$\mathcal{B}\ddot{\imath}\mathcal{L}\ddot{\mathcal{U}}\mathcal{M}$ 5

GRUP ÖRNEKLERİ : $\mathbb{Z}_n$, $\mathbb{Z}_n^*$, $\mathcal{S}_n$, $\mathcal{D}_n$

Bu bölümü bitirdiğinizde,

- $\mathbb{Z}_n$ ve $\mathbb{Z}_n^*$ gruplarını
- n-inci simetrik grup $\mathcal{S}_n$ yi
- permütasyon, çevrim, devrinim kavramlarını
- tek-çift permütasyonları
- n-inci almaşık grup $\mathcal{A}_n$ yi
- n-inci dihedral grup $\mathcal{D}_n$ yi

öğrenmiş olabileceksiniz.

BÖLÜM 5

GRUP ÖRNEKLERİ : $\mathbb{Z}_n$, $\mathbb{Z}_n^*$, $\mathcal{S}_n$, $\mathcal{D}_n$

Bu bölümde, bazı grupları yakından tanıyacağız. Bu gruplardan her biri, $n \in \mathbb{N}$ olmak üzere n ye bağlı olarak tanımlanır.

Örnek 2.3'te, $n \in \mathbb{N}$, $n \geq 2$ olmak üzere $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ kümesi içinde n modunda toplama işlemi, $\oplus$ ve n modunda çarpma işlemi, $\odot$, tanımlanmıştı.

Teorem 1. *Her $n \geq 2$ için $< \mathbb{Z}_n, \oplus >$ bir devirli gruptur.*

Kanıt. Örnek 2.4'te, $< \mathbb{Z}_n, \oplus >$ nın birleşme özelliği bulunduğunu gördük. Ayrıca, $0 \in \mathbb{Z}_n$ nin birim eleman olduğunu ve $\mathbb{Z}_n$ nin her sıfırdan farklı x elemanının, $\oplus$ işlemine göre tersinin, $n - x$ olduğunu biliyoruz. O halde, $< \mathbb{Z}_n, \oplus >$ bir gruptur. Ek olarak,

$$< 1 > = \{\ k1 :\ k \in \mathbb{Z}\ \} = \{0, 1, \cdots, n-1\} = \mathbb{Z}_n$$

ve böylece, $\mathbb{Z}_n$ bir devirli gruptur. 1, $\mathbb{Z}_n$ nin bir üretecidir. ∎

Bundan böyle, $\mathbb{Z}_n$ toplamsal grubunun işlemini, $\oplus$ yerine $+$ ile gösterece- ğiz. $\mathbb{Z}$'de olduğu gibi, burada da $a \in \mathbb{Z}_n$ nin tersi, $(-a)$ ile gösterilecek ve $b \in \mathbb{Z}_n$ için, $b - a = b + (-a)$ alınacaktır.

Örnek 2.7'de, $\mathbb{Z}_n$ nin n modunda çarpma işlemine göre tersinir olmayan elemanları bulunabileceğini görmüştük. Bu nedenle, $< \mathbb{Z}_n, \odot >$ bir grup değildir. Bununla beraber, eğer n bir asal sayı ve $x, y \in \mathbb{Z}_n \backslash \{0\}$ ise, $x \odot y \in \mathbb{Z}_n \backslash \{0\}$ olur. Gerçekten, $\mathbb{Z}$ içinde xy çarpımına bölme algoritması uygulandığında,

$$xy = an + (x \odot y) \quad , \quad a \in \mathbb{Z}, (x \odot y) \in \mathbb{Z}_n$$

elde edilir. Burada n asal, $n \nmid x$ ve $n \nmid y$ olduğundan, $n \nmid xy$ ve dolayısıyla, $x \odot y \neq 0$ dır. Başka bir deyişle, eğer n bir asal sayı ise,

$\odot$ işlemi $\mathbb{Z}_n\backslash\{0\}$ içinde bir ikili işlemdir. n asal ise, $\mathbb{Z}_n\backslash\{0\}$ daki tüm elemanların n ile aralarında asal olduğuna dikkat ediniz. Bu durumu göz önüne alarak, herhangi bir $n \geq 2$ için $\mathbb{Z}_n$ nin n ile aralarında asal olan elemanlarının oluşturduğu kümeyi $\mathbb{Z}_n^*$ ile gösterelim:

$$\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n : k \text{ ve } n \text{ aralarında asal}\}.$$

Kolayca görülebileceği gibi, $\mathbb{Z}_n$ üzerindeki çarpma işlemi, $\odot$, $\mathbb{Z}_n^*$ üzerinde de bir ikili işlem indirger. Gerçekten, x ve y aralarında asal olduğundan, xy ile n ve dolayısıyla, $x \odot y$ ile n, aralarında asal olur ve böylece, $x \odot y \in \mathbb{Z}_n^*$ olur.

