CEBİR I, CEVAP ANAHTARI
(ARASINAV)

22.11.2018
Perşembe

1) a) $m,n \in G$ olsun. $o(mnm^{-1})=k$ ve $o(n)=\ell$ olsun. Mertebe pozitif tamsayı olduğundan $k=\ell$ olduğunu göstermek için $k|\ell$ ve $\ell|k$ olduğunu göstermeliyiz.

$$o(mnm^{-1})=k \Rightarrow (mnm^{-1})^k = e$$
$$\Rightarrow \underbrace{(mnm^{-1})(mnm^{-1})\cdots(mnm^{-1})}_{k \text{ tane}} = e$$
$$\Rightarrow mn(\underbrace{m^{-1}m}_{e})n(\underbrace{m^{-1}m}_{e})\cdots(\underbrace{m^{-1}m}_{e})nm^{-1}=e$$
$$\Rightarrow mn^k m^{-1}=e \quad \text{soldan } m$$
$$\Rightarrow n^k m^{-1}=m^{-1}$$
$$\Rightarrow n^k = e \Rightarrow \ell|k \quad ...(1)...$$

şimdi de

$$(mnm^{-1})^{\ell} = \underbrace{(mnm^{-1})(mnm^{-1})\cdots(mnm^{-1})}_{\ell \text{ tane}}$$
$$= mn(m^{-1}m)n(m^{-1}m)\cdots(m^{-1}m)nm^{-1}$$
$$= mn^{\ell}m^{-1}$$
$$= mem^{-1}$$
$$= mm^{-1}=e \Rightarrow k|\ell \quad ...(2)...$$

(1) ve (2) den istenen eşitlik elde edilir.

b) $15x \equiv 5 (20)$ kongrüansının çözümü olması için $(15,20)=5|5$ olmalıdır. O halde kongrüansın mod 20 de 5 farklı kalan sınıf çözümü vardır.

$$15x \equiv 5(20) \iff 3x \equiv 1(4)$$
$$\bar{3}^{-1} = \frac{1}{3}(4) \equiv 3 \iff x \equiv 3(4)$$
$$\iff 4|x-3$$
$$\iff x-3=4k$$
$$\iff x=4k+3, \quad k=\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$$

$$\bar{x}=\bar{3},\bar{7},\bar{11},\bar{15},\bar{19}$$
$$\text{Ç.K} = \{\bar{3},\bar{7},\bar{11},\bar{15},\bar{19}\}$$

2) Öncelikle $gHg^{-1} \leq G$ old. gösterelim.

$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ olup G bir grup olduğundan $e \in G$ dir.

$H \leq G$ olduğundan aynı zamanda $e \in H$ olup $geg^{-1} \in gHg^{-1}$

$\Rightarrow gg^{-1} = e \in gHg^{-1}$ olur

$\Rightarrow gHg^{-1} \neq \emptyset$

$H \leq G$ olduğundan $\forall h \in H \Rightarrow h \in G$ olup $ghg^{-1} \in G \Rightarrow gHg^{-1} \subseteq G$

$\forall gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$ için

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1})$$
$$= gh_1(g^{-1}g)h_2^{-1}g^{-1}$$
$$= g(h_1h_2^{-1})g^{-1}$$

$H \leq G$ old. $h_1h_2^{-1} \in H$. $\in gHg^{-1}$ olup $gHg^{-1} \leq G$

Şimdi de $|gHg^{-1}| = |H|$ old. gösterelim.

$f : H \longrightarrow gHg^{-1}$

$h \longrightarrow f(h) = ghg^{-1}$ tanımlayalım

Kapalılık tanımdan açıktır

$h = h' \Rightarrow ghg^{-1} = gh'g^{-1}$ olup f iyi tanımlıdır

$f(h) = f(h') \Rightarrow ghg^{-1} = gh'g^{-1}$

soldan g^{-1} $\Rightarrow hg^{-1} = h'g^{-1}$

sağdan g $\Rightarrow h = h'$ olup f birebirdir

$\forall a \in gHg^{-1}$ için $a = ghg^{-1}, h \in H$ ol. $f(h) = ghg^{-1} = a$ var olduğundan

f örtendir O halde $|H| = |gHg^{-1}|$ bulunur

3) a) $\mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ olup

$\bar{2}^1 = 2$, $\bar{2}^2 = 4$, $\bar{2}^3 = 1$

$\bar{3}^1 = 3$, $\bar{3}^2 = 2$, $\bar{3}^3 = 6$, $\bar{3}^4 = 4$, $\bar{3}^5 = 5$, $\bar{3}^6 = 1$ $\Rightarrow \mathbb{Z}_7^* = \langle \bar{3} \rangle$

$\bar{4}^1 = 4$, $\bar{4}^2 = 2$, $\bar{4}^3 = 1$

$\bar{5}^1 = 5$, $\bar{5}^2 = 4$, $\bar{5}^3 = 6$, $\bar{5}^4 = 2$, $\bar{5}^5 = 3$, $\bar{5}^6 = 1$ $\Rightarrow \mathbb{Z}_7^* = \langle \bar{5} \rangle$

