3.3. DEVİRLİ GRUPLAR:

Tanım 3.3.1. G bir grup ve M, G nin bir alt kümesi olsun. G nin M yi kapsayan bütün alt gruplarının kesişimine ***M* nin ürettiği (doğurduğu) alt grup** denir ve genellikle $< M >$ ile ifade edilir. M nin elemanlarına da $< M >$ grubunun **üreteçleri (doğurayları)** denir.

Not: $H < G$ ve $M \subset H$ ise tanimdan $< M > \subset H$ olduğu anlaşılır. Dolayısıyla $< M >$, G nin M yi kapsayan en küçük alt grubudur.

Not: G bir grup ve $M = \varnothing$ ise $< M > = \{e\}$ dir.

Teorem 3.3.2. G bir grup ve $\varnothing \neq M \subset G$ olsun. Bu durumda

$$< M > = \left\{ a_1^{n_1} a_2^{n_2} ... a_r^{n_r} \,\middle|\, r \in \mathbb{Z}^+,\ n_1, n_2, ..., n_r \in \mathbb{Z},\ a_1, a_2, ..., a_r \in M \right\}$$

olur.

İspat: $A = \left\{ a_1^{n_1} a_2^{n_2} ... a_r^{n_r} \,\middle|\, r \in \mathbb{Z}^+,\ n_1, n_2, ..., n_r \in \mathbb{Z},\ a_1, a_2, ..., a_r \in M \right\}$ diyelim. $\forall a \in M$ için $a = a^1 \in A$ olup $M \subset A$ olur. Burada $M \neq \varnothing$ olduğundan $A \neq \varnothing$ olur. Ayrıca $A \subset G$ olduğu da açıktır. Yani $\varnothing \neq A \subset G$ olur. Herhangi $x, y \in A$ alalım. $x, y \in A$ olduğundan

$x = a_1^{n_1} a_2^{n_2} ... a_r^{n_r}$ ve $y = b_1^{m_1} b_2^{m_2} ... b_s^{m_s}$ olacak şekilde $\exists r, s \in \mathbb{Z}^+$, $\exists n_1, n_2, ..., n_r, m_1, m_2, ..., m_s \in \mathbb{Z}$ ve $\exists a_1, a_2, ..., a_r, b_1, b_2, ..., b_s \in M$ vardır. $x = a_1^{n_1} a_2^{n_2} ... a_r^{n_r}$ ve $y = b_1^{m_1} b_2^{m_2} ... b_s^{m_s}$ olduğundan $xy^{-1} = a_1^{n_1} a_2^{n_2} ... a_r^{n_r} \left(b_1^{m_1} b_2^{m_2} ... b_s^{m_s} \right)^{-1} = a_1^{n_1} a_2^{n_2} ... a_r^{n_r} b_s^{-m_s} b_{s-1}^{-m_{s-1}} ... b_1^{-m_1}$ olup burada $n_1, n_2, ..., n_r, -m_s, -m_{s-1}, ..., -m_1 \in \mathbb{Z}$ ve $a_1, a_2, ..., a_r, b_s, b_{s-1}, ..., b_1 \in M$ olduğundan A nın tanımından $xy^{-1} = a_1^{n_1} a_2^{n_2} ... a_r^{n_r} b_s^{-m_s} b_{s-1}^{-m_{s-1}} ... b_1^{-m_1} \in A$ olur. Yani $\forall x, y \in A$ için $xy^{-1} \in A$ olup ilgili teoremden $A < G$ olur. $M \subset A$ ve $A < G$ olduğundan $< M > \subset A$ olur.

Herhangi $x \in A$ alalım. $x \in A$ olduğundan $x = a_1^{n_1} a_2^{n_2} ... a_r^{n_r}$ olacak şekilde $\exists r \in \mathbb{Z}^+$, $\exists n_1, n_2, ..., n_r \in \mathbb{Z}$ ve $\exists a_1, a_2, ..., a_r \in M$ vardır. Burada $a_1, a_2, ..., a_r \in M$ ve $M \subset < M >$ olduğundan $a_1, a_2, ..., a_r \in < M >$ olup $< M > < G$ olduğundan $x = a_1^{n_1} a_2^{n_2} ... a_r^{n_r} \in < M >$ olur. Yani $\forall x \in A$ için $x \in < M >$ olup $A \subset < M >$ olur. Ayrıca $< M > \subset A$ olduğundan $< M > = A = \left\{ a_1^{n_1} a_2^{n_2} ... a_r^{n_r} \,\middle|\, r \in \mathbb{Z}^+,\ n_1, n_2, ..., n_r \in \mathbb{Z},\ a_1, a_2, ..., a_r \in M \right\}$ olup istenen elde edilir.

