BÖLÜM **7**

EŞKÜMELER - LAGRANGE TEOREMİ

Bu bölümü bitirdiğinizde,

- bir grubun bir altkümesinin sol ve sağ eşkümeleri
- bir grubun bir altgrubunun sol ve sağ eşkümeleri
- eşkümelere parçalanış ve indeks kavramı
- Lagrange Teoremi ve bazı uygulamaları
- bir devirli grubun altgrupları, altgruplar kafesi
- Fermat'ın Küçük Teoreminin grup kuramsal kanıtı

hakkında bilgi sahibi olabileceksiniz.

BÖLÜM **7**

EŞKÜMELER - LAGRANGE TEOREMİ

Bu bölümde, gruplarla ilgili araştırmalarda en güçlü araçlardan biri olan *eşküme* kavramını sunacağız ve bu kavram yardımıyla sonlu gruplar kuramının en önemli teoremi olan *Lagrange Teoremi*'ni kanıtlayacağız. Eşküme kavramı, ilk kez 1830'larda, E. Galois tarafından kullanılmıştır.

Tanım 1. G bir grup, $A \subseteq G$ ve $x \in G$ olsun. Bu takdirde

$$xA = \{xa : a \in A\} \quad \text{ve} \quad Ax = \{ax : a \in A\}$$

tanımlanır. xA kümesine, *A nın, G içinde x tarafından belirlenen sol eşküme*si, Ax kümesine de *A nın, G içinde x tarafından belirlenen sağ eşküme*si denir. □

Örnek 1. $G = \mathcal{D}_4$, $A = \{t_1, k_1\}$ için $d_1A = \{k_2, t_1\}$, $Ad_1 = \{k_1, t_2\}$, $k_1A = \{d_3, d_0\}$, $Ak_1 = \{d_1, d_0\}$ dır.

Eşkümelerle ilgili bazı özellikleri aşağıdaki önermede özetliyoruz:

Önerme 1. *G bir grup; $A, B \subseteq G; x, y \in G$ olsun. Bu takdirde,*

(i) $eA = A$ $\qquad$ (ii) $x(yA) = (xy)A$

(iii) $\Lambda \subseteq B \iff x\Lambda \subseteq xB$ $\qquad$ (iv) $\Lambda \subseteq B \iff \Lambda x \subseteq Bx$

(v) $A = B \iff xA = xB$ $\qquad$ (vi) $A = B \iff Ax = Bx$

(vii) $|xA| = |A|$.

Kanıt. Sadece (iii) ve (vii) yi kanıtlayacağız; diğer şıkların kanıtını okuyucuya bırakacağız. $A \subseteq B$ ise, $xA \subseteq xB$ olduğu açıktır.

Diğer yandan, $xA \subseteq xB$ ise, $x^{-1}(xA) \subseteq x^{-1}(xB)$, yani $A \subseteq B$ olduğu görülür. Bu, (iii) yi kanıtlar. (vii) nin kanıtına gelince; her $a \in A$ için $f(a) = xa$ olarak tanımlanan $f : A \longrightarrow xA$ fonksiyonunu düşünelim. f, iyi tanımlı, bire-bir ve örten bir fonksiyondur. Dolayısıyla, $|xA| = |A|$ dır. ∎

Bu bölümde daha çok altgrupların eşkümeleri ile ilgileneceğiz.

Örnek 2. $G = \mathcal{D}_4$, $H = \{d_0, t_1\}$ için H nin $\mathcal{D}_4$ içindeki sol ve sağ eşkümeleri aşağıda listelenmiştir:

$$d_0H = H = \{d_0, t_1\} = t_1H \quad ; \quad Hd_0 = H = \{d_0, t_1\} = Ht_1,$$
$$d_1H = \{d_1, d_1t_1\} = \{d_1, k_2\} = k_2H \quad ; \quad Hd_1 = \{d_1, k_1\} = Hk_1,$$
$$d_2H = \{d_2, d_2t_1\} = \{d_2, t_2\} = t_2H \quad ; \quad Hd_2 = \{d_2, t_2\} = Ht_2,$$
$$d_3H = \{d_3, d_3t_1\} = \{d_3, k_1\} = k_1H \quad ; \quad Hd_3 = \{d_3, k_2\} = Hk_2. \qquad \square$$