$\bar{6}^1 = 6$

$\bar{6}^2 = 1$

$$\mathbb{Z}_7^* = \langle \bar{3} \rangle = \langle \bar{5} \rangle$$

3) b) $85^{8579} \equiv x \ (53)$

$32^{8579} \equiv x \ (53)$ olup $(32,53)=1$ old. Euler Teo. göre

$32^{\varphi(53)} \equiv 1 \ (53)$

$\Rightarrow 32^{52} \equiv 1 \ (53)$

$(32^{52})^{164} \cdot (32)^{51} \equiv x \ (53)$

$32 / 1 \cdot (32)^{51} \overset{32}{\equiv} x \ (53)$

$1 \equiv 32x \ (53)$

$\Rightarrow 32x \equiv 1 \ (53)$

$\Rightarrow 53 \mid 32x-1$

$\Rightarrow 32x-1=53y$

$\Rightarrow 32x-53y=1$

$\Rightarrow \boxed{x=5}$

$53 = 1.32+21$
$32 = 1.21+11$
$21 = 1.11+10$
$11 = 1.10+1$

$1 = 11-1.10$
$1 = 11-(21-1.11)$
$1 = 2.11-21$
$1 = 2.(32-1.21)-21$
$1 = 2.32-3.21$
$1 = 2.32-3.(53-1.32)$
$1 = \underbrace{5}_{x}.32-\underbrace{3}_{y}.53$

4) a) Yarı grup olması için birleşmeli bir cebirsel yapı olması gerekir.

Kümenin boştan farklı old. açıktır. "Δ" işlemi de ikili işlem olduğundan $(Q^*-\{-1\}, \Delta)$ cebirsel yapıdır.

$\forall x,y,z \in Q^*-\{-1\}$ için

$(x \Delta y) \Delta z = (|x|.y) \Delta z = ||x|.y|.z = |x.y|.z$

$x \Delta (y \Delta z) = x \Delta (|y|.z) = |x|.|y|.z = |x.y|z$

$(x \Delta y) \Delta z = x \Delta (y \Delta z)$ olduğundan birleşme öğ. sağlar

$(Q^*-\{-1\}, \Delta)$ yarı gruptur

b) Birim elemanı olup olmadığına bakalım. Birim eleman olması için $\forall x \in Q^*-\{-1\}$ için $x \Delta e = x$ ve $e \Delta x = x$ o.ş $e \in Q^*-\{-1\}$ bulmalıyız.

$\forall x \in Q^*-\{-1\}$ için

$x \Delta e = x \Rightarrow |x|.e = x$ olmaz. Örneğin $x=-2$ için $2e=-2$
$\Rightarrow e=-1 \notin Q^*-\{-1\}$

old. birim elemanı yoktur

$(Q^*-\{-1\}, \Delta)$ grup değildir

5) a) $a \equiv b(m)$ olması için $(\Leftrightarrow)$ a ve b'nin m ile bölümünden elde edilen kalanların aynı olmasıdır.

Çözüm

$(\Rightarrow)$: $a \equiv b(m)$ olsun. a ve b'yi m ile kalanlı bölelim

$a = qm + r$ ve $b = q'm + r'$, $0 \le r < m$, $0 \le r' < m$ o.ş $\exists q, q', r, r' \in \mathbb{Z}$ var

$a \equiv b(m) \Rightarrow m \mid a-b \Rightarrow a-b = m \cdot t$ o.ş $t \in \mathbb{Z}$

$a - b = (qm+r) - (q'm+r')$ ve $a-b = m \cdot t$

$\Rightarrow qm - q'm + r - r' = m \cdot t$

$\Rightarrow (q - q' - t)m = r' - r$

$\Rightarrow m \mid r' - r \Rightarrow r' \equiv r(m)$

$r < m, r' < m$ olduğundan $\Rightarrow r' = r$

$(\Leftarrow)$ Tersine a ve b'nin m ile bölümünden elde edilen kalanlar aynı ve r olsun.

$a = qm + r$ ve $b = q'm + r$ yazılabilir

$\Rightarrow a - b = (q - q')m \Rightarrow m \mid a-b \Rightarrow a \equiv b(m)$

b) $G = \langle a \rangle$, m. mertebeden olduğundan $a^m = e$ dir

a^n'nin G'nin üreteci olduğunu göstermek için $G = \langle a \rangle = \langle a^n \rangle$ olduğunu göstermeliyiz

Keyfi bir $x \in \langle a^n \rangle \Rightarrow x = (a^n)^k$ o.ş $k \in \mathbb{Z}$.

$\Rightarrow x = a^{nk}$

$\Rightarrow x \in \langle a \rangle$ olup $\langle a^n \rangle \subseteq \langle a \rangle$ ... (1) ...

$(m,n) = 1$ olduğundan $mu + nv = 1$ o.ş $u, v \in \mathbb{Z}$ vardır.

Keyfi bir $y \in \langle a \rangle \Rightarrow y = a^t$ o.ş $t \in \mathbb{Z}$

$\Rightarrow y = (a^1)^t$

$\Rightarrow y = (a^{mu+nv})^t$

$\Rightarrow y = (a^m)^{ut} \bullet (a^n)^{vt}$

$\Rightarrow y = e \cdot (a^n)^{vt}$

$\Rightarrow y = (a^n)^{vt} \in \langle a^n \rangle$ olup $\langle a \rangle \subseteq \langle a^n \rangle$ ... (2)

(1) ve (2) den istenen eşitlik elde edilir

$G = \langle a \rangle = \langle a^n \rangle$ dir