cisimde sıfırdan farklı her elemanın çarpımsal tersi var ve tektir.

Örnek 5: Q, $\mathbb{R}$ ve C adi toplama ve çarpıma işlemlerine göre bir cisimdirler. Fakat $\mathcal{Z}$ bir cisim değildir.

Not: R halkasında $-a$ ya a nın ters işaretlisi, varsa a^{-1} çarpımsal tersine de tersi diyelim.

Önerme 4.1.3 Sonlu elemanlı bir tamlık bölgesi cisimdir.

İspat: R sonlu bir tamlık bölgesi olsun. R nin bir cisim olduğunu göstermek için $\forall 0 \neq a \in R$ tersinin varlığını göstermek yeter.

$R = \{a_1, a_2, \ldots, a_n\}$ diyelim ve R nin herhangi bir (sabit) elemanı da a $(a = a_k)$ olsun.

$$f(a_i) = aa_i, \ \ (i = 1, 2, \ldots, n) \ \text{ile} \ f : R \longrightarrow R$$

fonksiyonu tanımlayalım. R tamlık bölgesi olduğundan, kısaltma özelliği sağlanır.

$$f(a_i) = f(a_j) \Longrightarrow aa_i = aa_j \Longrightarrow a_i = a_j$$

den, f nin 1-1 olduğu anlaşılır.

Fakat R sonlu bir küme olduğundan, f nin 1-1 olması örtenliğini gerektirir. Özel olarak $1_R \in R$ için, $1_R = f(a_i) = aa_i$ olacak şekilde $\exists i = 1, 2, \ldots, n$ nin varlığı gösterilmiş olur. Değişme özelliği de sağlandığından a nın tersinin varlığı görülür.

Örnek 6: p asal ise $\mathcal{Z}_p$, p elemanlı bir cisimdir.

Yukarıdaki önermede sonluluk hipotezi kaldırılırsa, iddia yanlış olur. $\mathcal{Z}$ tam sayılar kümesi bir tamlık bölgesidir, fakat bir cisim değildir.

Gruplarda olduğu gibi bir elemanın katı ve kuvveti de tanımlanabilir.

Tanım 4.1.5 R bir tamlık bölgesi olsun. $m1_R = O_R$ olacak şekilde bir $m > 0$ tam sayısı varsa böyle m lerin en küçüğüne R nin **karakteristiği** denir. Eğer bu özellikte hiçbir $m > o$ bulunamıyorsa R nin **karakteristiği sıfır** denir.

Önerme 4.1.4 R bir tamlık bölgesi ise sıfırdan farklı her elemanın, R nin toplamsal grubundaki mertebeleri aynıdır.

İspat: $0_R \neq a \in R$ ve a nın $(R, +)$ grubundaki mertebesi k olsun. Şu halde $ka = 0_R$ yapan en küçük pozitif tam sayı k dır. Kat özelliklerinden ve sıfır bölen olmamasından;

$$ka = k(1_R a) = (k1_R)a = 0_R \Longrightarrow k1_R = 0_R$$

bulunur. $\forall b \in R$ için de $kb = (k1_R)b = 0_R b = 0_R$ olur. Şu halde $\forall b \in R$ için b nin mertebesi k yı böler. Eğer R de sıfırdan farklı ve mertebesi en küçük elemanı alırsak R deki sıfırdan farklı tüm elemanların mertebeleri bu elemanın mertebesi ile aynı olur.

Eğer R de, sıfırdan farklı elemanların mertebeleri sonsuz ise iddianın doğruluğu açıktır.

Sonuç: Tamlık bölgesinin karakteristiği sıfır değil ise asaldır.

İspat: R tamlık bölgesinin karakteristiği p olsun. Karakteristik tanımına göre, 1_R nin mertebesi p dir.

Eğer $p = rs, (r, s < p)$ olsa;

$0_R = p1_R = (rs)1_R = (r1_R)(s1_R) \Longrightarrow r1_R = 0_R$ veya $s1_R = 0_R$ bulunur. Bu ise $r, s < p$ olması ile çelişir. Şu halde p asaldır.

Örnek 7: Q, $\mathbb{R}$ ve $\mathbb{C}$ cisimlerinin karakteristikleri sıfırdır.

Örnek 8: $\mathcal{Z}_p$ (p asal) tamlık bölgesinin karakteristiği p dir.

4.1 ALIŞTIRMALAR

1-) R bir halka olsun. $\forall a, b, c \in R$ için $a(b - c) = ab - ac$ olduğunu gösteriniz.

2-) R bir halka olsun. $\forall a \in R$, $\forall m, n \in \mathcal{Z}$ için,

$$(m + n)a = ma + na \quad \text{ve} \quad (mn)a = m(na)$$

olduğunu gösteriniz.

3-) R bir halka olsun. $\forall a, b \in R$, $\forall m \in \mathcal{Z}$ için,

$$m(a + b) = ma + mb \quad \text{ve} \quad m(ab) = (ma)b$$

olduğunu gösteriniz.

4-) Bir birimli R halkasında, her elemanın toplamsal mertebeleri sonlu ise $\forall a \in R$ için $na = O_R$ olacak şekilde bir $n > o$ tam sayısının bulunabileceğini gösteriniz.

5-) Bir birimli halkada, sıfır bölen olmayan elemanların toplamsal mertebelerinin aynı olduğunu gösteriniz.

6-) R değişmeli bir halka ise $\forall a, b \in R$ için $(a + b)^2 = a^2 + 2ab + b^2$ olduğunu gösteriniz. R değişmeli değil ise ne söylenebilir.

7-) R halka, A herhangi bir küme ve

$$R_A = \{f \ : \ A \longrightarrow R \ \text{ fonksiyon}\}$$

olsun. $\forall f, g \in R_A$ için;

$$(f + g)(a) = f(a) + g(a), \quad (fg)(a) = f(a)g(a)$$

ile tanımlı ise $(R_A, +, .)$ nın da bir halka olduğunu gösteriniz.

8-) R bir halka olsun. $a \in R$ için $a^m = 0_R$ olacak şekilde $\exists m \geq 1$ tam sayısı varsa a ya **nilpotent eleman** denir. n kare çarpansız bir tam sayı ise $\mathcal{Z}_n$ de $\bar{0}$ den başka nilpotent eleman olmadığını gösteriniz.

9-) Değişmeli bir halkada iki nilpotent elemanın toplamının da nilpotent olduğunu gösteriniz.

10-) R tamlık bölgesinde $x^2 = 1_R$ eşitliğini sağlayan elemanların -1_R ve 1_R olduğunu gösteriniz.

11-) R bir halka, A herhangi bir küme ve $f : A \longrightarrow R$ örten, 1-1 bir fonksiyon olsun. $\forall a, b \in A$ için;

$$a + b = f^{-1}(f(a) + f(b)) \quad \text{ve} \quad ab = f^{-1}(f(a)f(b))$$

ile tanımlı işlemler altında $(A, +, .)$ nın bir halka olduğunu gösteriniz.

12-) $\mathbb{R}[\sqrt{2}] = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{R}\}$ nin bir cisim olduğunu gösteriniz.

13-) $\mathcal{Z}[\sqrt{2}] = \{a + b\sqrt{2} \ : \ a, b \in \mathcal{Z}\}$ nin bir tamlık bölgesi olduğunu gösteriniz. $\mathcal{Z}[\sqrt{2}]$ bir cisim midir, araştırınız.

14-) Cismin içinde kapsanan bir halkanın tamlık bölgesi olduğunu gösteriniz.

15-) R birimli bir halka olsun. $\{m1_R \ : \ m \in \mathcal{Z}\}$ nin R de kapsanan bir halka olduğunu gösteriniz.

16-) Birimli bir halkada, tersi mevcut elemanlara **birimsel elemanlar** denir. R de birimsel elemanların çarpımsal bir grup oluşturduğunu gösteriniz.

4.2 ALT HALKA VE İDEALLER

Tanım 4.2.1 R bir halka ve $\emptyset \neq S \subset R$ olsun. R deki işlemlere göre S alt kümesi kendi başına bir halka ise S ye R halkasının bir alt halkası denir.

Örnek 1: $\{0_R\}$ ve R, her R halkasının alt halkalarıdır. Bunlara R nin **aşikar alt grupları** denir. Bunlardan farklı alt halkalara da **öz alt halkaları** denir.

Örnek 2: $\mathbb{Z}$, $\mathbb{Q}$ nın bir öz alt halkasıdır.

Örnek 3: Q, $\mathbb{R}$ nin bir öz alt halkasıdır.

Önerme 4.2.1 R bir halka ve $\emptyset \neq S \subset R$ olsun. S nin, R nin bir alt halkası olması için gerek ve yeter koşul $\forall a, b \in S$ için, $a - b \in S$ ve $ab \in S$ olmasıdır.

İspat: $\Longrightarrow$: S, R nin bir alt halkası olsun. Alt halka tanımına göre S, R deki işleme göre bir halka ve dolayısı ile S, R nin toplamsal grubunun bir alt halkası olur. Şu halde alt grup olma kriterine göre, $\forall a, b \in S$ için, $a - b \in S$ bulunur. Ayrıca, S halka olması sebebi ile çarpma işlemine göre kapalı da olacağından, $\forall a, b \in S$ için, $ab \in S$ olacağı açıktır.

$\Longleftarrow$: $\forall a, b \in S$ için, $a - b \in S$ ve $ab \in S$ olsun. Alt grup olma kriterine göre,

$$\forall a, b \in S \quad \text{için,} \quad a - b \in S \Longrightarrow (S, +) < (R, +)$$

dir Şu halde halka aksiyomlarından $H1$ sağlanır. S de çarpma işlemi kapalı ve halka aksiyomlarından $H2$ ve $H3$, R deki tüm elemanlar için sağlandığından, S deki tüm elemanlar da $H2$ ve $H3$ aksiyomlarını sağlar. Şu halde S, R nin bir alt halkasıdır.

Önerme 4.2.2 Bir halkanın bir takım alt halkaarının arakesiti de bir alt halkadır.

İspat: $(H_i)_{i \in I}$ ailesi, bir R halkasının alt halkalarının bir ailesi olsun. Yani $\forall i \in I$ için, H_i ler R nin bir alt halkası olsunlar. $H = \bigcap_{i \in I} H_i$ nin de bir alt halka olduğunu, önceki önermeyi kullanarak gösterelim.

$\forall a, b \in H = \bigcap_{i \in I} H_i$ için, arakesit tanımından $\forall i \in I$ için $a, b \in H_i$ ve H_i ler alt halka olması sebebi ile $\forall i \in I$ için, $a - b \in Hi, ab \in Hi$ elde edilir. Bu da arakesit tanımından, $a - b \in H$ ve $ab \in H$ demektir.

Tanım 4.2.2 A, R halkasının bir alt kümesi olsun. R nin A yı kapsayan bütün alt halkalarının arakesitine **A nın ürettiği alt halka** denir ve $< A >$ ile gösterilir. A nın elemanlarına da $< A >$ nın üreteçleri denir.

$< A >$ nın tanımından, $< A >$ nın A yı kapsayan en küçük alt halka olduğu, yani $A \subset H$ ve H, R nin bir alt halkası ise $< A > \subset H$ olduğu görülür. $A = \emptyset$ ise $< A >$ sıfır halkadır.

Bir alt kümenin ürettiği alt grubun elemanlarının nasıl olduğunu Bölüm 3 de incelemiştik. Benzer düşünce ile aşağıdaki önerme de ispatlanabilir.

Önerme 4.2.3 $< A >$ alt halkası, A alt kümesinin elemanları üzerinde (sonlu sayıda) toplama ve çarpma işlemleri yapmakla elde edilir.

Örnek 4: Q da, $A = \{\frac{1}{2}\}$ nin ürettiği alt halka;

$$\{a_0 + \frac{a_1}{2} + \frac{a_2}{2^2} + \ldots + \frac{a_r}{2^r} \; : \; r \in \mathbb{N}, \; a_i \in \mathbb{Z}, \; i = 1, 2, \ldots, r\}$$

dir.

Tanım 4.2.3 R bir halka ve $\emptyset \neq I \subset R$ olsun.

i) $\forall a, b \in I$ için $a - b \in I$ ve

ii) $\forall a \in I$ ve $\forall r \in R$ için, $ra \in I$ (veya $ar \in I$)

ise I ya R nin bir **sol** (veya **sağ**) **ideali** denir.

Hem sol, hem de sağ bir ideale **iki taraflı ideal** veya kısaca **ideal** denir. İdealin tanımından, idealin bir alt halka olduğu anlaşılır.

Örnek 5: $\{0_R\}$ ve R, her R halkasının bir idealidirler. Bunlara R nin **aşikar idealleri** denir. Bunlardan farklı ideallerine de **öz idealleri** denir.

Önerme 4.2.4 Bir halkanın bir takım ideallerinin arakesiti de bir idealdir.

İspat: Önerme 4.2.2 de alt halkaların arakesitinin bir alt halka olduğu gösterilmişti. Bu önermenin ispatı da benzer şekilde yapılır.

Tanım 4.2.4 A, R halkasının bir alt kümesi olsun. R nin, A yı

kapsayan bütün ideallerinin arakesitine **A nın ürettiği ideal** denir ve (A) ile gösterilir. Eğer $A = \{a\}$ tek elemanlı bir küme ise A nın ürettiği ideale **temel ideal** denir ve (a) ile gösterilir.

Eğer $A = \emptyset$ ise (A) sıfır ideali olur. (A) nın tanımından, (A) nın A yı kapsayan en küçük ideal olduğu, yani $A \subset I$ ve I, R nin bir ideali ise $(A) \subset I$ olduğu anlaşılır.

Önerme 4.2.5 R değişmeli bir halka ve $\emptyset \neq A \subset R$ ise

$$(A) = \{\sum_{i=1}^{s} r_i a_i + \sum_{j=1}^{t} n_j b_j \ : \ r_i \in R,\ n_j \in \mathcal{Z},\ a_i, b_j \in A,\ s,t \in \mathbb{N}\}$$

dir.

İspat: $M = \{\sum_{i=1}^{s} r_i a_i + \sum_{j=1}^{t} n_j b_j \ : \ r_i \in R,\ n_j \in \mathcal{Z},\ a_i, b_j \in A\}$ kümesinin, R nin A yı kapsayan bir ideali olduğu kolaylıkla gösterilebilir. Şu halde $(A) \subset M$ bulunur.

Ters kapsamayı göstermek için, M nin herhangi bir

$$\sum_{i=1}^{s} r_i a_i + \sum_{j=1}^{t} n_j b_j$$

elemanını alalım. $a_i, b_j \in A$ ve A yı kapsayan bir ideal olması sebebi ile alınan elemanın (A) da olduğu anlaşılır.

Sonuç 1: R değişmeli ve birimli bir halka ise

$$(A) = \{\sum_{i=1}^{s} r_i a_i \ : \ r_i \in R,\ a_i \in A,\ s \in \mathbb{N},\ 1 \leq j \leq s\}$$

dir.

İspat: R birimli ise $n \in \mathcal{Z}$ ve $a \in A$ için,

$$na = n(1_R a) = (n1_R)a \quad \text{ve} \quad n1_R = r \in R$$

olduğundan, yukarıdaki önermeden istenen elde edilir.

Sonuç 2: R değişmeli ve birimli bir halka ve $a \in R$ ise

$$(a) = aR = \{ar \ : \ r \in R\}$$

dir.

Şimdi tam sayılar halkasının önemli bir özelliğini ispatlayalım.

Önerme 4.2.6 Tam sayılar halkasının her ideali, bir temel idealdir.

İspat: I, $\mathcal{Z}$ nin bir ideali olsun. Eğer $I = (0)$ ise temel idealdir. $I \neq (0)$ olsun. Şu halde $\exists 0 \neq u \in I$ bulunabilir. $-u$ da I idealinde olacağından, genelliği bozmadan I idealinde pozitif bir tam sayının varlığını kabul edebiliriz. Pozitif tam sayılar iyi sıralı bir küme olması nedeni ile I da bir en küçük pozitif tam sayı vardır. Bunu a ile gösterelim. Açıktır ki $a \in I$ olduğundan, $(a) = \{ra \ : \ r \in R\} \subset I$ dır.

Şimdi ters kapsamayı gösterelim. $b \in I$ alalım. b yi a ile kalanlı bölerek, $b = aq + r$ ve $0 \leq r < a$ olacak şekilde $\exists q, r \in \mathcal{Z}$ bulunabilr. b ve $qa \in I$ olduğundan, $r = b - aq \in I$ ve $0 \leq r < a$ bulunur. Buradan, a nın seçimi nedeni ile $r = 0$ olması gerektiği anlaşılır. Şu halde $b = aq \in (a)$ elde edilir.

Tanım 4.2.5 Her ideali temel ideal olan bir tamlık bölgesine bir **temel ideal bölgesi** denir ve kısaca TİB ile gösterilir.

Örnek 6: Önceki önermeye göre $\mathcal{Z}$ bir TİB dir.

Şimdi $\mathcal{Z}$ de ideallerin bazı özelliklerini inceliyelim.

Önerme 4.2.7 $a_1, a_2, \ldots, a_n \in \mathcal{Z}$ ve $ekok(a_1, a_2, \ldots, a_n) = a$ ise

$$\bigcap_{i=1}^{n} (a_i) = (a)$$

dır.

İspat: İdeallerin arakesiti de bir ideal ve $\mathcal{Z}$ deki her ideal de bir temel ideal olduğundan, $\bigcap_{i=1}^{n} (a_i) = (c)$ de bir temel idealdir.

Şimdi c nin a_i lerin ekok'ı olarak alınabileceğini görelim.

$$c \in \bigcap_{i=1}^{n}(a_i) \implies \forall i = 1,2,\ldots,n \; ; \quad c \in (a_i)$$
$$\implies \forall i = 1,2,\ldots,n; \; a_i|c$$

olduğundan, c nin a_i lerin bir ortak katı olduğu anlaşılır.

Eğer b, a_i lerin herhangi bir ortak katı ise $\forall i = 1,2,\ldots,n$;

$$b|a_i \implies b \in (a_i), \quad i = 1,2,\ldots,n \implies b \in \bigcap_{i=1}^{n}(a_i) = (c)$$
$$\implies b|c$$

bulunur. Şu halde ekok tanımına göre $c = ekok(a_1, a_2, \ldots, a_n)$ dir.

Örnek 7: $\mathcal{Z}$ de, $(3) \cap (5) \cap (6) = (30)$ dur.

Tanım 4.2.6 I ve J bir R halkasının ideali olsun.

$$I + J = \{a + b \; : \; a \in I, b \in J\}$$

ye ve I ve J **ideallerinin toplamı** denir.

$I + J$ nin de bir ideal olduğu gösterilebilir.

Önerme 4.2.8 $a_1, a_2, \ldots, a_n \in \mathcal{Z}$ ve ebob $(a_1, a_2, \ldots, a_n) = d$ ise $(a_1) + (a_2) + \ldots + (a_n) = (d)$ dir.

İspat: Bölüm 2 de, iki tam sayının ebob' inin bu tam sayıların lineer toplamı olarak yazılabildiğini gördük. Bu sonucu tümevarımla genelleştirerek, ebob $(a_1, a_2, \ldots, a_n) = d$ ise

$$d = x_1a_1 + x_2a_2 + \ldots x_na_n$$

olacak şekilde $\exists x_i \in \mathcal{Z}$ bulunabilir. Şu halde

$$d \in (a_1) + (a_2) + \ldots + (a_n) \quad \text{ve} \quad (d) \subset (a_1) + (a_2) + \ldots + (a_n)$$

bulunur.

Şimdi ters kapsamayı gösterelim. d, e b o b olduğundan bir ortak bölen olup,

$$d|a_1,\ d|a_2,\ \ldots,\ d|a_n \Longrightarrow$$
$$\forall x_i \in \mathcal{Z},\ i = 1,2,\ldots,n;\ \ x_1a_1 + x_2a_2 + \ldots + x_na_n \in (d)$$
$$\Longrightarrow (a_1) + (a_2) + \ldots + (a_n) \subset (d)$$

elde edilir.

Örnek 8: $\mathcal{Z}$ de, (4)+ (6)+ (8)= (2) dir.

Şimdiki gruplarda bir normal alt gruba göre oluşturduğumuz bölüm gruplarına paralel olarak, halkanın bir idealine göre oluşturulan bölüm halkalarını tanımlayalım.

Tanım 4.2.7 R bir halka ve I, R nin bir ideali olsun. $\forall a, b \in R$ için,

$$a \equiv b(mod\ I) \iff a - b \in I$$

ile tanımlayalım.

Önerme 4.2.9 R halkasının, bir I idealine göre tanımlanan $\equiv$ bağıntısı, R de bir denklik bağıntısıdır. $r \in R$ nin denklik sınıfı da

$$\bar{r} = r + I = \{r + a\ :\ a \in I\}$$

dır. Bütün denklik sınıfları kümesi R/I ile gösterilir.

İspat: $\equiv$ nın bir denklik bağıntısı olduğunu göstermek kolaydır.

$$s \in R \text{ için } s \equiv r(mod\ I) \iff s \in r + I$$

denkliğinden, r ile denk elemanların kümesinin yani, r nin denklik sınıfının $r + I$ olduğu görülür.

Not: R halkasının, I idealine göre tanımlanan denklik sınıflarının, R nin toplamsal grubunun I alt grubuna göre tanımlanan denklik sınıfları olduğuna dikkat edelim.

Önerme 4.2.10 R halkasının, bir I idealine göre tanımlanan denklik sınıfları arasında;

$$(a + I) \oplus (b + I) = (a + b) + I, \quad (a + I) \odot (b + I) = (ab) + I$$

ile tanımlanan $\oplus$ ve $\odot$ işlemlerine göre R/I bir halkadır. Bu halkaya R nin I idealine göre **bölüm halkası** denir.

İspat: Önce $\oplus$ ve $\odot$ işlemlerinin iyi tanımlı olduğunu göstermek gerekir, yani

$$a \equiv a'(mod\ I) \quad \text{ve} \quad b \equiv b'\ (mod\ I)$$

ise

$$a + b \equiv a' + b'(mod\ I) \quad \text{ve} \quad ab \equiv a'b'(mod\ I)$$

dır. Bunların ispatı gruplardaki gibi yapılabilir.

R/I, yukarıdaki notta belirtildiği gibi, R nin I toplamsal alt grubuna göre denklik sınıfları olduğundan, bölüm gruplarını anlatırken $(R/I, \oplus)$ nın bir grup olduğunu görmüştük. Dolayısı ile $H1$ aksiyomu sağlanır. $H2$ ve $H3$ aksiyomlarının da sağlandığı gösterilebilir.

Örnek 9: $\mathcal{Z}$ nin (m) idealine göre bölüm halkası $\mathcal{Z}_m$ dir. Gerçekten,

$$a, b \in \mathcal{Z} \text{ için } a \equiv b(mod\ (m)) \Longleftrightarrow a - b \in (m) \Longleftrightarrow m|a - b$$

ile tanımlıdır. Bunun tam sayılar arasında $mod\ m$ denklik bağıntısı ile aynı olduğu görülür.

Önerme 4.2.11 R bir halka ve I bir ideali olsun. S, R nin I yı kapsayan bir alt halkası ise S/I da, R/I nın bir alt halkasıdır. Tersine, R/I nın her alt halkası da S, R nin I yı kapsayan bir alt halkası olmak üzere S/I şeklindedir.

İspat: S, R nin I idealini kapsayan bir alt halkası ise I, S nin de bir ideali olur ve $S/I \subset R/I$ olduğu açıktır. $\forall s + I, t + I \in S/T$ için;

$$(s + I) \oplus (t + I) = (s + t) + I, \quad (s + I) \odot (t + I) = (st) + I$$

ve $s, t \in S$ olduğundan; $s + t, st \in S$ olduğu göz önünde tutularak, alt halka olma kriterine göre S/I nın R/I nın bir alt halkası olduğu görülür.

Tersine, $\overline{U}$ nin R/T nin bir alt halkası olduğunu kabul edelim. $U = \{r \in R : r + I \in \overline{U}\}$ diyelim. $I \subset U$ ve U nun, R nin bir alt halkası olduğunu göstermek kolaydır. Bölüm halkası tanımına göre $U/I = \overline{U}$ olduğu da açıktır.

4.2 ALIŞTIRMALAR

1-) $\mathcal{Z}$ de 3'ün ürettiği alt halkayı ve ideali bulunuz.

2-) Q da 3'ün ürettiği alt halkayı ve ideali bulunuz.

3-) Birimli halkanın bir ideali, halkanın birimini kapsarsa idealin halkaya eşit olacağını gösteriniz.

4-) Cismin aşikar ideallerden başka idealinin olmadığını gösteriniz.

5-) R değişmeli olmayan bir halka ise $a \in R$ nın ürettiği ideali belirleyiniz.

6-) R birimli ve değişmeli bir halka ise R nin a ve b elemanları ile üretilen idealini bulunuz.

7-) R birimli bir halka olsun. R de sıfırdan farklı her elemanın terslenebilmesi için gerek ve yeter koşul R nin hiçbir öz sol idealinin olmamasıdır, gösteriniz.

8-) $a_1, a_2, \ldots, a_n$ tam sayılarının ürettiği ideali bulunuz.

9-) $a, b \in \mathcal{Z}$ ise $(a+b)$ ve $(a)+(b)$ ideallerinin eşit olup olmadığını araştırınız.

10-) R bir halka ve I ile J iki ideali olsun.

$$IJ = \{\sum_{i=1}^{n} a_i b_i \ : \ a_i \in I, \ b_i \in J\}$$

nin, R nin bir ideali olduğunu gösteriniz. (İdeal çarpımı)

11-) $a, b \in \mathcal{Z}$ için, $(ab) = (a)(b)$ olduğunu gösteriniz.