Teorem 2. *Her $n \geq 2$ için $< \mathbb{Z}_n^*, \odot >$ bir değişmeli gruptur.*

Kanıt. $\odot$ işleminin $\mathbb{Z}_n^*$ üzerinde (hatta $\mathbb{Z}_n$ üzerinde) birleşme ve değişme özelliği bulunduğunu ve $1 \in \mathbb{Z}_n^*$ nin $\odot$ işlemine göre birim eleman olduğunu Bölüm 2'de görmüştük. $k \in \mathbb{Z}_n^*$ ise, k ile n aralarında asal olduklarından, öyle $x, y \in \mathbb{Z}$ vardır ki $xk + yn = 1 = kx + yn$ olur. Burada x in n ile bölünmesinden elde edilen en küçük negatif olmayan kalan t ise, $t \in \mathbb{Z}_n^*$ ve $t \odot k = k \odot t = 1$ olduğu görülür. Demek ki, her $k \in \mathbb{Z}_n^*$ tersinirdir. O halde, $< \mathbb{Z}_n^*, \odot >$ bir değişmeli gruptur. ∎

Bundan böyle, $x, y \in \mathbb{Z}_n$ için $x \odot y$ yerine xy veya $x \cdot y$ yazacağız. $\mathbb{Z}_n^*$ ın mertebesi, $\varphi(n)$ ile gösterilir. Şu halde, $n \geq 2$ için, $\varphi(n)$, n den küçük ve n ile aralarında asal olan doğal sayıların sayısıdır. Ek olarak, $\varphi(1) = 1$ tanımlanır. Böylece, sayılar kuramında büyük öneme sahip olan bir fonksiyon tanımlamış olduk:

Tanım 1. $\varphi(n)$ yukarıda tanımlandığı gibi olmak üzere $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$, $n \longrightarrow \varphi(n)$ fonksiyonuna *Euler'in φ-fonksiyonu* denir. □

Şimdi, gruplar kuramında önemli bir yer tutan permütasyon gruplarını tanımlayalım.

Tanım 2. Boş olmayan bir K kümesi ve bir $f : K \longrightarrow K$ fonksiyonu verilmiş olsun. Eğer f fonksiyonu bire-bir ve örten ise, f ye K üzerinde bir *permütasyon* (devşirim, dizilim) denir. K üzerindeki tüm permütasyonlardan oluşan küme, $\mathcal{S}(K)$ ile gösterilir. □

$\mathcal{S}(K)$ nın, fonksiyonlardaki bileşke işlemi ile, bir grup olduğu ko-

layca görülür.

Tanım 3. Boş olmayan bir K kümesi için $S(K)$ grubuna K *nın permutasyonlar grubu* denir. Özel olarak, $K_n = \{1, 2, \ldots, n\}$ kümesi için K_n nin permütasyonlar grubu, $\mathcal{S}_n$ ile gösterilir. $\mathcal{S}_n$ ye *n-inci simetrik grup* denir. □

$\mathcal{S}_n$ nin bir α elemanının $\alpha = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{pmatrix}$ biçiminde gösterilmesi çeşitli yararlar sağlamaktadır. Örneğin, $\mathcal{S}_n$ nin mertebesini hesaplamak için bu gösterim çok elverişlidir. Bu gösterimde, $\alpha(1)$, K_n nin herhangi bir elemanı olabilir; başka bir deyişle $\alpha(1)$ görüntüsü, n farklı biçimde seçilebilir. α fonksiyonu bire-bir olduğundan, α nın yukarıdaki gösteriminde ikinci satırdaki tüm elemanlar birbirinden farklı olmalıdır. Bu nedenle, $\alpha(1)$ seçildikten sonra, $\alpha(2)$, tam $(n-1)$ değişik biçimde seçilebilir. Bu düşünce ile, α için yukarıdakine benzer $n!$ gösterim mümkündür; $|\mathcal{S}_n| = n!$ dir. Bu gösterimin bir diğer yararı da $\mathcal{S}_n$ içinde hesap yaparken görülür. $\mathcal{S}_n$ nin ikili işlemi(fonksiyon bileşkesi) için çarpımsal gösterim kullanacağız. $\alpha, \beta \in \mathcal{S}_n$ ise, $\alpha\beta$ çarpımı, her $j \in K_n$ için $\alpha\beta(j) = \alpha(\beta(j))$ olarak tanımlanır. Yukarıdaki gösterimle,