Tanım 3.3.3. G bir grup ve $M \subset G$ olmak üzere $G = < M >$ ise G ye ***M* ile üretilmiş grup** denir. $G = < M >$ olacak şekilde G nin sonlu elemanlı bir M alt kümesi varsa G ye bir **sonlu**

üretilmiş grup denir. Eğer $G =< \{a\} >$ olacak şekilde $\exists a \in G$ varsa G ye ***a*** **elemanı ile üretilmiş bir devirli grup** denir ve genellikle $G =< a >$ olarak yazılır.

Not: Teoremden $< a >= \left\{ a^n \middle| n \in \mathbb{Z} \right\}$ olur. Eğer burada G toplamsal grup olarak alınırsa a elemanının ürettiği devirli grup $< a >= \left\{ na \middle| n \in \mathbb{Z} \right\}$ olur.

Not: Devirli bir grup değişmelidir.

ÖRNEK: $\mathbb{Z}$ Tamsayılar kümesi bildiğimiz + işlemine göre 1 ile üretilmiş bir sonsuz devirli gruptur.

ÖRNEK: $G = \{1, -1, i, -i\}$ kümesi kompleks sayılarda bildiğimiz çarpma işlemine göre i ile üretilmiş 4. mertebeden bir devirli gruptur.

Teorem 3.3.4. $G =< a >$ bir devirli grup olsun. Bu takdirde G nin mertebesinin sonlu olması için gerek ve yeter koşul a nın bazı farklı pozitif tamsayı kuvvetlerinin aynı olmasıdır.

Sonuç 3.3.5. $G =< a >$, t. mertebeden bir devirli grup olsun. Bu durumda t, $a^k = e$ olan k pozitif tamsayıların en küçüğüdür. Ayrıca $G = \{a, a^2, ..., a^t = e\}$ olur.

Sonuç 3.3.6. $G =< a >$ bir devirli grup olsun. Bu takdirde G nin mertebesinin sonlu olması için gerek ve yeter koşul a nın bazı farklı tamsayı kuvvetlerinin aynı olmasıdır.

Sonuç 3.3.7. $G =< a >$ bir devirli grup olsun. Eğer $G = \{a^n \mid n \in \mathbb{Z}^+\}$ ise G nin mertebesi sonludur.

Teorem 3.3.8. Devirli bir grubun her alt grubu da devirlidir.

Teorem 3.3.9. $G =< a >$ bir sonsuz devirli grup ise G nin $\{e\}$ den farklı her alt grubu da bir sonsuz devirli gruptur.

İspat: $G =< a >$ bir sonsuz devirli grup, $H < G$ ve $H \neq \{e\}$ olsun. Bir önceki teoremden H de devirli olup $H =< b >$ olacak şekilde $\exists b \in H$ vardır. Şimdi H nin mertebesinin sonlu olmadığını gösterirsek istenen elde edilir. Aksini kabul edelim. Yani H nin mertebesinin sonlu olduğunu kabul edelim. Bu durumda ilgili teoremden $b^{s_1} = b^{s_2}$ ve $s_1 \neq s_2$ olacak şekilde

$\exists s_1, s_2 \in \mathbb{Z}$ vardır. $H = < b >$ ve $H \neq \{e\}$ olduğundan $b \neq e$ olur. $b \in H \subset G = < a >$ olduğundan $b = a^n$ olacak şekilde $\exists n \in \mathbb{Z}$ vardır. $b = a^n$ ve $b \neq e$ olduğundan $n \neq 0$ olur. $s_1 \neq s_2$ ve $n \neq 0$ olduğundan $ns_1 \neq ns_2$ olur. $b = a^n$ ve $b^{s_1} = b^{s_2}$ olduğundan $a^{ns_1} = \left(a^n\right)^{s_1} = b^{s_1} = b^{s_2} = \left(a^n\right)^{s_2} = a^{ns_2}$ olup $ns_1 \neq ns_2$ ve $G = < a >$ olduğunudan ilgili teoremden *G* nin mertebesi sonlu olur ki bu da *G* nin bir sonsuz devirli grup olmasıyla çelişir. O halde kabulümüz yanlış olup *H* nin mertebesi sonlu değildir.

