3.7. SİMETRİK GRUPLAR:

Tanım 3.7.1. $n \in \mathbb{Z}^+$ olmak üzere n elemanlı bir kümenin kendi üzerine birebir bir fonksiyonuna bu kümenin bir **permütasyonu** denir.

Not: n elemanlı bir kümenin her permütasyonu bu kümenin elemanlarının bir sıralanışını belirtir. Tersine n elemanlı bir kümenin elemanlarının her sıralanışı bu kümenin bir permütasyonunu belirtir. n elemanlı bir kümenin tüm permütasyonları kümesinin fonksiyonlarda bileşke işlemine göre bir grup olduğunu daha önce gösterdik. Bu gruba bir **simetrik grup** denir.

Teorem 3.7.2. n elemanlı bir kümenin tüm permütasyonları sayısı $n!$dir.
İspat: n elemanlı herhangi $A=\{a_1,a_2,...,a_n\}$ kümesini alalım. $A=\{a_1,a_2,...,a_n\}$ kümesinin elemanlarını sıraladığımızda birinci sıraya n tane farklı eleman, bunların her birinde ikinci sıraya $n-1$ tane farklı eleman, bunların her birinde üçüncü sıraya $n-2$ farklı eleman, …, bunların her birinde $n.$ sıraya $n-(n-1)=1$ farklı eleman yazabiliriz. Böylece $A=\{a_1,a_2,...,a_n\}$ kümesinin elemanlarının farklı sıralanışları sayısı $n(n-1)(n-2)...1=n!$ olup n elemanlı bir kümenin tüm permütasyonları sayısı $n!$ olur.

Not: σ, $L=\{x_1,x_2,...,x_n\}$ kümesinin bir permütasyonu ve $\sigma(x_1)=x_{i_1}$, $\sigma(x_2)=x_{i_2}$, ..., $\sigma(x_n)=x_{i_n}$ ise bu permütasyon genellikle $\sigma=\begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_{i_1} & x_{i_2} & ... & x_{i_n} \end{pmatrix}$ şeklinde de gösterilir. $M=\{1,2,...,n\}$ kümesinin tüm permütasyonları kümesi genellikle S_n ile gösterilir.

Teorem 3.7.3. $L=\{x_1,x_2,...,x_n\}$ kümesinin tüm permütasyonları kümesi T_n olsun. Bu durumda

$$\varphi: T_n \to S_n, \sigma=\begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_{i_1} & x_{i_2} & ... & x_{i_n} \end{pmatrix} \to \varphi(\sigma)=\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$$

ile tanımlı φ dönüşümü bir grup izomorfizmasıdır.
İspat: φ nin bir fonksiyon olduğu açıktır. Herhangi $\sigma_1,\sigma_2 \in T_n$ alalım. $\sigma_1=\begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_{i_1} & x_{i_2} & ... & x_{i_n} \end{pmatrix}$ ve $\sigma_2=\begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_{j_1} & x_{j_2} & ... & x_{j_n} \end{pmatrix}$ olsun. Bu durumda $\sigma_1 \circ \sigma_2=\begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_{i_{j1}} & x_{i_{j2}} & ... & x_{i_{jn}} \end{pmatrix}$ olur. φ nin tanımından $\varphi(\sigma_1)=\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$, $\varphi(\sigma_2)=\begin{pmatrix} 1 & 2 & ... & n \\ j_1 & j_2 & ... & j_n \end{pmatrix}$ ve $\varphi(\sigma_1 \circ \sigma_2)=\begin{pmatrix} 1 & 2 & ... & n \\ i_{j_1} & i_{j_2} & ... & i_{j_n} \end{pmatrix}$ olur. Burada $\varphi(\sigma_1) \circ \varphi(\sigma_2)=\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & ... & n \\ j_1 & j_2 & ... & j_n \end{pmatrix}=\begin{pmatrix} 1 & 2 & ... & n \\ i_{j_1} & i_{j_2} & ... & i_{j_n} \end{pmatrix}$ olup $\varphi(\sigma_1 \circ \sigma_2)=\varphi(\sigma_1) \circ \varphi(\sigma_2)$ olur. O halde φ bir grup homomorfizmasıdır. $\varphi(\sigma_1)=\varphi(\sigma_2)$

olan herhangi $\sigma_1, \sigma_2 \in T_n$ alalım. Kabul edelim ki $\sigma_1 = \begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_{i_1} & x_{i_2} & ... & x_{i_n} \end{pmatrix}$ ve $\sigma_2 = \begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_{j_1} & x_{j_2} & ... & x_{j_n} \end{pmatrix}$ olsun. φ nin tanımından $\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix} = \varphi(\sigma_1) = \varphi(\sigma_2) = \begin{pmatrix} 1 & 2 & ... & n \\ j_1 & j_2 & ... & j_n \end{pmatrix}$ olup $i_1 = j_1,\ i_2 = j_2, ..., i_n = j_n$ olur. O halde $\sigma_1 = \begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_{i_1} & x_{i_2} & ... & x_{i_n} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_{j_1} & x_{j_2} & ... & x_{j_n} \end{pmatrix} = \sigma_2$ olur. Böylece φ birebir olur. Burada T_n ve S_n sonlu elemanlı ve $s(T_n) = s(S_n) = n!$ olduğundan Soyut Matematik Dersindeki ilgili teoremden φ aynı zamanda örtendir. Böylece $\varphi : T_n \to S_n$ bir grup izomorfizması olup istenen elde edilir.

Not: Teoremdeki izomorfizmadan dolayı bundan sonra simetrik grup denildiğinde S_n grubu, permütasyon denildiğinde S_n nin elemanları anlaşılacaktır. S_n deki $\circ$ işlemi yerine de genellikle $\cdot$ kullanılacaktır.

Tanım 3.7.4. f, $M = \{1, 2, ..., n\}$ kümesinin bir permütasyonu olmak üzere eğer birbirinden farklı $j_1, j_2, ..., j_k \in M$ $(k > 1)$ elemanları için $f(j_1) = j_2$, $f(j_2) = j_3$, …, $f(j_{k-1}) = j_k$, $f(j_k) = j_1$ ve varsa $\forall x \in M - \{j_1, j_2, ..., j_k\}$ için $f(x) = x$ ise f permütasyonuna ***k* uzunluğunda bir devir** denir ve genellikle $f = (j_1 \ \ j_2 \ \ ... \ \ j_k)$ ile ifade edilir. 1 uzunluğundaki bir devir özdeşlik fonksiyonu olarak alınır.

Not: $f = (j_1 \ \ j_2 \ \ ... \ \ j_k)$ bir devir ise tanımdan $f = (j_1 \ \ j_2 \ \ ... \ \ j_k) = (j_2 \ \ j_3 \ \ ... \ \ j_k \ \ j_1) = (j_3 \ \ ... \ \ j_k \ \ j_1 \ \ j_2) = ... = (j_k \ \ j_1 \ \ ... \ \ j_{k-2} \ \ j_{k-1})$ olduğu anlaşılır. $f = (j_1 \ \ j_2 \ \ ... \ \ j_k)$ ise f devirinin tersi $f^{-1} = (j_k \ \ j_{k-1} \ \ ... \ \ j_2 \ \ j_1) = (j_1 \ \ j_k \ \ j_{k-1} \ \ ... \ \ j_2)$ olur.