$$\beta = \begin{pmatrix} 1 & \ldots & j & \ldots & n \\ \beta(1) & \ldots & \beta(j) & \ldots & \beta(n) \end{pmatrix}, \alpha = \begin{pmatrix} 1 & \ldots & \beta(j) & \ldots & n \\ \alpha(1) & \ldots & \alpha\beta(j) & \ldots & \alpha(n) \end{pmatrix}$$

ise, $\alpha\beta(j)$ yi bulmak için α nın ilk satırında $\beta(j)$ bulunacak ve onun altındaki sayı $\alpha(\beta(j))$ olarak alınacaktır.

Örnek 1. $\mathcal{S}_3$ ün $3! = 6$ elemanı vardır:

$$\imath = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, d_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, d_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Bu gösterimden yararlanarak

$$d_1 d_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \imath,$$

$$d_1 s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = s_3$$

olduğu görülür. Benzer hesaplamalarla, $\mathcal{S}_3$ ün yanda gösterilen çarpım tablosu elde edilir. □

	$\imath$	d_1	d_2	s_1	s_2	s_3
$\imath$	$\imath$	d_1	d_2	s_1	s_2	s_3
d_1	d_1	d_2	$\imath$	s_3	s_1	s_2
d_2	d_2	$\imath$	d_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	$\imath$	d_1	d_2
s_2	s_2	s_3	s_1	d_2	$\imath$	d_1
s_3	s_3	s_1	s_2	d_1	d_2	$\imath$

Tanım 4. Eğer $\delta \in \mathcal{S}_n$ permütasyonu, K_n nin, $k_1, \ldots, k_r$ gibi bir takım elemanlarını art arda değiştirip geri kalan elemanlarını sabit bırakıyorsa, daha açık bir ifadeyle, $\delta(k_1) = k_2$, $\delta(k_2) = k_3$, $\ldots$, $\delta(k_{r-1}) = k_r$, $\delta(k_r) = k_1$ ve her $j \in K_n \backslash \{k_1, \ldots, k_r\}$ için $\delta(j) = j$ ise, δ ya bir *çevrim* denir. □

Bu tanımdaki gibi bir çevrim, $\delta = (k_1\ k_2\ \cdots\ k_r)$ ile gösterilir. Bununla beraber,

$$\delta = (k_1\ k_2\ \cdots\ k_r) = (k_2\ k_3\ \cdots\ k_r\ k_1) = \cdots = (k_r\ k_1\ \cdots\ k_{r-1})$$

yazılabileceği açıktır. $\mathcal{S}_3$ içinde $\delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ permütasyonu bir çevrimdir ve $\delta = (1\ 3) = (3\ 1)$ biçiminde ifade edilebilir.

Tanım 5. Bir çevrimin gösterimindeki eleman sayısı, o çevrimin *uzunluğu* olarak adlandırılır. □

Örneğin, $\delta = (1\ 3)$ ün uzunluğu 2 dir. Bu bağlamda, birim permütasyon, $\imath$, uzunluğu 1 olan çevrim olarak düşünülebilir.

$$\imath = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} = (1) = (2) \cdots$$

Ayrıca, uzunluğu r olan bir çevrimin tersinin de uzunluğu r olan bir çevrim olduğu görülebilir: $\delta = (k_1\ k_2\ \cdots\ k_r)$ ise, $\delta^{-1} = (k_r\ k_{r-1}\ \cdots\ k_1)$ dir. Bu iddiayı kanıtlamak için $(k_1\ k_2\ \cdots\ k_r)$ ile $(k_r\ k_{r-1}\ \cdots\ k_1)$ in çarpımını hesaplamak yeter.

Uzunluğu r olan $\delta = (k_1\ k_2\ \cdots\ k_r)$ çevrimi verilmiş olsun. $i + j$ ile, i ve j nin "r modunda" toplamı gösterilirse, her $1 \leq i, j \leq r$ için, $\delta^j(k_i) = k_{i+j}$ dir. Buradan, uzunluğu r olan her çevrimin

$$\delta = (k_1\ \delta(k_1)\ \delta^2(k_1)\ \cdots\ \delta^{r-1}(k_1))$$

biçiminde ifade edilebileceği ve mertebesinin r olduğu görülür.

