

EL-CEBR ALGEBRA CEBİR

Babamın Anısına...

ve Aileme...

Erhan GÜLER

3.10.1995
Salı

$$A = \{a \mid p(a)\}$$

$$A = \{a \in \mathbb{Z} \mid a > 0\} = \{1, 2, 3, \dots\}$$

$$B = \{a \in \mathbb{R} \mid \sqrt{a} \in \mathbb{Z}\} = \{0, 1, 4, 9, 16\}$$

$A \times A$ nin boş olmayan herhangi bir alt kümesi

$A \times B$ nin " " "

$$\emptyset \neq f \subset A \times B$$

$$(a, b) \in \sim a \sim b$$

$$(a, b) \in f \quad a f b \quad b = f(a) \quad \text{fonksiyon: özel bir bağıntı.}$$

i- $\forall a \in A, (a, *) \in f \quad * = f(a)$

ii- $(a, *) \notin f \quad \text{fonksiyonda } A \text{ nin bir elemanı } B \text{ nin farklı bir elemanına gitmez.}$
 $(a, \square) \notin f$

• $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \quad (\text{bire-bir olma})$

• $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\forall b \in B$ için $f(a) = b$ o.s. $\exists a \in A \quad (\text{örten olma})$

Fonksiyon 1:1 ve örten ise tersi vardır.

$f: A \rightarrow B \quad b \in B, f^{-1}(b) = \{a \in A \mid f(a) = b\} \quad 1:1 \text{ ve örten ise bu}$
 küme bir tek elemandan oluşur.

$f: \mathbb{R} \rightarrow \mathbb{R}$
 $x \rightarrow |x| \quad f^{-1}(3) = \{3, -3\}, f^{-1}(-4) = \emptyset$

Denklik bağıntısı : Yansıma, Simetri, Geçişme

$$\emptyset \neq \sim \subset A \times A$$

i- $\forall a \in A, a \sim a \quad (a, a) \in \sim \quad (\text{yansıma})$

ii- $(a, b) \in \sim \Rightarrow (b, a) \in \sim \quad a \sim b \Rightarrow b \sim a \quad (\text{simetri})$

iii- $(a, b) \in \sim \text{ ve } (b, c) \in \sim \Rightarrow (a, c) \in \sim$

$a \sim b \text{ ve } b \sim c \Rightarrow a \sim c \quad (\text{geçişme})$

Denklik sınıfı :

$a \in A, \bar{a} = \{b \in A \mid a \sim b\} \quad a \text{ ile bağıntılı olan tüm bağıntıların}$
 kümesi.

$$a, b \in \mathbb{Z}, \quad a \sim b \stackrel{tm}{\iff} 5 \mid a-b$$

($\stackrel{tm}{\iff}$: tanım)

$$a \equiv b \pmod{5} \iff 5 \mid a-b$$

$$\bar{8} = \{\dots, -7, -2, 3, 8, 13, \dots\} \quad \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}$$

Herbiri $\mathbb{Z}$ nin bir alt kümesidir. Bu kümelerin birleşimi $\mathbb{Z}$ yi verir.

$$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \cup \bar{4} \cup \bar{5} \cup \bar{6} \cup \bar{7}$$



Denklik bağıntısı varsa, kümeyi ayrık kümelere ayırabiliriz.

Kümenin ayrışımı verilir, denklik bağıntısı istenirse ;

$$A = \bigcup_{i \in I} A_i \quad i \neq j \quad i, j \in I \text{ için } A_i \cap A_j = \emptyset$$

$$\forall a, b \in A, \quad a \sim b \stackrel{tm}{\iff} a, b \in A_i \text{ denklik bağıntısıdır. Gösterelim.}$$

$$a \sim b \Rightarrow a, b \in A_i \quad A_i \neq A_j \text{ olsa } b \in A_i \cap A_j \text{ olur.}$$

$$b \sim c \Rightarrow b, c \in A_j \quad \text{O halde } A_i = A_j \text{ dir.}$$

$$A = \{a, b, c\} \quad A \text{ üzerinde denklik bağıntısı yazalım.}$$

$$\textcircled{1} \quad A = \{a\} \cup \{b\} \cup \{c\}$$

$$\textcircled{3} \quad A = \{b\} \cup \{a, c\}$$

$$\textcircled{5} \quad A = \{a, b, c\}$$

$$\textcircled{2} \quad A = \{a\} \cup \{b, c\}$$

$$\textcircled{4} \quad A = \{c\} \cup \{a, b\}$$

Her üçü birbiriyle bağıntılı olsun.

$$\beta_5 = \{(a, a), (b, b), (c, c), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b)\}$$

$$\bar{a} = \{a, b, c\} \quad \bar{c} = \bar{b} = \{a, b, c\}$$

$$\beta_1 = \{(a, a), (b, b), (c, c)\}$$

$$\beta_2 = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$$

$$\beta_3 = \{(a, a), (b, b), (c, c), (b, c), (c, b)\}$$

$$\beta_4 = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$$

$$\bullet \forall x, y \in A, \quad x \sim y \stackrel{tm}{\iff} x = y$$

Denklik bağıntısı eşitliğin genelleştirilmiş halidir.

$$3, 8 \in \mathbb{Z} \quad 3 \neq 8 \quad 3 \equiv 8 \pmod{5}$$

$$A, \sim \quad A/\sim = \{\bar{a} \mid a \in A\}$$

denklik sınıflarından oluşan kümeyi $A/\sim$ ile gösteririz.

$$** \quad a \sim b \Leftrightarrow 5 \mid a - b$$

$$\mathbb{Z}_5 = \mathbb{Z}/\sim = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} \rightarrow \text{denklik sınıflarının kümesi.}$$

Ödev // 4 ve 5 elemanlı küme üzerinde denklik sınıflarını yazın.

$\{0, 1, 2, 3, 4\}$ bağıntının tam temsilciler kümesidir.

Her denklik sınıfından birer tane eleman almakla oluşturulan kümeye tam temsilciler sistemi diyoruz.

$\{5, 11, 17, 13, 24\}$ tam temsilciler kümesidir.

TAM SAYILAR

$\forall a, b \in \mathbb{Z}, (b \neq 0) \quad b \mid a$ diyeceğiz. Eğer $a = bt$ o.s. $\exists t \in \mathbb{Z}$.

$(b \mid a : b \text{ böler } a'yı)$ b ve t 'ye a 'nın çarpan veya bölenleri denir.

1°) $\forall n \in \mathbb{Z}$ için $\pm 1 \mid n$ dir.

$$n \mid \pm 1 \Leftrightarrow n = \pm 1$$

2°) $m \mid n$ ve $n \mid p \Rightarrow m \mid p$

3°) $m \mid n$ ve $n \mid m \Rightarrow m = \pm n$

4°) $m \mid n$ ise $\pm m \mid \pm n$

$$3 \mid 6 \quad 6 = 2 \cdot 3, \quad -3 \mid 6 \quad 6 = (-2)(-3), \quad -3 \mid -6 \quad -6 = 2(-3)$$

$$3 \mid -6 \quad -6 = (-2) \cdot 3$$

5°) $\left. \begin{matrix} m \mid n \\ m \mid p \end{matrix} \right\} \Rightarrow \forall x, y \in \mathbb{Z}, m \mid nx + py$

6°) $m \neq 0 \quad m \mid n \Rightarrow |m| \leq |n|$

4. özellikten dolayı $\mathbb{Z}^+$ da incelenir (bölünebilme) yapacağız.

$\mathbb{Z}^-$ de aynı şekilde incelenebilir.

Asal Sayı: Kendisinden ve 1'den başka bir böleni olmayan pozitif sayılara asal sayı denir.

Önerme // Sıfır ve $\neq 1$ den farklı her tamsayının en az bir asal bölene vardır.

İspat // $a \in \mathbb{Z}$ ve $a \neq 0, \neq 1$ olsun.

$$M = \{d \in \mathbb{Z}^+ \mid d|a, d \neq 1\} \quad M \subset \mathbb{Z}^+$$

$$|a| \neq 1, |a| < M \Rightarrow M \neq \emptyset \quad (p : M \text{ nin en küçük elemanı.})$$

$\mathbb{Z}^+$ dan alınan her tamsayının alt kümelerinin en küçük elemanı vardır.

$\mathbb{Z}^-$ den " " " " " en büyük " " .

En küçük elemanı p ile gösterelim. p asal ise önerme ispatlanır.

p asal değilse, p nin öz böleneri (q ve r gibi) vardır.

p asal değilse : $p = qr$ ve $1 < q, r < p$ b.ş $\exists q, r \in \mathbb{Z}^+$ vardır.

$$q|p, p|a \Rightarrow q|a \Rightarrow q \in M \quad \# \text{ (çelişki)}$$

q 'yu en küçük bulduk. Fakat p yi en küçük asal olarak aldığımız için çelişki olur. O halde p en küçük asal olmak zorundadır.

Teorem : (Euclide) Sonsuz sayıda asal vardır.

İspat // $P = \{p_1, p_2, \dots, p_n\}$ Kabul edelim ki P sonlu tane asal sayıyı gösterebilir. Bu kümede bulunmayan bir tane de olsa asal bulursak, kümenin asal olduğu ortaya çıkar.

$a = p_1 p_2 \dots p_n + 1$ tamsayısını düşünelim. a 'nın bir asal bölene vardır. Bunu q ile gösterelim. Kabulden dolayı $q \in P \Rightarrow$

$$q | p_1 p_2 \dots p_n \quad (\text{5. özellikten } q | a)$$

$$q | a - p_1 p_2 \dots p_n = 1 \quad \# \text{ çelişkidir.} \quad (m | nx + py)$$

O halde $q \notin P$

$$\left\{ \begin{array}{l} q | a \\ q | (p_1 p_2 \dots p_n) \end{array} \right\} \Rightarrow q | 2x + (p_1 p_2 \dots p_n)y, \quad \left. \begin{array}{l} 5 | 15 \\ 5 | 20 \end{array} \right\} \Rightarrow 5 | 20x + 15y \quad \exists x, y$$

$x=1$ ve $y=-1$ için $q | a - p_1 p_2 \dots p_n$ olur.

O halde sonsuz sayıda asal sayı vardır.

Teorem : $\forall m, n \in \mathbb{Z}, (m \neq 0) \quad n = qm + r$ ve $0 \leq r < |m|$ o.s. $q, r \in \mathbb{Z}$ vardır.

$$7 = 1 \cdot 5 + 2, \quad -7 = (-2) \cdot 5 + 3, \quad 5 = 0 \cdot 7 + 5, \quad 5 < |-7| = 7.$$

Tümevarımla ispatlanır. //

TANIM : Pozitif d tamsayısına a ve b tamsayılarının ebob denir, eğer :

i- $d|a$ ve $d|b$

ii- a ve b nin her ortak k böleni için $k|d$ oluyorsa,

$d = (a, b)$ veya $\text{ebob}(a, b)$ ile gösterilir.

$$(a, b) = (a, -b) = (-a, b) = (-a, -b)$$

Önerme // $\forall 0 \neq a, b \in \mathbb{Z}$ nin ebob vardır. $(a, b) = d$ ise $ax + by = d$

o.s. $\exists x, y \in \mathbb{Z}$ vardır.

İspat // $i-S := \{ ax + by \mid \exists x, y \in \mathbb{Z}, ax + by > 0 \}$

$x=a$ ve $y=b$ alırsak, $aa + bb = a^2 + b^2 > 0$ olur.

Dolayısıyla $S \neq \emptyset$ olur. S nin en küçük elemanı vardır. Bunu d ile gösterelim. İddia ediyoruz ki, d : a ile b'nin ebob'dur. (yani d, hem a'yı hem de b'yi böler.)

$a = qd + r$ ve $0 \leq r < d$ o.s. (Bölme algoritmasından dolayı.)

$\exists q, r \in \mathbb{Z}$ vardır. $\exists x, y \in \mathbb{Z}, d = ax + by$ dir.

$$a = q(ax + by) + r \Rightarrow r = (1 - qx)a + (-qy)b \Rightarrow r \in S, r \neq 0$$

ve d, S nin en küçük elemanı olduğundan $r=0$ olmalıdır.

$a = qd$ olur. Ve $d|a$ olur. Aynı işlemler yapılarak $d|b$ olduğu gösterilebilir. 1. şart sağlanmış oldu. 2. şartın sağlandığını göstereyim.

ii- k, a ve b nin herhangi bir ortak böleni olsun.

$a = km, b = kn$ o.s. $\exists m, n \in \mathbb{Z}$ vardır.

$$d = ax + by = k(mx + ny) \Rightarrow k|d \quad \text{2. şart sağlanır. //}$$

$\left\{ \begin{array}{l} -34 \text{ ve } 16 \text{ sayılarının ortak böleni } 2 \text{ dir.} \\ -34(-1) + 16(-2) = 2 \end{array} \right\}$

İki tamsayının ebob'u 1 ise bu tamsayılara aralarında asaldır denir.

Teorem: $(m,n)=1$ ve $m|nc \Rightarrow m|c$

İspat: $(m,n)=1 \Rightarrow 1=mx+ny$ o.s. $\exists x,y \in \mathbb{Z}$ vardır.

$$\Rightarrow c = m \underline{c}x + ncy \quad \left. \begin{matrix} m|mc \\ m|nc \end{matrix} \right\} \Rightarrow m|(mc)x + (nc)y = c$$

p asal sayısı verilsin. $\exists n \in \mathbb{Z}$, $(p,n)=1$ veya $p|n$

Sonuç: $p|ab \Rightarrow p|a$ veya $p|b$

$$6|3.4 \Rightarrow 6 \nmid 3 \text{ ve } 6 \nmid 4 \Rightarrow 6 \text{ asal değildir.}$$

Eski sınav sorusu: $\left(\frac{a}{b}\right)^n \in \mathbb{Z} \Rightarrow \frac{a}{b} \in \mathbb{Z}$ dir. }

Önerme: $(a,b)=d$ olsun.

$$\left. \begin{matrix} a=a'd \\ b=b'd \end{matrix} \right\} \Rightarrow (a',b')=1 \text{ dir.}$$

$$\bullet (34,16)=2 \quad \left(\frac{34}{2}=17, \frac{16}{2}=8\right)=1 \text{ dir.}$$

İspat: $(a',b')=k > 1$ olsun. $a'=k\ell$, $b'=kt$ o.s. $\exists \ell, t \in \mathbb{Z}$.

$$\left. \begin{matrix} a=\ell(kd) \\ b=t(kd) \end{matrix} \right\} \Rightarrow (kd), a \text{ ve } b \text{ nin bir ortak böleni olur.}$$

$kd > d$ bir gelişkidir. $k > 1$ kabul ettik. O halde a ve b nin ebob'u d verildiğinden $k > 1$ olamaz. $(a',b')=1$ olmalıdır. //

$$\left\{ \begin{matrix} (a,b)=d \\ a'=ad \\ b'=bd \end{matrix} \right\} \Rightarrow \left(\frac{a}{d}, \frac{b}{d} \right)=1 \quad (a',b')=1$$

$$\forall n \in \mathbb{Z} (n > 1), n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t} \quad (p_i \text{ asal}, \alpha_i \in \mathbb{N})$$

Önerme: $(m,n)=1$ olsun. $(a,mn)=1 \Leftrightarrow \exists r,s \in \mathbb{Z}$ vardır ki,

$$(r,m)=1=(s,n) \text{ ve } a=nr+ms \text{ dir. Veya ;}$$

$$\left\{ (a,mn)=1 \Leftrightarrow (r,m)=1=(s,n) \text{ ve } a=nr+ms \text{ o.s. } \exists r,s \in \mathbb{Z} . \right\}$$

$$n \in \mathbb{Z}^+, \varphi(n) = \# \{ 1 \leq A < n, (A,n)=1 \}$$

$$\varphi(2)=1$$

$$\varphi(4)=2$$

$$\varphi(6)=2$$

$$\varphi(8)=4$$

$$\varphi(269)=268$$

$$\varphi(3)=2$$

$$\varphi(5)=4$$

$$\varphi(7)=2$$

↓
asal.

17 den önce hiçbir sayı bölmez.

Teorem: $(m,n)=1 \Rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n)$

133

$$\varphi(mn) = \# \{ 1 \leq a < mn, (a, mn) = 1 \}$$

$$\varphi(m) = \# \{ 1 \leq r < m, (r, m) = 1 \}$$

$$\varphi(n) = \# \{ 1 \leq s < n, (s, n) = 1 \}$$

$$\left\{ \begin{array}{l} (n?+m?, mn)=1 \\ \varphi(m)\varphi(n) \leq \varphi(mn) \end{array} \right\}$$

ispat// $(m,n)=1 \Rightarrow nX+mY = 1$ o.f. $\exists X,Y \in \mathbb{Z}$.

$$\Rightarrow: a = n(ax) + m(ay) \quad r = ax, s = ay$$

$$(r,m) = t \Rightarrow t|r \text{ ve } t|m \Rightarrow t|a, t|mn \Rightarrow t|(a, mn) = 1 \Rightarrow t = 1$$

$(s,n) = 1$ olduğu benzer şekilde gösterilir.

$$\Leftarrow: (a,m) = d \text{ diyelim. } d|a - ms = nr \left\{ \begin{array}{l} \Rightarrow d|r, d|(r,m) = 1 \quad d=1 \\ (m,n)=1 \text{ ve } d|m \Rightarrow (d,n)=1 \end{array} \right. \quad (a,n)=1 \text{ dir. //}$$

Benzer şekilde $(a,n)=1$ olur.

Euler Fonksiyonunun özellikleri :

1- $(m,n)=1 \Leftrightarrow \varphi(mn) = \varphi(m) \varphi(n)$

2- p asal ise $\varphi(p) = p-1 = p(1-\frac{1}{p})$ $\left\{ \begin{array}{l} \varphi(p): p \text{ den küçük, } p \text{ ile aralarında} \\ \text{asal sayıların sayısı.} \end{array} \right\}$

3- p asal ve $n > 0$, $\varphi(p^n) = p^n - p^{n-1} = p^n(1-\frac{1}{p})$

4- $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_t^{\alpha_t} \Rightarrow \varphi(m) = m(1-\frac{1}{p_1})(1-\frac{1}{p_2}) \dots (1-\frac{1}{p_t})$

$$\varphi(m) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_t^{\alpha_t})$$

$$= p_1^{\alpha_1} (1-\frac{1}{p_1}) p_2^{\alpha_2} (1-\frac{1}{p_2}) \dots p_t^{\alpha_t} (1-\frac{1}{p_t})$$

$$= \underline{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_t^{\alpha_t}} (1-\frac{1}{p_1})(1-\frac{1}{p_2}) \dots (1-\frac{1}{p_t})$$

$$= \underline{m} (1-\frac{1}{p_1})(1-\frac{1}{p_2}) \dots (1-\frac{1}{p_t}) \text{ dir. //}$$

3. özellik: $\# \{ 1 \leq s < p^n, (s, p^n) \neq 1 \} = p^{n-1}$

$$1p, 2p, \dots, p \cdot p, \dots, p^2 \cdot p, \dots, p^{n-1} \cdot p = p^n$$

p nin, p^{n-1} -inci katına kadar olan sayılar p^n ile aralarında

asal değildir.

$$(s, p^n) \neq 1 \Rightarrow s = kp \quad \{ (p^n, p^n) \neq 1 \}$$

Sorular:

13.05.2021

1- $\forall m, n \in \mathbb{Z}$ ($m \neq 0$) için $n = qm + r$ ve $|r| \leq \frac{|m|}{2}$ o.s. $\exists q, r \in \mathbb{Z}$.

(Bu yazılış tek türlü değildir.)

Gözüm // Euclide bölme algoritmasından (tam sayılarda kalanlı bölmeden),

$n = qm + r$ ve $0 \leq r < |m|$ o.s. $q, r \in \mathbb{Z}$ vardır.

i- $r \leq \frac{|m|}{2}$ ise ispat tamamdır.

ii- $r > \frac{|m|}{2}$ ise $n = \underbrace{(q+1)}_{q'}m + \underbrace{r-m}_{r'} = q'm + r'$

$r > \frac{|m|}{2} \Rightarrow |r-m| < \frac{|m|}{2}$ dir. //

2- $(a, mn) = 1 \Leftrightarrow (a, m) = 1 = (a, n)$ dir.

Gözüm // $\Rightarrow$: $(a, mn) = 1$ olsun. $(a, m) = d > 1$ olsa, d 'nin p gibi bir asal böleni vardır.

$\frac{p|a}{p|m} \Rightarrow p|mn$ ve $p|a \Rightarrow p|(a, mn) = 1 \neq \{ (a, n) = 1 \text{ olduğu da görülür.} \}$

$\Leftarrow$: $(a, mn) = k > 1$ olsa, k 'nin bir q asal böleni vardır.

$q|mn \Rightarrow q|m$ veya $q|n \neq \Rightarrow k=1$ olur. //

3- $\forall a, b \in \mathbb{Z}$ için $ax + by = 1$ o.s. $\exists x, y \in \mathbb{Z}$ ise $(a, b) = 1$ dir.

Gözüm // $(a, b) = k \Rightarrow k|a$ ve $k|b \Rightarrow k|ax$ ve $k|by \Rightarrow k|ax + by = 1$
 $\Rightarrow k=1 = (a, b)$ dir. //

4- $(m, n) = 1$, $a, b, m \in \mathbb{Z}$, $\frac{m|a}{n|a} \Rightarrow mn|a$ dir.

Gözüm // $m|a \Rightarrow a = mk$, $\exists k \in \mathbb{Z}$ ve $n|a \Rightarrow a = nt$, $\exists t \in \mathbb{Z}$

$a = mk = nt \Rightarrow m|t \Rightarrow t = mr$ o.s. $r \in \mathbb{Z}$.

$a = nt = (mn)r \Rightarrow mn|a$ dir. //

5- $(m, n) = 1 \Rightarrow (m+n, mn) = 1$ dir.

Gözüm // $(m+n, mn) = d > 1$ olsun. d 'nin en az bir p asal böleni vardır.

$p|d$ olduğundan $p|m+n$, $p|mn \Rightarrow p|m$ veya $p|n$

$p|m$ olsa $p|m+n$ olduğundan $p|n$ olur. $p|(m, n) = 1$ olduğundan gelibidir. //

$$\left. \begin{array}{l} A|B \\ A|B+C \end{array} \right\} \Rightarrow A|C \text{ dir, } B=AK \Rightarrow C=AT-B = AT-AK = A(T-K) \Rightarrow A|C \text{ olur. //}$$

6- Bir tamsayının n -inci dereceden kökü rasyonel sayı ise bu sayı tamsayı olmak zorundadır.

Gözüm // $n\sqrt{a} \in \mathbb{Q} \Rightarrow n\sqrt{a} \in \mathbb{Z} \quad (a \in \mathbb{Z}^+)$

1. $n\sqrt{a} = \frac{r}{s} \quad (r,s)=1 \text{ o.ü. } a = \left(\frac{r}{s}\right)^n = \frac{r^n}{s^n} \Rightarrow r^n = a s^n \text{ olur.}$

$(r,s)=1$ dir. $s > 1$ olsa s nin bir p asal böleni vardır.

$p|s \Rightarrow p|as^n = r^n \Rightarrow p|r$ olur. $p|(r,s)=1$ olduğundan

1'i bölemez. $s > 1$ olamaz. $s=1$ dir.

2. $\frac{r}{s} \in \mathbb{Q} \Rightarrow \left(\frac{r}{s}\right)^n \in \mathbb{Z}$ o.p. $\exists n \in \mathbb{N}$ varsa $\frac{r}{s} \in \mathbb{Z}$ old. gösterin.

$\left(\frac{r}{s}\right)^n = a \in \mathbb{Z} \Rightarrow \frac{r^n}{s^n} = a \Rightarrow r^n = a s^n \Rightarrow (r,s)=1$ dir.

$s > 1$ olsa s nin bir p asal böleni vardır.

$p|s \Rightarrow p|as^n = r^n \Rightarrow p|(r,s)=1$ dir. p asal olduğundan $s > 1$ old.

olması ile gelişir. 0 halde $s=1$ dir. //

7- $(a,b)=1 \Rightarrow (a+b, a-b)=1$ veya 2 dir.

Gözüm // $(a+b, a-b)=d$ olsun.

$d|(a+b+a-b)=2a \quad \left. \begin{array}{l} d|(a+b+a-b)=2a \\ d|(a+b-a+b)=2b \end{array} \right\} \Rightarrow d|(2a, 2b) = 2(a,b)$

$d|(a+b-a+b)=2b \quad d|2 \Rightarrow d|1 \vee d|2 //$

8- $(a,b)=1 \Rightarrow (a+b, a^2-ab+b^2)=1$ veya 3 olur.

Gözüm // $a^2-ab+b^2 = (a+b)^2 - 3ab$

$(a,b)=1 \Rightarrow (a+b, a^2-ab+b^2)=d > 1$ olsun.

$d|a+b, d|a^2-ab+b^2 = (a+b)^2 - 3ab$

$d|a+b \Rightarrow d|(a+b)^2$ ve $d|(a+b)^2 - 3ab \Rightarrow d|3ab$

d nin bir p asal böleni vardır. Çünkü $d > 1$

$p|d ; p|d|3ab \Rightarrow p|3ab \Rightarrow p|a$ veya $p|b$ veya $p|3$;

$p|a+b$ old. $p|a$ olsa $p|b$ olur. $p=3$ old. gösterelim. $t > 1$ olsa

$t-1 > 0 \quad d=3^t, 3^t = d|3ab \Rightarrow 3|3^{t-1}|ab. 3|a \vee 3|b$ olamaz.

Modüler Aritmetik

$m \neq 0$ olsun. $\forall a, b \in \mathbb{Z}$ için ;

$$a \equiv b \pmod{m} \iff m \mid a-b$$

$(m \in \mathbb{Z})$ " $\equiv$ " $\mathbb{Z}$ de bir denklik bağıntısıdır.

i- $\forall a \in \mathbb{Z}, m \mid (a-a) = 0 \Rightarrow a \equiv a \pmod{m}$ (yansıma)

ii- $a \equiv b \pmod{m} \Rightarrow m \mid a-b \Rightarrow m \mid -(a-b) = (b-a)$

$$\Rightarrow b \equiv a \pmod{m} \text{ (simetri)}$$

iii- $a \equiv b \pmod{m}$ ve $b \equiv c \pmod{m} \Rightarrow m \mid a-b$ ve $m \mid b-c$

$$\Rightarrow m \mid (a-b) + (b-c) = a-c$$

$$\Rightarrow a \equiv c \pmod{m} \text{ (geçirgenlik)}$$

$$a \equiv b \pmod{m} \vee a \equiv b \pmod{m}$$

$$a \in \mathbb{Z}, \bar{a} = \{b \in \mathbb{Z} \mid m \mid a-b\}$$

$$\left\{ \begin{array}{l} m=5, \bar{13} = \{ \dots, 8, 13, 18, 23, \dots \} \end{array} \right.$$

Önerme // $a \equiv b \pmod{m} \iff a$ ve b 'nin m ile bölümünden kalanlar eşittir.

İspat // $\Rightarrow$: $m \mid a-b \Rightarrow a-b = mk, \exists k \in \mathbb{Z}$

$$\left. \begin{array}{l} a = q_1 m + r_1 \\ b = q_2 m + r_2 \end{array} \right\} \Rightarrow 0 \leq r_1, r_2 < m \text{ o.s. } \exists q_1, q_2, r_1, r_2 \in \mathbb{Z}.$$

$$a = mk + b = q_1 m + r_1 \Rightarrow b = (q_1 - k)m + r_1 = q_2 m + r_2$$

$$q_1 - k = q_2, r_1 = r_2 \text{ (kalanlar eşittir.)}$$

$$\Leftarrow : \left. \begin{array}{l} a = q_1 m + r \\ b = q_2 m + r \end{array} \right\} \Rightarrow (a-b) = (q_1 - q_2)m \Rightarrow m \mid a-b \Rightarrow a \equiv b \pmod{m} \text{ dir. //}$$

$$\mathbb{Z}/\equiv = \mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\} \text{ (m-tane denklik sınıfı vardır.)}$$

$(\mathbb{Z}, +, \cdot)$ $\mathbb{Z}$ de çarpma işlemine göre tersi yoktur.

$$\bar{a} \oplus \bar{b} = \overline{a+b}, \bar{a} \odot \bar{b} = \overline{a \cdot b}$$

Önerme // $a = a_1(m), b = b_1(m)$ ise

i- $a+b \equiv (a_1+b_1) \pmod{m}$

ii- $a \cdot b \equiv (a_1 \cdot b_1) \pmod{m}$

(0 halde tanım kümesinde iki fonksiyonun farklı iki elemanı yoktur. = iyi tanımlıdır.)

İspat //
$$\left. \begin{array}{l} a - a_1 = mk \\ b - b_1 = mt \end{array} \right\} \Rightarrow (a+b) - (a_1+b_1) = m(k+t)$$

$$\Rightarrow m \mid (a+b) - (a_1+b_1)$$

$$\Rightarrow (a+b) \equiv (a_1+b_1) (m)$$

ii -
$$\left. \begin{array}{l} a = a_1 + mk \\ b = b_1 + mt \end{array} \right\} \Rightarrow ab = a_1b_1 + m(a_1t + b_1k + mkt)$$

$$\Rightarrow m \mid ab - a_1b_1$$

$$\Rightarrow ab \equiv a_1b_1 (m) //$$

$$\mathbb{Z}_6 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$$

$\bar{2} \circ ? = \bar{1}$ 2'nin tersi yok. 3 ve 4'ün de yok.

$\bar{1} \circ \bar{1} = \bar{1}$, $\bar{5} \circ \bar{5} = \bar{1}$ 1 ve 5'in tersi var.

$\mathbb{Z}_m$ deki denklik sınıfları = kalan sınıfı

$\mathbb{Z}_6$ da, $\bar{2} \circ \bar{3} = \bar{0}$ $\bar{3} \circ \bar{4} = \bar{0}$

TANIM: $\bar{a} \neq \bar{0}$ olsun. Eğer, $\bar{a} \cdot \bar{b} = \bar{0}$ o.p. $\exists \bar{0} \neq \bar{b} \in \mathbb{Z}_m$ varsa,

$\bar{a}$ ya ($\bar{b}$ 'ye de) sıfır bölen denir.

TANIM: $(a, m) = 1 \Rightarrow \bar{a} \in \mathbb{Z}_m$ 'ye asal kalan sınıf denir.

$\bar{a}_1 = \bar{a}$ asal, $m \mid a - a_1$ $(a_1, m) = 1$?

Önerme // $a \equiv b (m) \Rightarrow (a, m) = (b, m)$ dir.

İspat // $m \mid a - b \Rightarrow a = b + mk$, $(a, m) = t$ dersek,

i - $t \mid a$ ve $t \mid m$ $t \mid a - mk = b$

ii - d, b ile m nin ortak böleni ise $d \mid t$ $\{ (b, m) = d \}$ İspat

$(a, m) = t \Rightarrow ax + my = t$ o.p. $\exists x, y \in \mathbb{Z}$.

$d \mid b + mk = a$ ve $d \mid ax + my = t \Rightarrow d \mid t$ dir. //

$\mathbb{Z}_m^* :=$ asal kalan sınıfları kümesi

$$:= \{ \bar{a} \in \mathbb{Z}_m \mid (a, m) = 1 \}$$

$$\phi(\mathbb{Z}_m^*) = \phi(m)$$

$$\phi(1453) = 1452.$$

↓
asal.

Önerme // İki asal kalan sınıfın çarpımı da asaldır.

$$\bar{a}, \bar{b} \in \mathbb{Z}_m^* \Rightarrow \overline{ab} \in \mathbb{Z}_m^* \text{ dir.}$$

İspat // $(a, m) = 1 = (b, m)$

$$(a, m) = 1 \Rightarrow ax + my = 1 \text{ o.p. } \exists x, y \in \mathbb{Z}.$$

$$\Rightarrow b = bax + bmy \quad (*) \text{ olur. } (ab, m) = k \text{ diyelim.}$$

$$(*) \text{ eşitliğinden dolayı } k | abx + mby = b$$

$$\begin{matrix} k | b \\ k | m \end{matrix} \Rightarrow k | (b, m) = 1 \Rightarrow k = 1 \text{ dir.}$$

Önerme // $0 \neq \bar{a} \in \mathbb{Z}_m$ olsun.

$\bar{a}$ sıfır bölendir $\Leftrightarrow \bar{a}$ asal kalan sınıf değildir.

İspat // $\Rightarrow$: $\exists \bar{0} \neq \bar{b} \in \mathbb{Z}_m$ ki, $\bar{a} \cdot \bar{b} = \bar{0} \Rightarrow m | ab$.

$\bar{a}$ asal kalan sınıf olsaydı $(a, m) = 1$ olurdu.

$$m | ab \Rightarrow m | b \Rightarrow \bar{b} = \bar{0} \quad \#$$

0 halde; $\bar{a}$, asal kalan sınıf değildir.

$\Leftarrow$: $\bar{a}$ asal kalan sınıf olmasın. $(a, m) = d > 1$

$$\left. \begin{array}{l} a = a'd \\ m = m'd \end{array} \right\} \Rightarrow \begin{array}{l} (a', m') = 1 \quad \exists a', m' \in \mathbb{Z}. \\ \Rightarrow am' = (a'd)m' = a'm \\ \Rightarrow \overline{am'} = \bar{0} \Rightarrow \bar{a} \cdot \overline{m'} = \bar{0} \end{array}$$

$$\left\{ \begin{array}{l} \overline{m'} = \bar{0} \Rightarrow m' = mk \\ m = m'kd \Rightarrow 1 = kd \end{array} \right. \quad \begin{array}{l} d > 1 \\ d > 1 \end{array}$$

$\overline{m'} \neq \bar{0} \Rightarrow \bar{a}$ sıfır bölendir //

ANIM : $\bar{0} \neq \bar{a} \in \mathbb{Z}_m$, $\bar{a} \cdot \bar{c} = \bar{1}$ o.p. $\exists \bar{0} \neq \bar{c} \in \mathbb{Z}_m$ varsa

$\bar{c}$ 'ye $\bar{a}$ nin tersi denir.

Önerme // $\bar{a} \in \mathbb{Z}_m$ olsun. $\bar{a}$ tersi var $\Leftrightarrow \bar{a}$ asal kalan sınıfıdır.

İspat // $\Rightarrow$: $\bar{a} \in \mathbb{Z}_m$ nin tersi olsun. Yani $\bar{a} \cdot \bar{c} = \bar{1}$ o.p. $\exists \bar{c} \in \mathbb{Z}_m$ olsun.

$\bar{a}$ nin sıfır bölen olmadığını gösterirsek, $\bar{a}$ asal kalan sınıf olur.

$$\exists \bar{0} \neq \bar{b} \in \mathbb{Z}_m, \bar{a} \cdot \bar{b} = \bar{0} \text{ olsun. } \bar{c}(\bar{a} \cdot \bar{b}) = (\bar{c}\bar{a})\bar{b} = \bar{b} = \bar{0} \quad \#$$

0 halde $\bar{a}$ sıfır bölen değildir.

$\Leftarrow$: $\bar{a}$ bir asal kalan sınıfı olsun. $(a, m) = 1$ ve $xa + ym = 1$: O. PLAT

$\exists x, y \in \mathbb{Z}$ vardır. $xa \equiv 1 \pmod{m}$ $\vee$ $\bar{x} \cdot \bar{a} = 1$ olur.

0 halde $\bar{a}$ nın tersi vardır.

* $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ tersi vardır.
 $(\bar{6}, \bar{1}) = \bar{1}$ $(\bar{6}, \bar{5}) = \bar{1}$ $\bar{5}$ ve $\bar{1}$ asal kalan sınıfıdır.

$\mathbb{Z}_{54}$ 'de kaç tane sıfır bölen eleman var?

$\varphi(54)$ tane asal sınıf vardır. 0 hariç 53 eleman vardır.

$53 - \varphi(54)$ tane $(53 - 18 = 35)$ sıfır bölen vardır.

Sıfırın kendisi, sıfır bölen değildir.

Sonuç : p asal ise $\mathbb{Z}_p$ de sıfırdan farklı her kalan sınıfının tersi vardır. $(\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \bar{p-1}\})$ $\bar{p}$ ile bu sayılar aralarında asal.)

Teorem : (EULER) :

$m \in \mathbb{Z}, (a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$ veya $\bar{a}^{\varphi(m)} = \bar{1}$ dir.

İspat // $(a, m) = 1 \Rightarrow a \in \mathbb{Z}_m^*$

$f : \mathbb{Z}_m^* \rightarrow \mathbb{Z}_m^*$ $(\bar{a} \cdot \bar{x} \in \mathbb{Z}_m^*)$ dir. Önceki önermeden.
 $\frac{f}{\bar{x}} \rightarrow \bar{a}\bar{x}$

$f(\bar{x}_1) = f(\bar{x}_2) \Rightarrow \bar{a}\bar{x}_1 = \bar{a}\bar{x}_2 \Rightarrow \bar{a} \in \mathbb{Z}_m^* \Rightarrow \exists \bar{z} \in \mathbb{Z}_m, \exists \bar{a}\bar{z} = \bar{1}$

$\Rightarrow \bar{x}_1 = \bar{x}_2$ dir. $\Rightarrow f, 1:1$ dir. $\mathbb{Z}_m^* = \{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\varphi(m)}\}$

olduğundan, sortedü elemanlı bu kümenin 1:1 olması örten

olmasını da gerektirir.

0 halde $f, \mathbb{Z}_m^*$ in elemanlarını aralarında değiştireceğinden

$$\bar{a} \cdot \mathbb{Z}_m^* = \mathbb{Z}_m^* \Rightarrow (\bar{a} \cdot \bar{a}_1)(\bar{a} \cdot \bar{a}_2) \dots (\bar{a} \cdot \bar{a}_{\varphi(m)}) = \bar{a}_1 \cdot \bar{a}_2 \dots \bar{a}_{\varphi(m)}$$

$$= \bar{a}^{\varphi(m)} \bar{a}_1 \cdot \bar{a}_2 \dots \bar{a}_{\varphi(m)}$$

$$\bar{a}_1 \cdot \bar{a}_2 \dots \bar{a}_{\varphi(m)} = \bar{a}^{\varphi(m)} \bar{a}_1 \bar{a}_2 \dots \bar{a}_{\varphi(m)} \quad (\text{tersleriyle çarparsak})$$

$$1 = \bar{a}^{\varphi(m)} \text{ olur.}$$

Sonuç : (FERMAT) : Özel olarak $m = p \in \mathbb{Z}$ asal ise $(\forall a \in \mathbb{Z},)$

$$p \nmid a \Rightarrow a^{\varphi(p)} \equiv 1 \pmod{p} (= a^{p-1} \equiv 1 \pmod{p})$$

TANIM: $ax \equiv b \pmod{m}$ şeklindeki bir denkleme bir bilinmeyenli lineer kongrüans denir.

Önerme // $(a, m) = 1 \Rightarrow ax \equiv b \pmod{m}$ çözümünü vardır. (Ve bir tek $\text{mod } m$ kalan sınıfıdır.)

İspat // $(a, m) = 1 \Rightarrow ax_0 + by_0$ o.s. $\exists x_0, y_0 \in \mathbb{Z}$ $\left\{ \begin{array}{l} 3x \equiv 5 \pmod{7} \\ (3, 7) = 1 = 3 \cdot 5 + 7(-2) \\ 5 = 3(5 \cdot 5) + 7(-2)5 \\ 3(5 \cdot 5) \equiv 5 \pmod{7} \end{array} \right.$
 $\Rightarrow b = ax_0 + by_0$
 $\Rightarrow a(x_0b) \equiv b \pmod{m}$ //

İspat // $(a, m) = 1 \Rightarrow \bar{a} \in \mathbb{Z}_m^* : \exists \bar{c} \in \mathbb{Z}_m^*$ için $\bar{a} \cdot \bar{c} = \bar{1}$ dir.
 $\bar{a} \cdot \bar{c} \cdot x = x \equiv cx \pmod{m}$ //

$$\left\{ \begin{array}{l} ax_1 \equiv b \pmod{m} \\ ax_2 \equiv b \pmod{m} \end{array} \right\} \Rightarrow a(x_1 - x_2) = ax_1 - ax_2 \equiv 0 \pmod{m} \Rightarrow \bar{a}(\bar{x}_1 - \bar{x}_2) = \bar{0}$$

$$\Rightarrow \bar{x}_1 - \bar{x}_2 = \bar{0} \Rightarrow \bar{x}_1 = \bar{x}_2 \Rightarrow x_1 \equiv x_2 \pmod{m} //$$

Önerme // $ax \equiv b \pmod{m}$ nin, (a, m) -tane $\text{mod } m$ çözümünü var $\Leftrightarrow (a, m) \mid b$: mersost

İspat // $\Rightarrow$: $ax_0 \equiv b \pmod{m} \Rightarrow ax_0 - b = mk$ o.s. $\exists k \in \mathbb{Z}$,
 $(a, m) \mid ax_0 - mk = b \Rightarrow (a, m) \mid b$

$\Leftarrow$: $(a, m) = d \Rightarrow d \mid b$ olsun. $b = dk, \exists k \in \mathbb{Z}$.

$$\left. \begin{array}{l} a = a'd \\ m = m'd \end{array} \right\} \Rightarrow (a', m') = 1, \exists a', m' \in \mathbb{Z}.$$

$(a', m') = 1 \Rightarrow a'x \equiv k \pmod{m'}$ kongrüansının bir x_0 çözümü vardır.

Yani $a'x_0 \equiv k \pmod{m'} \Rightarrow a'x_0 - k = m't, t \in \mathbb{Z}$.

$$\Rightarrow d a'x_0 - dk = d m't$$

$$\Rightarrow ax_0 - b = mt$$

$$\Rightarrow ax_0 \equiv b \pmod{m}$$

$$x_0 + tm', \forall t \in \mathbb{Z}$$

$$t = qd + r, 0 \leq r < d \text{ o.s. } \exists q, r \in \mathbb{Z}.$$

$$x_0 + (qd + r)m' = x_0 + rm' + m'dq = x_0 + rm' + mq \equiv x_0 + rm' \pmod{m} \text{ pundaz}$$

Örnek,, $12X \equiv 9 \pmod{15}$, $(12, 15) = 3$, $3|9$

3 tane çözüm vardır.

$\Rightarrow 4X \equiv 3 \pmod{5}$ (4 ün tersi 4 olduğundan 4 ile denklemini çarparsak,) $\Rightarrow \pmod{5}'te$

$\Rightarrow X \equiv 2 \pmod{5}$

$\Rightarrow X = 2 + 5k$, $\forall k \in \mathbb{Z}$.

$k = 9 \cdot 3 + r$ $0 \leq r < 3$ o.ş. $\exists q, r \in \mathbb{Z}$.

$X = 2 + 5k = 2 + 5(9 \cdot 3 + r) = 2 + 5r + 15 \cdot 9 \equiv 2 + 5r \pmod{15}$

$r=0 \Rightarrow \bar{2}$, $r=1 \Rightarrow \bar{7}$, $r=2 \Rightarrow \bar{12}$

$\bar{2} \pmod{5}$, $\bar{2}, \bar{7}, \bar{12} \pmod{15}$
5'e bölünürse 2 kalanını verirler.

5'e bölündüğünde 2 kalanını veren sayılar, 15'e bölünürse;

$\bar{2}, \bar{7}, \bar{12}$ kalanını verir. //

Örnek,, $25X \equiv 10 \pmod{35}$

$(25, 35) = 5$, $5|10$, 5 tane çözüm vardır.

$\Rightarrow 5X \equiv 2 \pmod{7}$ $(5, 7) = 1$ 5 in $\pmod{7}$ deki tersi 3 olur.

Denklemini 3 ile çarparsak ;

$\Rightarrow X \equiv 6 \pmod{7}$

$\Rightarrow X = 6 + 7k$, $\forall k \in \mathbb{Z}$.

$\Rightarrow k = 5q + r$ $0 \leq r < 5$ o.ş. $\exists q, r \in \mathbb{Z}$.

$X = 6 + 7(5q + r) = 6 + 7r + 35q \equiv 6 + 7r \pmod{35}$

$r=0 \Rightarrow \bar{6}$, $r=1 \Rightarrow \bar{13}$, $r=2 \Rightarrow \bar{20}$, $r=3 \Rightarrow \bar{27}$, $r=4 \Rightarrow \bar{34}$ olur. //

Teorem: (ÇİN KALAN TEOREMİ):

$(m, n) = d$ olsun.