ÖRNEK: $(1 \ \ 3 \ \ 4) \in S_5$ deviri $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5$ permütasyonudur.

ÖRNEK: $(2 \ \ 4 \ \ 1 \ \ 3) \in S_6$ deviri için $(2 \ \ 4 \ \ 1 \ \ 3) = (4 \ \ 1 \ \ 3 \ \ 2) = (1 \ \ 3 \ \ 2 \ \ 4) = (3 \ \ 2 \ \ 4 \ \ 1)$ olur. Bu devirin açık şekilde yazılışı $(2 \ \ 4 \ \ 1 \ \ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 1 & 5 & 6 \end{pmatrix}$ olur.

Not: İki permütasyonun çarpımı (bileşkesi) değişmeli olmayabilir. Fakat iki devir ortak eleman bulundurmuyorsa, yani ayrık devirler ise çarpımları değişmelidir.

Teorem 3.7.5. Ayrık iki devirin çarpımı değişmelidir.

İspat: $f=(i_1 \quad i_2 \quad ... \quad i_k), g=(j_1 \quad j_2 \quad ... \quad j_s) \in S_n$ iki ayrık devir olsun. $fg=gf$ olduğunu gösterirsek istenen elde edilir. Herhangi $x \in M=\{1,2,...,n\}$ alalım. Eğer $x \notin \{i_1,i_2,...,i_k,j_1,j_2,...,j_s\}$ ise $f(x)=x$ ve $g(x)=x$ olup $(fg)(x)=f(g(x))=f(x)=x=g(x)=g(f(x))=(gf)(x)$ olur. Kabul edelim ki $x \in \{i_1,i_2,...,i_k,j_1,j_2,...,j_s\}$ olsun. Bu durumda $x \in \{i_1,i_2,...,i_k\}$ veya $x \in \{j_1,j_2,...,j_s\}$ olur. Eğer $x \in \{i_1,i_2,...,i_k\}$ ise $f(x) \in \{i_1,i_2,...,i_k\}$ olup $x \notin \{j_1,j_2,...,j_s\}$ ve $f(x) \notin \{j_1,j_2,...,j_s\}$ olduğundan $g(x)=x$ ve $g(f(x))=f(x)$ olur. Bu durumda $(gf)(x)=g(f(x))=f(x)$ ve $(fg)(x)=f(g(x))=f(x)$ olup $(fg)(x)=(gf)(x)$ olur. Eğer $x \in \{j_1,j_2,...,j_s\}$ ise $g(x) \in \{j_1,j_2,...,j_s\}$ olup $x \notin \{i_1,i_2,...,i_k\}$ ve $g(x) \notin \{i_1,i_2,...,i_k\}$ olduğundan $f(x)=x$ ve $f(g(x))=g(x)$ olur. Bu durumda da $(gf)(x)=g(f(x))=g(x)$ ve $(fg)(x)=f(g(x))=g(x)$ olup $(fg)(x)=(gf)(x)$ olur. Yani $\forall x \in M=\{1,2,...,n\}$ için $(fg)(x)=(gf)(x)$ olup $fg=gf$ olur.

Teorem 3.7.6. r uzunluğundaki bir devirin mertebesi r olur.

İspat: $f=(i_1 \quad i_2 \quad ... \quad i_r) \in S_n$ r uzunluğunda bir devir ve $M=\{1,2,...,n\}$ olsun. $\circ(f)=r$ olduğunu gösterirsek istenen elde edilir. $1 \le j,k \le r$ için $j+k \le r$ ise $f^k(i_j)=f(f(...f(f(i_j))...))=f(f(...f(i_{j+1})...))=...=i_{j+k}$ ve $j+k>r$ ise $f^k(i_j)=i_{j+k-r}$ olur. Bu durumda $1 \le j \le r$ için $j+r>r$ olduğundan $f^r(i_j)=i_{j+r-r}=i_j$ olup $f^r=I_M$ olur. Ayrıca $1 \le t<r$ için $1+t \le r$ olduğundan $f^t(i_1)=i_{1+t} \neq i_1$ olup $f^t \neq I_M$ olur. O halde $\circ(f)=r$ olup istenen elde edilir.

Teorem 3.7.7. S_n deki her permütasyon ayrık devirlerin çarpımı olarak yazılabilir ve bu yazılış birim ve sıra düşünülmeksizin tek türlüdür.

İspat: Herhangi $f \in S_n$ alalım. f nin mertebesi sonlu olduğundan $f^k(1)=1$ olacak şekilde $\exists k \in \mathbb{Z}^+$ vardır. Bu şekildeki k pozitif tamsayılarının en küçüğüne t dersek $f(1),f^2(1),...,f^t(1)=1$ elemanları birbirinden farklı olur. Böylece t uzunluğundaki $(f(1) \quad f^2(1) \quad ... \quad f^t(1))$ deviri elde edilir. İşleme 1 yerine bu devirde gözükmeyen başka bir sayı alarak devam edersek elde ettiğimiz devirler ayrık ve çarpımları f yi verir. Böylece f ayrık devirlerin çarpımı olarak yazılabilir.

Şimdi bu yazılışın birim ve sıra düşünülmeksizin tek türlü olduğunu gösterelim. Eğer f birim permütasyon ise birim düşünülmediğinden istenen elde edilir. Kabul edelim ki f birimden farklı olsun. f nin birimden farklı ayrık devirlerin çarpımı şeklinde $f=f_1f_2...f_s$ ve $f=g_1g_2...g_t$ yazılışlarını alalım. $s=t$ ve $f_1,f_2,...,f_s$ devirleri ile $g_1,g_2,...,g_t$ devirlerinin aynı olduğunu gösterirsek istenen elde edilir. $1 \le k \le s$ olan herhangi $k \in \mathbb{Z}$ alalım. $f_k=(i_1 \quad i_2 \quad ... \quad i_r)$ diyelim. $f=f_1f_2...f_s$ ve $f_1,f_2,...,f_s$ devirleri ayrık olduğundan $f(i_1)=i_2$, $f(i_2)=i_3$, …, $f(i_{r-1})=i_r$ ve $f(i_r)=i_1$ olup $f=g_1g_2...g_t$ ve $g_1,g_2,...,g_t$ devirleri ayrık olduğundan $\exists j=1,2,...,t$ için $g_j(i_1)=i_2$, $g_j(i_2)=i_3$, …, $g_j(i_{r-1})=i_r$ ve

$g_j(i_k)=i_1$ olur. Buradan $f_k=(i_1 \quad i_2 \quad ... \quad i_r)=g_j$ olduğu anlaşılır. Böylece $s\le t$ ve $f_1,f_2,...,f_s$ devirlerinin $g_1,g_2,...,g_t$ devirleri içinde olduğu anlaşılır. Benzer şekilde f_k ve g_j devirlerinin rolleri değiştirilerek $t\le s$ ve $g_1,g_2,...,g_t$ devirlerinin de $f_1,f_2,...,f_s$ devirleri içinde olduğu gösterilebilir. Böylece $s=t$ ve $f_1,f_2,...,f_s$ devirleri ile $g_1,g_2,...,g_t$ devirleri aynı olup istenen elde edilir.