12-) R bir halka ve I ile J iki ideali olsun. $IJ \subset I \cap J$ olduğunu gösteriniz.

13-) R nin her I, J, K idealleri için, $I(J+K) = IJ + IK$ olduğunu gösteriniz.

14-) I ve J bir R tamlık bölgesinin iki ideali ve $I + J = R$ ise $IJ = I \cap J$ olduğunu gösteriniz.

15-) R bir halka ve $a \in R$ olsun.

$$I_a = \{x \in R \ : \ ax = 0\}$$

kümesinin, R nin bir sağ ideali olduğunu gösteriniz.

16-) I, R halkasının bir ideali olsun.

$$(R : I) = \{x \in R \ : \ \forall r \in R, \ rx \in I\}$$

kümesinin, R nin I yı kapsayan bir ideali olduğunu gösteriniz.

17-) I, R nin bir sol ideali ise

$$J = \{x \in R \ : \ \forall a \in I, xa = 0\}$$

ın, R nin bir ideali olduğunu gösteriniz.

18-) F bir cisim ve $a, b \in F$ için, $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ şeklindeki matrisler kümesinin F cismi üzerindeki 2×2 matrisler halkasının bir sağ ideali, fakat bir sol ideali olmadığını gösteriniz.

19-) $H = \{f \ : \ [0,1] \longrightarrow I\!R \ : \ f$ surekli fonksiyon$\}$ kümesinin, fonksiyonlar arasında toplama ve çarpma işlemleri altında bir grup olduğunu ve $I = \{f \in H \ : \ f(\frac{1}{2}) = 0\}$ nın H nın bir ideali olduğunu gösteriniz.

20-) I ve J bir R halkasının ideali ve $I \cap J = (0)$ olsun. $\forall a \in I$ ve $\forall b \in J$ için, $ab = 0$ olduğunu gösteriniz.

21-) R bir halka olsun. $M = \{x \in R \ : \ \forall y \in R, xy = yx\}$ nin, R nin bir alt halkası olduğunu gösteriniz. **(Merkez).**

22-) R değişmeli bir halka olsun.

$$N = \{x \in R \ : \ \exists n \in I\!N, \ x^n = 0\}$$

kümesinin, R nin bir ideali olduğunu ve $\bar{x} \in R/N$ için $\bar{x}^m = \bar{0}$ olacak şekilde $\exists m \in I\!N$ varsa $\bar{x} = \bar{0}$ olduğunu gösteriniz.

23-) R değişmeli bir halka ve I, R nin bir ideali olsun.

$$N(I) = \{x \in R \ : \ \exists n \in I\!N, \ x^n \in I\}$$

nın, R nin I yı kapsayan bir ideali olduğunu gösteriniz. Bu ideale I nın radikali denir.

24-) Önceki probleme göre, $N(N(I)) = N(I)$ olduğunu gösteriniz.

25-) $\mathcal{Z}[i] = \{a + bi \ : \ a, b \in \mathcal{Z}\}$ nın bir tamlık bölgesi olduğunu gösteriniz. **Gauss Tam Sayılar Bölgesi.**

26-) d kare çarpansız bir tam sayı olsun.

$$Q[\sqrt{d}] = \{a + b\sqrt{d} \ : \ a, b \in Q\}$$

nın bir cisim olduğunu gösteriniz.

27-) $\mathcal{Z}[\sqrt{2}] = \{a + b\sqrt{2} \ : \ a, b \in \mathcal{Z}\}$ nin bir tamlık bölgesi, fakat cisim olmadığını gösteriniz. $\sqrt{2}$ nin, $\mathcal{Z}[\sqrt{2}]$ de ürettiği alt halka ve ideali bulunuz.

28-) $\mathcal{Z}[i]$ de 2 nin ürettiği idealin, 1+i nin ürettiği idealin karesi olduğunu gösteriniz.

4.3 HOMOMORFİZMALAR

Gruplarda, grup işlemini koruyan fonksiyonların önemli bir rol oynadığını görmüştük. Benzer kavramlar halkalar için de tanımlanabilir.

Tanım 4.3.1 R ve S iki halka ve $f : R \longrightarrow S$ bir fonksiyon olsun. Eğer $\forall a, b \in R$ için;

i) $f(a + b) = f(a) + f(b)$ ve

ii) $f(ab) = f(a)f(b)$

ise f ye, R den S ye bir **halka homomorfizması** denir. (i) ve (ii) eşitliklerinde, soldaki $+$ ve $\cdot$ nın R deki ve sağdaki $+$ ve $\cdot$ nın da S deki işlemler olduğuna dikkat edelim. (i) ye göre f, R den S ye toplamsal grupları için bir grup homomorfizmasıdır. Şu halde grup homomorfizmasının Bölüm 3 de anlatılan özellikleri de sağlanır. Aşağıdaki önerme bunun bir sonucudur.

Önerme 4.3.1 $f : R \longrightarrow S$ bir homomorfizma ise

i) $f(0_R) = 0_S$ ve
ii) $\forall a \in R$ için, $f(-a) = f(a)$ dır.

Örnek 1: $\forall a \in R$ için $f(a) = 0_S$ ile tanımlı $f : R \longrightarrow S$ bir homomorfizmadır. Bu homomorfizmaya **sıfır homomorfizma** denir.

Örnek 2: $\forall n \in \mathcal{Z}$ için, $f(n) = \bar{n}$ ile tanımlı $f : \mathcal{Z} \longrightarrow \mathcal{Z}_m$ fonksiyonu bir homomorfizmadır.

Önerme 4.3.2 $f : R \longrightarrow S$ örten bir homomorfizma olsun.
i) U, R nin bir alt halkası ise $f(U), S$ nin bir alt halkası,
ii) R değişmeli ise S de değişmeli
iii) R birimli ise S de birimli ve $f(1_R) = 1_S$ dir.

İspat: i) $\forall x, y \in f(U)$ için $x = f(a)$ ve $y = f(b)$ olacak şekilde $\exists a, b \in U$ bulunabilir. U, R nin bir alt halkası olduğu için, $a - b \in U$ ve $ab \in U$ olacağından, $f(a - b) = f(a) - f(b) = x - y \in f(U)$ ve $f(ab) = f(a)f(b) = xy \in f(U)$ bulunur. Alk halka olma kriterine göre $f(U)$ nun, S nin bir alt halkası olduğu anlaşılır.

ii) $\forall x, y \in S$ için, f örten olduğundan, $x = f(a)$ ve $y = f(b)$ olacak şekilde $\exists a, b \in R$ bulunabilir. R değişmeli ise

$$xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx$$

dan, S nin değişmeli olduğu görülür.

iii) $\forall x \in S$ için, f örten olduğundan, $x = f(a)$ olacak şekilde $\exists a \in R$ bulunabilir.

$$f(1_R) = f(a)f(1_R) = f(a1_R) = f(a) = x$$

ve benzer şekilde $f(1_R)x = x$ olduğundan, $f(1_R) \in S$ nin S nin birimi olduğu görülür.

Tanım 4.3.2 $f : R \longrightarrow S$ homomorfizması 1-1 ve örten ise f ye bir **izomorfizma**, R ile S ye de **izomorf halkalar** denir ve $R \cong S$ ile gösterilir.

Tanım 4.3.3 $f : R \longrightarrow S$ bir homomorfizma ise f nin **çekirdeği**

$$\text{Çek } f = \{a \in R \ : \ f(a) = 0_R\} = f^{-1}(0_R)$$

ile tanımlanır.

Homomorfizma Teoremi 4.3.1 $f : R \longrightarrow S$ bir halka homomorfizması ise

i) Çek $f = I$, R nin bir idealidir.

ii) $\forall r \in R$ için, $\phi(r) = r + I$ ile tanımlı $\phi : R \longrightarrow R/I$ fonksiyonu bir örten homomorfizmadır. ϕ ye **doğal homomorfizma** denir.

iii) $R/I \cong f(R)$ dir.

İspat: i) $\forall a, b \in$ Çek f için;

$$f(a-b) = f(a) - f(b) = 0_S - 0_S = 0_S \Longrightarrow a - b \in \text{Çek } f,$$

$\forall a \in$ Çek f, $\forall r \in R$ için;

$$f(ar) = f(a)f(r) = 0_S f(a) = 0_S \Longrightarrow a_r \in \text{Çek } f \text{ ve}$$

$$f(ra) = f(r)f(a) = f(a)0_S = 0_S \Longrightarrow r_a \in \text{Çek } f$$

olduğundan, Çek f nin bir ideal olduğu görülür.

ii) $\forall r \in R$ için, $\phi(r) = r + I$ ile $\phi : R \longrightarrow R/I$ fonksiyonu tanımlayalım.

$$\begin{aligned} \forall a, b \in R \text{ için } \phi(a+b) &= (a+b) + I = (a+I) \oplus (b+I) \\ &= \phi(a) \oplus \phi(b), \end{aligned}$$

$$\phi(ab) = (ab) + I = (a+I) \odot (b+I) = \phi(a) \odot \phi(b)$$

eşitliklerinden, ϕ nin bir homomorfizma olduğu görülür.

Ayrıca $\forall \overline{r} = r + I \in R/I$ için $\phi(r) = r + I$ olacak şekilde $\exists r \in R$ bulunabildiğinden ϕ, örtendir.

iii) $\forall r + I \in R/I$ için, $\bar{f}(r+I) = f(r)$ ile $\bar{f} : R/I \longrightarrow f(R)$ tanımlayalım.

$\bar{f}$ iyi tanımlıdır: Gerçekten,

$$\begin{aligned} r + I = s + I &\Longrightarrow r - s \in I = \text{Çek } f \\ &\Longrightarrow f(r-s) = f(r) - f(s) = 0_S \\ &\Longrightarrow f(r) = f(s) \end{aligned}$$

dir.

$\bar{f}$ nin örten olduğu açıktır. $\bar{f}$, 1-1 dir. Gerçekten,

$$\begin{aligned}\bar{f}(r+I)=\bar{f}(s+I) &\Longrightarrow f(r)=f(s)\\ &\Longrightarrow f(r-s)=0, \Longrightarrow r-s\in \text{Çek } f=I\\ &\Longrightarrow r+I=s+I\end{aligned}$$

dır.

Şimdi $\bar{f}$ nin bir homomorfizma olduğunu gösterelim. $\forall r+I, s+I \in R/I$ için;

$$\begin{aligned}\bar{f}[(r+I)\oplus(s+I)] &= \bar{f}(r+s+I)\\ &= f(r+s)=f(r)+f(s)\\ &= \bar{f}(r+I)+\bar{f}(s+I),\\ \bar{f}[(r+I)\odot(s+I)] &= \bar{f}(rs+I)=f(rs)=f(r)f(s)\\ &= \bar{f}(r+I)\bar{f}(s+I)\end{aligned}$$

olduğundan, $\bar{f}$ bir homomorfizmadır. Şu halde $\bar{f}$ bir izomorfizmadır.

Sonuç 1: $f : R \longrightarrow S$ bir homomorfizma ise $f = \bar{f}o\phi$ olacak şekilde bir $\phi : R \longrightarrow R/I$ örten homomorfizması (doğal homomorfizma) ve bir $\bar{f} : R/I \longrightarrow f(R) = S$ izomorfizması vardır. Bu ayrışıma f nin **doğal ayrışımı** denir.

Sonuç 2: $f : R \longrightarrow S$ bir homomorfizma ise $f = io\bar{f}o\phi$ olacak şekilde bir $\phi : R \longrightarrow R/I$ örten homomorfizması (**doğal homomorfizma**), bir $\bar{f} : R/I \longrightarrow f(R)$ izomorfizması ve bir $i : f(R) \longrightarrow S$ 1-1 homomorfizması (gömme) vardır. Bu ayrışıma f nin doğal ayrışımı denir.

1.İzomorfizma Teoremi 4.3.2 R bir halka ve S de bir alt halkası olsun. I, R nin bir ideali ise $S+I=\{s+a : a\in I\}$ R nin I idealini kapsayan bir alt halkasıdır. Ayrıca şu izomorfizma vardır:

$$(S+I)/I \cong S/(S\cap I)$$

İspat: $S+I$ nın, R nin I yı kapsayan bir alt halkası olduğu açıktır.

$\forall s\in S$ için, $f(s)=s+I$ ile $f : S \longrightarrow R/I$ fonksiyonu tanımlayalım. f nin bir halka homomorfizması ve $f(S)=S+I/I$ olduğu gösterilebilir.

Şimdi Çek f yi bulalım. $s \in S$ için,

$$s \in \text{Çek } f \iff f(s) = s + I = I \iff s \in I$$

olduğundan, Çek $f = S \cap I$ dir. Homomorfizma teoremine göre, $S/(S \cap I) \cong (S + I)/I$ elde edilir.

2.İzomorfizma Teoremi 4.3.3 $f : R \longrightarrow S$ bir örten homomorfizma ve Çek $f = K$ olsun. S nin idealleri ile R nin K yı kapsayan idealleri arasında 1-1 bir eşleme yapılabilir. Bu eşleme S nin bir I ideali verildiğinde I ya; R nin K yı kapsayan,

$$J = \{x \in R : f(x) \in I\} = f^{-1}(I)$$

idealini karşılık getirmekle yapılabilir. Bu takdirde, $R/J \cong S/I$ dır.

İspat: $f : R \longrightarrow S$ bir örten homomorfizma ve Çek $f = K$ olsun. I, S nin bir ideali ise $f^{-1}(I) = J$ nin de, R nin K yı kapsayan bir ideali olduğunu gösterelim. $\forall x, y \in f^{-1}(I)$ için, $f(x) \in I$ ve $f(y) \in I$ olduğundan,

$$f(x - y) = f(x) - f(y) \in I \Longrightarrow x - y \in f^{-1}(I)$$

ve $\forall x \in f^{-1}(I)$ ve $\forall r \in R$ için, I nın S nin bir ideali olduğu göz önünde tutularak,

$$f(xr) = f(x)f(r) \in I, \quad f(rx) = f(rx) = f(r)f(x) \in I$$

bulunur. Ayrıca $K = \text{Çek } f = f^{-1}(0_S) \subset f^{-1}(I)$ olduğu da açıktır.

S nin idealleri ile R nın K yı kapsayan idealleri arasında $I \longrightarrow f^{-1}(I)$ fonksiyonunun 1-1 ve örten olduğunu gösterelim.

I_1 ve I_2, S nin iki ideali iseler

$$f^{-1}(I_1) = f^{-1}(I_2) \Longrightarrow I_1 = I_2$$

olduğu açıktır. Şu halde yukarıda tanımlanan fonksiyon 1-1 dir.

Önce J, R nin bir ideali ise $f(J)$ nin de S nin bir ideali olduğunu gösterelim. Önerme 4.3.2 ye göre $f(J)$, S nin bir alt halkasıdır.

$\forall x \in f(J)$ için, $x = f(a)$ olacak şekilde $\exists a \in J$ ve f örten olduğundan, $\forall s \in S$ için $s = f(r)$ olacak şekilde $\exists r \in R$ bulunabildiğinden, $\forall s \in S$ ve $\forall x \in f(J)$ için,

$$\begin{aligned} sx &= f(r)f(a) = f(ra) \in f(J) \quad \text{ve} \\ xs &= f(a)f(r) = f(ar) \in f(J) \end{aligned}$$

olduğu göz önüne alınarak, $f(J)$ nin S nin bir ideali olduğu anlaşılır.

Şimdi J yi, R nin $K = Çek\ f$ yi kapsayan bir ideali olarak alalım. $f(J) = I$ de S nin bir ideali ve $f^{-1}(I) = f^{-1}(f(J)) = J$ olduğunu gösterirsek, yukarıdaki fonksiyonun örten olduğu da gösterilmiş olur.

$J \subset f^{-1}(f(J))$ olduğu açıktır. Şimdi ters kapsamayı gösterelim.

$$\begin{aligned} x \in f^{-1}(f(J)) &\Longrightarrow f(x) \in f(J) \\ &\Longrightarrow f(x) = f(a), \exists a \in J \\ &\Longrightarrow f(x) - f(a) = f(x-a) = 0, \\ &\Longrightarrow x - a \in K = Çek\ f \subset J, \quad (a \in J) \\ &\Longrightarrow x \in J \end{aligned}$$

olduğundan, $f^{-1}(f(J)) \subset J$ elde edilir.

Son olarak I, S nin bir ideali olmak üzere, $f^{-1}(I) = J$ için; $R/J \cong S/I$ olduğunu gösterelim.

$\phi : R \longrightarrow S/I$ fonksiyonunu, $\phi(r) = f(r) + I$ ile tanımlayalım. $f : R \longrightarrow S$ örten homomorfizma olduğundan, ϕ nin de örten bir homomorfizma olduğunu görmek kolaydır. $r \in R$ için,

$$\begin{aligned} r \in Çek\ \phi &\Longleftrightarrow \phi(r) = f(r) + I = I \\ &\Longleftrightarrow f(r) \in I \Longleftrightarrow r \in f^{-1}(I) = J \end{aligned}$$

olduğundan, $Çek\ \phi = J$ ve homomorfizma teoreminden $R/J \cong S/I$ elde edilir.

Tanım 4.3.4 Birimli bir halkanın, biriminin ürettiği alt halkaya halkanın **asal alt halkası** denir.

Asal alt halka, halkanın en küçük alt halkasıdır.

Önerme 4.3.3 Bir tamlık bölgesi; karakteristiği sıfır olan bir asal alt halkaya sahip ise $\mathcal{Z}$ ye, karakteristiği p asal tam sayısı olan bir asal alt halkaya sahip ise $\mathcal{Z}_p$ ye izomorf alt halka kapsar.

İspat: R bir tamlık bölgesi olsun. $\forall n \in \mathcal{Z}$ için, $f(n) = n1_R$ ile tanımlı $f : \mathcal{Z} \longrightarrow R$ fonksiyonunun bir homomorfizma olduğu kolaylıkla gösterilebilir.

Eğer R nin karakteristiği sıfır ise Çek $f = (0)$ olacağından, f 1-1 ve dolayısı ile $\mathcal{Z} \cong f(R) \subset R$ dir.

Eğer R nin karakteristiği p asal tam sayısı ise, Çek $f = (p)$ ve dolayısı ile homomorfizma teoremine göre, $\mathcal{Z}/(p) = \mathcal{Z}_p \cong f(R) \subset R$ dir.

4.3 ALIŞTIRMALAR

1-) $f : R \longrightarrow S$ sıfırdan farklı bir homomorfizma, R birimli bir halka ve S bir tamlık bölgesi ise $f(1_R) = 1_S$ olduğunu gösteriniz.

2-) R birimli bir halka ise $\forall n \in \mathcal{Z}$ için, $f(n) = n1_R$ ile tanımlı $f : \mathcal{Z} \longrightarrow R$ fonksiyonunun bir homomorfizma olduğunu gösteriniz.

3-) $f : R \longrightarrow S$ bir örten homomorfizma olsun. J, R nin bir ideali ise $f(J)$ nin de S nin bir ideali olduğunu gösteriniz.

4-) $f : R \longrightarrow S$ bir homomorfizma olsun. I, S nin bir ideali ise $f^{-1}(I)$ nın da R nin bir ideali olduğunu gösteriniz.

5-) $\forall a + b\sqrt{2} \in \mathcal{Z}[\sqrt{2}]$ için, $f(a + b\sqrt{2}) = a - b\sqrt{2}$ ile tanımlı $f : \mathcal{Z}[\sqrt{2}] \longrightarrow \mathcal{Z}[\sqrt{2}]$ fonksiyonunun bir izomorfizma olduğunu gösteriniz.

6-) $\forall a, b \in \mathcal{Z}$ için, $a \oplus b = a + b + 1$ ve $a \odot b = ab + a + b$ olsun. $(\mathcal{Z}, \oplus, \odot)$ nın bir halka ve $(\mathcal{Z}, +, .)$ ile izomorf olduğunu gösteriniz.

7-) $f : R \longrightarrow S$ bir izomorfizma ise $f^{-1} : R \longrightarrow S$ nin de bir izomorfizma olduğunu gösteriniz.

8-) İki homomorfizmanın bileşkesinin de bir homomorfizma olduğunu gösteriniz.

9-) $f : R \longrightarrow S$ bir homomorfizma olsun. f nin 1-1 olması için gerek ve yeter koşul Çek $f = (0_R)$ olmasıdır, gösteriniz.

10-) Bir temel ideal bölgesinin homomorf resminin de bir temel ideal bölgesi olduğunu gösteriniz.

11-) R birimli bir halka, $f : R \longrightarrow S$ örten bir homomorfizma ve $r \in R$ terslenebilsin. $f(r) \in S$ nin de terslenebilmesi için gerek ve yeter koşul $r \notin Çek\ f$ olmasıdır, gösteriniz.

12-) $f : R \longrightarrow S$ bir homomorfizma ve R bir cisim ise f nin ya sıfır homomorfizma, ya da 1-1 olduğunu gösteriniz.

13-) $f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ ile tanımlı $f : \mathbb{C} \longrightarrow \mathbb{R}_2^2$ fonksiyonunun bir 1-1 homomorfizma olduğunu gösteriniz.

4.4 KESİR CİSMİ

Bu kesimde bir tamlık bölgesinin kesir cisminden bahsedeceğiz. Tam sayılar tamlık bölgesinden, rasyonel sayılar cisminin inşa edilmesi gibi, bir tamlık bölgesi verildiğinde onu bir cisim içinde düşünebiliriz ve bu cismi en küçük cisim olarak alabiliriz.

Tanım 4.4.1 R ve S tamlık bölgeleri verildiğinde, R den S ye 1-1 bir homomorfizma bulunabiliyorsa R, S içine **gömülebilir** veya S, R nin bir **genişlemesidir** denir.

Önce bir cisim içinde bir D tamlık bölgesi verildiğinde, D yi kapsayan en küçük F cisminin veya D nin ürettiği F alt cisminin elemanlarının nasıl olacağını araştıralım.

Eğer $a, b \in D$ ve $b \neq o$ ise $ab^{-1} \in F$ olacağı açıktır. Ayrıca F cismi tam olarak böyle elemanlardan oluşur, yani

$$F = \{ab^{-1} \ : \ a, b \in D,\ b \neq 0\}$$

dir. Rasyonel sayılardan alışık olduğumuz şekilde ab^{-1} yerine $\frac{a}{b}$ şeklinde yazacak olursak, F deki işlemler de şöyledir:

$$\frac{a}{b} = \frac{c}{1} \Longleftrightarrow ad = bc,$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{ve} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Ayrıca $\forall a \in D$ için, $a = \frac{a}{1}$ şeklinde düşünerek, D yi de F nin içinde düşünebiliriz.

Şimdi bir D tamlık bölgesi verildiğinde, D nin bir cisim içine gömülebileceğini, yukarıdaki açıklamalar ışığında, kesin olarak ispatlıyalım.

Teorem 4.4.1 Her tamlık bölgesi bir cisim içine gömülebilir.

İspat: D bir tamlık bölgesi olsun. $D^* = D - \{0\}$ ile gösterelim.

$$D \times D^* = \{(a,b) \ : \ a,b \in D, \ b \neq 0\}$$

kümesi üzerinde bir denklik bağıntısı tanımlayalım. (a,b) çiftinin denklik sınıfının, yukarıdaki açıklamalar ışığında $\frac{a}{b}$ nin rolünü oynayacağına dikkat edelim.

$$(a,b) \sim (c,d) \Longleftrightarrow ad = bc$$

$\sim$ bağıntısının, $D \times D^*$ da bir denklik bağıntısı olduğunu göstermek kolaydır. (a,b) çiftinin denklik sınıfını a/b ile ve bütün denklik sınıfları kümesini F ile gösterelim. F üzerinde toplama ve çarpma işlemleri tanımlayıp cisim olduğunu gösterelim.

$$a/b + c/d = (ad + bc)/bd \quad \text{ve} \quad (a/b)(c/d) = ac/bd$$

ile tanımlansın. Bu tanımlar iyi tanımlıdır, yani toplama ve çarpma işlemleri sınıflardan alınan temsilcilere bağlı değildir. Bunun için şunları göstermek gerekir:

$a/b = a'/b'$ ve $c/d = c'/d'$ ise

$$(ad + bc)/bd = (a'd' + b'c')/b'd' \quad \text{ve} \quad ac/bd = a'c'/b'd'.$$

Bu eşitliklerin sağlanmasını okuyucuya bırakıyoruz.

Şimdi F nin bir cisim olduğunu ana hatları ile görelim.

1) $(F,+)$ bir değişmeli gruptur: İşlemin kapalılık, birleşme ve değişme özellikleri vardır. Sıfır eleman $(0_D, 1_D)$ çiftinin sınıfı yani $0/1$ dir. a/b sınıfının ters işaretlisi $-a/b$ dir.

2) F nin sıfırdan farklı elemanları kümesi F^*, çarpma işlemine göre bir değişmeli gruptur: İşlemin kapalılık, birleşme ve değişme özellikleri vardır. Birim eleman, $(1_D, 1_D)$ çiftinin sınıfı $1/1$ olarak alınabilir. $a, b \in D$, sıfırdan farklı elemanlar ise $(a/b)^{-1} = b/a$ olduğu gösterilebilir.

3) Çarpmanın, toplama üzerine dağılma özelliği gösterilebilir.