Teorem 3.3.10. $G = < a >$, *n*. mertebeden bir devirli grup ise *G* nin her alt grubunun mertebesi *n* yi böler ve *n* nin her pozitif *q* böleni için *G* nin mertebesi *q* olan bir ve yalnız bir tane alt grubu vardır. Eğer burada $s \in \mathbb{Z}^+$ olmak üzere $n = sq$ ise bu mertebesi *q* olan alt grup $< a^s >$ olur.

Tanım 3.3.11. *G* bir grup ve $a \in G$ olsun. *a* elemanının ürettiği $< a >$ devirli grubunun mertebesine ***a* elemanının mertebesi** denir ve genellikle $\circ(a)$ ile gösterilir.

Not: İlgili teoremden $\circ(a)$ varsa $a^n = e$ koşulunu sağlayan n pozitif tamsayıların en küçük olanıdır.

Teorem 3.3.12. G bir grup, $a \in G$ ve $\circ(a) = n$ olsun. $m \in \mathbb{Z}$ olmak üzere $a^m = e$ olması için gerek ve yeter koşul $n \mid m$ olmasıdır.

İspat: $(\Rightarrow)$ $a^m = e$ olsun. $\circ(a) = n$ olduğundan n sayısı $a^k = e$ olan k pozitif tamsayıların en küçüğüdür. $n \in \mathbb{Z}^+$ olduğundan m sayısını n ye kalanlı olarak bölebiliriz. Bu durumda $m = qn + r$ ve $0 \le r < n$ olacak şekilde $\exists q, r \in \mathbb{Z}$ vardır. $a^m = a^n = e$ ve $m = qn + r$ olduğundan $e = a^m = a^{qn+r} = \left(a^n\right)^q a^r = e^q a^r = a^r$ olur. Eğer burada $r \neq 0$ olsa $0 < r < n$ olup $a^r = e$ olduğundan bu durum n sayısının $a^k = e$ olan k pozitif tamsayıların en küçüğü olmasıyla çelişir. O halde $r = 0$ olup $m = qn + r = qn$ ve buradan da $n \mid m$ elde edilir.

$(\Leftarrow)$ $n \mid m$ olsun. Bu durumda $m = nc$ olacak şekilde $\exists c \in \mathbb{Z}$ vardır. $\circ(a) = n$ olduğundan $a^n = e$ olur. Bu durumda $m = nc$ olduğundan $a^m = a^{nc} = \left(a^n\right)^c = e^c = e$ olup istenen elde edilir.

Teorem 3.3.13. $G=<a>$, n. mertebeden bir devirli grup olsun. $s\in\mathbb{Z}$ olmak üzere a^s elemanının G nin bir üreteci (yani $G=<a^s>$) olması için gerek ve yeter koşul $(s,n)=1$ olmasıdır.

İspat: $(\Rightarrow)$ $s\in\mathbb{Z}$ olmak üzere $G=<a^s>$ olsun. $a\in G=<a^s>$ olduğundan $a=\left(a^s\right)^x=a^{sx}$ olacak şekilde $\exists x\in\mathbb{Z}$ vardır. $a=a^{sx}$ olduğundan $a^{1-sx}=e$ olup $\circ(a)=\circ(G)=n$ olduğundan ilgili teoremden $n\mid 1-sx$ olur. $n\mid 1-sx$ olduğundan $1-sx=ny$ olacak şekilde $\exists y\in\mathbb{Z}$ vardır. $1-sx=ny$ olduğundan $sx+ny=1$ olup burada $x,y\in\mathbb{Z}$ olduğundan ilgili teoremden $(s,n)=1$ olur.