ÖRNEK: $f=\begin{pmatrix}1&2&3&4&5&6\\5&3&1&6&2&4\end{pmatrix}$ permütasyonunun ayrık devirlerin çarpımı şeklinde yazılışı $f=(1 \quad 5 \quad 2 \quad 3)(4 \quad 6)$, $g=\begin{pmatrix}1&2&3&4&5&6\\4&1&5&2&3&6\end{pmatrix}$ permütasyonunun ayrık devirlerin çarpımı şeklinde yazılışı $g=(1 \quad 4 \quad 2)(3 \quad 5)$, $h=\begin{pmatrix}1&2&3&4&5&6\\3&6&5&2&1&4\end{pmatrix}$ permütasyonunun ayrık devirlerin çarpımı şeklinde yazılışı $h=(1 \quad 3 \quad 5)(2 \quad 6 \quad 4)$ olur.

Teorem 3.7.8. G bir grup, $a,b\in G$ ve $ab=ba$ olsun. Bu durumda $\forall t\in\mathbb{Z}^+$ için $(ab)^t=a^tb^t$ olur.

İspat: $ab=ba$ olduğundan $\forall t\in\mathbb{Z}^+$ için

$$(ab)^t=\underbrace{(ab)(ab)...(ab)}_{t \text{ tane}}=(aa)(bb)\underbrace{(ab)(ab)...(ab)}_{t-2 \text{ tane}}=...=\underbrace{a\cdot a\cdot ...\cdot a}_{t \text{ tane}}\cdot\underbrace{b\cdot b\cdot ...\cdot b}_{t \text{ tane}}=a^tb^t$$

olup istenen elde edilir.

Sonuç3.7.9. G bir grup, $a_1,a_2,...,a_n\in G$ ve $a_1,a_2,...,a_n$ elemanları kendi aralarında değişmeli olsun. Bu durumda $\forall t\in\mathbb{Z}^+$ için $(a_1a_2...a_n)^t=a_1{}^ta_2{}^t...a_n{}^t$ olur.

İspat: $a_1,a_2,...,a_n$ elemanları kendi aralarında değişmeli olduğundan ilgili teoremden $\forall t\in\mathbb{Z}^+$ için $(a_1a_2...a_n)^t=a_1{}^t(a_2a_3...a_n)^t=a_1{}^ta_2{}^t(a_3...a_n)^t=...=a_1{}^ta_2{}^t...a_n{}^t$ olup istenen elde edilir.

Teorem 3.7.10. Bir $f\in S_n$ permütasyonunun mertebesi ayrıldığı ayrık devirlerin uzunluklarının en küçük ortak katıdır.

İspat: f nin ayrık devirlerin çarpımı şeklinde yazılışı $f=f_1f_2...f_t$ olsun. Kabul edelim ki $\circ(f)=m$ ve $1\le i\le t$ için $\circ(f_i)=m_i$ olsun. $k=[m_1,m_2,...,m_t]=OKEK(m_1,m_2,...,m_t)$ ve $M=\{1,2,...,n\}$ diyelim. $m=k$ olduğunu gösterirsek istenen elde edilir. $1\le i\le t$ için $m_i\mid k$ olduğundan $f_i^k=I_M$ olur. Bu durumda $f_1,f_2,...,f_t$ elemanları kendi aralarında değişmeli olduğundan ilgili teoremden $f^k=(f_1f_2...f_t)^k=f_1^kf_2^k...f_t^k=I_M$ olup $\circ(f)=m$ olduğundan $m\le k$ olur.

$1\le i\le t$ olan herhangi $i\in\mathbb{Z}$ alalım. $f_i=(j_1 \quad j_2 \quad ... \quad j_{m_i})$ diyelim. $f^m=I_M$ ve $f_1,f_2,...,f_t$ devirleri ayrık olduğundan $1\le s\le m_i$ için $f_i^m(j_s)=f^m(j_s)=j_s$ olup ayrıca varsa $\forall x\in M-\{j_1,j_2,...,j_{m_i}\}$ için $f_i^m(x)=x$ olduğundan $f_i^m=I_M$ olur. Bu durumda $\circ(f_i)=m_i$ olduğundan (Cebir Dersindeki) ilgili teoremden $m_i\mid m$ olur. Yani $1\le i\le t$ için $m_i\mid m$ olup

$m>0$ ve $k=[m_1,m_2,...,m_t]=OKEK(m_1,m_2,...,m_t)$ olduğundan $k\le m$ olur. $m\le k$ ve $k\le m$ olduğundan $m=k$ olup istenen elde edilir.

ÖRNEK: $f=\begin{pmatrix}1&2&3&4&5&6\\6&5&1&4&2&3\end{pmatrix}$ permütasyonunun ayrık devirlerin çarpımı şeklinde yazılışı $f=(1\ \ 6\ \ 3)(2\ \ 5)$ olduğundan ilgili teoremden $\circ(f)=[3,2]=6$ olur.

Teorem 3.7.11. Her devir sonlu sayıda ikili devirlerin (transpozisyonların) bir çarpımı olarak yazılabilir.

İspat: $(i_1\ \ i_2\ \ ...\ \ i_k)\in S_n$ deviri verilsin. $(i_1\ \ i_2\ \ ...\ \ i_k)=(i_1\ \ i_k)(i_1\ \ i_{k-1})...(i_1\ \ i_2)$ olduğundan bu devir sonlu sayıda ikili devirlerin çarpımı olarak yazılabilir. Yani her devir sonlu sayıda ikili devirlerin bir çarpımı olarak yazılabilir.

Not: Bir devirin ikili devirlerin çarpımı olarak yazılışı tek türlü değildir. Ancak bir permütasyonun ayrıldığı ikili devirlerinin sayısının teklik ve çiftliği değişmez.

ÖRNEK: $f=(1\ \ 4\ \ 5\ \ 2)\in S_5$ deviri için

$f=(1\ \ 4\ \ 5\ \ 2)=(1\ \ 2)(1\ \ 5)(1\ \ 4)=(1\ \ 2)(1\ \ 5)(1\ \ 4)(2\ \ 3)(2\ \ 3)$

olur.

Tanım 3.7.12. Bir permütasyon çift sayıda ikilinin çarpımı ise bu permütasyona bir **çift permütasyon**, aksi halde bir **tek permütasyon** denir. S_n deki tüm çift permütasyonlar kümesi genellikle A_n ile gösterilir.

Teorem 3. 7.13. $n\ge 2$ olmak üzere S_n deki tüm çift permütasyonlar kümesi A_n, S_n nin $n!/2$ elemanlı bir alt grubudur. Bu alt gruba ***n*. alterne grup** denir.