Tanım 6. Eğer iki çevrimin gösterimlerinde ortak bir harf (veya rakam) yoksa, bu iki çevrime *ayrık* çevrimler denir. □

Daha açık bir ifadeyle, $\delta = (k_1\ \cdots\ k_r)$ ve $\tau = (h_1\ \cdots\ h_s)$ çevrimlerinin ayrık olması için gerek ve yeter koşul, $\{k_1, \ldots, k_r\} \cap \{h_1, \ldots, h_s\} = \emptyset$ olmasıdır. $\mathcal{S}_n$ nin yapısını araştırırken ayrık çevrimlerin aşağıdaki özelliği ile başlayabiliriz.

Önerme 1. *δ ve γ, $\mathcal{S}_n$ içinde iki ayrık çevrim ise, $\delta\gamma = \gamma\delta$ dır.*

Kanıt. $\delta, \gamma \in \mathcal{S}_n$ ayrık çevrimler olsun. K_n nin her elemanı, ya hem δ hem de γ tarafından sabit bırakılır ya da bunlardan biri tarafından sabit bırakılıp diğeri tarafından değiştirilir. $k \in K_n$ alalım. Eğer k, hem δ hem de γ tarafından sabit bırakılıyorsa, $\gamma\delta(k) = k = \delta\gamma(k)$ olur. Eğer k, δ ve γ dan biri tarafından sabit bırakılıp diğeri tarafından değiştiriliyorsa, genelliği bozmadan, $\gamma(k) \neq k$ ve $\delta(k) = k$ kabul edebiliriz. O zaman, γ bire-bir olduğundan, $\gamma(\gamma(k)) \neq \gamma(k)$ ve dolayısıyla, $\delta(\gamma(k)) = \gamma(k) = \gamma(\delta(k))$ olur. Böylece, $\gamma\delta = \delta\gamma$ dır. ∎

Şimdi vereceğimiz tanım ve gösterimler, bir sonraki teoremimizin kanıtında yardımcı olacaktır.

IIer $\alpha \in \mathcal{S}_n$ ve $k \in K_n$ için

$$Y_\alpha(k) = \{\alpha^j(k) : j \in \mathbb{Z}\}$$

tanımlayalım. α nın mertebesi sonlu olduğundan, $Y_\alpha(k)$, sonlu bir kümedir. Ayrıca, eğer $\alpha^r(k) = k$ özelliğine sahip en küçük pozitif r tamsayısı seçilirse, $Y_\alpha(k)$ nın tam r tane elemanı vardır ve

$$Y_\alpha(k) = \{k, \alpha(k), \alpha^2(k), \ldots, \alpha^{r-1}(k)\}$$

dır. $Y_\alpha(k)$ nın belirlediği

$$[k]_\alpha = (k\ \alpha(k)\ \alpha^2(k)\ \cdots\ \alpha^{r-1}(k))$$

çevrimine α *ve* k *nın tanımladığı çevrim* denir. Kolayca görülebilir ki

- $\alpha(k) = k \iff Y_\alpha(k) = \{k\} \iff [k]_\alpha = 1$,
- $\alpha(k) = h \iff Y_\alpha(k) = Y_\alpha(h) \iff [k]_\alpha = [h]_\alpha$,
- $Y_\alpha(k)$, $k \in K_n$, kümeleri K_n nin bir parçalanışını oluştururlar.

Teorem 3. $\mathcal{S}_n$ *içinde birim permütasyon dışında her permutasyon, uzunluğu en az iki olan sonlu sayıda ayrık çevrimin çarpımı olarak yazılabilir; bu yazılış, çarpanların sıralanışı dışında tek türlü belirlidir.*

Kanıt. $\alpha \in \mathcal{S}_n$, $\alpha \neq 1$ olsun ve $K_n^* = \{k \in K_n : \alpha(k) \neq k\}$ tanımlayalım. $K_n^* \neq \emptyset$ dir ve $\{Y_\alpha(k) : k \in K_n^*\}$ kümeler topluluğu, K_n^* ın bir parçalanışı olur. Sonlu sayıda hücre bulunan bu parçalanıştaki farklı hücreler, $Y_\alpha(k_1), Y_\alpha(k_2), \ldots, Y_\alpha(k_s)$ ve bunlara karşılık gelen çevrimler, $[k_1]_\alpha, [k_2]_\alpha, \ldots, [k_s]_\alpha$ olsun. Bunlar, ayrık çevrimler olup her $i = 1, \ldots, s$ için $[k_i]_\alpha$ nın uzunluğu; yani $Y_\alpha(k_i)$ nin kardinalitesi, en az 2 dir. Ayrıca, her $k \in K_n^*$ için $k \in Y_\alpha(k_i)$ olacak biçimde bir $i \in \{1, \ldots, s\}$ vardır. Dolayısıyla, $k = \alpha^j(k_i), j \geq 0$;