$(\Leftarrow)$ $(s,n)=1$ olsun. Bu durumda ilgili teoremden $sx+ny=1$ olacak şekilde $\exists x,y\in\mathbb{Z}$ vardır. $\circ(a)=\circ(G)=n$ olduğundan $a^n=e$ olur. O halde $a=a^1=a^{sx+ny}=\left(a^s\right)^x\left(a^n\right)^y=\left(a^s\right)^x e^y=\left(a^s\right)^x\in<a^s>$ olup $<a^s>\prec G$ olduğundan $G=<a>\subset<a^s>$ olur. Ayrıca $<a^s>\subset G$ olduğundan $G=<a^s>$ olup istenen elde edilir.

Teorem 3.3.14. $G=<a>$ bir sonsuz devirli grup ise üreteçleri sadece a ve a^{-1} olur.

İspat: $G=<a>$ bir sonsuz devirli grup olsun. $a=\left(a^{-1}\right)^{-1}\in<a^{-1}>$ ve $<a^{-1}><G$ olduğundan $G=<a>\subset<a^{-1}>$ olup ayrıca $<a^{-1}>\subset G$ olduğundan $G=<a^{-1}>$ olur. Şimdi $s\in\mathbb{Z}$ olmak üzere $G=<a^{s}>$ olsun. $s=1$ veya $s=-1$ olduğunu gösterirsek istenen elde edilir. $a\in G=<a^{s}>$ olduğundan $a=\left(a^{s}\right)^{x}=a^{sx}$ olacak şekilde $\exists x\in\mathbb{Z}$ vardır. Eğer burada $1\neq sx$ olsa $a^{1}=a=a^{sx}$ ve $G=<a>$ olduğundan ilgili teoremden G nin mertebesi sonlu olur ki bu da $G=<a>$nın bir sonsuz devirli grup olmasıyla çelişir. O halde $1=sx$ olup $s\left|1\right.$ olur. $s\left|1\right.$ ve 1 in bölenleri sadece 1 ve -1 olduğundan $s=1$ veya $s=-1$ olup istenen elde edilir.

ÖRNEK: $(\mathbb{Z},+)$ grubunun her alt grubu devirli olduğundan $(\mathbb{Z},+)$ grubunun alt grupları $m\in\mathbb{Z}$ olmak üzere $<m>=m\mathbb{Z}=\left\{mk\,\middle|\,k\in\mathbb{Z}\right\}$ şeklindedir.

ÖRNEK: $G=<a>$, 20. mertebeden bir devirli grup olsun. Bu grubun

(i) alt gruplarını belirtiniz.

(ii) mertebesi 4 olan elemanlarını bulunuz.

(iii) mertebesi 5 olan elemanlarını bulunuz.

Çözüm: (i) $G =< a >$, 20. mertebeden bir devirli grup olduğundan ilgili teoremden G nin her alt grubunun mertebesi 20 sayısını böler ve 20 nin her pozitif q böleni için G nin mertebesi q olan bir ve yalnız bir alt grubu vardır. Burada $s \in \mathbb{Z}^+$ olmak üzere $20 = sq$ ise bu mertebesi q olan alt grup $< a^s >$ olur. 20 nin pozitif bölenleri 1, 2, 4, 5, 10 ve 20 sayılarıdır. Buna göre,

$20 = 20 \cdot 1$ olduğundan G nin mertebesi 1 olan alt grubu $< a^{20} >= \{e\}$ ve mertebesi 20 olan alt grubu $< a^1 >= G$ olur,

$20 = 10 \cdot 2$ olduğundan G nin mertebesi 2 olan alt grubu $< a^{10} >= \{a^{10}, a^{20} = e\}$ ve mertebesi 10 olan alt grubu $< a^2 >= \{a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}, a^{20} = e\}$ olur,

$20 = 5 \cdot 4$ olduğundan G nin mertebesi 4 olan alt grubu $< a^5 >= \{a^5, a^{10}, a^{15}, a^{20} = e\}$ ve mertebesi 5 olan alt grubu $< a^4 >= \{a^4, a^8, a^{12}, a^{16}, a^{20} = e\}$ olur.

Sonuç olarak G nin alt grupları $< a^1 >= G$, $< a^2 >$, $< a^4 >$, $< a^5 >$, $< a^{10} >$ ve $< a^{20} >= \{e\}$ olur.