İspat: $M=\{1,2,...,n\}$ diyelim. $a,b\in M$ ve $a\ne b$ olmak üzere $I_M=(a\ \ b)(a\ \ b)$ olduğundan $I_M\in A_n$ olup $\varnothing\ne A_n\subset S_n$ olur. Herhangi $f,g\in A_n$ alalım. $f,g\in A_n$ olduğundan f ve g permütasyonları çift sayıda ikili devirlerin çarpımı olup fg de çift sayıda ikili devirlerin çarpımı olur. O halde $fg\in A_n$ olup ayrıca S_n bir sonlu grup olduğundan (Cebir Dersindeki) ilgili teoremden $A_n<S_n$ olur.

Şimdi S_n deki çift permütasyonların sayısı ile tek permütasyonların sayısının eşit olduğunu gösterirsek $\circ(S_n)=n!$ olduğundan istenen elde edilir. S_n de çift permütasyonların sayısı n_1 ve tek permütasyonların sayısı da n_2 olsun. $n\ge 2$ olduğundan $a\ne b$ olacak şekilde $\exists a,b\in M$ vardır. S_n deki her f çift permütasyonu için $(a\ \ b)f$ bir tek permütasyondur. Bu şekilde birbirinden farklı çift permütasyonlardan birbirinden farklı tek permütasyonlar elde edilir. O halde $n_1\le n_2$ olur. Tersine, S_n deki her g tek permütasyonu için $(a\ \ b)g$ bir çift permütasyondur. Bu şekilde birbirinden farklı tek permütasyonlardan birbirinden farklı çift permütasyonlar elde edilir. O halde $n_2\le n_1$ olur. $n_1\le n_2$ ve $n_2\le n_1$ olduğundan $n_1=n_2$ olup istenen elde edilir.

Sonuç 3.7.14. $n\ge 2$ olmak üzere A_n, S_n nin indeksi 2 olan bir normal alt grubudur.

İspat: (Cebir Dersindeki) ilgili teoremlerden $\left(S_n : A_n\right) = \dfrac{n!}{n!/2} = 2$ ve $A_n \lhd S_n$ olup istenen elde edilir.

ÖRNEK: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} \in S_5$ permütasyonu için

$$f(3\ \ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}(3\ \ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}$$

ve

$$(3\ \ 5)f = (3\ \ 5)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

olur.

Tanım 3.7.15. G bir grup ve $a,b \in G$ olsun. Eğer $b = xax^{-1}$ olacak şekilde $\exists x \in G$ varsa b elemanına a nın (x ile) bir **eşleniği** denir ve genellikle $a \approx b$ ile ifade edilir.

Teorem 3.7.16. Yukarıda tanımlanan $\approx$ eşlenik olma bağıntısı G de bir denklik bağıntısıdır.
İspat: Yansıma: $\forall a \in G$ için $a = eae^{-1}$ olduğundan $a \approx a$ olup $\approx$ bağıntısının yansıma özelliği vardır.
Simetri: $a \approx b$ olan herhangi $a,b \in G$ alalım. $a \approx b$ olduğundan $b = xax^{-1}$ olacak şekilde $\exists x \in G$ vardır. $b = xax^{-1}$ olduğundan $a = x^{-1}bx = x^{-1}b\left(x^{-1}\right)^{-1}$ olup $x^{-1} = y$ dersek $y \in G$ ve $a = yby^{-1}$ olur. O halde $b \approx a$ olup $\approx$ bağıntısının simetri özelliği vardır.
Geçişme: $a \approx b$ ve $b \approx c$ olan herhangi $a,b,c \in G$ alalım. $a \approx b$ olduğundan $b = xax^{-1}$ olacak şekilde $\exists x \in G$ vardır. $b \approx c$ olduğundan $c = yby^{-1}$ olacak şekilde $\exists y \in G$ vardır. Burada $c = yby^{-1} = yxax^{-1}y^{-1} = yxa(yx)^{-1}$ olup $z = yx$ dersek $z \in G$ ve $c = zaz^{-1}$ olur. O halde $a \approx c$ olup $\approx$ bağıntısının geçişme özelliği vardır.

Böylece $\approx$ bağıntısı bir denklik bağıntısı olup istenen elde edilir.

Tanım 3.7.17. G de $\approx$ denklik bağıntısının belirttiği denklik sınıflarına **eşlenik sınıfları** denir. Bir $a \in G$ nin belirttiği eşlenik sınıfı genellikle $C(a)$ ile gösterilir. Burada $C(a) = \left\{x \in G \middle| a \approx x\right\}$ olur.

Not: Denklik sınıfları kümenin ayrışımını belirttiğinden G bir sonlu grup ise grubun mertebesi birbirinden farklı eşlenik sınıflarındaki elemanların sayıları toplamıdır. $a \in G$ olmak üzere $C(a)$ eşlenik sınıfının eleman sayısı genellikle c_a ile gösterilir. Burada c_a, G de a ile eşlenik olan elemanların sayısıdır. Eğer G de birbirinden farklı tüm eşlenik sınıflarının kümesi $a_1, a_2, ..., a_k \in G$ olmak üzere $\left\{C(a_1), C(a_2), ..., C(a_k)\right\}$ ise G nin eşlenik sınıflarına ayrılışı $G = C(a_1) \cup C(a_2) \cup ... \cup C(a_k)$ olup $\circ(G) = c_{a_1} + c_{a_2} + ... + c_{a_k}$ olur.

Şimdi S_n deki bir elemanın eşleniklerini ve S_n nin eşlenik sınıflarına ayrışımını inceleyelim.

Teorem 3.7.18. Bir $\sigma \in S_n$ için $\sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1} = (\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))$ olur.

İspat: Herhangi $x \in M = \{1,2,...,n\}$ alalım. Eğer $x \notin \{\sigma(i_1), \sigma(i_2), ..., \sigma(i_r)\}$ ise $\sigma^{-1}(x) \notin \{i_1, i_2, ..., i_r\}$ olur. Bu durumda $(\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))(x) = x$ ve $(\sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1})(x) = \sigma((i_1 \quad i_2 \quad ... \quad i_r)(\sigma^{-1}(x))) = \sigma(\sigma^{-1}(x)) = x$ olup $(\sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1})(x) = (\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))(x)$ olur. Kabul edelim ki $x \in \{\sigma(i_1), \sigma(i_2), ..., \sigma(i_r)\}$ olsun. Bu durumda $\exists k = 1,2,...,r$ için $x = \sigma(i_k)$ olur. $x = \sigma(i_k)$ olduğundan $\sigma^{-1}(x) = i_k$ olur. Eğer $k < r$ ise $(\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))(x) = (\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))(\sigma(i_k)) = \sigma(i_{k+1})$ ve $(\sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1})(x) = \sigma((i_1 \quad i_2 \quad ... \quad i_r)(\sigma^{-1}(x))) = \sigma((i_1 \quad i_2 \quad ... \quad i_r)(i_k)) = \sigma(i_{k+1})$ olup $(\sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1})(x) = (\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))(x)$ olur. Eğer $k = r$ ise $(\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))(x) = (\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))(\sigma(i_r)) = \sigma(i_1)$ ve $(\sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1})(x) = \sigma((i_1 \quad i_2 \quad ... \quad i_r)(\sigma^{-1}(x))) = \sigma((i_1 \quad i_2 \quad ... \quad i_r)(i_r)) = \sigma(i_1)$ olup yine $(\sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1})(x) = (\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))(x)$ olur. Yani $\forall x \in M = \{1,2,...,n\}$ için $(\sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1})(x) = (\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))(x)$ olup $\sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1} = (\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r))$ olur.

