Hatırlatma. Eğer $g^n = e$ eşitliğini sağlayan bir $n > 0$ varsa bu eşitliği sağlayan pozitif sayıların en küçüğüne g'nin *derecesi* (veya *mertebesi*) denir ve bu sayı $o(g)$ ile gösterilir. Eğer $g^n = e$ hiçbir $n > 0$ için sağlanmıyorsa, g'nin derecesi sonsuzdur deriz ve $o(g) = \infty$ yazarız.

Alıştırma 1. 4^{237}'nin $\pmod 5$'te neye denk geldiğini hesaplayalım. Yukarıdaki hatırlatmayı göz önünde bulundurarak, bu hesaplamayı grup teoritik olarak yorumlayalım.

Çözüm. Liseden de bildiğiniz gibi, böyle soruları çözerken, önce verilen sayının istenilen mod 'da en küçük hangi kuvvetinin 1'e denk geldiğini hesaplayıp, üssü ona göre düzenleyerek sonuca ulaşırız. Bu durumda

$$4.4 \equiv 1 \pmod 5 \Rightarrow 4^{237} = (4^2)^{118}.4 \equiv 1.4 \pmod 5 \equiv 4 \pmod 5$$

olarak buluruz. Dikkat edersek, burada yaptığımız aslında $(\mathbb{Z}_5^*, .)$ grubunda 4 elemanının derecesini bulmaktan başka bir şey değil. Yani bu grupta, $o(4) = 2$ ve derecenin tanımından $4^{o(4)} = 1$ olduğundan, istenilen hesabı kolayca bulabildik.

O zaman bu grupta 4'ün tersi nedir?

Alıştırma 2. G bir grup ve $x, y \in G$ olsun. Her $g \in G$ için, $o(x) = o(gxg^{-1})$ ve $o(xy) = o(yx)$ olduğunu gösterin.

Çözüm. Soruda verilen elemanların dereceleri için sonlu ya da sonsuz denmediğinden, her iki durum için de değerlendirme yapmalıyız. (**Dikkat:** Eğer G sonlu bir grup denmiş olsaydı, o zaman elemanların derecelerinin sadece sonlu olabileceğini anlardık. Neden?)

İlk olarak, $o(x) = \infty$ olsun. Varsayalım ki, $o(gxg^{-1}) \neq \infty$ olsun. O zaman

$$e = (gxg^{-1})^{o(gxg^{-1})} = \underbrace{(gxg^{-1})(gxg^{-1})\cdots(gxg^{-1})}_{o(gxg^{-1}) \text{ adet}} = gx^{o(gxg^{-1})}g^{-1} \Rightarrow e = x^{o(gxg^{-1})}$$

olur. Bu da x'in derecesinin sonsuz olması ile çelişir. Demek ki $o(gxg^{-1}) = \infty$ olmak zorundadır.

Benzer şekilde, $o(gxg^{-1}) = \infty$ ise $o(x) = \infty$ olduğunu da siz gösterin. Sonuç olarak,

$$o(gxg^{-1}) = \infty \Leftrightarrow o(x) = \infty$$

olduğunu göstermiş oluruz.

Şimdi, bir pozitif m tam sayısı için, $o(x) = m$ olsun. Bu durumda,

$$(gxg^{-1})^m = gx^m g^{-1} = geg^{-1} = e$$

elde ederiz. Bu da $o(gxg^{-1})|m$ olduğunu gösterir. Diğer taraftan,

$$e = (gxg^{-1})^{o(gxg^{-1})} = gx^{o(gxg^{-1})}g^{-1} \Rightarrow e = x^{o(gxg^{-1})}$$

olduğundan, $m|o(gxg^{-1})$ elde edilir. O halde $m = o(gxg^{-1})$ olur.

İstenilen diğer ifadeyi göstermek için, $o(x) = o(gxg^{-1})$ eşitliğinde x yerine xy, g yerine de y elemanlarını yazarsak işimiz biter.

Bu alıştırmadan sonra, derste verilen Alıştırma 2'yi çözmek kolay olacaktır.