Örnek 3. $G = \mathcal{S}_3$, $H = \{\imath, (2\ 3)\}$ için H nin $\mathcal{S}_3$ içindeki sol eşkümeleri aşağıda listelenmiştir:

$$\imath H = \{\imath, (2\ 3)\} = (2\ 3)H,$$
$$(1\ 2)H = \{(1\ 2), (1\ 2)(2\ 3)\} = \{(1\ 2), (1\ 2\ 3)\} = (1\ 2\ 3)H,$$
$$(1\ 3)H = \{(1\ 3), (1\ 3)(2\ 3)\} = \{(1\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H. \qquad \square$$

Toplamsal gösterimde, xH yerine $x + H$, Hx yerine $H + x$ yazılacağına dikkat ediniz.

Örnek 4. $\mathbb{Z}_{12}$ içinde $H = \{0, 4, 8\}$ in sol eşkümeleri aşağıda listelenmiştir:

$$0 + H = \{0, 4, 8\} = 4 + H = 8 + H,\ 1 + H = \{1, 5, 9\} = 5 + H = 9 + H,$$
$$2 + H = \{2, 6, 10\} = 6 + H = 10 + H,\ 3 + H = \{3, 7, 11\} = 7 + H = 11 + H.$$

Bu örnekte, her $x \in \mathbb{Z}_{12}$ için $x + II = II + x$ olduğuna dikkat ediniz. $\square$

Yukarıdaki örnekler, altgrupların eşkümelerinin bazı özelliklerini yansıtmakta ve bazı sorular akla getirmektedir. Önce, bir eşkümenin genelde

bir altgrup olmadığını görüyoruz. Bazı durumlarda, $xH = Hx$, fakat genelde, $xH \neq Hx$ dir. Bazı durumlarda ise $x \neq y$ olduğu halde $xH = yH$ dir. Bunlara ek olarak, bu örneklerde, bir altgrubun herhangi iki eşkümesinin ya ayrık ya da özdeş olduğunu görüyoruz. Bu bağlamda akla gelebilecek sorular şunlardır: Her altgrubun herhangi iki eşkümesi ya ayrık ya özdeş midir? Hangi koşullar altında $xH = yH$ olur? Hangi koşullar altında $xH = Hx$ olur?

Bu soruların bir kısmının yanıtı aşağıdaki önermemizde verilmektedir.

Önerme 2. *G bir grup, $H \leq G$ ve $x, y \in G$ olsun. Bu takdirde,*

(i) $x \in xH$, (ii) $xH = H \iff x \in H$,

(iii) $xH = yH \iff x \in yH$, (iv) $xH = yH \iff y^{-1}x \in H$,

(v) *ya* $xH = yH$ *ya da* $xH \cap yH = \emptyset$.

Kanıt. (i) $x = xe \in xH$.

(ii) $xH = H$ ise, $x \in xH = H$ dir. Karşıt olarak, $x \in H$ ise, $x^{-1} \in H$ olup $xH \subseteq H$ ve $x^{-1}H \subseteq H$ dir. İkinci kapsanma bağıntısına Önerme $1(iii)$ uygulanırsa, $x(x^{-1}H) \subseteq xH$, yani $H \subseteq xH$ elde edilir. Sonuç olarak, $xH = H$ dir.

(iii) $xH = yH$ ise, $x \in xH = yH$ dir. Karşıt olarak, $x \in yH$ ise, $x = yh$, $h \in H$ olur. Kanıtladığımız (ii) ve Önerme $1(ii)$ kullanılarak, $xH = (yh)H = y(hH) = yH$ elde edilir.