Sonuç 3.7.19. İki devirin eşlenik olması için gerek ve yeter koşul aynı uzunlukta olmalarıdır.

İspat: $(\Rightarrow)$ Bir önceki teoremden açıktır.

$(\Leftarrow)$ S_n de uzunlukları eşit herhangi iki $(i_1 \quad i_2 \quad ... \quad i_r)$ ve $(j_1 \quad j_2 \quad ... \quad j_r)$ devirleri verilsin. Bu devirlerin eşlenik olduklarını gösterirsek istenen elde edilir. $1 \le k \le r$ için j_k elemanını i_k nın altına ve $M = \{1,2,...,n\}$ kümesinin varsa $j_1, j_2, ..., j_r$ dışımdaki elemanlarını da bu kümenin $i_1, i_2, ..., i_r$ elemanları dışındaki elemanlarının altına yazarak bir σ permütasyonu oluşturabiliriz. $1 \le k \le r$ için $\sigma(i_k) = j_k$ olduğundan bir önceki teoremden $(j_1 \quad j_2 \quad ... \quad j_r) = (\sigma(i_1) \quad \sigma(i_2) \quad ... \quad \sigma(i_r)) = \sigma(i_1 \quad i_2 \quad ... \quad i_r)\sigma^{-1}$ olup $(i_1 \quad i_2 \quad ... \quad i_r)$ ve $(j_1 \quad j_2 \quad ... \quad j_r)$ devirleri eşlenik olur.

Teorem 3.7.20. S_n deki iki permütasyonun eşlenik olması için gerek ve yeter koşul bu permütasyonların ayrık devirlere ayrılışındaki devirlerin sayısının ve uzunluklarının aynı olmasıdır.

İspat: $(\Rightarrow)$ S_n de eşlenik herhangi iki f ve g permütasyonlarını alalım. f ve g nin ayrık devirlere ayrılışındaki devirlerin sayısının ve uzunluklarının aynı olduğunu gösterirsek istenen elde edilir. f nin ayrık devirlerin çarpımı şeklinde yazılışı $f = f_1 f_2 ... f_r$ olsun. $f \approx g$ olduğundan $g = \sigma f \sigma^{-1}$ olacak şekilde $\exists \sigma \in S_n$ vardır. Burada $g = \sigma f \sigma^{-1} = \sigma f_1 f_2 ... f_r \sigma^{-1} = \sigma f_1 \sigma^{-1} \sigma f_2 \sigma^{-1} ... \sigma f_r \sigma^{-1}$ olup $1 \le i \le r$ için $g_i = \sigma f_i \sigma^{-1}$ dersek g nin ayrık devirlere ayrılışı $g = g_1 g_2 ... g_r$ olur. Ayrıca $1 \le i \le r$ için $g_i = \sigma f_i \sigma^{-1}$ olduğundan f_i ile g_i devirlerinin uzunlukları aynı olup istenen elde edilir.

$(\Leftarrow)$ $f,g\in S_n$ için f ve g nin ayrık devirlere ayrılışı sırasıyla $f=f_1f_2...f_r$ ve $g=g_1g_2...g_r$ olmak üzere kabul edelim ki $1\le i\le r$ için f_i ile g_i devirlerinin uzunlukları aynı olsun. $f\approx g$ olduğunu gösterirsek istenen elde edilir. Burada $1\le i\le r$ için g_i devirinin elemanlarını f_i devirinin aynı sıradaki elemanlarının altına ve $M=\{1,2,...,n\}$ kümesinin varsa $g_1,g_2,...,g_r$ devirlerinin elemanları dışındaki elemanlarını da bu kümenin $f_1,f_2,...,f_r$ devirlerinin elemanları dışındaki elemanlarının altına yazarak bir σ permütasyonunu oluşturabiliriz. Bu durumda $1\le i\le r$ için $g_i=\sigma f_i\sigma^{-1}$ olup $g=g_1g_2...g_r=\sigma f_1\sigma^{-1}\sigma f_2\sigma^{-1}...\sigma f_r\sigma^{-1}=\sigma f\sigma^{-1}$ olup $f\approx g$ olur.

ÖRNEK: $\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&5&1&4&2&3\end{pmatrix}\in S_6$ permütasyonu için

$\sigma(2\ \ 1\ \ 3\ \ 4)\sigma^{-1}=(\sigma(2)\ \ \sigma(1)\ \ \sigma(3)\ \ \sigma(4))=(5\ \ 6\ \ 1\ \ 4)$

olur.

ÖRNEK: S_6 da $(2\ \ 1\ \ 5)$ ile $(4\ \ 2\ \ 3)$ devirleri birbirine denktir. Şimdi S_6 da $\sigma(2\ \ 1\ \ 5)\sigma^{-1}=(4\ \ 2\ \ 3)$ şartını sağlayan σ permütasyonlarının kümesini bulalım. Bunun için $(\sigma(2)\ \ \sigma(1)\ \ \sigma(5))=(4\ \ 2\ \ 3)$ şartını sağlayan permütasyonlar bulunmalıdır. Bu permütasyonlar

$\sigma_1=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&5&3&6\end{pmatrix}$, $\sigma_2=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&6&3&5\end{pmatrix}$, $\sigma_3=\begin{pmatrix}1&2&3&4&5&6\\2&4&5&1&3&6\end{pmatrix}$,

$\sigma_4=\begin{pmatrix}1&2&3&4&5&6\\2&4&5&6&3&1\end{pmatrix}$, $\sigma_5=\begin{pmatrix}1&2&3&4&5&6\\2&4&6&1&3&5\end{pmatrix}$, $\sigma_6=\begin{pmatrix}1&2&3&4&5&6\\2&4&6&5&3&1\end{pmatrix}$

$\sigma_7=\begin{pmatrix}1&2&3&4&5&6\\4&3&1&5&2&6\end{pmatrix}$, $\sigma_8=\begin{pmatrix}1&2&3&4&5&6\\4&3&1&6&2&5\end{pmatrix}$, $\sigma_9=\begin{pmatrix}1&2&3&4&5&6\\4&3&5&1&2&6\end{pmatrix}$,

$\sigma_{10}=\begin{pmatrix}1&2&3&4&5&6\\4&3&5&6&2&1\end{pmatrix}$, $\sigma_{11}=\begin{pmatrix}1&2&3&4&5&6\\4&3&6&1&2&5\end{pmatrix}$, $\sigma_{12}=\begin{pmatrix}1&2&3&4&5&6\\4&3&6&5&2&1\end{pmatrix}$

$\sigma_{13}=\begin{pmatrix}1&2&3&4&5&6\\3&2&1&5&4&6\end{pmatrix}$, $\sigma_{14}=\begin{pmatrix}1&2&3&4&5&6\\3&2&1&6&4&5\end{pmatrix}$, $\sigma_{15}=\begin{pmatrix}1&2&3&4&5&6\\3&2&5&1&4&6\end{pmatrix}$,

$\sigma_{16}=\begin{pmatrix}1&2&3&4&5&6\\3&2&5&6&4&1\end{pmatrix}$, $\sigma_{17}=\begin{pmatrix}1&2&3&4&5&6\\3&2&6&1&4&5\end{pmatrix}$, $\sigma_{18}=\begin{pmatrix}1&2&3&4&5&6\\3&2&6&5&4&1\end{pmatrix}$

olup yukarıdaki şartı sağlayan σ permütasyonlarının kümesi $\{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6,\sigma_7,\sigma_8,\sigma_9,\sigma_{10},\sigma_{11},\sigma_{12},\sigma_{13},\sigma_{14},\sigma_{15},\sigma_{16},\sigma_{17},\sigma_{18}\}$ kümesidir.