(ii) $20 = 5 \cdot 4$ olduğundan ilgili teoremden G nin mertebesi 4 olan tek alt grubu $< a^5 >= \{a^5, a^{10}, a^{15}, a^{20} = e\}$ olur. Dolayısıyla G nin mertebesi 4 olan elemanları $< a^5 >= \{a^5, a^{10}, a^{15}, a^{20} = e\}$ grubunun üreteçleri olur. İlgili teoremden $< a^5 >= \{a^5, a^{10}, a^{15}, a^{20} = e\}$ grubunun üreteçleri $s \in \mathbb{Z}$, $1 \le s \le 4$ ve $(s,4) = 1$ olmak üzere $(a^5)^s = a^{5s}$ şeklindedir. Burada $1 \le s \le 4$ ve $(s,4) = 1$ koşuluna uyan s tamsayıları 1 ve 3 olduğundan G nin mertebesi 4 olan elemanları $a^{5 \cdot 1} = a^5$ ve $a^{5 \cdot 3} = a^{15}$ olur.

(iii) $20 = 4 \cdot 5$ olduğundan ilgili teoremden G nin mertebesi 5 olan tek alt grubu $< a^4 >= \{a^4, a^8, a^{12}, a^{16}, a^{20} = e\}$ olur. Dolayısıyla G nin mertebesi 5 olan elemanları $< a^4 >= \{a^4, a^8, a^{12}, a^{16}, a^{20} = e\}$ grubunun üreteçleri olur. İlgili teoremden $< a^4 >= \{a^4, a^8, a^{12}, a^{16}, a^{20} = e\}$ grubunun üreteçleri $s \in \mathbb{Z}$, $1 \le s \le 5$ ve $(s,5) = 1$ olmak üzere $(a^4)^s = a^{4s}$ şeklindedir. Burada $1 \le s \le 5$ ve $(s,5) = 1$ koşuluna uyan s tamsayıları 1, 2, 3 ve 4 olduğundan G nin mertebesi 5 olan elemanları $a^{4 \cdot 1} = a^4$, $a^{4 \cdot 2} = a^8$, $a^{4 \cdot 3} = a^{12}$ ve $a^{4 \cdot 4} = a^{16}$ olur.

Not: $G =< a >$, n. mertebeden bir devirli grup olsun. Bu durumda

(i) G nin alt grupları sayısı n nin pozitif bölenleri sayısıdır.

(ii) G nin üreteçleri sayısı $\varphi(n)$ olur.

(iii) q, n nin bir pozitif böleni olmak üzere G nin mertebesi q olan elemanları sayısı $\varphi(q)$ olur.

Burada φ Euler fonksiyonudur.

3.4. NORMAL ALT GRUPLAR:

Teorem 3.4.1. G bir grup ve $H < G$ olsun. G de $\equiv$ bağıntısı $a,b \in G$ olmak üzere

$$a \equiv b \pmod{H} \Leftrightarrow ab^{-1} \in H$$

olarak tanımlansın. Bu takdirde $\equiv$ bağıntısı G de bir denklik bağıntısıdır.

İspat: Yansıma: $\forall a \in G$ için $aa^{-1} = e \in H$ olduğundan $a \equiv a \pmod{H}$ olup $\equiv$ bağıntısının yansıma özelliği vardır.
Simetri: $a \equiv b \pmod{H}$ olan herhangi $a, b \in G$ alalım. $a \equiv b \pmod{H}$ olduğundan $ab^{-1} \in H$ olup $H < G$ olduğundan $ba^{-1} = \left(b^{-1}\right)^{-1} a^{-1} = \left(ab^{-1}\right)^{-1} \in H$ olur. O halde $b \equiv a \pmod{H}$ olup $\equiv$ bağıntısının simetri özelliği vardır.
Geçişme: $a \equiv b \pmod{H}$ ve $b \equiv c \pmod{H}$ olan herhangi $a, b, c \in G$ alalım. $a \equiv b \pmod{H}$ ve $b \equiv c \pmod{H}$ olduğundan $ab^{-1}, bc^{-1} \in H$ olup $H < G$ olduğundan $ac^{-1} = ab^{-1}bc^{-1} \in H$ olur. O halde $a \equiv c \pmod{H}$ olup $\equiv$ bağıntısının geçişme özelliği vardır.