Son olarak D nin F içine gömülebileceğini görelim. $a \in D$ için $\phi(a) = a/1$ ile $\phi : D \longrightarrow F$ tanımlanırsa $\phi(1_D) = 1/1$ ve ϕ nin 1-1 homomorfizma olduğu gösterilebilir.

Tanım 4.4.2 Yukarıdaki teoremdeki F cismine D tamlık bölgesinin **kesir cismi** denir.

4.4 ALIŞTIRMALAR

1-) Teorem 4.4.1 de tanımlanan $\sim$ bağıntısının $D \times D^*$ de bir denklik bağıntısı olduğunu gösteriniz.

2-) Teorem 4.4.1 de F üzerinde tanımlı toplama ve çarpma işlemlerinin iyi tanımlı olduğunu gösteriniz.

3-) Teorem 4.4.1 de tanımlanan işlemlere göre F nin bir cisim olduğunu gösteriniz.

4-) K, D tamlık bölgesini kapsayan herhangi bir cisim ise K nın D nin kesir cismine izomorf bir alt cisim kapsadığını gösteriniz. Buna göre, F kesir cismi D yi kapsayan en küçük cisimdir.

4.5 POLİNOM HALKALARI

Polinomlar, matematikte önemli bir yer tutarlar. Liseden de polinomlarla ilgili birçok kavramla karşılaşılmıştır. Bu kesimde polinomların cebirsel özelliklerini inceleyeceğiz.

Tanım 4.5.1 R bir halka, x bir bilinmeyen ve $a_0, a_1, \ldots, a_k$ lar R nin elemanları olmak üzere,

$$a_0 + a_1 x + \ldots + a_k x^k$$

şeklindeki bir ifadeye R den katsayılı bir **polinom** denir. R den katsayılı tüm polinomlar kümesi $R[x]$ ile gösterilir.

Tanım 4.5.2 $p(x) = a_0 + a_1x + \ldots + a_kx^k$ ve $q(x) = b_0 + b_1x + \ldots + b_tx^t$, $R[x]$ de iki polinom olsunlar.

$$p(x) = q(x) \Longleftrightarrow \forall i \geq 0, a_i = b_i,$$

yani, polinomların eşitliği karşılıklı katsayıların eşit olması ile tanımlanır.

Örnek 1: R bir halka olsun. Bütün katsayıları sıfır olan polinoma **sıfır polinom** denir. R nin herbir elemanı da bir polinom olarak düşünülebilir. Bu polinomlara **sabit polinomlar** denir.

Bir polinomda sıfır katsayılı terimler yazılmayabilir.

Örnek 2: $p(x) = 1 - x + x^2 \in \mathcal{Z}[x]$ dir.

Tanım 4.5.3 $p(x) = a_0 + a_1x + \cdots a_nx^n \in R[x]$ ve $a_n \neq 0$ ise a_n ye polinomunun **baş katsayısı** ve n ye de polinomun **derecesi** denir. Sıfır polinomun derecesi $-\infty$ olarak tanımlanır. $p(x)$ polinomunun derecesi $d^0p(x)$ ile gösterilir.

Örnek 3: Sıfırdan farklı bir sabit polinomun derecesi 0 dır. Örnek 2 deki polinomun derecesi 2 dir.

Polinomlar arasında toplama ve çarpma, liseden alışık olduğumuz şekilde yapılır.

Tanım 4.5.4 $p(x) = a_0+a_1x+\ldots+a_mx^m, q(x) = b_0+b_1x+\ldots b_nx^n$ olsun. $\forall i \geq 0$ için, $c_i = a_i + b_i$ olmak üzere,

$$p(x) + q(x) = c_0 + c_1x + \ldots + c_tx^t$$

ile tanımlanır.

İki polinomun toplamı, karşılıklı katsayıların toplanması ile elde edilir.

Tanım 4.5.5 Yukarıdaki $p(x)$ ve $q(x)$ polinomları için, $\forall i \geq 0$ için, $c_i = a_ib_0 + a_{i-1}b_1 + \ldots a_0b_i$ olmak üzere,

$$p(x)q(x) = c_o + c_1x + \ldots + c_kx^k$$

ile tanımlanır.

Örnek 4: $p(x) = 1 - x + x^2, q(x) = x - x^2 + 2x^3 \in Z[x]$ için;

$$\begin{aligned} p(x) + q(x) &= 1 + 2x^3, \\ p(x)q(x) &= x - 2x^2 + 4x^3 - 3x^4 + 2x^5 \end{aligned}$$

dir.

Önerme 4.5.1 R bir halka ise $R[x]$ de bir halkadır.

İspat: $R[x]$ de tanımlanan toplama ve çarpma işlemlerine göre $R[x]$ in bir halka olduğunu göstermeyi okuyucuya bırakıyoruz.

Önerme 4.5.2 R bir halka olsun.
i) R birimli ise $R[x]$ de birimli,
ii) R değişmeli ise $R[x]$ de değişmeli ve
iii) R tamlık bölgesi ise $R[x]$ de tamlık bölgesidir.

İspat: i) R nin birimi 1_R ise $R[x]$ in de birimi, 1_R sabit polinomudur. Gerçekten, $\forall f \in R[x]$ için $f1_R = 1_R f = f$ olduğu açıktır.

ii) $\forall a, b \in R$ için $ab = ba$ ise $\forall p(x), q(x) \in R[x]$ için de $p(x)q(x) = q(x)p(x)$ olacağı, polinomlar arasındaki çarpma işleminin tanımından anlaşılır.

iii) R bir tamlık bölgesi olsun. Şu halde (i) ve (ii) den $R[x]$ birimli ve değişmeli halka olur. Eğer $R[x]$ de sıfır bölen olmadığını gösterirsek ispat tamamlanmış olur.

$f, g \in R[x]$ sıfır polinomdan farklı polinomlar olsun.

$$f = a_0 + a_1x + \ldots + a_mx^m, \quad (a_m \neq 0) \quad \text{ve} \quad g = b_0 + b_1x + \ldots b_nx^n,$$

$(b_n \neq 0)$ diyelim. $c_{m+n} = a_{m+n}b_0 + \ldots + a_mb_n + \ldots + b_{m+n}$ dir. $i > m$ için $a_i = 0$ ve $j > n$ için $b_j = 0$ olduğundan, $c_{m+n} = a_mb_n$ bulunur. R yi bir tamlık bölgesi ve $a_m \neq 0$, $b_n \neq 0$ kabul ettiğimizdan, $c_{m+n} = a_mb_n \neq 0$ olur. Şu halde $R[x]$ de, $f \neq 0$ ve $g \neq 0$ iken $fg \neq 0$ bulunduğundan sıfır bölen yoktur.

Sonuç 1: F bir cisim ise $F[x]$ bir tamlık bölgesidir.

Sonuç 2: R bir tamlık bölgesi ise $\forall f, g \in R[x]$ için,

$$d^0(fg) = d^0 f + d^0 g$$

dir.

Not: R tamlık bölgesi değil ise $d^0(fg) < d^0 f + d^0 g$ olabilir.

Örnek 5: $\mathcal{Z}_6$ da $f(x) = T - x + \bar{2}x^2$, $g(x) = \bar{2} - \bar{3}x$ olsun. $f(x)g(x) = \bar{2} - \bar{5}x + x^2$ dir $d^0 f = 2, d^0 g = 1$ ve $d^0(fg) = 2 < d^0 f + d^0 g = 3$ bulunur.

Tanım 4.5.6 $f(x) = a_0 + a_1 k + \ldots a_n x^n \in R[x]$ ve $r \in R$ olsun. $f(r) = a_0 + a_1 r + \ldots a_n r^n \in R$ ye f polinomunun r deki **değeri** denir. Eğer $r \in R$ için, $f(r) = 0$ ise r ye f polinomunun bir **kökü** denir.

Şimdi polinomlar halkasında **kalanlı bölme** veya **bölme algoritmasının** yapılabileceğini görelim.

Teorem 4.5.1 R değişmeli bir halka ve $f,\ g \in R[x]$ olsun. $g(x) \neq 0$ ve $g(x)$ polinomunun baş katsayısı terslenebilsin. Bu takdirde;

$$f(x) = q(x)g(x) + r(x) \quad \text{ve} \quad d^0 r < d^0 g$$

olacak şekilde tek türlü olarak belirli $\exists q, r \in R[x]$ polinomları bulunabilir.

İspat: $f(x) = a_n x^n + \cdots a_0$; $d^0 f = n$ ve $b_m^{-1} \in R$ olmak üzere, $g(x) = b_m x^m + \ldots b_0$; $d^0 g = m$ olsun.

Varlık: n üzerine tümevarım uygulayalım.

$n = 0$ olsun. $0 = d^0 f < d^0 g$ ise $q = 0$ ve $r = f$ alınabilir.

$0 = d^0 f = d^0 g$ ise $r = 0$, $q = a_0 b_0^{-1}$ alınabilir.

Tümevarım hipotezi olarak, derecesi n den küçük olan polinomlar için iddianın doğruluğunu kabul edelim. Genelliği bozmadan, $d^0 g \leq d^0 f$ alabiliriz. Çünkü, aksi halde $q = 0$, $r = f$ alınır.

$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ diyelim. $d^0 f_1 < n$ olduğundan, tümevarım hipotezine göre $\exists q_1, r \in R[x]$ ve $d^0 r < d^0 g$ vardır ki, $f_1(x) = q_1(x)g(x) + r(x)$ olur.

$$\begin{aligned} f(x) &= a_n b_m^{-1} x^{n-m} g(x) + q_1(x)g(x) + r(x) \\ &= [a_n b_m^{-1} x^{n-m} + q_1(x)]g(x) + r(x), \quad d^0 r < d^0 g \end{aligned}$$

olacak şekilde $q(x) = a_n b_m^{-1} x + n - m + q_1(x)ver(x) \in R[x]$ bulunmuş olur.

Teklik: $f(x) = q_1(x) + r_1(x) = q_2(x)g(x) + r_2(x)$, $d^0 r_1 < d^0 g$ ve $d^0 r_2 < d^0 g$ olsun. $(q_1(x) - q_2(x)g(x) = r_2(x) - r_1(x)$ eşitliğinden, $g(x)$ in baş katsayısı terslenebildiğinden, dereceleri karşılaştırılırsa,

$$d^0(r_2(x) - r_1(x) = d^0(q_1(x) - q_2(x) = d^0(q_1(x) - q_2(x) + d^0 g$$

bulunur. $d^0(r_2(x) - r_1(x)) < d^0 g$ olduğundan, son eşitlik ancak $q_1(x) = q_2(x)$ olması ile sağlanır. Dolayısı ile $r_1(x) = r_2(x)$ de elde edilir.

Sonuç 1: F, bir cisim ise $\forall f, g \in F[x], g \neq 0$ polinomuna bölme algoritması uygulanabilir.

Sonuç 2: $f \in R[x]$ ve $a \in R$ olsun. $f(x) = (x - a)q(x) + f(a)$ olacak şekilde bir ve yalnız bir $q(x) \in R[x]$ vardır.

İspat: $f(x)$ ve $x - a$ polinomlarına bölme algoritması uygulayalım. $f(x) = (x - a)q(x) + r(x)$ olacak şekilde $\exists q_1 r \in R[x]$ bulunabilir ve $d^0 r < d^0(x - a) = 1$, yani $r(x) = r \in R$ sabittir. Yukarıdaki eşitlikte $x = a$ alınırsa, $f(a) = r(a) = r$ bulunur ve $q(x)$ teklikle belirlidir.

Önerme 4.5.3 F bir cisim ve $f \in F[x]$, $d^0 f \geq 1$ olsun.
$(f) = f(x)F[x]$ temel ideali için $\frac{F[x]}{(f)}$ bölüm halkasının tam temsilciler sistemi olarak, $d^0 r < d^0 f$ olan $r \in F[x]$ polinomları alınabilir.

İspat: $\forall g \in F[x]$ polinomu için, f ile kalanlı bölerek;

$$g(x) = f(x)g(x) + r(x), \quad d^0 r < d^0 f$$

olacak şekilde $\exists q, r \in F[x]$ bulunabilir. Şu halde $g \equiv r(mod\ (f))$ dir. yani her $mod\ (f)$ denklik sınıfında $d^0 r < d^0 f$, olmak üzere $\exists r \in F[x]$ vardır.

Ayrıca $r_1 \neq r_2, d^0 r_1 < d^0 f, d^0 r_2 < d^0 f$ ise $r_1, r_2 \in F[x]$ polinomları aynı denklik sınıfında olamazlar. Gerçekten,

$$\begin{aligned} r_1 \equiv r_2(mod\ (f)) &\iff r_1 - r_2 \in (f) \\ &\iff r_1 - r_2 = fg \quad \exists g \in F[x] \end{aligned}$$

demektir. $d^0(r_1-r_2) \leq max\,(d^0r_1, d^0r_2) < d^0f$ olduğundan, yukarıdaki denklik, ancak $r_1 = r_2$ olması halinde sağlanır.

Sonuç olarak $\frac{F[x]}{(f)}$ bölüm halkası için,

$$\{r \in F[x] \ : \ d^0r < d^0f\}$$

kümesi her sınıftan bir ve yalnız bir eleman alınarak elde edilmiştir, yani bir **tam temsilciler sistemidir.**

Örnek 6: $f = 1+x+x^2 \in \mathcal{Z}_2[x]$ polinom için $\frac{\mathcal{Z}_2[x]}{(f)}$ bölüm halkasının tam temsilciler sistemi olarak,

$$\{\overline{a}+\overline{b}x \ : \ \overline{a},\overline{b} \in \mathcal{Z}_2\} = \{\overline{0},\ \overline{1},\ x,\ \overline{1}+x\}$$

alınabilir. Bu küme, 4 elemanlı bir kümedir.

$$\frac{\mathcal{Z}_2[x]}{(f)} = \{(f),\ \ \overline{1}+(f),\ \ x+(f),\ \ \overline{1}+x+(f)\}$$

olup, bölüm halkasının sıfırı olan (f) çıkarıldıktan sonra geri kalan elemanların çarpım tablosu aşağıdaki gibidir.

o	$\overline{1}+(f)$	$x+(f)$	$\overline{1}+x+(f)$
$\overline{1}+(f)$	$\overline{1}+(f)$	$x+(f)$	$\overline{1}+x+(f)$
$x+(f)$	$x+(f)$	$\overline{1}+x+(f)$	$\overline{1}+(f)$
$\overline{1}+x+(f)$	$\overline{1}+x+(f)$	$\overline{1}+(f)$	$x+(f)$

Bu tablodan $\frac{\mathcal{Z}_2[x]}{(f)}$ nin sıfırdan farklı elemanlarının çarpma işlemine göre bir değişmeli grup olduğu anlaşılır. Şu halde $\frac{\mathcal{Z}_2[x]}{(f)}$ bir cisimdir.

4.5 ALIŞTIRMALAR

1-) $\mathcal{Z}_6[x]$ de $f(x) = \overline{1} - x + 3x^2, g(x) = \overline{2} - \overline{3}x + 2x^2$ olduğuna göre $f+g$ ve fg polinomlarını bulunuz.

2-) $f(x) = x^3 - x$ polinomunun $\mathcal{Z}_6$ daki köklerini bulunuz.

3-) $\mathcal{Z}_5[x]$ de, $(\bar{1}+\bar{2}x+x^2)^2$ ve $(\bar{3}+x)(\bar{2}+x)$ polinomlarını bulunuz.

4-) $\mathcal{Q}[x]$ de $3x^3-x^2+2$ ve x^2-1 polinomlarına bölme algoritmasını uygulayınız.

5-) R bir halka ve $a \in R$ olsun. $\phi(f(x)) = f(a)$ ile tanımlı $\phi : R[x] \longrightarrow R$ fonksiyonunun bir örten halka homomorfizması olduğunu gösteriniz ve Çek ϕ yi bulunuz.

6-) R bir tamlık bölgesi ve F kesir cismi olsun. $\forall f \in F[x]$ için $f(x) = \frac{1}{a} f_0(x)$ olacak şekilde $\exists f_0 \in R[x]$, $\exists a \in R$ bulunabildiğini gösteriniz.

7-) R bir tamlık bölgesi ise $R[x]$ deki terslenebilir elemanların R deki terslenebilir elemanlar olduğunu gösteriniz.

8-) F cisim olmak üzere, $F[x]$ tamlık bölgesinin kesir cismini (tek değişkenli rasyonel fonksiyonlar cismi) bulunuz.

9-) $\forall f, g \in R[x]$ için $d^0(f+g) \leq max\ (d^0 f, d^0 g)$ olduğunu ve $d^0 f \neq d^0 g$ ise eşitlik sağlandığını gösteriniz.

10-) $\mathcal{Z}[x]$ de x ile 2 nin ürettiği ideali belirtiniz.

11-) R bir halka ve $a \in R$ olsun. $\frac{R[x]}{(x-a)} \cong R$ olduğunu gösteriniz.

12-) $\mathcal{Z}[x]$ ve $\mathcal{Z}[x]$ de 2. ve 3. dereceden tüm asal polinomları bulunuz.

13-) F bir cisim ise $F[x]$ de 1. dereceden tüm polinomların asal olduğunu gösteriniz.

14-) $f \in \mathcal{Q}[x]$ ve $d^0 f = 2, 3$ olsun. f nin $\mathcal{Q}[x]$ de asal olması için gerek ve yeter koşulun f nin $\mathcal{Q}$ da bir kökünün bulunmamasıdır, gösteriniz.

15-) $a_0 + a_2 x + \ldots + a_n x^n \in \mathcal{Z}[x]$ polinomunun bir $\frac{a}{b} \in \mathcal{Q}$ rasyonel kökü varsa $b|a_n$ ve $a|a_0$ olduğunu gösteriniz.

16-) $a_0 + a_2 x + \ldots + x^n \in \mathcal{Z}[x]$ polinomunun bir rasyonel kökü varsa tam sayı olacağını gösteriniz.

17-) $f \in \mathbb{R}[x]$ polinomunun, bir komplex kökü α ise α' komplex

eşleniğinin de kök olduğunu gösteriniz.

18-) Reel katsayılı bir polinom $\mathbb{R}[x]$ de asal ise derecesinin ≤ 2 olduğunu gösteriniz.

19-) $\mathbb{C}[x]$ deki asal polinomların birinci dereceden olduğunu gösteriniz.

20-) $\mathbb{Q}[x]$ de $\{2, x\}$ ile üretilen ideali bulunuz.

21-) R bir halka olsun.

$$R[[x]] = \{\sum_{i=0}^{\infty} a_i x^i \ : \ a_i \in R\}$$

kuvvet serilerinin kümesi üzerinde toplama ve çarpma işlemleri polinomlardaki gibi tanımlansın. $R[[x]]$ in bir halka olduğunu gösteriniz.

22-) F bir cisim ise,

a) $F[[x]]$ in, terslenebilen elemanlarını (aritmetik birimlerini) bulunuz.

b) $F[[x]]$ in her idealinin $n \geq 0$ olmak üzere $x^n F[[x]]$ şeklinde olduğunu gösteriniz.

4.6 HALKALARDA ARİTMETİK

Bölüm 2 de tam sayılar üzerinde yapılan aritmatiği, herhangi bir tamlık bölgesine genelleştirmeye çalışalım. Bu kesimde R halkasını, bir tamlık bölgesi olarak alacağız.

Tanım 4.6.1 $a, b \in R$ için, $a = bc$ olacak şekilde $\exists c \in R$ varsa, b, a yı böler denir ve $b|a$ ile gösterilir.

Önerme 4.6.2 $\forall a, b, c \in R$ için,

i) $a|b$ ve $b|c \Longrightarrow a|c$,

ii) $a|b \Longrightarrow \forall c \in R, a|bc$,

iii) $a|b$ ve $a|c \Longrightarrow \forall x, y \in R, a|xb + yc$ dir.

İspat: Bölünebilmenin tanımı göz önünde tutularak, tam sayılarda yapılan ispata benzer şekilde ispatlanır.

Tanım 4.6.2 Bir R tamlık bölgesinin tüm elemanlarını bölen R nin bir elemanına **aritmetik birim** veya **birimsel eleman** denir ve R nin tüm aritmetik birimleri kümesi U_R ile gösterilir.

Önerme 4.6.3 R nin aritmetik birimleri, R deki terslenebilen elemanlardan ibarettir.

İspat: i) Önce bir aritmetik birimin terslenebildiğini gösterelim. $u \in U_R$ ise tanıma göre, R deki her elemanı böler.

Özel olarak $u|1_R \Longrightarrow 1_R = uu'$, $\exists u' \in R$ vardır. Şu halde u terslenebilir.

ii) Şimdi terslenebilen bir elemanın bir aritmetik birim olduğunu gösterelim. u nun tersi var ve $u^{-1} \in R$ olsun.

$uu^{-1} = 1_R \Longrightarrow u|1_R$ olduğundan, Önerme 4.6.2 (ii) ye göre $u|1_R a = a$, $\forall a \in R$ bulunur. Şu halde $u \in U_R$ dir.

Sonuç: R nin aritmetik birimleri kümesi U_R, R de çarpımsal bir gruptur.

Bölünebilme açısından, bir elemanın bir aritmetik birimle çarpılması sonucu değiştirmez. Onun için şu tanımı yapalım.

Tanım 4.6.3 $a, b \in R$ için, $b = au$ olacak şekilde R de bir u aritmetik birimi varsa, a, b ile **ilgilidir** denir ve $a \approx b$ ile gösterilir.

Önerme 4.6.4 R de ilgili olma bağıntısı bir denklik bağıntısıdır.

İspat: Aşağıdaki özelliklerin sağlandığını görmek kolaydır:
i) Yansıma: $\forall a \in R$ için, $a \approx a$ dır.
ii) Simetri: $a, b \in R$ için, $a \approx b$ ise $b \approx a$ dır.
iii) Geçişme: $a, b, c \in R$ için, $a \approx b$ ve $b \approx c$ ise $a \approx c$ dir.

Önerme 4.6.5 $a, b \in R$ olsun.
i) $a|b \Longleftrightarrow (b) \subset (a)$
ii) $b \neq 0$ olsun. $a|b$ ve $b|a \Longleftrightarrow a \approx b$ dir.

İspat: i) $a|b \iff b = ac,\ \exists c \in R \iff b \in (a) \iff (b) \subset (a)$.

ii) $a|b$ ve $b|a \implies b = ac$ ve $a = bd, \exists c, d \in R$ olduğundan $b = (bd)c \implies 1 = dc \implies c, d \in U_R$ olur. Şu halde $a \approx b$ dir.

Tersine $a \approx b$ olsun. $b = au, \exists u \in U_R$ olduğundan $a|b$ dir. $b = au \implies a = bu^{-1}, (u^{-1} \in R)$ olduğundan $b|a$ dır.

Tanım 4.6.4 R bir tamlık bölgesi ve $a, b \in R$ olsun.
i) $c|a$ ve $c|b$ olacak şekilde bir $c \in R$ varsa, c ye a ile b nin bir **ortak böleni** denir.
ii) c, a ile b nin bir ortak böleni olsun. Eğer a ile b nin bir **en büyük ortak böleni** , (e b o b) denir.

Önerme 4.6.6 $a, b \in R$ ve ebob leri c olsun. c', R nin c ile ilgili bir elemanı ise c' de a ile b nin bir ebob'leridir. Tersine olarak, a ile b nin ebob'leri ilgilidirler.

İspat: c, a ile b nin bir ebobleri $c' \in R$, $c' \approx c$ olsun. $c|c'$ ve $c'|c$ olduğu göz önünde tutularak, $c|a$ ve $c|b$ olmasından, $c'|a$ ve $c'|b$ olduğu görülür. d, a ile b nin herhangi bir ortak böleni d ise $c|d$ dir. Buradan $c'|d$ bulunur. Şu halde c' de bir ebob dir.

Tersine, c ve c'; a ile b nin iki ebobleri olsunlar. c bir ebob olarak düşünülürse c' ortak bölenini, c' bir ebob olarak düşünülürse c ortak bölenini böleceğinden $c|c'$ ve $c'|c$. Şu halde Önerme 4.6.5 (ii) ye göre $c \approx c'$ bulunur.

Not: İlgili elemanlar aynı bölünebilme özelliklerine sahip olduklarından, ilgililik düşünülmeksizin iki elemanın ebob leri varsa tektir. Bundan sonra a ile b nin ebob lerini (a, b) ile göstereceğiz. Ancak her tamlık bölgesinde ebob nin varlığından bahsedemeyiz.

Tanım 4.6.5 Ebob leri aritmetik birimler olan elemanlara **aralarında asal** denir ve $(a, b) = 1$ ile gösterilir.

TİB lerinde ebob nin varlığını gösterelim.

Önerme 4.6.7 R bir temel ideal bölgesi (TİB) olsun. R nin her

ikisi de sıfır olmayan her iki elemanın bir ebob leri vardır.

İspat: $a, b \in R$ ve a ile b nin ürettiği ideal, $I = (\{a, b\})$ olsun. R bir TİB olduğu için, $\exists c \in R$ vardır ki $I = (c)$ dir. a ve b nin her ikisi de sıfır olmadığından, $I = (c) \neq (0)$, yani $c \neq 0$ dır. Şimdi $(a, b) = c$ olduğunu gösterelim.

$$\begin{aligned} a, b \in I = (c) &\Longrightarrow a = cx,\ b = cy,\ \exists x, y \in R \\ &\Longrightarrow c|a \text{ ve } c|b \text{ dir.} \end{aligned}$$

Şu halde c, a ile b nin bir ortak bölenidir.

a ile b nin herhangi bir ortak böleni d olsun. R de a ile b nin ürettiği ideal

$$I = \{xa + yb \ : \ x, y \in R\} = (c)$$

olduğundan, $c = xa + yb$ olacak şekilde $\exists x, y \in R$ bulunabilir. $d|a$ ve $d|b$ olması nedeni ile $d|xa + yb = c$ elde edilir. Sonuç olarak $c = (a, b)$ bulunur.