$$\alpha(k) = \alpha^{j+1}(k_i) = [k_i]_\alpha(\alpha^j(k_i)) = [k_i]_\alpha(k) = [k_1]_\alpha[k_2]_\alpha \cdots [k_s]_\alpha(k)$$

dır. Eğer $k \notin K_n^*$ ise, $\alpha(k) = k$ ve her $i = 1, \ldots, s$ için $[k_i]_\alpha(k) = k$ dır. Sonuç olarak, her $k \in K_n$ için $\alpha(k) = ([k_1]_\alpha[k_2]_\alpha \cdots [k_s]_\alpha)(k)$ olduğu, yani $\alpha = [k_1]_\alpha[k_2]_\alpha \cdots [k_s]_\alpha$ olduğu görülür ki bu, teoremin ilk kısmının kanıtıdır. Kanıtı tamamlamak için, α nın ayrık çevrimlerin çarpımı olarak herhangi bir yazılışını alalım:

$$\alpha = \delta_1\delta_2 \cdots \delta_m.$$

Bu takdirde, $s = m$ eşitliğini ve gerekirse sıralama değiştirilerek, $\delta_i = [k_i]_\alpha$, $1 \leq i \leq s$ olduğunu göstermeliyiz. Her $i = 1, \ldots, s$ için $\delta_t(k_i) \neq k_i$ olan bir ve yalnız bir δ_t vardır, $1 \leq t \leq m$. Bu durumda, $\alpha(k_i) = \delta_l(k_i) = [k_i]_\alpha(k_i)$ olacağından, $[k_i]_\alpha = \delta_l$ olur. Böylece, $s \leq m$ dir. Diğer yandan, her bir δ_t nin uzunluğu en az 2 olduğundan, en az bir $k \in K_n^*$ için $\delta_t(k) \neq k$ dır. Bu durumda, $k \in Y_\alpha(k_i)$ olacak biçimde bir ve yalnız bir i vardır ve bu i için $\delta_t = [k_i]_\alpha$ dır, $1 \leq i \leq s$. Böylece, $m \leq s$ dir. Sonuç olarak, $s = m$ olduğunu ve ayrıca, gerekirse sıralama değiştirilerek, her $i = 1, \ldots, s$ için $\delta_i = [k_i]_\alpha$ olduğunu göstermiş bulunuyoruz. ∎

Örnek 2. $\mathcal{S}_8$ içinde $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 8 & 7 & 2 & 6 & 1 & 5 \end{pmatrix}$ elemanının ayrık çevrimlerin çarpımı olarak yazılışı, $\alpha = (1\ 4\ 7)(2\ 3\ 8\ 5) = [1]_\alpha[2]_\alpha$ biçimindedir. Bu yazılış ile Teorem 3 ün kanıtını karşılaştırınız. □

Tanım 7. $\mathcal{S}_n$ içinde uzunluğu 2 olan her çevrime bir *devrinim* (transpozisyon) denir. □

Her devrinim, $\delta = (k_1\ k_2)$ biçimindedir ve $\delta^2 = \imath$; dolayısıyla, $\delta^{-1} = \delta$ dır.

Önerme 2. *Uzunluğu $r > 1$ olan her çevrim, $r-1$ tane devrinimin çarpımı olarak yazılabilir.*

Kanıt. $\delta = (k_1\ \cdots\ k_r)$ ise, $\delta = (k_1\ k_r)(k_1\ k_{r-1})\cdots(k_1\ k_3)(k_1\ k_2)$ olduğu kolayca görülür. ∎

Sonuç 1. *$\mathcal{S}_n$ içindeki her permütasyon, sonlu sayıda devrinimin çarpımı olarak yazılabilir.*

Kanıt. $\alpha \in \mathcal{S}_n$ olsun. $\alpha = \imath$ ise, herhangi iki eleman