$\left. \begin{array}{l} X \equiv a \pmod{m} \\ X \equiv b \pmod{n} \end{array} \right\} \text{çözümü var} \Leftrightarrow a \equiv b \pmod{d}$

Örnek //
$$\left. \begin{array}{l} x \equiv 3 \pmod{12} \\ x \equiv 5 \pmod{14} \end{array} \right\} \text{çözümü var} \Leftrightarrow \begin{array}{c} a \quad b \quad d \\ 3 \equiv 5 \pmod{2} \\ \parallel \\ (14, 12) = 2 \\ d \end{array}$$

$$x = 3 + 12k, \forall k \in \mathbb{Z}.$$

$$\Rightarrow 3 + 12k \equiv 5 \pmod{14}$$

$$\Rightarrow 12k \equiv 2 \pmod{14}$$

$$\Rightarrow 6k \equiv 1 \pmod{7} \Rightarrow k \equiv 6 \pmod{7} \quad (6 \text{ nın } \pmod{7} \text{ de tersi } 6 \text{ dir.})$$

$$\Rightarrow k = 6 + 7r \text{ olur. Buradan,}$$

$$x = 3 + 12(6 + 7r) = 75 + 84r$$

$$\Rightarrow x \equiv 75 \pmod{84} \text{ olur. //}$$

Örnek // $x \equiv 2 \pmod{3}$

$$x \equiv 3 \pmod{4}$$

$$x \equiv 4 \pmod{5} \quad \text{çözümünü bulalım.}$$

$$\left. \begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \end{array} \right\} \Rightarrow x = 2 + 3k \equiv 3 \pmod{4}$$

$$k \equiv 3 \pmod{4} \quad k = 3 + 4r$$

$$\Rightarrow x = 2 + 3(3 + 4r) = 11 + 12r$$

$$\Rightarrow x = 11 + 12r \equiv 4 \pmod{5}$$

$$\Rightarrow x = 1 + 12r \equiv 4 \pmod{5}$$

$$\Rightarrow 2r \equiv 3 \pmod{5} \Rightarrow r \equiv 4 \pmod{5} \Rightarrow r = 4 + 5l, l \in \mathbb{Z}.$$

$$x = 11 + 12(4 + 5l) = 59 + 60l$$

$$\Rightarrow x \equiv 59 \pmod{60} //$$

Soru // 7'nin öyle bir katını bulun ki, 12'ye bölündüğünde 5, 13'e bölündüğünde 6, 8'e bölündüğünde 3 kalanını versin. : mod 1

$$x \equiv 0 \pmod{7}$$

$$x \equiv 5 \pmod{12}$$

$$x \equiv 6 \pmod{13}$$

$$x \equiv 3 \pmod{8}$$

Soru // $(\pmod{1})$ 'in denklik sınıfları nedir.

• Yalnızca 0 dir. kalan olmadığı için.

Örnek // $\left. \begin{array}{l} X \equiv 7 \pmod{10} \\ X \equiv 5 \pmod{27} \end{array} \right\} \text{çözümü nedir?}$

$(10, 27) = 1$ olduğundan, çin kalan teoremine göre sistemin mod 270 tek çözümü vardır.

* $X \equiv 7 \pmod{10} \Rightarrow X = 7 + 10k \equiv 5 \pmod{27}, k \in \mathbb{Z}$

$$\Rightarrow 10k \equiv -2 \equiv 25 \pmod{27}$$

$$\Rightarrow 10k - 27t = 25, k, t \in \mathbb{Z}$$

$$\Rightarrow -27t \equiv 3t \equiv 25 \equiv 5 \pmod{10}$$

$$\Rightarrow t \equiv 7.5 \equiv 5 \pmod{10}, t = 5$$

$$\Rightarrow 10k = 27 \cdot 5 + 25 = 160 \Rightarrow k = 16$$

$$\Rightarrow X = 7 + 10k = 7 + 10 \cdot 16 = 167$$

mod 270, $\overline{167}$ sınıfını oluşturur. Veya bir diğer çözüm :

* $X \equiv 5 \pmod{27} \Rightarrow X = 5 + 27k \equiv 7 \pmod{10}$

$$\Rightarrow X \equiv 27k \equiv 2 \pmod{10} \Rightarrow k \equiv 8 \pmod{10}$$

$$k = 6 + 10r \quad X = 5 + 27(6 + 10r) \Rightarrow X = 167 + 270r$$

$$\Rightarrow X \equiv 167 \pmod{270} //$$

Örnek // $\left. \begin{array}{l} 3X \equiv 2 \pmod{4} \\ 4X \equiv 3 \pmod{5} \end{array} \right\} \text{çözünüz.}$

$$\left. \begin{array}{l} 3X \equiv 2 \pmod{4} \Leftrightarrow X \equiv 2 \pmod{4} \\ 4X \equiv 3 \pmod{5} \Leftrightarrow X \equiv 2 \pmod{5} \end{array} \right\} \Rightarrow X = 2 + 4k \equiv 2 \pmod{5} \quad k \in \mathbb{Z}$$

$$\Rightarrow 4k \equiv 0 \pmod{5} \Rightarrow k \equiv 0 \pmod{5} \Rightarrow k = 5q \quad \forall q \in \mathbb{Z}$$

$$\Rightarrow X = 2 + 4(5q) = 2 + 20q$$

$$\Rightarrow X \equiv 2 \pmod{20} //$$

GRUPLAR

TANIM: $G \neq \emptyset$, $* : G \times G \rightarrow G$
 $(a,b) \rightarrow *(a,b) = a * b$? Eğer;

- i - $\forall a,b,c \in G$, $a * (b * c) = (a * b) * c$ (birleşme)
- ii - $\forall a \in G$, $a * e = e * a = a$ o.ş. $\exists e \in G$. (etkisiz eleman.)
- iii - $\forall a \in G$, $a * X = e$ ve $X * a = e$ o.ş. $\exists X \in G$, ise
 X 'e a 'nın tersi denir ve $X = a^{-1}$ olur. (ters eleman)

Bu üç özellik birden sağlanıyorsa $(G, *)$ 'e grup denir. (G 'ye grup denir.)
 Bunların yanında :

- iv - $\forall a,b \in G$, $a * b = b * a$ ise G 'ye değişmeli (abelyen) grup denir.

<u>Grup</u>	<u>Grup değil</u>
$(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +)$	$(\mathbb{Z}, \cdot)$ 3. özelliği sağlanmaz.
$F = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \dots \Rightarrow (F^*, \cdot)$ $F^* : F \setminus \{0\}$	$(\mathbb{R}, \cdot), (\mathbb{C}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{N}, +)$
$(F_n^m, +)$ ($G = \{1\}, \cdot$)	$(F_n^m, \cdot)$ tersi yoktur.
$(G = \{0\}, +), (\{I_n\}, \cdot)$	
$(G = \{1, -1, i, -i\}, \cdot)$	

$$a, b \in G \Rightarrow ab = a * b \text{ olur.}$$

Örnek, G ve H iki grup olsun. $\forall (g_1, h_1), (g_2, h_2) \in G \times H$,

$$(g_1, h_1) o (g_2, h_2) := (g_1 g_2, h_1 h_2)$$

$$o : (G \times H) \times (G \times H) \rightarrow G \times H \quad (\text{işlemdir.})$$

- i - $\forall (g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$,

$$\begin{aligned} (g_1, h_1) o [(g_2, h_2) o (g_3, h_3)] &= (g_1, h_1) o (g_2 g_3, h_2 h_3) \\ &= (g_1 (g_2 g_3), h_1 (h_2 h_3)) \\ &= ((g_1 g_2) g_3, (h_1 h_2) h_3) \\ &= [(g_1, h_1) o (g_2, h_2)] o (g_3, h_3) \end{aligned}$$

birleşme özelliği vardır.

ii- $\forall (g, h) \in G \times H$, $(e_G, e_H) \circ (g, h) = (e_G g, e_H h) = (g, h)$ ve
 $(g, h) \circ (e_G, e_H) = (g, h)$ (etkisiz eleman)

iii- $\forall (g, h) \in G \times H$,

$(g, h)^{-1} = (g^{-1}, h^{-1})$; $(g, h) \circ (g^{-1}, h^{-1}) = (g g^{-1}, h h^{-1}) = (e_G, e_H)$
 (ters eleman) $(g^{-1}, h^{-1}) \circ (g, h) = (g^{-1} g, h^{-1} h) = (e_G, e_H)$

iv- G ve H değişmeli grup ise $G \times H$ da değişmelidir.

1- Kapalılık var. $g_1, g_2 \in G$ ve $h_1, h_2 \in H$ olur.

2- $g_1 g_2$ ve $h_1 h_2$ çarpımları bir tek olduğundan farklı olamaz.

Yani iyi tanımlılık özelliği vardır.

Bu iki özellik işlemin tanımlı olduğunu gösterir.

Örnek // $A \neq \emptyset$, $S := \{ f: A \xrightarrow{1:1} A \}$ olsun. $(S, \circ)$ bir gruptur. (ödev)

$f, g \in S$, $f: A \xrightarrow{1:1} A$ $g: A \xrightarrow{1:1} A$ $(f \circ g) \in S$

$(f \circ g): A \longrightarrow A$
 $a \longrightarrow (f \circ g)(a) = f(g(a))$

$(f \circ g) \circ h \stackrel{?}{=} (f \circ (g \circ h))$ $\forall a \in A, f(a) = g(a) \Rightarrow f = g$

Önerme // i- G bir grup olsun. $\forall a, b, c \in G$ için,

$ab = ac \Rightarrow b = c$
 $ba = ca \Rightarrow b = c$ } dir. (Grupta kısaltma özelliği.)

Önerme // ii- G bir grup olsun. $\forall a, b \in G$ için,

$ax = b$
 $ya = b$ } o.s. $\exists x, y \in G$ vardır.

$ax_1 = ax_2 \Rightarrow x_1 = x_2$ dir.

tüm çözümler eşittir.

$(\mathbb{Z}, \cdot)$ grup değildir.

$ax = ay \Rightarrow ax - ay = 0$

$\Rightarrow a(x - y) = 0 \Rightarrow a \neq 0$

ve $x = y$ dir. //

$7x = 6$ çözümünü $\mathbb{Z}$ de yoktur.

TANIM: $a \in G, n \in \mathbb{Z}$,

$a^n := \begin{cases} \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ defa}}, & n > 0 \\ e, & n = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_{|n| \text{ defa}}, & n < 0 \end{cases}$

$na := \begin{cases} \underbrace{a + a + \dots + a}_{n \text{ defa}}, & n > 0 \\ e, & n = 0 \\ \underbrace{(-a) + (-a) + \dots + (-a)}_{|n| \text{ defa}}, & n < 0 \end{cases}$

Önerme // G bir grup olsun. $a \in G; m, n \in \mathbb{Z}$, (G çarpımsal grup)

i- $a^m \cdot a^n = a^{m+n}$

ii- $(a^m)^n = a^{mn}$

iii- G değişmeli ise $(ab)^n = a^n b^n$ dir.

İspat // i- $a^m \cdot a^n = (\underbrace{a \cdot a \cdot \dots \cdot a}_m) (\underbrace{a \cdot a \cdot \dots \cdot a}_n) = a^{m+n}$

ii- $(a^m)^n = (\underbrace{a^m \cdot a^m \cdot \dots \cdot a^m}_n)$

$= (\underbrace{a \cdot a \cdot \dots \cdot a}_m) (\underbrace{a \cdot a \cdot \dots \cdot a}_m) \dots (\underbrace{a \cdot a \cdot \dots \cdot a}_m)_{n \text{ tane}}$

$= a^{mn}$

iii- $(ab)^n = abab \dots ab = a^n b^n$

($ab=ba$ değişmeli olduğundan.)

Önerme // G bir grup olsun. $a \in G, m, n \in \mathbb{Z}$, (G toplamsal grup)

i- $m+na = (m+n)a$

ii- $m(na) = (mn)a$

G değişmeli ise

iii- $n(a+b) = na+nb$ dir.

İspat // Ödev.

Önerme // $G \neq \emptyset$ bir küme, " $\cdot$ " da G üzerinde birleşme

özellliğini sağlayan bir işlem olsun.

i- $\forall a \in G, e \cdot a = a$ o.ş $\exists e \in G$.

ii- $\forall a \in G, x \cdot a = e$ o.ş $\exists x \in G$.

sol birim

a 'nın sol tersi.

($e_{sol} = e_{sol} \cdot e_{sağ} = e_{sağ}$.)

İspat // $e=ax$ olduğunu gösterirsek $ae=a$ olduğunu göstermiş oluruz.

$xa=e$ as. $\exists x \in G$. (hipotezden), ($\forall a \in G$ için, i ve ii var olsun.)

$yx=e$ o.ş $\exists y \in G$.

$\Rightarrow (yx)a = ea$ (i. özellik)

$\Rightarrow y(\underbrace{xa}_e) = a \Rightarrow ye = a \Rightarrow y \underbrace{e}_x = ax \Rightarrow yx = ax = e = ax //$

$$ae = a(\underset{i-}{a^{-1}} \underset{i-}{a}) = (\underset{i-}{a} \underset{i-}{a^{-1}}) a = \underset{i-}{e} a = a$$

Not // Sol birim ve sol ters var ise, sağ birim ve sağ ters de vardır. Sadece sol ters varsa, sağ ters vardır diyemeyiz.

Önerme // $G \neq \emptyset$ bir küme ve, " $\cdot$ " da, G üzerinde birleşme özelliğini sağlayan bir işlem olsun.

$$\left. \begin{array}{l} \forall a, b \in G, ax = b \quad (i) \\ ya = b \quad (ii) \end{array} \right\} \text{o.ş. } \exists x, y \in G \Leftrightarrow G \text{ gruptur.}$$

$\Rightarrow$: İkinci denklemden $b = a$ alınırsa, $ya = a$ o.ş. $\exists y \in G$.

$$\forall a \in G; g = an \text{ o.ş. } \exists n \in G.$$

$$\Rightarrow yg = y(an) \text{ (Soldan } y \text{ ile çarparak)}$$

$$= (ya)n \text{ (birleşme öz.)}$$

$$\Rightarrow yg = an = g$$

$$\forall k \in G \text{ için } lk = y \text{ o.ş. } \exists l \in G.$$

$\Leftarrow$: G grup olsun. O halde her elemanın tersi vardır.

$$ax = b \Rightarrow a^{-1}(ax) = a^{-1}b \Rightarrow x = a^{-1}b \in G$$

$$ya = b \Rightarrow (ya)a^{-1} = ba^{-1} \Rightarrow y = ba^{-1} \in G \quad \left. \vphantom{\begin{array}{l} ax = b \\ ya = b \end{array}} \right\} \text{ olur.}$$

$\forall a, b \in G$ için sağlanır. //

Önerme // (Kısaltma Özelliği):

$G \neq \emptyset$ sonlu bir küme ve " $\cdot$ " da, G üzerinde birleşme

özelliğini sağlayan bir işlem olsun. Eğer $\forall a, b \in G$ için,

$$\left. \begin{array}{l} \text{soldan } ab = ac \Rightarrow b = c \\ \text{sağdan } ba = ca \Rightarrow b = c \end{array} \right\} \Rightarrow G \text{ bir gruptur.}$$

İspat // $G = \{x_1, x_2, \dots, x_n\}$ olsun. $a \in G$;

$$f: G \longrightarrow aG$$

$$x \longrightarrow f(x) = ax$$

$$f(x_1) = f(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2 \text{ (kıs. öz.)}$$

O halde f , 1:1 dir.

$aG \subset G$ olduğundan dolayı, ve
 G sonlu olduğundan f örterdir.

$$aG = G //$$

$$\left\{ \begin{array}{l} f^*: \mathbb{Z} \rightarrow 2\mathbb{Z} \\ x \mapsto 2x \end{array} \right.$$

1:1 dir fakat $\mathbb{Z}$ sonlu olmadığından örter değildir.

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

$$4.\mathbb{Z}_6 = \{\bar{0}, \bar{2}, \bar{4}\} \subset \mathbb{Z}_6 \text{ dir.}$$

$G \subset aG$ olamaz.

$\mathbb{Z}_7$ de kısıltma özelliği vardır.

$$\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}, \quad 4.\mathbb{Z}_7 = \{\bar{0}, \bar{4}, \bar{1}, \bar{5}, \bar{2}, \bar{6}, \bar{3}\} = \mathbb{Z}_7$$

Aynı ispat, sağ birim ve sağ ters varken de yapılır.

ispat// $\forall a \in G, f: G \rightarrow Ga$
 $x \mapsto f(x) = xa$

$$f(x_1) = f(x_2) \Rightarrow x_1 a = x_2 a \Rightarrow x_1 = x_2 \quad f, 1:1 \text{ dir.}$$

$Ga \subset G$ ve G sonlu olduğundan f örterdir. $Ga = G //$

$ea = e$ o.ş $\exists e \in G$ vardır. ($Ga = G$ olduğundan.)

e nin sol birim olduğunu göstermeliyiz. Bu e sadece a' ya etki etmediğini gösterdik. Halbuki e 'nin tüm elemanlara da sağdan etki etmediğini göstermeliyiz.

$$\forall b \in G \text{ için, } ab \in G = Gb$$

$$e(ab) = (ea)b = ab \quad (e, ab \text{ 'lere soldan etki etmedi.})$$

O halde e sol birimdir. Şimdi sol tersi bulalım.

$$\forall b \in G, Gb = G \text{ olduğundan ve } e \in G \text{ den,}$$

$$tb = e \text{ o.ş } \exists t \in G.$$

O halde b , sol ters olur. Buna göre;

Her elemanın sağ tersi ve sağ birimi olduğunda, sol tersi ve sol birimi de vardır. Önceki teoremlerden dolayı;

G bir gruptur. //

Alıstırmalar

1- G bir grup olsun. $\forall a \in G, a^2 = e \Rightarrow G$ deęiřmelidir.

Çözüm // $\forall x, y \in G$ alalım.

$$(xy)^2 = xyxy = e$$

$$x^{-1}(xyxy) = x^{-1}e \Rightarrow \underbrace{x^{-1}x}_e (yxy) = x^{-1}e$$

$$\Rightarrow yxy = x^{-1}e \text{ olur. Buradan,}$$

$$y^{-1}(yxy) = y^{-1}x^{-1}e \Rightarrow xy = y^{-1}x^{-1} \text{ olur.}$$

$$(x^2 = e \Rightarrow x.x = e \Rightarrow x = x^{-1} \text{ dir.})$$

x^{-1} yerine x , ve y^{-1} yerine de y yazarsak,

$$\Rightarrow xy = yx \Rightarrow G \text{ grubu deęiřmeli olur. //}$$

2- G bir grup olsun. $\forall a, b \in G$ için $(ab)^2 = a^2b^2 \Rightarrow G$ deęiřmelidir.

Çözüm // $(ab)^2 = abab = a^2b^2$

$$a^{-1}(abab) = a^{-1}(a^2b^2)$$

$$bab = ab^2$$

$$(bab)b^{-1} = (ab^2)b^{-1}$$

$$ba = ab$$

$\forall$ eleman için G deęiřmeli gruptur. //

3- 3 elemanlı bir grubun işlen tablosunu gösterip (deęiřmeli olduęunu) gösterin. $G = \{e, a, b\}$, $(G, *)$ grup.

Çözüm //

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$$a * e = e * a$$

4- Aynı soruyu 4 elemanlı küme için yapalım.

Çözüm // $G = \{e, a, b, c\}$, $(G, *)$ grup.

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$*$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

5- (20. soru) Eleman sayısı çift olan bir grupta tersi kendisine

eşit olan birimden farklı bir eleman daha bulunduğunu gösterin.

Çözüm // $* \quad e \quad \text{çift sayıda eleman (tekeleman)} \Rightarrow \text{eleman sayısı çift olur.}$

e	$\dots$	(x, x^{-1})	$\dots$	(y, y^{-1})	$\dots$
çift	$+$	$-$	$-$	$+$	$-$
sayıda	1	$-$	$-$	1	$-$
eleman	1	$-$	$-$	1	$-$
tek eleman	$-$	$-$	$-$	$-$	$-$

asıkta kalır.

örneğin, $(G = \{1, -1, i, -i\}, \cdot)$ grubunda birimden farklı (1'den farklı), tersi kendisi olan en az bir eleman vardır. Bu ise (-1) dir.

$\cdot$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	1	-1
-i	-i	i	-1	1

$(G, \cdot)$ gruptur.

$$(-1) \cdot (-1) = 1 \text{ olur.}$$

6- (2. soru) $G = \{a \in \mathbb{R} \mid -1 < a < 1\}$ ve $\forall a, b \in G$ için

$$a * b = \frac{a+b}{1+ab} \text{ ile bir } * \text{ işlemi tanımlansın. } (G, *) \text{ değişmeli}$$

bir grup mudur?

Çözüm // Kapalılık, birleşme, birim ve ters eleman ve değişmeli olduğunu gösterirsek, değişmeli grup olduğunu göstermiş oluruz.

i- Kapalılık : $\forall a, b \in G, \quad a * b = \frac{a+b}{1+ab} \in \mathbb{R} \text{ ve } -1 < a, b < 1$

$$-1 < \frac{a+b}{1+ab} < 1 \text{ dir.}$$

$$-1 < ab < 1 \Rightarrow -1 < ab \Rightarrow 1+ab > 0 \text{ olduğundan,}$$

$$a < 1, 1-b > 0 \Rightarrow a(1-b) < (1-b) \Rightarrow a+b < 1+ab \Rightarrow \frac{a+b}{1+ab} < 1$$

$$-1 < a, 1+b > 0 \Rightarrow -(1+b) < a(1+b) \Rightarrow -(1+ab) < a+b$$

$$\Rightarrow \frac{a+b}{1+ab} > -1 //$$

ii- Birleşme : $\forall a, b, c \in G$ için,

$$(a * b) * c = \frac{a+b+c+abc}{1+ab+ac+bc} = a * (b * c) \text{ dir. //$$

iii- Birim elemanı: $\forall a \in G$,

$$a * e = e * a = a \text{ o.ş } \exists e \in G ?$$

$$a * e = \frac{a+e}{1+ae} = a \Leftrightarrow a+e = a(1+ae) = a + a^2e$$

$$\Leftrightarrow a+e = a + a^2e$$

$$\Leftrightarrow e(1-a^2) = 0$$

$1-a^2 \neq 0$ olduğundan $e=0$ olur. $0 \in G$. //

iv - Ters elemanı: $a \in G$ olsun.

$$a * x = 0 \Leftrightarrow \frac{a+x}{1+ax} = 0 \Leftrightarrow x = -a$$

$-1 < a < 1$ olduğundan $-1 < -a < 1$ yani $-a \in G$ dir. //

v - $\forall a, b \in G$ için

$$\frac{a+b}{1+ab} = \frac{b+a}{1+ba} \text{ olduğundan değişme özelliği vardır.}$$

0 halde $(G, *)$ değişmeli gruptur.

Alt Gruplar

8.11.95/ Çarşamba

TANIM: G bir grup olsun. $\emptyset \neq A \subset G$ olsun. Eğer A , G 'nin işlevine göre bir grup oluyorsa, A ya G nin alt grubu denir. $A < G$ ile gösterilir.

$H = \{e\} < G$, $G < G$ aşıkâr (belli) alt gruptur. Bunlardan farklı ^{alt} gruplara özalt gruplar denir.

Önerme // G bir grup olsun. $\emptyset \neq H \subset G$ olsun.

$$H < G \Leftrightarrow \begin{cases} \text{i- } \forall a, b \in H, ab \in H, \text{ kapalılık} \\ \text{ii- } \forall a \in H, a^{-1} \in H, \text{ ters elemanı} \end{cases}$$

İspat // $\Rightarrow$: aşıktır.

$\Leftarrow$: $\forall a, b, c \in H \subset G$, $a(bc) = (ab)c$, birleşme

$\forall a \in H$, $a^{-1} \in H$ $aa^{-1} = e \in H$, Birim

Önerme // $H < G \Leftrightarrow \forall a, b \in H, ab^{-1} \in H$ (veya $a^{-1}b \in H$) olmasıdır.

İspat // $\Rightarrow$: $\forall b \in H$ için $b^{-1} \in H$ ve $\forall a, b \in H$ için

$ab^{-1} \in H$ olduğu görülür.

$\Leftarrow$: $\forall a, b \in H$ için $ab^{-1} \in H$ olsun. Birim elemanın olduğunu ve her elemanın da tersinin bulunduğunu gösterirsek, H nin alt grup olduğunu göstermiş oluruz.

$\forall a \in H, aa^{-1} = e \in H$ olur. (birim eleman)

$\forall b \in H$ için $eb^{-1} = b^{-1} \in H$ (ters eleman)

$\forall a, b \in H$ için $b^{-1} \in H$ olur. a ve b^{-1} için hipotezden

$a(b^{-1})^{-1} = ab \in H$ olur. (kapalılık.)

Soru // (4. soru) $G = \{z \in \mathbb{C} \mid |z| = 1\} \subset \mathbb{C}^*$ G alt grup mudur?

Çözüm // $\forall z_1, z_2 \in G, |z_1| = 1, |z_2| = 1$

$z_1 z_2^{-1} \in G$?

$$|z_1 z_2^{-1}| = |z_1 \frac{1}{z_2}| = \left| \frac{z_1}{z_2} \right| = \frac{|z_1|}{|z_2|} = 1 \Rightarrow z_1 z_2^{-1} \in G$$

O halde G bir alt gruptur.

Önerme // G sonlu bir grup ve $\emptyset \neq H < G$ olsun.

$H < G \Leftrightarrow \forall a, b \in H$ için $ab \in H$

İspat // $\forall a \in H$ alalım. (Her elemanın tersinin olduğunu ve birim elemanın bulunduğunu göstermeliyiz.)

$$a = e \Rightarrow a^{-1} = e \in H$$

$\Rightarrow$: aşıkıtır.

$\Leftarrow$: $a \neq e$ olsun. Hipotezden (kapalılıktan)

$$a, a^2, a^3, \dots, a^s, \dots, a^r, \dots \in H$$

a 'nın bazı kuvvetleri, H sonlu olduğundan $\exists r < s > 0$ için,

$$\exists a^r = a^s \text{ olur. } \Rightarrow a^{r-s} = e$$

$r-s > 0$ olduğundan $e \in H$ olur.

$\{ \forall a, b, c \in G, a(bc) = (ab)c \text{ birleşme özelliği vardır. } \}$

Şimdi a 'nın tersinin $a^{-1} \in H$ olduğunu gösterelim.

$a \neq e$ olduğundan $r-s > 1 \Rightarrow r-s-1 > 0$

$\Rightarrow a^{r-s-1} = a^{-1} \in H$ olur. Yani;

$$a \cdot \frac{a^{r-s-1}}{a^{-1}} = a^{r-s} = e \text{ dir. } //$$

a^{r-s-1} , a 'nın tersidir. $(a^{-1} = a^{r-s-1}) //$

$$\{ (\mathbb{Z} \setminus \{0\}, \cdot) \subset (\mathbb{R} \setminus \{0\}, \cdot) \}$$

$\{ \mathbb{R}, \text{sonlu olmadığından } \mathbb{Z} \text{ grup değildir. } \}$

Önerme // Bir grubun birtakım alt gruplarının arakesiti de alt gruptur.

İspat // $\{H_i\}_{i \in I}$ ailesi, G grubunun birtakım alt grupları olsunlar.

$H = \bigcap_{i \in I} H_i$ dersek, $\forall a, b \in H$ için $ab^{-1} \in H$ olduğunu gösterirsek,

$H < G$ olduğu anlaşılar.

$$a, b \in H \Rightarrow \forall i \in I, a, b \in H_i$$

$$\Rightarrow \forall i \in I, ab^{-1} \in H_i \quad (H_i < G)$$

$$\Rightarrow ab^{-1} \in H = \bigcap_{i \in I} H_i \text{ olur. } //$$

Önerme // $A, B < G \Rightarrow A \cup B \not< G$

A ve B alt grup ise birleşimleri alt grup olmayabilir.

$$\left\{ \begin{array}{l} \text{Örneğin: } 4\mathbb{Z} = \{4n \mid n \in \mathbb{Z}\} < (\mathbb{Z}, +) \end{array} \right\}$$

$$4n - 4b = 4(n-b) \in \mathbb{Z} \Rightarrow 4\mathbb{Z} \text{ alt gruptur.}$$

$$7\mathbb{Z} = \{7k \mid k \in \mathbb{Z}\} < (\mathbb{Z}, +)$$

$$7k - 7t = 7(k-t) \in \mathbb{Z} \Rightarrow 7\mathbb{Z} \text{ alt gruptur.}$$

$$8 \in 4\mathbb{Z}, 14 \in 7\mathbb{Z} \Rightarrow 14 + 8 = 22 \notin 4\mathbb{Z} \cup 7\mathbb{Z}$$

TANIM: G bir grup, $H, K \neq \emptyset < G$ olsun.

$$HK := \{ab \mid a \in H, b \in K\} \subset G$$

$x \in HK$ alalım. $\Rightarrow x = hk$ o.p. $\exists h \in H, \exists k \in K$.

$$H = \{a\} \Rightarrow HK = : aK = \{ax \mid x \in K\}$$

Önerme // $H, K < G$ olsun.

$HK < G \Leftrightarrow HK = KH$ olmasıdır.

İspat // $HK = \{ \dots, hk, \dots \} = \{ \dots, kh, \dots \} = KH$

$\left\{ \begin{array}{l} hk \text{ diğer kümeden bir elemana, } kh \text{ ise öteki kümeden bir} \\ \text{elemana eşittir. } H \text{ ve } K \text{ değişmeli ise } (hk = kh) \text{ } HK = KH \text{ olur.} \end{array} \right\}$ değişmeli

$\Rightarrow: \forall x \in HK$ alalım. $HK < G$ olduğundan $x^{-1} \in HK$.

$x^{-1} = hk$ olacak şekilde $\exists h \in H, k \in K$.

$$x = (x^{-1})^{-1} = \underset{EK}{k^{-1}} \underset{EH}{h^{-1}} \in KH$$

$$\Rightarrow HK \subset KH \quad (1)$$

$\forall y \in KH$ alalım. $KH < G$ olduğundan $y^{-1} \in KH$

$y^{-1} = kh$ olacak şekilde $\exists k \in K, h \in H$.

$$y = (y^{-1})^{-1} = \underset{EH}{h^{-1}} \underset{EK}{k^{-1}} \in HK$$

$$\Rightarrow KH \subset HK \quad (2)$$

(1) ve (2) den $HK = KH$ olur.

$\Leftarrow: HK = KH$ olduğunu kabul edelim. $\forall x, y \in HK$

$x = h_1 k_1 \quad y = h_2 k_2$ o.s. $h_1, h_2 \in H$ ve $k_1, k_2 \in K$.

$xy^{-1} \in HK$? bakalım.

$$xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$$

$$= h_1 (k h_2^{-1})$$

$$= (h_1 k) k'$$

$$= (h_1 h) k' \in HK$$

$$\left\{ \begin{array}{l} k_1 k_2^{-1} = k \in K \\ k h_2^{-1} \in HK \\ h h_2^{-1} = h k' \text{ o.s. } h \in K, k' \in K \end{array} \right.$$

$\Rightarrow HK < G$ olur. //

Soru // G bir grup olsun.

$$M = \{ a \in G \mid \forall x \in G, \overset{\text{değişmeli}}{ax = xa} \} < G \text{ dir.}$$

Bu kümeye G 'nin merkezi denir.

$$\forall g \in G \text{ için } eg = ge = g \Rightarrow e \in M \Rightarrow e \in M \neq \emptyset$$

M de bapten farklı en az bir tane elemanı (e) vardır.

$\forall a, b \in M$ alalım. $\forall g \in G$, $ag = ga$, $bg = gb$.

: minör

$b^{-1}g = gb^{-1}$? bakalım.

$$bg = gb \Rightarrow b^{-1}bg = b^{-1}gb \Rightarrow g = b^{-1}gb$$

$$\Rightarrow gb^{-1} = b^{-1}gb b^{-1}$$

$$\Rightarrow gb^{-1} = b^{-1}g \quad (\text{tersi de değişmeli})$$

$$0 \text{ halde, } (ab)g = a(bg) = (ag)b = (ga)b = g(ab)$$

$$\therefore (ab)g = g(ab) \quad //$$

9./ Soru // G bir grup olsun. $a \in G$ ike

: soru

$M(a) = \{g \in G \mid ga = ag\}$ kümesinin, G nin bir alt grubu olduğunu gösterin. Bu alt gruba a 'nın merkezleştiricisi denir.

$M(a) < G$ dir. $ea = ae = a$ olduğundan $e \in M(a)$, $M(a) \neq \emptyset$.

$\forall x, y \in M(a)$ alalım. $xa = ax$ ve $ya = ay$ dir.

$(xy^{-1})a = a(y^{-1}x)$ olduğunu, veya $(xy)a = a(xy)$ olduğunu göstermeliyiz.

$$ya = ay \Rightarrow \underbrace{y^{-1}}_e ya = y^{-1}ay \Rightarrow a = y^{-1}ay \Rightarrow ay^{-1} = y^{-1}a \underbrace{yy^{-1}}_e \\ \Rightarrow ay^{-1} = y^{-1}a$$

$$(xy)a = x(ya) = (xa)y = (ax)y = a(xy) \text{ dir.}$$

$$0 \text{ halde } \underline{(xy)a = a(xy)} \Rightarrow xy \in M(a) //$$

: MÜHÜR

Devirli Alt Gruplar

Tanım: G bir grup olsun. $\emptyset \neq M \subseteq G$ olsun. M yi kapsayan G 'nin tüm alt gruplarının arakesitine M kümesiyle üretilmiş alt grup denir. $\langle M \rangle$ ile gösterilir.

$$\langle M \rangle := \bigcap_{i \in I} G_i \quad \forall i \in I, G_i < G \text{ ve } M \subseteq G_i$$

$$\left\{ \begin{array}{l} (\mathbb{Z}, +), \\ M = \{-9, -3, 5, 15, 23\} \end{array} \right.$$

$\emptyset$ ve M den farklı birim elemanı içeren alt kümeler M yi kapsayanların arakesiti, M kümesinde üretilen alt grubu verir.

Önerme: $\langle M \rangle = \{ a_1^{n_1} a_2^{n_2} \dots a_t^{n_t} \mid t \in \mathbb{N}, n_i \in \mathbb{Z}, a_i \in M \}$

yani M nin ürettiği alt grup bu kümeyle gösterilir.

İspat // $A := \{ a_1^{n_1} a_2^{n_2} \dots a_t^{n_t} \mid t \in \mathbb{N}, n_i \in \mathbb{Z}, a_i \in M \}$ olsun.

$\Rightarrow: M \subseteq A$ ve $A < G$ olduğunu göstermeliyiz.

$M \subseteq A \Rightarrow \langle M \rangle \subseteq A$ olur.

$A < G$

$$x, y \in A, \quad x = a_1^{n_1} a_2^{n_2} \dots a_t^{n_t} \quad y = b_1^{m_1} b_2^{m_2} \dots b_s^{m_s}$$

$$xy^{-1} = (a_1^{n_1} a_2^{n_2} \dots a_t^{n_t} \cdot b_s^{-m_s} b_{s-1}^{-m_{s-1}} \dots b_2^{-m_2} b_1^{-m_1}) \in A.$$

$$\forall x = a_1^{n_1} a_2^{n_2} \dots a_t^{n_t} \quad \forall 1 \leq i \leq t \text{ için } a_i \in M \subseteq G_j, \forall j \in J \text{ için}$$

$G_j < G$ dir.

$$\forall 1 \leq i \leq t, a_i^{n_i} \in G_j, \forall i \in I \text{ için,}$$

$$x = a_1^{n_1} a_2^{n_2} \dots a_t^{n_t} \in G_j$$

$$x \in \bigcap_{j \in J} G_j = \langle M \rangle \Rightarrow A \subseteq \langle M \rangle$$

O halde $\langle M \rangle = A$. yani

$$M = \{ a_1^{n_1} a_2^{n_2} \dots a_t^{n_t} \mid t \in \mathbb{N}, n_i \in \mathbb{Z}, a_i \in M \}$$

TANIM: $M = \{a\}$ tek elemanlı bir küme ise $\langle M \rangle$ alt grubuna devirli alt grup denir. (Gösterim olarak içeriye a eleman yazılır.)

$$M = \{a\} \Rightarrow \langle M \rangle =: \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

$$\langle M \rangle = \langle a \rangle$$

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ çarpımsal alt grup için devirli grup.

$\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$ toplamsal alt grup için devirli grup.

Örnek // $(\mathbb{Z}, +) = \langle 1 \rangle$ ile üretilmiştir.

$$(\mathbb{Z}, +) = \langle 1 \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\}$$

$$(\mathbb{Z}, +) = \langle -1 \rangle = \{n(-1) \mid n \in \mathbb{Z}\}$$

$\Rightarrow$ farklı elemanlar aynı küneyi üretebilir. -15

Örnek // $(G = \{1, -1, i, -i\}, \cdot)$ için, (4. mertebeden sonlu devirli gruptur.)

$$G = \langle i \rangle = \{1, -1, i, -i\} = \langle -i \rangle = \{i^n \mid n \in \mathbb{Z}\}$$

Örnek // $(\mathbb{Z}_6, +)$ için,

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \langle \bar{1} \rangle = \{n \cdot \bar{1} \mid n \in \mathbb{Z}\} \Rightarrow o(\bar{1}) = 6$$

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \langle \bar{5} \rangle = \{n \cdot \bar{5} \mid n \in \mathbb{Z}\} \Rightarrow o(\bar{5}) = 6$$

TANIM: G bir grup ve $a \in G$ olsun.

$o(G) = |G|$ grubun eleman sayısını verir.

$o(a) := \langle a \rangle$ a 'nın ürettiği devirli grubun eleman sayısına a elemanın mertebesi denir.

Örnek // $\mathbb{Z}_6$ da, $o(\bar{2}) = 3$. $\bar{2}$ nin mertebesi 3 olur. yani

$$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{0}\} < \mathbb{Z}_6 \quad \bar{2} \text{ ile üretilen devirli alt gruptaki eleman}$$

sayısı 3 olur. //

$$\mathbb{Z}_6, o(\bar{5}) = 6 \text{ dir. //$$

Örnek // $\mathbb{Z}_m, \bar{1}$ ile üretilmiş m . mertebeden devirli gruptur.

• $G = \langle a \rangle$ olsun. a nın tüm pozitif kuvvetleri için :

1- Eğer $o(G) = \infty$ ise a 'nın tüm pozitif kuvvetleri birbirinden farklıdır.

$$a, a^2, a^3, \dots, a^s, \dots, a^r, \dots \in G.$$

Gerçekten, $r > s > 0$ için $a^r = a^s$ olsa,

$$a^{r-s} = e \text{ olur. } (r-s > 0)$$

$$\langle M \rangle = \langle a \rangle$$

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ çarpımsal alt grup için devirli grup.

$\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$ toplamsal alt grup için devirli grup.

Örnek // $(\mathbb{Z}, +) = \langle 1 \rangle$ ile üretilmiştir.

$$(\mathbb{Z}, +) = \langle 1 \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\}$$

$$(\mathbb{Z}, +) = \langle -1 \rangle = \{n(-1) \mid n \in \mathbb{Z}\}$$

$\Rightarrow$ farklı elemanlar aynı kümeyi üretebilir.

Örnek // $(G = \{1, -1, i, -i\}, \cdot)$ için, (4. mertebeden sonlu devirli gruptur.)

$$G = \langle i \rangle = \{1, -1, i, -i\} = \langle -i \rangle = \{i^n \mid n \in \mathbb{Z}\}$$

Örnek // $(\mathbb{Z}_6, +)$ için,

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \langle \bar{1} \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\} \Rightarrow o(\bar{1}) = 6$$

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \langle \bar{5} \rangle = \{n \cdot 5 \mid n \in \mathbb{Z}\} \Rightarrow o(\bar{5}) = 6$$

TANIM: G bir grup ve $a \in G$ olsun.

$o(G) = |G|$ grubun eleman sayısını verir.

$o(a) := \langle a \rangle$ a 'nın ürettiği devirli grubun eleman sayısına a elemanın mertebesi denir.

Örnek // $\mathbb{Z}_6$ da, $o(\bar{2}) = 3$. $\bar{2}$ nin mertebesi 3 olur. yani

$$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{0}\} < \mathbb{Z}_6 \quad \bar{2} \text{ ile üretilen devirli alt gruptaki eleman}$$

sayısı 3 olur. //

$$\mathbb{Z}_6, o(\bar{5}) = 6 \text{ dir. //$$

Örnek // $\mathbb{Z}_m$, $\bar{1}$ ile üretilmiş m . mertebeden devirli gruptur.

• $G = \langle a \rangle$ olsun. a nın tüm pozitif kuvvetleri için ;

1- Eğer $o(G) = \infty$ ise a 'nın tüm pozitif kuvvetleri birbirinden farklıdır.

$$a, a^2, a^3, \dots, a^s, \dots, a^r, \dots \in G.$$

Gerçekten, $r > s > 0$ için $a^r = a^s$ olsa,

$$a^{r-s} = e \text{ olur. } (r-s > 0)$$

$$a^n = e, m = qn + r, 0 \leq r < n$$

$$a^m = a^{qn+r} = a^r.$$

Eğer a nın tüm pozitif kuvvetleri birbirinden farklı ise G sonsuz gruptur. (a nın tüm kuvvetleri farklıdır.)

ii- a nın bazı pozitif kuvvetleri birbirinin aynı ise,

$$a, a^2, a^3, \dots, a^s, \dots, a^r, \dots$$

$$r > s > 0 \text{ için } a^r = a^s \text{ olsa } \Rightarrow a^{r-s} = e \quad r-s > 0$$

$a^m = e$ olan en küçük pozitif tam sayı m olsun.

($\mathbb{Z}^+$ nın en küçük elemanı var olduğundan.)

G nin eleman sayısı m olur. $o(G) = m$ dir.

$$x \in G = \langle a \rangle \text{ alalım. } x = a^t \text{ o.s. } \exists t \in \mathbb{Z}.$$

$$t = qm + r \quad 0 \leq r < m \quad \text{o.s. } \exists q, r \in \mathbb{Z}.$$

$$G = \{e, a, a^2, \dots, a^{m-1}\} \text{ olduğunu göstereceğiz.}$$

$$x = a^t = (a^m)^q a^r = a^r \in \{e, a, a^2, \dots, a^{m-1}\}$$

$$\Rightarrow G \subset \{e, a, a^2, \dots, a^{m-1}\} \text{ ve}$$

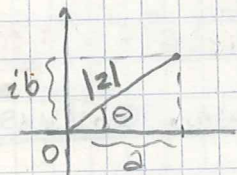
$$\Rightarrow G \supset \{e, a, a^2, \dots, a^{m-1}\} \text{ olduğu aşiktır.}$$

O halde G nin eleman sayısı m tane dir. //

{ Bir grubun kendisi devirli olmadan alt grubu devirli olabilir. }
 $\mathbb{C} \setminus \{0\}$ i ve $-i$ ile üretilir. $(\mathbb{C} \setminus \{0\}, \cdot)$

Soru // $(\mathbb{C}^*, \cdot)$ gruptur. $z = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ z nin ürettiği devirli alt grupları belirleyin. $o\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = ?$ mertebesini bulun.

$$z = a + ib \quad |z| = \sqrt{a^2 + b^2}$$



$$\cos \theta = \frac{a}{|z|} \quad \sin \theta = \frac{b}{|z|}$$

$$z = |z|(\cos(\theta + 2k\pi) + i \sin(\theta + 2k\pi))$$

z nin pozitif kuvvetlerini alacağız. Birimi bulana kadar, elemanlar bu devirli grubun elemanı olur. $z^6 = 1$ olduğundan bu grupta $\langle z \rangle = \{1, z, z^2, z^3, z^4, z^5\}$ olur. Negatif kuvvetler için yine bu elemanlar bulunur. Şimdi bunu görelim:

$$\theta = \pi/3 \quad z^n = |z|^n (\cos(\theta + 2k\pi) + i \sin(\theta + 2k\pi))^n$$

$$\Rightarrow z^n = |z|^n (\cos n(\theta + 2k\pi) + i \sin n(\theta + 2k\pi))$$

$$\Rightarrow z^n = |z|^n (\cos(n\theta + 2nk\pi) + i \sin(n\theta + 2nk\pi))$$

$$\text{Buradan } |z| = \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = \sqrt{\frac{1}{4} + \frac{3}{4}} = 1$$

$$\begin{aligned} \Rightarrow \left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^n &= 1 \left(\cos\left(\frac{\pi}{3} + 2k\pi\right) + i \sin\left(\frac{\pi}{3} + 2k\pi\right)\right)^n \\ &= \cos\left(\frac{n\pi}{3} + 2k\pi n\right) + i \sin\left(\frac{n\pi}{3} + 2k\pi n\right) \stackrel{?}{=} 1 \text{ olmalı.} \end{aligned}$$

n 'i bulmanız gerekir.

$$n=6 \text{ olmalıdır. } (2\pi \text{ nin katlarında } \overset{=\theta}{\cos\theta} = 1, \sin\theta = 0)$$

$$o\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = 6$$

$$\langle z \rangle = \{1, z, z^2, z^3, z^4, z^5\} //$$

$$z^{-1} = \frac{1}{z} \in \langle z \rangle ?$$

$$z \cdot \frac{1}{z} = 1. ? \quad z^{-1} = ? \quad \frac{1}{z} = \frac{1}{\frac{1}{2} + i\frac{\sqrt{3}}{2}} = \frac{2}{1 + i\sqrt{3}} = \frac{1 - i\sqrt{3}}{2}$$

$$\left. \begin{aligned} z^5 &= \cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3} \\ &= \frac{1}{2} - i\frac{\sqrt{3}}{2} \end{aligned} \right\} \text{Gerekten, } z^{-1} = z^5 \text{ olduğu görülür.}$$

$$\text{Buna göre ; } z^{-2} = (z^{-1})^2 = z^4, \quad z^{-3} = z^3, \quad z^{-4} = z^2 \text{ dir.}$$

Önerme: Devirli bir grubun her alt grubu devirlidir.