Böylece $\equiv$ bağıntısı G de bir denklik bağıntısı olup istenen elde edilir.

Teorem 3.4.2. Yukarıdaki $\equiv$ denklik bağıntısına göre bir $a \in G$ elemanının denklik sınıfı G nin $\bar{a} = Ha = \{ha \mid h \in H\}$ alt kümesidir. Ha ya a elemanının H alt grubuna göre **sağ denklik sınıfı** denir.

İspat: Herhangi $x \in \bar{a}$ alalım. $x \in \bar{a}$ olduğundan $x \equiv a \pmod{H}$ olup $xa^{-1} \in H$ olur. Burada $xa^{-1} = h$ dersek $h \in H$ olur. $xa^{-1} = h$ olduğundan $x = ha$ olup $h \in H$ olduğundan $x = ha \in Ha$ olur. O halde

$$\bar{a} \subset Ha \ \ldots (1)$$

olur. Herhangi $x \in Ha$ alalım. $x \in Ha$ olduğundan $x = ha$ olacak şekilde $\exists h \in H$ vardır. $x = ha$ olduğundan $xa^{-1} = h \in H$ olup $x \equiv a \pmod{H}$ olur. O halde $x \in \bar{a}$ olup

$$Ha \subset \bar{a} \ \ldots (2)$$

olur. (1) ve (2) den $\bar{a} = Ha = \{ha \mid h \in H\}$ olup istenen elde edilir.

Teorem 3.4.3. G bir grup ve $H < G$ olsun. G de $\equiv_L$ bağıntısı $a, b \in G$ olmak üzere

$$a \equiv_L b \pmod{H} \Leftrightarrow a^{-1}b \in H$$

ile tanımlansın. Bu takdirde $\equiv_L$ bağıntısı G de bir denklik bağıntısıdır ve bu bağıntıya göre bir $a \in G$ elemanının denklik sınıfı G nin $\bar{a} = aH = \{ah \mid h \in H\}$ alt kümesidir. aH ye a elemanının H alt grubuna göre **sol denklik sınıfı** denir.

İspat: ÖDEV.

Teorem 3.4.5. *G* bir grup, $H < G$ ve *H* sonlu elemanlı olsun. Bu durumda *H* alt grubuna göre bütün sağ ve sol denklik sınıflarında sonlu sayıda eleman olup aynı sayıda eleman bulunur.
İspat: Herhangi $a \in G$ alalım.

$$f : H \to Ha, x \to f(x) = xa$$

dönüşümünü tanımlayalım. f nin bir fonksiyon olduğu açıktır. $f(x_1) = f(x_2)$ olan herhangi $x_1, x_2 \in H$ alalım. $f(x_1) = f(x_2)$ olduğundan $x_1 a = x_2 a$ olup kısaltma özelliğinden $x_1 = x_2$ olur. O halde f birebir olur. Herhangi $y \in Ha$ alalım. $y \in Ha$ olduğundan $y = xa$ olacak şekilde $\exists x \in H$ vardır. Burada f nin tanımından $f(x) = xa = y$ olup f örtendir. $f : H \to Ha$ birebir ve örten bir fonksiyon ve *H* sonlu elemanlı olduğundan Ha da sonlu elemanlı ve $s(Ha) = s(H) = \circ(H)$ olur. Benzer şekilde

$$g : H \to aH, x \to g(x) = ax$$

dönüşümünü tanımlayarak aH kümesinin de sonlu elemanlı ve $s(aH) = s(H) = \circ(H)$ olduğu gösterilebilir (ÖDEV). Yani *H* alt grubuna göre bütün sağ ve sol denklik sınıflarında sonlu sayıda eleman olup aynı sayıda eleman bulunur.

Not: $H < G$ ise $He = eH = H$ olduğundan *H, e* elemanının *H* ye göre hem sağ, hem de sol denklik sınıfıdır.

LAGRANGE TEOREMİ: Sonlu bir grubun her alt grubunun mertebesi grubun mertebesini böler.