(iv) Önerme $1(ii)$, Önerme $1(v)$ ve kanıtladığımız (ii) ye göre

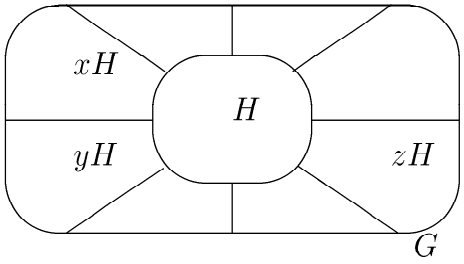
$$xH = yH \iff y^{-1}(xH) = y^{-1}(yH) \iff (y^{-1}x)H = H \iff y^{-1}x \in H.$$

(v) $xH \cap yH \neq \emptyset$ varsayalım ve $z \in xH \cap yH$ alalım. Bu takdirde, (iii) den, $zH = xH$ ve $zH = yH$ ve sonuç olarak, $xH = yH$ olur. ∎

Kanıtlamış olduğumuz önerme, yukarıda sorulan soruları yanıtladığı gibi başka önemli gerçekleri de ifade etmektedir. Özel olarak, (i) ve (v)

den, H nin tüm sol eşkümelerinin G grubunun bir parçalanışını verdiği sonucu çıkar. Gerçekten, H nin G içindeki sol eşkümelerinin kümesini

$$Sol(H) = \{\ xH : \quad x \in G\}$$



ile gösterirsek, $\bigcup_{x\in G} xH = G$ dir ve $xH \neq yH$ ise, $xH \cap yH = \emptyset$ dir.

Önerme 2 deki ifadelerin sağ eşkümeler için benzerleri kolayca kanıtlanabilir ve H nin G içindeki tüm sağ eşkümelerinin de G nin bir parçalanışını verdiği görülebilir. Biz tartışmalarımızı sol eşkümeler için sürdüreceğiz; elde edilen sonuçların sağ eşkümeler için ne anlama geldiğini düşünmeyi okuyucuya bırakıyoruz.

$Sol(H)$ nin, G nin bir parçalanışı olduğu gerçeğini iki şekilde değerlendireceğiz. Bunlardan birincisi, bu gerçeği Önerme $1(vii)$ ile birleştirerek yapılacaktır. G nin mertebesi, G nin parçalanışı olan $Sol(H)$ içindeki altkümelerinin (yani eşkümelerin) her birinin kardinalitesi hesaplanıp, bunlar toplanarak elde edilebilir. Her bir eşkümenin kardinalitesi, H nin mertebesi ile aynı olduğundan, bu düşünce ile,

$$|G| \ = \sum_{xH\in Sol(H)} |xH| \ = \sum_{xH\in Sol(H)} |H| \ = \ |Sol(H)| \cdot |H|$$

olduğu görülür.

Tanım 2. G bir grup, $H \leq G$ olsun. H nin G içindeki tüm sol eşkümelerinden oluşan kümenin kardinalitesi, H nin G içindeki *indeks*i olarak adlandırılır ve $(G : H)$ ile gösterilir: $(G : H) = |Sol(H)|$. □

Bu tanımla birlikte, yukarıda kanıtlanmış olan sonucu şöyle ifade edebiliriz:

Teorem 1. *G bir grup, $H \leq G$ olsun. Bu takdirde,*

$$|G| = (G : H) \cdot |H|$$

dir. ∎

Eşküme kavramı ile kolayca elde ettiğimiz bu teorem, sonlu gruplar için düşünüldüğünde, sonlu gruplar kuramının en önemli teoremlerinden birini verir. Gerçekten, eğer G bir sonlu grup ise, $(G : H)$ ve $|H|$ de sonlu olur. Teorem 1 in ifadesi, $|H|$ nin $|G|$ yi böldüğünü gösterir. Teorem 1 in doğrudan sonucu olmasına rağmen bu sonucu da teorem olarak isimlendiriyoruz.

Teorem 2 (Lagrange Teoremi). *G bir sonlu grup, $H \leq G$ ise, H nin mertebesi G nin mertebesini böler: $|H| \mid |G|$.*

Kanıt. Teorem 1'de $|G|$ sonlu olunca, $(G : H)$ ve $|H|$ de sonlu olur ve
$|G| = (G : H) \cdot |H|$ ifadesi $|H|$ nin $|G|$ yi böldüğünü gösterir. ∎

Teorem 6.2'de kanıtlanan sonuç, Lagrange Teoremi'nin sonlu devirli gruplar için ifadesini içermektedir. Teorem 6.2, mertebesi m olan bir G devirli grubunun, $d \mid m$ olan her d için mertebesi d olan bir alt gruba sahip olduğunu da ifade etmektedir. Lagrange Teoremi'nin devirli gruplar için karşıtı olan bu sonuç, herhangi bir grup için geçerli değildir. Örneğin, mertebesi 12 olan, ancak altgruplarının hiçbirinin mertebesi 6 olmayan bir grup vardır (Bak. Alıştırma 8.6).