İspat // $G = \langle a \rangle$ ve $H \leq G$ olsun.

H 'in devirli alt grup olduğunu göstereceğiz.

$i - H = \{e\} \Rightarrow H = \langle e \rangle$ yani H 'in e ile üretilen devirli grup olduğu aşiktır. (Tüm alt gruplar e 'yi kapsar ve bunların arkasittleri e yi verir.)

ii- $H \neq \{e\}$ ise $\exists e \neq x \in H$ ve $x = a^t$, $\exists t \in \mathbb{Z}$ ($t \neq 0$)

$$x^{-1} = a^{-t} \in H \quad \left(H \leq G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \text{ olduğundan} \right)$$

a 'nın bazı pozitif kuvvetleri H 'in içine düşer. Bunların en küçüğünü m ile gösterelim. Yani $a^m \in H$ olan en küçük pozitif tamsayı m olsun.

$$a^m \in H \Rightarrow \langle a^m \rangle \subset H \quad \dots (1)$$

(a^m yi kapsayan grupların arakesiti)

$$\left\{ \langle m \rangle := \bigcap_{i \in I} G_i \quad m \text{ yi kapsayan } G \text{ gruplarının arakesiti.} \right\}$$

Şimdi de ters kapsamayı gösterelim.

$\forall a^s \in H$ alalım. s 'yi m 'ye bölelim.

$$s = qm + r, \quad 0 \leq r < m \quad \text{o.ş. } \exists q, r \in \mathbb{Z}.$$

$$a^s = a^{mq} \cdot a^r \Rightarrow \underbrace{a^{mq}}_{\in H} \cdot \underbrace{a^r}_{\in H} = a^r \in H \text{ olur.}$$

m nin en küçük seçilişinden dolayı $r = 0$ olur. 0 halde,

$$a^s = a^{mq} = (a^m)^q \in \langle a^m \rangle$$

$$\Rightarrow H \subset \langle a^m \rangle \quad \dots (2)$$

(1) ve (2) den dolayı $H = \langle a^m \rangle$ olur. Yani

H alt grubu da devirli dir. //

Örnek₁₁ $(\mathbb{Z}, +)$ 'de $\langle n, a \rangle = \langle n \rangle = \mathbb{Z}$ olur.

$\langle 5 \rangle = \mathbb{Z}$ dir. Çünkü 5 tamsayısını hiçbir alt grubun kesipimi vermez yalnız $\mathbb{Z}$ nin kendisi 5'i içinde bulundurur. (kapsar.)

Örnek₁₁ $A = \{3, 5\} \subset \mathbb{Z}$, $\langle A \rangle = \mathbb{Z}$ dir. Çünkü 3, 5 tamsayılarını kapsayıp, diğer alt gruplarla kesipimi A yı veren grup yoktur. Sadece $\mathbb{Z}$ nin kendisi A yı kapsar. Arakesitleri A 'yı verir.

Örnek₁₁ $A = \{6, 9\} \subset \mathbb{Z}$ $\langle A \rangle = \langle 3 \rangle$ olur. Çünkü 3 ve $\mathbb{Z}$, A kümesini kapsar. (3 ün katları). Kesipimleri $\langle 3 \rangle$ olur. $\{\text{obeb}(6, 9) = 3, //\}$

21.11.95

SALI

iki küme arasında 1:1 ve örten bir fonksiyon varsa, bu kümeler aynı mertebededir denir.

İkisi de sonlu küme ise eleman sayıları aynı olmalıdır. Eğer, sonsuz kümeler ise eleman sayısından bahsedemeyiz, bunun yerine mertebeyi kullanırız.

Örnek // $f: \mathbb{Z} \rightarrow \mathbb{Z}$
 $x \rightarrow f(x) = \frac{x}{3}$

$$f(x_1) = f(x_2) \Rightarrow \frac{x_1}{3} = \frac{x_2}{3} \Rightarrow x_1 = x_2 \quad f, 1:1 \text{ dir.}$$

$$\forall y \in \mathbb{Z}, x = 3y \in \mathbb{Z} \quad f(3y) = f(x) = y \quad \text{o.s. } \exists x \in \mathbb{Z}. \quad f, \text{ örten dir.}$$

Örnek // $f: (0,1) \rightarrow \mathbb{R}$
 $x \rightarrow f(x) = \frac{a+b}{1+ab} \in \mathbb{R} \quad f \text{ fonksiyonu } 1:1 \text{ ve örten dir.}$

Önerme: G bir grup ve $a \in G$, $o(a) = n$ olsun. $\rightarrow a$ 'nın mertebesi.

$$a^k = e \Leftrightarrow n | k //$$

İspat // $\Rightarrow: a^k = e$ olsun. $k = qn + r$, $0 \leq r < n$ o.s. $\exists q, r \in \mathbb{Z}$.

$$e = a^k = a^{qn+r} = a^{qn} \cdot a^r = e \cdot a^r = a^r$$

$o(a) = n$ olduğundan $r = 0$ olmalıdır.

$$\Rightarrow k / qn \Rightarrow n | k$$

$\Leftarrow: n | k$ olsun. $k = nt$ i $\exists t \in \mathbb{Z}$ ise

$$a^k = (a^n)^t = e^t = e \quad \text{olur.} //$$

Önerme: $G = \langle a \rangle$ ve $o(a) = n$ olsun.

$$\langle a^s \rangle = G \Leftrightarrow (s, n) = 1 //$$

$$\langle a \rangle = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\} \text{ olsun. } \Rightarrow o(a) = 8$$

$$\langle a^3 \rangle = \{a^3, a^6, a, a^4, a^7, a^2, a^5, a^8 = e\} = \langle a \rangle, \quad (8, 3) = 1 \text{ old.}$$

$\phi(n)$ tane üreteç vardır. //

İspat // $\Rightarrow a^s, G$ nin bir üreteci ise $G = \langle a \rangle = \langle a^s \rangle$ dir.

$$\langle a^s \rangle = \langle a \rangle \text{ olsun.}$$

$a \in \langle a^s \rangle \Rightarrow a = a^{st}$ o.s. $\exists t \in \mathbb{Z}$. Kısaltma özelliğini kullanarak,

$a^{st-1} = e$ ve önceki önermeden,

$n/st-1 \Rightarrow st-1 = kn$ o.s. $\exists k \in \mathbb{Z}$.

$\Rightarrow st - nk = 1 \Rightarrow (s, n) = 1$ olur. //

$\Leftarrow$: Tersine $(s, n) = 1$ olsun.

$sx + ny = 1$ o.s. $\exists x, y \in \mathbb{Z}$.

$a^s \in \langle a \rangle \Rightarrow \langle a^s \rangle \subset \langle a \rangle$ (üretme tanımından)
 $\downarrow$
 a^s yi kapsayan alt grupların arakesiti
(bu alt gruplardan birisi de a^s olur.)

0 halde $\langle a^s \rangle \subset \langle a \rangle$ dir. --- ①

$$a = a^{sx+ny} = a^{sx} \cdot a^{ny} = a^{sx} \cdot e = a^{sx}$$

$$\Rightarrow a = (a^s)^x \quad x \in \mathbb{Z}$$

$$\Rightarrow a \in \langle a^s \rangle \Rightarrow \langle a \rangle \subset \langle a^s \rangle \text{ dir. --- ②}$$

Sonuç olarak ① ve ② den $\langle a \rangle = \langle a^s \rangle = G$ olur. //

Önerme: $G = \langle a \rangle$ sonsuz devirli grubunun tüm üreteçleri a ve a^{-1} dir.

(Sonsuz devirli grubun üreteçleri a ve tersidir.)

İspat // $\langle a^s \rangle = \langle a \rangle$ olsa, $a \in \langle a^s \rangle$

$$\Rightarrow a = a^{st} \text{ o.s. } \exists t \in \mathbb{Z}.$$

$$\Rightarrow a^{st-1} = e \quad (G \text{ sonsuz olduğundan})$$

$$\Rightarrow st-1 = 0 \text{ olmalıdır. 0 halde.}$$

$$st = 1 \Rightarrow s=1, t=1 \vee s=-1, t=-1 \text{ olurdu.}$$

Soru // $\langle A \rangle = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$ üreteçleri nelerdir.

$$\left[\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right]^n = \left[\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \right] \quad \forall n \in \mathbb{N}. \quad (\text{Bunu gösterelim.})$$

Tümevarımı kullanarak,

$$n=1 \text{ için, } \left[\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right]^1 = \left[\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right] \text{ olur.}$$

$$\left\{ o(\langle A \rangle) = o(\langle A^{-1} \rangle) = \text{sonsuzdur.} \right\}$$

$n=k$ için, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$ olsun.

$n=k+1$ için $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k+1} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}$ olur mu, bakalım.

$$\Rightarrow \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix} \text{ oldu.}$$

0 halde $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{n+1} = \begin{bmatrix} 1 & n+1 \\ 0 & 1 \end{bmatrix}$ dir. //

$$\langle A^{-1} \rangle = \langle \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \rangle$$

0 halde verilen $\mathbb{Z}^k$ grup, sonsuz devirli gruptur.

A^{-1} ve A , determinanı 1 olan 2×2 tipinde matrisleri üretir.

Soru // G bir grup ve $a, b \in G$ olsun. $o(a) = 5$ ve $aba^{-1} = b^2$ ise $o(b) = ?$

$$aba^{-1} = b^2 \Rightarrow (aba^{-1})^2 = b^4$$

$$(aba^{-1})(aba^{-1}) = b^4$$

$$\underline{ab^2a^{-1}} = b^4$$

$$a(aba^{-1})a^{-1} = b^4$$

$$a^2ba^{-2} = b^4$$

$$(a^2ba^{-2})^2 = b^8$$

$$(a^2ba^{-2})(a^2ba^{-2}) = b^8$$

$$\underline{a^2b^2a^{-2}} = b^8$$

$$a^2(aba^{-1})a^{-2} = b^8$$

$$a^3ba^{-3} = b^8$$

$$(a^3ba^{-3})(a^3ba^{-3}) = b^{16}$$

$$\underline{a^3b^2a^{-3}} = b^{16}$$

$$a^3(aba^{-1})a^{-3} = b^{16}$$

$$a^4ba^{-4} = b^{16}$$

$$(a^4ba^{-4})(a^4ba^{-4}) = b^{32}$$

$$\underline{a^4b^2a^{-4}} = b^{32} \Rightarrow \uparrow$$

$$\left\{ \begin{array}{l} o(a) = 5 \text{ ise} \\ a^5 = e \text{ olur.} \end{array} \right.$$

$$\Rightarrow a^4(aba^{-1})a^{-4} = b^{32}$$

$$\underline{a^5ba^{-5}} = b^{32}$$

$$ebe = b^{32}$$

$$b = b^{32}$$

$$\underline{e = b^{31}}$$

$$o(b) \mid 31$$

$$\Rightarrow o(b) = 31 \vee 1 \quad (b=e \text{ ise})$$

3 Soru // $Q^* = \langle \frac{a}{b} \rangle$? $(a,b)=1$ $\{(Q^*, \cdot)\}$ devirli grup olamaz.

Çözüm: $\forall x = \frac{c}{d}, \frac{c}{d} = (\frac{a}{b})^k$ o.s $\exists k \in \mathbb{Z}$. $(c,d)=1$.

$$\Rightarrow cb^k = da^k \Rightarrow \begin{matrix} c|a^k \\ d|b^k \end{matrix} \quad (b,d)=1 \text{ olsun.}$$

o halde $Q^* = Q \setminus \{0\}$ devirli grup olamaz.

9 Soru // G bir grup ve $a \in G$ ise $o(a) = o(a^{-1})$ dir.

Çözüm: $a \in G, o(a) = n$ ve $o(a^{-1}) = m$ olsun.

$$a^m = e \Leftrightarrow n|m \text{ olduğundan,}$$

$$\left. \begin{aligned} a^n = e &\Rightarrow (a^n)^{-1} = a^{-n} = (a^{-1})^n = e \Rightarrow m = o(a^{-1}) | n \\ (a^{-1})^m = a^{-m} = (a^m)^{-1} = e &\Rightarrow a^m = e \Rightarrow n = o(a) | m \end{aligned} \right\} \Rightarrow m=n \text{ olur.}$$

G grubu sonsuz ise, sonsuz devirli grubun üreteçleri yalnız

a ve a^{-1} olduğundan $o(a) = o(a^{-1})$ olur. //

10 Soru // G bir grup, $a, b \in G$ ise $o(a) = o(bab^{-1})$?

Çözüm // $o(a) = m$ ve $o(bab^{-1}) = n$ olsun.

$$(bab^{-1})^m = \underbrace{(bab^{-1})(bab^{-1}) \dots (bab^{-1})}_{m \text{ tane}} = ba^mb^{-1} = e$$

$$ba^mb^{-1} = e \Rightarrow b^{-1}ba^mb^{-1}b = b^{-1}eb \Rightarrow a^m = e \Rightarrow n|m$$

$$(bab^{-1})^n = \underbrace{(bab^{-1})(bab^{-1}) \dots (bab^{-1})}_{n \text{ tane}} = ba^n b^{-1} = e$$

$$ba^n b^{-1} = e \Rightarrow b^{-1}ba^n b^{-1}b = b^{-1}eb \Rightarrow a^n = e \Rightarrow m|n$$

$$\Rightarrow m=n \Rightarrow o(a) = o(bab^{-1}) \text{ olur. //$$

Soru // (Sınav Sorusu) $\mathbb{Z}_{42}$ de $o(\overline{30}) = ?$

Çözüm: $\mathbb{Z}_{42} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{30}, \dots, \overline{41}\}$

$$o(a) = n \text{ olsun, } \begin{cases} o(a^m) = \frac{n}{(\min)} \\ \text{grupsal grupta.} \end{cases}$$

$$\left. \begin{aligned} \text{Toplamasal grupta} \\ na = e \\ o(ma) = \frac{n}{(\min)} \end{aligned} \right\}$$

$$\mathbb{Z}_{42} = \langle \overline{1} \rangle, \quad o(\overline{1}) = 42$$

$$o(30.\overline{1}) = \frac{42}{(30,42)} = \frac{42}{6} = 7 // \quad 30.\overline{1} = \overline{30}$$

$$\star G = \langle a \rangle, \quad o(a) = n \text{ olsun.}$$

$$\langle a^s \rangle = \langle a \rangle \Leftrightarrow (s, n) = 1 \text{ dir.}$$

$$\varphi(42) = \varphi(6)\varphi(7) = \underbrace{\varphi(2)}_1 \underbrace{\varphi(3)}_2 \underbrace{\varphi(7)}_6 = 12 \text{ tane.}$$

$$S := 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$$

$$\textcircled{1} \text{ } \cancel{2} \text{ } \cancel{3} \text{ } \cancel{4} \text{ } \textcircled{5} \text{ } \cancel{6} \text{ } \cancel{7} \text{ } \cancel{8} \text{ } \cancel{9} \text{ } \cancel{10} \text{ } \textcircled{11} \text{ } \dots \text{ } \cancel{40} \text{ } \textcircled{41}$$

$$\langle S, \cdot \rangle = \mathbb{Z}_{42} //$$

→ 42 ile aralarında
asal olan
sayılar.

Önerme: Devirli grubun her alt grubu devirlidir. Buna bağlı olarak;

- i - Sonsuz devirli grubun her alt grubu da sonsuz devirlidir.
- ii - $\langle a \rangle$, n . mertebeden bir devirli grup ise her alt grubun mertebesi n 'yi böler. Tersine n 'nin her pozitif q böleni için mertebesi q olan ($\langle a \rangle$ 'nin) bir tek alt grubu vardır.

$$H < \langle a \rangle \Rightarrow H = \langle a^s \rangle \text{ olsun. } s > 0 \in \mathbb{Z}^+$$

İspat, i - $o(H) = k$ olsa, $\Rightarrow o(a^s) = k \Rightarrow (a^s)^k = e$

$$\Rightarrow a^{sk} = e \quad \# \quad sk > 0 \text{ olmalıdır.}$$

O halde, sonsuz devirli grubun her alt grubu da sonsuz devirlidir.

İspat, ii - $n = sq + r, \quad 0 \leq r < s \text{ o.ş } \exists q, r \in \mathbb{Z}.$

$$a^n = e = a^{sq+r} = a^{sq} \cdot a^r \Rightarrow a^r = (a^s)^{-q} \in H$$

$$H = \langle a^s \rangle$$

$0 \leq r < s$ olmak zorunda. $r = 0$ olmalıdır. Yani;

$$n = sq \Rightarrow q \mid n //$$

Tersine $q \mid n$ olsun.

$$\Rightarrow n = ql \text{ o.ş } \exists l \in \mathbb{Z}^+.$$

$$\left. \begin{array}{l} H = \langle a^s \rangle \\ H = \{a^s, a^{2s}, \dots, a^{(q-1)s}, a^{qs} = e\} \\ o(H) = q \end{array} \right\}$$

($n \in \mathbb{Z}^+$ ve $s \in \mathbb{Z}^+$ old.) $o(\langle a^q \rangle) = q$ olur. Grubun mertebesi q olur.
 a^q ile üretilen alt grup.

Bir tek olması; n ve q verilmiş iken $\frac{n}{q}$ tek, yani l tektir.

O halde $\langle a^q \rangle$ de tek olur. //

Soru // $\mathbb{Z} \times \mathbb{Z}$ ne ile üretilmiştir?

$$(a,b) + (c,d) = (a+c, b+d) \quad \text{etkisiz eleman sıfırdır.}$$

$$\begin{cases} \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \\ = \{na \mid n \in \mathbb{Z}\} \end{cases}$$

$$\begin{aligned} \langle M \rangle &= \{a_1^{n_1} \dots a_t^{n_t}\} \quad \text{grupsal grp.} \\ &= \{na_1 + \dots + na_t \mid n_i \in \mathbb{Z}, t \in \mathbb{N}, a_i \in M\} \\ &\quad \text{toplamsal grp.} \end{aligned}$$

$\forall (x,y) \in \mathbb{Z} \times \mathbb{Z}$ için,

$$(x,y) = k(a,b) \text{ o.s } k \in \mathbb{Z} \text{ yoktur.}$$

(yani $\mathbb{Z} \times \mathbb{Z} \neq \langle (a,b) \rangle$ tek elemanla üretilemez.)

0 halde $\mathbb{Z} \times \mathbb{Z} = \langle (a,b), (c,d) \rangle$ olsun.

$$(x,y) = k(a,b) + l(c,d) \quad \text{o.s } \exists k, l \in \mathbb{Z}.$$

$$\begin{aligned} ka + lc &= x \\ kb + ld &= y \end{aligned}$$

$$k = \frac{\begin{vmatrix} x & c \\ y & d \end{vmatrix}}{\begin{vmatrix} a & c \\ b & d \end{vmatrix}} = \frac{xd - yc}{ad - bc}$$

$$l = \frac{\begin{vmatrix} a & x \\ b & y \end{vmatrix}}{\begin{vmatrix} a & c \\ b & d \end{vmatrix}} = \frac{ay - bx}{ad - bc}$$

$ad - bc = +1 \vee -1$ ise k ve l tamsayı olacağından

$ad - bc = 1$ veya $ad - bc = -1$ olmalıdır.

Örneğin $(5,7) = k(2,3) + l(3,4) \Rightarrow k=1$ ve $l=1$ olur. //

Soru // $\mathbb{Z}_2 \times \mathbb{Z}_2$ nin alt gruplarını bulalım. (Devirli dâirleri)

merkezi 2'dir.

tüm //

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

gıftı, tek
sayıların kümesi.

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$$

birim
merkezi 1'dir.

$$H_1 = \{(\bar{0}, \bar{0})\}$$

$$H_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \Rightarrow \text{devirli değildir.}$$

$$H_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1})\} \Rightarrow (\bar{0}, \bar{1}) \text{ ile üretilir.}$$

$$H_4 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0})\} \Rightarrow (\bar{1}, \bar{0}) \text{ ile üretilir.}$$

$$H_5 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\} \Rightarrow (\bar{1}, \bar{1}) \text{ ile üretilir.}$$

$$\left. \begin{aligned} o((\bar{0}, \bar{0})) &= 1 \\ o((\bar{0}, \bar{1})) &= 2 \\ o((\bar{1}, \bar{0})) &= 2 \\ o((\bar{1}, \bar{1})) &= 2 \end{aligned} \right\}$$

kendisi devirli olmadığı halde, tüm alt grupları devirlidir.

Ödev // $\mathbb{Z}_{20} = \{0, 1, \dots, 19\}$ ise $\mathbb{Z}_{20}$ nin devirli alt grupları nelerdir?

{ Mertebe : 0 elemanı tarafından üretilen grubun eleman sayısına, 0 elemanın mertebesi denir.

Grup sonlu ise, a'nın birimi veren en küçük kuvvettir.

{ yani, mertebe sonlu ise ($o(a) < \infty$) birimi veren en küçük pozitif kuvvettir.

Soru : (16) $G = \langle a \rangle$, $o(a) = mn$ ise $o(a^n) = m$ dir. Gösterin.

($a^m = e \Leftrightarrow n|m$ idi. $o(a) = n$ için.)

Görüm // $a^{mn} = e \Rightarrow (a^n)^m = e$ o halde

$o(a^n) | m$ dir. Tersine : $o(a^n) = k$ diyelim.

$$a^{nk} = e \Rightarrow mn | nk \Rightarrow m | k = o(a^n)$$

$$\Rightarrow m = o(a^n) \text{ olur. //}$$

Soru // $a, b \in \mathbb{Z}^+$, $a|b$ ve $b|a \Rightarrow a=b$ dir. ?

Görüm // $a|b \Rightarrow b = ak$ o.s. $\exists k \in \mathbb{Z}^+$.

$b|a \Rightarrow a = bt$ o.s. $\exists t \in \mathbb{Z}^+$.

$$b = ak = (bt)k = b(tk) \Rightarrow tk | 1 \Rightarrow t = k = 1 \text{ dir.}$$

O halde, $a = b$ olur. //

Soru // (1) G grup ve $a, b \in G$ olsun. $o(a) = n \Rightarrow$

$$a^r = a^s \Leftrightarrow r \equiv s (n) \text{ dir.}$$

Görüm // $\Leftrightarrow : a^r = a^s \Leftrightarrow a^{r-s} = e \Leftrightarrow n | r-s \Leftrightarrow r \equiv s (n)$ //

Soru // (13) G grup, $a \in G$ ve $o(a) = n$ olsun. $o(a^m) = \frac{n}{(m,n)}$ dir.

Görüm // $(m, n) = d$, $o(a) = n$ $a \in G$ olsun. $m = m'd$ $n = n'd$

$(m', n') = 1$ o.s. $\exists m', n' \in \mathbb{Z}$. $o(a^m) = k$ diyelim.

$$\Rightarrow (a^m)^k = e \Rightarrow a^{mk} = e \text{ dir. } \Rightarrow n | mk \Rightarrow n'd | m'dk \Rightarrow n' | m'k$$

$$(n', m') = 1 \Rightarrow n' | k \dots \textcircled{1} \quad (a^m)^{n'} = a^{mn'} = a^{m'dn'} = a^{m'n} =$$

$$= (a^n)^{m'} = e \Rightarrow k | n' \dots \textcircled{2} \quad 1 \text{ ve } 2 \text{ den } n' = k \text{ olur.}$$

$$n' = n'd \Rightarrow n' = \frac{n}{d} \quad o(a^m) = k = n' = \frac{n}{d} = \frac{n}{(m,n)} \text{ // olur.}$$

Normal Alt Gruplar

$$\left\{ \begin{array}{l} a, b \in \mathbb{Z}, m > 0 \quad \overline{a} \odot \overline{b} = \overline{ab} \quad \overline{a} \oplus \overline{b} = \overline{a+b} \\ a \equiv b(m) \Leftrightarrow m | a-b \\ a \preceq b \stackrel{tn}{\Leftrightarrow} a > 0, b > 0 \text{ denklik bağıntısı değildir.} \\ a \preceq b \Leftrightarrow ab > 0 \text{ yansıma yok.} \\ a \preceq b \Leftrightarrow ab \geq 0 \text{ yansıma var.} \end{array} \right.$$

$$a \equiv b(m) \Leftrightarrow m | a-b$$

$$a \preceq b \stackrel{tn}{\Leftrightarrow} a > 0, b > 0 \text{ denklik bağıntısı değildir.}$$

$$a \preceq b \Leftrightarrow ab > 0 \text{ yansıma yok.}$$

$$a \preceq b \Leftrightarrow ab \geq 0 \text{ yansıma var.}$$

$$\bullet \forall a \in \mathbb{Z}, aa \geq 0 \Rightarrow a \preceq a$$

$$\bullet a \preceq b \Rightarrow ab \geq 0 \Rightarrow ba \geq 0 \Rightarrow b \preceq a$$

$$\bullet a \preceq b \text{ ve } b \preceq c \Rightarrow ab \geq 0, bc \geq 0$$

$$\downarrow 0 \\ \Rightarrow ab = 0 \quad \text{Denklik bağıntısı değil.}$$

Ödev // 3 elemanlı ve 4 elemanlı kümeler üzerinde kaç tane farklı denklik bağıntısı vardır.

10 * $H < G$ olsun. $\forall a, b \in G$ için,

$$a \equiv_R b(H) \stackrel{tn}{\Leftrightarrow} ab^{-1} \in H \quad (\text{Sag koset})$$

G üzerinde bir denklik bağıntısıdır.

i- $\forall a \in G$ için, $aa^{-1} = e$ ve $H < G$ olduğundan $e \in H$

$$\Rightarrow a \equiv a(H) \quad (\text{yansıma})$$

ii- $\forall a, b \in G$ için, $a \equiv b(H) \Rightarrow ab^{-1} \in H$ dir. $H < G$ olduğundan

$$(ab^{-1})^{-1} = ba^{-1} \in H \Rightarrow b \equiv a(H) \quad (\text{simetri})$$

iii- $\forall a, b, c \in G$ için,

$$a \equiv b(H) \text{ ve } b \equiv c(H) \Rightarrow ab^{-1} \in H \text{ ve } bc^{-1} \in H \quad H < G \text{ olduğundan}$$

$$(ab^{-1})(bc^{-1}) = ac^{-1} \in H \Rightarrow a \equiv c(H) \quad (\text{geçişme}) //$$

$$a \in G \text{ için } \overline{a} = ?$$

$$\overline{a} = \{x \in G \mid xa^{-1} \in H\} = \{x \in G \mid xa^{-1} = h \text{ o.s } \exists h \in H\}$$

$$= \{x \in G \mid x \in Ha\} = Ha$$

$$\overline{a} = Ha //$$

$$x \in \bar{a} \text{ alalım. } (\Leftrightarrow) a \equiv x(H) (\Leftrightarrow) xa^{-1} \in H$$

$$(\Leftrightarrow) xa^{-1} = h \text{ o.ş } \exists h \in H.$$

$$(\Leftrightarrow) x = ha \text{ o.ş } \exists h \in H$$

$$(\Leftrightarrow) x \in Ha$$

$$G = \bigcup_{i \in I} Ha_i \quad (Ha_i = Ha_j \Leftrightarrow i = j) \quad a_i \in G.$$

denklik bağıntısının
ayrık ailelerinin birleşimi bir gruptur.
farklı denklik sınıfları.

2° ★ $H < G$ olsun. $\forall a, b \in G$ için,

$$\underline{a \equiv_L b(H) \Leftrightarrow a^{-1}b \in H} \quad (\text{sol koset})$$

G üzerinde bir denklik bağıntısıdır.

i- $\forall a \in G$ için, $aa^{-1} = e$ ve $H < G$ olduğundan $e \in H$
 $\Rightarrow a \equiv a(H)$ (yansıma)

ii- $\forall a, b \in G$ için, $a \equiv b(H) \Rightarrow a^{-1}b \in H$ dir. $H < G$ olduğundan
 $(a^{-1}b)^{-1} = b^{-1}a \in H \Rightarrow b \equiv a(H)$ (simetri)

iii- $\forall a, b, c \in G$ için,

$a \equiv b(H)$ ve $b \equiv c(H) \Rightarrow a^{-1}b \in H$ ve $b^{-1}c \in H$, $H < G$ den
 $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H \Rightarrow a \equiv c(H)$ (gesirme)

$a \in G$ için $\bar{a} = ?$

$$\bar{a} = \{x \in G \mid a^{-1}x \in H\} = \{x \in G \mid a^{-1}x = h \text{ o.ş } \exists h \in H\}$$

$$= \{x \in G \mid x \in aH\} = aH$$

$\bar{a} = aH //$

$$x \in \bar{a} \text{ alalım } (\Leftrightarrow) a \equiv x(H) (\Leftrightarrow) a^{-1}x \in H$$

$$(\Leftrightarrow) a^{-1}x = h \text{ o.ş } \exists h \in H$$

$$(\Leftrightarrow) x = ah \text{ o.ş } \exists h \in H.$$

$$(\Leftrightarrow) x \in aH$$

O halde $\equiv_R$ ve $\equiv_L$, G üzerinde birer denklik bağıntısıdır.

Bu bağıntılara göre bir elemanın denklik sınıfına KOSET denir.

$\bar{a} = Ha$, sağ koset (sağ denklik bağıntısı) }
 $\bar{a} = aH$, sol koset (sol " " ") } denir.

(Değişme özelliği varsa $aH = Ha$ olur.)

i- $o(aH) = o(H) = o(Ha)$

Her denklik sınıfında aynı mertebeden eleman vardır.

$f: aH \rightarrow H$ (f, 1:1 ve örten bir fonksiyondur.)
 $aH \rightarrow h$ (f: $Ha \rightarrow H$ 'da vardır.)
 $ha \rightarrow h$

$f(ah_1) = f(ah_2) \Rightarrow h_1 = h_2 \Rightarrow ah_1 = ah_2 \therefore f, 1:1$ dir.

$\forall h \in H$ için $ah \in aH$ dir ve $f(ah) = h \therefore f, \text{örten}$ dir.

ii- $Ha = Hb \Leftrightarrow ab^{-1} \in H$, $aH = bH \Leftrightarrow a^{-1}b \in H$

iii- $\mathcal{R}$: farklı sağ kosetlerin kümesi

$\mathcal{L}$: farklı sol kosetlerin kümesi

iddia ediyoruz ki, $o(\mathcal{R}) = o(\mathcal{L})$ dir.

$\mathcal{R} \xrightarrow[örten]{1:1} \mathcal{L}$ olur mu?

$Ha \rightarrow a^{-1}H$ tanımlayalım. $\forall a \in G$ için $a^{-1} \in G$ bir tektir.

(Bir tek sol koset bulunur.) O halde bir fonksiyondur.

$\left\{ \begin{array}{l} f: A \rightarrow B, \text{ farklı görüntü yollar.} \\ \forall x, y \in A \text{ için } x=y \Rightarrow f(x)=f(y) \text{ iyi tanımlılık.} \\ a \neq b, ab^{-1} \in H, \Rightarrow aH = Hb \Rightarrow a^{-1}H = b^{-1}H \text{ olmalı} \end{array} \right.$

Aşıktaki hiçbir eleman kalmaz, yani,

$Ha \rightarrow a^{-1}H$ $Ha = Hb \Leftrightarrow ab^{-1} \in H.$

Görüntüler farklı olsa, yani,

$Ha = Hb \Rightarrow (a^{-1})^{-1}b^{-1} = ab^{-1} \in H$
 $\Rightarrow a^{-1} \in b^{-1}(H) \Rightarrow a^{-1}H = b^{-1}H$

(kendileri eşitse, görüntüleri de eşittir.

1:1 liği gösterelim:

$\psi(Ha) = \psi(Hb) \Rightarrow a^{-1}H = b^{-1}H \Rightarrow (a^{-1})^{-1}b^{-1} \in H$
 $\Rightarrow Ha = Hb$ //

örtenliği gösterelim:

$\forall a \in L$ için $\psi(x) = aH$ o.s. $\exists x \in L$ varsa $Ha^{-1} \in R$ dir.

$\Rightarrow \psi(Ha^{-1}) = (a^{-1})^{-1}H = aH$ olur. 1:1 ve örten olduğundan;

$\phi(R) = \phi(L)$ dir. //

Her sağ denklik bağıntısı, hem de sol denklik bağıntısına göre H 'in elemanları birbirine denktir.

$h, k \in H$ ve $H < G$ olduğundan $h^{-1}k, hk^{-1} \in H$

$\Rightarrow h \equiv_{L,R} k(H)$ dir.

H 'daki elemanların denklik sınıfı, H 'in kendisidir.

iv- $\forall h \in H$ için $hH = H = Hh$ olur. //

$\left\{ \begin{array}{l} 3\mathbb{Z} \neq \mathbb{Z} \text{ çünkü } (\mathbb{Z}, \cdot) \text{ grup değildir.} \\ 3 + \mathbb{Z} = \mathbb{Z} \text{ dir. } (\mathbb{Z}, +) \text{ grup olduğundan.} \end{array} \right\}$

Soru // G değişmeli ise sağ denklik bağıntısı ile sol denklik bağıntısı birbirinin aynıdır.

$a \equiv_L b(H) \Leftrightarrow a \equiv_R b(H)$ dir. (G değişmeli ise)

Çözüm: $a \equiv_L b(H) \Leftrightarrow a^{-1}b \in H$ G değişmeli olduğundan $\Leftrightarrow$

$a^{-1}b = ba^{-1} \Rightarrow ba^{-1} \in H \Leftrightarrow (ba^{-1})^{-1} = ab^{-1} \in H \Leftrightarrow a \equiv_R b(H)$ //

Soru // $A = \{12, -6, 9\} \subset (\mathbb{Z}, +)$, $\langle A \rangle \stackrel{?}{=} \langle 3 \rangle$

$\langle A \rangle = \{12k + (-6)l + 9m \mid k, l, m \in \mathbb{Z}\} = \langle d \rangle$ olsun.

$3 = (12, 6, 9) \Rightarrow 3 = 12x + 6y + 9z$ o.s. $\exists x, y, z \in \mathbb{Z}$ vardır.

$\Rightarrow 3 \in \langle d \rangle \Rightarrow \langle 3 \rangle \subset \langle d \rangle$

Tersine, $d \in \langle A \rangle \Rightarrow d = 12k + 6l + 9m$ o.s. $\exists k, l, m \in \mathbb{Z}$.

$3 \mid d \Rightarrow d = 3t$ o.s. $\exists t \in \mathbb{Z}$.

$\Rightarrow d \in \langle 3 \rangle \Rightarrow \langle d \rangle \subset \langle 3 \rangle$

O halde $\langle d \rangle = \langle A \rangle = \langle 3 \rangle$ olur. //

Tanım: $[G:H] := o(R) = o(L)$

G bir grup, $H < G$ olsun. H 'a göre sağ veya sol (denklik sınıfı) kosetleri sayısına, H alt grubunun G içindeki indeksi denir ve $[G:H]$ ile gösterilir.

Örnek // $\langle 3 \rangle < \mathbb{Z}$ ise $[\mathbb{Z} : \langle 3 \rangle] = ?$ (3'ün ürettiği grubun indeksi)

$\left\{ \begin{array}{l} H \text{ 'a göre olan sağ veya sol kosetlerin sayısını bulmalıyız.} \\ aH = bH \Leftrightarrow a^{-1}b \in H \quad \forall h \in H; hH = Hh = H \\ Ha = Hb \Leftrightarrow ab^{-1} \in H \quad eH = He = H \end{array} \right\}$

Çözüm // $\forall m \in \mathbb{Z}, m = 3q + r \quad 0 \leq r < 3 \quad \text{o.s. } \exists q, r \in \mathbb{Z}.$

$$(-r) + m = m - r = 3q \in \langle 3 \rangle \Rightarrow m \equiv_L r (\langle 3 \rangle)$$

$$\Rightarrow m + \langle 3 \rangle = r + \langle 3 \rangle \quad \{r = \bar{0}, \bar{1}, \bar{2} \text{ olabilir}\}$$

$$\underset{1=}{0 + \langle 3 \rangle}, \quad \underset{2=}{1 + \langle 3 \rangle}, \quad \underset{3=}{2 + \langle 3 \rangle} \quad (3 \text{ tane dir.})$$

$$0 \leq r_1 \neq r_2 < 3 \text{ olsa } r_1 - r_2 < 3 \text{ olur.}$$

Yani 3'ün katı olamaz. $r_1 - r_2 < |3|$ olur.

$$r_1 - r_2 = 3k \quad \text{o.s. } k \in \mathbb{Z} \text{ yoktur. } r_1 - r_2 \notin \langle 3 \rangle.$$

$$0 \text{ halde } r_1 \neq r_2 (\langle 3 \rangle) \Rightarrow [\mathbb{Z} : \langle 3 \rangle] = 3 \text{ olur. //}$$

Genelleştirirsek; $[\mathbb{Z} : \langle n \rangle] = n$ dir.

Soru // $G = \langle a \rangle$ sonsuz devirli grup, $H = \langle a^r \rangle < G$, $[G:H] = ?$

Yukarıdaki soruda $\mathbb{Z}$ sonsuz devirli grup idi.

$$0 \text{ halde } [G:H] = r \text{ olur. //}$$

Soru // $[Q : \mathbb{Z}] = ?$

Teorem: $K < H < G \Rightarrow [G:K] = [G:H][H:K]$ dir.

İspat // $G = \bigcup_{i \in I} Ha_i$, $a_i \in G$ ($Ha_i = Ha_j \Leftrightarrow i = j$)

(Denklik sınıflarının ikiser ikiser arakesitleri boştur ve birleşimleri G dir.)

$$H = \bigcup_{j \in J} Kb_j, \quad b_j \in H \quad (Kb_r = Kb_s \Leftrightarrow r = s)$$

$$[G:H] = o(I) \quad \text{ve} \quad [H:K] = o(J) \text{ olsun.}$$

$$\Rightarrow G = \bigcup_{i \in I} \left(\bigcup_{j \in J} K b_j \right) a_i = \bigcup_{(i,j) \in I \times J} K b_j a_i$$

$$[G:K] \leq o(I \times J) = o(I) \cdot o(J)$$

$\forall (i,j)$ için eşitliği göstermeliyiz.

$$K b_j a_i = K b_r a_t \Rightarrow b_j a_i = k b_r a_t \text{ o.ş. } \exists k \in K.$$

$$\Rightarrow a_i = b_j^{-1} k b_r a_t \text{ dir.}$$

$$b_j^{-1}, k, b_r \in H.$$

$$H a_i = H (b_j^{-1} k b_r) a_t = H a_t \Rightarrow i = t$$

$$\Rightarrow b_j a_i = k b_r a_t \Rightarrow b_j = k b_r \Rightarrow j = r$$

$$\left\{ \begin{array}{l} k_1 b_j a_i \in K b_j a_i = K b_r a_t \\ k_1 b_j a_i = k_2 b_r a_t \text{ o.ş. } k_2 \in K. \\ b_j a_i = k^{-1} k_2 b_r a_t = k b_r a_t \end{array} \right\}$$

$$\text{O halde } [G:K] = o(I \times J) = o(I) \cdot o(J) \text{ dir.}$$

$$\text{yani, } [G:K] = [G:H][H:K] \text{ olur. //}$$

1. Sonuç : (Lagrange) :

Sonlu bir grubun her alt grubunun mertebesi grubun mertebesini böler. Yani $|o(H)| \mid o(G)$ dir.)

$$H < G \Rightarrow o(G) = [G:H] o(H) \text{ olur. } (o(G) < \infty \text{ ise})$$

İspat // Teorende $K = \{e\} < H < G$ alırsak,

$$[G:K] = o(G) \text{ ve } [H:K] = o(H) \text{ olur. Buradan,}$$

$$[G:K] = o(G) = [G:H] o(H) \text{ olur. //}$$

$\left\{ \begin{array}{l} 4 \text{ elemanlı grubun, alt grubunun 3 elemanı olamaz. Fakat 2 elemanı} \\ \text{olabilir de, olmayabilir de.} \end{array} \right.$

$$\left\{ \begin{array}{l} o(\mathbb{Z}_2 \times \mathbb{Z}_2) = 4 \quad 3 \text{ elemanlı alt grubu yoktur.} \end{array} \right.$$

2. Sonuç : $o(G) = n \Rightarrow \forall a \in G$ için $a^n = e$ dir.

İspat // $\langle a \rangle < G \Rightarrow o(a) := o(\langle a \rangle) \mid n$

$$o(a) := m \text{ dersen } n = mt \text{ o.ş. } \exists t \in \mathbb{Z}.$$

$$e = a^m \Rightarrow e^t = a^{mt} = e = a^n \quad // \quad (o(a) | o(G) = n \text{ dir.})$$

Örnek // $o(\mathbb{Z}_m^*) = \varphi(m)$ (Euler)

$$(a, m) = 1 \Rightarrow \bar{a} \in \mathbb{Z}_m^* \quad \bar{a}^{\varphi(m)} = \bar{1} \quad (a^{\varphi(m)} \equiv 1 (m))$$

3. Sonuç: $o(G) = p$, p asal $\Rightarrow G$ devirli'dir.

$$e \neq a \in G \quad \langle a \rangle < G, \quad o(\langle a \rangle) \nmid p \Rightarrow o(\langle a \rangle) = p \\ \Rightarrow G = \langle a \rangle \quad (\text{yani, mertebesi asal olan grup devirli'dir.})$$

Örnek // 13 elementli bir grup devirli'dir. // $o(a) = 13$ devirli'dir.

Teorem: $N < G$ olsun. Aşağıdaki ifadeler denktir;

i- $\forall a \in G$ ve $\forall n \in N$ için, $ana^{-1} \in N$.

ii- $\forall a \in G$ için, $aNa^{-1} \subset N$

iii- $\forall a \in G$ için, $aNa^{-1} = N$

iv- $\forall a \in G$ için, $aN = Na$ dir.

Tanım: Yukarıdaki koşullardan birini sağlayan G 'nin bir N alt grubuna, normal alt grup denir ve $N \triangleleft G$ ile gösterilir.

ii $\rightarrow$ iii: Hipotezden, $a^{-1} \in G$ için,

$$a^{-1}N(a^{-1})^{-1} \subset N \Rightarrow a^{-1}Na \subset N \Rightarrow a(a^{-1}Na)a^{-1} \subset aNa^{-1} \\ \Rightarrow N \subset aNa^{-1} //$$

iii $\rightarrow$ iv: $aNa^{-1} = N$ olsun.

$$\Rightarrow (aNa^{-1})a = Na \Rightarrow aN = Na \text{ olur.} //$$

$N \triangleleft G$ olsun.

$G/N = \{aN | a \in G\}$ grup olduğunu göstermeye çalışalım.

$$aN \odot bN := (ab)N$$

$$\odot: G/N \times G/N \longrightarrow G/N \quad \text{işlemi tanımlansın.} \\ (aN, bN) \longrightarrow (ab)N$$

Kapalılık vardır.

$$aa_1^{-1} \in N \Leftrightarrow aN = a_1N \quad \text{ve} \quad bb^{-1} \in N \Leftrightarrow bN = b_1N$$

$(ab)N = (a_1b_1)N$ ise iyi tanımlı olur. Bunun için,

$(ab)(a_1b_1)^{-1} \in N$? bakalım.

$$aa_1^{-1} \in N \Leftrightarrow aN = a_1N$$

$$n = bb_1^{-1} \in N \Leftrightarrow bN = b_1N$$

$$\underline{abb_1^{-1}a_1^{-1}} = an a_1^{-1} \in N$$

{ 0 halde G/N bir
işlerdir.
↑

$\Rightarrow$ i. den dolayı iv olur. $(ab)N = (a_1b_1)N$ dir. //

Tanım : G/N , $\odot$ işlemine göre bir gruptur. Bu gruba, G 'nin N 'ye göre bölüm grubu denir.