$a,\ b \in K_n$ için $\imath = (a\ b)(b\ a)$ olduğunu biliyoruz. $\alpha \neq \imath$ ise, Teorem 3 e göre, α, her birinin uzunluğu en az iki olan sonlu sayıda çevrimin çarpımı olarak yazılabilir. Önerme 2 ye göre, bu yazılıştaki her çevrim de sonlu sayıda devrinimin çarpımı olarak yazılabildiğinden, α, sonlu sayıda devrinimin çarpımı olarak yazılabilir. ∎

Örnek 3. Örnek 2'de verilen α elemanının, ayrık çevrimlerin çarpımı olarak yazılışının, $\alpha = (1\ 4\ 7)(2\ 3\ 8\ 5)$ olduğunu biliyoruz. Önerme 2 yi kullanarak, α yı devrinimlerin çarpımı olarak şöyle ifade edebiliriz: $\alpha = (1\ 7)(1\ 4)(2\ 5)(2\ 8)(2\ 3)$. Bu ifade, tek türlü belirli değildir; örneğin, α için bir başka yazılış, $\alpha = (4\ 1)(5\ 8)(4\ 7)(3\ 2)(8\ 5)(3\ 5)(3\ 8)$ dir. Bu yazılışlarda da değişmeyen bir husus vardır. Onun ne olduğu bir sonraki teoremde verilecek. □

Önerme 3. *Eğer $\delta_1, \ldots, \delta_{r-1}, \delta_r$ devrinimler ve $\delta_1 \cdots \delta_{r-1}\delta_r = \imath$, birim permütasyon, ise, r çifttir.*

Kanıt. Bir devrinim, birim permütasyona eşit olamayacağından, $r > 1$ dir. İddiamızı tümevarımla kanıtlayacağız. $r = 2$ ise, kanıtlanacak bir şey yoktur. $r > 2$ olsun. Son çarpan, $\delta_r = (a\ x)$ olsun. $(a\ b) = (b\ a)$ olduğundan, $\delta_{r-1}\delta_r$ çarpımı için aşağıdaki durumlardan biri geçerlidir:

- $\delta_{r-1}\delta_r = (a\ x)(a\ x) = 1$
- $\delta_{r-1}\delta_r = (b\ x)(a\ x) = (a\ x)(a\ b)$
- $\delta_{r-1}\delta_r = (a\ b)(a\ x) = (b\ x)(a\ b)$
- $\delta_{r-1}\delta_r = (b\ c)(a\ x) = (a\ x)(b\ c)$.

Eğer ilk durum geçerli ise, verilen çarpımdan $\delta_{r-1}\delta_r$ çarpımını silebiliriz; tümevarımla, $r-2$ ve dolayısıyla r, çifttir. Eğer diğer üç durumdan biri geçerli ise, verilen çarpımdaki $\delta_{r-1}\delta_r$ çarpımını yukarıda karşılık gelen ifadenin sağındaki çarpım ile değiştirerek yine birim permütasyona eşit olan ve r tane devrinimden oluşan bir çarpım elde ederiz:

$$\delta_1' \cdots \delta_{r-1}'\delta_r' = 1.$$

Bu yeni çarpımda, en sondaki devrinim, x tamsayısını değiştirmez. Şimdi, aynı işlemi $\delta_{r-2}'\delta_{r-1}'$ çarpımına uygularsak, ya $r-2$ tane devrinimden oluşan ve birim permütasyona eşit olan bir çarpım elde ederiz ya da r tane devrinimden oluşan ve birim permütasyona eşit olan bir çarpım elde ederiz ki, bu çarpımda sondaki iki devrinim, x tamsayısını değiştirmez. Her defasında x i değiştiren son çarpanı bir sola kaydıran bu işlem sürdürülürse, adımlardan birinde $r-2$ devrinimden oluşan ve birim permütasyona eşit olan bir çarpım elde edilir. Çünkü, aksi halde, r devrinimden oluşan ve birim permütasyona eşit olan öyle bir çarpım elde edilir ki x tamsayısı sadece soldan itibaren ilk çarpan tarafından değiştirilmektedir. Bu mümkün değildir, zira birim permütasyon, x i değiştirmez. ∎

Teorem 4. *$\alpha \in \mathcal{S}_n$ verilmiş olsun. α nın devrinimlerin çarpımı olarak her yazılışındaki devrinim sayısı ya daima tek ya da daima çifttir.*

Kanıt. $\alpha \in \mathcal{S}_n$ için devrinimlerin çarpımı olarak iki yazılış düşünelim:

$$\alpha = \delta_1 \cdots \delta_{r-1}\delta_r = \tau_1 \cdots \tau_{s-1}\tau_s.$$