Tam sayılarda olduğu gibi şu sonuca varabiliriz.

Sonuç 1: R bir TİB, a ve b ikisi de sıfır olmayan iki elemanı olsunlar. a ve b nin her ebob leri, $x, y \in R$ olmak üzere, $xa + yb$ şeklindedir. Özel olarak, $(a, b) = 1$ ise $1_R = xa + yb$ olacak şekilde $\exists x, y \in R$ bulunabilir.

Tanım 4.6.6 $x \in R, x \notin U_R$ ve $x \neq 0_R$ olsun. x in aritmetik birimlerden ve x ile ilgili elemanlardan başka bir böleni yoksa n elemanına R nin bir **asal elemanı** denir.

Önerme 4.6.8 R bir TİB, $a, b \in R$ ve π, R nin bir asal elemanı olsun.

$$\pi \mid ab \Longrightarrow \pi \mid a \text{ veya } \pi \mid b$$

dir.

İspat: Kabul edelim ki $\pi \nmid a$ olsun. Önceki önermeye göre (π, a) mevcuttur. $(\pi, a) = c$ diyelim. $c|\pi$ ve $c|a$ olacağından, π nin asal olduğu göz önünde tutularak, c nin ya π ile ilgili ya da aritmetik birim olduğu anlaşılır. Fakat $c \approx \Pi$ olsa, $c|a$ olduğundan $\pi|a$ çelişkisi elde

edileceğinden, $c \in U_R$ bulunur. Bu durumda, $(\pi, a) = 1$ ve Sonuç 1 e göre, $1 = x\pi + ya$ olacak şekilde $\exists x, y \in R$ bulunabilir.

Son eşitliğin her iki yanını b ile çarparak, $b = (bx)\pi + (ab)y$ ve

$$\pi|\pi \text{ ve } \pi|\text{ab} \Longrightarrow \pi|(\text{bx})\pi + (\text{ab})\text{y} = \text{b}$$

elde edilir.

Tanım 4.6.7 Bir R tamlık bölgesi aşağıdaki özellikleri sağlıyorsa R ye bir **tek türlü asal çarpanlara ayrılabilen bölge** denir ve kısaca TAÇ ile gösterilir.

i) R deki sıfır ve aritmetik birimlerden farklı her eleman R nin asal elemanlarının bir çarpımı olarak yazılabilir.

ii) (i) deki yazılış, çarpanların sırasını ve teklik düşünülmeksizin tek türlüdür.

Örnek 1: $\mathcal{Z}$, bir TAÇ bölgedir.

Teorem 4.6.1 R bir TİB ise TAÇ dır.

İspat: Önce TAÇ tanımındaki (i) özelliğini sağlayalım.

$0 \neq x \in R, x \notin U_R$ olsun. Olmayana ergi metodunu kullanarak, x in asal elemanların bir çarpımı olarak yazılamadığını kabul edelim. Şu halde x in kendisi de asal olamaz ve $x = ab$ olacak şekilde aritmetik birim olmayan $\exists a_1, a_1 \in R$ bulunabilir. x asallarının bir çarpımı olması kabulünden dolayı, a_1 ile b_1 den en az biri de bu özelliktedir. Kabul edelim ki a_1 bu özellikte olsun. $a_1|x$ olduğundan, Önerme 4.6.5 (i) ye göre $(x) \subset (a_1)$ dir. $b_1 \notin U_R$ olduğundan, Önerme 4.6.5 (ii) ye göre $(x) \neq (a_1)$ dir. Yukarıdaki işlemi x yerine a_1 alarak devam edilirse,

$$(a_0) = (x) \subset (a_1) \subset (a_2) \subset \ldots$$

şeklinde, herbiri bir sonrakinin içinde ve eşitliğin sağlanmadığı bir idealler zinciri elde edilir. $I = \cup_{i \geq 0}(a_i)$ nin de bir ideal olduğu gösterilebilir. Fakat R bir TİB olduğundan, $I = (a)$ olacak şekilde $\exists a \in R$ bulunabilir. $a \in I$ olacağından, $\exists k \geq 0$ için, $a \in (a_k)$ dolayısı ile $(a) \subset (a_k)$ bulunur. Diğer taraftan $(a_k) \subset I = (a)$ olduğundan, $I = (a) = (a_k) \subset\neq (a_{k+1})$ çelişkisi elde edilir. Şu halde başlangıçta

kabul ettiğimiz şekilde bir x elemanı yoktur. Yani $\forall 0 \neq x \in R$, $x \notin U_R$ elemanı bir takım asalların çarpımıdır.

Şimdi yazılışın tekliğini, yani TAÇ tanımındaki (ii) özelliğini sağlayalım.

π_i ve λ_j ler asallar olmak üzere $x = \pi_1\pi_2 \dots \pi_s = \lambda_1\lambda_2 \dots \lambda_t$ olsun. Önerme 4.6.8 göz önünde tutularak,

$$\pi|\lambda_1\lambda_2 \dots \lambda_t \Longrightarrow \exists i = 1, 2, \dots, t; \pi_1|\lambda_i \Longrightarrow \pi_1 \approx \lambda_i$$

olur. Sırayı ve ilgililiği göz önüne almadığımızdan, $\pi_1 = \lambda_1$ kabul edebiliriz. Tamlık bölgesinde kısaltma yapılabileceğinden, yukarıdaki eşitlikten π_1 ile λ_1 kısaltarak, $\pi_2 \dots \pi_s = \lambda_2 \dots \lambda_t$ bulunur.

$\pi_2|\lambda_2 \dots \lambda_t$ olduğundan, yukarıdaki düşünce ile $\pi_2 = \lambda_2$ alınabilir ve bu şekilde devam edilirse tüm π_i lerin, sıra ve ilgililik düşünülmeksizin, λ_j lerden biri olduğu anlaşılır. π_i ve λ_j lerin rolleri simetrik olduğundan $r = s$ olacağı da açıktır.

Genel olarak bir tamlık bmlgesinin TİB olup olmadığını araştırmak kolay değildir. Fakat $\mathcal{Z}$ deki gibi bir bölme algoritması mevcutsa, özel olarak tamlık bölgeleri TİB olur.

Tanım 4.6.8 R bir TİB olsun. Aşağıdaki özellikleri sağlayacak şekilde bir $d : R \longrightarrow \mathcal{Z}$ varsa, R ye bir **Euclid Bölgesi** denir ve kısaca EB ile gösterilir.

i) $\forall x \in R$ için, $d(x) \geq 0$,

ii) $d(x) = 0 \Longleftrightarrow x = 0_R$,

iii) $\forall x, y \in R$ için, $d(xy) = d(x)d(y)$,

iv) $\forall x, y \in R, y \neq 0_R$ için, $x = qy + r$ ve $0 \leq d(r) < d(y)$ olacak şekilde $\exists q, r \in R$ bulunabilir.

Tanım 4.6.9 Yukarıdaki tanımda (i), (ii) ve (iii) özelliklerini sağlayan bir d fonksiyonuna, R tamlık bölgesi üzerinde verilmiş bir **çarpımsal norm** ve (iv) özelliğine de **bölme algoritması** veya **Euclid algoritması** denir.

Örnek 2: $\mathcal{Z}$ bir EB dir. $d : \mathcal{Z} \longrightarrow \mathcal{Z}$ fonksiyonu olarak mutlak değer fonksiyonu alınabilir. (i), (ii) ve (iii) özelliklerinin sağlandığı

açıktır. (iv) özellik de Z deki bölme algoritmasından başka birşey değildir.

Örnek 3: F bir cisim olmak üzere, $F[x]$ polinomlar halkası bir EB dir. $F[x]$ in bir tamlık bmlgesi olduğunu biliyoruz.

$$d(f) = \begin{cases} 2^{\partial^0 f}; & f \neq 0 \text{ ise;} \\ 0\ ; & f = 0 \text{ ise} \end{cases}$$

ile tanımlı $d : F[x] \longrightarrow \mathcal{Z}$ fonksiyonunun (i), (ii) ve (iii) özelliklerini sağladığı kolaylıkla gösterilebilir. $\forall f, g \in F[x]$ ve $g \neq 0$ polinomları için.

$$f = qg + r, \quad \partial^0 r < \partial^0 g$$

olacak şekilde $\exists q, r \in F[x]$ bulunabilir. (Teorem 4.5.1, Sonuç 1) $\partial^0 r < \partial^0 g$ olduğundan, $0 \leq d(r) < d(g)$ eşitsizliği de sağlanır. (iv) özelliği de sağlandığından, $F[x]$ bir EB dir.

Teorem 4.6.2 R bir EB ise TİB dir.

İspat: R bir EB ve I herhangi bir ideali olsun.

$I = (0)$ ise temel ideal olacağından, $I \neq (o)$ alalım. I idealinde, sıfırdan farklı ve $d(a)$ en küçük tam sayı olacak şekilde bir $a \in I$ alalım. $a \in I \Longrightarrow (a) \subset I$ olur.

R bir EB olduğundan, $\forall x \in I$ için, $x = qa + r$ ve $0 \leq d(r) < d(a)$ olacak şekilde $\exists q, r \in R$ bulunabilir. Fakat $r \neq 0$ ise $r = x - qa \in I$ olduğundan, $d(r) < d(a)$ olması a nın seçimi ile çelişir. Şu halde $r = 0$, yani $x = qa \in (a)$ bulunur. Buradan, $I \subset (a)$ olur. Her iki kapsamadan $I = (a)$ temek ideal bulunur.

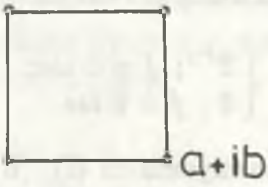
Sonuç 1: R bir EB ise TAÇ dır.

İspat: Teoreme göre EB $\Longrightarrow$ TİB ve Teorem 4.6.1 e göre TİB $\Longrightarrow$ TAÇ olduğundan, istenen elde edilir.

Tanım 4.6.10 $\mathcal{Z}[i] = \{a + bi : a, b \in \mathcal{Z}\}$ tamlık bölgesine **Gauss tam sayılar bölgesi** denir.

Önerme 4.6.9 $\mathcal{Z}[i]$ Gauss tam sayılar bölgesi bir EB dir.

İspat: $\mathcal{Z}[i] \subset C$ ve her $a+bi$ komplex sayısını düzlemde bir nokta olarak düşünebiliriz. Eğer $a, b \in \mathcal{Z}$, yani $a+bi/in\mathcal{Z}[i]$ ise bu noktalar, köşelerinin koordinatları tam sayılar olan birim karelerin köşeleridirler.



$d : \mathcal{Z}[i] \longrightarrow \mathcal{Z}$ fonksiyonunu,

$$d(a+bi) = |a+bi|^2 = a^2 + b^2$$

ile tanımlarsak, EB olma koşullarından (i), (ii) ve (iii), yani çarpımsal norm olma özelliklerinin sağlanacağı kolaylıkla gösterilebilir.

Son olarak (iv), bölme algoritmasının geçerliliğini gösterelim.

$\alpha, \beta \in \mathcal{Z}[i]$ ve $\beta \neq 0$ olsun. $\frac{\alpha}{\beta} \in C$ olup, düzlemde bir noktaya karşılık gelir. Bu noktanın kenarlarına veya içine düştüğü birim kareyi düşünelim. $\frac{\alpha}{\beta}$ ya en yakın olan köşe (bu köşe birden çok ise herhangi biri) $\gamma \in \mathcal{Z}[i]$ olsun.

$$|\frac{\alpha}{\beta} - \gamma| \leq \frac{\sqrt{2}}{2} \Longrightarrow |\frac{\alpha}{\beta} - \gamma|^2 \leq \frac{1}{2} \Longrightarrow |\alpha - \beta\gamma|^2 \leq \frac{1}{2}|\beta|^2 < |\beta|^2$$

olduğundan, $d(\alpha - \beta\gamma) < d(\beta)$ bulunur. $\alpha - \beta\gamma = \delta \in \mathcal{Z}[i]$ dersek, $\alpha = \beta\gamma + \delta$ ve $d(\delta) < d(\beta)$ olacak şekilde $\exists \gamma, \delta \in \mathcal{Z}[i]$ nin varlığı gösterilmiş olur.

Sonuç: $\mathcal{Z}[i]$ bir EB olması nedeni ile TİB ve TAÇ dır.

Son olarak, TAÇ olmayan bölgeye bir örnek verelim:

Örnek 4: $\mathcal{Z}[\sqrt{-5}] = \{a + bi\sqrt{5} \ : \ a, b \in \mathcal{Z}\}$ tamlık bölgesi TAÇ değildir.

$\forall \alpha = a + b_i\sqrt{5} \in \mathcal{Z}[\sqrt{-4}]$ için $d(\alpha) = |a + b_i\sqrt{4}|^2 = a^2 + 5b^2$ ile $d : \mathcal{Z}[\sqrt{-5}] \longrightarrow \mathcal{Z}$ fonksiyonu tanımlayalım. d nin bir çarpımsal norm olduğu gösterilebilir.

$$9 = 3^2 = (2 - \sqrt{-5})(2 - \sqrt{-5})$$

olduğundan; $3, 2+\sqrt{-5}$ ve $2-\sqrt{-5}$ elemanlarının $\mathcal{Z}[\sqrt{-5}]$ da asal olduklarını gösterirsek, $\mathcal{Z}[\sqrt{-5}]$ in TAÇ olmadığı anlaşılır.

$\alpha, \beta \in \mathcal{Z}[\sqrt{-5}]$ olmak üzere,

$$\alpha\beta = 3 \Longrightarrow d(\alpha\beta) = d(\alpha)d(\beta) = d(3) = 9$$

olduğundan, $d(\alpha) = 1, 3, 9$ olabilir.

$d(\alpha) = 3 = a^2 + 5b^2$ olacak şekilde $a, b \in \mathcal{Z}$ yoktur. (Neden ?). $d(\alpha) = 9$ ise $d(\beta) = 1$ olur.

$d(\alpha) = 1 \Longleftrightarrow 1 = a^2 + 5b^2 \Longleftrightarrow a = \pm 1, \quad b = 0 \Longleftrightarrow \alpha$ aritmetik birim olduğundan, 3 ün bölenlerinin aritmetik birimler ve kendisi ile ilgili olanlar olduğu, yani 3 ün asal olduğu anlaşılır.

Benzer şekilde $2+\sqrt{-5}$ ve $2-\sqrt{-5}$ in de asal oldukları gösterilebilir.

4.6 ALIŞTIRMALAR

1-) Bir tamlık bölgesinde ekok tanımlayınız. $a, b \in R$ nin ekok'ını $[a, b]$ ile gösterirsek, $u \in U_R$ olmak üzere $[a, b](a, b) = uab$ olduğunu gösteriniz.

2-) Bir R tamlık bölgesinde $a, b \in R$ için,

$$(a) = (b) \Longleftrightarrow a \approx b \quad \text{(ilgili)}$$

olduğunu gösteriniz.

3-) Bir TAÇ bölgede ekok ve ebob'i asal çarpanlara ayrılış ile ifade ediniz.

4-) R bir TAÇ bölge ise $\forall a, b, c \in R$ için,

$$(a, b) = 1 \quad \text{ve} \quad a \mid bc \Longrightarrow a \mid c$$

olduğunu gösteriniz.

5-) R bir EB olsun. $\forall a, b \in R$ için, $(a, b) = d$ nin varlığını ve $d = xa + yb$ olacak şekilde $\exists x, y \in R$ bulunabildiğini gösteriniz.

6-) R bir EB olsun. $a \in U_R$ ise $d(a) = d(1) = 1$ olduğunu gösteriniz.

7-) $\mathcal{Z}[\sqrt{-5}]$ ve $\mathcal{Z}[i]$ nin aritmetik birimlerini bulunuz.

8-) $\pi, \mathcal{Z}[i]$ nin bir asal elemanı ise $d(\pi)$ nin bir p asal sayısının kuvveti olduğunu gösteriniz.

9-) $\mathcal{Z}[i]$ de 5 ve 3+3 i elemanlarını asal çarpanlara ayırınız.

10-) $\mathcal{Z}[i]$ de 5-i ve 2+3 i nin ebob lerini bulunuz.

11-) n bir kare çarpanı olmayan herhangi bir pozitif tam sayı ve $\mathcal{Z}[\sqrt{-n}] = \{a + bi\sqrt{n} \ : \ a, b \in \mathcal{Z}\}$ olsun.

i) $d(a+bi\sqrt{n}) = a^2+nb^2$ ile tanımlı, $d : \mathcal{Z}[\sqrt{-n}] \longrightarrow \mathcal{Z}$ fonksiyonun bir çarpımsal norm olduğunu gösteriniz.

ii) $\alpha \in \mathcal{Z}[\sqrt{-n}]$ için $d(\alpha) = 1 \iff \alpha, \mathcal{Z}[\sqrt{-n}]$ de aritmetik birim olmasıdır, gösteriniz.

iii) $\mathcal{Z}[\sqrt{-n}]$ de aritmetik birim ve sıfırdan farklı her elemanın asal elemanlarının bir çarpımı olarak yazılabileceğini gösteriniz.

12-) 11. soruda $n > 0$, $\mathcal{Z}[\sqrt{n}] = \{a + b\sqrt{n} \ : \ a, b \in \mathcal{Z}\}$ ve $d(a + b\sqrt{n}) = |a^2 - nb^2|$ alarak yeniden cevaplayınız.

13-) $\mathcal{Z}[\sqrt{-5}]$ de $3|(2 + \sqrt{-5})(2 - \sqrt{-5})$, fakat $3 \not| 2 + \sqrt{-5}$ ve $3 \not| 2 - \sqrt{-5}$ olduğunu gösteriniz.

14-) $\mathcal{Z}[\sqrt{-5}]$ de $21 = 3.7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$ eşitliğinden yararlanarak, $\mathcal{Z}[\sqrt{-5}]$ in bir TAÇ bölge olmadığını gösteriniz.

15-) R bir tamlık bölgesi, $d : R \longrightarrow \mathcal{Z}$ bir çarpımsal norm olsun. $a \in R$ için, $d(a) = 1 \iff a \in U_R$ olduğunu gösteriniz. Bir $p \in \mathcal{Z}$ asalı için $d(\pi) = p$ olan $\pi \in R$ nin asallığını gösteriniz.

16-) $\pi, \mathcal{Z}[i]$ nin bir asal elemanı ise π nin bir ve yalnız bir p asal tam sayısını böldüğünü gösteriniz.

4.7 ASAL ÇARPANLARA AYRILIŞ

Bu kesimde polinom halkalarını daha detaylı olarak inceleyeceğiz. R aksi söylenmedikçe bu kesimde TAÇ bölge olarak alınacaktır. R de ebob varlığı ile (Bak.9.6 Alıştırma 2) aşağıdaki tanımı yapabiliriz.

Tanım 4.7.1 $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ polinomunun katsayılarının ebob ine f nin **kapsamı** denir ve $c(f)$ ile gösterilir. Eğer $c(f) = 1$ ise yani polinomun katsayıları aralarında asal iseler f ye **ilkel** polinom denir.

Önerme 4.7.1 $f \in R[x]$ ve $f \neq 0$ ise $f = c(f)f^*$ olacak şekilde $\exists f^* \in R[x]$ ilkel polinomu bulunabilir. Bu yanlış, aritmetik birimle çarpım düşünülmeksizin tek türlüdür.

İspat: $f = a_0+a_1x+\ldots+a_nx^n \in R[x]$ ve $c = c(f) = (a_0, a_1, \ldots, a_n)$ olsun. Şu halde, $i = 1, 2, \ldots, n$ için $a_i = ck_i$ ve $(k_0, k_1, \ldots, k_n) = 1$ olacak şekilde $\exists k_i \in R$ bulunabilir.

$$f^*(x) = k_0 + k_1x + \ldots + k_nx^n$$

istenen özelliktedir.

$f \in R[x]$ nin, R deki bir elemanla $R[x]$ deki bir ilkel polinomun çarpım olarak $f = cf^* = dg^*$ şeklinde iki yazılışı olsun. $c(f^*) = c(g^*) = 1$ olduğundan, her iki yanının kapsamları düşünülürse, $c(f) = c$ ve $c(f) = d$ olur. ebob'ler dolayısı ile kapsam ilgililik farkı ile tek olduğundan istenen elde edilir.

Önerme 4.7.2 $f, g \in R[x]$ ilkel iseler fg de ilkeldir.

İspat: $f = a_0 + a_1x + \ldots + a_nx^n$ ve $g = b_0 + b_1x + \ldots + b_mx^m$ olsun. $\forall i \geq 0$ için, $c_i = a_0b_i + a_1b_{i-1} + \ldots + a_ib_0$ olmak üzere,

$$fg = c_0 + c_1x + \ldots + c_{m+n}x^{m+n}$$

dir.

π, R nin bir asal elemanı olsun. f ilkel olduğu için a_i lerin, g ilkel olduğu için b_j lerin bazısı π ile bölünemez. a_i ve b_j, π ile bölünmemeyen ilk katsayılar olsunlar. Şu halde, $\pi \nmid a_i b_j$ dir.

$$c_{i+j} = a_0 b_{i+j} + \ldots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0$$

ve $0 \leq k < i$ için $\pi \mid a_k$, $0 \leq t < j$ için $\pi \mid b_t$ olduğundan $\pi \mid c_{i+j}$ olması $\pi \mid a_i b_j$ olmasını gerektirir. Bu ise π asal olduğu için $\pi \mid a_i$ veya $\pi \mid b_j$ demek olduğundan, a_i ve b_j nin seçimi ile çelişir. Şu halde c_k $(k = 1, 2, \ldots, m+n)$ lerin hepsini bölen R nin bir asal elemanı yoktur, yani $c(fg) = 1$ bulunur.

Önerme 4.7.3 F, R nin kesir cismi ve $f, F[x]$ in sıfır olmayan bir polinom olsun. $f = a^* f^*$ olacak şekilde $\exists a^* \in F$ ve $\exists f^* \in R[x]$ ilkel polinomu bulunabilir.

İspat: F nin her elemanı $a, b \in R$ ve $b \neq 0$ olmak üzere; $\frac{a}{b}$ şeklindedir. Şu halde $f \in F[x]$ polinomu f nin uygun bir elemanı ile çarparak $R[x]$ in bir polinomu yapılabilir. Önerme 4.7.1 kullanılarak verilen $f \in R[x]$ polinomu, F nin bir elemanı ile $R[x]$ in bir ilkel polinomunun çarpımı olarak yazılabilir.

Örnek 1: $f = \frac{1}{5}x^4 - \frac{2}{3}x^2 + \frac{1}{6}x + 1 \in Q[x]$ olsun. f polinomunu $[5, 3, 6] = 30$ ile çarparsak, $30f = 6x^4 - 20x^2 + 5x + 30 \in \mathcal{Z}[x]$ olur. $(6, 20, 5, 30) = 1$ ve $f = \frac{1}{30}(6x^4 - 20x^2 + 5x + 30)$ bulunur. Burada $\frac{1}{30} \in Q$, $6x^4 - 20x^2 + 5x + 30 \in \mathcal{Z}[x]$ ise ilkeldir.

Önerme 4.7.4 $f \in R[x]$ ilkel bir polinom olsun. f nin $R[x]$ de asal olması için gerek ve yeter koşul F, R nin kesir cismi olmak üzere, f nin $F[x]$ de asal olmasıdır.

İspat: $\Longrightarrow$: $f \in R[x]$ ilkel bir asal olsun. $g, h \in F[x]$ için, $f = gh$ kabul edelim. Önerme 4.7.3 e göre $g = a^* g^*$ ve $h = b^* h^*$ olacak şekilde $\exists a^*, b^* \in F$ ve $\exists g^*, h^* \in R[x]$ ilkel polinomları bulunabilir. Burada $f = (a^* b^*) g^* h^*$ ve Önerme 4.7.2 ye göre iki ilkel polinomun çarpımı da ilkel olduğundan, $g^* h^* \in R[x]$ ilkeldir. $f = (a^* b^*) g^* h^*$ eşitliğin her iki yanının kapsamını düşünerek $a^* b^* = 1$ olduğu gösterilebilir. $f = g^* h^*$ ve f yi asal aldığımızdan f^* veya g^* dan birinin $R[x]$ de sabit, dolayısı

ile f veya g den birinin $F[x]$ de sabit olduğu anlaşılır. Şu halde f, $F[x]$ de asaldır.

$\Longleftarrow$: $f \in F[x]$ in asal olduğunu kabul edelim. f nin $R[x]$ de bir ayrışımı $g, h \in R[x]$ için $f = gh$ olsun. $R[x] \subset F[x]$ olduğundan, g veya h dan birinin $F[x]$ de birim, yani sabit polinom olduğu görülür. Diyelim ki g sabit polinom ve $g \in R$ olsun. $f = gh$ ve f ilkel olduğundan $g \in U_R$ de asaldır.

Önerme 4.7.5 R bir TAÇ bölge ve f, $R[x]$ in ilkel bir polinomu olsun. f, $R[x]$ de asal elemanların çarpımı olarak yazılabilir ve bu yazılış tek türlüdür.