(Denklik sınıflarından olan kümeyi grup yapmak için, yukarıdaki teoreni yazıldı.) //

(Grup < Normal < Değişmeli < Devirli)

$$N \trianglelefteq G \text{ olsun. } (aN)(bN) := (ab)N$$

$G/N = \{aN \mid a \in G\} \Rightarrow (G/N, \cdot)$ bir gruptur. Gösterelim.

i - $\forall aN, bN, cN \in G/N$ için,

$$\begin{aligned} aN(bNcN) &= aN((bc)N) = a(bc)N = (ab)cN = (ab)NcN \\ &= (aNbN)cN \quad (\text{birleşme}) \end{aligned}$$

ii - $eN = N \quad \forall aN \in G/N$ için

$$\left. \begin{aligned} aNeN &= aeN = aN \\ eNaN &= eaN = aN \end{aligned} \right\} \text{ (birim elemanı)}$$

$$\left. \begin{aligned} \text{iii - } aNa^{-1}N &= eN = N \\ a^{-1}NaN &= eN = N \end{aligned} \right\} \Rightarrow (aN)^{-1} = a^{-1}N \in G/N \quad (\text{ters elemanı})$$

Soru // G değişmeli ise G/N de değişmelidir. Yani; $ab = ba$ ise
 $aNbN = (ab)N = (ba)N = bNaN$ dir. //

G/N ile G karşılaştırılmaz. G/N kümelerin kümesidir.

Mertebesi G den küçüktür. G/N ile G farklı şeylerdir. //

normal < değişmeli
örnek,, $(\mathbb{Z}, +) \triangleleft (\mathbb{Q}, +)$ dir. $\mathbb{Q}/\mathbb{Z} = ?$

$$\left\{ (\mathbb{Q}, +) \text{ değişmelidir. } \frac{a}{b} + \mathbb{Z} = \mathbb{Z} + \frac{a}{b} \right\}$$

çözüm,, $(r, s) = 1$ olmak üzere $\forall \frac{r}{s} \in \mathbb{Q}$ ve $\forall x \in \mathbb{Z}$ için $+$ işlenine göre

$\mathbb{Q}$ bir grup olduğundan $-\frac{r}{s}, \frac{r}{s}$ elemanının toplamsal tersidir.

Buna göre, $\frac{r}{s} + x + (-\frac{r}{s}) \in \mathbb{Z}$ olmalıdır. Değişmeli olduğundan,

$\frac{r}{s} + (-\frac{r}{s}) + x = x$ olur. Zaten $x \in \mathbb{Z}$ idi. Öyleyse $(\mathbb{Z}, +)$ normal

alt grup olma özelliklerinden birincisini sağlar.

Şimdi $\mathbb{Q}/\mathbb{Z}$ nin elemanlarını bulalım.

$\forall x \in \mathbb{Q}$ için $x = [x] + \{x\}$ $0 \leq x < 1$ şeklinde tam kısmı ve kesirsel kısmının toplamı olarak yazılabilir.

$x - \{x\} = [x] \in \mathbb{Z}$ dir. O halde $x \equiv \{x\} \pmod{\mathbb{Z}}$ dir. Demek ki,

$\bar{x} = \{x\} \Rightarrow \bar{x} = x + \mathbb{Z}$ ve $\{\bar{x}\} = \{x\} + \mathbb{Z}$ dir.

Şimdi farklı elemanların farklı kosetlerinin olduğunu gösterelim.

$r_1 \neq r_2$ olmak üzere $r_1, r_2 \in \mathbb{Q}$ alalım.

$$0 \leq r_1, r_2 < 1 \Rightarrow |r_1 - r_2| \notin \mathbb{Z}$$

$$\Rightarrow r_1 + \mathbb{Z} \neq r_2 + \mathbb{Z}$$

$$0 \leq r_1 < 1 \text{ ve } 0 \leq r_2 < 1 \text{ ise } -1 < -r_2 \leq 0$$

$$0 - 1 < r_1 - r_2 < 1 + 0 \Rightarrow -1 < r_1 - r_2 < 1 \Rightarrow |r_1 - r_2| < 1$$

Her sayının mutlak değeri pozitif olduğundan $0 < |r_1 - r_2| < 1$ dir.

Öyleyse $|r_1 - r_2| \notin \mathbb{Z}$ dir. Demek ki $\forall x \in \mathbb{Q}$ nun denklik sınıfı

0 ile 1 arasında bir rasyonel sayı ile ifade edilebilmektedir, bu ise ;

$$\mathbb{Q}/\mathbb{Z} = \{ r + \mathbb{Z} \mid 0 \leq r < 1, r \in \mathbb{Q} \} \text{ sonsuz gruptur. (sonsuz elemanlı)}$$

O halde sonsuz bir grubun elemanlarının mertebesi sonludur. Bunun için ;

$\forall x \in \mathbb{Q}$ alalım. $t, s \in \mathbb{Z}$ olmak üzere $x = \frac{t}{s}$ yazılabilir.

x in denklik sınıfı $x + \mathbb{Z}$ dir. $s \in \mathbb{Z}$ nin denklik sınıfı $s + \mathbb{Z}$ dir.

$$(x + \mathbb{Z}) \odot (s + \mathbb{Z}) = xs + \mathbb{Z} \text{ olur. } x = \frac{t}{s} \Rightarrow t = sx$$

$$= t + \mathbb{Z} \text{ olur.}$$

($a \in G$ için $\bar{a} = aH$ idi. $a \in G$ değilse, $a \in H$ alırsak $\bar{a} = aH = a$ idi.)

$t \in \mathbb{Z}$ olduğundan $t + \mathbb{Z} = \mathbb{Z}$ olur.

$o(x + \mathbb{Z}) \mid s \Rightarrow o(x + \mathbb{Z})$ sonludur. //

Sınav sorusu)

Örnek //

$G = \langle a \rangle$ sonsuz devirli grup, $H = \langle a^r \rangle$ $r \in \mathbb{N}$ ise

$[G:H] = r$ olduğunu gösterin.

Gözüm //

$\forall x \in G$ için $x = a^m$ olacak şekilde $\exists m \in \mathbb{Z}$.

$m = qr + s$, $0 \leq s < r$ o.p. $\exists q, r \in \mathbb{Z}$.

$$a^m = a^{qr} a^s \Rightarrow a^m (a^s)^{-1} = (a^r)^q \in \langle a^r \rangle = H$$

$$a^m \equiv_R a^s (H)$$

$\Rightarrow H a^m = H a^s$ G nin her elemanını a^s ile temsil ediyoruz.

$$\{He = H, Ha, Ha^2, \dots, Ha^{(r-1)}\} \Rightarrow [G:H] \leq r \text{ olur.}$$

$$0 \leq s_1 \neq s_2 < r \Rightarrow -r < s_1 - s_2 < r$$

$\Rightarrow s_1 - s_2 = rt$ o.p. $\exists t \in \mathbb{Z}$ bulunamaz.

$$\Rightarrow a^{s_1} (a^{s_2})^{-1} \notin \langle a^r \rangle \Rightarrow a^{s_1} \notin a^{s_2} \langle a^r \rangle \Rightarrow H a^{s_1} \neq H a^{s_2}$$

O halde $[G:H] = r$ dir. //

TANIM: $\forall a, b \in G$, $ab = ? ba \Rightarrow ?$ 'a a ve b nin komütatörü

(değişme ölçüsü) denir. $ab = (aba^{-1}b^{-1})ba$ dir.

$$[a, b] = aba^{-1}b^{-1} \text{ ile gösterilir. } ab = [a, b]ba \text{ dir. //$$

Tüm komütatörlerle üretilen alt gruba komütatör grup denir. Ve

$[G, G] < G$ ile gösterilir.

$$[G, G] = \{c_1 c_2 \dots c_m\}$$

$$[a, b]^{-1} = bab^{-1}a^{-1} \text{ dir.}$$

$$[e, a] = eae^{-1}a^{-1}$$

$$= eaa^{-1} = e = [a, e] //$$

Önerme: G abelyen $\Leftrightarrow [G, G] = \{e\}$

(değişmeli)

($\forall a, b \in G$ için $[a, b] = e$ dir.)

$$\left\{ \begin{array}{l} (ab)^{-1} = (b^{-1}a^{-1}) \text{ dir.} \\ (ab)(b^{-1}a^{-1}) = e \text{ ve} \\ (b^{-1}a^{-1})(ab) = e \text{ 'den dolayı} \end{array} \right.$$

İspat, $\Rightarrow$: G değişmeli ise $\forall a, b \in G$,

$$ab = ba \text{ ve } [a, b] = aba^{-1}b^{-1} = ba a^{-1}b^{-1} = beb^{-1} = e //$$

$\Leftarrow$: $\forall a, b \in G$ için $[a, b] = aba^{-1}b^{-1} = e$ ise $ab = ba$ olur. //

Önerme : $[G, G]$, G nin normal alt grubudur. ($[G, G] \triangleleft G$)

İspat, $\forall x = [a_1, b_1][a_2, b_2], \dots, [a_k, b_k] \in [G, G]$ ve $\forall g \in G$ için,
 $gxg^{-1} \in [G, G]$ dir.

$$\begin{aligned} gxg^{-1} &= g[a_1, b_1][a_2, b_2] \dots [a_k, b_k]g^{-1} \\ &= (g[a_1, b_1]g^{-1})(g[a_2, b_2]g^{-1}) \dots (g[a_k, b_k]g^{-1}) \end{aligned}$$

$$\begin{aligned} \Rightarrow g \underbrace{[a_i, b_i]}_{c_i} g^{-1} &= g c_i g^{-1} = g c_i g^{-1} c_i^{-1} c_i = [g, c_i] c_i \in [G, G] \\ &= g[a_i, b_i]g^{-1}[a_i, b_i]^{-1}[a_i, b_i] \\ &= [g, [a_i, b_i]][a_i, b_i] \end{aligned}$$

O halde $[G, G] \triangleleft G$ dir. //

13.12.1995

Çarşamba

Teorem : G bir grup ve $N \triangleleft G$ olsun.

$$G/N \text{ abelyen} \Leftrightarrow [G, G] \subset N$$

İspat, $\forall aN, bN \in G/N$ değişmeli ise ;

$$aNbN = bNaN \Leftrightarrow (ab)N = (ba)N$$

$$\Leftrightarrow (ab)(ba)^{-1} \in N$$

$$\Leftrightarrow aba^{-1}b^{-1} = [a, b] \in N \quad \forall a, b \in G,$$

$$\Leftrightarrow [G, G] \subset N //$$

Veya $\Rightarrow$: G/N değişmeli $\Rightarrow [G/N, G/N] = N \quad \forall a, b \in G$ için,

$$[aN, bN] = N \Rightarrow aNbN(aN)^{-1}(bN)^{-1} = N$$

$$\Rightarrow (aba^{-1}b^{-1})N = N$$

$$\Rightarrow [a, b] = aba^{-1}b^{-1} \in N$$

Sonuç : $G/[G, G]$ değişmelidir.

Bölüm grubunu değişmeli yapan en küçük normal alt grup, komütatör alt grubudur.

Teorem: $N \triangleleft G$ olsun.

i- $N < K < G \Rightarrow K/N < G/N$ dir. Ayrıca,

$K \triangleleft G \Rightarrow K/N \triangleleft G/N$ dir.

ii- Tersine G/N nin her alt grubu $N < A < G$ olmak üzere A/N şeklindedir. (G/N nin her H alt grubu için $N < A$ ve $H = A/N$ olacak şekilde $\exists A < G$ vardır.)

İspat, i- $N \triangleleft G \Rightarrow N \triangleleft K, K/N \subset G/N$

$\forall k_1 N, k_2 N \in K/N$ alalım. $k_1, k_2 \in K, K < G$ olduğundan $k_1 k_2^{-1} \in K$ dir.

$$(k_1 N)(k_2 N)^{-1} = (k_1 N)(k_2^{-1} N) = \underbrace{(k_1 k_2^{-1})}_\in K N \in K/N \therefore K/N < G/N.$$

Ayrıca, $K \triangleleft G \Rightarrow \forall g \in G$ ve $\forall k \in K$ için $gk g^{-1} \in K$ dir.

$\forall k N \in K/N$ ve $\forall g N \in G/N$ için,

$$(g N)(k N)(g N)^{-1} = (g N)(k N)(g^{-1} N) = \underbrace{(g k g^{-1})}_\in K N \in K/N$$

$$\Rightarrow K/N \triangleleft G/N //$$

İspat, ii- $H < G/N$ nin herhangi bir alt grubu olsun.

$$A := \{g \in G \mid gN \in H\} \quad N \overset{?}{\subset} A$$

$$\forall x \in N, xN = N \in H \Rightarrow x \in A \text{ olur.}$$

$\left. \begin{array}{l} G/N \text{ nin birimi, } N \text{ dir.} \end{array} \right\}$

$H < G/N$ olduğundan $N \in H$.

O halde $N < A$ dir. $A < G$ olduğunu gösterebiliriz;

$\forall a, b \in A$ olsun. $\Rightarrow aN, bN \in H$. $H < G/N$ olduğundan

$$(aN)(bN)^{-1} = (ab^{-1})N \in H \Rightarrow ab^{-1} \in A \therefore A < G$$

$$N \subset A \Rightarrow N < A \text{ oldu. } A/N = H.$$

Herhangi bir alt grup için $H = A/N$ olduğundan bunu her alt grup için yapabiliriz. //

$\left\{ \begin{array}{l} G/N = \{ N, \underbrace{\{ \dots \}}_{\text{denklik sınıfı}}, \dots \} \text{ bu kümeleri açarsak } G \text{ 'yi verir.} \\ H = \{ N, \{ \dots \}, \{ \dots \}, \dots \} \subset G/N \text{ } G/N \text{ de bazı kümeler.} \\ A := \{ \text{H'daki kümelerin, ağırlımı} \} \subset G \end{array} \right.$

Örnek // $N < G$ ve $[G:N] = 2$ (2 sağ ve 2 sol koset) olsun.

$eN = N$, $aN \Rightarrow$ sol kosetler

$Ne = N$, $Na \Rightarrow$ sağ kosetler.

$$N \cap aN = \emptyset \text{ ve } N \cup aN = G \Rightarrow G - N = aN$$

$$N \cap Na = \emptyset \text{ ve } N \cup Na = G \Rightarrow G - N = Na$$

$\left. \begin{array}{l} \text{Normal alt grup} \\ aN = Na \\ 4. \text{ özellik} \end{array} \right\}$

O halde $G - N = aN = Na$; yani indeksi 2 olan grubun, alt grubu normaldir. $N \triangleleft G$ dir. //

HOMOMORFİZMA

Tanım: G ve H herhangi iki grup olsun. Eğer bir $f: G \rightarrow H$ fonksiyonu; $\forall x, y \in G$ için;

$$\begin{array}{ccc} f(xy) = f(x) \cdot f(y) \\ \downarrow \qquad \qquad \downarrow \\ \{G \text{ nin işlemi} \} \quad \{H \text{ nin işlemi} \} \end{array}$$

şartını sağlıyorsa, f 'ye G grubundan H grubuna homomorfizma denir.

Bu şartların yanında:

1° f , 1:1 ise monomorfizma

2° f örten ise epimorfizma

3° f , 1:1 ve örten ise izomorfizma denir. $G \cong H$ ile gösterilir.

($\cong \rightarrow$ tilda)

Örnek // $I: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ $I =$ özdeşlik (birim) fonksiyon.

Örnek // $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \cdot)$
 $x \mapsto 2^x$

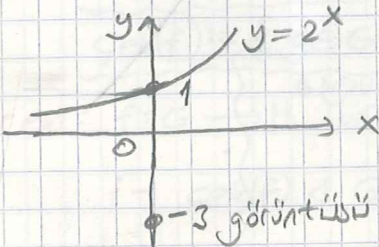
$$f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$$

$$f(x) = f(y) \Rightarrow x = y ? \text{ bakalım.}$$

$$2^x = 2^y \Rightarrow \log_2 2^x = \log_2 2^y \Rightarrow x = y \quad \therefore f \text{ 1:1 dir.}$$

$\forall 2^x \in (\mathbb{R}^*, \cdot)$ için $f(x) = 2^x$ o.s. $x \in (\mathbb{R}, +)$ var mıdır? bakalım

$$f(x) = -3 \Rightarrow 2^x = -3 \text{ o.s. } x \in (\mathbb{R}, +) \text{ yoktur.}$$



$\therefore$ O halde f örten değildir.

f monomorfizmadır. //

$\phi - 3$ görüntüsü yoktur.

Örnek // $3\mathbb{Z} \cong \mathbb{Z} ? \quad (\mathbb{Z}, +)$

$$f: 3\mathbb{Z} \rightarrow \mathbb{Z} \quad x \mapsto x/3 \quad f(x+y) = \frac{x+y}{3} = \frac{x}{3} + \frac{y}{3} = f(x) + f(y)$$

$$f(x_1) = f(x_2) \Rightarrow \frac{x_1}{3} = \frac{x_2}{3} \Rightarrow x_1 = x_2 \quad f, \text{ 1:1 dir. } \therefore$$

$\forall y \in \mathbb{Z}$ için $f(x) = y$ o.s. $\exists x = 3y \in 3\mathbb{Z}$ vardır. $f(3y) = y$ f örtendir.

$3\mathbb{Z} \cong \mathbb{Z}$ dir. //

Örnek // $\mathbb{Z} \cong 3\mathbb{Z}$? $(\mathbb{Z}, +)$

$$f: \mathbb{Z} \longrightarrow 3\mathbb{Z}$$
$$x \longmapsto 3x$$

$$f(x+y) = 3(x+y) = 3x + 3y = f(x) + f(y)$$

$$f(x_1) = f(x_2) \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2 \quad f, 1:1 \text{ dir. } \therefore$$

$$\forall y \in 3\mathbb{Z} \text{ için } f(x) = y \text{ o.s. } \exists x = \frac{y}{3} \in \mathbb{Z} \text{ vardır.}$$

$$f\left(\frac{y}{3}\right) = y \text{ dir. O halde } f \text{ örterdir. } \therefore \mathbb{Z} \cong 3\mathbb{Z} \text{ dir. //}$$

Teorem: $f: G \longrightarrow H$ homomorfizma olsun.

i - $f(e_G) = e_H$

ii - $\forall a \in G$ için, $f(a^{-1}) = f(a)^{-1}$

iii - $\forall N < G$ için, $f(N) < H$

iv - $\forall K < H$ için, $f^{-1}(K) < G$

v - $\forall K \triangleleft H$ için, $f^{-1}(K) \triangleleft G$

vi - f örter ise $\forall N \triangleleft G$ için $f(N) \triangleleft H$ dir.

İspat // i - $e_G \cdot e_G = e_G \Rightarrow f(e_G \cdot e_G) = f(e_G)$

$$\Rightarrow f(e_G) \cdot f(e_G) = f(e_G) \quad (\text{homom. old.})$$

$$\Rightarrow f(e_G) = e_H //$$

$$\begin{aligned} \text{ii - } \left. \begin{array}{l} aa^{-1} = e_G \\ a^{-1}a = e_G \end{array} \right\} \Rightarrow \left. \begin{array}{l} f(aa^{-1}) = f(e_G) = e_H \\ f(a^{-1}a) = f(e_G) = e_H \end{array} \right\} \Rightarrow \left. \begin{array}{l} f(a)f(a^{-1}) = e_H \\ f(a^{-1})f(a) = e_H \end{array} \right\} \end{aligned}$$

$$\Rightarrow f(a)^{-1} = f(a^{-1}) \text{ dir. //}$$

$$\text{iii - } \left\{ \begin{array}{l} f(N) = \{h \in H \mid f(x) = h \text{ o.s. } \exists x \in N\} \text{ veya} \\ f(N) = \{f(x) \in H \mid x \in N\} \\ f^{-1}(K) = \{x \in G \mid f(x) \in K\} \end{array} \right\}$$

$$f(N) \neq \emptyset ? \text{ bakalım.}$$

$$N < G \Rightarrow e_G \in N \Rightarrow f(e_G) = e_H \Rightarrow e_H \in f(N) \Rightarrow f(N) \neq \emptyset$$

$$\forall a, b \in f(N) \text{ için } a = f(n_1), b = f(n_2) \text{ o.s. } n_1, n_2 \in N.$$

$$ab^{-1} = f(n_1)f(n_2)^{-1} = f(n_1)f(n_2^{-1}) = f(\underbrace{n_1n_2^{-1}}_{\in N})$$

$$\Rightarrow ab^{-1} \in f(N) \text{ dir. } \Rightarrow f(N) < H //$$

$$iv - f^{-1}(K) = \{x \in G \mid f(x) \in K\}$$

$f^{-1}(K) \neq \emptyset$? bakalım.

$$f(e_G) = e_H \text{ ve } K \triangleleft H \text{ olduğundan } f(e_G) = e_H \in K \Rightarrow e_G \in f^{-1}(K)$$

$$\forall g_1, g_2 \in f^{-1}(K) \Rightarrow f(g_1), f(g_2) \in K, K \triangleleft H \text{ olduğundan}$$

$$f(g_1 g_2^{-1}) = f(g_1) f(g_2)^{-1} \in K \Rightarrow g_1 g_2^{-1} \in f^{-1}(K)$$

O halde $f^{-1}(K) \triangleleft G$ dir. //

$$v - \forall a \in f^{-1}(K) \text{ ve } \forall g \in G \text{ için, } gag^{-1} \in f^{-1}(K) ?$$

$$f(a) \in K, f(g) \in H \text{ dir. } K \triangleleft H \text{ olduğundan}$$

$$f(gag^{-1}) = f(g) f(a) f(g)^{-1} \in K \Rightarrow gag^{-1} \in f^{-1}(K) \text{ olur.}$$

$\Rightarrow f^{-1}(K) \triangleleft G$ dir. //

$$vi - f(N) = \{f(x) \in H \mid x \in N\} \quad N \triangleleft G \text{ için } f(N) \triangleleft H ?$$

$$\forall f(a) \in f(N) \quad (a \in N).$$

$$\forall h \in H \text{ alalım. } f \text{ örten olduğundan } f(x) = h \text{ o.s. } \exists x \in G \text{ vardır.}$$

$$hf(a)h^{-1} \in f(N) ?$$

$$hf(a)h^{-1} = f(x) f(a) f(x)^{-1} = f(x) f(a) f(x^{-1})$$

$$= f(\underbrace{xax^{-1}}_{\in N}) \in f(N) \quad (N \triangleleft G \text{ old.})$$

$\Rightarrow f(N) \triangleleft H$ dir. //

Tanım: $f: G \rightarrow H$ bir homomorfizma olsun.

$$\ker(f) := \{g \in G \mid f(g) = e_H\} = f^{-1}(e_H)$$

Teorem: $f: G \rightarrow H$ bir homomorfizma olsun.

$$i - \ker(f) \triangleleft G \text{ dir.}$$

$$ii - h \in H \text{ ve } g \in G \text{ için } f(g) = h \text{ ise } f^{-1}(h) = g\ker(f) \text{ dir.}$$

$$iii - G/\ker(f) \cong f(G) \quad (f \text{ örten ise } G/\ker(f) \cong f(G) \cong H \text{ dir.})$$

İspat: $i - f(e_G) = e_H$ olduğundan, $e_G \in \ker(f) \Rightarrow \ker(f) \neq \emptyset$ olur.

$$\forall x, y \in \ker(f) \text{ alalım } \Rightarrow f(x) = e_H = f(y) \text{ olur.}$$

$$f(xy^{-1}) = f(x) f(y)^{-1} = f(x) f(y)^{-1} = e_H e_H^{-1} = e_H$$

$$\Rightarrow xy^{-1} \in \ker(f) \Rightarrow \ker(f) \trianglelefteq G \text{ dir.}$$

$$\forall x \in \ker(f), \forall g \in G \text{ için,}$$

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)e_H f(g)^{-1} = f(g)f(g)^{-1} = e_H$$

$$\Rightarrow gxg^{-1} \in \ker(f) \Rightarrow \ker(f) \trianglelefteq G \text{ dir. //$$

$$\text{ii - } x \in f^{-1}(h) \Leftrightarrow f(x) = h \text{ dir. Aynı zamanda } f(g) = h \text{ dir.}$$

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

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

$$\Leftrightarrow g^{-1}x \in (\ker(f))$$

$$\Leftrightarrow x \in g(\ker(f))$$

$$\Leftrightarrow x \in g \ker(f)$$

$$\Leftrightarrow f^{-1}(h) = g \ker(f) \text{ dir. //$$

$$\text{iii - } \psi : G/\ker(f) \longrightarrow H$$

$$g \ker(f) \longrightarrow \psi(g \ker(f)) = f(g) \text{ ile tanımlanıyor.}$$

$$g_1 \ker(f) = g_2 \ker(f) \Rightarrow g_1 g_2^{-1} \in \ker(f)$$

$$\Rightarrow f(g_1 g_2^{-1}) = e_H$$

$$\Rightarrow f(g_1) f(g_2)^{-1} = e_H$$

$$\Rightarrow f(g_1) = f(g_2)$$

$$\Rightarrow \psi(g_1 \ker(f)) = \psi(g_2 \ker(f))$$

$$\therefore \psi \text{ iyi tanımlıdır. //$$

$$\psi(g_1 \ker(f) \cdot g_2 \ker(f)) = \psi((g_1 g_2) \ker(f))$$

$$= f(g_1 g_2)$$

$$= f(g_1) f(g_2) \quad (f \text{ hom. old.})$$

$$= \psi(g_1 \ker(f)) \psi(g_2 \ker(f))$$

$$\therefore \psi \text{ homomorfizma olur. //$$

$$\psi(g_1 \ker(f)) = \psi(g_2 \ker(f)) \Rightarrow f(g_1) = f(g_2)$$

$$\Rightarrow f(g_1) f(g_2)^{-1} = e_H$$

$$\Rightarrow f(g_1 g_2^{-1}) = e_H$$

$$\Rightarrow g_1 g_2^{-1} \in \ker(f)$$

$$\Rightarrow g_1 = g_2 (\ker(f))$$

$$\Rightarrow g_1 \ker(f) = g_2 \ker(f)$$

$\therefore \psi$ 1:1 dir. //

ψ nin tanımından $\psi: G/\ker(f) \rightarrow f(G)$ örten olur.

$\therefore \psi$ izomorfizma olup,

$$\therefore G/\ker(f) \cong f(G) //$$

Not: Eğer $f: G \rightarrow H$ örten ise $f(G) = H$ olduğundan

$$G/\ker(f) \cong H \text{ olur.} //$$

Teorem: $f: G \rightarrow H$ örten homomorfizma ve $M \triangleleft H, N := f^{-1}(M)$ olsun.

Bu durumda, $G/N \cong H/M \cong (G/\ker f)/(N/\ker f)$ dir.

İspat // (önceki teorem v. sıktan) $N \triangleleft G$ dir.

G/N bir gruptur. Bir önceki teoremden $\ker f \triangleleft G$ dir.

$$\forall x \in \ker f \Rightarrow f(x) = e_H \in M \Rightarrow x \in f^{-1}(M) \Rightarrow \ker f \subset f^{-1}(M) =: N$$

$\ker f \triangleleft N \therefore N/\ker f$ bir gruptur.

$N \triangleleft G$ olduğundan $N/\ker f \triangleleft G/\ker f$

$$\therefore (G/\ker f)/(N/\ker f) //$$

$\psi: G \rightarrow H/M$
 $\forall a \in G, a \mapsto \psi(a) := f(a)M$ ile tanımlanıyor.

$$a_1 = a_2 \Rightarrow f(a_1) = f(a_2) \Rightarrow f(a_1)M = f(a_2)M \Rightarrow \psi(a_1) = \psi(a_2) \quad \text{kapalıdır.}$$

Ayrıca iyi tanımlı olduğundan ψ bir fonksiyon olur.

$$\psi(ab) = f(ab)M = f(a)f(b)M = (f(a)M)(f(b)M) = \psi(a)\psi(b) \quad \psi \text{ homomorfizmadır.}$$

$\forall f(a)M \in H/M$ için $\psi(a) = f(a)M$ o.s. $\exists a \in G$?

$\forall hM \in H/M$ için, $h \in H$ ve f örten olduğundan

$$f(g) = h \text{ o.s. } \exists g \in G \text{ vardır.}$$

$$hM = f(g)M = \psi(g) \quad \text{O halde } \psi \text{ örten dir.} \therefore$$

ψ nin çekirdeğini bulalım.

$$\forall x \in \ker f \Leftrightarrow \psi(x) = f(x)M = M \Leftrightarrow f(x) \in M \Leftrightarrow x \in f^{-1}(M) = N$$

$$\ker \psi = N.$$

$$G/\ker \psi \cong \psi(G) = H/M \quad (\text{önceki teoremden})$$

$$G/N \cong H/M \text{ olur.}$$

$$\begin{aligned} \psi: G/\ker f &\longrightarrow G/N \\ a\ker f &\longmapsto aN \end{aligned}$$

$$a_1 \ker f = a_2 \ker f \Rightarrow a_1 a_2^{-1} \in \ker f \Rightarrow f(a_1 a_2^{-1}) = e_H$$

$$\Rightarrow f(a_1) f(a_2)^{-1} = e_H \Rightarrow f(a_1) = f(a_2)$$

$$\Rightarrow f(a_1)M = f(a_2)M$$

$$g\ker f \in \ker \psi \Leftrightarrow \psi(g\ker f) = f(g)M = M$$

$$\Leftrightarrow f(g) \in M$$

$$\Leftrightarrow g \in f^{-1}(M) = N$$

$$\Leftrightarrow g\ker f \in N/\ker f$$

$$\therefore \ker \psi = N/\ker f //$$

$$(G/\ker f) / \ker \psi \cong \psi(G/\ker f) = H/M$$

$$\Rightarrow (G/\ker f) / (N/\ker f) \cong H/M \cong G/N //$$

SİMETRİK GRUPLAR

$A \neq \emptyset$, $S(A) := \{ f: A \xrightarrow{1:1 \text{ örten}} A \}$ $(S(A), \circ)$ gruptur.

$S(A)$ nin her alt grubuna dönüşüm grubu denir.

$$\forall f, g \in S(A), \quad fog: A \rightarrow A \\ x \rightarrow fog(x) := f(g(x)) \Rightarrow fog \in S(A)$$

$$1^{\circ} \quad \forall f, g, h \in S(A) \text{ için } fo(goh) = (fog)oh ?$$

$\forall x \in A$ için,

$$\left. \begin{aligned} [fo(goh)](x) &= f((goh)(x)) = f(g(h(x))) \\ [(fog)oh](x) &= (fog)(h(x)) = f(g(h(x))) \end{aligned} \right\} \text{(birleşme)}$$

$$2^{\circ} \quad I: A \xrightarrow{x \rightarrow x} A \text{ fonksiyonu } 1:1 \text{ ve örten olup, } I \in S(A) \text{ dir ve}$$

$I, "o"$ işleminin etkisiz (birim) elemanıdır. Gerçekten,

$foI = Iof = f$ dir. Çünkü, $\forall x \in A$ için

$$\left. \begin{aligned} (foI)(x) &= f(I(x)) = f(x) \\ (Iof)(x) &= I(f(x)) = f(x) \end{aligned} \right\} \text{ eşitlik sağlanır. (birim eleman)}$$

$$3^{\circ} \quad \forall f \in S(A), \quad f^{-1}: A \xrightarrow{x \rightarrow f^{-1}(x)} A$$

bir tek
↑

f örten olduğundan $\forall x \in A$ için $f(a) = x$ olacak şekilde $\exists! a \in A$.

f^{-1} fonksiyonu, f in, " o " işlemine göre tersidir. (ters eleman)

$fof^{-1} = f^{-1}of = I$ (?) ve f^{-1} , 1:1 ve örten ise (?) $f^{-1} \in S(A)$ dir

$\circ$ halinde $(S(A), \circ)$ işlemi bir gruptur.

Teorem : Her grup, bir dönüşüm grubuna izomorftur. (CAYLEY)

G bir grup, $a \in G$ için,

$$T_a: G \rightarrow G \\ x \rightarrow T_a(x) := ax$$

T_a , 1:1 ve örten dir. ($T_a \in S(G)$?)

$$\bullet T_a(x) = T_a(y) \Rightarrow ax = ay \Rightarrow a^{-1}ax = a^{-1}ay \Rightarrow x = y \therefore T_a, 1:1$$

$$\bullet \forall y \in G \text{ için } T_a(x) = y \text{ o.f. } \exists x \in G ?$$

$x = a^{-1}y \in G$ alırsak $T_a(x) = a(a^{-1}y) = y$ $\therefore T_a \circ T_{a^{-1}} = \text{id}$, örnektir.

• $\forall a, b \in G$ için $T_a \circ T_b = T_{ab}$?

$$\forall x \in G \text{ için } T_a \circ T_b(x) = T_a(T_b(x)) = T_a(bx) = a(bx) = (ab)x = T_{ab}(x)$$

$$\Leftrightarrow T_a \circ T_b = T_{ab} //$$

$$\psi: G \longrightarrow \psi(G) < S(G)$$

$$a \longrightarrow \psi(a) := T_a \longrightarrow (\text{elemenin görüntüsü fonksiyon oldu.})$$

$$\psi(ab) = T_{ab} = T_a \circ T_b = \psi(a) \circ \psi(b)$$

• ψ , 1:1 dir. ?

$$\psi(a) = \psi(b) \Rightarrow T_a = T_b \Rightarrow \forall x \in G, ax = bx \quad (e \in G) x = e \text{ için } a = b \text{ olur.} //$$

Buradan ψ , 1:1 olur.

$$G \cong \psi(G) < S(G) //$$

$$\left\{ \begin{array}{l} a \in G, \psi(a) \in \psi(G) \end{array} \right.$$

izomorf olduğu için işlemleri $\psi(G)$ 'de yapabiliriz

$$\star A = \{x_1, x_2, \dots, x_n\} \quad S_n := S(A)$$

n elemanlı bir kümeden kendi üzerine 1:1 ve örten, $n!$ tane eleman vardır. Yani, $|S_n| = n!$ dir.

$$f \in S_n \text{ için } \{f(x_1), f(x_2), \dots, f(x_n)\} = A$$

$i_1, i_2, \dots, i_n$ doğal sayıları $1, 2, 3, \dots, n$ sayılarının değişik bir sırada yazılışı ve $f(x_k) = x_{i_k} \quad (k=1, 2, \dots, n)$ ise

$$f := \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ f(x_1) & f(x_2) & \dots & f(x_n) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$$

$$A = \{1, 2, \dots, n\}$$

S_n grubuna permütasyon (simetrik) grubu denir.

Örnek // $A = \{1, 2, 3\}$, $S_3 = 3! = 6$

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \text{ birim fonk.} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$f_5 f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_4, \quad f_5 f_3(1) = f_5(f_3(1)) = f_5(3) = 1$$

$$f_3 f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_2, \quad f_3 f_5(1) = f_3(f_5(1)) = f_3(2) = 2$$

$f_5 f_3 \neq f_3 f_5$ O halde, permütasyon grubu değişmeli değildir. //

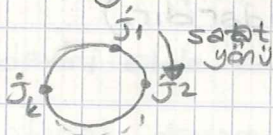
$1 \leq j_1, j_2, \dots, j_k \leq n$ farklı doğal sayılar ve $f \in S_n$ için eğer,

$f(j_1) = j_2, f(j_2) = j_3, \dots, f(j_{k-1}) = j_k, f(j_k) = j_1$ ise ve $\forall x \notin \{j_1, j_2, \dots, j_k\}$ için $f(x) = x$ ise,

f permütasyonuna k -uzunluğunda bir devir denir ve

$$f := (j_1 j_2 \dots j_k) = (j_2 j_3 \dots j_k j_1) = (j_k j_1 \dots j_{k-1}) = \dots$$

ile gösterilir.



$$f_1 = (1) = (2) = (3) = I \quad \text{1-uzunluğundaki devir. (birim dönüşüm)}$$

$$f_2 = (1 \ 2) \quad f_3 = (1 \ 3) \quad f_4 = (2 \ 3) \quad f_5 = (1 \ 2 \ 3)$$

$$f_6 = (1 \ 3 \ 2)$$

$$f_5 f_4 = (1 \ 2 \ 3)(2 \ 3) = (1 \ 2)(3) = (1 \ 2) = f_2$$

$$f_2 f_3 = (1 \ 2)(1 \ 3) = (1 \ 3 \ 2)$$

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

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

Önerme: Ayrık devirler değişmelidir.

İspat // $f = (i_1 i_2 \dots i_r)$, $g = (j_1 j_2 \dots j_s)$ ve

$$\underbrace{\{i_1, i_2, \dots, i_r\}}_A \cap \underbrace{\{j_1, j_2, \dots, j_s\}}_B = \emptyset$$

A

B

olmak üzere $fg = gf$ olduğunu göstereceğiz.

$f, g \in S_n$, $\forall 1 \leq x \leq n$ için,

i - $x \notin A$ ve $x \notin B \Rightarrow f(x) = x$ ve $g(x) = x$
 $\Rightarrow fg(x) = x \Rightarrow fg = gf$
 $gf(x) = x$

ii - $x \in A$ ve $x \notin B \Rightarrow f(x) \notin B$

$$\left. \begin{array}{l} x, f(x) \notin B \Rightarrow g(x) = x \quad gf(x) = g(f(x)) = f(x) \\ fg(x) = f(g(x)) = f(x) \end{array} \right\} \Rightarrow gf = fg //$$

iii - $x \notin A$ ve $x \in B$

Örnek // $f = (25)$ $g = (136)$

$$fg = (25)(136) = (136)(52)(4) = gf$$

Önerme // r uzunluğundaki bir devirin mertebesi r dir.

(Dairesel permütasyonun mertebesi uzunluğu kadardır.)

Yani; $f = (i_1 i_2 \dots i_r) \in S_n \Rightarrow o(f) = r$ dir.

İspat // $i_j < r$ $f(i_j) = i_{j+1}$ $f^2(i_j) = i_{j+2}$

$1 \leq k, j \leq r$ için,

$$\left. \begin{array}{l} j+k \leq r \Rightarrow f^k(i_j) = i_{j+k} \\ j+k > r \Rightarrow f^k(i_j) = i_{j+k-r} \end{array} \right\} f^r(i_j) = i_j$$

$$\left\{ \begin{array}{l} f(x) = x \text{ ise} \\ f^2(x) = f(f(x)) = f(x) = x \end{array} \right.$$

$\forall 1 \leq x \leq n$ için,

$$f^r(i_j) = i_j \quad \therefore f^r(x) = x \Rightarrow f^r = I //$$

Örnek // $g = (136) \in S_6$ da,

$$g^2 = (136)(136) = (316)$$

$$g^3 = g^2 \cdot g = (316)(136) = (1)(3)(6) = I$$

$$o(g) = 3 //$$

Örnek // $f = (1356) \in S_6$ da,

$$f^2 = (1356)(1356) = (15)(36)$$

$$f^3 = (15)(36)(1356) = (1653)$$

$$f^4 = (1653)(1356) = (1)(3)(5)(6) = I$$

$$o(f) = 4 //$$

Önerme // S_n deki her permütasyon, sıra gözetmeksizin,

ayrık devirlerin çarpımı olarak tek türlü yazılabilir.

$$\left\{ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix} = \underbrace{(1)}_1 \underbrace{(2 \ 5)}_2 \underbrace{(3 \ 4 \ 6)}_3 = (3 \ 4 \ 6)(2 \ 5) \right\}$$

(Ayrık devirlerin çarpımı değişmelidir.)

İspat // $\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix} = (1)(2 \ f(2)f^2(2)f^3(2)) \dots \right\}$

$\text{ekok}(1, 2, 3) = 6$ simonö

$f \in S_n$, 1 in f altında ardarda görüntülerini alırsak,
 $1, f(1), f^2(1), \dots$ dizisi sonlu olduğundan, belli bir adımdan sonra tekrar eder. Yani, $f^k(1) = 1$ olacak şekilde en küçük bir $k \in \mathbb{Z}^+$ vardır. Buradan,

$$(1, f(1) \ f^2(1) \ f^3(1) \ \dots \ f^{k-1}(1))$$

deviri elde edilir. İşleme, burada gözükmeyen başka bir sayı olarak devam edilirse, elde edilen devirler ayrıktırlar ve çarpımları f yi verir. Ayrık devirlerin çarpımı değişmeli olduğundan, bu yazılış sıra gözetmeksizin tek türlü olur.

Önerme // Bir $f \in S_n$ permütasyonunun mertebesi, ayrıldığı ayrık devirlerin uzunluklarının en küçük ortak katıdır.

İspat // $\forall f \in S_n$, $f = c_1 c_2 \dots c_r$ ve c_i ler ayrık devirleri gösterebiliriz. $o(c_i) =: t_i$ ve $1 \leq i \leq r$

$$\text{ekok}(t_1, t_2, \dots, t_r) = m \text{ olsun.}$$

$$f^m = (c_1 c_2 \dots c_r)^m = c_1^m c_2^m \dots c_r^m$$

$$t_i | m \Rightarrow m = t_i k_i \text{ o.s. } \exists k_i \in \mathbb{Z}.$$

$$\Rightarrow f^m = c_1^{t_1 k_1} c_2^{t_2 k_2} \dots c_r^{t_r k_r}$$

$$\Rightarrow f^m = I, I, \dots, I \Rightarrow f^m = I \Rightarrow o(f) | m \text{ olur.}$$

Diğer taraftan, $o(f) = s$ olsun. $c_i = (i_1 \ i_2 \ \dots \ i_{t_i})$ $f|_A = c_i$ (kısıtlama ile)
 $c_i^s = I$ olur.

$$\left\{ f = \begin{pmatrix} 1 \\ c_1 \end{pmatrix} \begin{pmatrix} 2 \\ c_2 \end{pmatrix} \begin{pmatrix} 3 \\ c_3 \end{pmatrix} \begin{pmatrix} 4 \\ c_3 \end{pmatrix} \begin{pmatrix} 5 \\ c_2 \end{pmatrix} \begin{pmatrix} 6 \\ c_1 \end{pmatrix} \quad f|_{(2,5)} = (2,5) = c_2 \right\}$$

11.3.96

$$f^S = I \Rightarrow c_i^S = I \Rightarrow t_i | m$$

$$m = [t_1, t_2, \dots, t_r] | S \text{ yani } m | o(f) \text{ olur. } //$$

$$\text{Bu iki sonuştan } o(f) = m = [t_1, t_2, \dots, t_r] = \text{ekok}(t_1, t_2, \dots, t_r)$$

olur ve ispat biter. //

11.3.96/P. test

Önerme: Her devir, ikili devirlerin (transpozisyonların) çarpımı şeklinde yazılabilir. Bu yazılış tek türlü değildir.

$$\text{İspat } // (i_1 i_2 \dots i_r) = (i_1 i_r)(i_1 i_{r-1}) \dots (i_1 i_3)(i_1 i_2) = (i_1 i_2 \dots i_r) //$$

$$\text{Örnek } // (1 2 3 4) = (1 4)(1 3)(1 2) = (1 4)(2 3)(2 3)(1 3)(1 2)$$

(teklik veya çiftlik değişmez.)

Sonuç: Her permütasyon (devir), transpozisyonların çarpımı şeklinde yazılabilir.

Tanım: Bir permütasyon, çift (tek) sayıda ikilinin (transpozisyonun) çarpımı şeklinde yazılabiliyorsa, bu permütasyona çift (tek) permütasyon denir.

$$\text{Örnek } // f = (3 4)(1 2 5) = (3 4)(1 5)(1 2) \text{ tek permütasyon}$$

11.3.96

$$g = (3 4)(1 2 3 5) = (3 4)(1 5)(1 3)(1 2) \text{ çift permütasyon}$$

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

11.3.96

$$\left\{ \begin{array}{l} (2 3)(4 5) = (4 5)(2 3) \\ \text{ayrık devirler değişmelidir.} \end{array} \right\}$$

Önerme // S_n 'in bütün çift permütasyonları kümesi A_n ,

S_n 'in bir alt grubudur ve eleman sayısı $o(A_n) = \frac{n!}{2}$ dir.

$$\left\{ \begin{array}{l} I \in A_n \text{ dir. Yani birim fonksiyon çift permütasyondur.} \\ \text{Çünkü; } I = (1 2)(1 2) = (2 3)(2 3)(4 1)(4 1) \text{ olur.} \end{array} \right\}$$

$$\text{İspat } // \forall f, g \in A_n \text{ olsun. } \Rightarrow fg \in A_n \text{ (kapalılık)}$$

A_n sonlu olduğundan kapalılık yeterlidir $\Rightarrow A_n < S_n$ dir.