Alıştırma 3. G bir grup, $a \in G$ ve $n > 0$ için, $o(a) = n$ olsun. Bir $k > 0$ için, $o(a^k) = \frac{n}{\text{ebob}(n,k)}$ olduğunu gösterin.

Çözüm. Bir $t > 0$ sayısı için, $o(a^k) = t$ olsun. ($o(a^k) = \infty$ olabilir mi? Neden?) Bu durumda,

$$e = (a^k)^t = a^{kt} \Leftrightarrow n|kt \Leftrightarrow \frac{n}{\text{ebob}(n,k)} | \frac{k}{\text{ebob}(n,k)} t \Leftrightarrow \frac{n}{\text{ebob}(n,k)} | t$$

olur. Son gerektirmenin sebebinin $\frac{n}{\text{ebob}(n,k)}$ tam sayısı ile $\frac{k}{\text{ebob}(n,k)}$ tam sayısının aralarında asal olması olduğuna dikkat edin.

Diğer yandan,

$$(a^k)^{\frac{n}{\text{ebob}(n,k)}} = (a^n)^{\frac{k}{\text{ebob}(n,k)}} = e^{\frac{k}{\text{ebob}(n,k)}} = e \Leftrightarrow t | \frac{n}{\text{ebob}(n,k)}$$

olur.

Sonuç olarak $n = \frac{n}{\text{ebob}(n,k)}$ olduğunu göstermiş olduk.

Bu alıştırmadan sonra, derste verilen Alıştırma 3'ü tekrar çözmeye çalışın.

Alıştırma 4. G abelyan bir grup, $g, h \in G$ ve g, h sonlu dereceli olsun. Eğer $\langle g \rangle \cap \langle h \rangle = \{e\}$ ise o zaman $o(gh) = \text{ekok}(o(g), o(h))$ olduğunu kanıtlayın. (Derste verilen Alıştırma 4)

Çözüm. $\text{ekok}(o(g), o(h)) = m$, $m > 0$ diyelim.

Biliyoruz ki, $m = o(g)r$ ve $m = o(h)s$ olacak şekilde r ve s tam sayıları vardır. Bu durumda,

$$(gh)^m = \underbrace{(gh)(gh)\cdots(gh)}_{m \text{ adet}} = \underbrace{g\cdots g}_{m \text{ adet}}\underbrace{h\cdots h}_{m \text{ adet}} = g^m h^m = g^{o(g)r} h^{o(h)s} = e^r e^s = e \Rightarrow o(gh)|m$$

olur. İkinci eşitliğin sebebinin G grubunun değişmeli olması olduğuna dikkat edin.

Diğer taraftan,

$$e = (gh)^{o(gh)} = g^{o(gh)} h^{o(gh)} \Rightarrow (g^{o(gh)})^{-1} = h^{o(gh)}$$

olur. Buradaki ikinci eşitlikte yine G'nin abelyan grup olduğunu kullandığımızı fark edin. Bu durumda, $(g^{o(gh)})^{-1} \in \langle h \rangle$ ve $(h^{o(gh)})^{-1} \in \langle g \rangle$ olur. Buradan, $\langle g \rangle \cap \langle h \rangle = \{e\}$ olduğundan, $g^{o(gh)} = e$ ve $h^{o(gh)} = e$ ifadelerini elde ederiz. Yani $o(g)|o(gh)$ ve $o(h)|o(gh)$'dir. Bu da, $m|o(gh)$ olmasını gerektirir.

Sonuç olarak, $m = o(gh)$ eşitliğini göstermiş olduk.

Hatırlatma. $(G, *)$ ve $(H, \diamond)$ iki grup olsun, her $(g_1, h_1), (g_2, h_2) \in G \times H$ eleman çifti için,

$$(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \diamond h_2) \in G \times H$$

işlemi altında $G \times H$ bir grup olur.