ÖRNEK: S_6 da $f=\begin{pmatrix}1&2&3&4&5&6\\4&6&1&3&5&2\end{pmatrix}$ permütasyonunun $\sigma=\begin{pmatrix}1&2&3&4&5&6\\3&1&4&6&2&5\end{pmatrix}$ permütasyonu ile eşleniğini bulalım.

Çözüm: f nin ayrık devirlerin çarpımı şeklinde yazılışı $f=(1\ \ 4\ \ 3)(2\ \ 6)$ dır. O halde f nin σ permütasyonu ile eşleniği

$\sigma f \sigma^{-1} = \sigma(1 \quad 4 \quad 3)(2 \quad 6)\sigma^{-1} = \sigma(1 \quad 4 \quad 3)\sigma^{-1}\sigma(2 \quad 6)\sigma^{-1} =$
$= (\sigma(1) \quad \sigma(4) \quad \sigma(3))(\sigma(2) \quad \sigma(6)) = (3 \quad 6 \quad 4)(1 \quad 5)$
olur.

Tanım 3.7.21. $n \in \mathbb{Z}^+$ olsun. $n_1 \le n_2 \le ... \le n_r$ ve $n = n_1 + n_2 + ... + n_r$ koşullarını sağlayan bir $n_1, n_2, ..., n_r$ pozitif tamsayılar dizisine n nin bir **ayrışımı** denir. n nin tüm ayrışımları sayısı genellikle $p(n)$ ile gösterilir.

ÖRNEK: 1 in ayrışımı sadece 1=1 olduğundan $p(1) = 1$ olur.
2 nin ayrışımları 2=2 ve 2=1+1 olduğundan $p(2) = 2$ olur.
3 ün ayrışımları 3=3, 3=1+2 ve 3=1+1+1 olduğundan $p(3) = 3$ olur.
4 ün ayrışımları 4=4, 4=1+3, 4=1+1+2, 4=1+1+1+1 ve 4=2+2 olduğundan $p(4) = 5$ olur.

Teorem 3.7.22. S_n deki farklı eşlenik sınıflarının sayısı $p(n)$ olur.
İspat: İlgili teoremden bir eşlenik sınıfındaki tüm permütasyonların ayrık devirlere ayrılışındaki devirlerin sayısı ve bu devirlerin uzunlukları aynıdır. S_n de bir permütasyonu ayrık devirlere ayırdığımızda bu devirlere $M = \{1, 2, ..., n\}$ kümesinin bu devirlerdeki elemanlar dışındaki eleman sayısı kadar 1 uzunluğunda devirler ilave ettiğimizde elde edilen devirlerin uzunlukları toplamı n yi verir. Yani S_n deki her permütasyona n nin bir ayrışımı karşılık gelir. Tersine, n nin her $n = n_1 + n_2 + ... + n_r \ (0 < n_1 \le n_2 \le ... \le n_r)$ ayrışımına karşılık uzunlukları sırasıyla $n_1, n_2, ..., n_r$ olan $f_1, f_2, ..., f_r$ devirleri ve bunların çarpımı olan $f = f_1 f_2 ... f_r \in S_n$ permütasyonu vardır. O halde S_n deki farklı eşlenik sınıflarının sayısı $p(n)$ olup istenen elde edilir.

ÖRNEK: $p(4) = 5$ olduğundan S_4 de farklı eşlenik sınıflarının sayısı 5 olur. Bu sınıflar aşağıdakilerdir:
$C_1 = \{I\}$,
$C_2 = \{(1 \quad 2 \quad 3), (1 \quad 2 \quad 4), (1 \quad 3 \quad 2), (1 \quad 4 \quad 2), (1 \quad 3 \quad 4), (1 \quad 4 \quad 3), (2 \quad 3 \quad 4), (2 \quad 4 \quad 3)\}$,
$C_3 = \{(1 \quad 2), (1 \quad 3), (1 \quad 4), (2 \quad 3), (2 \quad 4), (3 \quad 4)\}$,
$C_4 = \{(1 \quad 2)(3 \quad 4), (1 \quad 3)(2 \quad 4), (1 \quad 4)(2 \quad 3)\}$,
$C_5 = \{(1 \quad 2 \quad 3 \quad 4), (1 \quad 2 \quad 4 \quad 3), (1 \quad 3 \quad 2 \quad 4), (1 \quad 3 \quad 4 \quad 2), (1 \quad 4 \quad 2 \quad 3), (1 \quad 4 \quad 3 \quad 2)\}$.

Teorem 3.7. 23. A_n tüm üçlü devirlerin kümesi ile üretilmiştir.
İspat: S_n nin tüm üçlü devirlerin ürettiği alt grubuna T diyelim. $T = A_n$ olduğunu gösterirsek istenen elde edilir. Herhangi $f = (i_1 \quad i_2 \quad i_3)$ üçlü devirini alalım. $f = (i_1 \quad i_2 \quad i_3) = (i_1 \quad i_3)(i_1 \quad i_2)$ olduğundan $f \in A_n$ olur. O halde $T \subset A_n$ olur. Şimdi ters kapsamayı gösterelim. Bunun için S_n de her $(a \quad b)$ ve $(c \quad d)$ ikili devirleri için $(a \quad b)(c \quad d) \in T$ olduğunu göstermemiz yeterlidir. S_n de herhangi $(a \quad b)$ ve $(c \quad d)$ ikili

devirleri verilsin. Eğer $(a\ \ b)=(c\ \ d)$ ise $(a\ \ b)(c\ \ d)=I_M\in T$ olur. Eğer $b=c$ ve $a\neq d$ ise $(a\ \ b)(c\ \ d)=(a\ \ b)(b\ \ d)=(a\ \ b\ \ d)\in T$ olur. Eğer a,b,c,d sayıları birbirinden farklı ise yine $(a\ \ b)(c\ \ d)=(a\ \ b\ \ c)(b\ \ c\ \ d)\in T$ olur. Böylece $A_n\subset T$ olup ayrıca $T\subset A_n$ olduğundan $T=A_n$ olur.

Teorem 3.7.24. $n\geq 5$ ve $N\lhd A_n$ olsun. Eğer N bir üçlü devir kapsarsa $N=A_n$ olur.