İspat: R nin kesir cismi F olsun. $F[x]$ TAÇ bölge olduğundan; $f_1, f_2, \ldots, f_h \in F[x]$ in asal polinomlar olmak üzere, $f = f_1, f_2, \ldots f_h$ şeklinde yazılabilir. Önerme 4.7.3 e göre, $i = 1, 2, \ldots, k$ için $f_1 = a_i^* g_i$ olacak şekilde $a_i^* \in F$ ve $g_i \in R[x]$ ilkel polinomları bulunabilir. f_i ler $F[x]$ de asal olduğundan g_i ler de $F[x]$ de asaldırlar. Önerme 4.7.4 e göre, g_i ler $R[x]$ de de asal olurlar. Buradan;

$$f = f_1 f_2 \ldots f_k = (a_1^* a_2^* \ldots a_k^*) g_1 g_2 \ldots g_k$$

bulunur. $a_1^* a_2^* \ldots a_k^* = a \in F$ olduğundan, $a = a_1/a_2$ olacak şekilde $a_1, a_2 \in R, a_2 \neq 0$ elemanları bulunabilir. Buradan $a_2 f = a_1 g_1 g_2 \ldots g_k$ elde edilir. f ve $g_1 g_2 \ldots g_k$ ilkel polinom olduklarından, sol ve sağ tarafın kapsamları düşünülerek, $a_2 = a_1$ bulunur ve $f = g_1 g_2 \ldots g_k$ elde edilir.

Şimdi f nin $R[x]$ de asal çarpanlara ayrılışının tek olduğunu göste relim. $r_1, r_2, \ldots, r_t \in R[x]$ in asal polinomları olmak üzere,

$$f = g_1 g_2 \ldots g_k = r_1 r_2 \ldots r_t$$

olsun. f ilkel olduğu için, r_i ler de ilkel olur. (Neden ?) Önerme 4.7.1 e göre r_i ler $F[x]$ de asaldırlar. Böylece f nin $F[x]$ de iki asal çarpanlara ayrılışı bulunmuş olur. Halbuki $F[x]$ TAÇ bölge olduğundan, bu bir çelişkidir.

Teorem 4.7.1 R bir TAÇ bölge ise $R[x]$ de TAÇ bölgedir.

İspat: f, $R[x]$ in sıfır olmayan herhangi polinom olsun. Önerme 4.7.1 e göre, $f = c(f) f^*$ olacak şekilde ilkel $\exists f^* \in R[x]$ bulunabilir.

Önerme 4.7.5 e göre f^*, $R[x]$ deki asal elemanların çarpımı olarak tek türlü yazılabilir. Şimdi $c = c(f) \in R$ nin $R[x]$ de asal çarpanlara ayrılışının nasıl olduğunu inceleyelim.

c nin $R[x]$ deki ayrılışı $c_1, c_2, \ldots, c_m \in R[x]$ olmak üzere $c = c_1 c_2 \ldots c_m$ olsun. $d^0 c = 0 = d^0 c_1 + \ldots + d^0 c_m$ eşitliğinden her $i = 1, 2, \ldots, m$ için $d^0 c_i = 0$ yani $c_i \in R$ bulunur. R, TAÇ bölge olduğundan c_i ler R de asal olmak üzere $c = c_1 c_2 \ldots c_m$ bulunur. R nin asalları $R[x]$ de de asal olduğu için böylece c nin $R[x]$ deki ayrılışı elde edilir. $f = cf^*$ eşitliğinden bu ayrılışlar yerine konularak teorem ispatlanmış olur.

Sonuç 1: R bir TAÇ bölge ise $R[x_1, x_2, \ldots, x_n]$ de bir TAÇ bölgedir.

İspat: $n = 1$ için teoremden ifade doğrudur.

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$$

olarak tanımlandığı için istenen tümevarımla görülür.

Sonuç 2: F bir cisim ise, $F[x_1, x_2, \ldots, x_n]$ de bir TAÇ bölgedir.

Örnek 2: F bir cisim ise Sonuç 1 den $F[x_1, x_2]$ TAÇ bölgesidir. Fakat TİB değildir. Gerçekten $F[x_1, x_2]$ de sabit terimi sıfır olan bütün polinomlar kümesinin, $F[x_1, x_2]$ nin bir ideali olduğu ve bu idealin $\{x_1, x_2\}$ nin ürettiği ideal olduğu gösterilebilir. Bu ideal temel ideal değildir. Çünkü $(\{x_1, x_2\}) = (f)$ olacak şekilde $\exists f \in F[x_1, x_2]$ bulunabilseydi, $x_1 = gf$ ve $x_2 = hf$ olacak şekilde $\exists g, h \in F[x_1, x_2]$ bulunabilirdi. Bu ise mümkün değildir. Onun için TİB olamaz.

Teorem 4.7.2 (Eisenstein Kriteri) R bir TAÇ bölge ve $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ bir ilkel polinom olsun. R de aşağıdaki özellikleri sağlayan bir π eleman varsa f, $R[x]$ de asaldır.

i) $\pi | a_0, a_1, \ldots, a_{n-1}$ dir.
ii) $\pi \nmid a_n$ dir.
iii) $\pi^2 \nmid a_0$ dır.

İspat: Kabul edelim ki $f \in R[x]$ de asal olmasın ve $R[x]$ de

$$a_0 + a_1 x + \ldots + a_n x^n = (b_0 + b_1 x + \ldots b_r x^r)(c_0 + c_1 x + \ldots + c_s x^s)$$

$(r+s=n, \quad r \geq 1, \quad s \geq 1)$ şeklinde yazılabilsin. $a_0 = b_0c_0$ ve $\pi^2 \nmid a_0$ olduğundan π, b_0 ve c_0 ın ikisini de bölmez. Fakat $\pi | a_0 = b_0c_0$ olduğundan, $\pi | b_0$ veya $\pi | c_0$ dır.

Kabul edelim ki $\pi \nmid b_0$ ve $\pi | c_0$ olsun. f ilkel olduğundan, $b_0 + b_1x + \ldots + b_rx^r$ ve $c_0 + c_1x + \ldots + c_sx^s$ de ilkel, dolayısı ile c_i lerin hepsi birden π ile bölünemez. Bu katsayılardan ilkini c_v ile gösterelim. Şu halde, $0 \leq i < v$ için $\pi | c_i$ ve (i) den $\pi | a_v$, $(v < n)$ dir.

$$a_v = b_0c_v + b_1c_{v-1} + \ldots + b_vc_0$$

eşitliğinden

$$\pi | b_0c_v = a_v - (b_1c_{v-1} + \ldots + b_vc_0)$$

elde edilir. Halbuki $\pi \nmid c_v$ ve $\pi \nmid b_0$ olarak seçildiğinden bu bir çelişkidir. Şu halde f, $R[x]$ de asal olur.

Sonuç: Teoremin koşulları altında, R nin kesir cismi F ise f, $F[x]$ de de asaldır.

Örnek 3 : $x^4 + 3x^3 - 3x + 6 \in \mathcal{Z}[x]$ polinomu $\mathcal{Z}[x]$ ve $\mathcal{Q}[x]$ de asaldır.

4.7 ALIŞTIRMALAR

1-) R bir tamlık bölgesi ve F bir cisim ise $R[x]$ ve $F[x]$ halkalarının aritmetik birimlerini bulunuz.

2-) R bir TAÇ bölge ve $f, g \in R[x]$ olsun. $c(fg) = c(f)c(g)$ olduğunu gösteriniz. Bu eşitlikten yararlanarak, f ve g nin ilkel polinom olması için gerek ve yeter koşul fg nin ilkel olmasıdır, ispatlayınız.

3-) $\mathcal{Z}[x]$ de $\{3, x\}$ in ürettiği ideali belirleyiniz ve bu idealin bir temel ideal olmadığını gösteriniz.

4-) $\mathcal{Z}[x]$ in bir TAÇ bölge olduğunu gösteriniz.

5-) $f(x) \in \mathcal{Z}[x]$ ve $f(x+1) = g(x)$ olsun. $g(x), \mathcal{Z}[x]$ de asal ise $f(x)$ in de $\mathcal{Z}[x]$ de asal olduğunu gösteriniz.

6-) p asal olmak üzere, $x^{p-1} + x^{p-2} + \cdots + x + 1$ polinomunun $\mathcal{Z}[x]$ ve $\mathcal{Q}[x]$ de asal olduğunu gösteriniz.

7-) Aşağıdaki polinomları $\mathcal{Z}[x]$ de asal çarpanlara ayırınız.

a) $x^3 + 2x + 3$ $b)x^3 + 5x^2 + x + 2$ $c)x^3 + 2x^2 - 4x + 6$

8-) $Q[x]$ de aşağıdaki polinomların ebob lerini bulunuz.

a) $x^3 - 6x^2 + x + 4$, $x^5 - 6x + 1$
b) $x^2 + 1$, $x^4 + v - 1$

9-) $x^3 - 9$ polinomunun $\mathcal{Z}_{31}[x]$ de asal olduğunu gösteriniz.

10-) p asal tam sayı ise $x^n - p \in \mathcal{Z}[x]$ in $\mathcal{Z}[x]$ ve $\mathcal{Q}[x]$ de asal olduğunu gösteriniz.

11-) $f \in \mathcal{Z}[x]$ olsun. f nin $\mathcal{Q}[x]$ de derecesi f den küçük polinomların çarpımı olarak yazılabilmesi için gerek ve yeter koşul f nin $\mathcal{Z}[x]$ de aynı dereceden polinomların çarpımı olarak yazılabilmesidir.

4.8 ASAL VE MAKSİMAL İDEALLER

Tanım 4.8.1 R değişmeli, birimli bir halka ve P de R nin (1) den farklı bir ideali olsun.

$$a, b \in R; \quad ab \in P \Longrightarrow a \in P \text{ veya } b \in P$$

ise P ye R nin bir **asal ideali** denir.

Örnek 1: p asal tam sayı olmak üzere, (p) ideali $\mathcal{Z}$ nin bir asal idealidir.

Örnek 2: R bir TAÇ bölge ve π, R nin bir asal elemanı ise (π) ideali R nin bir asal idealidir.

Örnek 3: $\mathcal{Z}$ de (6) ideali asal değildir, çünkü $2.3 \in (6)$ fakat, $2 \notin (6)$ ve $3 \notin (6)$ dır.

Önerme 4.8.1 R bir TİB olsun.R nin bir (π) idealinin asal olması için gerek ve yeter koşul $\pi \in R$ nin asal veya sıfır olmasıdır.

İspat: $\Longrightarrow$: P, R nin bir asal ideali olsun. P, bir tamlık bölgesi olduğundan, $P = (0)$ ise P bir asal idealdir.

$P \neq (0)$ ve asal ideali $R = (1)$ den farklı aldığımızdan, $P = (a)$ olacak şekilde $\exists a \in R, a \neq 0$, $a \notin U_R$ bulunabilir. R bir TİB ve dolayısı ile bir TAÇ bölge olması nedeni ile π ler asal olmak üzere, $a = \pi_1\pi_2 \dots \pi_r$ şeklindedir. $r = 1$ ise istenen elde edilir.

$r \geq 2$ olsun. $b = \pi_1$ ve $c = \pi_2\pi_3 \dots \pi_r$ diyelim. Bu takdirde, $a = bc \in P$ fakat, $b \notin P$ ve $c \notin P$ dir. Çünkü, $b \in P$ kabul etsek, bir $d \in R$ için, $b = da = d(bc)$ olacağı için, $dc = 1$ yani, $c \in U_R$ bulunur ki bu bir çelişkidir. Benzer şekilde $c \in P$ olduğu da gösterilebilir. $bc \in P$ iken $b \notin P$ ve $c \notin P$ olması, P nin asal ideal oluşu ile çelişir. Şu halde $r = 1$, yani a asaldır.

$\Longleftarrow$: $\pi \in R$ asal ve $P = (\pi)$ olsun. $a, b \in R$ için, TİB de

$$ab \in (\pi) \Longrightarrow \pi | ab \Longrightarrow \pi | a \text{ veya } \pi | b$$

olduğundan, (π) asal idealdir.

Şimdi bir idealin asal olması için bir kriter ifade edelim:

Önerme 4.8.2 P değişmeli ve birimli bir R halkasının (1) den farklı bir ideali olsun. P nin asal olması için gerek ve yeter koşul R/P bölüm halkasının bir tamlık bölgesi olmasıdır.

İspat: $\Longrightarrow$: P bir asal ideal olsun. R değişmeli ve birimli bir halka olduğundan, R/P de değişmeli ve birimli bir halkadır. R/P nin bir tamlık bölgesi olduğunu göstermek için, içinde hiçbir sıfır bölen olmadığını göstermek yeter.

$a + P, b + P \in R/P$ ve $(a + P)(b + P) = ab + P = 0 + P$ olsun. Buradan, $ab \in P$ olduğu anlaşılır. P yi bir asal ideal olarak aldığımız için, $a \in P$ veya $b \in P$, yani $a + P = P$ veya $b + P = P$ bulunur. Şu halde, R/P de sıfır bölen yoktur.

$\Longleftarrow$: R/P nin bir tamlık bölgesi olduğunu kabul edelim. $a, b \in R$

için, $ab \in P$ olsun. R/P de sıfır bölen olmadığından,

$$P = ab + P = (a+P)(b+P) \implies a+P = P \text{ veya } b+P = P$$
$$\implies a \in P \text{ veya } b \in P$$

elde edilir. Şu halde, P bir asal idealdir.

Önerme 4.8.3 R bir TİB ve I, R nin (0) ve (1) den farklı bir ideali olsun. I, R nin asal ideallerinin bir çarpımı olarak yazılabilir ve bu yazılış sıra gözetmeksizin tek türlüdür.

İspat: $I = (a)$ ve $I \neq (0)$, $I \neq (1)$ olsun.$a \neq 0$, $a \notin U_R$ ve R, TAÇ bölge olduğundan, π ler asal olmak üzere $a = \pi_1\pi_2 \dots \pi_t$ şeklinde yazılabilir. Buradan,

$$(a) = (\pi_1\pi_2 \dots \pi_t) = (\pi_1)(\pi_2)\dots(\pi_t)$$

ve Önerme 4.8.1 e göre, (π_i) ler asal idealler olduğundan, alınan I ideali asal ideallerin bir çarpımı olarak yazılmış olur.

Şimdi bu yazılışın tekliğini gösterelim. π_i ve π_j' ler R nin asal elemanları olmak üzere;

$$I = (\pi_1)(\pi_2)\dots(\pi_t) = (\pi_1')(\pi_2')\dots(\pi_s')$$

olsun. Bu eşitlikten,

$$\pi_1\pi_2 \dots \pi_t = u\pi_1'\pi_2' \dots \pi_s', \ (u \in U_R)$$

olduğu görülür. R de asal çarpanlara ayrılışın tek türlü oluyşu nedeni ile $r = s$, π_i ve π_j' lerin ilgili, dolayısı ile $(\pi_i) = (\pi_j')$ elde edilir.

Bir tamlık bölgesinde, elemanların asal çarpanlara ayrılışı tek olmasa da, ideallerin asal ideallerin çarpımı olarak yazılışları tek türlü olabilir ve bu özellik de sayılar teorisinde önemli bir rol oynar.

Tanım 4.8.2 Her ideali, bir takım asal ideallerin çarpımı olarak tek türlü yazılabilen bir tamlık bölgesine bir **Dedekind bölgesi** denir.

Dedekind bölgesi üzerinde daha fazla durmayacağız. Yalnız şunu belirtelim ki $\mathcal{Z}[\sqrt{-5}]$ böyle bir tamlık bölgesidir.

Tanım 4.8.3 R değişmeli ve birimli bir halka ve M de R nin (1) den farklı bir ideali olsun.R nin, M yi kapsayan M ve R den başka hiçbir ideali yoksa, M ye R nin bir **maksimal ideali** denir.

Önerme 4.8.4 M, R nin bir (1) den farklı bir ideali olsun. M nin maksimal olması için gerek ve yeter koşul $\forall x \in R-M$ için, $M+(x) = R$ olmasıdır.

İspat: $\Longrightarrow$: M, R nin bir maksimal ideali olsun.

$$x \in R - M \Longrightarrow M \subset_{\neq} M + (x) \subset R$$

ve M maksimal olduğundan, $M + (x) = R$ bulunur.

$\Longleftarrow$: $\forall x \in R-M$ için, $M+(x) = R$ kabul edelim. M nin maksimal olduğunu göstermek için, R nin M yi kapsayan ve R den farklı her I idealinin M ye eşit olduğunu göstermek yeter.

$M \subset I$ ise $\exists x \in I - M$ ve hipotezden, $R = M + (x) \subset I$ ve $I \subset_{\neq} R$ aldığımız için, bir çelişki elde edilir. Şu halde $M = I$ dır.

Örnek 4: $\mathcal{Z}$ de, (5) bir maksimal idealdir. Çünkü, $\forall x \in \mathcal{Z} - (5)$ için, $(5) + (x) = \mathcal{Z}$ dir. Gerçekten, $(5, x) = 1$ olacağından, $\exists a, b \in \mathcal{Z}$ vardır ki $5a + xb = 1$ ve $(5) + (x) = (1) = \mathcal{Z}$ dir.

Şimdi bir idealin maksimal olması için bir kriter verelim.

Önerme 4.8.5 Birimli ve değişmeli bir R halkasının bir M idealinin, maksimal olaması için gerek ve yeter koşul R/M bölüm halkasının bir cisim olmasıdır.

İspat: M, R nin bir maksimal ideali olsun. $M \neq R$ olduğundan, $R/M \neq \{0 + M\}$ dir. $0 + M$ den farklı $\forall x + M \in R/M$ nin tersinin varlığını gösterirsek, R/M birimli ve değişmeli bölüm halkasının bir cisim olduğu anlaşılır.

$$x + M \neq 0 + M \Longrightarrow x \in R - M$$

ve Önerme 4.8.4 den, $M + (x) = R$ olduğundan, $m + ax = 1$ olacak şekilde $\exists m \in M$ ve $\exists a \in R$ bulunabilir. Şu halde $m = 1 - ax \in M$ ve

$(a+M)(x+M) = ax+M = 1+M$ den $x+M$ nin tersinin $a+M$ olduğu görülür.

$\Longleftarrow$: R/M bir cisim olsun. Şu halde, $R/M \neq (0+M)$ yani, $M \neq R$ dir. $\forall x \in R-M$ için, $x+M \neq 0+M$ ve R/M bir cisim kabul ettiğimizden,

$$(a+M)(x+M) = ax+M = 1+M \Longrightarrow 1-ax \in M$$

olacak şekilde $\exists a \in R$ bulunabilir. Şu halde, $1 \in M+(x)$ ve birimi kapsayan bir ideal R nin kendisi olduğundan, $M+(x) = R$ elde edilir. Önerme 4.8.4 gereğince M ideali maksimal bulunur.

Sonuç: Her maksimal ideal, bir asal idealdir.

İspat: M maksimal ise R/M bir cisim, dolayısı ile bir tamlık bölgesi olacağından, Önerme 4.8.2 gereğince M asaldır.

Fakat yukarıdaki sonucun tersi doğru değildir.

Örnek 5: F bir cisim olmak üzere, $F[x,y]$ bir TAÇ bölgedir. x asal polinomunun ürettiği (x) ideali asaldır. Fakat, $F[x,y]$ nin maksimal ideali değildir. Çünkü,

$$(x) \subset_{\neq} (x,y) \subset_{\neq} F[x,y]$$

dir.

Örnek 6: Z de sıfırdan farklı her asal ideal maksimaldir. Z deki sıfırden farklı asal idealler, p asal tam sayı olmak üzere, (p) ler olup, $\mathcal{Z}/(p) = \mathcal{Z}_p$ bir cisimdir. Şu halde (p) bir maksimal idealdir. (0) ideali ise Z nin bir asal ideali, fakat maksimal ideali değildir.

4.8 ALIŞTIRMALAR

1-) R bir TAÇ bölge olsun. $\pi \in R$ asal $\Longleftrightarrow$ (π) asal ideal olduğunu gösteriniz.

2-) TİB de sıfırdan farklı bir idealin asal olması için gerek ve yeter koşul maksimal olmasıdır.

3-) $f = x^3 - 3x + 1$ ise $\mathcal{Q}[x]/(f)$ nin bir cisim olduğunu gösteriniz.

4-) $f = x^3 - \bar{3}x + \bar{1} \in \mathcal{Z}_5[x]$ ise $\mathcal{Z}_5[x]/(f)$ nin sonlu bir cisim olduğunu gösteriniz.

5-) $\mathcal{Q}[x,y]$ de aşağıdaki ideallerin asal ve maksimal olup-olmadığını araştırınız.

a) $(x-1)$ b) $(x^2+1, y-1)$

6-) F bir cisim ve

$$\phi : F[x,y] \longrightarrow F,\ \phi(f) = f(0,0)$$

ile tanimlansın. ϕ nin bir örten homomorfizma ve

$$F[x,y]/(x,y) \cong F$$

olduğunu gösteriniz.

7-) $\mathcal{Z}[x]$ de (x) idealinin asal ve maksimal olup-olmadığını araştırınız.

8-) $\mathcal{Q}[x]$ de (x) idealinin asal ve maksimal olup-olmadığını araştırınız.

9-) $\mathcal{Z}[x]$ de $(6,x)$ idealinin asal olup-olmadığını araştırınız.

10-) $\mathcal{Z}[i]$ Gauss tam sayılar halkasının bir asal ideali P ise $P \cap \mathcal{Z}$ nin de $\mathcal{Z}$ nin bir asal ideali olduğunu gösteriniz. Bunun yardımı ile $\pi \in \mathcal{Z}[i]$ asal ise $\pi | p$ olacak şekilde bir p asal tam sayısının varlığını ve tekliğini gösteriniz.

11-) $\mathbb{Q}[x]$ de aşağıdaki ideallerin asal olup-olmadığını araştırınız.

12-) $f : R \longrightarrow S$ bir halka homomorfizması ve S sıfır bölensiz bir halka ise Çek f nin bir asal ideal olduğunu gösteriniz.

13-) $\phi : \mathbb{R}[x] \longrightarrow \mathbb{C}$, $\phi(f) = f(i)$ ile tanımlansın. $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{C}$ olduğunu gösteriniz.

14-) $\phi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\sqrt{2}]$, $\phi(f) = f(\sqrt{2})$ ile tanımlansın.

$$\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}]$$

olduğunu gösteriniz.

15-)R bir tamlık bölgesi, P bir asal ideal ve I_1, I_2, ..., I_r bir takım idealleri olsun.

$$I_1 I_2 \dots I_r \subset P \Longrightarrow \exists i = 1, 2, \dots, r;\ I_i \subset P$$

olduğunu gösteriniz.

BÖLÜM 5

CİSİMLER

Halkalar bölümünde, cismin özel bir halka olduğunu görmüştük. Cisim; birimli, değişmeli ve sıfırdan farklı her elemanın tersi olan bir halka idi. Cisim, cebir ve sayılar teorisinde önemli bir yer alır. Denklem çözümlerinde birçok uygulamaları vardır. Bu bölümde genel olarak cisim genişlemelerini tanımlayacak ve cebirsel sayı cisimleri üzerinde duracağız. Bu bölümde gerekli olan, Vektör Uzayları hakkındaki ön bilgiler Lineer Cebir kitaplarından edinilebilir.

5.1 CİSİM GENİŞLEMELERİ

Tanım 5.1.1. F bir cisim ve $S \subset F$ olsun. S kendi başına F cismindeki işlemlere göre bir cisim ise S ye F nin bir **alt cismi** denir.

Önerme 5.1.1 S, F cisminin en az iki elemanını kapsayan bir alt halkası olsun. S nin, F nin bir alt cismi olması için gerek ve yeter koşul $\forall s \in S, s \neq 0$ için, $s^{-1} \in S$ olmasıdır.

İspat: $\Longrightarrow$: S alt cisim ise sıfırdan farklı her elemanın tersinin S de olacağı tanımdan anlaşılır.

$\Longleftarrow$: S de sıfırdan farklı her elemanın tersinin S de olduğunu kabul edelim. S yi bir alt halka kabul ettiğimizden, çarpma işlemine göre kapalı da olacağından $S\{0\}$ kümesi, F nin çarpma işlemine göre bir alt

grubu olur. Şu halde S, F nin bir alt cismidir.

Sonuç: S, F nin bir alt cismi ise O_F ve $1_F \in S$ dir.

Tanım 5.1.2 Kendinden başka hiçbir alt cismi bulunmayan bir cisme **asal cisim** denir.

Örnek 1: $\mathcal{Q}$ rasyonel sayılar cismi bir asal cisimdir. Gerçekten S, Q nun bir alt cismi olsa, $1 \in S$ olacağından, $\mathcal{Z} \subset S$ ve sıfırdan farklı her tam sayının tersini de kapsayacağından, çarpma işleminin kapalılığından dolayı her rasyonel sayıyı da kapsar.

Örnek 2: p asal tam sayı ise $\mathcal{Z}_p$ bir asal cisimdir.

Önerme 5.1.2 Karakteristiği sıfır olan bir cismin asal olan cismi Q ya, karakteristiği p olan bir cismin asal cismi de $\mathcal{Z}_p$ ye izomorftur.

İspat: F bir cisim olsun. $f : \mathcal{Z} \longrightarrow F$, $f(n) = n1_F$ ile tanımlı fonksiyon, bir halka homomorfizmasıdır.

i) Eğer F nin karakteristiği sıfır ise

$$n.1_F = 0 \Longrightarrow n = 0$$

olacağından, $\mathcal{C}ek\ f = (0)$ dolayısı ile f, 1-1 olur. Homomorfizma teoremine göre, $\mathcal{Z} \cong f(\mathcal{Z}) \subset F$ bulunur. $\mathcal{Z}$ nin kesir cismi $\mathcal{Q}$ olduğundan, F nin $\mathcal{Q}$ ya izomorf bir alt cismi kapsadığı anlaşılır.

ii) Eğer F nin karakteristiği p asal tam sayısı ise yukarıdaki f homomorfizmasının çekirdeği, $\mathcal{Z}$ nin (p) asal idealidir. Gerçekten,

$$n.1_F = 0_F \Longleftrightarrow p|n \Longleftrightarrow n \in (p)$$

olacağından, $\mathcal{C}ek\ f = (p)$ dir. Homomorfizma teoremine göre,
$\mathcal{Z}/(p) = \mathcal{Z}_p \cong f(\mathcal{Z}) \subset F$ bulunur.