$o(S_n) = n!$ dir. S_n de, tek ve çift permütasyonların sayısının aynı olduğunu gösterirsek $o(A_n) = \frac{n!}{2}$ olur.

$A_n = \{f_1, f_2, \dots, f_k\}$ çift permütasyonların kümesi olsun. $(i_1 i_2)A_n = \{(\underbrace{i_1 i_2}_{\text{tek}})f_1, (\underbrace{i_1 i_2}_{\text{tek}})f_2, \dots, (\underbrace{i_1 i_2}_{\text{tek}})f_k\}$ olur.

Kabul edelim ki, bunlardan başka (farklı) en az bir g tek permütasyonu olsun.

$$(i_1 i_2)g \in A_n \Rightarrow (i_1 i_2)g = f_r \quad \text{o.s. } \exists 1 \leq r \leq k.$$

$$\Rightarrow g = (i_1 i_2)f_r \quad ((i_1 i_2) \text{nin tersi kendisidir.})$$

Buradan, başka tek permütasyon olmadığı görülür.

(Tek permütasyonların sayısını çift olmadığından, bu teorem tek permütasyonlar için geçerli değildir.)

Sonuç: $A_n \triangleleft S_n$ dir.

$$[S_n : A_n] = \frac{o(S_n)}{o(A_n)} = \frac{n!}{n!/2} = 2 \Rightarrow A_n \triangleleft S_n \text{ dir.}$$

$\left\{ \begin{array}{l} \forall a, b \in G \text{ için, } a \approx b \Leftrightarrow b = xax^{-1} \text{ o.s. } \exists x \in G. \text{ (eşlenik olma.)} \\ \text{eşlenik olma, denklik bağıntısıdır.} \\ c(a) = \{xax^{-1} \mid x \in G\} = \{a, b_1, b_2, \dots, b_k\} \\ \downarrow \\ a \text{ ile eşlenik olan elementlerin kümesidir.} \end{array} \right\}$

Bir elementin eşlenik sınıfını bulmak için bir formül gereklidir.

Şimdi, buna bakalım.

Önerme: $\sigma \in S_n$, $(i_1 i_2 \dots i_r)$ için

$$\sigma(i_1 i_2 \dots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\dots\sigma(i_r))$$

(Bir devirin herhangi uzunlukta bir devirle eşleştiği yine aynı uzunluktaadır.)

İspat: $\forall 1 \leq x \leq n$ için,

$$[\sigma(i_1 i_2 \dots i_r)\sigma^{-1}](x) = (\sigma(i_1)\sigma(i_2)\dots\sigma(i_r))(x)$$

i - $\sigma^{-1}(x) \notin \{i_1, i_2, \dots, i_r\}$ olsun.

$$\begin{aligned} [\sigma(i_1 i_2 \dots i_r) \sigma^{-1}](x) &= \sigma(i_1 i_2 \dots i_r) (\sigma^{-1}(x)) \\ &= \sigma((i_1 i_2 \dots i_r) (\sigma^{-1}(x))) \\ &= \sigma(\sigma^{-1}(x)) = x \end{aligned}$$

$\sigma^{-1}(x) \notin \{i_1, i_2, \dots, i_r\} \Rightarrow x \notin \{\sigma(i_1), \sigma(i_2), \dots, \sigma(i_r)\}$ $\left\{ \begin{array}{l} 1:1 \text{ ve örten} \\ \text{olduğundan} \end{array} \right.$

ii - $\sigma^{-1}(x) \in \{i_1, i_2, \dots, i_r\}$ olsun.

$\sigma^{-1}(x) = i_j \quad 1 \leq j \leq r$ ise $x = \sigma(i_j)$ olur.

$$\underbrace{[\sigma(i_1 i_2 \dots i_r) \sigma^{-1}]}_{\text{sol taraf}}(x) = (\sigma(i_1 i_2 \dots i_r))(\sigma^{-1}(x)) = \begin{cases} \sigma(i_{j+1}), & j < r \text{ ise} \\ \sigma(i_1), & j = r \text{ ise} \end{cases}$$

$$\begin{aligned} \underbrace{(\sigma(i_1) \sigma(i_2) \dots \sigma(i_r))}_{\text{sağ taraf}}(x) &= (\sigma(i_1) \sigma(i_2) \dots \sigma(i_r))(\sigma(i_j)) \\ &= \begin{cases} \sigma(i_{j+1}), & j < r \text{ ise} \\ \sigma(i_1), & j = r \text{ ise} \end{cases} \end{aligned}$$

O halde $1 \leq x \leq n$ için bu iki fonksiyon eşittir. Ve

$$\sigma(i_1 i_2 \dots i_r) \sigma^{-1} = (\sigma(i_1) \sigma(i_2) \dots \sigma(i_r)) \quad \text{dir.} //$$

Örnek $\sigma = (1 2 3)(4 5)$, $f = (2 5 3)$ ise

f nin σ ile eşlenliğini bulun. $\sigma f \sigma^{-1} = ?$

Gözüm $//$ 1.yol : $\sigma f \sigma^{-1} = \sigma(2) \sigma(5) \sigma(3) = (3 4 1) \checkmark$

$$2.\text{yol : } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$\sigma(1)=2 \quad \sigma(2)=3 \quad \sigma(3)=1 \quad \sigma(4)=5 \quad \sigma(5)=4$ olduğundan

$1=\sigma^{-1}(2) \quad 2=\sigma^{-1}(3) \quad 3=\sigma^{-1}(1) \quad 4=\sigma^{-1}(5) \quad 5=\sigma^{-1}(4)$ olur.

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

$$\sigma f \sigma^{-1} = (1 2 3)(4 5)(2 5 3)(3 1 2 5 4) = (5)(4 1 3) = (3 4 1) \checkmark$$

$$\left\{ \begin{array}{l} f, \sigma \in S_n, \quad f = c_1 c_2 \dots c_k \text{ (ayrık devirler çarpımı.)} \\ \sigma f \sigma^{-1} = \sigma c_1 c_2 \dots c_k \sigma^{-1} \\ \quad = (\sigma c_1 \sigma^{-1})(\sigma c_2 \sigma^{-1}) \dots (\sigma c_k \sigma^{-1}) \quad \text{olur.} \end{array} \right. //$$

Örnek // $f \circ f^{-1} = ?$ (Önceki örnek için sözelim.)

$$\begin{aligned} f(123)(45)f^{-1} &= (f(123)f^{-1})(f(45)f^{-1}) \\ &= (f(1)f(2)f(3))(f(4)f(5)) \\ &= (152)(43) \end{aligned}$$

Örnek // S_4 deki eşlenik sınıflarını bulun.

13.3.96/Çarşamba

S_4 de $P(4)=5$ tane eşlenik sınıfı vardır. Bunlar ;

$$C_1 = \{I\} \quad C_2 = \{(12), (13), (14), (23), (24), (34)\}$$

$$C_3 = \{(12)(34), (13)(24), (14)(23)\}$$

$$C_4 = \{(123), (132), (124), (142), (134), (143), (234), (243)\}$$

$$C_5 = \{(1234), (1243), (1324), (1342), (1423), (1432)\} \text{ olur.}$$

98/4 - S_n de $r < n$ olmak üzere kaç tane r -li devir vardır ?

Çözüm // S_n de r 'li devirlerin sayısı ;

$$\begin{aligned} n\text{-tane} \left\{ \begin{array}{l} \{i_1, i_2, \dots, i_r\} \rightarrow (r-1)! \\ \vdots \\ \{j_1, j_2, \dots, j_r\} \rightarrow (r-1)! \end{array} \right\} &= \frac{n!}{r \cdot (n-r)!} \\ (1 \leq r \leq n) \quad r=n \text{ ise } (n-1)! \text{ tane sıralama mümkündür.} \end{aligned}$$

Örneğin, S_5 de, 5 lilerin sayısı $(5-1)! = 4! = 24$ olur. //

97/2 - $f = (1234)(253) \quad \sigma = (135)$

σ nın f ile eşlenliğini bulun. $f \circ \sigma^{-1} = ?$

f nin σ ile eşlenliğini bulun. $\sigma f \sigma^{-1} = ?$

Çözüm // $f = (1234)(253) = (1254)(3) = (1254)$

$$f \circ \sigma^{-1} = f(135)f^{-1} = (f(1)f(3)f(5)) = (234)$$

$$\sigma f \sigma^{-1} = \sigma(1254)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(5)\sigma(4)) = (3214)$$

99/6 - S_4 de $\sigma = (123)$ 'ün eşlenik sınıfını ve $M(\sigma)$ merkezleştiricisini bulunuz.

Çözüm // S_4 de σ nın eşlenikleri 3'lü devirlerdir.

Bunların sayısı da, $(r-1)! \cdot \binom{n}{r} = \frac{n!}{r \cdot (n-r)!}$ de, $r=3$ $n=4$ alarak,

$$\frac{4!}{3 \cdot (4-3)!} = 2 \cdot 4 = 8 \text{ olur. Bunlar,}$$

$C(\sigma) = \{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}$ dir.
(iki devir; eşlenik $\Leftrightarrow$ aynı uzunluktadır.)

$a \in G$ için, $M(a) = \{x \in G \mid ax = xa \Leftrightarrow a = xax^{-1}\}$ idi. Buradan,

$$f \in M(\sigma) \Rightarrow f\sigma f^{-1} = \sigma$$

$$f\sigma f^{-1} = f(1\ 2\ 3)f^{-1} = (f(1)f(2)f(3)) = (1\ 2\ 3)$$

$$= (2\ 3\ 1) = (3\ 1\ 2) \text{ olur.}$$

$$\begin{array}{ccc} f(1)=1 & f(1)=2 & f(1)=3 \\ f(2)=2 & f(2)=3 & f(2)=1 \\ f(3)=3 & f(3)=1 & f(3)=2 \end{array} \text{ olduğundan,}$$

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

permütasyonları bulunur. O halde,

$$M(\sigma) = \{I, (1\ 2\ 3), (1\ 3\ 2)\} \text{ bulunur.}$$

$f\sigma = \sigma f$ bakalım.

$$(1\ 3\ 2)(1\ 2\ 3) = (1)(2)(3) = I = (1\ 2\ 3)(1\ 3\ 2) \text{ bulunur. //}$$

* S_8 de 3.2 tipindeki ayrıklar; $f = (1\ 3\ 7)(2\ 5)(4)(6)(8) \in S_8$ 18.3.96 / P. test.
3 + 2 + 1 + 1 + 1

8 tane dir. //

$f \in S_n$, $f = \sigma_1 \sigma_2 \dots \sigma_r$ (r i ayrık) $n = t_1 + t_2 + \dots + t_r$ $\sigma(\sigma_i) = t_i$ dir. //

f in g ile eşleniği;

$$gfg^{-1} = (g\sigma_1 g^{-1})(g\sigma_2 g^{-1}) \dots (g\sigma_r g^{-1}) \text{ dir.}$$

f in eşleniğinin belirttiği ayrışım, f in ayrışımı aynıdır.

* (Aynı ayrışımı belirten permütasyonlar eşleniktir.)

* (Uzunlukları eşit olan devirler eşleniktir.)

S_4 de, uzunluğu 2 eden devirler, $2+1+1 \Rightarrow 2$ tane dir.

$2+2$ ise ayrık ikililerin çarpımıdır.

Önerme // A_n , 3'lü devirlerle üretilmiştir. $! (A_n \triangleleft S_n \text{ idi})$

İspat // $\bar{U} := \{3 \text{ lü devirler kümesi}\}$ diyelim. $A_n = \langle \bar{U} \rangle$

Her 3'lü devir çift permütasyon olduğundan,

$$\bar{U} \subseteq A_n \Rightarrow \langle \bar{U} \rangle = A_n \text{ dir. //}$$

($\langle \bar{U} \rangle := \bar{U}$ 'ü kapsayan tüm alt grupların arakesiti.)

Ters kapsamayı gösterelim.

$\forall f \in A_n$ alalım. $f = \dots (i_1 i_2)(i_3 i_4) \dots$ (çift sayıda ikili)

i- $i_1 = i_3, i_2 = i_4$ olsa, ikisi eşit olduğundan birim olur.

ii- $i_1 = i_3$ olsun. $(i_1 i_2)(i_1 i_4) = (i_1 i_4 i_2)$

iii- $(i_1 i_3 i_2)(i_1 i_3 i_4) = (i_1 i_2)(i_3 i_4)$ olur.

O halde f , 3'lülerin grpmı şeklindedir. $f \in \langle \bar{U} \rangle$ olur.

Önerme // $n \geq 5$, $N \triangleleft A_n$ olsun. N bir 3'lü devir kapsarsa $N = A_n$ dir.

İspat // $\bar{U} \subseteq N \Rightarrow A_n = \langle \bar{U} \rangle \subseteq N \Rightarrow A_n \subseteq N$ olduğunu göstermeliyiz.

$(i_1 i_2 i_3) \in N$ olsun. $\forall (j_1 j_2 j_3) \in S_n$ için, aynı uzunluktaki devirler eşlelik olduğundan:

$$f(i_1 i_2 i_3) f^{-1} = (j_1 j_2 j_3) \text{ o.p. } \exists f \in S_n.$$

i- $f \in A_n$ olsun. $N \triangleleft A_n$ olduğundan,

$$N \ni f(i_1 i_2 i_3) f^{-1} = (j_1 j_2 j_3) \text{ olur.}$$

ii- $f \notin A_n$ olsun. (f tek permütasyon olsun.)

$n \geq 5$ olduğundan, $\{a, b\} \cap \{j_1, j_2, j_3\} = \emptyset$ o.p. $\exists 1 \leq a, b \leq n$.

$$(1 \leq i_1, i_2, i_3 \leq n)$$

$$f \notin A_n \Rightarrow (ab)f \in A_n. \quad \tau := (ab)f \text{ olsun.}$$

$$N \triangleleft A_n \text{ olduğundan, } \tau(i_1 i_2 i_3) \tau^{-1} \in N$$

$$\Rightarrow (ab)f(i_1 i_2 i_3)[(ab)f]^{-1} = (ab)f.(i_1 i_2 i_3).f^{-1}(ab)$$

$$\Rightarrow (ab)(j_1 j_2 j_3)(ab) = (a)(b)(j_1 j_2 j_3)$$

$$= (j_1 j_2 j_3) \in N$$



$\mathbb{U} \subset \mathbb{N}$ dir. Bir önceki teoremden $A_n = \langle \mathbb{U} \rangle \subset \mathbb{N}$ idi. //

O halde $\mathbb{N} = A_n$ olur. //

Tanım: (Basit Grup): Öz normal alt grubu olmayan gruptur.

Asal mertebeden devirli grup basit idi.

Teorem: (Abel): $n \neq 4$ için A_n , basit gruptur. ($\mathbb{N} \triangleleft A_n \triangleleft S_n$)

İspatı yapılmayacak. $n \neq 4$ için, A_4 ün basit grup olmadığını gösterelim. $V_4 < A_4$? $V_4 \triangleleft A_4$?

$$V_4 = \{I, (12)(34), (13)(24), (14)(23)\} < A_4$$

Bu gruba Klein'in 4'lü grubu denir.

$\sigma_1 \sigma_2, \sigma_1 \sigma_3, \sigma_2 \sigma_3 \in V_4 \Rightarrow V_4 < S_4$ olur. V_4 değişmeli gruptur.

$\forall \sigma_i \in V_4$ ve $\forall f \in A_4$ için;

$$\sigma_i \approx f \sigma_i f^{-1} \in V_4 \text{ olur. } \Rightarrow V_4 \triangleleft S_4 \text{ olur.}$$

(eşlenik permütasyonlar aynı ayrışımı belirtir idi.)

S_4 içinde, 2+2 ayrışimleri belirten permütasyonlar, yalnız V_4 dedir.

Soru // $\sigma = (143)(25) \in S_5 \Rightarrow M(\sigma) = ?$

$$M(\sigma) = \{f \in S_n \mid f\sigma = \sigma f \Rightarrow f\sigma f^{-1} = \sigma\}$$

$$f\sigma f^{-1} = (f(1)f(4)f(3))(f(2)f(5))$$

$$= (143)(25) = (143)(52)$$

$$= (431)(25) = (431)(52)$$

$$= (314)(25) = (314)(52)$$

$$f(1) = 1, 1, 4, 4, 3, 3$$

$$f(4) = 4, 4, 3, 3, 1, 1$$

$$f(3) = 3, 3, 1, 1, 4, 4$$

$$f(2) = 2, 5, 2, 5, 2, 5$$

$$f(5) = 5, 2, 5, 2, 5, 2$$

$$M(\sigma) = \{I, (143), (134), (25), (143)(25), (134)(25)\} //$$

$$103/16 - \beta := \{(12)(13), \dots, (1n)\} \quad S_n \stackrel{?}{=} \langle \beta \rangle$$

Gözüm // $S_n \subset \langle \beta \rangle$ olduğu aşıktır. Ters kapsamayı gösterelim.

$$\forall f \in S_n, f = \dots (i)(ij) \dots \in \langle \beta \rangle$$

$$(ij) = (1i)(1j)(1i) \text{ dir. } //$$

$$103/17 - P := \{(12)(23) \dots (n-1 n)\} \quad S_n \stackrel{?}{=} \langle P \rangle$$

$$\text{Gözüm // } (1i)(i-1 i)(1 i-1)$$

$$(14) = (13)(34)(13)$$

$$= (12)(23)(12)(34)(12)(23)(12) //$$

$$103/18 - Q := \{(12)(123 \dots n)\} \quad S_n \stackrel{?}{=} \langle Q \rangle$$

$$\text{Gözüm // } (123 \dots n)(i-1 i)(123 \dots n)^{-1}$$

$$= (123 \dots n)(i-1 i)(n \dots 321) = (i' i'+1) \text{ eşitliğinden,}$$

$$(23) = (12 \dots n)(12)(12 \dots n)^{-1}$$

$$(34) = (12 \dots n)(23)(12 \dots n)^{-1}$$

şeklinde devam ederek 17. problemleri istenen bulunur. // 20.3.96
Görüşme

$$98/5 - S_n \text{ de } \sigma = (12 \dots n) \text{ eşlenik sınıfını ve } M(\sigma) \text{ yı bulun.}$$

Gözüm // n -uzunluğundaki bir devirin eşlenikleri de n -uzunluğundadır.

Bu nedenle σ 'nin eşlenikleri, S_n de n -uzunluğundaki tüm

devirlerdir. Bunların sayısı $(n-1)!$ dir.

$$c(\sigma) = [S_n : M(\sigma)] \Rightarrow o(M(\sigma)) = \frac{n!}{(n-1)!} = n$$

ve $o(\sigma) = n$ olduğundan,

$$\sigma \in M(\sigma) \Rightarrow \langle \sigma \rangle \subset M(\sigma) \Rightarrow \langle \sigma \rangle = M(\sigma) \text{ olur. } //$$

HALKALAR

25.3.96/P.tesi

$R \neq \emptyset, (R, +, \cdot)$ yapısına bir halka denir, eğer :

- × i - $(R, +)$ değişmeli grup,
- × ii - $\forall a, b, c \in R, a(bc) = (ab)c$, (birleşme öz.)
- × iii - $a(b+c) = ab+ac$, $(a+b)c = ac+bc$, özellikleri varsa.
- iv - $0_R :=$ halkanın sıfırı. $1_R :=$ halkanın birimi.

(ikinci işleme göre) halkanın birimi varsa halkaya birimli halka denir.

v - İkinci işlemin, $ab=ba$ değişme özelliği varsa, halkaya değişmeli halka denir.

Örnekler // 1 - $(\mathbb{Z}, +, \cdot)$ birimli, değişmeli halkadır.

2 - $(2\mathbb{Z}, +, \cdot)$ değişmeli halkadır. (birim yok)

3 - $(\mathbb{Z}_n, \oplus, \otimes)$ birimli, değişmeli halkadır.

4 - $(\mathbb{R}[X], +, \cdot)$ birimi 1 olan değişmeli halkadır.

5 - $(\mathbb{R}_n^1, +, \cdot)$ birimli halkadır.

6 - $(\mathbb{Z} \times \mathbb{Z}, \oplus, \otimes)$ birimi $(1,1)$, sıfırı $(0,0)$ olan değişmeli halkadır. $\alpha = (x_1, y_1)$ $\beta = (x_2, y_2)$

$$(\alpha \oplus \beta) := (x_1 + x_2, y_1 + y_2) \quad (\alpha \otimes \beta) := (x_1 \cdot x_2, y_1 \cdot y_2)$$

R bir halka ve $\emptyset \neq A$ bir küme olsun.

$$M(A, R) := \{f: A \longrightarrow R\}$$

$$\forall f, g \in M(A, R), \quad f \oplus g: A \longrightarrow R$$

$$x \longmapsto (f \oplus g)(x) := f(x) + g(x)$$

ile tanımlarsak, $f \oplus g \in M(A, R)$ olur.

$$\begin{aligned} (H_1) \quad G_1: [f \oplus (g \oplus h)](x) &= f(x) + [(g \oplus h)(x)] \\ &= f(x) + [g(x) + h(x)] \\ &= [f(x) + g(x)] + h(x) \\ &= [f \oplus g](x) + h(x) \\ &= [(f \oplus g) \oplus h](x) \end{aligned}$$

$\Rightarrow f \oplus (g \oplus h) = (f \oplus g) \oplus h$ olur. Birleşme özelliği vardır.

İkinci işlen ise şöyle tanımlansın:

$$\begin{aligned} f \odot g &: A \longrightarrow R \\ x &\longrightarrow (f \odot g)(x) := f(x) \cdot g(x) \end{aligned}$$

G₂: $\mathcal{O} : A \longrightarrow R$
 $x \longrightarrow \mathcal{O}(x) = 0_R$ ile tanımlı $\mathcal{O}$ fonksiyonu (sıfır dönüşümü), $M(A, R)$ nin bir elemanı olup, $\oplus$ işleninin etkisiz elemanıdır. Gerçekten $f \oplus \mathcal{O} = \mathcal{O} \oplus f = f$ dir. Çünkü,

$$(f \oplus \mathcal{O})(x) = f(x) + \mathcal{O}(x) = f(x) + 0_R = f(x)$$

$$(\mathcal{O} \oplus f)(x) = \mathcal{O}(x) + f(x) = 0_R + f(x) = f(x) \text{ dir.}$$

G₃: $f \in M(A, R)$ nin $\oplus$ işlenine göre tersi vardır. Bulalım.

Tersini $-f$ ile gösterelim.

$$f \oplus -f = -f \oplus f = \mathcal{O} \text{ dir. Öyle ki,}$$

$$\begin{aligned} -f &: A \longrightarrow R \\ x &\longrightarrow -f(x) = -f(x) \end{aligned} \text{ ile tanımlarsak, } -f \in M(A, R) \text{ ve}$$

$$(f \oplus -f)(x) = f(x) + (-f(x)) = f(x) - f(x) = 0_R = \mathcal{O}(x) \text{ // doğru}$$

$$(-f \oplus f)(x) = -f(x) + f(x) = (-f(x)) + f(x) = 0_R = \mathcal{O}(x) \text{ olur.}$$

G₄: $f \oplus g = g \oplus f$ değişmeli olduğunu gösterelim. -i

$$\forall x \in A \text{ için, } (f \oplus g)(x) = f(x) + g(x) = g(x) + f(x) = (g \oplus f)(x) \text{ dir.}$$

↓
 $\{ (R, +) \text{ değişmeli olduğundan. } \}$

$\Rightarrow (M(A, R), \oplus)$ değişmeli grup olur.

(H₂) • $\forall f, g, h \in M(A, R)$ için $f \odot (g \odot h) = (f \odot g) \odot h$? bakalım.

$$[f \odot (g \odot h)](x) = f(x) [(g \odot h)(x)]$$

$$= f(x) [g(x) h(x)]$$

$$= [f(x) g(x)] h(x)$$

$$= [f(x) g(x)] \odot h(x)$$

$$= [(f \odot g)(x)] \odot h(x) = [(f \odot g) \odot h](x) \text{ dir.}$$

$\Rightarrow f \odot (g \odot h) = (f \odot g) \odot h$ olur. //

H3 · $f \odot (g \oplus h) = (f \odot g) \oplus (f \odot h)$? bakalım.

$$\begin{aligned}[f \odot (g \oplus h)](x) &= f(x)(g \oplus h)(x) = f(x)(g(x) + h(x)) \\ &= f(x)g(x) + f(x)h(x) = (f \odot g)(x) + (f \odot h)(x) \\ &= [(f \odot g) \oplus (f \odot h)](x) \quad //\end{aligned}$$

O halde $(M(A, R), \oplus, \odot)$ yapısı bir halkadır.

$1_R \in R$ ise $I : A \longrightarrow R$
 $x \longrightarrow I(x) := 1_R$ fonksiyonu $M(A, R)$ nin birimidir.

$f \odot I = I \odot f = f$ olur. Çünkü,

$$(f \odot I)(x) = f(x) \cdot I(x) = f(x) \cdot 1_R = f(x)$$

$$(I \odot f)(x) = I(x) \cdot f(x) = 1_R \cdot f(x) = f(x) \quad \text{dir.}$$

Önerme // R bir halka ve $a, b \in R$ olsun.

i- $a \cdot 0_R = 0_R \cdot a = 0_R$

ii- $a(-b) = (-a)b = -(ab)$

iii- $(-a)(-b) = ab$ olur.

İspat // i- $a \cdot 0_R = a(0_R + 0_R) = a \cdot 0_R + a \cdot 0_R \Rightarrow 0_R = a \cdot 0_R \quad //$

$$0_R \cdot a = (0_R + 0_R) \cdot a = 0_R \cdot a + 0_R \cdot a \Rightarrow 0_R = 0_R \cdot a \quad //$$

ii- $a \cdot 0_R = 0_R$, $\bullet a \cdot 0_R = a(b + (-b)) = 0_R$

$$= ab + a(-b) = 0_R \Rightarrow a(-b) = -(ab) \quad //$$

$$\bullet 0_R \cdot b = (a + (-a))b = 0_R$$

$$= ab + (-a)b = 0_R \Rightarrow (-a)b = -(ab) \quad //$$

iii- $(-a)(-b) \stackrel{\text{ii'den}}{=} -[a(-b)] = -[-(ab)] = ab \quad //$

$1_R \in R$ ise,

a) $-a = -1_R \cdot a$

b) $(-1_R) \cdot (-1_R) = 1_R$ dir. //

{ Bir elemanın, bir iplene göre
tersi varsa; tersinin tersi
yine o elemandır.
 $aX = e = Xa$
 $a = (a^{-1})^{-1} = x^{-1}$ dir.

- $R = \{x\}$ ise $x \square x := x$ ve $x \triangle x := x$ şeklinde ise $(R, \square, \triangle)$ yapısı bir halka olur. //
- $R = \{0\}$ ise $(R, +, \cdot)$ halkadır. //
- Birimli bir halkada en az iki eleman vardır. Bunlar halkanın sıfırı ve birimidir. $(A = \{0, 1\}, +, \cdot)$ yapısı halkadır. //

Tanım: $0 \neq a \in R$ olsun. $ab = 0_R$ olacak şekilde $\exists 0 \neq b \in R$ varsa a 'ya 'sıfır bölen' denir (sıfır bölen eleman)

Örnek // $(\mathbb{Z}_6, +, \cdot)$ halkasında $2 \cdot 3 = 0$ $3 \cdot 4 = 0$

2, 3 ve 4 sıfır bölen elemanlardır. //

$(\mathbb{Z}, +, \cdot)$ halkasında sıfır bölen yoktur. (T.B.'dir)

Bir halkada hiçbir eleman sıfır bölen değilse, o halkaya sıfır bölensiz halka denir.

Tanım: Birimli, değişmeli ve sıfır bölensiz bir halkaya TAMLIK BÖLGESİ (T.B.) denir.

Önerme // R sıfır bölensizdir $\Leftrightarrow$ sağ ve sol kısaltma özelliği vardır.

$$\begin{cases} ab = ac \Leftrightarrow b = c \\ ba = ca \Leftrightarrow b = c \end{cases} \quad \forall a, b, c \in R, \quad a \neq 0$$

İspat // $(\Rightarrow): ab = ac \Rightarrow ab + (-ac) = 0$

$$\Rightarrow a(b - c) = 0$$

hipotezden ve $a \neq 0$ olduğundan $b - c = 0$ olmalıdır. $\Rightarrow b = c$ olur.

$(\Leftarrow): \forall 0 \neq a \in R$ için $\exists b \in R$ için $ab = 0$ olsa $a \cdot 0 = 0$ idi. (örnek)

$\Rightarrow$ hipotezden $b = 0$ olmalıdır. $\therefore a$ sıfır bölen değildir.

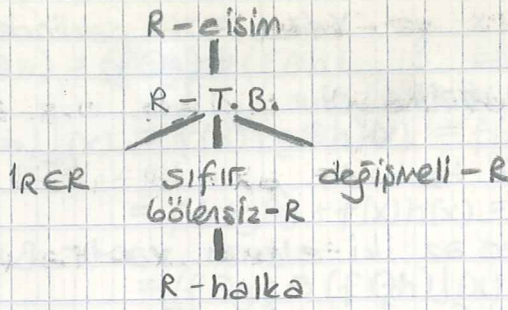
O halde R halkası sıfır bölensizdir. //

Sıfır bölensizlik, kısaltma özelliğine denktir.

Sonuç: Sıfır bölensiz bir halkada $a \neq 0$ için $ax = b$ denkleminin bir tek x çözümü vardır. Fakat böyle bir x bulunmayabilir.

Çünkü halka ikinci işleme göre grup değil.

$$\left\{ \begin{array}{l} 2 \cdot x = 3 \text{ çözüm yoktur. (Halka sıfır bölensiz ise)} \end{array} \right\}$$



Tanım: R birimli ve değişmeli bir halka ve $R - \{0_R\} = R^*$ ikinci işleme göre bir grup ise yani her elemanın tersi varsa (sifirdan farklı elemanların) R ye bir cisim denir. Veya :

$(F, +, \cdot)$ cisimdir. Eğer

i - $(F, +)$ değişmeli grup,

ii - $(F^*, \cdot)$ değişmeli grup ise.

Örnek // $(\mathbb{Z}, +, \cdot)$ bir T.B. dir. İkinci işleme göre sifirdan farklı her elemanın tersi olmadığından cisim değildir.

$(\mathbb{Q}, +, \cdot)$ bir T.B. dir.

$(\mathbb{C}, +, \cdot)$ bir T.B. dir.

$(\mathbb{R}, +, \cdot)$ bir T.B. dir.

Önerme // Sonlu elemanlı tanımlık bölgesi cisimdir.

İspat // $R = \{x_1, x_2, \dots, x_n\}$ bir tanımlık bölgesi olsun. Birimli, değişmeli ve sifir bölensiz bir halkadır. Bunlara ilaveten ikinci işleme göre halka olduğunu gösterirsek (yani $\neq 0$ her elemanın tersinin olduğunu gösterirsek) ispat biter.

$\forall 0 \neq a \in R$ için, $f: R \rightarrow R$
 $x \mapsto f(x) := ax$ tanımlayalım.

Fonksiyon olur mu, bakalım.

$x_1 = x_2$ iken $f(x_1) = f(x_2)$ dir. (iyi tanımlılık)

$f(x_i) = f(x_j) \Rightarrow ax_i = ax_j \Rightarrow x_i = x_j \Rightarrow f$ 1:1 dir.

$\downarrow$
 R bir T.B. old.

R sonlu küme olduğundan, f 'nin 1:1 olması örten olmasını gerektirir.

R sonlu küme; $(f \text{ 1:1} \Leftrightarrow f \text{ örten})$

$1_R \in R$ için $(f \text{ örten olduğundan}) f(x) = 1_R$ o.s. $\exists x \in R$.

$$\Rightarrow ax = 1_R$$

$$\Rightarrow 1_R = ax = xa \text{ (} R \text{ deę. old.)}$$

$$\Rightarrow x = a^{-1} \in R \text{ dir.}$$

Dolayısıyla her elemanın tersi vardır.

Yani sonlu elemanlı tanımlık bölgesi bir cisimdir. //

* R sonlu olmasaydı örtenlikten söz edilemezdi. Yani a 'nın tersi gösterilemez ve cisim olmazdı.

$\mathbb{Z}$ tamsayılar halkası T.B. dir. Fakat tamsayılar kümesi

sonsuz olduğundan; $f: \mathbb{Z} \rightarrow \mathbb{Z}$

$$x \mapsto f(x) = ax \text{ fonksiyonu 1:1 dir.}$$

fakat örten değildir. O halde $(\mathbb{Z}, +, \cdot)$ cisim değildir. *

Örnek // $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ p asal sayı ise $(\mathbb{Z}_p, +, \cdot)$ sonlu T.B. ve cisimdir. Çünkü $(\mathbb{Z}_p, +, \cdot)$ birimli, deęişmeli ve sıfır bölensiz halkadır. $\mathbb{Z}_p, \langle \bar{1} \rangle$ ile üretildiğinden birimi $\bar{1}$ dir.

Sıfır bölensizdir $\Leftrightarrow$ Asal kalan sıfıftır. $\Leftrightarrow$ Her $\neq 0$ elemanın tersi vardır.

O halde sıfır bölensiz, birimli ve deęişmeli halka olduğundan,

$\mathbb{Z}_p$ bir T.B. dir. Ayrıca her elemanın (sıfırdan farklı) tersi olduğundan

$\mathbb{Z}_p$ bir cisimdir. //

Tanım ! R bir T.B. olsun. $m \cdot 1_R = 0_R$ olacak şekilde en küçük $m \in \mathbb{Z}^+$ varsa, bu m sayısına R 'nin karakteristięi denir. Böyle bir $m \in \mathbb{Z}^+$ yoksa R nin karakteristięi sıfırdır denir.

Örnek // $(\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Q}, +, \cdot)$ karakteristięi sıfır olan halkalardır.

$$m \cdot 1 = 0 \text{ o.s. } m > 0 \text{ yoktur. //$$

Örnek // $(\mathbb{Z}_8, +, \cdot)$ nin karakteristięi; $8 \cdot \bar{1} = \bar{0} \Rightarrow \bar{1} + \bar{1} + \dots + \bar{1} = \bar{0}$

$\text{kar}(\mathbb{Z}_8) = 8$ dir. $\mathbb{Z}_8$, T.B. değildir. //

$\{(\mathbb{Z}, +, \cdot) \text{ kar}(\mathbb{Z}) = 0 \text{ dir.}\}$

R sonlu küme; $(f \text{ 1:1} \Leftrightarrow f \text{ örten})$

$1_R \in R$ için $(f \text{ örten olduğundan}) f(x) = 1_R$ o.s. $\exists x \in R$.

$$\Rightarrow ax = 1_R$$

$$\Rightarrow 1_R = ax = xa \text{ (} R \text{ değ. old.)}$$

$$\Rightarrow x = a^{-1} \in R \text{ dir.}$$

Dolayısıyla her elemanın tersi vardır.

Yani sonlu elemanlı tanlık bölgesi bir cisimdir. //

* R sonlu olmasaydı örtenlikten söz edilemezdi. Yani a 'nın tersi gösterilemez ve cisim olmazdı.

$\mathbb{Z}$ tamsayılar halkası T.B. dir. Fakat tamsayılar kümesi sonsuz olduğundan; $f: \mathbb{Z} \rightarrow \mathbb{Z}$
 $x \mapsto f(x) = ax$ fonksiyonu 1:1 dir. $\checkmark$

fakat örten değildir. O halde $(\mathbb{Z}, +, \cdot)$ cisim değildir. $\star$ *teğai*

Örnek // $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ p asal sayı ise $(\mathbb{Z}_p, +, \cdot)$ sonlu T.B. ve cisimdir. Çünkü $(\mathbb{Z}_p, +, \cdot)$ birimli, değişmeli ve sıfır bölensiz halkadır. $\mathbb{Z}_p, \langle \bar{1} \rangle$ ile üretildiğinden birimi $\bar{1}$ dir.

Sıfır bölensizdir $\Leftrightarrow$ Asal kalan sıfıftır. $\Leftrightarrow$ $\neq 0$ Her elemanın tersi vardır. O halde sıfır bölensiz, birimli ve değişmeli halka olduğundan, $\mathbb{Z}_p$ bir T.B. dir. Ayrıca her elemanın (sıfırdan farklı) tersi olduğunda $\mathbb{Z}_p$ bir cisimdir. //

Tanım : R bir T.B. olsun. $m \cdot 1_R = 0_R$ olacak şekilde en küçük $m \in \mathbb{Z}^+$ varsa, bu m sayısına R 'nin karakteristiği denir. Böyle bir $m \in \mathbb{Z}^+$ yoksa R nin karakteristiği sıfırdır denir.

Örnek // $(\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Q}, +, \cdot)$ karakteristiği sıfır olan halkalardır.

$$m \cdot 1 = 0 \text{ o.s. } m > 0 \text{ yoktur. //$$

Örnek // $(\mathbb{Z}_8, +, \cdot)$ nin karakteristiği; $8 \cdot \bar{1} = \bar{0} \Rightarrow \bar{1} + \bar{1} + \dots + \bar{1} = \bar{0}$

$\text{kar}(\mathbb{Z}_8) = 8$ dir. $\mathbb{Z}_8$, T.B. değildir. //

$\{(\mathbb{Z}, +, \cdot) \text{ kar}(\mathbb{Z}) = 0 \text{ dir.}\}$

Önerme // R bir T.B ise sıfırdan farklı her elemanın R nin toplamsal grubundaki mertebeleri aynıdır.

(R bir T.B ise $\forall a, b \in R$, $o(a) = o(b)$ dir. (+) ya göre.)

İspat // $\forall 0 \neq a \in R$ ve $o(a) = k$ olsun. $\Rightarrow k \cdot a = 0_R$ ($k \in \mathbb{Z}^+$)

$$k \cdot a = k \cdot (1_R \cdot a) = \underbrace{1_R \cdot a + 1_R \cdot a + \dots + 1_R \cdot a}_{k\text{-tane}}$$

$$\Rightarrow (\underbrace{1_R + 1_R + \dots + 1_R}_{k\text{-tane}}) \cdot a = 0_R \Rightarrow (k \cdot 1_R) \cdot a = 0_R$$

R bir T.B. ve $a \neq 0$ olduğundan $k \cdot 1_R = 0_R$ olur.

$$\forall 0 \neq b \in R \text{ alalım. } k \cdot b = k \cdot (1_R \cdot b) = (k \cdot 1_R) \cdot b = 0_R \cdot b = 0_R$$

$\Rightarrow o(b) \mid k$ olur. Burada a 'yı mertebesi en küçük eleman

olarak seçersek $o(b) = k$, yani $o(a) = k = o(b)$ olur. //

Önerme // T.B. nin karakteristiği sıfır değilse, asal sayıdır.

İspat // R bir T.B. ve karakteristiği $0 \neq m$ olsun.

$k \cdot 1_R = 0_R$ o.s. $k = p \cdot q$ $1 \leq p, q \leq k$ olsa;

$$k \cdot 1_R = (p \cdot q) \cdot 1_R = (p \cdot 1_R) \cdot (q \cdot 1_R) = 0_R$$

$$(p \cdot q) \cdot 1_R = \underbrace{(1_R + \dots + 1_R)}_{q\text{-tane}} + \underbrace{(1_R + \dots + 1_R)}_{q\text{-tane}} + \dots + \underbrace{(1_R + \dots + 1_R)}_{q\text{-tane}}$$

$$= \underbrace{(1_R + \dots + 1_R)}_{q\text{-tane}} \cdot 1_R + \underbrace{(1_R + \dots + 1_R)}_{q\text{-tane}} \cdot 1_R + \dots + \underbrace{(1_R + \dots + 1_R)}_{q\text{-tane}} \cdot 1_R$$

$$= (q \cdot 1_R) \cdot 1_R + (q \cdot 1_R) \cdot 1_R + \dots + (q \cdot 1_R) \cdot 1_R$$

$$= (q \cdot 1_R) \cdot (\underbrace{1_R + 1_R + \dots + 1_R}_{p\text{-tane}})$$

$$(p \cdot q) \cdot 1_R = (q \cdot 1_R) \cdot (p \cdot 1_R) = 0_R$$

$$\Rightarrow (p \cdot 1_R) = 0_R \vee (q \cdot 1_R) = 0_R \vee k \text{ asaldır.}$$

İlk iki hâl, gelişkiye neden olur. Eğer bunlardan birisi sıfır olursa, k çarpanlarına ayrılmaz. Bu ise k 'nin karakter (en küçük, $1 \leq p, q \leq k$) olmasıyla gelişir.

0 halde k asaldır. //

Örnek // $\mathbb{Z}_p$ (p asal) T.B. nin karakteristiği p dir. //

Alt Halka ve İdealler

Tanım: R halka ve $\emptyset \neq H \subset R$ olsun. R deki işlemlere göre H alt kümesi de bir halka ise, H 'ye R halkasının bir alt halkası denir.

Örnek // $(2\mathbb{Z}, +, \cdot)$ halkası, $(\mathbb{Z}, +, \cdot)$ halkasının bir alt halkasıdır.

Önerme // H, R nin alt halkasıdır $\Leftrightarrow \forall a, b \in H, a, b \in R,$

$$i - a - b \in H \quad (H, +) < (R, +)$$

$$ii - ab \in H$$

Önerme // Bir halkanın bir takım alt halkalarının arakesiti de bir alt halkadır.

İspat // H_i, R nin alt halkaları, $\bigcap_{i \in I} H_i$

$$a, b \in \bigcap_{i \in I} H_i \Rightarrow \forall i \in I \text{ için } a, b \in H_i \text{ dir.}$$

H_i ler alt halka olduğundan $\forall i \in I$ için $a - b, ab \in H_i$ dir.

$$\Rightarrow a - b, ab \in \bigcap_{i \in I} H_i \text{ olur. //}$$

{ iki alt halkanın birleşimi alt halka olmayabilir.

{ $(2\mathbb{Z}, +, \cdot)$ ve $(3\mathbb{Z}, +, \cdot)$ alt halka fakat, $2+3=5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ dir.

Tanım: R bir halka ve $\emptyset \neq A \subset R$ olsun. R nin, A yı kapsayan alt halkalarının arakesitine, A kümesiyle üretilen alt halka denir ve $\langle A \rangle$ ile gösterilir. Yani;

$$\langle A \rangle := \bigcap_{i \in I} H_i \quad \forall i \in I \text{ için } A \subset H_i \text{ ve } H_i \text{ ler alt halka.}$$

Tanım: R bir halka, $\emptyset \neq I \subset R$ olsun.

$$i - \forall a, b \in I, \underline{a - b} \in I \quad (I, +) < (R, +)$$

$$ii - \forall a \in I, \forall r \in R, \underline{r \cdot a} \in I \quad (a \in I)$$

İse I 'ya R nin bir sol (veya sağ) ideali denir.

Her sağ, herde sol ideale iki taraflı ideal veya

kısaca ideal denir. İdeal bir alt halkadır.

I ideal $\Rightarrow$ Alt halkadır.

Değişmeli halkada, ar ve ra olması fark etmez. İdeal halkadan daha güçlüdür. Çünkü, her ideal aynı zamanda bir alt halkadır.

★ ★ İdealde, kümenin dışından bir eleman aldığımızda, kümenin elemanı ile çarparsak yine kümede kalır. $(2\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ nin bir idealidir. Bu kümenin dışından 3 sayısını alıp, bu kümedeki bir elementle çarparsak yine bu kümede kalır. $2 \cdot 3 = 6 \in 2\mathbb{Z}$

Örnek // $I = \{0_R\}$ ve R , her R halkasının bir idealidir. Bunlara R nin Aşıkâr idealleri denir. Bunlardan farklı idealler ise özideallerdir.

Örnek // $(2\mathbb{Z}, +, \cdot)$ ideal midir?

$\forall a, b \in 2\mathbb{Z}$ için $a = 2t, b = 2m$ o.ş $t, m \in \mathbb{Z}$.

i- $a - b = 2t - 2m = 2(t - m) \in 2\mathbb{Z}$

ii- $\forall a \in 2\mathbb{Z}, \forall r \in \mathbb{Z}$ için,

$$\underbrace{ar = ra = r \cdot 2t = 2(rt)}_{\mathbb{Z} \text{ def. old.}} \in 2\mathbb{Z}$$

O halde $(2\mathbb{Z}, +, \cdot)$ idealdir. //

Örnek // Benzer şekilde $(3\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}\mathbb{Z}, +, \cdot)$ ideal olduğu gösterilir. //

Örnek // $A = \{2n+1 \mid n \in \mathbb{Z}\} \subset \mathbb{Z}$ kümesi ideal midir?