İspat: N bir üçlü $(i_1\ \ i_2\ \ i_3)$ devirini kapsasın. N nin bütün üçlü devirleri kapsadığını gösterirsek istenen elde edilir. $n\geq 5$ olduğundan S_n de $(i_1\ \ i_2\ \ i_3)$ deviri ile ayrık en az bir $(a\ \ b)$ ikili deviri vardır. Herhangi $(j_1\ \ j_2\ \ j_3)$ üçlü devirini alalım. İlgili teoremden $(i_1\ \ i_2\ \ i_3)$ ile $(j_1\ \ j_2\ \ j_3)$ devirleri eşlenik olup $(j_1\ \ j_2\ \ j_3)=\sigma(i_1\ \ i_2\ \ i_3)\sigma^{-1}=(\sigma(i_1)\ \ \sigma(i_2)\ \ \sigma(i_3))$ olacak şekilde $\exists\sigma\in S_n$ vardır. Eğer burada $\sigma\in A_n$ ise $(i_1\ \ i_2\ \ i_3)\in N$ ve $N\lhd A_n$ olduğundan $(j_1\ \ j_2\ \ j_3)=\sigma(i_1\ \ i_2\ \ i_3)\sigma^{-1}\in N$ olur. $\sigma\notin A_n$ olsun. Bu durumda $f=\sigma(a\ \ b)$ dersek $f\in A_n$ olur. Burada $(i_1\ \ i_2\ \ i_3)$ deviri ile $(a\ \ b)$ deviri ayrık olduğundan $f(i_1)=\sigma(i_1)$, $f(i_2)=\sigma(i_2)$ ve $f(i_3)=\sigma(i_3)$ olup $(j_1\ \ j_2\ \ j_3)=(\sigma(i_1)\ \ \sigma(i_2)\ \ \sigma(i_3))=(f(i_1)\ \ f(i_2)\ \ f(i_3))=f(i_1\ \ i_2\ \ i_3)f^{-1}$ olur. Bu durumda yine $N\lhd A_n$ olduğundan $(j_1\ \ j_2\ \ j_3)=f(i_1\ \ i_2\ \ i_3)f^{-1}\in N$ olur. Yani N bütün üçlü devirleri kapsar.

Teorem 3.7. 25. A_n alterne grubunun basit olması için gerek ve yeter koşul $n\neq 4$ olmasıdır.

İspat: $(\Rightarrow)$ A_n alterne grubu basit olsun. Eğer $n=4$ olsa A_4 ün $V_4=\{I,(1\ \ 2)(3\ \ 4),(1\ \ 3)(2\ \ 4),(1\ \ 4)(2\ \ 3)\}$ alt grubu için $V_4\lhd A_4$ olur. Dahası, $V_4\lhd S_4$ olur. Çünkü V_4 deki her elemanın her $\sigma\in S_4$ ile eşleniği yine V_4 ün bir elemanı olur. Ayrıca $V_4\neq\{I\}$ ve $V_4\neq A_4$ olduğundan A_4 basit değildir. O halde $n\neq 4$ olup istenen elde edilir.

$(\Leftarrow)$ $n\neq 4$ olsun. Eğer $n=2$ ise $s(A_2)=\dfrac{2!}{2}=1$ olduğundan $A_2=\{I\}$ olup basittir. Eğer $n=3$ ise $s(A_3)=\dfrac{3!}{2}=3$ ve 3 bir asal sayı olduğundan A_3 grubu da basittir. Kabul edelim ki $n\geq 5$ olsun. A_n nin $\{I_M\}$ den farklı herhangi N normal alt grubunu alalım. $N=A_n$ olduğunu gösterirsek istenen elde edilir. Bunun için ispatı aşağıdaki altı durumda yapmamız yeterlidir.

1. durum: Eğer N normal alt grubu bir üçlü devir kapsarsa ilgili teoremden $N=A_n$ olur.

2. durum: N normal alt grubu $r\geq 4$ olmak üzere ayrık devirlere ayrılışında r uzunluğunda en az bir $(i_1\ \ i_2\ \ \ldots\ \ i_r)$ deviri bulunan bir σ permütasyonu kapsasın. Burada σ nın ayrık devirlere ayrılışındaki (varsa) $(i_1\ \ i_2\ \ \ldots\ \ i_r)$ deviri dışındaki devirlerin çarpımına f dersek $\sigma=(i_1\ \ i_2\ \ \ldots\ \ i_r)f$ şeklinde olur. $g=(i_1\ \ i_2\ \ i_3)\in A_n$ elemanını alırsak $\sigma\in N$ ve $N\lhd A_n$ olduğundan $g\sigma g^{-1}\in N$ olup ayrıca $\sigma^{-1}\in N$ olduğundan $\sigma^{-1}g\sigma g^{-1}\in N$ olur. Öte yandan

$\sigma^{-1}g\sigma g^{-1} = f^{-1}(i_r \quad i_{r-1} \quad ... \quad i_1)(i_1 \quad i_2 \quad i_3)(i_1 \quad i_2 \quad ... \quad i_r) f (i_3 \quad i_2 \quad i_1) =$
$= f^{-1} f (i_r \quad i_{r-1} \quad ... \quad i_1)(i_1 \quad i_2 \quad i_3)(i_1 \quad i_2 \quad ... \quad i_r)(i_3 \quad i_2 \quad i_1) = (i_1 \quad i_3 \quad i_r)$

olur. O halde $(i_1 \quad i_3 \quad i_r) \in N$ olup 1. durumdan $N = A_n$ olur.

3. durum: N normal alt grubu ayrık devirlere ayrılışında iki tane ayrık $(i_1 \quad i_2 \quad i_3)$ ve $(i_4 \quad i_5 \quad i_6)$ devirleri bulunan bir σ permütasyonu kapsasın. Burada σ nın ayrık devirlere ayrılışındaki (varsa) $(i_1 \quad i_2 \quad i_3)$ ve $(i_4 \quad i_5 \quad i_6)$ devirleri dışındaki devirlerin çarpımına f dersek $\sigma = (i_1 \quad i_2 \quad i_3)(i_4 \quad i_5 \quad i_6) f$ şeklinde olur. $g = (i_1 \quad i_2 \quad i_4) \in A_n$ elemanını alırsak $\sigma \in N$ ve $N \lhd A_n$ olduğundan $g\sigma g^{-1} \in N$ olup ayrıca $\sigma^{-1} \in N$ olduğundan $\sigma^{-1}g\sigma g^{-1} \in N$ olur. Öte yandan

$\sigma^{-1}g\sigma g^{-1} = f^{-1}(i_6 \quad i_5 \quad i_4)(i_3 \quad i_2 \quad i_1)(i_1 \quad i_2 \quad i_4)(i_1 \quad i_2 \quad i_3)(i_4 \quad i_5 \quad i_6) f (i_4 \quad i_2 \quad i_1) =$
$= f^{-1} f (i_6 \quad i_5 \quad i_4)(i_3 \quad i_2 \quad i_1)(i_1 \quad i_2 \quad i_4)(i_1 \quad i_2 \quad i_3)(i_4 \quad i_5 \quad i_6)(i_4 \quad i_2 \quad i_1) = (i_1 \quad i_4 \quad i_2 \quad i_6 \quad i_3)$

olur. O halde $(i_1 \quad i_4 \quad i_2 \quad i_6 \quad i_3) \in N$ olup 2. durumdan $N = A_n$ olur.