Tanım 5.1.3 F cismi bir K cisminin alt cismi ise K ya, F nin bir **genişlemesi** denir.

F ve K iki cisim, $F \subset K$ ise K ya F üzerinde bir vektör uzayı olarak düşünebiliriz.

Tanım 5.1.4 K, F nin bir genişlemesi ise $Boy_F K$ ya K nın F üzerindeki **derecesi** denir ve $[K : F]$ ile gösterilir.

Tanım 5.1.5 K, F nin bir genişlemesi ve $[K : F]$ sonlu ise genişlemeye **sonlu genişleme** denir.

Sonlu genişlemelerin dereceleri arasında aşağıdaki eşitlik sağlanır.

Önerme 5.1.3 L, K nın ve K, F nin sonlu genişlemeleri iseler $[L : F] = [L : K][K : F]$ dir.

İspat: $[K : F] = m$ ve $[L : K] = n$ olsun. $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$, K nın F üzerindeki bir tabanı ve $\{\beta_1, \beta_2, \ldots, \beta_n\}$ de L nin K üzerindeki bir tabanı kabul edelim.

$$\{\alpha_i \beta_j \ : \ 1 \leq i \leq m, \ \ 1 \leq j \leq n\}$$

nin de L nin F üzerindeki bir tabanı olduğunu gösterirsek, ispat tamamlanmış olur.

x, L nin herhengi bir elemanı olsun. $\{\beta_1, \beta_2, \ldots, \beta_n\}$, L nin K üzerindeki bir tabanı olduğundan,

$$x = b_1\beta_1 + b_2\beta_2 + \ldots + b_n\beta_n$$

olacak şekilde (tek türlü belirli) $b_i \in K$ lar bulunabilir.

Diğer taraftan $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$, K nın F üzerinde bir tabanı olduğundan, $\forall b_i \in K$ için;

$$b_i = \sum_{j=1}^{m} a_{ij}\alpha_j, \quad (i = 1, 2, \ldots, n)$$

olacak şekilde (tek türkü belirli) $a_{ij} \in F$ ile bulunabilir. Her iki eşitlikten;

$$x = \sum_{i=1}^{n}(\sum_{j=1}^{m} a_{ij}\alpha_j)\beta_i = \sum_{i=1}^{n} a_{ij}(\alpha_j\beta_i)$$

bulunur. Şu halde L deki her x elemanı, $\alpha_j\beta_i$ lerin bir lineer toplamı olarak yazılabilir, yani $\{\alpha_j\beta_i\}$ ler L nin F üzerindeki bir üreteç sistemidir.

Şimdi de $\{\alpha_j\beta_i\}$ lerin F üzerinde lineer bağımsız olduklarını gösterelim:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}\alpha_i = 0 \Longrightarrow \sum_{i=1}^{n}(\sum_{j=1}^{m} a_{ij}\alpha_j)\beta_i = 0$$

ve $\{\beta_i\}$ ler K üzerinde lineer bağımsız olduğundan, son eşitlikten;

$$\sum_{j=1}^{m} a_{ij}\alpha_j = 0, \quad (i = 1, 2, \ldots, n)$$

bulunur. $\{\alpha_j\}$ ler de Füzerinde lineer bağımsız olduğundan, son eşitlikten de $a_{ij} = 0, (i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m)$ elde edilir.

Sonuç: $F \subset K \subset L$ sonlu genişlemelerin bir zinciri ise;

$$[K : F] \mid [L : F]$$

dir. Şu halde $[L : F]$ derecesi asal ise L nin F ve kendinden başka ara cismi yoktur.

Tanım 5.1.6 K, F nin bir genişlemesi olsun. Bir $\alpha \in K$ için, $f(\alpha) = 0$ olacak şekilde, sıfır polinomdan farklı bir

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]$$

polinomu varsa α ya, F üzerinde bir **cebirsel eleman** denir. Cebirsel olmayan elemanlar da **transandant** denir.

Örnek 3: F nin her elemanı F üzerinde cebirseldir. Gerçekten, $\forall a \in F, f(x) = x - a \in F[x]$ polinomunun köküdür.

Örnek 4: $1 + i$ kompleks sayısı $\mathbb{Q}$ üzerinde cebirseldir. Gerçekten, $1 + i$, $f(x) = x^2 - 2x + 2 \in \mathbb{Q}[x]$ polinomunun bir köküdür.

Örnek 5: π sayısı, $\mathbb{Q}$ üzerinde cebirsel değildir. Bunun ispatını yapmayacağız. Şu halde π transandant bir elemandır.

Not: $\alpha \in K, F$ üzerinde bir cebirsel eleman ise $f(\alpha) = 0$ olacak şekilde bir $f(x) \in F[x]$ vardır. F cisim olduğundan, $F[x]$ bir TAÇ

bölgesidir. (Bak,) Şu halde $p_i(x)$ ler, $F[x]$ de farklı olmaları gerekmeyen bir takım polinomlar olmak üzere;

$$f(x) = p_1(x)p_2(x)\dots p_r(x)$$

şeklinde yazılabilir.

$$0 = f(\alpha) = p_1(\alpha)p_2(\alpha)\dots p_r(\alpha)$$

ve $p_i(\alpha) \in K$ cisminde sıfır bölen olmadığından, α nın $F[x]$ daki bir asal polinomun bir kökü olduğu anlaşılır. Gerekirse bu asal polinomun katsayılarını, baş katsayı ile bölerek, en yüksek derecedeki katsayıyı 1 yapabiliriz. Baş katsayısı 1 olan polinoma **monik polinom** denir. Şu halde aşağıdaki tanım yapılabilir.

Tanım 5.1.7 $F[x]$ de, F üzerinde cebirsel bir $\alpha \in K$ nın kök olduğu asal ve monik bir polinoma α nın sağladığı **minimal polinom** denir.

Önerme 5.1.4 F üzerinde cebirsel bir $\alpha \in K$ nın sağladığı minimal polinom teklikle belirli olup, minimal polinom, $F[x]$ de α yı kök kabul eden her polinomu böler.

İspat: Önce minimal polinomun tekliğini gösterelim. α nın kök olduğu farklı iki asal ve monik polinom $f_1, f_2 \in F[x]$ olsunlar. $(f_1, f_2) = 1$ ve $F[x]$ bir EB olduğundan,

$$1 = a(x)f_1(x) + b(x)f_2(x)$$

olacak şekilde $\exists a, b \in F[x]$ bulunabilir. $f_1(\alpha) = f_2(\alpha) = 0$ olduğundan, yukarıdaki eşitlikten bir çelişki elde edilir. Şu halde minimal polinom tekdir.

Şimdi α nın kök olduğu her $g(x)$ polinomunun, $f(x)$ minimal polinomu tarafından bölündüğünü gösterelim.

Eğer $f(x) \not| g(x)$ ise $f(x)$ asal polinomu olduğundan, $(f, g) = 1$ olur ve yukarıdaki şekilde bir çelişkiye gidilir.

Tanım 5.1.8 F üzerindeki cebirsel $\alpha \in K$ sağladığı minimal polinomu $P_F(\alpha, x)$ ile gösterelim. $d^0 P_F(\alpha_1 x)$ 'e α nın F üzerindeki derecesi denir.

Örnek 6: $1+i$ nin $\mathbb{Q}$ üzerindeki derecesi 3 ve $\sqrt[3]{2}$ nin $\mathbb{R}$ üzerindeki derecesi 1 dir. Çünkü

$$P_{\mathbb{Q}}(1+i,x) = x^2-2x+2, \quad P_{\mathbb{Q}}(\sqrt[3]{2},x) = x^3-2, \quad P_{\mathbb{R}}(\sqrt[3]{2},x) = x-\sqrt[3]{2}$$

dir.

Tanım 5.1.9 K, F nin bir genişlemesi ve $S \subset K$ alt kümesi verilsin. Knın F ve S yi kapsayan tüm alt cisimlerinin arakesiti (veya K nın $F \cup S$ ile üretilen alt cismi) $F(S)$ ile gösterilir.

Bu tanıma göre, $F(S)$ cismi F ve S yi kapsayan K nın en küçük alt cismidir.

Örnek 7: $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \ : \ a,b \in \mathbb{Q}\}$ olduğu gösterilebilir.

Önerme 5.1.5 $\alpha \in K$, F üzerinde cebirsel bir eleman ve $d^0 P_F(\alpha,x) = n$ olsun.

i) $(F(\alpha):F] = n$

ii) $F(\alpha)$ nın Füzerindeki bir tabanı $\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$ dir.

İspat: $\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$ in, $F(\alpha)$ nın F üzerindeki bir tabanı olduğunu gösterirsek, $[F(\alpha):F] = Boy_F(F(\alpha)) = n$ olduğu da gösterilmiş olur.

$$P_F(\alpha_1 x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} + x^n \in F[x]$$

olsun. α, bu polinomun bir kökü olduğundan,

$$\alpha^n = -c_0 - c_1\alpha - \cdots - c_{n-1}\alpha^{n-1}$$

dir. Tümevarımla, $\forall r \in \mathbb{N}$ için, $a_i \in \mathbb{Z}$ olmak üzere,

$$\alpha^r = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$$

olduğu gösterilebilir.

K nın $F \cup \{a\}$ ile üretilen alt halkası, yani F ve α yı kapsayan en küçük alt halka;

$$F[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \ : \ a_i \in F\}$$

olur. $F[\alpha] \subset F(\alpha)$ olacağı açıktır. Eğer $F[\alpha]$ nın bir cisim olduğunu gösterirsek, $F[\alpha] = F(\alpha)$ bulunur.

$0 \neq b \in F[\alpha]$ alalım. $\phi_\alpha : F[x] \longrightarrow F[\alpha]$ fonksiyonunu, $\phi_\alpha(f(x)) = f(\alpha)$ ile tanımlayalım. ϕ_α fonksiyonunun örten bir homomorfizma olduğu kolayca gösterilebilir.

$F[x]$ bir TİB olduğu için Çek ϕ_{alpha} bir temel idealdir. Çek $\phi_\alpha = (P_F(\alpha, x))$ olduğunu gösterelim. $(P_F(\alpha, x)) \subset$ Çek ϕ_α olduğu açıktır.

$$g \in \text{Çek } \phi_\alpha \Longrightarrow \phi_\alpha(g) = g(\alpha) = 0 \Longrightarrow P_F(\alpha, x) | g(x)$$

olduğundan, $g \in (P_F(\alpha, x))$ bulunur. Şu halde Çek $\phi_\alpha \subset (P_F(\alpha, x))$ dir. $P_F(\alpha, x)$ asal polinom olduğundan, Çek $\phi_\alpha = (P_F(\alpha, x))$ de bir asal idealdir.

TİB sinde asal ve maksimal idealler aynı olduğundan, (Bak, 4.8 Alıştırma 2). Çek ϕ_α bir maksimal ideal olur. Şu halde

$$\frac{F[x]}{\text{Çek } \phi_\alpha}$$

bir cisim ve homomorfizma teoremine göre;

$$\frac{F[x]}{\text{Çek } \phi_\alpha} \cong F[\alpha]$$

olduğundan, $F[\alpha]$ nın da bir cisim ve $F[\alpha] = F(\alpha)$ olduğu anlaşılır.

Sonuç olarak, $\forall x \in F(\alpha) = F[\alpha]$ nın

$$x = a_0 + a_1\alpha \ldots + a_{n-1}\alpha^{n-1}, (a_i \in F)$$

şeklinde yazılabildiği, yani $\{1, \alpha, \ldots, \alpha^{n-1}\}$ in $F(\alpha)$ nın bir üreteç sistemi olduğu görülür. Taban olduğunu göstermek için bu yazılışın tekliğini göstermek yeter.

$$x = a_0 + a_1 x + \ldots + a_{n-1}\alpha^{n-1} = b_o + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

$(a_i, b_i \in F)$ olsun. Bu eşitlikten;

$$(a_0 - b_0) + (a_1 - b_1)\alpha + \ldots + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0$$

bulunur. Bu eşitlik ise α nın,

$$g(x) = (a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_{n-1} - b_{n-1})x^{n-1} \in F[x]$$

polinomunun bir kökü olduğunu gösterir. Fakat $d^0 P_F(\alpha_1 x) = n$ ve $P_F(\alpha_1 x) \mid g(x)$ olduğundan; $a_0 = b_0, a_1 = b_1, \ldots, a_{n-1} = b_{n-1}$ elde edilir.

Tanım 5.1.10 $F(\alpha)$ cismine, F ye α katmakla elde edilen basit **genişleme** denir.

Tanım 5.1.11 K, F nin bir genişlemesi ve $\forall \alpha \in K$, F üzerinde cebirsel ise K ya Fnin bir **cebirsel genişlemesi** denir.

Önerme 5.1.6 Her sonlu genişleme bir cebirsel genişlemedir.

İspat: $[K : F] = n$ olsun. Herhangi bir $\alpha \in K$ alalım.
$1, \alpha, \alpha^2, \ldots, \alpha^n$ elemanlarının sayısı $n + 1 > n$ olduğundan, F üzerinde lineer bağlıdırlar. Şu halde, hepsi birden sıfır olmayan öyle $c_i \in F$ ler bulunabilir ki

$$c_0 + c_1\alpha + \ldots + c_n\alpha^n = 0,$$

yani α, $f(x) = c_0 + c_1 x + \ldots + c_n x^n \in F[x]$ polinomunun bir köküdür. Bu ise α nın F üzerinde cebirsel olması demektir.

Önerme 5.1.7 $\alpha_1, \alpha_2 \in K$, F üzerinde cebirsel iseler $\alpha_1 \mp \alpha_2$, $\alpha_1\alpha_2$ ve $\alpha_2 \neq 0$ ise $\frac{\alpha_1}{\alpha_2}$ de F üzerinde cebirseldirler.

İspat: α_1, F üzerinde cebirsel olduğundan,

$$[F(\alpha_1) : F] = d^0 P_F(\alpha_1, x)$$

(Önerme 5.1.5) dir. $F \subset F(\alpha_1) = K \subset F(\alpha_1, \alpha_2) = L$ genişleme zincirini düşünelim. $\alpha_2 \in K, F$ üzerinde cebirsel olduğundan $F(\alpha_1)$ üzerinde de cebirseldir. $L = K(\alpha_2)$ olduğundan,

$$[L : K] \leq d_F^0 P(\alpha_2, x)$$

ve Önerme 5.1.3'e göre;

$$[F(\alpha_1, \alpha_2) : F] \leq d^0 P_F(\alpha_1, x)\ d^0 P_F(\alpha_2, x)$$

dir. Şu halde $F(\alpha_1, \alpha_2)$, F nin sonlu bir genişlemesi ve Önerme 5.1.6 ya göre cebirsel bir genişlemedir. $\alpha_1 \mp \alpha_2$, $\alpha_1\alpha_2$, $\frac{\alpha_1}{\alpha_2} \in F(\alpha_1, \alpha_2)$ de F üzerinde cebirsel olur.

Tümevarımla yukarıdaki önermeyi genelleştirerek;

Sonuç: $\alpha_1, \alpha_2, \ldots, \alpha_n$ elemanları F üzerinde cebirsel iseler $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ cismi de F nin sonlu ve cebirsel bir genişlemesidir.

Tanım 5.1.12 Bir kompleks sayı Q üzerinde cebirsel ise **cebirsel** sayı denir.

Önerme 5.1.8 Tüm cebirsel sayılar kümesi bir cisimdir.

İspat: Önerme 5.1.7 den, tüm cebirsel sayılar kümesinin, kompleks sayılar cisminin bir alt cismi olduğu görülür.

Tanım 5.1.13 α bir cebirsel sayı olsun. $f(\alpha) = 0$ olacak şekilde bir,

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_n \in \mathcal{Z}[x]$$

polinomu varsa α ya **cebirsel tam sayı** denir.

Önerme 5.1.9 Bir rasyonel sayının, cebirsel tam sayı olması için gerek ve yeter koşul, tam sayı olmasıdır.

İspat: Her tam sayının bir cebirsel tam sayı olduğu açıktır. Şimdi gerekliliğini gösterelim.

$\frac{a}{b} \in Q, (a, b) = 1$ olsun. $\frac{a}{b}$ cebirsel tam sayı ise

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_n \in \mathcal{Z}[x]$$

için,

$$f(\frac{a}{b}) = \frac{a^n}{b^n} + a_1\frac{a^{n-1}}{b^{n-1}} + \ldots + a_n = 0$$

olur. Bu eşitliğin her iki yanını b^n ile çarparak,

$$a^n + a_1ba^{n-1} + \ldots + b^na_n = 0 \Longrightarrow a^n = -b(a_1a^{n-1} + \ldots + b^{n-1}a_n) \Longrightarrow b|a^n$$

elde edilir. Fakat baştan $(a, b) = 1$ kabul ettiğimiz için, $b \neq \mp 1$ ise $b|a^n$ bir çelişkidir. Şu halde $b = \mp 1$, yani $\frac{a}{b}$ bir tam sayı olmalıdır.

5.1 ALIŞTIRMALAR

1-) $[F(\alpha) : F]$ = sonlu olması için gerek ve yeter koşul α nın F üzerinde cebirsel olmasıdır, gösteriniz.

2-) $[\mathbb{Q}(\sqrt[3]{5}, i) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]$ ve $[\mathbb{Q}(i) : \mathbb{Q}]$ yı hesaplayınız.

3-) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ün $\mathbb{Q}$ üzerinde bir tabanını bulunuz.

4-) $\sqrt[3]{2} + \sqrt{3}$ ün $\mathbb{Q}$ üzerinde cebirsel olduğunu gösteriniz ve minimal polinomunu bulunuz.

5-) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$ olduğunu gösteriniz ve Q ile $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ cisimleri arasındaki ara cisimleri bulunuz.

6-) $\frac{\sqrt{2}-\sqrt{3}}{\sqrt{2}+\sqrt{3}}$ ün $\mathbb{Q}$ üzerindeki minimal polinomunu bulunuz.

7-) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = Q(\sqrt[6]{2})$ olduğunu gösteriniz.

8-) $x^4 - 2x^2 + 1$ polinomunun köklerini kapsayan, $\mathbb{Q}$ nun en küçük genişlemesini bulunuz.

9-) α, F üzerinde cebirsel bir eleman ise α yı kök kabul eden $\forall f \in F[x]$ polinomu için $d^0 P_F(\alpha, x) \leq d^0 f$ olduğunu gösteriniz.

10-) $[K : F] = 1 \iff K = F$ olduğunu gösteriniz.

11-) $F \subset K \subset L$ bir genişleme zinciri ve $\alpha \in L$, F üzerinde cebirsel ise K üzerinde de cebirsel olduğunu gösteriniz.

12-) $n_1 < n_2 < \ldots < n_r$ tam sayıları için,

$$[\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_r}) : \mathbb{Q}] \leq 2^r$$

olduğunu gösteriniz. Ne zaman kesin eşitsizlik olacağını araştırınız.

13-) $\zeta = e^{\frac{2\pi i}{8}}$ ise
a) $(\zeta + \zeta^{-1})^2 = 2$ ve
b) $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta)$ olduğunu gösteriniz.
c) $[\mathbb{Q}(\zeta) : \mathbb{Q}(\sqrt{2})]$ yi bulunuz.

14-) $\sqrt{1 + \sqrt{1 + \sqrt{3}}}$ ün $\mathbb{Q}$ üzerinde sağladığı minimal polinomu bulunuz.

15-) K, F nin bir cebirsel genişlemesi ve A, E nin F yi kapsayan bir alt halkası olsun. A nın bir cisim olduğunu gösteriniz. Eğer K, F nin bir cebirsel genişlemesi değil ise iddianın doğru olmadığını gösteriniz.

16-) $\alpha \in K$, F üzerinde cebirsel ve minimal polinomu $p(x) = P_F(\alpha, x)$ ise $F(\alpha) \cong \frac{F[x]}{(p(x))}$ olduğunu gösteriniz.

17-) $\mathbb{Q}(\sqrt[3]{2}) \cong \frac{\mathbb{Q}[x]}{(x^3-2)}$ olduğunu gösteriniz.

18-) $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[3]{24}) : \mathbb{Q}] = ?$

19-) $[\mathbb{Q}(\sqrt{2}, \sqrt{6}, \sqrt{10}) : \mathbb{Q}(\sqrt{2} + \sqrt{6})] = ?$

20-) $K = F(\alpha, \beta)$, Fnin cebirsel bir genişlemesi ve $f = P_F(\alpha, x)$ olsun. $(d^0 f, d^0 g) = 1$ ise,

a) $g(x)$ in $F(\alpha)[x]$ de asal,

b) $[K : F] = d^0 f . d^0 g$ olduğunu gösteriniz.

22-) α bir cebirsel sayı ise $n\alpha$ bir cebirsel tam sayı olacak şekilde bir $n \in \mathbb{Z}$ bulunabileceğini gösteriniz.

22-) α bir cebirsel sayı ve $m \in \mathbb{Z}$ olsun. $\alpha + m$ ve $m\alpha$ nın bir cebirsel tam sayı olduğunu gösteriniz.

23-) α, $x^3 + x + 1 = 0$ polinomunun ve β, $x^2 + x - 3 = 0$ polinomunun bir kökü ise $\alpha+\beta$ ve $\alpha\beta$ nın sağladığı polinomları bulunuz.

24-) Tüm cebirsel tam sayılar kümesinin, bir sayılabilir sonsuz küme olduğunu gösteriniz.

25-) F sonlu bir cisim ise F nin eleman sayısının, p bir asal sayı olmak üzere p nin bir kuvveti olduğunu gösteriniz.

26-) 9 elemanlı bir cisim inşa ediniz.

27-) 25 elemanlı bir cisim inşa ediniz.

5.2 NORMAL GENİŞLEMELER

F cisim ise F[x] in bir Euclid Bölgesi (E.B) olduğunu ve bir $f \in F[x]$ polinomunun, F cismi içinde en çok $d^o f = n$ tane kökü olabileceğini biliyoruz.

Önerme 5.2.1 $f \in F[x]$ derecesi ≤ 1 olan bir polinom ise F nin, f(x) polinomunun bir kökünü kapsayan bir genişlemesi vardır.

İspat: f(x) polinomunun bir asal böleni $f_1(x)$ ise $f_1(x)$ in bir kökü $f(x)$ in de bir kökü olacağından, genelliği bozmadan, bir asal polinomun kökünü kapsayan bir genişlemenin varlığını göstermek yeter.

$f(x)$ asal bir polinom olsun. $f(x)$ in $F[x]$ de ürettiği ideale I dersek, $I = (f) = f(x)F[x]$ asal bir ideal ve $F[x]$ bir TİB olduğundan, aynı zamanda maksimal bir idealdir. Şu halde $F[x]/I$ bir cisim olur.

$\phi : F \longrightarrow F[x]/I$, $f(a) = a + I$ ile tanımlı fonksiyonun 1-1 bir homomorfizma olduğunu göstermek kolaydır. $F[x]/I = K$ cismi, F ye izomorf $\phi(F)$ alt cismine sahiptir. İzomorfizmayı bir eşitlik gibi alarak, K yı F nin bir genişlemesi olarak düşünebiliriz. Ayrıca, $\alpha = x + I \in F[x]/I = K$ için

$$f(\alpha) = f(x) + I = I$$

eşitliğinden, $\alpha \in K$ nın f(x) in bir kökü olduğu anlaşılır.

Sonuç 1: $f \in F[x]$ olsun.

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i), \quad (\alpha_i \in K, \quad d^o f = n)$$

olacak şekilde F nin bir K genişlemesi vardır. Ayrıca, $[K : F] \leq n!$ dir.

İspat: Önermeden, F nin f(x) in bir α_1 kökünü kapsayacak şekilde bir K_1 genişlemesi var ve $[K_1 : F] \leq n$ dir. $f(x) = (x - \alpha_1)f_1(x)$ diyelim ve $f_1(x)$ için önermeyi tekrar kullanalım. K_1 in $f_1(x)$ in kökünü kapsayacak şekilde bir K_2 genişlemesi var ve $[K_2 : K_1] \leq n - 1$ dir. Bu şekilde devam ederek,

$$f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)g_n(x)$$

ve $\alpha_i \in K_n$, $g_n(x) \in K_n[x]$ olacak şekilde,

$$F \subset K_1 \subset K_2 \subset \ldots \subset K_n = K$$

genişlemeler zinciri elde edilmiş olur. Fakat, $d^o f = n$ kabul ettiğimiz için, $d^o g_n = 0$ dır. Genelliği bozmadan, f(x) monik polinom olarak alınabileceğinden $g_n = 1$ dir. Şu halde K cismi verilen f(x) polinomunun n kökünü de kapsayan bir genişleme ve

$$[K : F] = [K : K_{n-1}] \ldots [K_2 : K_1][K_1 : F] \leq n!$$

dir.

Bu sonucu tümevarımla genelleştirerek;

Sonuç 2: $f_1, f_2, \ldots, f_k \in F[x]$ polinomlarının tüm köklerini kapsayan, F nin bir K genişlemesi vardır.