Bu takdirde, $1 = \delta_1 \cdots \delta_{r-1}\delta_r\tau_s^{-1}\tau_{s-1}^{-1} \cdots \tau_1^{-1} = \delta_1 \cdots \delta_{r-1}\delta_r\tau_s\tau_{s-1} \cdots \tau_1$ olur. Önerme 3 e göre, $r+s$ çifttir. Dolayısıyla, r ve s nin ya her ikisi

de tek veya her ikisi de çifttir. ∎

Tanım 8. $\alpha \in \mathcal{S}_n$ verilmiş olsun. α nın devrinimlerin çarpımı olarak yazılışındaki devrinim sayısı tek ise, α ya bir *tek permütasyon*; bu sayı çift ise, α ya bir *çift permütasyon* denir. □

Teorem 5. *$\mathcal{S}_n$ içindeki tüm çift permütasyonlardan oluşan kümeyi $\mathcal{A}_n$ ile gösterelim. Bu takdirde, $\mathcal{A}_n \leq \mathcal{S}_n$ ve $|\mathcal{A}_n| = \frac{n!}{2}$ dir.*

Kanıt. Birim permütasyon, ı, çifttir: $\imath \in \mathcal{A}_n$. Her çift permutasyonun tersi ve iki çift permütasyonun çarpımı yine bir çift permütasyondur. Böylece, Önerme 4.2 ye göre $\mathcal{A}_n \leq \mathcal{S}_n$ dir. $\mathcal{S}_n$ içindeki tek permütasyonların kümesini $\mathcal{B}_n$ ile gösterelim ve $\mathcal{S}_n$ nin bir $(a\ b)$ devrinimini alalım. Bu takdirde, $\mathcal{S}_n = \mathcal{A}_n \cup \mathcal{B}_n$, $\mathcal{A}_n \cap \mathcal{B}_n = \emptyset$ dir ve $f : \mathcal{A}_n \longrightarrow \mathcal{B}_n$, $f(\alpha) = (a\ b)\alpha$ fonksiyonu, bire-bir ve örtendir. Buradan, $|\mathcal{A}_n| = |\mathcal{B}_n| = \frac{n!}{2}$ dir. ∎

Tanım 9. Teorem 5'te tanımlanan $\mathcal{A}_n$ grubuna *n-inci almaşık grup* denir. □

Bu bölümde ele alacağımız grup örneklerinden sonuncusu, düzlemde bir düzgün n-genin simetrilerinin oluşturduğu gruptur. Düzlemde bir şeklin bir *simetrisi* denince düzlemden kendi üzerine, uzaklık koruyan ve sözü edilen şekli kendi üzerine dönüştüren bir fonksiyon anlaşılır. Burada uzaklık koruyan deyiminin anlamı, P ve Q gibi iki noktanın arasındaki uzaklık ile onların görüntülerinin arasındaki uzaklığın aynı olmasıdır. Düzlemde bir şeklin tüm simetrileri, fonksiyon bileşkesi ile bir grup oluşturur.

Tanım 10. Düzlemde bir şeklin simetrilerinden oluşan gruba söz konusu şeklin *simetriler grubu* denir. Bir düzgün n-genin simetriler grubuna *n-inci dihedral grup* denir ve bu grup, $\mathcal{D}_n$ ile gösterilir. □

Düzlemde bir şeklin simetrileri şöyle de açıklanabilir. Söz konusu şekli bir karton üzerine çizdiğinizi, sonra da oradan kesip çıkardığınızı varsayınız. Çıkardığınız bu şekli tekrar yerine yerleştirmeye çalışınız. Bu işi yaparken kullandığınız kartonun saydam olduğunu varsayabilirsiniz. O zaman, her bir yerleştiriş, o şeklin bir simetrisine karşılık gelir. Köşeleri 1 den n ye kadar numaralanmış bir düzgün n-genin

her simetrisi, köşelerin yer değiştirmesi anlamına geleceğinden, $\mathcal{D}_n$ nin her elemanı, $K_n = \{1, 2, \ldots, n\}$ nin bir permütasyonu, yani $\mathcal{S}_n$ nin bir elemanı olarak kabul edilebilir. Numaralama işlemini düzgün 4-gen, yani kare için yandaki gibi yapalım.