Lagrange Teoremi'nin ne kadar güçlü bir teorem olduğu aşağıdaki sonuçlarından da açıkça görülecektir.

Sonuç 1. *G bir sonlu grup, $x \in G$ ise, x in mertebesi G nin mertebesini böler: $|x| \mid |G|$.*

Kanıt. $x \in G$ için $|x| = |< x >|$ olduğunu anımsayınız. ∎

Bu sonuç yardımıyla, örneğin mertebesi 15 olan bir grup içinde mertebesi 6 olan bir eleman aramanın anlamsız olduğunu görüyoruz.

Sonuç 2. *Mertebesi bir asal sayı olan her grup bir devirli gruptur.*

Kanıt. $|G| = p$ asal olsun. $x \in G \backslash \{e\}$ alalım. $|< x >| \neq 1$ dir ve $|< x >| \mid |G| = p$. O halde, $|< x >| = p$ ve dolayısıyla, $< x >= G$ dir. ∎

Sonuç 3. *G bir sonlu grup, $|G| = m$ ise, her $x \in G$ için $x^m = e$ dir.*

Kanıt. $x \in G$, $|x| = k$ olsun. Sonuç 1 den, $k \mid m$. $m = kd$ olsun. Bu takdirde, $x^m = x^{kd} = (x^k)^d = e^d = e$ olur. ∎

Sonuç 4 (Fermat'ın Küçük Teoremi). *p bir asal sayı ise, her $a \in \mathbb{Z}$ için $a^p \equiv a \pmod{p}$ dir.*

Kanıt. p asal, $a \in \mathbb{Z}$ olsun. Bölme algoritması ile

$$a = pq + r \quad ; \quad q, r \in \mathbb{Z} \quad , \quad 0 \leq r < p$$

ve dolayısıyla, $a \equiv r \pmod{p}$ dir. Kanıt için $r^p \equiv r \pmod{p}$ olduğunu göstermek yeter. Eğer $r = 0$ ise bu doğrudur; $r \neq 0$ ise, $r \in \mathbb{Z}_p^*$ olur ve $|\mathbb{Z}_p^*| = \varphi(p) = p - 1$ olduğundan, Sonuç 3 e göre, $\mathbb{Z}_p^*$ içinde, $r^{p-1} = 1$, $r^p = r$ dir. O halde, $r^p \equiv r \pmod{p}$ dir ve kanıt biter. ∎

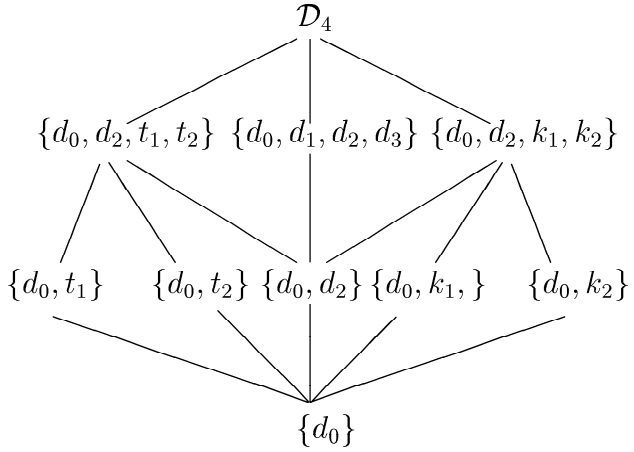
Görüldüğü gibi, çok basit bir ifadeye sahip olan Fermat'ın Küçük Teoremi'nin Lagrange Teoremi kullanılarak yapılan yukarıdaki ispatı da oldukça basittir. İfadesi ve ispatı bu denli basit olan bu teoremin, sayılar kuramında çok önemli uygulamaları vardır. Örneğin, bu teorem, bilgisayar desteği ile, verilen bir sayının asal olup olmadığını araştırırken kullanılmaktadır. Eğer, $n > 1$ sayısı için $a^n \not\equiv a \pmod{n}$ olacak biçimde bir $a \in \mathbb{Z}$ varsa, o zaman n asal olamaz. $n = 2^{257} - 1$ sayısı için bu yapılmış ve $10^n \not\equiv 10 \pmod{n}$ olduğu görülerek $2^{257} - 1$ in

asal olmadığı kanıtlanmıştır.