Alıştırma 5. $\mathbb{Z} \times \mathbb{Z}$ grubunu devirli olmadığını gösterin.(Derste verilen Alıştırma 8)

Çözüm. Varsayalım ki, $\mathbb{Z} \times \mathbb{Z}$ grubu devirli olsun ve bir $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ elemanı için, $\mathbb{Z} \times \mathbb{Z} = \langle (a, b) \rangle$ diyelim. O zaman, $(1, 0) \in \mathbb{Z} \times \mathbb{Z}$ olduğundan, bir $n > 1$ sayısı vardır öyle ki, $n(a, b) = (na, nb) = (1, 0)$ eşitliği sağlanır. (Neden $n = 1$ durumunu hesaba katmadık, düşünün!). Bu durumda, $na = 1$ ve $nb = 0$ olur ve buradan $b = 0$ olduğunu görürüz. Demek ki $\mathbb{Z} \times \mathbb{Z}$'nin üreteci $(a, 0)$ elemanıdır. Fakat, $(0, 1) \in \mathbb{Z} \times \mathbb{Z}$ olduğundan ve $m(a, 0) = (0, 1)$ eşitliğini sağlayan hiç bir m tam sayısı bulamayacağımızdan, $(a, 0)$ elemanı $\mathbb{Z} \times \mathbb{Z}$'yi üretmeye yetmez. Bu durumda $\mathbb{Z} \times \mathbb{Z}$ devirli bir grup olamaz.

Ancak $\mathbb{Z} \times \mathbb{Z}$'yi iki elemanla üretmek mümkündür. Örneğin,

$$\langle (1, 0), (0, 1) \rangle = \{m(1, 0) + n(0, 1) | m, n \in \mathbb{Z}\} = \{(m, n) | m, n \in \mathbb{Z}\} = \mathbb{Z} \times \mathbb{Z}$$

sağlanır. Burada ilk eşitliği yazarken, $\mathbb{Z}$'nin ve dolayısıyla $\mathbb{Z} \times \mathbb{Z}$'nin abelyan grup olmasını kullandığımızı fark edin. $\mathbb{Z} \times \mathbb{Z}$ grubu için iki elemanlı başka üreteç kümesi bulabilir misiniz?

Alıştırma 6. G bir grup olsun ve $D = \{(x, x) | x \in G\}$ kümesi tanımlansın. D'nin, $G \times G$ grubunun bir alt grubu olduğunu gösterin.

Çözüm. $(x, x), (y, y) \in D$ olacak şekilde iki eleman alalım. $(x, x)(y, y) = (xy, xy) \in D$ olduğundan kapalılık özelliği sağlanır.

$G \times G$'nin birim elemanı (e_G, e_G)'dir ve $(e_G, e_G) \in D$ sağlanır.

Herhangi bir $(x, x) \in D$ elemanı için, $(x, x)^{-1} = (x^{-1}, x^{-1})$ olur ve $(x^{-1}, x^{-1}) \in D$ sağlanır.

Alt grup olma kriterlerine bakarken, birleşme özelliğini kontrol etmeye gerek olmadığını daha önce söylemiştik.

Bu durumda $D \leqslant G \times G$ olduğunu göstermiş olduk.

Alıştırma 7. $\mathbb{Z}_{10} \times \mathbb{Z}_{75}$ grubundaki, $(5, 15), (3, 2)$ ve $(1, 1)$ elemanlarının derecelerini bulun.

Çözüm. $(5, 15) + (5, 15) = (0, 30),\ 3(5, 15) = (5, 45),\ 4(5, 15) = (0, 60),\ 5(5, 15) = (5, 0), \cdots,$ $9(5, 15) = (5, 60),\ 10(5, 15) = (0, 0)$ olur. Bu durumda $o((5, 15)) = 10$'dir ve $10 = \text{ekok}(o(5), o(15))$ olduğuna dikkat edin.

Benzer şekilde, $2(3, 2) = (6, 4), 3(3, 2) = (9, 6), \cdots, 10(3, 2) = (0, 20), \cdots,$
$75(3, 2) = (5, 0), \cdots, 150(3, 2) = (0, 0)$ olur. Yani $o(3, 2) = 150 = \text{ekok}(o(3), o(2))$ olur.

$(1, 1)$ elemanı için de siz hesaplayın ve buradan yola çıkarak derste bırakılan Alıştırma 7 ve 9'u rahatça çözebilirsiniz.