Tanım 5.2.1 $f(x) \in F[x]$ nin tüm köklerini F ye katmakla elde edilen genişlemeye f nin F üzerindeki **parçalanış cismi** denir ve K_f ile gösterilir.

Sonuç 1 den, K_f nin varlığı ve $[K_f : F] \leq n!$ olduğu görülür. Ayrıca parçalanış cisimleri izomorfizma farkı ile tekdirler.

Tanım 5.2.2 Sabitten farklı her polinom $F[x]$ de lineer çarpanlara ayrılabiliyorsa F cismine **cebirsel kapalı cisim** denir.

Aşağıdaki teorem Cebirin Esas Teoremi olarak bilinir ve Gauss tarafından 19. yüzyılın başında ispatlanmıştır.

Teorem 5.2.1 Kompleks sayılar cismi cebirsel kapalı bir cisimdir.

Bundan sonra aksi belirtilmedikçe cisimlerimizi kompleks sayılar cisminin alt cisimleri olarak alacağız.

Örnek 1: $f(x) = x^3 - 2$ polinomunun Q üzerindeki parçalanış cismini bulalım.

$f(x) = x^3 - 2$ nin C deki kökleri; $w = (-1 + i\sqrt{3})/2$ olmak üzere $\sqrt[3]{2}$, $\sqrt[3]{2}w$, $\sqrt[3]{2}w^2$ dir. Şu halde $K_f = Q(\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2)$ dir.Bu

cismi daha basit olarak da ifade edebiliriz:

$$\sqrt[3]{2},\ \sqrt[3]{2}w \in K_f \Longrightarrow w \in K_f$$

ve

$$\sqrt[3]{2},\ \ w \in K_f \Longrightarrow Q(\sqrt[3]{2},\ w) \subset K_f$$

dir.

Tersine,

$$\sqrt[3]{2},\ w \in Q(\sqrt[3]{2},\ w) \Longrightarrow \sqrt[3]{2},\ \sqrt[3]{2}w,\ \ \sqrt[3]{2}w^2 \in Q(\sqrt[3]{2},\ \ w)$$

olduğundan,

$$K_f = Q(\sqrt[3]{2},\ \sqrt[3]{2}w,\ \ \sqrt[3]{2}w^2) \subset Q(\sqrt[3]{2},\ w)$$

dır. Şu halde parçalanış cismi,

$$K_f = Q(\sqrt[3]{2},\ w)$$

olarak alınabilir.

Şimdi $[Q(\sqrt[3]{2},\ w) : Q]$ derecesini hesaplayalım:
$[Q(\sqrt[3]{2}) : Q] = 3$ ve $[Q(w) : Q] = 2$ olduğundan, 5.1 Alıştırma 20 ye göre $[Q(\sqrt[3]{2},\ w) : Q] = 6$ bulunur.

Örnek 2: $f(x) = x^4 + x^2 + 1 \in Q[x]$ polinomunun kökleri $w = (-1+i\sqrt{3})/2$ olmak üzere; $\pm w,\ \pm w^2$ dirler. Şu halde f nin Q üzerindeki parçalanış cismi olarak, $Q(w)$ alınabilir ve Q üzerindeki derecesi 2 dir.

Örnek 3: p asal ise $f = x^p - 1$ polinomunun parçalanış cismini bulalım;

f nin kökleri; $\zeta = e^{2\pi i/p}$ olmak üzere, $1,\ \zeta,\ \zeta^2,\ \ldots,\ \zeta^{p-1}$ dirler. Tüm bu kökler $Q(\zeta)$ da kapsandığından, parçalanış cismi $Q(\zeta)$ bulunur.

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + x + 1)$$

p asal ise $x^{p-1} + x^{p-2} + \ldots + x + 1$, $Q[x]$ de asal olduğundan, ζ nın minimal polinomu;

$$P_Q(\zeta, x) = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$$

ve $[Q(\zeta) : Q] = p - 1$ bulunur.

Tanım 5.2.3: $f(x) = a_0 + a_1x + \ldots + a_rx^r$ polinomunun türevi formel olarak;

$$f'(x) = a_1 + 2a_2x^2 + \ldots + ra_rx^{r-1}$$

olarak tanımlanır.

Tanımdan türevin, analizden de bilindiği gibi şu özelliklere sahip olduğu gösterilebilir:

$\forall a, b \in F$, $\forall f, g \in F[x]$ için,

i) $(af + bg)' = af' + bg'$,

ii) $(fg)' = fg' + f'g$,

iii) $[(x - a)^k]' = k(x - a)^{k-1}$,

iv) $d^\circ f = d_\circ f' + 1$.

Önerme 5.2.2 f(x) in katlı bir kökünün olması için gerek ve yeter koşul, f(x) ile $f'(x)$ in $F[x]$ de, sabitten farklı bir ortak çarpanlarının bulunmasıdır.

İspat: $\Longrightarrow$: α, $f(x)$ in bir katlı kökü ve $f(x) = (x-\alpha)^k g(x)$, $k \leq 2$ olsun.

$$f'(x) = k(x - \alpha)^{k-1}g(x) + (x - \alpha)^k g'(x) =$$

olduğundan, $f'(\alpha) = 0$ bulunur.

f ve f' nün $F[x]$ de sabitten farklı bir ortak bölenleri yoksa,

$$1 = a(x)f(x) + b(x)f'(x)$$

olacak şekilde $\exists a, b \in F[x]$ bulunabilir. Bu eşitlikde $x = \alpha$ yerleştirilirse, $1 = 0$ çelişkisi elde edilir. Şu halde f ve f' nin $F[x]$ de sabitten farklı bir ortak bölenleri vardır.

$\Longrightarrow$: f ve f' nin $F[x]$ de sabitten farklı bir ortak çarpanları varsa, bu çarpanın bir kökünün hem f hem de f' nin bir ortak kökü olduğu anlaşılır. Şu halde f nin katlı bir kökü vardır. (Neden ?).

Önerme 5.2.3 $f \in F[x]$ asal polinomunun tüm kökleri basittir.

İspat: f nin katlı bir kökü olsa idi, önceki önermeye göre f ile f' nin $F[x]$ de sabitten farklı bir ortak bölenleri bulunurdu. Fakat f yi asal kabul ettiğimiz için, bu ortak bölen ancak f olabilir. $f|f'$ ise $d^0 f' < d^0 f$ olduğundan bu bir çelişkidir.

Aşağıdaki teorem karakteristiği sıfır olan cisimler için ilkel eleman teoremi olarak bilinir ve her sonlu genişlemenin bir basit genişleme olduğunu gösterir.

Teorem 5.2.2 $f = P_F(\alpha, x)$, $g = P_F(\beta, x)$ diyelim. f ve g nin L deki lineer çarpanlara ayrılışı;

$$f = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n), \quad (\alpha = \alpha_1)$$

$$g = (x - \beta_1)(x - \beta_2)\dots(x - \beta_m), \quad (\beta = \beta_1)$$

olsun. L de

$$\frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}, \quad (i \neq 1,\ j \neq 1)$$

lerin kümesini göz önüne alalım. Bunların sayısının sonlu ve $Q \subset F$ sonsuz elemanlı olduğundan, bunlardan farklı bir $t \in F$ bulunabilir.

$$\gamma = \alpha + t\beta \in K = F(\alpha, \beta) \Longrightarrow F(\gamma) \subset K$$

olduğu açıktır.

Ters kapsamayı göstermek için,

$$h(x) = f(\gamma - tx) \in F(\gamma)[x]$$

polinomunu düşünelim.

$$h(\beta) = f(\gamma - t\beta) = f(\alpha = 0 \Longrightarrow x - \beta | h(x)$$

dir. β dan başka hiçbir kök $h(x)$ in kökü olamaz. Gerçekten, $j > 1$ için, $h(\beta_j) = 0$ olsa, $f(\gamma - t\beta_j) = 0$ dolayısı ile $1 < j \leq n$ için, $\gamma - t\beta_j = \alpha_i$ bulunur. $\gamma = \alpha + t\beta$ koyarsak, $t = \frac{\alpha_i - \alpha}{\beta - \beta_j}$ çelişkisi elde edilir. Çünkü bu t nin seçimine aykırıdır.

Şu halde $x - \beta | h(x)$, fakat $j < 1$ için $x - \beta_j \not| h(x)$ dir. Buradan $L[x]$ de $h(x)$ ve $g(x)$ in ebob lerinin $x - \beta$ olduğu anlaşılır. $F(\gamma)[x]$ de $h(x)$ ve $g(x)$ in ebob lerinin de 1 ya da $x - \beta$ olabilir.

$(h,g) = 1$ olsa,

$$a(x)h(x) + b(x)g(x) = 1$$

olacak şekilde $\exists a, b \in F(\gamma)[x]$ bulunabilir. Bu eşitlikde, $x = \beta$ konursa $0 = 1$ çelişkisi elde edilir. Şu halde $(h,g) = x - \beta \in F(\gamma)[x]$ bulunur. Özel olarak, $\beta = \beta_1 \in F(\gamma)$ ve $\gamma t\beta = \alpha \in F(\gamma)$ olacağından, $F(\alpha,\beta) \subset F(\gamma)$ bulunmuş olur.

Tümevarımla şu sonuç elde edilir:

Sonuç: $K = F(\alpha_1, \alpha_2, \ldots \alpha_n)$, F nin bir cebirsel genişlemesi ise $F(\alpha_1, \alpha_2, \ldots \alpha_n) = F(\gamma)$ olacak şekilde bir $\gamma \in K$ vardır.

Tanım 5.2.4 α, F cismi üzerinde cebirsel ve minimal polinomu $f(x)$ olsun.

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n), \quad (\alpha_1 = \alpha)$$

ise $\alpha_1, \alpha_2, \ldots, \alpha_n$ ye, α nın F **üzerindeki eşlenikleri** denir.

Örnek 4: $\sqrt{2}$ nin $\mathbb{Q}$ üzerindeki eşlenikleri; $P_{\mathbb{Q}}(\sqrt{2}, x) = x^2 - 2)$ olduğundan, $\pm\sqrt{2}$ dir.

Örnek 5: $w = (-1 + i\sqrt{3})/2$ nin $\mathbb{Q}$ üzerindeki eşlenikleri; $P_{\mathbb{Q}}(w, x) = x^2 + x + 1$ olduğundan, w ve $\bar{w} = w^2$ dir.

Örnek 6: $\sqrt[3]{2}$ nin $\mathbb{Q}$ üzerindeki eşlenikleri; $P_{\mathbb{Q}}(\sqrt[3]{2}, x) = x^3 - 2$ olduğundan, $\sqrt[3]{2}$, $\sqrt[3]{2}w$, $\sqrt[3]{2}w^2$ dir. (Örnek 1)

Tanım 5.2.5 E ve K bir F cisminin iki genişlemesi ve $\sigma : E \longrightarrow K$ bir $1-1$, homomorfizma ise σ ya bir **monomorfizma** denir. Eğer $\forall a \in E$ için, $\sigma(a) = a$ ise σ ya E den K ya bir **F-monomorfizma** denir. Ayrıca σ örten de ise bir **F-izomorfizma** denir.

Not: E cisim ise sıfır homomorfizmadan farklı her $\sigma : E \longrightarrow K$ halka homomorfizması $1-1$ olacağından, bir monomorfizmadır.

Her sonlu genişlemenin bir cebirsel genişleme ve ilkel eleman teoremine göre bir basit genişleme olduğunu yukarıda gördük. Şimdi bir sonlu genişlemenin tüm F-monomorfizmalarını belirleyelim:

Teorem 5.2.3: $[E : F] = n$ ve $\beta \in E$ için $E = F(\beta)$ olsun. $\sigma : E \longrightarrow \mathcal{L}$ bir F-monomorfizma ise $\sigma(\beta)$, β nın F üzerinde bir eşleniğidir. E nin tüm F-monomorfizmalarının sayısı tam n tane olup, β nın eşlenikleri $\beta = \beta_1, \beta_2, \ldots, \beta_n$ iseler bunlar; $\sigma(\beta) = \beta_i$, $i = 1, 2, \ldots n$ ile belirlidirler.

İspat: Her $x \in E$,

$$x = a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}, \quad a_i \in F$$

şeklinde olduğundan σ, F nin elemanlarını sabit bıraktığından,

$$\sigma(x) = a_0 + a_1\sigma(\beta) + \cdots + a_{n-1}(\beta)^{n-1}$$

dir. Şu halde σ monomorfizması, β da aldığı değerlerle tamamen belirlidir.

$$f = P_F(\beta, x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + x^n$$

ise

$$0 = b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1} + \beta^n \Longrightarrow$$

$$0 = \sigma(0) = b_0 + b_1\sigma(\beta) + \cdots + b_{n-1}\sigma(\beta)^{n-1} + \sigma(\beta)^n = f(\sigma(\beta))$$

bulunur. Şu halde $\sigma(\beta)$ F nin bir kökü, yani β nın bir eşleniğidir. f asal polinom olduğundan, tüm kökleri farklı ve dolayısı ile β nın eşlenikleri sayısı tam n tanedir. Bu eşlenikler;

$$\beta = \beta_1, \beta_2, \ldots, \beta_n$$

olsunlar.

$$\sigma_i(\beta) = \beta_i$$

ile tanımlı σ_i lerin $(i = 1, 2, \ldots, n)$, E den $\mathcal{L}$ ye mümkün olan tüm monomorfizmalar olduğu gösterilmiş olur. σ_i lerin herhangi bir $x \in E$ üzerindeki etkisini bulmak için, bu eleman

$$x = a_0 + a_1\sigma(\beta) + \cdots + a_{n-1}\beta^{n-1}, \quad (a_i \in F)$$

şeklinde yazılır ve

$$\sigma(x) = a_0 + a_1\sigma(\beta) + \cdots + a_{n-1}\sigma(\beta)^{n-1}$$

bulunur.

Tanım 5.2.6: E den $\mathcal{C}$ ye tüm F-monomorfizmalarının kümesi G(E/F) ile gösterilir.

Örnek 7: $E = \mathcal{Q}(\sqrt{2})$ ise $G(E/F) = \{\sigma_1, \sigma_2\}$ dir. Burada,

$$\begin{aligned} \sigma_1(\sqrt{2}) &= \sqrt{2} \\ \sigma_2(\sqrt{2}) &= -\sqrt{2} \end{aligned}$$

ile tanımlıdır.

Örnek 8: $E = \mathcal{Q}(\sqrt[3]{2})$ ise $G(E/F) = \{\lambda_1, \lambda_2, \lambda_3\}$ dir. Burada,

$$\begin{aligned} \lambda_1(\sqrt[3]{2}) &= \sqrt[3]{2} \\ \lambda_2(\sqrt[3]{2}) &= w\sqrt[3]{2} \\ \lambda_3(\sqrt[3]{2}) &= w^2\sqrt[3]{2} \end{aligned}$$

ile tanımlıdır.

Not: $G(E/F)$ nin eleman sayısının $[E : F]$ olduğuna ve $G(E/F)$ nin elemanlarının E den $\mathcal{C}$ ye olduğuna dikkat edelim. Örnek 7 de σ_1 ve σ_2 monomorfizmaları E den E ye olduğu halde, Örnek 8 deki λ_2 ve λ_3 monomorfizmaları E den E ye değildirler. Gerçekten, $\lambda_2(\sqrt[3]{2}) \notin E$ ve $\lambda_3(\sqrt[3]{2}) \notin E$ dir.

Ayrıca bir $\sigma \in G(E/F)$ monomorfizmasının E den E ye olması için $\sigma(E) \subset E$ olması yeter. Çünkü, $E \cong \sigma(E)$ olduğundan,

$$[\sigma(E) : \sigma(F)] = [E : F]$$

olur ve $F \subset \sigma(E) \subset E$ den $E = \sigma(E)$ bulunur.Bu not göz önüne alınarak şu tanımı yapmak yerinde olur:

Tanım 5.2.7 E, F nin sonlu bir genişlemesi olsun. Eğer $\forall \sigma \in G(E/F)$ için, $\sigma(E) = E$ ise genişlemeye bir **normal genişleme** denir.

Aşağıdaki denklikler yardımı ile normal genişlemeyi değişik şekillerde de tanımlamak mümkündür:

Normal Genişleme Teoremi 5.2.4 E, F nin sonlu bir genişlemesi olsun. Aşağıdaki ifadeler birbirine denktirler:

i) E, bir $f \in F[x]$ polinomunun parçalanış cismidir.

ii) E, sonlu sayıda $f_1, f_2, \ldots, f_n \in F[x]$ polinomlarının köklerini F ye katmakla elde edilmiştir.

iii) Her $\sigma \in G(E/F)$ için, $\sigma(E) = E$ dir.

iv) Her $x \in E$ için, x in F üzerindeki tüm eşlenikleri de E dedir.

İspat: (i) $\Longrightarrow$ (ii) gerektirmesinin doğruluğu açıktır.

(ii) $\Longrightarrow$ (iii): E, F ye sonlu sayıda f_1, f_1, ..., $f_n \in F[x]$ polinomunun köklerini katmakla elde edilen cisim olsun. Bu polinomların bütün kökleri; α_1, $\alpha_2, \ldots$, α_s ile gösterilirse, $E = F(\alpha_1, \alpha_2, \ldots, \alpha_s)$ olur. $\sigma \in G(E/F)$ ise $\forall i = 1, 2, \ldots, s$ için $\sigma(\alpha_i)$, α_i nin bir eşleniği olduğundan, $\sigma(\alpha_i) \in \{\alpha_1, \ldots, \alpha_s\}$ dir. Şu halde $F \subset \sigma(E) \subset E$ dir. Yukarıdaki notta da belirttiğimiz gibi, $\sigma(E) = E$ bulunur.

(iii) $\Longrightarrow$ (iv): Her $\sigma \in G(E/F)$ için, $\sigma(E) = E$ olsun. $a \in E$ ve a nın F üzerindeki bir eşleniği a' olsun. Teorem 5.2.3'e göre, $\sigma(a) = a'$ ile bir $\sigma : F(a) \longrightarrow \mathcal{L}$ F-monomorfizması tanımlanabilir. İlkel eleman teoremine göre, $E = F(a)(\beta)$ olacak şekilde bir $\beta \in E$ bulunabilir.

Şimdi σ F-monomorfizmasının bir $\eta : E \longrightarrow \mathcal{L}$ F-monomorfizmasına genişletilebileceğini gösterelim:

Bunun için, $\eta(\beta)$ yı β nın bir eşleniği olarak almak yeter. Bu takdirde, $\forall \alpha \in E$ ve $\alpha = a_0 + a_1\beta + \cdots + a_{r-1}\beta^{r-1}$ ($a_i \in F(a)$, $r = [E : F(a)]$) elemanı için,

$$\eta(\alpha) = \sigma(a_0) + \sigma(a_1)\eta(\beta) + \cdots + \sigma(a_{r-1})\eta(\beta_{r-1})$$

olacağından, η bir F-monomorfizmadır ve $F(a)$ ya kısıtlanışı da σ yı verir. (iii) ye göre, $\eta(E) = E$ kabul ettiğimizden, $a' = \eta(a) \in \eta(E) = E$ olur.

(iv) $\longrightarrow$(i): $\forall a$ E için, a nın F üzerindeki her eşleniğinin E de olduğunu kabul edelim. İlkel eleman teoremine göre $E = F(\beta)$ olacak şekilde $\exists \beta \in E$ bulunabilir. β nın F üzerindeki eşlenikleri; β_1, β_2, ..., β_n iseler (iv)'e göre, $\forall \beta_i \in E$ dir. Şu halde E, $f = P_F(\beta, x)$

polinomunun bütün köklerini F ye katmakla elde edilmiştir. Yani, E, $f(x) \in F[x]$ polinomunun parçalanış cismidir.

Örnek 9: $\zeta_n = e^{2\pi i/n}$ birin n. primitif kökü olmak üzere, $\mathbb{Q}(\zeta_n)$, $\mathbb{Q}$ nun bir normal genişlemesidir. Çünkü ζ_n nin eşlenikleri; $x^n - 1$ polinomunun kökleri olan $\zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$ lerin arasındadır ve bunların hepsi $\mathbb{Q}(\zeta_n)$ cismindedir.

Örnek 10: $\mathbb{Q}(\sqrt[3]{2})$ cismi $\mathbb{Q}$ nun bir normal genişlemesi değildir. (Bak Örnek 1)

5.2 ALIŞTIRMALAR

1-) $x^6 - 1$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismini bulunuz.

2-) $x^n - 1$ polinomunun köklerinin C de n. mertebeden bir devirli grup oluşturduğunu gösteriniz. Bu grubun üreteçlerine, birin n. **primitif kökleri** denir.

3-) $x^n - 1$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismini ve $\mathbb{Q}$ üzerindeki derecesini bulunuz.

4-) $x^9 + x^3 + 1$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismini ve $\mathbb{Q}$ üzerindeki derecesini bulunuz.

5-) E, F nin bir genişlemesi ve $f \in F[x]$ olsun. E nin, F nin elemanlarını sabit bırakan bir otomorfizması ϕ ise E deki bir kökünün ϕ altındaki görüntüsünün de bir kök olduğunu gösteriniz.

6-) $\mathbb{Q}(\sqrt[3]{2})$ cisminin birim otomorfizmadan başka bir otomorfizmasının olmadığını gösteriniz.

7-) n. dereceden bir polinomun bir F cismi üzerindeki parçalanış cisminin, köklerinden herhangi n-1 tanesini F ye katmakla elde edilen cisim olduğunu gösteriniz.

8-) $x^4 - 2x^2 - 2$ polinomunun $\mathbb{Q}$ üzerinde asal olduğunu gösteriniz. İzomorf olmayan iki genişleme üreten köklerinden ikisini bulunuz.

9-) $\mathbb{Q}(\sqrt[3]{2})$ genişlemesini kapsayan $\mathbb{Q}$ nun bir normal genişlemesini

bulunuz.

10-) Aşağıdaki polinomların katlı köklerinin bulunup bulunmadığını araştırınız.

a) $x^6 - 4x^3 + 4$ b)$x^3 - 6x^2 + 12x - 8$ c) $x^5 - 3x^3 + 10x + 3$

11-) E, F nin bir genişlemesi ve $f, g \in F[x]$ olsun. f ve g nin $F[x]$ deki ebob'lerinin $E[x]$ deki ebob'leri olduğunu gösteriniz.

12-) Aşağıdaki elemanların $\mathbb{Q}$ üzerindeki eşleniklerini bulunuz.

a) $\sqrt[4]{3}$, b) $\sqrt{2+\sqrt{3}}$, c) $\sqrt{1+\sqrt{1+\sqrt{2}}}$

13-) F bir cisim, α ve β da F nin kare olmayan iki elemanı olmak üzere, $E_1 = F(\sqrt{\alpha})$ ve $E_2 = F(\sqrt{\beta})$ olsunlar.

$$E_1 = E_2 \iff \exists \gamma \in F, \quad \alpha = \gamma^2 \beta$$

olduğunu gösteriniz.

14-) $E = \mathbb{Q}(\sqrt[3]{3})$ olduğuna göre, $G(E/\mathbb{Q})$ kümesini bulunuz.

15-) $E = F(\beta)$ ve β nın F üzerindeki eşlenikleri; $\beta = \beta_1, \beta_2, \ldots, \beta_n$ olsunlar. $\alpha = a_0 + a_1\beta + \cdots + n\beta^{n-1} \in E$ ve $m = [F(\alpha) : F]$ ise

a) $m \mid n$ olduğunu,

b) α nın E den $\mathbb{C}$ ye her F-monomorfizması altındaki görüntüsünün her eşlenik n/m defa tekrarlanmak üzere,

$$a_0 + a_1\beta_i + \cdots + a_{n-1}\beta_i^{n-1} \quad (i = 1, 2, \ldots, n)$$

ler olduğunu gösteriniz.

5.3 GALOIS GENİŞLEMELERİ

Bu kesimde de göz önüne aldığımız cisimler kompleks sayılar cisminin alt cisimleri ve $\mathbb{Q}$ nun sonlu genişlemeleridirler.

Tanım 5.3.1 E, F nin bir genişlemesi ise E nin kendisi üzerine bir F-monomorfizmasına E nin bir **F-otomorfizması** denir. E nin bütün F-otomorfizmalarının kümesi de **Gal(E/F)** ile gösterilir.

$Gal(E/F) \subset G(E/F)$ olduğu açıktır. Teorem 5.2.3'e göre, $G(E/F)$ kümesinin eleman sayısı [E:F]=n olduğundan,
$Gal(E/F)$ kümesinin de eleman sayısı en fazla n olabilir. Ayrıca 5.2 Kesimde bir $\sigma \in G(E/F)$ için,

$$\sigma \in Gal(E/F) \Longleftrightarrow \sigma(E) \subset E$$

olduğunu belirtmiştik. Şimdi bir normal genişleme için,
$G(E/F)$ ve $Gal(E/F)$ kümelerinin aynı olduğunu gösterelim:

Önerme 5.3.1 E, F nin sonlu bir genişlemesi, $[E : F] = n$ ve $E = F(\beta)$ olsun. β nin F üzerindeki eşlenikleri; $\beta_1, \beta_2, \ldots, \beta_n$ ve $\sigma_i \in G(E/F)$, $\sigma_i(\beta) = \beta_i$ ile tanımlansın.

$$\sigma_i \in Gal(E/F) \Longleftrightarrow \beta_i \in E$$

olmasıdır.