Lagrange Teoremi'nin önemi ve yararı, gruplar hakkındaki bilgilerimiz arttıkça daha iyi anlaşılacaktır. Bu teorem, bir sonlu grubun altgruplarının mertebelerine kısıtlama getirmektedir. Böylece, bir sonlu grubun altgruplarını belirlerken, eleman sayılarına bakarak, bazı altkümele ri baştan tartışma dışı tutabiliriz. Daha açık bir ifadeyle, eğer bir altkümedeki eleman sayısı, grubun mertebesini bölmüyorsa, o altküme bir altgrup olamaz.

Aşağıdaki örnekte, $\mathcal{D}_4$ ün altgrupları araştırılırken, bu grubun mertebesi 8 ve onun bölenleri, $1, 2, 4, 8$ den ibaret olduğundan, herhangi bir altgrubun mertebesinin, $1, 2, 4, 8$ sayılarından biri olması gerektiği göz önüne alınmaktadır.

Örnek 5. $\mathcal{D}_4 = \{d_0, d_1, d_2, d_3, t_1, t_2, k_1, k_2\}$ nin altgruplarını belirleyelim. Birim grup $\{d_0\}$ ve $\mathcal{D}_4$ ün kendisi dışındaki bir altgrubun mertebesi ya 2 ya da 4 olacaktır. Mertebesi 2 olan alt gruplar Sonuç 2 ye göre devirli gruplardır ve $< d_2 >= \{d_0, d_2\}$, $< t_1 >= \{d_0, t_1\}$, $< t_2 >= \{d_0, t_2\}$, $< k_1 >= \{d_0, k_1\}$, $< k_2 >= \{d_0, k_2\}$ den ibarettir. Mertebesi 4 olan bir altgrubun d_0 ile birlikte üç eleman içereceğine dikkat ederek, $\mathcal{D}_4$ ün mertebesi 4 olan altgruplarının $\{d_0, d_2, t_1, t_2\}$, $\{d_0, d_2, k_1, k_2\}$, $\{d_0, d_1, d_2, d_3\}$ den ibaret olduğu görülür. $\mathcal{D}_4$ ün altgruplar kafesi aşağıda verilmiştir.



□

$Sol(H)$ nin G nin bir parçalanışını oluşturması gerçeğinin iki şekilde değerlendirileceğini belirtmiş ve birincisinden Lagrange Teoremi'ni ve ilgili sonuçları elde etmiştik. İkincisi, denklik bağıntılarıyla ilişki kurmaktır. Her parçalanışın bir denklik bağıntısına yol açtığını anımsayalım ve G grubunun H altgrubu verildiğinde, $x, y \in G$ için

$$x \ \beta_H \ y \Longleftrightarrow xH = yH$$

tanımlayalım. β_H nin bir denklik bağıntısı olduğunu biliyoruz. Bu denklik bağıntısına göre denklik sınıfları, H nin G içindeki sol eşkümelerinden ibarettir.

Şimdi, ikili işlemlerle ilgili olarak Bölüm 2'de tanımlanan denklik sınıflarına taşınabilme kavramını anımsayalım ve şu soruyu soralım:

Soru: *G nin ikili işlemi sol eşkümelere taşınabilir mi? Başka bir ifade ile, $(xH)(yH) = (xy)H$ tanımlanırsa, $Sol(H)$ içinde bir ikili işlem elde edilir mi?*

Bölüm 2 den biliyoruz ki yukarıdaki sorunun yanıtının olumlu olması için gerek ve yeter koşul,

$$xH = aH, \ yH = bH \Longrightarrow (xy)H = (ab)H \tag{1}$$

olmasıdır. Bu koşul, her zaman sağlanmaz. Bu koşulu sağlayan altgruplar ve ilgili hususlar, bir sonraki bölümün konusu olacaktır.