$\forall a, b \in A$ için, $a = 2k+1, b = 2l+1$ o.ş $k, l \in \mathbb{Z}$.

i- $a - b = (2k+1) - (2l+1) = 2(k-l) \notin A$ olduğundan,

tek sayılar kümesi ideal değildir. //

$$\left\{ \begin{array}{l} a \in I, r \in R \Rightarrow ar \in I \text{ idi.} \\ \end{array} \right.$$

$$\left\{ \begin{array}{l} x, y \in I, 12 = 3 \cdot 4 \in 6\mathbb{Z}, \\ \quad \quad \quad \downarrow \quad \downarrow \\ \quad \quad \quad 3 \notin 6\mathbb{Z} \quad 4 \notin 6\mathbb{Z} \end{array} \right. \quad \left. \begin{array}{l} 3 \text{ ve } 4 \text{ alt halkanın elemanı} \\ \text{olmadığı halde çarpımları} \\ \text{alt halkodadır. ileride bu konu} \\ \text{hakkında bahsedilecektir.} \end{array} \right\}$$

★ $\{0_R\}$, $M = \emptyset$ (ideal değildir.)

$$\Rightarrow \langle M \rangle = \{0_R\} = \langle 0_R \rangle \text{ dir.}$$

Önerme // Bir R halkasının herhangi sayıdaki ideallerinin arakesiti de idealdir.

İspat // Ödev.

Tanım : M, R halkasının bir alt kümesi olsun. ($M \subset R$)

R 'nin, M 'yi kapsayan ideallerinin arakesitine, M nin Ürettiği ideal denir. ve ;

$$\langle M \rangle := \bigcap_{i \in J} I_i \quad \forall i \in J \text{ için } I_i \text{ ler } R \text{ nin ideali ve } M \subset I_i \text{ dir.}$$

Eğer $M = \{a\}$ tek elemanlı bir küme ise, M nin ürettiği ideale tek üreteçli ideal denir.

$$\left\{ \begin{array}{l} (\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2, \oplus, \odot) \text{ birimi } (1,1), \text{ sıfırı } (0,0) \text{ olan} \\ \text{birimli ve değişmeli halkadır.} \\ (a,b) \oplus (c,d) = (a+c, b+d) \\ (a,b) \odot (c,d) = (ac, bd) \end{array} \right\} \text{ olmak şartıyla.}$$

$$\{ M = \emptyset \text{ nin ürettiği ideal } \langle M \rangle = \{0_R\} = \langle 0_R \rangle \text{ dir.} \}$$

Önerme // $\emptyset \neq M \subset R$,

$$\langle M \rangle = \left\{ \sum_{i=1}^x r_i a_i + \sum_{i=1}^y b_i s_i + \sum_{i=1}^z k_i c_i l_i + \sum_{i=1}^t m_i d_i \mid \begin{array}{l} a_i, b_i, c_i, d_i \in M \\ r_i, s_i, k_i, l_i \in R \\ x, y, z, t \in \mathbb{N}, m_i \in \mathbb{Z} \end{array} \right\}$$

İspat // iddia; $\langle M \rangle = A$ dir. $\langle M \rangle$ yerine A yazalım, yani :

$$A := \left\{ \sum_{i=1}^x r_i a_i + \sum_{i=1}^y b_i s_i + \sum_{i=1}^z k_i c_i l_i + \sum_{i=1}^t m_i d_i \mid \dots \right\}$$

olsun. $\begin{array}{l} i - A \text{ ideal} \\ ii - M \subset A \end{array} \Rightarrow \langle M \rangle \subset A$

A nin ideal olduğunu göstermek için iki eleman alalım.

i - $\forall \alpha \in M, \alpha = 0_R \cdot \alpha + \alpha \cdot 0_R + 0_R \cdot \alpha + 1 \cdot \alpha \in A$ dir.

$\forall \alpha, \beta \in A$, A 'nin tanımından ;

$$\alpha = \sum_{i=1}^x r_i a_i + \sum_{i=1}^y b_i s_i + \sum_{i=1}^z k_i c_i l_i + \sum_{i=1}^t m_i d_i \quad \text{o.s.} \quad \begin{array}{l} a_i, b_i, c_i, d_i \in M \\ r_i, s_i, k_i, l_i \in R \\ x, y, z, t \in \mathbb{N}, m_i \in \mathbb{Z} \end{array}$$

$$\beta = \sum_{i=1}^{x'} r'_i a'_i + \sum_{i=1}^{y'} b'_i s'_i + \sum_{i=1}^{z'} k'_i c'_i l'_i + \sum_{i=1}^{t'} m'_i d'_i \quad \text{o.s.} \quad \begin{array}{l} a'_i, b'_i, c'_i, d'_i \in M \\ r'_i, s'_i, k'_i, l'_i \in R \\ x', y', z', t' \in \mathbb{N}, m'_i \in \mathbb{Z} \end{array}$$

$$-\beta = \sum_{i=1}^{x'} \underline{r_i'' a_i'} + \sum_{i=1}^{y'} \underline{b_i' s_i''} + \sum_{i=1}^{z'} \underline{k_i'' c_i' l_i'} + \sum_{i=1}^{t'} \underline{m_i'' d_i'}$$

$$(-r_i'') = r_i''', (-s_i'') = s_i''', (-k_i'') = k_i''' \text{ yazarak.}$$

$$\begin{aligned} \alpha - \beta &= \sum_{i=1}^x \underline{r_i a_i} + \sum_{i=1}^{x'} \underline{r_i'' a_i'} + \sum_{i=1}^y \underline{b_i s_i} + \sum_{i=1}^{y'} \underline{b_i' s_i''} + \sum_{i=1}^z \underline{k_i c_i l_i} + \sum_{i=1}^{z'} \underline{k_i'' c_i' l_i'} + \\ &\quad + \sum_{i=1}^t \underline{m_i d_i} + \sum_{i=1}^{t'} \underline{m_i'' d_i'} \\ &= \sum_{i=1}^{x+x'} \underline{r_i''' a_i'''} + \sum_{i=1}^{y+y'} \underline{b_i''' s_i'''} + \sum_{i=1}^{z+z'} \underline{k_i''' c_i''' l_i'''} + \sum_{i=1}^{t+t'} \underline{m_i''' d_i'''} \in A \end{aligned}$$

$$\Rightarrow \alpha - \beta \in A \text{ olur.}$$

ii- $\forall u \in R$ ve $\forall \alpha \in R$ için,

$$\begin{aligned} u \cdot \alpha &= u \left(\sum_{i=1}^x \underline{r_i a_i} + \sum_{i=1}^y \underline{b_i s_i} + \sum_{i=1}^z \underline{k_i c_i l_i} + \sum_{i=1}^t \underline{m_i d_i} \right) \\ &= \sum_{i=1}^x (u r_i) a_i + \sum_{i=1}^y u b_i s_i + \sum_{i=1}^z (u k_i) c_i l_i + \sum_{i=1}^t u m_i d_i \end{aligned}$$

Dağılım özelliğinden yazabiliriz. Sondaki eşitliği gösterelim.

$$\left\{ \begin{aligned} u(m d) &= u(\underbrace{d + d + \dots + d}_{m \text{-tane}}) = u d + u d + \dots + u d \\ &= (u + u + \dots + u) d = (m u) d \end{aligned} \right\}$$

$$\Rightarrow u \cdot \alpha = \sum_{i=1}^x \underbrace{(u r_i) a_i}_{\in A} + \sum_{i=1}^y \underbrace{u b_i s_i}_{\in A} + \sum_{i=1}^z \underbrace{(u k_i) c_i l_i}_{\in A} + \sum_{i=1}^t \underbrace{(m_i u) d_i}_{\in A}$$

$$\Rightarrow u \cdot \alpha \in A \text{ dir. Benzer şekilde } \alpha \cdot u \in A \text{ dir.}$$

O halde A idealdir.

Ters kapsanayı gösterelim.

$$\alpha = \sum r_i a_i + \sum b_i s_i + \sum k_i c_i l_i + \sum m_i d_i \text{ o.p. } a_i, b_i, c_i, d_i \in M, m_i \in \mathbb{Z}, r_i, s_i, k_i, l_i \in R, x, y, z, t \in \mathbb{N}.$$

$M \subset \langle M \rangle$ ve $\langle M \rangle$ de ideal olduğundan,

$$a_i \in M, r_i \in R; \sum_{i=1}^x \underline{r_i a_i} \in \langle M \rangle,$$

$$b_i \in M, s_i \in R; \sum_{i=1}^y \underline{b_i s_i} \in \langle M \rangle,$$

$$\sum_{i=1}^z \underline{k_i c_i l_i} \in \langle M \rangle, \quad \sum_{i=1}^t \underline{m_i d_i} \in \langle M \rangle$$

$$m > 0, m_i d_i = \underbrace{d_i + \dots + d_i}_{m \text{-tane}} \in \langle M \rangle$$

$$\Rightarrow \alpha \in \langle M \rangle \quad A \subset \langle M \rangle \text{ olur.}$$

$$0 \text{ halde } A = \langle M \rangle \text{ dir.} //$$

Sonuç 1: R değişmeli halka ise ;

$$\langle M \rangle = \left\{ \sum_{i=1}^k r_i a_i + \sum_{i=1}^m m_i d_i \mid a_i, d_i \in M, r_i \in R, k, t \in \mathbb{N}, m_i \in \mathbb{Z} \right\} \text{ dir.} //$$

$$\left\{ \begin{array}{l} \sum_{i=1}^y b_i s_i = \sum_{i=1}^y s_i b_i, \quad \sum_{i=1}^z k_i c_i l_i = \sum_{i=1}^z (k_i c_i) l_i = \sum_{i=1}^z k_i' c_i \\ \sum_{i=1}^x r_i a_i + \sum_{i=1}^y s_i b_i = \sum_{i=1}^{x+y} r_i'' a_i'' + \sum_{i=1}^y k_i' c_i = \sum_{i=1}^{x+y+z} r_i''' a_i''' \end{array} \right\}$$

Sonuç 2: R birimli halka ise ;

$$\left\{ \begin{array}{l} m a = m(1_R \cdot a) = (\underbrace{m}_r 1_R) a = r \cdot a, \quad a \in R, m \in \mathbb{Z} \\ \sum_{i=1}^t m_i d_i = \sum_{i=1}^t (\underbrace{m_i}_r 1_R) d_i = \sum_{i=1}^t r_i' d_i, \quad m_i \in \mathbb{Z}, d_i \in R, r_i' \in R \end{array} \right\}$$

$$\langle M \rangle = \left\{ \sum_{i=1}^x r_i a_i + \sum_{i=1}^y b_i s_i + \sum_{i=1}^z k_i c_i l_i \mid \begin{array}{l} x, y, z \in \mathbb{N} \\ a_i, b_i, c_i \in M \\ r_i, s_i, k_i, l_i \in R \end{array} \right\} \text{ dir.} //$$

Sonuç 3: R birimli ve değişmeli halka ise ;

$$\langle M \rangle = \left\{ \sum_{i=1}^n r_i a_i \mid a_i \in M, r_i \in R, n \in \mathbb{N} \right\} \text{ dir.} //$$

Örnek // $\mathbb{Z}$ de, $M = \{2, 5, 9, 285\}$ ise

$$\langle M \rangle = \{2x + 5y + 9z + 285t \mid x, y, z, t \in \mathbb{Z}\} \text{ dir.}$$

Örnek // $M = \{a\}$ ve R halka ise,

$$\langle a \rangle = \{r a + a s + k a l + m a \mid r, s, k, l \in R, m \in \mathbb{Z}\} \text{ olur.} //$$

$$\left\{ \sum_{i=1}^t r_i a = \left(\underbrace{\sum_{i=1}^t r_i}_r \right) a = r a \right\}$$

Örnek // $M = \{a\}$ ve R birimli halka ise, (ma kalkar.)

$$\langle a \rangle = \{r a + a s + k a l \mid r, s, k, l \in R\} \text{ olur.}$$

Örnek // $M = \{a\}$ ve R birimli, değişmeli halka ise,

$$\langle M \rangle = \langle a \rangle = \{r a \mid r \in R\} \text{ olur.}$$

Tanım: Eğer bir T.B. nin her ideali tek elemanla üretilmişse bu halkaya tek üreteçli ideal bölgesi (T.Ü.i.B) denir.

Örnek // $\mathbb{Z}$ bir T.Ü.i.B. dir. Gösterelim ;

$$I, \mathbb{Z} \text{ ideali olsun. } I = \{0\} \Rightarrow I = \langle 0 \rangle$$

$$I = \mathbb{Z} \Rightarrow I = \langle 1 \rangle$$

$$\{0\} \neq I \Rightarrow \exists 0 \neq a \in I \text{ dir. } I \text{ ideal olduğundan } -a \in I$$

$\Rightarrow I$ da birtakım pozitif tamsayılar vardır.

I 'da bulunan $\mathbb{Z}^+$ 'ların en küçüğü $k \in I$ olsun. k 'dan daha küçük $\mathbb{Z}^+$ yoktur. $k \in I$ olduğundan ,

$$\langle k \rangle \subset I \text{ dr. (üretme tanımından)}$$

$$\forall x \in I \text{ alalım. } x = qk + r, 0 \leq r < k \text{ o.s. } \exists q, r \in \mathbb{Z}.$$

$$x - qk = r \in I \text{ olur. } k, I \text{ daki en küçük } \mathbb{Z}^+ \text{ oldu.}$$

$(\in I) \leftarrow (\forall \in I)$

$$r = 0 \text{ olmalıdır.}$$

$$\Rightarrow x = qk \in \langle k \rangle \Rightarrow I \subset \langle k \rangle$$

$$0 \text{ halde } I = \langle k \rangle \text{ olur. } \Rightarrow \mathbb{Z}, \text{ T.Ü.i.B. dir. //}$$

Önerme // $M = \{a_1, a_2, \dots, a_n\} \subset \mathbb{Z}$ ve M , birimli ve değişmeli ve

$$\langle M \rangle = \left\{ \sum_{i=1}^n m_i a_i \mid m_i \in \mathbb{Z} \right\} = \langle d \rangle \text{ ise } d = \text{ebob}(a_1, a_2, \dots, a_n) \text{ dir.}$$

İspat // $\left\{ \begin{array}{l} M = \{-7, 3, 7, 12\} \Rightarrow \langle M \rangle = \langle 1 \rangle \text{ dir.} \\ \text{ebob}(-7, 3, 7, 12) = 1 \end{array} \right\}$

$\downarrow$
 $\mathbb{Z}$ nin kendisidir.

$$\langle M \rangle = \left\{ \sum_{i=1}^n m_i a_i \mid m_i \in \mathbb{Z} \right\} = \langle d \rangle \text{ (birimli, değişmeli olduğundan) o.s.}$$
$$d \in \mathbb{Z}^+. \quad k := \text{ebob}(a_1, a_2, \dots, a_n)$$

$$d = m_1 a_1 + m_2 a_2 + \dots + m_n a_n \text{ o.s. } \exists m_i \in \mathbb{Z}.$$

$$\Rightarrow k \mid d \text{ dir. } M \subset \langle d \rangle \text{ olduğundan } 1 \leq i \leq n \text{ için ,}$$

$$a_i \in \langle d \rangle \Rightarrow a_i = d t_i \text{ o.s. } \exists t_i \in \mathbb{Z}.$$

$$\Rightarrow d \mid a_i \quad \forall i \text{ için. } \therefore d, a_i \text{ lerin ortak bölenidir.}$$

$$\text{ebob tanımından } d \mid k \text{ ve buradan } d = k \text{ olur. //}$$

Önerme // $a_1, a_2, \dots, a_m \in \mathbb{Z}$ ve $d = \text{ekok}(a_1, a_2, \dots, a_m)$ ise

$$\bigcap_{i=1}^m \langle a_i \rangle = \langle d \rangle$$

dir.

İspat // İdeallerin arakesiti de ideal ve $\mathbb{Z}$ deki her ideal de, tek üreteçli ideal olduğundan $\bigcap_{i=1}^m \langle a_i \rangle = \langle d \rangle$ o.ş. $\exists d \in \mathbb{Z}$.

$$\Rightarrow d \in \langle a_i \rangle, \quad 1 \leq i \leq m \text{ için}$$

$$\Rightarrow d = a_i t_i \text{ o.ş. } \exists t_i \in \mathbb{Z}. \quad \therefore d, a_i \text{ lerin ortak katıdır.}$$

k, a_i lerin başka bir katı olsun.

$$\Rightarrow k = a_i x_i \text{ o.ş. } \exists x_i \in \mathbb{Z}. \quad \forall 1 \leq i \leq m.$$

$$\Rightarrow k \in \langle a_i \rangle, \quad \forall 1 \leq i \leq m.$$

$$\Rightarrow k \in \bigcap_{i=1}^m \langle a_i \rangle = \langle d \rangle \Rightarrow k = d x \text{ o.ş. } \exists x \in \mathbb{Z}.$$

$$\Rightarrow d | k \text{ dir. (ekok tanımından)}$$

$$\Rightarrow d = \text{ekok}(a_1, a_2, \dots, a_m) \text{ olur. //}$$

Tanım: I ve J , R halkasının iki ideali olsun.

$$I+J := \{a+b \mid a \in I, b \in J\} \quad (\text{Çözümü: 138-18})$$

ye, I ve J ideallerinin toplamı denir.

- $I+J$ kümesi de idealdir, gösterelim.

$$(i-) \quad \forall (a_1+b_1), (a_2+b_2) \in I+J, \quad (a_1, a_2 \in I, \quad b_1, b_2 \in J)$$

$$(a_1+b_1) - (a_2+b_2) = \underbrace{(a_1-a_2)}_{\in I} + \underbrace{(b_1-b_2)}_{\in J} \in I+J$$

$$(ii-) \quad \forall r \in R, \quad r(a_1+b_1) = \underbrace{ra_1}_{\in I} + \underbrace{rb_1}_{\in J} \in I+J$$

$$(a_1+b_1)r = \underbrace{a_1r}_{\in I} + \underbrace{b_1r}_{\in J} \in I+J \quad \Rightarrow I+J \text{ idealdir. //}$$

Tanım: I ve J , R halkasının iki ideali olsun.

$$I \cdot J = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N} \right\}$$

ye, I ve J ideallerinin çarpımı denir.

- $I \cdot J$ kümesi de idealdir, gösterelim.

I ve J ideal olduğundan $I, J \neq \emptyset$ ve $\exists x \in I, \exists y \in J$,

$$xy = \sum_{i=1}^1 xy \in IJ$$

$\forall \alpha, \beta \in IJ$ alalım. $\alpha = \sum_{i=1}^t a_i b_i, \beta = \sum_{i=1}^m a_i' b_i'$

o.ş. $\exists t, m \in \mathbb{N}, \exists a_i, a_i' \in I, \exists b_i, b_i' \in J$.

$$\textcircled{i} - \alpha - \beta = \alpha + (-\beta) = \sum_{i=1}^t a_i b_i + \sum_{i=1}^m (-a_i') b_i' \quad \left\{ \begin{array}{l} -\beta = \sum_{i=1}^m (-a_i') b_i' \\ = \sum_{i=1}^m c_i b_i' \end{array} \right.$$

$$\alpha - \beta = a_1 b_1 + \dots + t a_t b_t + c_1 b_1' + \dots + m c_m b_m'$$

$$= \sum_{i=1}^{t+m} x_i y_i \quad \begin{array}{l} 1 \leq i \leq t, \quad x_i = a_i \\ 1 \leq i \leq t+m, \quad x_i = c_i \end{array}$$

$$\Rightarrow \alpha - \beta \in IJ$$

$\textcircled{ii} - \forall \alpha \in IJ, \forall r \in R$ için,

$$\alpha \cdot r = \left(\sum_{i=1}^t a_i b_i \right) r = \sum_{i=1}^t a_i (b_i r) \in IJ$$

$$r \alpha = r \left(\sum_{i=1}^t a_i b_i \right) = \sum_{i=1}^t (r a_i) b_i \in IJ$$

0 halde IJ kümesi de idealdir. //

minet

Önerme // $a_1, a_2, \dots, a_n \in \mathbb{Z}$ ve $\text{ebob}(a_1, a_2, \dots, a_n) = k$ olsun.

$\langle a_1 \rangle + \langle a_2 \rangle + \dots + \langle a_n \rangle = \langle k \rangle$ dır. (Çözümü: 139-19)

İspatı, soru şekline çevirerek yapalım.

Soru // $\langle a_1 \rangle + \langle a_2 \rangle + \dots + \langle a_n \rangle = \langle d \rangle \Rightarrow d = ?$

Çözüm // $\langle a_1 \rangle + \langle a_2 \rangle + \dots + \langle a_n \rangle = \langle d \rangle$ o.ş. $\exists d \in \mathbb{Z}$.

$\forall 1 \leq i \leq n$ için $\langle a_i \rangle \subseteq \langle d \rangle$ dir.

$$\Rightarrow a_i \in \langle d \rangle \Rightarrow a_i = d t_i \text{ o.ş. } \exists t_i \in \mathbb{Z}.$$

$\Rightarrow \forall i$ için $d | a_i \therefore d, a_i$ lerin ortak bölenidir.

Kabul edelim ki, $k := \text{ebob}(a_1, a_2, \dots, a_n)$ olsun.

$$\Rightarrow d | k \text{ (ebob tanımından)}$$

$\langle a_i \rangle \subseteq \langle d \rangle$ den, $d \in \langle a_1 \rangle + \langle a_2 \rangle + \dots + \langle a_n \rangle$

$$\Rightarrow d = a_1 m_1 + \dots + a_n m_n \text{ o.ş. } m_i \in \mathbb{Z}, 1 \leq i \leq n.$$

minet

$$\Rightarrow k \mid a_1 m_1 + \dots + a_n m_n = d$$

0 halde $k=d=\text{Ebob}(a_1, a_2, \dots, a_n)$ dir. //

BÖLÜM HALKASI

15.4.1996 / P.tesi

I, R halkasının bir ideali olsun. $(I, +) \triangleleft (R, +)$ dir.

$\forall a, b \in R$ için $a \equiv b \pmod{I} \Leftrightarrow a - b \in I$

$$\bar{a} = a + I = \{a + r \mid r \in I\}, \quad R/I = \{a + I \mid a \in R\}$$

$$\bullet (a+I) \oplus (b+I) := (a+b) + I$$

R değişmeli olduğundan, R/I da değişmelidir.

{Gruplarda; $N \triangleleft G, G/N$; G değişmeli $\Rightarrow G/N$ de değişmelidir.}

$$\bullet (a+I) \odot (b+I) := (ab) + I$$

I ideal olursa, verilen bağıntılar işlem olur.

(işlem olması için, 'kapalılık, ve 'tek türlü yazım, gereklidir.)

Birleşme ve dağılma özellikleri, R deki işlemlerden ortaya çıkar.

Verilen bağıntının işlem olduğunu gösterelim:

$$\left. \begin{array}{l} a+I = a'+I \\ b+I = b'+I \end{array} \right\} \Rightarrow \left. \begin{array}{l} a-a' \in I \\ b-b' \in I \end{array} \right\} \Rightarrow \left. \begin{array}{l} a-a' = x \\ b-b' = y \end{array} \right\} \text{ö.s. } \exists x, y \in I.$$

$$\Rightarrow \left. \begin{array}{l} a = x + a' \\ b = y + b' \end{array} \right\} \Rightarrow ab = (x+a')(y+b') = xy + xb' + a'y + a'b'$$

$$\Rightarrow ab - a'b' = \underbrace{xy}_{\in I} + \underbrace{xb'}_{\in I} + \underbrace{a'y}_{\in I} \in I$$

$$\Rightarrow ab \equiv a'b' \pmod{I}$$

$$\Rightarrow (ab) + I = (a'b') + I \quad 0 \text{ halde işlem olur.}$$

Birleşme özelliğini gösterelim:

$$(a+I) \odot [(b+I) \odot (c+I)] = (a+I) \odot [(bc) + I]$$

$$= [a(bc)] + I$$

$$= [(ab)c] + I$$

$$= [(ab+I) \odot (c+I)]$$

$$= [(a+I) \odot (b+I)] \odot (c+I) //$$

sağ ve soldan dağılma özellikleri de vardır.

Örnek,, $\mathbb{Z}$ de, $I = \langle 5 \rangle \Rightarrow \mathbb{Z}/I = ?$

$$\forall n \in \mathbb{Z}, n = 5q + r, 0 \leq r < 5 \text{ o.s. } \exists q, r \in \mathbb{Z}.$$

$$n - r = 5q \in I \Rightarrow n + I = r + I$$

$$r = 0, 1, 2, 3, 4$$

$$\{I, 1+I, 2+I, 3+I, 4+I\} \quad (\text{Bu aralıkta başka sayı yoktur.})$$

$$r_1 \neq r_2, r_1, r_2 \in \mathbb{Z} \text{ için } (0 \leq r_1, r_2 < 5) \quad r_1 + I \neq r_2 + I$$

$$\Rightarrow r_1 - r_2 = 5k \text{ o.s. } \exists k \in \mathbb{Z} \text{ yoktur.}$$

$$0 \text{ halde, } \mathbb{Z}/I = \mathbb{Z}/\langle 5 \rangle = \{ \langle 5 \rangle, 1+\langle 5 \rangle, 2+\langle 5 \rangle, 3+\langle 5 \rangle, 4+\langle 5 \rangle \} //$$

nerme,, I, R nin bir ideali ve S, R 'nin I 'yı kapsayan bir alt halkası ise S/I da R/I nin bir alt halkasıdır.

Tersine, R/I nin her alt halkası J, R 'nin I 'yı kapsayan bir alt halkası olmak üzere K/I şeklindedir. Yani;

$$\forall J \subset R/I \text{ alt halkası için } J = K/I \text{ o.s. } I \subset K \subset R \text{ alt halkası vardır.}$$

$$\text{spat,, } I \subset S \subset R \quad \left\{ \begin{array}{l} S/I = \{s+I \mid s \in S\} \\ 0 \in S \Rightarrow 0+I = I \in S/I, S/I \neq \emptyset \end{array} \right\}$$

$$\forall s_1 + I, s_2 + I \in S/I, (s_1, s_2 \in S)$$

$$(s_1 + I) \oplus (s_2 + I) = (s_1 + I) \oplus (-s_2 + I)$$

$$= (s_1 - s_2) + I \in S/I$$

alt halka özelliklerini gösteriyoruz.

$$(s_1 + I) \odot (s_2 + I) = (\underbrace{s_1 s_2}_{\in S}) + I \in S/I$$

$$\Rightarrow S/I, R/I \text{ nin alt halkasıdır.}$$

Tersine, $J \subset R/I$ alt halka olsun.

$$K := \{r \in R \mid r + I \in J\}$$

$\left\{ \begin{array}{l} K \text{ kümesi, denklik sınıfları } J' \text{ de} \\ \text{kalan elemanlardan oluşmuştur.} \end{array} \right\}$

$\forall x \in I$ için, $x + I = I$ ve $J, R/I$ alt halka olduğundan

$$x + I = I \in J \Rightarrow x \in K \therefore I \subset K.$$

K nin alt halka olduğunu gösterelim.

$I \neq \emptyset$ olduğundan $K \neq \emptyset$ olur. $\forall x, y \in K$ alalım.

$\Rightarrow x+I, y+I \in J$ dir.

J ideal olduğundan; $(x+I) - (y+I) = (x-y) + I \in J$

$\Rightarrow x-y \in K$. ve

$(xy) + I = (x+I) \odot (y+I) \in J$

$\Rightarrow xy \in K$

$\Rightarrow K$ alt halkadır.

K 'nin tanımından $K/I = J$ olur. //

Tanım: $(R/I, \oplus, \odot)$ yapısı bir halkadır. Buna, R nin I idealine göre bölüm halkası denir.

134-4 $d \in \mathbb{Z}$, d kare çarpansız olsun.

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

nun bir cisim olduğunu gösterin.

Çözüm, $d > 0 \Rightarrow \mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$ alt halkasıdır. $d < 0 \Rightarrow \mathbb{Q}[\sqrt{d}] \subset \mathbb{C}$ alt halkasıdır. } birimli, değişmeli.

$\mathbb{R}$ ve $\mathbb{C}$ de sıfır bölen eleman olmadığından $\mathbb{Q}[\sqrt{d}]$ alt halkasında da sıfır bölen yoktur. O halde sıfırdan farklı her elemanın tersinin olduğunu gösterirsek verilen kümenin bir cisim olduğunu göstermiş oluruz.

$\forall 0 \neq a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ nin ikinci işleme göre tersi:

$$(a + b\sqrt{d})^{-1} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - db^2} = \frac{a}{a^2 - db^2} - \frac{b\sqrt{d}}{a^2 - db^2} \in \mathbb{Q}[\sqrt{d}]$$

$(a^2 - db^2 \neq 0)$ bulunur.

O halde $(\mathbb{Q}[\sqrt{d}], +)$ değişmeli grup, $(\mathbb{Q}^*[\sqrt{d}], \cdot)$ değişmeli grup olduğundan $(\mathbb{Q}[\sqrt{d}], +, \cdot)$ yapısı bir cisimdir. //

Tanım: $f: R \rightarrow S$ bir fonksiyon ve R, S iki halka olsun. Eğer,

$$\forall x, y \in R \text{ için, } f(x+y) = f(x) + f(y)$$

$$f(xy) = f(x)f(y)$$

özellikleri sağlanıyorsa f 'ye halka homomorfizması denir.

$f, 1:1$ homomorfizma ise f 'ye monomorfizma,

f , örten homomorfizma ise f 'ye epimorfizma,

$f, 1:1$ ve örten homomorfizma ise f 'ye izomorfizma ($R \cong S$) denir.

Önerme // $f: R \rightarrow S$ halka homomorfizması olsun.

i - $f(0_R) = 0_S$.

ii - $\forall a \in R, f(-a) = -f(a)$.

$$\left\{ \begin{array}{l} \text{Grup hom.'da } f(e_R) = e_S \\ f(a^{-1}) = f(a)^{-1} \text{ idi.} \end{array} \right\}$$

iii - R nin her U alt halkasının görüntüsü $f(U)$ 'da, S nin alt halkasıdır.

iv - $\forall K \subset S$ (alt halka) için $f^{-1}(K) \subset R$ alt halkadır.

v - $\forall J \subset S$ ideali için $f^{-1}(J) \subset R$ nin idealidir.

f aynı zamanda örten olsun.

vi - $\forall I \subset R$ için $f(I) \subset S$ idealidir.

vii - R değişmeli ise S 'de değişmelidir.

viii - R birimli ise S 'de birimlidir. ($1_R \in R \Rightarrow f(1_R) = 1_S$)

İspat // $f: R \rightarrow S$ halka homomorfizması olsun.

i - $0_R = 0_R + 0_R \Rightarrow f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$

$$\Rightarrow 0_S = f(0_R) //$$

ii - $0_S = f(0_R) = f(a - a) = f(a + (-a))$

$$\Rightarrow 0_S = f(a) + f(-a)$$

$$\Rightarrow -f(a) = f(-a) //$$

iii - $f(U) = \{s \in S \mid f(u) = s \text{ o.y. } \exists u \in U\}$

$$= \{f(x) \mid x \in U\}$$

i. den dolayı $f(U) \neq \emptyset$ olur.

$\forall a, b \in f(U)$ için, $a = f(x), b = f(y)$ o.s. $\exists x, y \in U$.

$$a - b = f(x) - f(y) = \underbrace{f(x-y)}_{\in U} \in f(U)$$

$$ab = f(x)f(y) = \underbrace{f(xy)}_{\in U} \in f(U)$$

$\Rightarrow f(U)$ alt halkadır. //

iv - $f^{-1}(K) = \{a \in R \mid f(a) \in K\}$

K alt halka $\Rightarrow 0_S \in K$.

$$f(0_R) = 0_S \in K \Rightarrow 0_R \in f^{-1}(K), \quad f^{-1}(K) \neq \emptyset \text{ olur.}$$

$$\forall x, y \in f^{-1}(K) \Rightarrow f(x), f(y) \in K$$

$$f(x-y) = f(x) - f(y) \in K \Rightarrow x-y \in f^{-1}(K)$$

$$f(xy) = f(x)f(y) \in K \Rightarrow xy \in f^{-1}(K)$$

$\{x \mid P(x)\}$, P özelliğini sağlayan x lerin kümesi

$\Rightarrow f^{-1}(K)$ alt halkadır. //

v - $J \subset S, f^{-1}(J) \subset R$

$$\forall x, y \in f^{-1}(J) \text{ için, } f(x), f(y) \in J$$

$$f(x-y) = f(x) - f(y) \in J \Rightarrow x-y \in f^{-1}(J)$$

$$\forall x \in f^{-1}(J) \text{ ve } f(x) \in J, r \in R \text{ için,}$$

$$\underbrace{f(rx)}_{\in J} = \underbrace{f(r)}_{\in J} \underbrace{f(x)}_{\in J} \in J \Rightarrow rx \in f^{-1}(J)$$

$$\underbrace{f(xr)}_{\in J} = \underbrace{f(x)}_{\in J} \underbrace{f(r)}_{\in J} \in J \Rightarrow xr \in f^{-1}(J)$$

$f^{-1}(J)$ idealdir. //

vi - $0_R \in I \Rightarrow 0_S = f(0_R) \in f(I) \Rightarrow f(I) \neq \emptyset$ olur.

$$\forall x, y \in f(I) \text{ alalım. } \Rightarrow x = f(a), y = f(b) \text{ o.s. } \exists a, b \in I.$$

I ideal olduğundan, $a - b \in I$ dir.

$$\Rightarrow x - y = f(a) - f(b) = f(a - b) \in f(I) \text{ olur.}$$

$$\forall x = f(a) \in f(I) \quad (a \in I) \text{ ve } \forall s \in S \text{ için,}$$

f örten olduğundan $s = f(r)$ o.s. $\exists b \in R$.

$$sx, xs \in f(I) \quad ?$$

$$sx = f(r)f(a) = \underbrace{f(ra)}_{\in I} \in f(I), \quad xs = f(a)f(r) = \underbrace{f(ar)}_{\in I} \in f(I)$$

$\Rightarrow f(I)$ idealdir. //

vii - $\forall x, y \in S$ için f örten $\Rightarrow x = f(a), y = f(b)$ o.s. $\exists a, b \in R$.

R değişmeli ise $ab = ba$ ve buradan,

$$xy = f(a)f(b) = \underbrace{f(ab)}_{R \text{ def. old.}} = f(ba) = f(b)f(a) = yx$$

$\Rightarrow S$ değişmeli olur. //

viii - $\forall x \in S, f$ örten $\Rightarrow x = f(a)$ o.s. $\exists a \in R$. (R birimli)

$$a = a \cdot 1_R = 1_R \cdot a \Rightarrow x = f(a) = f(a \cdot 1_R) = f(a)f(1_R) = x \cdot f(1_R)$$

$$x = f(a) = f(1_R \cdot a) = f(1_R) \cdot f(a) = f(1_R) \cdot x$$

$$\Rightarrow \forall x \in S, x = x \cdot f(1_R) = f(1_R) \cdot x \Rightarrow f(1_R) = 1_S$$

$\Rightarrow S$ de birimlidir. //

137/15 - $1_R \in R$ olsun.

$\forall 0_R \neq a \in R, a^{-1} \in R \Leftrightarrow R$ nin öz sol ideali yoktur.

$\Rightarrow \{0_R\} \neq I \subset R$ nin sol ideali olsun.

$\Rightarrow \exists 0 \neq a \in I$ hipotezden, $a^{-1} \in I$.

$$1_R = a^{-1}a \in I \Rightarrow I = R$$

$\Leftarrow \forall 0 \neq a \in R$ alalım.

$$\forall r_1 a, r_2 a \in Ra \text{ için, } r_1 a - r_2 a = \overbrace{(r_1 - r_2)}^{ER} a \in Ra$$

$$\forall s \in R, \forall r \in Ra \text{ için, } s(ra) = \underbrace{(sr)}_{ER} a \in Ra$$

$\{0\} \neq Ra$ hipotezden $Ra = R$ ve $1_R \in R$ olduğundan

$$1_R \in Ra \Rightarrow 1_R = ra \text{ o.s. } \exists r \in R.$$

$$1_R = ar \text{ o.s. } \exists r \in R.$$

$\Rightarrow r = a^{-1} \in R$ dir. //

Tanım : $f: R \rightarrow S$ homomorfizma olsun.

$$\ker f := \{a \in R \mid f(a) = 0_S\} = f^{-1}(0_S)$$

dir.

Teorem : (Homomorfizma Teoremi) :

$f: R \rightarrow S$ halka homomorfizması olsun.

i- $\ker f$, R nin idealidir.

ii- I , R nin herhangi ideali ise $\varphi: R \rightarrow R/I$ epimorfizmadır.
 $r \mapsto r+I$

iii- $R/\ker f \cong f(R)$ dir.

İspat // i- $\ker f = \{a \in R \mid f(a) = 0_S\}$, R nin idealidir. Gösterelim.

$$\bullet f(0_R) = 0_S \Rightarrow 0_R \in \ker f \Rightarrow \ker f \neq \emptyset \text{ olur.}$$

$$\bullet \forall a, b \in \ker f \Rightarrow f(a) = 0_S = f(b)$$

$$f(a-b) = f(a+(-b)) = f(a) + f(-b) = f(a) - f(b) = 0_S - 0_S = 0_S$$

$$\Rightarrow a-b \in \ker f.$$

$$\forall a \in \ker f, \forall r \in R,$$

$$f(ar) = f(a)f(r) = 0_S f(r) = 0_S \Rightarrow ar \in \ker f$$

$$f(ra) = f(r)f(a) = f(r)0_S = 0_S \Rightarrow ra \in \ker f.$$

$$\Rightarrow \ker f, R \text{ nin idealidir. //}$$

$$\text{ii- } \varphi: R \rightarrow R/I$$

$$r \mapsto r+I$$

$$\varphi \text{ örtendir. } r_1+I = r_2+I \text{ dir. } (\forall r_1, r_2 \in R \text{ için})$$

$$\varphi(r_1+r_2) = (r_1+r_2)+I = (r_1+I) \oplus (r_2+I) = \varphi(r_1) \oplus \varphi(r_2)$$

$$\varphi(r_1 \cdot r_2) = (r_1 r_2)+I = (r_1+I) \odot (r_2+I) = \varphi(r_1) \odot \varphi(r_2)$$

$$\Rightarrow \varphi \text{ örtten homomorfizma yani epimorfizmadır. //}$$

$$\text{iii- } \bar{f}: R/\ker f \rightarrow S$$

$$r+\ker f \mapsto \bar{f}(r+\ker f) := f(r) \text{ tanımlayalım.}$$

$$\bullet r+\ker f = r'+\ker f \Rightarrow r-r' \in \ker f \Rightarrow f(r-r') = 0_S$$

$$\Rightarrow f(r) - f(r') = 0_S \Rightarrow f(r) = f(r')$$

$$\Rightarrow \bar{f}(r+\ker f) = \bar{f}(r'+\ker f) \text{ iyi tanımlıdır. //}$$

$$\bullet \bar{f}(r+\ker f) = \bar{f}(r'+\ker f) \Rightarrow f(r) = f(r') \Rightarrow f(r) - f(r') = 0_S$$

$$\Rightarrow f(r-r') = 0_S \Rightarrow r-r' \in \ker f \text{ - ii}$$

$$\Rightarrow r+\ker f = r'+\ker f, f \text{ 1:1 dir. //}$$

$$\bullet \bar{f}[(r+sekf) \oplus (r'+sekf)] = \bar{f}[(r+r') + sekf]$$

$$= f(r+r')$$

$$= f(r) + f(r')$$

$$= \bar{f}(r+sekf) + \bar{f}(r'+sekf)$$

ve,

$$\bar{f}[(r+sekf) \odot (r'+sekf)] = \bar{f}[(r \cdot r') + sekf]$$

$$= f(rr')$$

$$= f(r)f(r')$$

$$= \bar{f}(r+sekf) \cdot \bar{f}(r'+sekf)$$

$\Rightarrow \bar{f}$ homomorfizmadır.

$$\bullet \bar{f}: R/sekf \longrightarrow f(R) \subset S \quad \bar{f} \text{ örten dir.}$$

f örten $\Rightarrow f(R) = S$ olur. $\Rightarrow R/sekf \cong f(R)$ dir.

Teorem: (1. İzomorfizma Teoremi):

S, R nin bir alt halkası ve I, R nin bir ideali olsun.

i- $S+I = \{s+a \mid s \in S, a \in I\}$ kümesi R nin I yı kapsayan alt halkasıdır.

ii- $(S+I)/I \cong S/(S \cap I)$ dir.

İspat // i- $\forall x \in I, x = 0_R + x \in S+I \Rightarrow I \subset S+I$

I ideal olduğundan $I \neq \emptyset$ ve üst küme de, $S+I \neq \emptyset$ olur.

$$\bullet \forall \underbrace{s_1+a_1}_{\in S+I}, \underbrace{s_2+a_2}_{\in S+I} \in S+I \text{ için,}$$

$$(s_1+a_1) - (s_2+a_2) = (s_1-s_2) + (a_1-a_2) \in S+I$$

$$(s_1+a_1) \cdot (s_2+a_2) = \underbrace{s_1 s_2}_{\in S} + \underbrace{s_1 a_2}_{\in I} + \underbrace{a_1 s_2}_{\in I} + \underbrace{a_1 a_2}_{\in I} \in S+I$$

$\Rightarrow S+I$ alt halkadır.

ii- $(S \cap I) \subset S$ ve $S \cap I, S$ nin idealidir.)

$$f: S \longrightarrow (S+I)/I$$

$$x \longrightarrow f(x) := x+I = \underbrace{(x+0)}_{\in S} + \underbrace{0}_{\in I} \in (S+I)/I$$

f iyi tanımlıdır. (Tek türlü yazılır.)

$$\bullet \forall x, y \in S, f(x+y) = (x+y) + I = (x+I) \oplus (y+I)$$

$$f(xy) = (xy) + I = (x+I) \odot (y+I)$$

$\Rightarrow f$ homomorfizmadır. //

$$\bullet \forall (x+I) + I \in (S+I)/I \text{ için } (x \in S, I \in I)$$

$$(x+I) + I = (x+I) \oplus (I) = x+I \text{ olduğundan } x \in S.$$

$$f(x) = x+I = (x+I) + I \quad \therefore f \text{ örtendir.}$$

$$\bullet x \in S \text{ için, } x \in \ker f \Leftrightarrow f(x) = x+I = I \Leftrightarrow x \in I$$

$$\Leftrightarrow x \in S \cap I \quad \therefore \ker f = S \cap I //$$

• Homomorfizma teoremi 3. özellikten,

$$S/(S \cap I) \cong (S+I)/I \text{ dir. //$$

24.4.96 / Çarşamba

Teorem: (2. izomorfizma Teoremi) :

$f: R \rightarrow S$ epimorfizma ve $\ker f =: K$ olsun. S 'nin idealleri

ile R 'nin K 'yı kapsayan idealleri arasında 1:1 eşleme

yapılabilir. Yani $I \subset S$ ideali ile $J := f^{-1}(I) = \{x \in R \mid f(x) \in I\}$

R 'nin I 'yı kapsayan bir idealidir. ve $R/J \cong S/I$ dir.

İspat // I , S 'nin bir ideali olduğu için $0_S \in I$ dir. Ve

$\forall x \in K = \ker f$ için $f(x) = 0_S$ olduğundan

$x \in J \Rightarrow K \subset S$ dir. $K \neq \emptyset$, $J \neq \emptyset$ olur.

$\forall x, y \in J$ alalım. $\Rightarrow f(x), f(y) \in I$ ve I ideal olduğundan

$f(x) - f(y) \in I$ ($f(x-y) = f(x) - f(y)$) homomorfizma olduğundan.

$\Rightarrow x-y \in J$.

Şimdi $R/J \cong S/I$ olduğunu gösterelim.

$$\varphi: R \rightarrow S/I$$

$$x \mapsto f(x) + I$$

$$x_1 = x_2 \Rightarrow f(x_1) = f(x_2) \Rightarrow f(x_1) + I = f(x_2) + I \Rightarrow \varphi(x_1) = \varphi(x_2)$$

$\Rightarrow \varphi$ iyi tanımlıdır.