3	2
4	1

Karenin yeniden yerleştirilmesi yapılırken, bir köşenin yerleştirilmesi, o yerleştirilişi tamamen belirler. Her bir köşenin, 4 köşeden her birine yazılan numara altta veya üstte kalacak biçimde yerleştirilebileceği açıktır. O halde, karenin tam 8 simetrisi vardır, yani $|\mathcal{D}_4| = 8$ dir. Aşağıda, $\mathcal{D}_4$ ün tüm elemanları, karenin ilk konumunun nasıl değiştirildiği gösterilerek, listelenmiştir.

d_0 : 0° lik dönme (ilk konum)
$d_0 = \imath$

3	2			3	2		
4	1	$\longmapsto$		4	1		

d_1 : 90° lik dönme (saat yönünün tersine)
$d_1 = (1\ 2\ 3\ 4)$

3	2			2	1		
4	1	$\longmapsto$		3	4		

d_2 : 180° lik dönme
$d_2 = (1\ 3)(2\ 4)$

3	2			1	4		
4	1	$\longmapsto$		2	3		

d_3 : 270° lik dönme
$d_3 = (1\ 4\ 3\ 2)$

3	2			4	3		
4	1	$\longmapsto$		1	2		

t_1 : Yatay eksen etrafında 180° lik dönme
$t_1 = (1\ 2)(3\ 4)$

3	2			4	1		
4	1	$\longmapsto$		3	2		

t_2 : Düşey eksen etrafında 180° lik dönme
$t_2 = (1\ 4)(2\ 3)$

3	2			2	3		
4	1	$\longmapsto$		1	4		

k_1 : 1 - 3 köşegeni etrafında 180° lik dönme
$k_1 = (2\ 4)$

3	2			3	4		
4	1	$\longmapsto$		2	1		

k_2 : 2 - 4 köşegeni etrafında 180° lik dönme
$k_2 = (1\ 3)$

$$\begin{array}{|c|c|}\hline 3 & 2 \\ \hline 4 & 1 \\ \hline \end{array} \longmapsto \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 4 & 3 \\ \hline \end{array}$$

Yukarıdaki elemanlardan her biri bir permütasyon olarak düşünüldüğünde, permütasyon çarpımı, bu yerleştirişlerin art arda (fakat uygun sırada) uygulanması demektir. Örneğin,

$$d_1t_1 : \begin{array}{|c|c|}\hline 3 & 2 \\ \hline 4 & 1 \\ \hline \end{array} \xrightarrow{t_1} \begin{array}{|c|c|}\hline 4 & 1 \\ \hline 3 & 2 \\ \hline \end{array} \xrightarrow{d_1} \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 4 & 3 \\ \hline \end{array} \quad ; \quad d_1t_1 = k_2,$$

$$t_1d_1 : \begin{array}{|c|c|}\hline 3 & 2 \\ \hline 4 & 1 \\ \hline \end{array} \xrightarrow{d_1} \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 3 & 4 \\ \hline \end{array} \xrightarrow{t_1} \begin{array}{|c|c|}\hline 3 & 4 \\ \hline 2 & 1 \\ \hline \end{array} \quad ; \quad t_1d_1 = k_1,$$

Bu işlemler, $\mathcal{D}_4$ ün *değişmeli olmayan* bir grup olduğunu da göstermektedir. $\mathcal{D}_4$ ün işlem tablosu aşağıdaki gibi oluşturulabilir.

	d_0	d_1	d_2	d_3	t_1	t_2	k_1	k_2
d_0	d_0	d_1	d_2	d_3	t_1	t_2	k_1	k_2
d_1	d_1	d_2	d_3	d_0	k_2	k_1	t_1	t_2
d_2	d_2	d_3	d_0	d_1	t_2	t_1	k_2	k_1
d_3	d_3	d_0	d_1	d_2	k_1	k_2	t_2	t_1
t_1	t_1	k_1	t_2	k_2	d_0	d_2	d_1	d_3
t_2	t_2	k_2	t_1	k_1	d_2	d_0	d_3	d_1
k_1	k_1	t_2	k_2	t_1	d_3	d_1	d_0	d_2
k_2	k_2	t_1	k_1	t_2	d_1	d_3	d_2	d_0

Burada kare için yapılan analizler, eşkenar üçgen, düzgün beşgen, düz- gün altıgen, veya genelde düzgün n-gen için tekrarlanabilir. O zaman görülür ki, düzgün n-genin simetrileri, mertebesi $2n$ olan bir grup oluşturur- lar: *n-inci dihedral grup.*