4. durum: N normal alt grubu ayrık devirlere ayrılışında bir tane $(i_1 \quad i_2 \quad i_3)$ üçlü deviri ve diğerleri ikili devirler olan bir σ permütasyonu kapsasın. Burada ikili devirlerin çarpımına f dersek $\sigma = (i_1 \quad i_2 \quad i_3) f$ olur. $N < A_n$ olduğundan $\sigma^2 \in N$ olur. Burada f ayrık ikili devirlerin çarpımı olduğundan $f^2 = I_M$ olup $\sigma^2 = (i_1 \quad i_2 \quad i_3)^2 f^2 = (i_1 \quad i_2 \quad i_3)(i_1 \quad i_2 \quad i_3) = (i_1 \quad i_3 \quad i_2)$ olur. O halde $(i_1 \quad i_3 \quad i_2) \in N$ olup 1. durumdan $N = A_n$ olur.

5. durum: N normal alt grubu iki ayrık $(i_1 \quad i_2)$ ve $(i_3 \quad i_4)$ devirlerinin çarpımı olan bir σ permütasyonu kapsasın. $n \geq 5$ olduğundan $\exists i_5 \in \{1,2,...,n\} - \{i_1, i_2, i_3, i_4\}$ vardır. $g = (i_1 \quad i_3 \quad i_5) \in A_n$ elemanını alırsak $\sigma \in N$ ve $N \lhd A_n$ olduğundan $g\sigma g^{-1} \in N$ olup ayrıca $\sigma^{-1} \in N$ olduğundan $\sigma^{-1}g\sigma g^{-1} \in N$ olur. Öte yandan

$\sigma^{-1}g\sigma g^{-1} = (i_1 \quad i_2)(i_3 \quad i_4)(i_1 \quad i_3 \quad i_5)(i_1 \quad i_2)(i_3 \quad i_4)(i_5 \quad i_3 \quad i_1) = (i_1 \quad i_2 \quad i_4 \quad i_5 \quad i_3)$

olur. O halde $(i_1 \quad i_2 \quad i_4 \quad i_5 \quad i_3) \in N$ olup 2. durumdan $N = A_n$ olur.

6. durum: N normal alt grubu ikiden fazla ayrık ikili devirlerin çarpımı olan bir σ permütasyonu kapsasın. Buradaki ikili devirlerin ilk üçü $(i_1 \quad i_2)$, $(i_3 \quad i_4)$ ve $(i_5 \quad i_6)$ ise diğerlerinin çarpımına f dersek $\sigma = (i_1 \quad i_2)(i_3 \quad i_4)(i_5 \quad i_6) f$ olur. $g = (i_1 \quad i_3 \quad i_5) \in A_n$ elemanını alırsak $\sigma \in N$ ve $N \lhd A_n$ olduğundan $g\sigma g^{-1} \in N$ olup ayrıca $\sigma^{-1} \in N$ olduğundan $\sigma^{-1}g\sigma g^{-1} \in N$ olur. Öte yandan

$\sigma^{-1}g\sigma g^{-1} = f^{-1}(i_1 \quad i_2)(i_3 \quad i_4)(i_5 \quad i_6)(i_1 \quad i_3 \quad i_5)(i_1 \quad i_2)(i_3 \quad i_4)(i_5 \quad i_6) f (i_5 \quad i_3 \quad i_1) =$
$= f^{-1} f (i_1 \quad i_2)(i_3 \quad i_4)(i_5 \quad i_6)(i_1 \quad i_3 \quad i_5)(i_1 \quad i_2)(i_3 \quad i_4)(i_5 \quad i_6)(i_5 \quad i_3 \quad i_1) = (i_1 \quad i_5 \quad i_3)(i_2 \quad i_4 \quad i_6)$

olur. O halde $(i_1 \quad i_5 \quad i_3)(i_2 \quad i_4 \quad i_6) \in N$ olup 3. durumdan $N = A_n$ olur.

Sonuç olarak $N = A_n$ olup istenen elde edilir.

Tanım 3.7.26. Teoremin ispatında geçen V_4 grubuna **Kleinin 4-lü grubu** denir.

Tanım 3.7.27. G bir grup ve p bir asal tamsayı olsun. Eğer G nin her elemanının mertebesi p nin bir kuvveti ise G ye bir ***p*-grup** denir. G nin bir H alt grubu bir p-grup ise H ye G nin bir ***p*-alt grubu** denir.

Teorem 3.7.28. G sonlu ve değişmeli bir grup ve p bir asal tamsayı olsun. G grubunun, mertebesi p nin bir kuvveti olan elemanlarının oluşturduğu

$$G_p = \left\{ a \in G \middle| \exists k \in \mathbb{N} \text{ için } \circ(a) = p^k \right\}$$

kümesi G nin bir alt grubudur. G_p ye G nin **maksimal *p*-alt grubu** veya **Sylow *p*-alt grubu** denir.

İspat: $\circ(e) = 1 = p^0$ olduğundan $e \in G_p$ olup $G_p \neq \varnothing$ olur. Ayrıca $G_p \subset G$ olduğu da açıktır. Yani $\varnothing \neq G_p \subset G$ olur. Herhangi $a, b \in G_p$ alalım. $a, b \in G_p$ olduğundan $\circ(a) = p^k$ ve $\circ(b) = p^t$ olacak şekilde $\exists k, t \in \mathbb{N}$ vardır. $s = \max\{k, t\}$ diyelim. Burada $p^k \mid p^s$ ve $p^t \mid p^s$ olup (Cebir Dersindeki) ilgili teoremden $a^{p^s} = e$ ve $b^{p^s} = e$ olur. Bu durumda G değişmeli olduğundan $\left(ab^{-1}\right)^{p^s} = a^{p^s} b^{-p^s} = e\left(b^{p^s}\right)^{-1} = ee^{-1} = e$ olup $\circ\left(ab^{-1}\right) \mid p^s$ olur. $\circ\left(ab^{-1}\right) \mid p^s$ olduğundan $\circ\left(ab^{-1}\right)$, p nin bir kuvveti olup G_p nin tanımından $ab^{-1} \in G_p$ olur. Yani $\forall a, b \in G_p$ için $ab^{-1} \in G_p$ olup (Cebir Dersindeki) ilgili teoremden $G_p < G$ olur.

ÖRNEK: Mertebesi bir p asal tamsayısının bir kuvveti olan bir grup bir p-gruptur.

ÖRNEK: Kleinin 4-lü grubu bir 2-gruptur.

ÖRNEK: $\left(\mathbb{Z}_{12}, +\right)$ grubunu göz önüne alalım. Bu grup bir p-grup değildir. Bu grubun 2-alt grupları $H = \left\{\overline{0}, \overline{6}\right\}$ ve $G_2 = \left\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\right\}$, 3-alt grubu $G_3 = \left\{\overline{0}, \overline{4}, \overline{8}\right\}$, 5-alt grubu $G_5 = \left\{\overline{0}\right\}$ olur.