- $\varphi(x_1 + x_2) = f(x_1 + x_2) + I = (f(x_1) + f(x_2)) + I$
 $= (f(x_1) + I) + (f(x_2) + I)$
 $= \varphi(x_1) + \varphi(x_2) \Rightarrow \varphi$ homomorfizmadır.
- $\forall s + I \in S/I$ için $s \in S$ ve f örten olduğundan $f(x) = s$ o.ş. $\exists x \in R$.
 $\Rightarrow \varphi(x) = f(x) + I = s + I \quad \therefore \varphi$ örtendir.
- $x \in \ker \varphi \Leftrightarrow \varphi(x) = f(x) + I = I \Leftrightarrow f(x) \in I \Leftrightarrow x \in f^{-1}(I) = J$
 $\ker \varphi = J$ dir. //

oru // $f: R \rightarrow S$ epimorfizma ve $I \subset R$ ideali $I = \langle a \rangle$ $a \in R$ olsun.
 $f(I)$, S 'nin tek üreteçli idealidir.

özüm // $a \in I \Rightarrow f(a) \in f(I) \Rightarrow \langle f(a) \rangle \subset f(I)$

$\forall x \in f(I)$ alalım $\Rightarrow x = f(r)$ o.ş. $\exists r \in I = \langle a \rangle$

$\Rightarrow r = ka + al + ma$ o.ş. $\exists k, l \in R, m \in R$.

$\Rightarrow x = f(r) = f(ka + al + ma)$

$\Rightarrow f(k)f(a) + f(a)f(l) + m f(a) \in \langle f(a) \rangle$

$D, T.R.$ olsun. $D^* := D - \{0_D\}$

$D \times D^*$ kümesi üzerinde bir " $\sim$ " bağıntısını aşağıdaki şekilde tanımlayalım:

$$(a, b) \sim (c, d) \iff ad = bc$$

" $\sim$ ", $D \times D^*$ üzerinde bir denklik bağıntısıdır. Denklik sınıfları:

$$\frac{a}{b} := (a, b)$$

olur. Denklik sınıflarının kümesi ise;

$$F := \left\{ \frac{a}{b} \mid a, b \in D, b \neq 0 \right\}$$

dir. Bu F kümesi üzerinde iki işlem tanımlayalım.

$$\forall \frac{a}{b}, \frac{c}{d} \in F, \quad \frac{a}{b} \oplus \frac{c}{d} := \frac{ad+bc}{bd}, \quad \frac{a}{b} \odot \frac{c}{d} := \frac{ac}{bd}$$

$$\left. \begin{array}{l} \frac{a}{b} = \frac{a'}{b'} \\ \frac{c}{d} = \frac{c'}{d'} \end{array} \right\} \Rightarrow \left. \begin{array}{l} ab' = ba' \\ cd' = dc' \end{array} \right\} \Rightarrow (ab')(c'd) = (cd')(ba')$$

$$\Rightarrow a'c'bd = b'd'ac \Rightarrow \frac{a'c'}{b'd'} = \frac{ac}{bd}$$

$$\frac{a'd' + b'c'}{b'd'} \stackrel{?}{=} \frac{ad+bc}{bd}$$

$$\Leftrightarrow (a'd' + b'c')bd = (ad+bc)b'd'$$

$$\Leftrightarrow (a'b)dd' + (c'd)bb' = (ab')dd' + (cd')bb'$$

$$ab' = ba' \Rightarrow (ab')dd' = (a'b)dd'$$

$$cd' = c'd \Rightarrow (cd')bb' = (c'd)bb'$$

Ödev // $(F, \oplus, \odot)$

i- $0_F = \frac{0}{1} = (\overline{0}, 1) = (\overline{0}, x)$

ii- $1_F = (\overline{1}, 1) = \frac{1}{1} = (\overline{x}, x) = \frac{x}{x}$

iii- $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$

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

v- $-(a, b) = (\overline{-a}, b) = (\overline{a}, -b)$

} birim elemanlarını bul.

Çözüm // $i - (F, \oplus, \odot)$, $\oplus$ işleminin etkisiz elemanı;

$$\forall \frac{a}{b} \in F, \frac{a}{b} \oplus \frac{x}{y} = \frac{a}{b} \Rightarrow \frac{ay+bx}{by} = \frac{a}{b}$$

$$\Rightarrow aby+bbx = aby \Rightarrow bbx = 0 \Rightarrow b \neq 0 \Rightarrow bb \neq 0, x=0$$

$$\Rightarrow 0_F = (\overline{0}, y), y \in D^*$$

Tanım: Bu şekilde oluşturulan F cisminin D nin kesir cismi denir.

$$\begin{aligned} \mathcal{Q}: D &\longrightarrow F \\ a &\longrightarrow \frac{a}{1} \end{aligned} \quad (\text{halka hom.})$$

$$\bullet a=b \Rightarrow a.1=b.1 \Rightarrow (a,1) \sim (b,1) \Rightarrow (\overline{a},1) = (\overline{b},1) \therefore \mathcal{Q} \text{ iyi tanımlı.}$$

$$\bullet \mathcal{Q}(x+y) = \frac{x+y}{1} = \frac{x}{1} \oplus \frac{y}{1} = \mathcal{Q}(x) \oplus \mathcal{Q}(y) \therefore \mathcal{Q} \text{ homomorfizmadır.}$$

$$\bullet \mathcal{Q}(x) = \mathcal{Q}(y) \Rightarrow \frac{x}{1} = \frac{y}{1} \Rightarrow x=y \therefore \mathcal{Q} \text{ 1:1 dir.}$$

$$\Rightarrow D \cong \mathcal{Q}(D) \subset F \text{ dir. //}$$

Teorem: K, D 'yi kapsayan bir cisim ise F, K nin bir alt cismine izomorftur. ($D, T.B$ ve F, D nin kesir cismi olsun.)

spat // $\begin{aligned} \psi: F &\longrightarrow K \\ \frac{a}{b} &\longrightarrow \psi\left(\frac{a}{b}\right) = ab^{-1} \end{aligned} \quad \begin{aligned} a, b \in D \subset K \quad (K \text{ cisim old.}) \\ b^{-1} \in K, ab^{-1} \in K \end{aligned}$

$$\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = ba'$$

$$a, a', b, b' \in D \subset K \Rightarrow b'^{-1}, b^{-1} \in K \text{ olduğundan}$$

$$\bullet ab = ba' \Rightarrow ab^{-1} = a'b'^{-1} \Rightarrow \psi\left(\frac{a}{b}\right) = \psi\left(\frac{a'}{b'}\right) \therefore \psi \text{ iyi tanımlı.}$$

$$\bullet \psi\left(\frac{x}{y}\right) = \psi\left(\frac{a}{b}\right) \Rightarrow xy^{-1} = ab^{-1}$$

$$\Rightarrow xb = ay$$

$$\Rightarrow (x, y) \sim (a, b)$$

$$\Rightarrow \frac{x}{y} = \frac{a}{b} \therefore \psi \text{ 1:1 dir.}$$

$\bullet \psi$ homomorfizma olduğundan bir monomorfizmadır.

$$\Rightarrow F \cong \psi(F) \subset K$$

$\begin{cases} \mathbb{Z} \subset K \subset \mathbb{Q} \\ \text{tamsayılar ile rasyonel sayılar} \\ \text{arasında hiçbir sayı yoktur.} \end{cases}$

Polinom Halkaları

Tanım: R bir halka ve X bir değişken olsun. $a_0, a_1, \dots, a_k \in R$ olmak

üzere, $a_0 + a_1 X + a_2 X^2 + \dots + a_k X^k$

şeklindeki ifadeye R den katsayılı bir polinom denir.

R den katsayılı polinomların kümesi ;

$$R[X] := \{a_0 + a_1 X + a_2 X^2 + \dots + a_k X^k \mid a_i \in R, k \in \mathbb{N}\}$$

ile gösterilir.

$a, b, c, d \in R$ için

$$a + bX^3 + cX^5 = a + 0_R X + 0_R X^2 + bX^3 + 0_R X^4 + cX^5 \text{ dir.}$$

$$\left\{ \begin{array}{l} \exists X \Rightarrow \text{bir ifadedir.} \\ \exists X=6 \Rightarrow \text{bir denklendir.} \end{array} \right\}$$

Tanım: $P(X) := a_0 + a_1 X + a_2 X^2 + \dots + a_k X^k$

$Q(X) := b_0 + b_1 X + b_2 X^2 + \dots + b_m X^m$ olmak üzere,

$$P(X) = Q(X) \stackrel{tn}{\iff} k=m \text{ ve } a_i = b_i, 0 \leq i \leq k \text{ (} k \leq m \text{) dir.}$$

$a_k \neq 0 \Rightarrow a_k$ ya polinomun başkatsayısı denir. k 'ya da

polinomun derecesi denir. $d^o P := k$ ile gösterilir.

$$P(X) + Q(X) := (a_0 + b_0) + (a_1 + b_1)X + \dots + (a_m + b_m)X^m \in R[X]$$

$\downarrow$ R 'nin ifadesi $\downarrow$ ifade $\downarrow$ ifade

($i > k$ için $a_i = 0_R$)

$$\Rightarrow P(X) + Q(X) := c_0 + c_1 X + \dots + c_m X^m \quad (c_i := (a_i + b_i) \in R)$$

Polinom, şu şekilde de tanımlanabilir :

Tanım: $(a_n)_{n \in \mathbb{N}}$ dizisi için, sonlu tane eleman sıfırdan farklıdır.

Şimdi $(R[X], \oplus, \odot)$ yapısının halka olduğunu gösterelim.

$H_1 : (R[X], \oplus)$ değişmeli gruptur.

G_1 : Birleşme özelliği vardır.

G_2 : $\forall a \in R, a + 0_R X + 0_R X^2 + \dots + 0_R X^k = a \in R[X] \Rightarrow$ bu tip

polinoma sabit polinom denir. 0_R 'de sıfır polinomdur. $0_R X := 0_R$

G₃: $\ominus P(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n$ ters polinomdur.

G₄: Değişme özelliği vardır.

$\Rightarrow (R[x], \oplus)$ değişmeli gruptur.

$$p(x) \oplus q(x) := a_0 + a_1x + \dots + a_nx^n \quad (\text{işlemdir})$$

$$(n \leq k+m, n \in \mathbb{N})$$

$$\forall 0 \leq i \leq n, d_i = \sum_{j=0}^i a_j b_{i-j} \quad \left\{ \begin{array}{l} j \geq k \Rightarrow a_j = 0_R \\ \text{ve} \\ j \geq m \Rightarrow b_j = 0_R \end{array} \right.$$

$$d_0 = a_0 b_0, d_1 = \sum_{j=0}^1 a_j b_{1-j} = a_0 b_1 + a_1 b_0$$

$$a_i, b_i \in R \Rightarrow a_i \cdot b_i \in R \Rightarrow d_i \in R$$

$\Rightarrow p(x) \oplus q(x)$ çarpımı tekidir.

H₂: " $\oplus$ " işleminin birleşme özelliği vardır.

H₃: " $\oplus$ " işleminin " $\oplus$ " işlemi üzerine (sağ ve sol) dağılma özelliği vardır.

O halde $(R[x], \oplus, \odot)$ yapısı bir halkadır.

Bu halkaya R den katsayılı polinom halkası denir.

$1_R \in R \Rightarrow 1_{R[x]} = 1_R$ dir. (Birimli halka ise halkanın birimi, polinom halkasının birimine eşit olur.)

R değişmeli $\Rightarrow R[x]$ de değişmelidir.

İspat: $R, T.B. \Rightarrow R[x]$ de T.B. dir.

$$P(x) = a_0 + a_1x + \dots + a_nx^n \neq 0_R \quad (a_n \neq 0_R)$$

$$Q(x) = b_0 + b_1x + \dots + b_mx^m \neq 0_R \quad (b_m \neq 0_R)$$

$$P(x)Q(x) = c_0 + c_1x + \dots + c_lx^l \quad (l = m+n)$$

$$c_l = \sum_{j=0}^{m+n} a_j b_{l-j}$$

$$= a_0 b_{m+n} + a_1 b_{m+n-1} + a_2 b_{m+n-2} + \dots + a_n b_m + a_{m+n} b_{n-1} + \dots + a_{m+n} b_0$$

$$\Rightarrow a_n b_m \neq 0_R \Rightarrow P(x)Q(x) \neq 0_R$$

$\Rightarrow$ Sıfır bölen değildir. //

Sonuç : F bir cisim ise $F[x]$, T.B. dir.

Sonuç : $f, g \in R[x]$, $d^0(fg) \leq d^0f + d^0g$ dir.

Eğer R , T.B. ise $d^0(fg) = d^0f + d^0g$ dir.

Örnek // $\mathbb{Z}_6[x]$ de,

$$f = 1 + x + 3x^4 \quad g = 2 + 5x + 2x^2$$

$$\Rightarrow fg = \dots + \underline{3x^5} + \underline{\frac{3 \cdot 2}{6}x^6}$$

$$5 = d^0(fg) < d^0f + d^0g = 4 + 2 = 6$$

$5 < 6$

Tanım : $r \in R$ olsun.

$$p(r) := a_0 + a_1r + \dots + a_nr^n \in R$$

ifadesine, polinomun r elemanındaki değeri denir.

$p(r) = 0_R \Rightarrow r$ 'ye $p(x)$ in kökü denir.

Teorem : $1_R \in R$, $f, g \in R[x]$, $(g(x) \neq 0_R)$ olsun.

Eğer $g(x)$ in başkatsayısı terslenebilir ise,

$f(x) = q(x)g(x) + r(x)$ ve $d^0r < d^0g$ o.s $\exists ! q(x), r(x) \in R[x]$.

İspat // $f(x) = a_0 + a_1x + \dots + a_nx^n$

$$g(x) = b_0 + b_1x + \dots + b_mx^m \quad (b_m^{-1} \in R)$$

$n=0$ iken, $0 = d^0f < d^0g$, $q(x) := 0$, $r(x) := f(x)$ $\left\{ \begin{array}{l} f(x) = 0g(x) + f(x) \\ 0 = d^0f = d^0g, r(x) := 0 \text{ ve } q(x) := a_0b_0^{-1} \text{ seçersek} \end{array} \right.$

$0 = d^0f = d^0g$, $r(x) := 0$ ve $q(x) := a_0b_0^{-1}$ seçersek

$$a_0 = \underbrace{(a_0b_0^{-1})}_{q} \underbrace{b_0}_{g} + \underbrace{0}_{r} \text{ olur.}$$

$\left\{ \star \text{ Sıfır polinomun derecesi } -\infty \text{ dir. } -\infty = d^0r < d^0g = 0 \right\}$

Derecesi n den küçük olan polinomlar için ifade doğru olsun. Genel olarak $d^0g \leq d^0f$ alabiliriz.

$d^0f < d^0g \Rightarrow q(x) = 0$ ve $r(x) = f(x)$ seçeriz.

$$f_1(x) := \underbrace{f(x)}_{\substack{\downarrow \\ a_n x^n \\ d^0f = n}} - \underbrace{a_n b_m^{-1} x^{n-m}}_{\substack{\downarrow \\ x^{n-m}}} \underbrace{g(x)}_{\substack{\downarrow \\ x^m}} \text{ diyelim}$$

derecesi n dir.

$\Rightarrow d^0 f_1 \leq n$ olur. Tümevarım hipotezinden,

$f_1(x) = q_1(x) \cdot g(x) + r(x)$ ve $d^0 r < d^0 g$ o.s. $\exists q_1(x), r(x) \in R[x]$

$$f(x) = (a_n b_m^{-1} x^{n-m}) g(x) = q_1(x) g(x) + r(x)$$

$$f(x) = \underbrace{(q_1(x) + a_n b_m^{-1} x^{n-m})}_{q_2(x)} g(x) + r(x)$$

olur.

$$\text{Teorik: } f(x) = q_1(x) g(x) + r_1(x) = q_2(x) g(x) + r_2(x)$$

$d^0 r_1, d^0 r_2 < d^0 g$ olsa,

$$(q_1(x) - q_2(x)) g(x) = r_2(x) - r_1(x)$$

$$d^0 g > d^0(r_2 - r_1) = d^0((q_1 - q_2)g) > d^0 g \quad \left\{ d^0(f+g) \leq \max\{d^0 f, d^0 g\} \right\}$$

eğer $q_1 - q_2 \neq 0_R$ olsa, $d^0((q_1 - q_2)g) > d^0 g$

g nin başkatsayısı sıfır bölünli demez ve çarpım da

sıfırdan farklıdır. O halde,

$$q_1 - q_2 = 0_R \Rightarrow q_1 = q_2 \Rightarrow r_1(x) = r_2(x) \text{ olur.}$$

1.Sonuç: F cisim ise $\forall f(x), g(x) \in F[x]$ için,

$$f(x) = q(x)g(x) + r(x), \quad d^0 r < d^0 g \text{ o.s. } \exists! q, r \in R[x] \text{ dir.}$$

2.Sonuç: $1_R \in R, \forall f(x) \in R[x]$ ve $a \in R$ olsun.

$$f(x) = (x-a)q(x) + f(a) \text{ o.s. } \exists! q(x) \in R[x] \text{ dir.}$$

İspat: Yukarıdaki teorende, $g(x) = x-a$ alırsak,

g nin başkatsayısı 1_R dir. $1_R \in R$ ve $1_R^{-1} \in R$ dir.

$$f(x) = (x-a)q(x) + r(x) \text{ ve } d^0 r < 1 \text{ o.s. } \exists! q, r \in R[x].$$

$$d^0 r < 1 \Rightarrow d^0 r = 0 \Rightarrow r(x) = c, \quad c \in R \text{ dir.}$$

$$f(a) = r(a) = c \text{ olur.} //$$

Önerme: F bir cisim, $f(x) \in F[x]$ $d^0 f \geq 1$ olsun.

$$\langle f(x) \rangle = f(x) F[x] \quad (\text{birimli, değişmeli halka})$$

$F[x]/\langle f(x) \rangle$ bölüm halkasının tam temsilciler sistemi;

$$A := \{p(x) \in F[x] \mid d^0 p < d^0 f\} \text{ dir.}$$

Tan temsilciler sistemi : her denklik sınıfından bir tek temsilcinin bulunduğu kümedir.

$F[x]/\langle f(x) \rangle$ 'in eleman sayısı ile A 'nın eleman sayısı eşittir.

$$F[x]/\langle f(x) \rangle = \{ p(x) + \langle f(x) \rangle \mid p(x) \in A \}$$

İspat // $\forall g \in F[x]$ için, teoremden dolayı;

$$g(x) = q(x)f(x) + r(x) \text{ ve } d^{\circ}r < d^{\circ}f \text{ o.s. } \exists! q(x), r(x) \in F[x].$$

$$\Rightarrow g(x) - r(x) = q(x)f(x) \in \langle f(x) \rangle$$

$$\Rightarrow g(x) \equiv r(x) \pmod{\langle f(x) \rangle}$$

$$\Rightarrow g(x) + \langle f(x) \rangle = r(x) + \langle f(x) \rangle$$

derecesi r den küçük iki polinom, aynı denklik sınıfını belirtir mi bakalım.

$$d^{\circ}r_1, d^{\circ}r_2 \text{ için, } r_1(x) \equiv r_2(x) \pmod{\langle f(x) \rangle} \text{ olsa}$$

$$\Rightarrow r_1(x) - r_2(x) \in \langle f(x) \rangle$$

$$\Rightarrow r_1(x) - r_2(x) = h(x)f(x) \text{ o.s. } \exists h(x) \in F[x].$$

$$\Rightarrow d^{\circ}(r_1 - r_2) = d^{\circ}f + d^{\circ}h \geq d^{\circ}f \quad \#$$

Çelişki olur. Çünkü, $d^{\circ}(r_1 - r_2) \leq \max\{d^{\circ}r_1, d^{\circ}r_2\} < d^{\circ}f$

$$\Rightarrow r_1 \not\equiv r_2 \pmod{\langle f(x) \rangle} \text{ dir.}$$

Örnek // $f(x) = 1 + x + x^3 \in \mathbb{Z}_2[x] \Rightarrow \mathbb{Z}_2[x]/\langle f(x) \rangle = ?$

$$A := \{ p(x) \in \mathbb{Z}_2[x] \mid d^{\circ}p < d^{\circ}f = 3 \}$$

$$p(x) = \bar{a} + \bar{b}x + \bar{c}x^2, \quad \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_2 = \{ \bar{0}, \bar{1} \}$$

$$\bar{A} = \{ \bar{0}, \bar{1}, \bar{x}, \bar{1} + \bar{x}, \bar{x}^2, \bar{1} + \bar{x}^2, \bar{1} + \bar{x} + \bar{x}^2, \bar{x} + \bar{x}^2 \}$$

$$\begin{aligned} \mathbb{Z}_2[x]/\langle f(x) \rangle = \{ & \bar{0} + \langle f(x) \rangle = \langle f(x) \rangle, \bar{1} + \langle f(x) \rangle, \bar{x} + \langle f(x) \rangle, \\ & (\bar{1} + \bar{x}) + \langle f(x) \rangle, \bar{x}^2 + \langle f(x) \rangle, (\bar{1} + \bar{x}^2) + \langle f(x) \rangle, \\ & (\bar{1} + \bar{x} + \bar{x}^2) + \langle f(x) \rangle, (\bar{x} + \bar{x}^2) + \langle f(x) \rangle \} \end{aligned}$$

bulunur. //

Halkalarda Aritmetik

$m|n \Rightarrow \overline{f}m | \overline{f}n$ ($\mathbb{Z}^+$ da incelenen yapı olacak deniştik)

{ 3 asal sayıdır. Asal sayı tanımında, kendisinden ve 1 den başka böleni olmayan sayı diyarduk. Oysa, $-3|3$ olur. $-3, 3$ ün bölenidir. }
{ 0 yüzden $\mathbb{Z}^+$ yi kullanacağız deniştik. }

Bundan sonra, R denildiğin de T.B. (birimli, değişmeli, sıfır bölensiz halka) yi kullanacağız.

$a, b \in R$ için $a = bc$ o.s. $\exists c \in R$ varsa " b, a yi böler" denir ve $b|a$ yazılır.

Önerme: $\forall a, b, c \in R,$

i - $a|b$ ve $b|c \Rightarrow a|c$ (bölmede geçişme)

ii - $a|b \Rightarrow \forall x \in R, a|bx$

iii - $a|b$ ve $a|c \Rightarrow \forall x, y \in R, a|bx + cy$

Tanım: R halkasının tüm elemanlarını bölen elemanlara,

aritmetik birim (birimsel elemanlar) denir. $U_R = \{a \in R | a^{-1} \in R\}$ dir.

{ $\sqrt{5}|\sqrt{2}, \sqrt{2} = \sqrt{5}(\frac{\sqrt{2}}{\sqrt{5}})$, $\mathbb{R}$ de }
{ $\sqrt{2}$ nin bölenleri sonsuz tanedir. }
{ en büyük böleni $+\infty$, en küçüğü $-\infty$ olur. }

Örnek // $U_{\mathbb{Z}} = \{-1, 1\}$ dir.

Önerme // $U_R = \{a \in R | a^{-1} \in R\}$

aritmetik birim $\Leftrightarrow$ terslenebilir elemanlar.

İspat // $\Rightarrow: \forall a \in U_R, \forall x \in R, u|x$, özel olarak $u|1_R$

$\Rightarrow 1_R = u.c$ o.s. $\exists c \in R, c = u^{-1} \Rightarrow u \in U_R$ dir.

$\Leftarrow: \forall a \in R$, öyle ki $a^{-1} \in R$ olsun.

$\Rightarrow a.a^{-1} = 1_R$. $\forall x \in R$ için,

$x = 1_R.x = a.(a^{-1}x) \Rightarrow a|x \quad \forall x \in R, a \in U_R$ dir. //

Önerme $\forall a, b \in R,$

$$a \approx b \text{ (ilgili)} \Leftrightarrow a = ub \text{ o.f. } \exists u \in U_R.$$

i - " $\approx$ " bağıntısı R de denklik bağıntısıdır.

İspat $\forall r \in U_R \Rightarrow a = r.a \Rightarrow a \approx a$ (yansıma)

$\forall a, b \in R, a \approx b \Rightarrow a = u.b \text{ o.f. } \exists u \in U_R.$

$u^{-1} \in U_R$ olduğundan $u^{-1}.a = u^{-1}(ub)$

$\Rightarrow u^{-1}.a = b \Rightarrow b \approx a$ (simetri)

$a \approx b \Rightarrow a = ub \text{ o.f. } \exists u \in U_R.$

$b \approx c \Rightarrow b = u'.c \text{ o.f. } \exists u' \in U_R$

$a = ub = u(u'.c) = (uu')c = u''.c \Rightarrow a \approx c$ (gesirme)

ii - $a, b \in R$ olsun.

a) $a|b \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$

b) $0 \neq a, 0 \neq b$ olsun. $a|b$ ve $b|a \Leftrightarrow a \approx b$

İspat $a|b \Leftrightarrow b = at \text{ o.f. } \exists t \in R.$

$\Leftrightarrow b \in \langle a \rangle \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle //$

b - ($\Rightarrow$): $a|b \Rightarrow b = at_1 \text{ o.f. } \exists t_1, t_2 \in R.$
 $b|a \Rightarrow a = bt_2$

$\Rightarrow b = at_1 = (bt_2)t_1 = b(t_2t_1) \Rightarrow 1_R = t_2t_1 \Rightarrow t_1^{-1} = t_2$

$\therefore t_1, t_2 \in U_R \Rightarrow a \approx b$

($\Leftarrow$): $a \approx b \Rightarrow a = ub \text{ o.f. } \exists u \in U_R$

$\Rightarrow b = u^{-1}.a, \quad a = ub \Rightarrow b|a$
 $b = u^{-1}.a \Rightarrow a|b$ } olur. //

Tanım: R bir T.B. ve $0 \neq a, b \in R$ olsun.

i - Bir $c \in R$ için $c|a$ ve $c|b \Rightarrow c$ ye " a ile b 'nin ORTAK BÖLENİ" denir.

ii- c bir ortak bölen olsun. Eğer a ve b nin her ortak k böleni için $k|c$ ise, c ye " a ile b nin ENBÜYÜK ORTAK BÖLENİ" denir ve $\text{ebob}(a,b)$ yazılır. (Kısacası; her ortak bölenin böldüğü ortak bölene, ebob denir.)

$\left\{ \begin{array}{l} \mathbb{Z} \text{ de bölünebilir sıralama bğıntısı değildir.} \\ \text{Çünkü } 0 \nmid 0 \text{ yansıma yoktur.} \end{array} \right\}$

Önerme: $\text{ebob}(a,b) = c$ olsun.

$$c' \approx c \Rightarrow \text{ebob}(a,b) = c' \text{ olur.}$$

Tersine, a ve b nin ebob'leri ilgilidir.

İspat // $\text{ebob}(a,b) = c \Rightarrow c|a$ ve $c|b$ dir.

$$c \approx c' \Rightarrow c'|c \text{ ve } c|c'$$

$$c'|c \xrightarrow{c|a \text{ ve } c|b} c'|a \text{ ve } c'|b \text{ dir.}$$

$\therefore c'$, a ve b nin ortak bölenidir.

$\text{ebob}(a,b) = c$ olduğundan, her k ortak böleni için, $k|c$ idi.

$$c|c' \Rightarrow k|c' \therefore \text{ebob}(a,b) = c'$$

Tersine, $\text{ebob}(a,b) = d_1$ ve $\text{ebob}(a,b) = d_2$ olsun.

$$\text{ebob}(a,b) = d_1 \Rightarrow d_2|d_1, \text{ebob}(a,b) = d_2 \Rightarrow d_1|d_2$$

$$\Rightarrow d_1 \approx d_2 \text{ olur.}$$

Sonuç: $\text{ebob}(a,b) = u$ ve $u \in U_{\mathbb{R}} \Rightarrow \text{ebob}(a,b) = 1$ yazılabilir.

Tanım: İki elemanın enbüyük ortak böleni aritmetik birim ise bu sayılara aralarında asaldır denir.

★ $\left\{ \begin{array}{l} \text{Herhangi bir T.B. için en büyük ortak bölen bulunamaz.} \\ \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C} \text{ T.B. dir. T.Ü.B. değil.} \\ 9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}), 6 + i \cdot 3\sqrt{5} = 3(2 + i\sqrt{5}) \\ \text{ebob}(9, 6 + i \cdot 3\sqrt{5}) = \text{yoktur.} \\ \text{O.B.}(9, 6 + i \cdot 3\sqrt{5}) = \{3, (2 + i\sqrt{5}), \text{aritmetik birimler, ilgili ortaklar}\} \end{array} \right\}$

Önerme: R , T.Ü.i.B. olsun. $\forall 0 \neq a, b \in R$ için $\text{ebob}(a, b) \in R$ dir. sm730

İspat // $I = \langle a, b \rangle$ idealini düşünelim.

$1_R \in R$ ve değişmeli $\Rightarrow I = \{ ar + bs \mid r, s \in R \}$

R , T.Ü.i.B. olduğundan $I = \langle d \rangle$ o.s. $\exists d \in R$.

$\left\{ \begin{array}{l} I \text{ idealinin} \\ \text{nasıl bulunacağını değil,} \\ \text{var olduğunu} \\ \text{belirten önermedir.} \end{array} \right.$

$$a, b \in I = \langle d \rangle \Rightarrow a = dt_1 \text{ ve } b = dt_2 \text{ o.s. } \exists t_1, t_2 \in R.$$

$$\Rightarrow d \mid a \text{ ve } d \mid b. \text{ (} d \text{ ortak bölenidir.)}$$

$$d \in I = \langle d \rangle \Rightarrow d = ax + by \text{ o.s. } \exists x, y \in R.$$

k : a ve b nin herhangi bir ortak böleni olsun.

$$k \mid a \text{ ve } k \mid b \Rightarrow k \mid ax + by = d \therefore d = \text{ebob}(a, b) \text{ dir. } \text{sm730}$$

(T.Ü.i.B. de ebob'un lineer toplam şeklinde yazıldığını gördük.)

27.5.96/P.tesi

Tanım: $0 \neq x \in R - U_R$ olsun. x 'e asal eleman denir eğer,

x 'in aritmetik birimlerden ve x ile ilgililerden başka böleni yoksa

Önerme: R , T.Ü.i.B. ve $\pi \in R$ asal elemanı olsun.

$$a, b \in R, \quad \pi \mid ab \Rightarrow \pi \mid a \vee \pi \mid b \text{ dir.}$$

İspat // $\pi \nmid a$ olsun. $\Rightarrow \pi \mid b$ dir. ?

$$\text{ebob}(\pi, a) = c \in R \text{ olsun } \Rightarrow c \mid \pi \text{ ve } c \mid a \text{ dir.}$$

π asal olduğundan ya $c \in U_R$ veya $c \approx \pi$ dir.

$c \approx \pi$ olsa $\pi \mid c$ olur. $c \mid a$ olduğundan $\pi \mid a$ bulunur. #

0 halde $c \approx \pi$ olamaz. $\Rightarrow c \in U_R$ (c aritmetik birimdir.)

$$\text{ebob}(\pi, a) = 1 \Rightarrow \pi x + ay = 1 \text{ o.s. } \exists x, y \in R.$$

$$\Rightarrow b(\pi x) + b(ay) = b \Rightarrow \pi bx + aby = b$$

$$\Rightarrow \left. \begin{array}{l} \pi \mid \pi bx \\ \pi \mid ab \end{array} \right\} \Rightarrow \pi \mid \pi bx + aby = b \quad (\pi \mid b)$$

bulunur. Bu ise teoremin ispatıdır. //

Tanım: Bir R , T.B.'ne "Tek türlü Asal Çarpanlara ayrılabilir Bölge" (TAGB) dir denir, eğer:

(TAGB) dir denir, eğer:

i- $\forall 0 \neq x \in R - U_R$ elemanı, asal elemanların çarpımı olarak yazılabiliyorsa.

ii- (i)'deki yazılış, ilgililik ve sıra düşünmeksizin tektürlü ise.

$$\left\{ \begin{array}{l} 12 = 3 \cdot 2 \cdot 2 = 2 \cdot 3 \cdot 2 = 2 \cdot 2 \cdot 3 \quad (\text{sıra}) \\ 12 = (-3)(-2)(2) = (2)(-2)(-3) = (-2)(-2)(3) \quad (\text{ilgililik}) \end{array} \right\}$$

$\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$ bu şartları sağlar mı, bilmiyoruz.

Ancak, $\mathbb{Z}$ bu şartları sağlayan bir T.A.Ç.B. dir.

Önerme: R , T.Ü.B. $\Rightarrow R$, TAGB dir.

İspat: R deki her eleman, asal elemanların çarpımı şeklinde yazılabilir. Kabul edelim ki, $0 \neq x \in R - U_R$ asalların çarpımı şeklinde yazılamasın.

$$\Rightarrow x = a_1 b_1 \quad \text{o.s.} \quad \exists a_1, b_1 \in R - U_R.$$

a_1 veya b_1 den en az biri asalların çarpımı şeklinde yazılamaz.

a_1 , asalların çarpımı şeklinde yazılamasın.

$$a_1 \mid x \Rightarrow \langle x \rangle \subset \langle a_1 \rangle \quad \text{ve} \quad b_1 \notin U_R \quad \text{olduğundan,}$$

$$\langle x \rangle \neq \langle a_1 \rangle \quad a_1 \text{ 'de asal değildir. Yani,}$$

$$\Rightarrow a_1 = a_2 b_2 \quad \text{o.s.} \quad \exists a_2, b_2 \in R - U_R.$$

a_2 veya b_2 den en az biri asalların çarpımı şeklinde yazılamaz.

a_2 asalların çarpımı şeklinde yazılamasın.

$$a_2 \mid a_1 \Rightarrow \langle a_1 \rangle \subset \langle a_2 \rangle \quad \text{ve} \quad b_2 \notin U_R \quad \text{olduğundan}$$

$$\langle a_1 \rangle \neq \langle a_2 \rangle \quad a_2 \text{ 'de asal değildir.}$$

----- Bu şekilde devam ederek -----,

$$\langle a_0 \rangle = x \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$$

şeklinde, idealler zinciri elde edilir.

$$I := \bigcup_{i \geq 0} \langle a_i \rangle \quad \text{idealdir. (ödev)}$$

{ i.s. ise alt kümeler zinciridir. }

R , Tübs olduğundan $I = \langle k \rangle$ o.s. $\exists k \in R$.

$\Rightarrow k \in I \Rightarrow k \in \langle an \rangle$ o.s. $\exists n \in \mathbb{N}$.

$\Rightarrow I \subset \langle k \rangle \subset \langle an \rangle \subsetneq \langle an+1 \rangle \subset I \quad \#$

O halde Tübs 'den alınan her X , asalların çarpımı şeklinde yazılabilir.

Şimdi bu yazılışın tek türlü olduğunu gösterelim.

$X = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ (p_i, q_i asallar) olarak iki türlü yazılsın.

$p_1 \mid q_1 q_2 \dots q_m \Rightarrow p_1 \mid q_i$ o.s. $\exists 1 \leq i \leq m$

p_i ve q_i asal olduğundan $p_1 \approx q_i$ dir.

Sıra önemli olmadığından q_i 'yi başa alıp, q_1 ile yer değiştirerek, $q_i = q_1$ yazabiliriz.

$p_1 = c q_1$ o.s. $\exists c \in UR$.

$c = q_1 p_2 \dots p_n = q_1 q_2 \dots q_m$

$\Rightarrow c_1 p_2 \dots p_n = q_2 \dots q_m \Rightarrow p_2 \approx q_2 \dots \Rightarrow m \leq n$ olur.

Benzer şekilde q 'lar için de aynısı yapılarak, $n \leq m$ olur.

O halde $m = n$, yani X tektürlü olarak asalların çarpımı şeklinde yazılır diyebiliriz. //

Tanım: $N: R \rightarrow \mathbb{Z}$ fonksiyonu, aşağıdaki şartları sağlarsa, N 'ye R üzerinde bir çarpımsal norm denir.

i- $\forall x \in R, N(x) \geq 0$

ii- $N(x) = 0 \Leftrightarrow x = 0_R$

iii- $\forall x, y \in R, N(xy) = N(x)N(y)$

Tanım: R , T.B. ve N 'de R üzerinde tanımlı bir norm olsun.

R 'ye Euclid Bölgesi (E.B.) denir, eğer :

$\forall x, y \in R, (y \neq 0) \quad x = qy + r$ ve $0 \leq N(r) < N(y)$ o.s. $\exists q, r \in R$.

{ Burada; $r, y \in R$ olduğundan ve bunlar arasında bir sıralama bağıntısı olmadığından $r < y$ diyemeyiz. Örneğin; $\mathbb{I}$ sayılar, sıralama bağıntısı olmadığından karşılaştırılamaz. }

R burada herhangi bir halkadır.

$$(R, EB \Rightarrow R, T\ddot{U}IB \Rightarrow R, TAGB.)$$

Önerme: $R, EB \Rightarrow R, T\ddot{U}IB$ dir.

İspat, $\mathbb{I} \subset R$ ideali olsun.

$$\mathbb{I} = \{0_R\} \Rightarrow \mathbb{I} = \langle 0_R \rangle$$

$$\mathbb{I} \neq \{0_R\} \Rightarrow \exists 0_R \neq a \in \mathbb{I}, N(a) \neq 0$$

$m, \mathbb{I}$ daki normu en küçük olan eleman olsun. (En küçük norm, birden fazla olabilir. Eşit olduğu için bunlardan birini $m \in \mathbb{I}$ yı alalım.)

$\Rightarrow \langle m \rangle \subset \mathbb{I}$ olacağı (üretme tanımından) aşiktir.

Tersine, $x \in \mathbb{I}$ alalım. $x = qm + r$ ve $0 \leq N(r) < N(m)$ o.p. $\exists q, r \in R$.

$$\begin{array}{l} x - qm = r \in \mathbb{I} \quad (m \text{'nin seçilişinden}) \Rightarrow N(r) = 0 \text{ olmalı.} \\ \downarrow \text{E.B.} \\ \mathbb{I} \quad \mathbb{I} \end{array} \Rightarrow r = 0_R$$

$$\Rightarrow x = qm \in \langle m \rangle \therefore \mathbb{I} \subset \langle m \rangle$$

$\Rightarrow \mathbb{I} = \langle m \rangle$ yani; $R, EB \Rightarrow R, T\ddot{U}IB$ olduğu görülür. //

$$\left\{ \begin{array}{l} R, TAGB \Rightarrow R, T\ddot{U}IB \text{ olmayabilir.} \\ \mathbb{Z}, E.B. \text{ dir.} \end{array} \right\}$$

Örnek, $N: \mathbb{Z} \rightarrow \mathbb{Z}$
 $a \rightarrow N(a) := |a| \quad |r| = r < |y|$

Örnek, F cisim ise $F[x]$ E.B. dir.

$$\begin{array}{l} N: F[x] \rightarrow \mathbb{Z} \\ p(x) \rightarrow N(p(x)) := 3^{d^o p} \geq 0 \quad (i) \end{array}$$

$$p(x) = 0 \Rightarrow N(p(x)) = 3^{-\infty} = 0$$

$$3^{d^o p} = 0 \Rightarrow d^o p = -\infty \Rightarrow p(x) = 0 \quad (ii)$$

$$N(pq) = 3^{d^o(pq)} = 3^{d^o p + d^o q} = 3^{d^o p} \cdot 3^{d^o q} = N(p)N(q) \quad (iii)$$

$p(x) = f(x)q(x) + r(x)$ ve $\deg r < \deg q$ yazılabiliyor idi.
 $\parallel$ $\parallel$ $3\deg r < 3\deg q \Rightarrow N(r) < N(q)$ (iv)

Örnek // $\mathbb{Z}[i] := \{a+ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$

25.5.96 / Garipamba

Gauss Tamsayılar Bölgesi bir E.B. dir.

$$N: \mathbb{Z}[i] \rightarrow \mathbb{Z}$$

$$a+ib \rightarrow N(a+ib) := a^2 + b^2 = (a+ib)(a-ib) = |a+ib|^2$$

$$(\text{Modül} \Rightarrow |a+ib| = \sqrt{a^2+b^2})$$

$$i- \forall \alpha = a+ib \in \mathbb{Z}[i] \text{ için, } N(\alpha) \geq 0.$$

$$ii- N(\alpha) = a^2 + b^2 = 0 \Leftrightarrow a^2 = b^2 = 0 \Leftrightarrow a = b = 0 \Leftrightarrow \alpha = 0$$

$$iii- \forall \alpha, \beta \in \mathbb{Z}[i],$$

$$N(\alpha\beta) = |\alpha\beta|^2 = (|\alpha| \cdot |\beta|)^2 = |\alpha|^2 |\beta|^2 = N(\alpha) \cdot N(\beta)$$

$\Rightarrow N, \mathbb{Z}[i]$ üzerinde bir çarpımsal normdur.

$$iv- \forall \alpha, \beta \in \mathbb{Z}[i], (\beta \neq 0) \text{ için,}$$

$$\alpha = \beta q + r \text{ ve } N(r) < N(\beta) \text{ o.s. } \exists q, r \in \mathbb{Z}[i].$$

$$\alpha\beta^{-1} = \frac{\alpha}{\beta} \in \mathbb{C} \quad (\beta^{-1} \notin \mathbb{Z}[i])$$

kompleks sayısının işine

düştüğü birim kareyi düşünelim.

Ve $\frac{\alpha}{\beta}$ nin en yakın olduğu

köşeyi q ile gösterelim. (Birden fazla köşe varsa q olarak herhangi birini seçelim.)

$$q \in \mathbb{Z}[i] \text{ dir.}$$

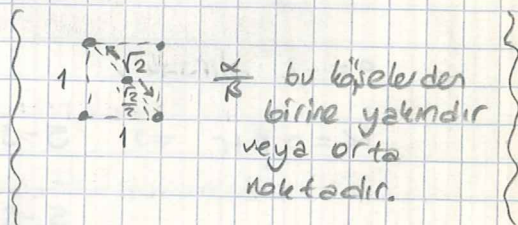
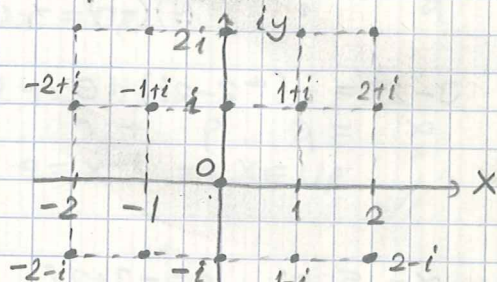
$$\left| \frac{\alpha}{\beta} - q \right| \leq \frac{\sqrt{2}}{2} \Rightarrow \frac{|\alpha - q\beta|}{|\beta|} \leq \frac{\sqrt{2}}{2}$$

$$\Rightarrow |\alpha - q\beta|^2 \leq \frac{|\beta|^2}{2} < |\beta|^2 \Rightarrow N(\alpha - q\beta) < N(\beta)$$

($\in \mathbb{Z}[i] - \mathbb{Z}[i]$)

$$\Rightarrow r := \alpha - q\beta \text{ dersek, } \alpha = q\beta + r \Rightarrow N(r) < N(\beta) \text{ o.s. } \exists q, r \in \mathbb{Z}[i]$$

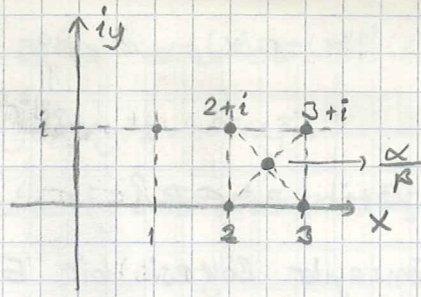
0 halde $\mathbb{Z}[i]$ bir E.B. olur. //



Örnek,, $\alpha = 3-2i$, $\beta = 1-i$

$$|(i+5)-q| \leq \frac{\sqrt{2}}{2}$$

$$\frac{\alpha}{\beta} = \frac{3-2i}{1-i} \cdot \frac{(1+i)}{(1+i)} = \frac{1+5}{2}$$



$q = 3+i$ seçilebilir.

$$r = \alpha - q\beta$$

$$r = (3-2i) - (3+i)(1-i) = -1 \Rightarrow r = -1$$

$$\alpha = q\beta + r \Rightarrow (3-2i) = (3+i)(1-i) - 1 \text{ ve } N(-1) = 1 < N(1-i) = 2$$

0 halde iki Gauss tamsayısı verildiğinde birini diğerine bölüp, kalanı bulabiliriz.

$$\mathbb{Z}[i], E.B. \Rightarrow \mathbb{Z}[i], T.Ü.i.B. \Rightarrow \mathbb{Z}[i], T.A.Ç.B.$$

Örnek,, $\alpha = 3-2i$, $\beta = i$

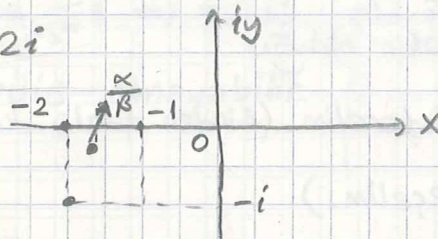
$$\frac{\alpha}{\beta} = \frac{3-2i}{i} = \frac{(3-2i)(-i)}{(i)(-i)} = \frac{-3+2}{+1} = -2-3i$$

$$\begin{aligned} 3-2i &= i(-2-3i) + 0 \\ \alpha &= \beta \cdot q + r \end{aligned}$$

Aritmetik birimler halkasının elemanını böler.
 $\left. \begin{aligned} U|X \\ U \in R \end{aligned} \right\} \Rightarrow X = Uq + 0$

Örnek,, $\alpha = 5-3i$, $\beta = -3+2i$

$$\frac{\alpha}{\beta} = \frac{-21-i}{13}$$



$q = -2$ alırsak,

$$\alpha = q\beta + r \Rightarrow 5-3i = -2(-3+2i) + r$$

$$5-3i = 6-4i + r \Rightarrow r = -1+i \text{ olur. } //$$

61/13- R , T.B ve $d: R \rightarrow \mathbb{Z}$ çarpımsal norm olsun.

$$d(x) = 1 \Leftrightarrow x \in U_R$$

özelligi sağlansın. Gösteriniz ki, $\pi \in R$ için $N(\pi) = p \in \mathbb{Z}$ (asal ise)

$\pi \in R$ asal elemandır. (Normu asal olan sayı asal elemandır.