İspat: Teorem 5.2.3'de $G(E/F)$ nin elemanlarının β nın eşlenikleri ile belirlendiğini görmüştük. Yukarıdaki nota göre, $\sigma_i \in G(E/F)$ için;

$$\sigma_i \in Gal(E/F) \Longleftrightarrow \sigma_i(E) \subset E \Longleftrightarrow \sigma_i(\beta) = \beta_i \in E$$

elde edilir.

Sonuç: E, F nin bir normal genişlemesi ise $Gal(E/F) = G(E/F)$ dir.

Tanım 5.3.2 Sonlu ve normal bir genişlemeye **Galois genişlemesi** denir.

Şimdi $Gal(E/F)$ kümesini, üzerinde bir işlem olarak bileşke işlemini alarak bir grup yapalım:

$\forall \sigma, \eta \in Gal(E/F)$ ve $\forall x \in E$ için,

$$\sigma\eta(x) = \eta(\sigma(x))$$

diyelim. $\sigma\eta \in Gal(E/F)$ olduğu ve $Gal(E/F)$ nin bu işleme göre bir grup olduğu gösterilebilir.

Tanım 5.3.4 $Gal(E/F)$ grubuna,E nin F genişlemesinin **Galois grubu** denir.

Örnek 1: $E = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}$ nun bir normal genişlemesi olduğundan,

$$Gal(E/\mathbb{Q}) = G(E/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$$

dir. Burada, $\sigma_1(\sqrt{2}) = \sqrt{2}$ ve $\sigma_2(\sqrt{2}) = -\sqrt{2}$ ile tanımlıdır. $Gal(E/\mathbb{Q})$ grubu 2 elemanlı bir grup ve $\mathcal{Z}_2$ ye izomorftur.

E, F nin bir Galois genişlemesi ise Galois Teorisinin Temel Teoremi, E ve F arasındaki cisimlerle, $Gal(E/F)$ grubunun alt grupları arasında 1-1 bir tekabül kurmaktır. Bunun için bazı hazırlıklar yapalım.

Önerme 5.3.2 $H < G = Gal(E/F)$ olsun.

$$\mathcal{F}(H) = \{x \in E \ : \ \forall\sigma \in G;\ \sigma(x) = x\},$$

E nin F yi kapsayan bir alt cismidir. Bu cisme H alt grubunun **sabit cismi** denir.

İspat: $\mathcal{F}(H) \subset E$ olduğu açıktır. $\forall\sigma \in H$ bir F-otomorfizma olduğundan, $\forall a \in F$ için $\sigma(a) = a$ dır. Buradan $F \subset \mathcal{F}(H)$ bulunur.

Şimdi, $\mathcal{F}(H)$ nın bir cisim olduğunu gösterelim.$\forall x, y \in \mathcal{F}(H)$ ve $\forall\sigma \in H$ için, $\sigma(x) = x$ ve $\sigma(y) = y$ olduğu göz önünde tututlarak;

$$\sigma(x \pm y) = \sigma(x) \pm \sigma(y) = x \pm y$$

ve $y \neq 0$ ise

$$\sigma(xy^{-1}) = \sigma(x)\sigma(y)^{-1} = xy^{-1}$$

bulunur. Şu halde

$$x \pm y,\ xy^{-1} \in \mathcal{F}(H)$$

yani, $\mathcal{F}(H)$ bir cisimdir.

Önerme 5.3.3 E, F nin bir Galois genişlemesi ve H, $Gal(E/F)$ nin bir alt grubu olsun. Bu takdirde E, $\mathcal{F}(H)$ nın bir Galois genişlemesi ve Galois grubu $Gal(E/\mathcal{F}(H)) = H$ dır.

İspat: E, $\mathcal{F}(H)$ nın sonlu ve normal bir genişlemesi ise E nin de $\mathcal{F}(H)$ nın sonlu ve normal bir genişlemesi yani bir Galois genişlemesi olur. (Neden ?).

$Gal(E/\mathcal{F}(H))$, E nin $\mathcal{F}(H)$-otomorfizmaları ile oluşur. $\sigma \in H$ elemanı $\mathcal{F}(H)$ nın tanımından dolayı $\mathcal{F}(H)$ nın elemanlarını sabit bıraktığından, $H \subset Gal(E/\mathcal{F}(H))$ bulunur.

Şimdi ters kapsamayı gösterelim. Kabul edelim ki,

$$H = \{\sigma_1, \sigma_2, \ldots, \sigma_s\}$$

s elemanlı ve $Gal(E/\mathcal{F}(H))$, t elemanlı bir grup olsunlar. Yukarıdaki kapsamadan, $s \leq t$ dir. $s = t$ olduğunu gösterirsek, $H = Gal(E/\mathcal{F}(H))$ olacağından teorem ispatlanmış olur.

Kabul edelim ki, $s < t$ olsun. $s + 1 \leq t$ olduğundan,

$$\alpha_1, \alpha_2, \ldots, \alpha_{s+1} \in E$$

elemanları $\mathcal{F}(H)$ üzerinde lineer bağımsız olacak şekilde seçilebilir.

$$\sum_{i=1}^{s+1} \sigma_j(\alpha_i) X_i = 0, \quad (j = 1, 2, \ldots, s)$$

lineer homojen denklem sistemi, s denklem ve $s + 1$ bilinmeyenden oluşur. Şu halde E de hepsi birden sıfır olmayan bir $(c_1, c_2, \ldots, c_{s+1})$ çözümü bulunabilir. Gerekirse α_i leri yeniden sıralayarak, bu çözümü $1 \leq i \leq r$ için $c_i \neq 0$ olmak üzere, $(c_1, c_2, \ldots, c_r, 0, 0, \ldots, 0)$ şeklinde düşünebiliriz. Ayrıca bu çözümde sıfır olmayan c_i lerin sayısı r yi de minumum olacak şekilde seçebilir ve denklem sistemi homojen olduğundan, $c_r = 1$ alabiliriz. Bunun için, yukarıdaki çözüm yerine

$$(c_1 c_r^{-1}, c_2 c_r^{-1}, \ldots, 1, 0, \ldots, 0)$$

almak yeter. Eğer her c_i çözümü $\mathcal{F}(H)$ da ise $\sigma_1(c_i) = c_i$ olduğundan,

$$\sum_{i=1}^{s+1} \sigma_1(\alpha_i)c_i = 0 \implies \sigma_1(\sum_{i=1}^{s+1} \alpha_i c_i) = 0$$
$$\implies \sum_{i=1}^{s+1} \alpha_i c_i = 0$$

bulunur. Bu ise α_i lerin $\mathcal{F}(H)$ üzerinde lineer bağımsız olmaları ile çelişir. Şu halde, c_i lerin hepsi de $\mathcal{F}(H)$ da olamaz. Genelliği bozmadan, $c_1 \notin \mathcal{F}(H)$ alabiliriz. Buradan, $\sigma(c_1) \neq c_1$ olacak şekilde bir $\sigma \in H$ nın varlığı çıkar. Yukarıdaki denklem sisteminde, her iki yana σ uygulayarak;

$$\sum_{i=1}^{s+1} \sigma_j(\alpha_i)c_i = 0 \implies \sum_{i=1}^{s+1} \sigma\sigma_j(\alpha_i)\sigma(c_i) = 0$$

elde edilir. σ_j ler H da değişirken, $\sigma\sigma_j$ ler de H da değişir. Buradan,

$$(\sigma(c_1), \sigma(c_2), \ldots, \sigma(c_{r-1}), 1, 0, \ldots, 0)$$

nın da bir çözüm olduğu anlaşılır.Fakat bu iki çözümün farkı da bir çözüm olacağından,

$$(\sigma(c_1) - c_1, \sigma(c_2) - c_2, \ldots, \sigma(c_{r-1}) - c_{r-1}, 0, \ldots, 0)$$

de bir çözümdür. $\sigma(c_1) \neq c_1$ olduğundan, sıfır çözüm de değildir. Bu ise, $(c_1, c_2, \ldots, c_r, 0, \ldots, 0)$ çözümünün seçiminde r nin minumum olması ile çelişir. Şu halde, $s = t$ olmalıdır.

Galois Teorisinin Temel Teoremi 5.3.1 E, F'nin bir Galois genişlemesi ve Galois grubu $G = Gal(E/F)$ olsun. G nin alt grupları ile E ve F arasındaki ara cisimler arasında yukarıda tanımlanan $\mathcal{F} : H \longrightarrow \mathcal{F}(H)$ fonksiyonu bir birebir eşlemedir.

İspat: G nin alt grupları ile E ve F arasındaki ara cisimler arasında Önerme 5.3.3 de tanımlanan $\mathcal{F} : H \longrightarrow \mathcal{F}(H)$ fonksiyonunun tersini de tanımlayabiliriz.

D, E ve F arasında bir ara cisim olsun.

$$\mathcal{G}(D) = \{\sigma \in Gal(E/F) \ : \ \forall x \in D;\ \sigma(x) = x\}$$

diyelim. $\mathcal{G}(D) = Gal(E/D)$ olduğu açıktır. Önerme 5.3.3'den, $H < Gal(E/F)$ ise

$$\mathcal{G}(\mathcal{F}(H)) = H$$

bulunur. Şu halde, $\mathcal{G}o\mathcal{F}$ bileşke fonksiyonu birim fonksiyon olduğundan, $\mathcal{F}$ nin $1-1$ ve $\mathcal{G}$ nin de örten olduğu anlaşılır. (Bak 1.3 Alıştırma 20 ve 21).

Şimdi de $\mathcal{F}o\mathcal{G}$ bileşke fonksiyonunun bir birim fonksiyon olduğunu gösterelim:

D herhangi bir ara cisim olsun. Yukarıdaki $\mathcal{G}(\mathcal{F}(H)) = H$ eşitliğinde $H = \mathcal{G}(D)$ yazarsak,

$$\mathcal{G}(\mathcal{F}(\mathcal{G}(D))) = \mathcal{G}(D)$$

bulunur. Genişlemelerin derecelerini hesaplayarak,

$$[E : \mathcal{F}(\mathcal{G}(D))] = o(\mathcal{G}(D)) = [E : D]$$

elde edilir. Buradan, $D \subset \mathcal{F}(\mathcal{G}(D))$ olduğu göz önüne alınarak, son eşitlikten;

$$D = \mathcal{F}(\mathcal{G}(D)),$$

yani $\mathcal{F}o\mathcal{G}$ nin birim fonksiyon olduğu görülür. Buradan, $\mathcal{G}$ nin $1-1$ ve $\mathcal{F}$ nin de örten olduğu anlaşılır. (Bak 1.3 Alıştırma 20 ve 21). Sonuç olarak, $\mathcal{F}$ ve $\mathcal{G}$ biribirlerinin tersleridirler.

Sonuç 1: E, F nin bir Galois genişlemesi ise E ve F arasındaki cisimlerin sayısı sonludur.

İspat: $Gal(E/F)$ sonlu bir grup olduğundan, sadece sonlu sayıda alt grubu vardır. Temel Teoremden, ara cisimlerin sayısının da aynı sayıda olduğu görülür.

Sonuç 2: E, F'nin bir Galois genişlemesi ve Galois grubu G olsun. Bir $x \in E$ elemanı, $\forall \sigma \in G$ için, $\sigma(x) = x$ ise $x \in F$ dir.

İspat: $\forall \sigma \in G$ için, $\sigma(x) = x$ ise $x \in \mathcal{F}(G)$ dir. $G = Gal(E/F)$ olduğundan, $\mathcal{G}(F) = G$ ve Temel Teoreme göre,

$$\mathcal{F}(\mathcal{G}(F)) = F$$

olacağından istenen elde edilir.

Örnek 2: $F = \mathbb{Q}$ ve $E = F(\sqrt{2}, \sqrt{3})$ olsun. E, F nin bir Galois genişlemesi ve $G = Gal(E/F) = \{e = \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ 4 elemanlı olup, σ lar şu şekilde belirlidir:

$$e = \sigma_1 : \begin{cases} \sqrt{2} \longrightarrow \sqrt{2} \\ \sqrt{3} \longrightarrow \sqrt{3} \end{cases} \quad \sigma_2 : \begin{cases} \sqrt{2} \longrightarrow -\sqrt{2} \\ \sqrt{3} \longrightarrow \sqrt{3} \end{cases}$$

$$\sigma_3 : \begin{cases} \sqrt{2} \longrightarrow \sqrt{2} \\ \sqrt{3} \longrightarrow -\sqrt{3} \end{cases} \quad \sigma_4 : \begin{cases} \sqrt{2} \longrightarrow -\sqrt{2} \\ \sqrt{3} \longrightarrow -\sqrt{3} \end{cases}.$$

Bu grupta, birimden farklı her elemanın mertebesi 2 dir. (Klein'in 4-lü grubu). G nin alt grupları: $H_1 = \{e\}$, $H_2 = \{e, \sigma_2\}$, $H_3 = \{e, \sigma_3\}$, $H_4 = \{e, \sigma_4\}$ ve $H_5 = G$ dir. Bu alt gruplara karşılık gelen ara cisimler de sırası ile;

$$\mathcal{F}(H_1) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = E, \quad \mathcal{F}(H_2) = \mathbb{Q}(\sqrt{3}),$$

$$\mathcal{F}(H_3) = \mathbb{Q}(\sqrt{2}), \quad \mathcal{F}(H_4) = \mathbb{Q}(\sqrt{6}) \mathbb{Q}(H_5) = \mathbb{Q}$$

durlar. Şu halde, 5 ara cisim vardır. Alt gruplara karşılık gelen ara cisimler bulunurken, o alt gruptaki otomorfizmaların sabit bıraktığı elemanlar araştırılmıştır. Örnek olarak, $H_4 = \{e, \sigma_4\}$ alt grubuna karşılık gelen ara cismi bulalım.

$$\sqrt{6} = \sqrt{2}\sqrt{3} \in \mathcal{F}(H_4) \Longrightarrow \mathbb{Q}(\sqrt{6}) \subset \mathcal{F}(H_4)$$

bulunur. $o(H_4) = 2$ olduğundan, Önerme 5.3.3'e göre, $[E : \mathcal{F}(H_4)] = 2$ dir. $[E : \mathbb{Q}(\sqrt{6})] = 2$ olduğundan, $\mathcal{F}(H_4) = \mathbb{Q}(\sqrt{6})$ elde edilir.

Örnek 3: E, $x^3 - 2$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismi olsun. $Gal(E/\mathbb{Q})$ grubunu ve alt gruplarına karşılık gelen ara cisimleri bulalım.

$$x^3 - 1 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{2^2})$$

$f(x) = x^3 - 2$ nin $\mathcal{C}$ deki kökleri; $w = (-1 + i\sqrt{3})/2$ olmak üzere $\sqrt[3]{2}$, $\sqrt[3]{2}w$, $\sqrt[3]{2}w^2$ dirler. f'nin parçalanış cismi, $E = \mathcal{Q}(\sqrt[3]{2}, \sqrt{3}i)$ şeklinde yazılabilir ve $\mathcal{Q}$ üzerindeki derecesi de 6 dır. Şu halde, $Gal(E/\mathcal{Q})$ 6 elemanlı bir grup ve E nin $\mathcal{Q}$-otomorfizmaları $\sqrt[3]{2}$ ve $i\sqrt{3}$ üzerindeki etkileri ile belirlidir. Bunlar;

$$e = \begin{cases} \sqrt[3]{2} \longrightarrow \sqrt[3]{2} \\ i\sqrt{3} \longrightarrow i\sqrt{3} \end{cases}, \tau_1 = \begin{cases} \sqrt[3]{2} \longrightarrow \sqrt[3]{2}w \\ i\sqrt{3} \longrightarrow i\sqrt{3} \end{cases}, \tau_2 = \begin{cases} \sqrt[3]{2} \longrightarrow \sqrt[3]{2}w^2 \\ i\sqrt{3} \longrightarrow i\sqrt{3} \end{cases},$$

$$\tau_3 = \begin{cases} \sqrt[3]{2} \longrightarrow \sqrt[3]{2} \\ i\sqrt{3} \longrightarrow -i\sqrt{3} \end{cases}, \tau_4 = \begin{cases} \sqrt[3]{2} \longrightarrow \sqrt[3]{2}w \\ i\sqrt{3} \longrightarrow -i\sqrt{3} \end{cases}, \tau_5 = \begin{cases} \sqrt[3]{2} \longrightarrow \sqrt[3]{2}w^2 \\ i\sqrt{3} \longrightarrow -i\sqrt{3} \end{cases}$$

olmak üzere $G = \{e, \tau_1, \tau_2, \tau_3, \tau_4, \tau_5\}$ dir.

G grubunda, $\tau_1 = \tau$ ve $\tau_3 = \rho$ dersek; $\tau_2 = \tau^2$, $\tau_4 = \tau\rho$, ve $\tau_5 = \tau^2\rho$ olur. Şu halde,

$$G = \{e, \tau, \tau^2, \rho, \tau\rho, \tau^2\rho\}$$

Galois grubunun bir D_3 dihedral grubu olduğu görülür. G nin 1. mertebeden alt grubu; $H_1 = \{e\}$, 2. mertebeden alt grupları;

$$H_2 = \{e, \rho\}, \quad H_3 = \{e, \tau\rho\}, \quad H_4 = \{e, \tau^2\rho\}$$

3. mertebeden alt grubu;

$$H_5 = \{e, \tau, \tau^2\}$$

ve 6. mertebeden alt grubu da grubun kendisi G dir. Bu alt gruplara karşılık gelen ara cisimler de sırası ile;

$$\mathcal{F}(H_1) = E, \quad \mathcal{F}(H_2) = \mathcal{Q}(\sqrt[3]{2}), \quad \mathcal{F}(H_3) = \mathcal{Q}(\sqrt[3]{2}w^2),$$

$$\mathcal{F}(H_4) = \mathcal{Q}(\sqrt[3]{2}w), \quad \mathcal{F}(H_5) = \mathcal{Q}(i\sqrt{3}) \text{ ve } \mathcal{F}(G) = \mathcal{Q}$$

bulunur.

Yukarıdaki örnekte de görüldüğü gibi E, $\mathcal{Q}$ nun bir Galois genişlemesi olduğu halde ara cisimler $\mathcal{Q}$ üzerinde Galois genişlemesi olmayabilir. Örneğin, $i = 2, 3, 4$ için $\mathcal{F}(H_i)$ cisimleri $\mathcal{Q}$ üzerinde Galois genişlemesi değildirler. Bir ara cismin ne zaman bir Galois genişlemesi olacağını aşağıdaki teoremden sonra göreceğiz.

Teorem 5.3.2 E, F'nin bir Galois genişlemesi ve Galois grubu G olsun. H_1, H_2, G'nin iki alt grubu ve bunlara karşılık gelen ara cisimler de D_1 ve D_2 olsunlar.

i) $H_1 \subset H_2 \iff D_1 \supset D_2$

ii) $H_1 \cap H_2$ ye karşılık gelen ara cisim, D_1 ve D_2 yi kapsayan E'nin en küçük alt cismidir. Bu cismi D_1D_2 ile gösterelim.

iii) H_1 ve H_2 'yi kapsayan G'nin en küçük alt grubunu $[H_1 \cup H_2]$ ile gösterelim. Bu alt gruba karşılık gelen ara cisim $D_1 \cap D_2$ dir.

İspat: Galois Teorisinin Temel Teoremindeki fonksiyonlarla, $D_1 = \mathcal{F}(H_1)$ ve $D_2 = \mathcal{F}(H_2)$ olsun.

(i) $H_1 \subset H_2 \Longrightarrow \mathcal{F}(H_1) \supset \mathcal{F}(H_2)$ olduğu açıktır. Ters kapsamayı gösterelim.

$$\mathcal{F}(H_1) \supset \mathcal{F}(H_2) \Longrightarrow H_1 = \mathcal{G}(\mathcal{F}(H_1)) \subset \mathcal{G}(\mathcal{F}(H_2)) = H_2$$

elde edilir.

(ii) $H_1 \cap H_2$, G nin H_1 ve H_2 de kapsanan en büyük alt grubudur. Şu halde, (i) ve temel teoreme göre, $\mathcal{F}(H_1 \cap H_2)$, E nin $\mathcal{F}(H_1)$ ve $\mathcal{F}(H_2)$ yi kapsayan en küçük alt cismidir.

(iii) $[H_1 \cup H_2]$, G nin H_1 ve H_2 yi kapsayan en küçük alt grubudur. Şu halde, (i) ve temel teoreme göre, $\mathcal{F}([H_1 \cup H_2])$, E nin $\mathcal{F}(H_1)$ ve $\mathcal{F}(H_2)$ de kapsanan en büyük alt cismidir. Yani, $\mathcal{F}([H_1 \cup H_2]) = \mathcal{F}(H_1) \cap \mathcal{F}(H_2)$ dir.

Teorem 5.3.3 E, F'nin bir Galois genişlemesi ve Galois grubu G olsun. Eğer D bir ara cisim ve $H = \mathcal{G}(D)$ ise;

i) D, F'nin bir normal genişlemesi $\iff H \triangleleft G$

ii) $H \triangleleft G$ ise D, F'nin Galois genişlemesi olup, $Gal(D/F) = G/H$ dır.

İspat: $\sigma \in G$ olsun. İspata geçmeden,

$$\mathcal{G}(\sigma D) = \sigma \mathcal{G}(D) \sigma^{-1}$$

olduğunu gösterelim.

$\eta \in \mathcal{G}(D)$ ise $\sigma\eta\sigma^{-1}$, σD yi sabit bırakır. Şu halde,

$$\mathcal{G}(\sigma D) \supset \sigma\mathcal{G}(D)\sigma^{-1}$$

dir.

$\lambda \in \mathcal{G}(\sigma D)$ ise $\sigma^{-1}\lambda\sigma$, D'yi sabit bırakır. Şu halde, $\sigma^{-1}\lambda\sigma \in \mathcal{G}(D)$ ve $\lambda \in \sigma\mathcal{G}(D)\sigma^{-1}$ dir. Buradan,

$$\mathcal{G}(\sigma D) \subset \sigma\mathcal{G}(D)\sigma^{-1}$$

elde edilir. Her iki kapsamadan da eşitlik bulunur.

(i) D, F'nin normal genişlemesi $\Longleftrightarrow \forall\sigma \in Gal(E/F)$ için, $\sigma D = D$ $\Longleftrightarrow \forall\sigma \in Gal(E/F)$ için, $\mathcal{G}(\sigma D) = \mathcal{G}(D) \Longleftrightarrow \forall\sigma \in Gal(E/F)$ için, $\sigma H\sigma^{-1} = H$

(ii) $H \triangleleft G$ ise (i) den D nin F üzerinde bir normal genişleme olduğu anlaşılır. Aynı zamanda sonlu bir genişleme olduğundan, bir Galois genişlemesidir.

$\psi : Gal(E/F) \longrightarrow Gal(D/F)$ fonksiyonunu, $\sigma \in Gal(E/F)$ için, $\psi(\sigma) = \sigma|_D$ ile tanımlarsak, ψ nin bir homomorfizma olduğu gösterilebilir. D nin her F-otomorfizması E nin bir F-otomorfizmasına genişletilebileceğinden ψ nin örten olduğu görülür.

$$Çek\ \psi = \{\sigma \in Gal(E/F) \ : \ \sigma = I_D\} = H$$

(I_D, D nin özdeşlik fonksiyonu). Homomorfizma teoreminden,

$$G/H \cong Gal(D/F)$$

elde edilir.

5.3 ALIŞTIRMALAR

1-) $x^3 - 1$ polinomunun parçalanış cismini ve Galois grubunu bulunuz. Ara cisimlerle, alt gruplar arasındaki tekabülü açıklayınız.

2-) $x^4 - 2$ polinomunun parçalanış cismini ve Galois grubunu bulunuz. Ara cisimlerle, alt gruplar arasındaki tekabülü açıklayınız.

3-) $E = Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$ olsun. $Gal(E/Q)$ grubunu, ara cisimlerle, alt gruplar arasındaki tekabülü açıklayınız.

4-) E, $x^8 - 2$ polinomunun Q üzerindeki parçalanış cismi olsun.

a) $\zeta_8 = e^{2\pi i/8}$ olmak üzere, $E = Q(\sqrt[8]{2}, \zeta_8)$,
b) $\sqrt{2} \in Q(\zeta_8)$,
c) $P_{Q(\zeta_8)}(\sqrt[8]{2}, x) = x^4 - \sqrt{2}$ ve
d) $[E : Q] = 16$ olduğunu gösteriniz.

5-) p asal tam sayı ve $\zeta = e^{2\pi i/p}$ (p. primitif kök) olmak üzere, $E = Q(\zeta)$ olsun. $a \in E$ ise $x^p - a$ polinomunun $E[x]$ de ya asal, ya da, lineer çarpanlara ayrılacağını gösteriniz.

KAYNAKLAR

[1] ÇALLIALP, F. : Soyut Cebir I,
Hacettepe Üniv. Fen Fak. Yay. No:15, 1981.

[2] ÇALLIALP, F. : Soyut Cebir ve Sayılar Teorisi,
Ondokuzmayıs Üniv. Fen-Ed. Fak. Yay. No:12, 1986.

[3] FRALEIGH, J. : A First Course in Abstract Algebra,
Addison-Wesley Pub. Co. London, 1973.

[4] GOLDSTEIN, I.N. : Abstract Algabra,
Prentice Hall, New York, 1973.

[5] HERSTEIN, I.N. : Topics in Algebra,
Blaisdell Int. Textbook Series, Toronto, 1964.

[6] HUNGERFORD, T.W. : Algebra,
Springer-Verlag, New York, 1974.

[7] Mc CARTY, P. : Algebraic Extensions of Fields,
Blaisdell Pub. co. Toronto, 1966

İndeks