(tersi doğru değildir.)

$a \in R$ için, $a | \pi \Rightarrow \pi = ab$ o.s. $\exists b \in R$.

$$N(\pi) = N(ab) = N(a)N(b)$$

$$p = N(a)N(b) \Rightarrow N(a) | p \quad (p \text{ asal})$$

$$\Rightarrow N(a) = 1 \vee N(a) = p \text{ dir.}$$

$$N(a) = 1 \Rightarrow a \in U_R \text{ dir. (özellikler)}$$

$$N(a) = p \Rightarrow N(b) = 1 \Rightarrow b \in U_R \text{ dir. ve bu durumda,}$$

$$\pi = ab \text{ dir, } \pi \approx a \text{ dir. //}$$

Örnek,, R , T.B ve $N: R \rightarrow \mathbb{Z}$ çarpımsal norm olsun.

$$x \in R \text{ için } N(x) = 1 \Leftrightarrow x \in U_R \text{ dir.}$$

$$\Leftarrow: x \in U_R \Rightarrow xy = 1_R \text{ o.s. } \exists y \in R.$$

$$\Rightarrow N(xy) = N(1_R) = 1$$

$$N(x)N(y) = 1 \Rightarrow N(x) = 1$$

$$\Rightarrow: N(x) = 1, \exists s \in R, t \in R \text{ i.e.}$$

$$1_R = sx + tr \text{ ve } N(r) < N(x) = 1 \Rightarrow r = 0_R$$

$$\Rightarrow sx = 1_R$$

$$\Rightarrow s = x^{-1} \Rightarrow x \in U_R //$$

$$1_R 1_R = 1_R \Rightarrow$$

$$N(1_R 1_R) = N(1_R)N(1_R) = N(1_R)$$

(Tamsayılarda
kısaltma)

$$\Rightarrow N(1_R) = 1 //$$

Polinom Halkalarında Asal Çarpanlara Ayrılış

3.6.96/P.tesi

Bu bölümde R yi TAGB olarak alacağız.

$R[x]$ de, R den katsayılı polinomlar halkasıdır.

Tanım: $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$ polinomunun katsayılarının ebob'ine f nin kapsamı denir. Ve,

$$c(f) := \text{ebob}(a_1, a_2, \dots, a_n)$$

ile gösterilir. Eğer $c(f) = 1$ ise f 'ye ilkel polinom denir.

Önerme: $0 \neq f(x) \in R[x]$ için, (tek türlü)

$$f(x) = c(f(x)) \cdot f^*(x) \quad \text{o.ş. } \exists f^*(x) \in R. \text{ (ilkel)}$$

İspat // $c(f) = d$ dersek, $a_i = a_i' d$ ve $(a_1', a_2', \dots, a_n') = 1$ o.ş. $\exists a_i' \in R$.

$$f(x) = c(f) \cdot (a_0' + a_1'x + \dots + a_n'x^n)$$

$f^*(x)$ ilkel.

$$\left\{ \text{ebob}(na, nb) = n \cdot \text{ebob}(a, b) \right\}$$

Eğer bu yazılış iki türlü ise,

$$\Rightarrow f = c(f) \cdot f^* = d g^*$$

$$\Rightarrow c(f) = c(f) c(\underbrace{f^*}_1) = d c(\underbrace{g^*}_1)$$

$$\Rightarrow c(f) = d //$$

Önerme: $f, g \in R[x]$ ve $c(f) = 1 = c(g) \Rightarrow c(fg) = 1$ dir.

İspat // $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \quad c(f) = 1$

$$g = b_0 + b_1x + b_2x^2 + \dots + b_mx^m \quad c(g) = 1$$

$\forall i \geq 0$ için, $c_i = a_0b_i + a_1b_{i-1} + \dots + a_ib_0$ olmak üzere

$$fg = c_0 + c_1x + c_2x^2 + \dots + c_{m+n}x^{m+n}$$

(T.B. olduğu için, çarpımın derecesi dereceler toplamına eşittir.)

$\pi \in R$ asal elemanı olsun. ve $c(f) = 1 = c(g)$ olduğundan,

π, a_i lerden ve b_i lerden bazılarını bölmez. f de π nin ilk

bölmediği katsayı a_i ve g de ilk bölmediği katsayı b_j olsun.

$$c_i = a_0b_i + a_1b_{i-1} + \dots + a_ib_j + a_{i+1}b_{j-1} + \dots + a_{i+j}b_0$$

$$\pi | c_i t_j \text{ olsa ; } \pi | a t \quad 0 \leq t \leq i$$

$$\pi | b t \quad 0 \leq k \leq j$$

π asal olduğundan (TAŞB de) $\pi | a_i b_j$ olmalıdır.

$$\Rightarrow \pi | a_i \text{ veya } \pi | b_j \neq \text{ (halbuki } \pi \text{ bunları bölmeyi idi.)}$$

$$\Rightarrow \pi \nmid c_i t_j$$

0 halde $\text{ebob}(c \text{ 'ler}) = 1$ (aritmetik birim) olur.

$$\Rightarrow c(fg) = 1 \text{ yani kapsam 1 olur. //}$$

Önerme : F, R nin kesir cismi ve $0 \neq f(x) \in R[x]$ olsun. 0 halde,

$$f(x) = a^* \cdot f^*(x) \text{ o.s. } \exists a^* \in F \text{ ve } \exists f^*(x) \in R[x]. \text{ (ilkel)}$$

İspat // $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \dots + \frac{a_n}{b_n}x^n \quad a_i, b_i \in R, b_i \neq 0$

$$0 \neq \alpha := b_0 b_1 \dots b_n \in R \quad (\text{halka TB olduğu için})$$

$$0 \neq \alpha \cdot f(x) \in R[x] \text{ olur.}$$

Önceki önermeden, $\alpha f(x) = c(\alpha f) \cdot f^*(x)$ o.s. $\exists f^*(x) \in R$. (ilkel)

$$\Rightarrow a^* := \frac{c(\alpha f)}{\alpha} \in F. \Rightarrow f(x) = a^* f^*(x) \text{ dir. //}$$

Önerme : F, R nin kesir cismi ve $f(x) \in R[x]$ ilkel polinom olsun. $f(x), R[x]$ de asal $\Leftrightarrow f(x), F[x]$ de asal.

İspat // $\Rightarrow$: $g(x) \in F[x]$ için ,

$$g(x) | f(x) \Rightarrow f(x) = g(x)h(x) \text{ o.s. } \exists h(x) \in F[x].$$

$$\left. \begin{array}{l} g(x) = a^* g^*(x) \\ h(x) = b^* h^*(x) \end{array} \right\} \Rightarrow g^*(x), h^*(x) \in R[x] \text{ ilkel, } a^*, b^* \in F.$$

$$f = a^* b^* g^* h^* \Rightarrow c(f) = a^* b^* c(g^* h^*) \Rightarrow a^* b^* = 1$$

$$\Rightarrow f = g^* h^* \in R[x]$$

$f \in R[x]$ asal olduğundan, $g^* \in U_R$ veya $h^* \in U_R$

$$\Rightarrow g = a^* g^* \in F \text{ veya } h = b^* h^* \in F$$

$\Rightarrow f$ in, (sabit polinom) aritmetik birim ve kendisiyle ilgili-lerden başka böleni yoktur.

$$\Leftarrow: R[x] \subset F[x] \quad \{Z[x] \subset Q[x]\}$$

$g(x) \in R[x]$, $g(x) | f(x)$ olsa, $\{f(x), R[x]$ de asal olmasa $\}$

yani, $f(x) = g(x)h(x)$ o.p. $\exists g(x), h(x) \in R[x] - U_R$,

$R[x] \subset F[x]$ olduğundan, $g, h \in F[x]$ ve hipotezden, $g \in R$ veya $h \in R$. (yani sabit polinomdur.)

Diyelim ki, $g \in R$ olsun.

$$f = gh \Rightarrow 1_R = c(f) = g \underbrace{c(h)}_{\in R} \Rightarrow g^{-1} = c(h) \in R \Rightarrow g \in U_R //$$

$\{ \begin{array}{l} \mathbb{Z} \text{nin kesir cismi } \mathbb{Q} \text{ dur.} \\ f, \mathbb{Z}[x] \text{ de asal} \Leftrightarrow f, \mathbb{Q}[x] \text{ de asal.} \end{array} \}$

$P = 2x+4 \in \mathbb{Z}[x]$ asal mıdır? bakalım.

$P = 2(x+2)$, $\text{ebob}(2,4)=2$ ilkel değil. $2 | P(x)$ $2 \notin U_{\mathbb{Z}[x]}$ asal değil.
 $x+2 | P(x)$

★ Halkada asal eleman (sayı, polinom, fonksiyon, ... v.s.):

$0 \neq a \in R - U_R$ ve kendisiyle ilgililerden başka böleni yoksa.

$P = 2x+4 \in \mathbb{Q}[x]$ de asal mıdır? bakalım.

$P = 2(x+2) \in \mathbb{Q}[x]$ $2 | P(x)$ $2 \in U_{\mathbb{Q}[x]}$ 2 sabit polinomdur, tersi var.
 $x+2 | P(x)$

Sabit polinom $= F = U_{F[x]}$ $F[x]$ polinomlar halkasında terslenebilir elemanlar sabit polinom idi.

$(x+2)$ asaldır. Çarpanlara ayrılmaz. $(x+2) \approx (2x+4)$ ilgilidir.

○ halde $2x+4 \in \mathbb{Q}[x]$ asaldır.

Eğer $P = 2x+5$ olsaydı, P polinomu ilkel olurdu.

$\text{ebob}(2,5)=1=c(P)$

Teorem: $R, \text{TAGB} \Rightarrow R[X]$ de TAGB dir.

1. Sonuç: F cisim $\Rightarrow F[X]$ TAGB dir.

2. Sonuç: $R \text{ TAGB} \Rightarrow R[X_1, X_2, \dots, X_n]$ TAGB dir.

Örnek: F cisim $\Rightarrow F[X, Y]$ TAGB dir. Fakat Tüib değildir.

$F[X, Y] = (F[X])[Y]$ dir.

$$\langle X, Y \rangle_{\text{ideal}} = \{ Xf(X, Y) + Yg(X, Y) \mid f, g \in F[X, Y] \} = \langle h(X, Y) \rangle \subsetneq F[X, Y]$$

($\langle X, Y \rangle$ nin tek bir polinomla üretilmediğini gösterelim)
olacak şekilde $\exists h(X, Y) \in F[X, Y]$ olsa çelişkiye düşeriz ve Tüib olmadığını göstermiş oluruz.

$$X \in \langle h \rangle \Rightarrow X = h(X, Y)t(X, Y)$$

$$Y = h(X, Y)k(X, Y)$$

$h(X, Y) \neq 1$ dir. Çünkü halkanın kendisi olamaz.

$$\Rightarrow h(X, Y) = X \text{ ve } t(X, Y) = 1, Y = Xk(X, Y)$$

$$\Rightarrow k(X, Y) = YX^{-1}$$

Halbuki bir polinomda X^{-1} olamaz. $F[X, Y]$ Tüib değildir. //

Teorem: (Eisenstein kriteri):

R, TAGB ve $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$ ve $c(f) = 1$ (ilkel) olsun. Aşağıdaki şartlayan bir $\pi \in R$ asal elemanı varsa, $f(x)$ polinomu asaldır.

i - $\pi \mid a_0, a_1, \dots, a_{n-1}$

ii - $\pi \nmid a_n$

iii - $\pi^2 \nmid a_0$

Örnek: // $P(X) = 12 + 6X + 15X^2 + 7X^3 \in \mathbb{Z}[X]$ $\mathbb{Z}, \text{TAGB}$.

$$c(P) = 1 \quad \pi = 3, \quad 3 \mid 12, 6, 15 \quad 3 \nmid 7 \quad 3^2 = 9 \nmid 7$$

$\Rightarrow p \in \mathbb{Z}[x]$ de asaldır.

Sonuç: R nin kesir cismi F ise; $f, F[x]$ de de asaldır. (Aynı koşullarda)

Aynı örnek için;

$\mathbb{Q}, \mathbb{Z}$ nin bir kesir cismi olduğundan, $p(x), \mathbb{Q}[x]$ de de asaldır. //

{	$I \subset R$ ideal $a, b \in R, a, b \in I$	}	Asal ve maksimal ideallerle ilgili.
{	$2 \cdot 4 = 8 \quad 2, 4 \notin \langle 8 \rangle$	}	
{	$\mathbb{Z}$ de $\langle 8 \rangle$ ideali asal değildir.	}	

Asal ve maksimal idealler

5.6.96 / P.tesi

Tanım: R , birimli ve değişmeli bir halka, $\forall a, b \in R$,
 $ab \in P \Rightarrow a \in P$ veya $b \in P$

İse P ye R nin bir asal ideali denir.

Örnek // $mn \in \langle P \rangle \Rightarrow p | mn \Rightarrow p | m$ veya $p | n$ (p , asal)

Önerme: R , T.B. olsun. $a \in R$ için,

$\langle a \rangle$ asal idealdir $\Leftrightarrow a$ asal elementtir.

İspat // $\Rightarrow$: $\langle a \rangle$ asal ideal olsun.

$a = \pi_1 \pi_2 \dots \pi_r$ o.s. $\exists \pi_i \in R$. (asal element)

$r \geq 2$ olsa, $b = \pi_1$ ve $c = \pi_2 \pi_3 \dots \pi_r$ olsun.

$a = bc \in \langle a \rangle \Rightarrow$ ya $b \in \langle a \rangle$ veya $c \in \langle a \rangle$.

$b \in \langle a \rangle$ olsa $a | b^{\text{asal}}$ # (ya ilgili ya da Ur olmalı.)
 olur ki, b asal olduğundan $a \in Ur$ veya $a \approx b$.

$\Rightarrow \langle a \rangle = \langle \pi_1 \rangle$

$c \in \langle a \rangle$ olsa $b = \pi_2$ ve $c = \pi_3 \pi_4 \dots \pi_r$ diyelim. // tege!

$c = b_1 c_1 \in \langle a \rangle \Rightarrow b_1 \in \langle a \rangle$ veya $c_1 \in \langle a \rangle$ # -----

benzer şekilde devam edersek ---

$\Rightarrow r = 1$ ve a asaldır.

$\Leftarrow$: a asal element olsun. $xy \in \langle a \rangle \Rightarrow a | xy \Rightarrow a | x$ veya $a | y$ dir. (tanımdan) $\Rightarrow a$ asal idealdir.

Önerme: R birimli ve değişmeli bir halka, $P \subsetneq R$ ideali olsun.

P asal ideal $\Leftrightarrow R/P$ T.B. dir.

İspat // $\left\{ \begin{array}{l} \text{T.B. de sıfırdan oluşan ideal, asal idealdir.} \\ ab = 0_R \quad I = \{0_R\} = \langle 0_R \rangle \end{array} \right\} \star$

R birimli ve değişmeli $\Rightarrow$ Bölüm halkası da birimli ve değişmelidir.

$\Rightarrow$: P asal ideal olsun. R/P de birimli ve değişmelidir.

$\forall a+P, b+P \in R/P,$

$$(a+P)(b+P) = P \Rightarrow ab+P = P \Rightarrow ab \in P$$

$\Rightarrow P$ asal olduğundan, $a \in P$ veya $b \in P$.

$$\Rightarrow a+P = P \text{ veya } b+P = P.$$

$\Rightarrow R/P$ sıfır bölensizdir. T.B. dir.

$\Leftarrow$: R/P T.B. olsun.

$\forall a, b \in R$ için $ab \in P$ olsun.

$$\Rightarrow ab+P = P \Rightarrow (a+P)(b+P) = P$$

$$\Rightarrow a+P = P \text{ veya } b+P = P \quad (\text{hipotezden})$$

$$\Rightarrow a \in P \text{ veya } b \in P \Rightarrow P \text{ asal idealdir.} //$$

Önerme : R , T.B. olsun. $\forall \langle a \rangle \neq \langle 0 \rangle \subsetneq R$ (birden farklı) ideali
asal elemanların çarpımı şeklinde yazılabilir. Bu yazılış, sıra
gözetmeksizin tek türdür.

İspat // $a = \pi_1 \pi_2 \dots \pi_r$ o.ş. $\exists \pi_i \in R$. (asal eleman)

$$\langle a \rangle = \langle \pi_1 \pi_2 \dots \pi_r \rangle = \langle \pi_1 \rangle \langle \pi_2 \rangle \dots \langle \pi_r \rangle$$

$$\pi_1 \pi_2 \dots \pi_r \in \langle \pi_1 \rangle \langle \pi_2 \rangle \dots \langle \pi_r \rangle \quad (\text{aH küme } \subseteq \text{ oldu.})$$

$x \in \langle \pi_1 \rangle \langle \pi_2 \rangle \dots \langle \pi_r \rangle$ alalım.

$$x = \sum_{i=1}^m (\pi_1 k_{1i})(\pi_2 k_{2i}) \dots (\pi_r k_{ri}) \quad k_{ji} \in R$$

$$= \sum_{i=1}^m (\pi_1 \pi_2 \dots \pi_r) (k_{1i} k_{2i} \dots k_{ri})$$

$$= (\pi_1 \pi_2 \dots \pi_r) \sum_{i=1}^m (k_{1i} k_{2i} \dots k_{ri})$$

$$= (\pi_1 \pi_2 \dots \pi_r) a \in \langle \pi_1 \pi_2 \dots \pi_r \rangle //$$

Tanım: R birimli ve değişmeli bir halka, $M \subsetneq R$ idealine, maksimal ideal denir. Eğer, R nin M yi kapsayan M ve R den başka ideali yoksa.

$$M \subset \overset{\text{varsa}}{I} \subset R \Rightarrow \text{ya } I=M \text{ veya } I=R \text{ dir.}$$

Önerme: $M \subsetneq R$ olsun.

$$M \text{ maksimaldir} \Leftrightarrow \forall x \in R \setminus M \text{ için, } M + \langle x \rangle = R.$$

$$\text{İspat} // \Rightarrow: \forall x \in R \setminus M \text{ için, } M \subsetneq \underbrace{M + \langle x \rangle}_{\text{ideal}}$$

$$x = 0_R + x \cdot 1_R \text{ olursa } M \subset I \text{ olamaz. } M=R \text{ olmalıdır.}$$

$$\Leftarrow: M \subsetneq I \text{ (} I, M \text{ yi kesin kapsarsa } I=M \text{ olur.)}$$

$$\Rightarrow \forall x \in I \setminus M \text{ hipotezden, } M + \langle x \rangle = \underline{R \subset I}$$

$$\left. \begin{array}{l} M \subset I \\ \langle x \rangle \subset I \end{array} \right\} \Rightarrow M + \langle x \rangle = I$$

$$I \text{ ideal olduğundan } \underline{I \subset R}$$

$$\left\{ \begin{array}{l} I \text{ asal} \Rightarrow R/I \text{ T.B idi.} \end{array} \right.$$

$$\text{Her iki kapsamadan } I=R \text{ dir.} //$$

Önerme: $M \subsetneq R$ ideali olsun.

$$M \text{ maksimaldir} \Leftrightarrow R/M \text{ cisimdir.}$$

İspat // $\Rightarrow: M$ maksimal olsun.

R birimli ve değişmeli iken R/M de birimli ve değişmeli idi. O halde yalnızca, sıfırdan farklı her elemanın terslenebilir olduğunu gösterirsek, R/M cisim olur.

$$\forall m \neq a + M \in R/M \text{ için } a \notin M \text{ ve } a \in R$$

$$\text{hipotezden, } \langle a \rangle + M = R \Rightarrow 1_R \in \langle a \rangle + M$$

$$\Rightarrow 1_R = ax + m \text{ o.ş } \exists m \in M, \exists x \in R.$$

$$\Rightarrow 1_R + M = (ax + m) + M$$

$$= (ax + M) + (\underbrace{m + M})$$

$$= (ax + M)$$

$$\Rightarrow 1_R + M = (a + M)(x + M)$$

Ve buradan $(a + M)^{-1} = x + M \in R/M$ dir. R/M cisim olur.

$\Leftarrow$: R/M cisim olsun.

$M \subsetneq I$ ideal olsun. $\exists x \in I \setminus M$ alalım. Bu durumda

$$\Rightarrow x + M \neq M$$

R/M cisim olduğundan,

$$(x + M)(r + M) = 1_R + M \text{ o.ş. } \exists M \neq r + M \in R/M.$$

$$\Rightarrow rx + M = 1_R + M$$

$$\Rightarrow 1_R - rx \in M$$

$$\Rightarrow 1_R - rx = m \text{ o.ş. } \exists m \in M$$

$$\Rightarrow 1_R = m + rx$$

$$\Rightarrow 1_R \in M + \langle x \rangle = R$$

Bir önceki önermeden, M maksimal idealdir. //

Örnek // $\mathbb{Z}$ de $\langle 5 \rangle$ bir maksimal idealdir.

$\forall a \in \mathbb{Z} - \langle 5 \rangle$ için, $\langle 5 \rangle + \langle a \rangle = \mathbb{Z}$ dir. Gerçekten,

ebob(5, a) = 1 dir. $1 = 5x + ay$ o.ş. $\exists x, y \in \mathbb{Z}$.

$$\langle 5 \rangle + \langle a \rangle = \langle 1 \rangle = \mathbb{Z} \text{ dir.}$$

$\left\{ \begin{array}{l} R/M \text{ cisim, } I = \{M\} \text{ veya } J = R/M \\ R/M \text{ nin her ideali } M \subsetneq K \subsetneq R \text{ o.ş. } K/M \text{ şeklinde idi.} \\ K = M \text{ veya } K = R \text{ dir.} \end{array} \right\}$

Sonuç : Her maksimal ideal bir asal idealdir. (Tersi doğru değildir.)

İspat // M maksimal ideal $\Rightarrow R/M$ cisim (ve T.B) dir. (önermeden)

$\Rightarrow M$ asal idealdir. (önermeden)

Eğer halka, T.Ü.B $\Rightarrow M$ ideali maksimaldir. //

Çözümlü Sorular :

16.6.96 / Pazar.

1- $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ ise $\mathbb{Z}_2[x]/\langle f(x) \rangle$ bölüm halkasını bulunuz ve cisim olup olmadığını gösteriniz.

Çözüm // $\mathbb{Z}_2$ cisim olduğundan ($\mathbb{Z}_2 = \{0, 1\}$), tan temsilciler sisteminde $d \circ f$ o.s. $\exists r(x) \in \mathbb{Z}_2[x]$.

$$T.T.S = \{ \bar{a} + \bar{b}x \mid a, b \in \mathbb{Z}_2 \} = \{ \bar{0}, \bar{1}, x, \bar{1} + x \}$$

$$\mathbb{Z}_2[x]/\langle f(x) \rangle = \{ \langle f \rangle, \bar{1} + \langle f \rangle, x + \langle f \rangle, \bar{1} + x + \langle f \rangle \} \text{ olur.}$$

Cisim olduğunu göstermek için ; $\forall a \in \mathbb{Z}_2[x]/\langle f(x) \rangle$ için , $a^{-1} \in \mathbb{Z}_2[x]/\langle f(x) \rangle$ 'in var olduğunu göstermeliyiz. Bunun için bölüm halkasının sıfırı olan $\langle f \rangle$ çıkarıldıktan sonra geri kalan elemanların çarpım tablosu aşağıdaki gibidir.

0	$\bar{1} + \langle f \rangle$	$x + \langle f \rangle$	$\bar{1} + x + \langle f \rangle$
$\bar{1} + \langle f \rangle$	$\bar{1} + \langle f \rangle$	$x + \langle f \rangle$	$\bar{1} + x + \langle f \rangle$
$x + \langle f \rangle$	$x + \langle f \rangle$	$\bar{1} + x + \langle f \rangle$	$\bar{1} + \langle f \rangle$
$\bar{1} + x + \langle f \rangle$	$\bar{1} + x + \langle f \rangle$	$\bar{1} + \langle f \rangle$	$x + \langle f \rangle$

Tablodan, $\mathbb{Z}_2[x]/\langle f \rangle$ nin sıfırdan farklı elemanlarının çarpmaya göre değişmeli grup olduğu anlaşıyor. O halde $\mathbb{Z}_2[x]/\langle f(x) \rangle$ cisimdir. //

2- $\mathbb{Q}[x]/\langle x^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}]$ olduğunu gösterin. Buna göre

$\mathbb{Q}[\sqrt{2}]$ bir cisim olur mu ?

Çözüm // $\phi : \mathbb{Q}[x] \rightarrow \mathbb{Q}[\sqrt{2}]$
 $f(x) \rightarrow \phi(f(x)) = f(\sqrt{2})$ olsun.

ϕ fonksiyonunun , örten homomorfizma olduğunu gösterelim.

$\forall f(x), g(x) \in \mathbb{Q}[x]$, (homomorfizma teoremini kullanacağız.)

$$\bullet \phi(f(x) + g(x)) = \phi((f+g)(x)) = (f+g)(\sqrt{2}) = f(\sqrt{2}) + g(\sqrt{2}) = \phi(f(x)) + \phi(g(x))$$

$$\phi(f(x) \cdot g(x)) = \phi((fg)(x)) = (fg)(\sqrt{2}) = f(\sqrt{2}) \cdot g(\sqrt{2}) = \phi(f(x)) \cdot \phi(g(x))$$

$\Rightarrow \phi$ homomorfizmadır.

• $\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ için $f(x) = \sqrt{2}$: sabit polinomu alınırsa ,

$$\phi(f(x)) = f(\sqrt{2}) = \sqrt{2} \text{ yani } \underline{\text{örten}} \text{ olduğu görülür.}$$

• Şek $\phi = 0 \Leftrightarrow f(\sqrt{2}) = 0$

$$\Leftrightarrow f(x) = (x^2 - 2)h(x) \text{ o.s. } \exists h(x) \in \mathbb{Q}[x].$$

$$\Leftrightarrow f(x) \in \langle x^2 - 2 \rangle$$

$$\Leftrightarrow \text{şek } \phi = \langle x^2 - 2 \rangle$$

olduğundan , $\phi : \mathbb{Q}[x] \rightarrow \mathbb{Q}[\sqrt{2}]$ örten homomorfizma ve

şek $\phi = \langle x^2 - 2 \rangle$ olduğundan , Homomorfizma Teoremi gereğince ,

$$\mathbb{Q}[x] / \langle x^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}] \text{ olur. //}$$

Buna göre $\mathbb{Q}[\sqrt{2}]$ cisim olur. Çünkü :

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

$\forall a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ alalım. $(a + b\sqrt{2})^{-1} \in \mathbb{Q}[\sqrt{2}]$ olduğunu göstermeliyiz.

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2 - 2b^2}}_{\in \mathbb{Q}} \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

o halde $\mathbb{Q}[\sqrt{2}]$ cisimdir. //

3 - $x^4 + 1$ polinomu ; $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ de asal mıdır ?

Çözüm // $x^4 + 1$ polinomunda $\nexists 1$ kök değildir. Şu halde $x^4 + 1$ 'in

$\mathbb{Z}[x]$ de ve $\mathbb{Q}[x]$ de birinci dereceden çarpanları olamaz.

2. derece çarpanlarının olup olmadığına bakalım.

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d) \text{ o.s. } \exists a, b, c, d \in \mathbb{Z}^? ?$$

$$x^4 + 1 = x^4 + (a+c)x^3 + (d+ac+b)x^2 + (bc+ad)x + bd$$

ve katsayılar karşılaştırılırsa, $bd = 1$, $a+c = 0$, $d+ac+b = 0$

$$\Rightarrow b = d = 1 \text{ veya } b = d = -1, a = -c \text{ bulunur.}$$

$$ac + 2 = 0 \Rightarrow \underline{a^2 = 2} \text{ ve } \underline{ac - 2 = 0} \Rightarrow \underline{a^2 = -2}$$

olacak şekilde $a, b, c, d \in \mathbb{Z}$ bulunamaz.

Bu halde x^4+1 polinomu $\mathbb{Z}[x]$ de ve $\mathbb{Q}[x]$ de asaldır. (Çarpanlara ayrılmadığı için.)

$$x^4+1 = (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1) \quad \mathbb{R}[x] \text{ de çarpanlara ayrılabilir.}$$

$\Rightarrow \mathbb{R}[x]$ de bu polinom asal değildir.

4- F cisim ise $F[x]$ E.B. olur mu? Neden.

Çözüm, F cisim ise $F[x]$ E.B. dir. Çünkü ;

E.B. tanımını hatırlayalım :

R , T.B ve N de R üzerinde tanımlı çarpımsal norm olsun.

i- $N(x) \geq 0, \forall x \in R.$

ii- $N(x) = 0 \Leftrightarrow x = 0_R$

iii- $N(xy) = N(x) \cdot N(y), \forall x, y \in R.$

iv- $\forall x, y \in R, (y \neq 0) \quad x = qy + r$ ve $0 \leq N(r) < N(y)$ o.s $\exists q, r \in R.$

Burada $N: R \rightarrow \mathbb{Z}$ tanımlı, çarpımsal normdur. Bu özellikleri sağlayan R 'ye Euclidean Bölgesi (E.B.) denir.

Sorumuza dönelim. F cisim olduğu için, aynı zamanda T.B. olur.

$$N: F[x] \rightarrow \mathbb{Z}$$

$$p(x) \mapsto N(p(x)) := 2^{d^0 p} \quad \text{şeklinde tanımlayalım.}$$

i- $\forall p(x) \in F[x], p(x) \neq 0$ olsun $\Rightarrow d^0(p(x)) \geq 0 \Rightarrow 2^{d^0 p(x)} > 0$

$$\Rightarrow N(p(x)) > 0$$

ii- $p(x) = 0 \Rightarrow N(p(x)) = 2^{-\infty} = 0$ (sıfır polinomun derecesi $-\infty$ dir.)

$$2^{d^0 p} = 0 \Rightarrow d^0 p = -\infty \Rightarrow p(x) = 0$$

$$\text{yani } N(p(x)) = 0 \Leftrightarrow p(x) = 0 \text{ olur.}$$

iii- $N(pq) = 2^{d^0(pq)} = 2^{d^0 p + d^0 q} = 2^{d^0 p} \cdot 2^{d^0 q} = N(p)N(q)$

$$(F, \text{T.B. olduğundan ; } d^0(pq) = d^0 p + d^0 q)$$

iv- Halkalarda kalanlı bölme yapılabiliyorduk.

p 'yi q 'ya kalanlı olarak bölelim.

$\Rightarrow p(x) = f(x)q(x) + r(x)$ ve $d^{\circ}r < d^{\circ}q$ yazabiliriz.

$$\parallel \\ 3^{d^{\circ}r} < 3^{d^{\circ}q} \Rightarrow N(r) < N(q) //$$

0 halde F cismi, E.B. olma şartlarını sağladığından E.B. olur.

5- TAÇB olduğu halde TÜİB olmayan halkaya bir örnek verin.

Örneğin, neden TÜİB olmadığını açıklayın.

Gözüm, $F[x,y]$ TAÇB dir, fakat TÜİB değildir. Çünkü, $\langle x,y \rangle$

tek eleman tarafından üretilemez. $x,y \in \langle x,y \rangle = \langle f(x,y) \rangle$

olduğunu varsayarsak, (tek elemanla üretildiğini varsayalım.)

$$x = f(x,y)h(x,y) \text{ ve } y = f(x,y)g(x,y) \text{ o.s. } \exists g(x,y), h(x,y) \in F[x,y]$$

bulunabilirdi. Halbuki,

$$x = f(x,y)h(x,y) \Rightarrow h(x,y) = \text{sabit ve } f(x,y) \text{ } x\text{'e bağılı.}$$

$$y = f(x,y)g(x,y) \Rightarrow g(x,y) = \text{sabit ve } g(x,y) \text{ } y\text{'ye bağılı. } \#$$

olacağından, $f(x,y)$ tek bir eleman tarafından üretilemez. //

6- Kesir cismini tanımlayınız ve bir örnek verin.

Gözüm, D bir T.B. olsun. $D^* := D - \{0\}$ ile gösterelim.

$D \times D^* = \{(a,b) \mid a,b \in D, b \neq 0\}$ kümesi üzerinde bir denklik

bağıntısını aşağıdaki gibi tanımlayalım :

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc$$

(a,b) nin denklik sınıfını da ;

$$\frac{a}{b} := (a,b)$$

ile gösterelim. Denklik sınıflarının kümesini ise ;

$$F_D := \left\{ \frac{a}{b} \mid a,b \in D \mid b \neq 0 \right\}$$

ile gösterelim. F_D üzerinde iki işlem tanımlayalım :

$$\frac{a}{b} \oplus \frac{c}{d} := \frac{ad+bc}{bd}, \quad \frac{a}{b} \odot \frac{c}{d} := \frac{ac}{bd}$$

olsun.

F_0 kümesi birinci işleme göre değişmeli (abel) grubu ve ikinci işlemin, birinci işlem üzerine sağdan ve soldan dağılıma özellikleri bulunduğu için, $(F_0, \oplus, \odot)$ yapısı bir cisimdir.

$$\varphi: D \longrightarrow F_0$$

$$x \longmapsto \varphi(x) = (\overline{x}, 1) := \frac{x}{1}$$

ile tanımlı φ fonksiyonu 1:1 ve homomorfizmadır. (monomorfizma)
Dolayısıyla D, F_0 içine gömülebilir. Bu F_0 cismine, D T.B.'nin kesir cismi denir.

$\mathbb{Z}$ nin kesir cismi $\mathbb{Q}$ dur. //

7 - $\mathbb{Z}[i]$ nin birim grubunu belirtin. Buna göre $2+3i$ ile ilgili olan elemanları belirtin. (161/13)

Gözüm // $\mathbb{Z}[i]$ bir E.B. olduğundan, $(N: \mathbb{Z}[i] \rightarrow \mathbb{Z}$ çarpımsal norm)

$\alpha = a+bi \in \mathbb{Z}[i]$ de aritmetik birim $\Leftrightarrow N(\alpha) = 1$ olmasıdır. (Burada $\mathbb{Z}$, bir T.B. olduğum da bilinmelidir.)

$$a, b \in \mathbb{Z}, \alpha = a+bi \Rightarrow N(\alpha) = \alpha \cdot \overline{\alpha} = a^2 + b^2 = 1$$

$$\Rightarrow a = \pm 1, b = 0 \text{ veya } a = 0, b = \pm 1$$

$$\Rightarrow U_{\mathbb{Z}[i]} = \{1, -1, i, -i\}$$

$$2+3i \approx x \stackrel{\text{tn.}}{\Leftrightarrow} x = (2+3i)u \text{ o.p. } \exists u \in U_{\mathbb{Z}[i]}.$$

$$\Rightarrow x_1 = (2+3i)(1) = 2+3i \in \mathbb{Z}[i]$$

$$\Rightarrow x_2 = (2+3i)(-1) = -2-3i \in \mathbb{Z}[i]$$

$$\Rightarrow x_3 = (2+3i)(i) = -5+2i \in \mathbb{Z}[i]$$

$$\Rightarrow x_4 = (2+3i)(-i) = 5-2i \in \mathbb{Z}[i]$$

$2+3i$ ile ilgili elemanlar: $2+3i, -2-3i, -5+2i, 5-2i$

$$\widetilde{2+3i} = \{\overline{2+3i}, \overline{-2-3i}, \overline{-5+2i}, \overline{5-2i}\}$$

dir. //

8- x^4+4 polinomu; $\mathbb{R}[x]$, $\mathbb{Q}[x]$ ve $\mathbb{Z}[x]$ de asal mıdır?

Gözüm,, $p(x)=x^4+4$ ebob(a,b,c,d,e) = 1 $\Rightarrow e(p(x))=1$

$$= ax^4+bx^3+cx^2+dx+e \Rightarrow p(x) \text{ ilkel polinomdur.}$$

$p(x)$ ilkel polinomu, $\mathbb{Q}[x]$ de asal $\Leftrightarrow \mathbb{Z}[x]$ de asal.

Burada $\mathbb{Q}, \mathbb{Z}$ nin kesir cismi olduğu için teoremden dolayı bunu söylüyoruz.

$$\begin{aligned} x^4+4 &= (x^2+ax+b)(x^2+cx+d) \\ &= (x^2+2x+2)(x^2-2x+2) \end{aligned}$$

Bu polinom çarpanlara ayrıldığı için $\mathbb{Z}[x]$ de ve dolayısıyla (teorem gereği $\mathbb{Z}$ nin kesir cismi $\mathbb{Q}$ olduğundan),

$\mathbb{Q}[x]$ de asal değildir. Aynı şekilde $\mathbb{R}[x]$ de de asal olmaz. //

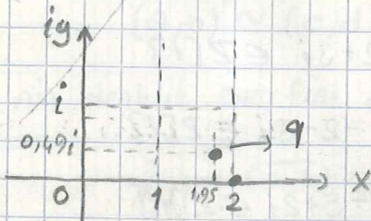
9- $\mathbb{Z}[i]$ de, ebob($10-i, 20+3i$) = ?

Gözüm,, $10-i$ ve $20+3i$ elemanlarının ebob'ini, bölme algoritması ile bulalım.

$\alpha=20+3i \in \mathbb{Z}[i]$ ve $\beta=10-i \in \mathbb{Z}[i]$ için,

$$\frac{\alpha}{\beta} = \frac{20+3i}{10-i} = \frac{(20+3i)(10+i)}{(10-i)(10+i)} = \frac{197+50i}{101} = \frac{197}{101} + \frac{50}{101}i$$

$$\approx 1,95 + 0,49i \Rightarrow q=2 \text{ alalım. (en yakın köşe)}$$



$$\alpha = q\beta + r \text{ den}$$

$$\Rightarrow 20+3i = 2 \cdot (10-i) + r$$

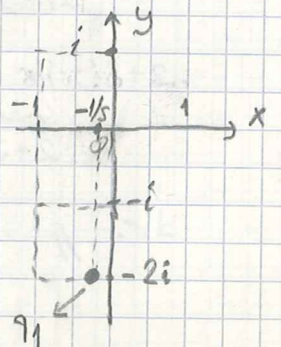
$$\Rightarrow 20+3i - 20+2i = r$$

$$\Rightarrow r = 5i$$

$\alpha_1=10-i$ $\beta_1=5i$ dersek,

$$\frac{\alpha_1}{\beta_1} = \frac{10-i}{5i} = \frac{(10-i)(-5i)}{25} = \frac{-5-50i}{25} = -\frac{1}{5} - 2i$$

$q_1=-2i$ (en yakın köşe) alalım.



$$\alpha_1 = q_1 \beta_1 + r_1 \Rightarrow (10-i) = (-2i)(5i) + r_1$$

$$\Rightarrow 10-i = 10 + r_1$$

$$\Rightarrow 10-i - 10 = r_1$$

$$\Rightarrow r_1 = -i$$

$$\alpha_2 = 5i, \beta_2 = -i \text{ dersek,}$$

$$\bullet \frac{\alpha_2}{\beta_2} = \frac{5i}{-i} = \frac{5i(i)}{(-i)(i)} = \frac{-5}{1} = -5 = q_2 \text{ diyelim. (en yakın köse) kendisi.}$$

$$\alpha_2 = q_2 \beta_2 + r_2 \Rightarrow 5i = (-5)(-i) + r_2$$

$$\Rightarrow 5i = 5i + r_2$$

$$\Rightarrow r_2 = 0 \text{ (tam olarak bölünmüş oldu.)}$$

0 halde, ebob $(20+3i, 10-i) = -i$ bulunur. //

10- $\mathbb{C}$ 'de bir asal idealin maksimal olduğunu gösterin. (185/3)

Çözüm // $\langle 0_R \rangle \neq I$ bir asal ideal olsun. $R, \mathbb{C}$ olduğundan,

$I = \langle a \rangle$ o.s. $\exists 0 \neq a \in R$. ($R, \mathbb{C}$ ve $I = \langle a \rangle$ asal ideal $\Leftrightarrow a \in R$ asal

$\forall x \in R \setminus I$ alalım. $\Rightarrow x \notin \langle a \rangle$

$\Rightarrow a \nmid x$ ve a asal olduğundan, $(a, x) = 1$ dir.

$\Rightarrow 1 = au + xr$ o.s. $\exists u, r \in R$.

$\Rightarrow 1 \in \langle a \rangle + \langle x \rangle$

$\Rightarrow \langle a \rangle + \langle x \rangle = R$

$\Rightarrow I + \langle x \rangle = R$, (önermeden) I maksimaldir. //

11- $\mathbb{Q}[x] / \langle x^4 - 22x^2 + 1 \rangle$ cisim midir ?

Çözüm // $f(x) = x^4 - 22x^2 + 1$ polinomunda $\nexists 1$ kök değildir. 0 halde

Bu polinomun $\mathbb{Q}[x]$ de birinci dereceden çarpanları olamaz.

2. dereceden çarpanlarının olup, olmadığına bakalım.

$$x^4 - 22x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

$$= x^4 + (a+c)x^3 + (d+ac+b)x^2 + (bc+ad)x + bd$$

ve katsayılar karşılaştırılırsa,

$$a+c=0, d+ac+b=-22, bc+ad=0, bd=1$$

$$a=-c, b=d=1 \text{ veya } b=d=-1$$

$$ac+2=-22 \Rightarrow a^2=24 \Rightarrow a=2\sqrt{6}, c=-2\sqrt{6}$$

$$ac-2=-22 \Rightarrow a^2=20 \Rightarrow a=2\sqrt{5}, c=-2\sqrt{5}$$

$a, c \notin \mathbb{Q}$ olduğundan, $x^4 - 22x^2 + 1$ polinomu $\mathbb{Q}[x]$ de çarpanlara ayrılmadığından asaldır.

$\mathbb{Q}[x]$, TüİB. ve $x^4 - 22x^2 + 1$ asal $\Leftrightarrow \langle x^4 - 22x^2 + 1 \rangle$ asal ideal

$\Leftrightarrow \langle x^4 - 22x^2 + 1 \rangle$ maksimal ideal

$\Leftrightarrow \mathbb{Q}[x] / \langle x^4 - 22x^2 + 1 \rangle$ cisimdir. //

12- $\mathbb{Z}_5[x] / \langle x^3 + 2x + 2 \rangle$ cisim midir?

Gözüm, $x^3 + 2x + 2$ monik polinomunun derecesi 3 olduğundan

2. dereceden çarpanları bulunamaz. Sabit terimi $\bar{2}$ olduğundan

bu polinomun rasyonel bir kökü varsa, bu kök bir tamsayı

ve $\bar{2}$ nin bölenleri olabilir. 2'nin bölenleri $\bar{1}, \bar{2}$ ve

bunlar kök olmadığından, $x^3 + 2x + 2$ polinomunun $\mathbb{Z}_5$ de

köleri yoktur ve dolayısıyla $\mathbb{Z}_5[x]$ de, verilen polinom

asaldır.

$\mathbb{Z}_5$ bir cisim $\Rightarrow \mathbb{Z}_5[x]$, TüİB dir.

$\mathbb{Z}_5[x]$ TüİB ve $x^3 + 2x + 2$ asal $\Leftrightarrow \langle x^3 + 2x + 2 \rangle$ asal ideal //

$\Leftrightarrow \langle x^3 + 2x + 2 \rangle$ maksimal ideal //

$\Leftrightarrow \mathbb{Z}_5[x] / \langle x^3 + 2x + 2 \rangle$ cisimdir. //