İspat: *G* bir sonlu grup ve $H < G$ olsun. $\circ(G) = n$ ve $\circ(H) = k$ diyelim. $k \mid n$ olduğunu gösterirsek istenen elde edilir. *G* bir sonlu grup olduğundan *G* de *H* ye göre sağ denklik sınıflarının sayısı da sonludur. Kabul edelim ki *G* de *H* ye göre birbirinden farklı sağ denklik sınıflarının ailesi $a_1, a_2, ..., a_t \in G \ \left(t \in \mathbb{Z}^+\right)$ olmak üzere $\{Ha_1, Ha_2, ..., Ha_t\}$ olsun. Soyut Matematik dersindeki ilgili teoremden $\{Ha_1, Ha_2, ..., Ha_t\}$ ailesi *G* nin bir ayrışımı olup yine Soyut Matematik dersindeki ilgili teoremden $n = s(G) = s(Ha_1) + s(Ha_2) + ... + s(Ha_t)$ olur. Öte yandan bir önceki teoremden $1 \le i \le t$ için $s(Ha_i) = \circ(H) = k$ olur. O halde $n = s(Ha_1) + s(Ha_2) + ... + s(Ha_t) = \underbrace{k + k + ... + k}_{t \text{ tane}} = kt$ olup $k \mid n$ olur ki bu da istenendir.

Sonuç 3.4.6. G bir sonlu grup ve $H < G$ ise G de H alt grubuna göre sağ ve sol denklik sınıflarının sayısı aynıdır. Bu sayıya H alt grubunun G içindeki **indeksi** denir ve genellikle $(G:H)$ ile gösterilir. Ayrıca $(G:H) = \dfrac{\circ(G)}{\circ(H)}$ olur.

İspat: ÖDEV.

Sonuç 3.4.7. G bir sonlu grup ve $\circ(G) = n$ ise $\forall a \in G$ için $\circ(a) \mid n$ olup $a^n = e$ olur.

İspat: ÖDEV.

Teorem 3.4.8. $N < G$ olsun. Aşağıdaki ifadeler birbirine denktir.

(i) $\forall a \in G$ ve $\forall x \in N$ için $axa^{-1} \in N$ dir.

(ii) $\forall a \in G$ için $aNa^{-1} \subset N$ dir.

(iii) $\forall a \in G$ için $aNa^{-1} = N$ dir.

(iv) $\forall a \in G$ için $aN = Na$ dır.

İspat: $(i) \Rightarrow (ii)$ $\forall a \in G$ ve $\forall x \in N$ için $axa^{-1} \in N$ olsun. Bu durumda $\forall a \in G$ için $aNa^{-1} = \{axa^{-1} \mid x \in N\} \subset N$ olup istenen elde edilir.

$(ii) \Rightarrow (iii)$ $\forall a \in G$ için $aNa^{-1} \subset N$ olsun. Herhangi $a \in G$ alalım. Hipotezden $aNa^{-1} \subset N$ olur. $a^{-1} \in G$ olduğundan hipotezden $a^{-1}Na = a^{-1}N\left(a^{-1}\right)^{-1} \subset N$ olur. Herhangi $x \in N$ alalım. $y = a^{-1}xa$ diyelim. Burada $y = a^{-1}xa \in a^{-1}Na$ olup $a^{-1}Na \subset N$ olduğundan $y \in N$ olur. Bu durumda $x = aa^{-1}xaa^{-1} = aya^{-1} \in aNa^{-1}$ olup $N \subset aNa^{-1}$ olur. Ayrıca $aNa^{-1} \subset N$ olduğundan $aNa^{-1} = N$ olur. Yani $\forall a \in G$ için $aNa^{-1} = N$ olup istenen elde edilir.

$(iii) \Rightarrow (iv)$ $\forall a \in G$ için $aNa^{-1} = N$ olsun. Herhangi $a \in G$ alalım. $aN = Na$ olduğunu gösterirsek istenen elde edilir. Hipotezden $aNa^{-1} = N$ olur. Herhangi $x \in aN$ alalım. $x \in aN$ olduğundan $x = an$ olacak şekilde $\exists n \in N$ vardır. $x = an$ olduğundan $xa^{-1} = ana^{-1} \in aNa^{-1} = N$ olup $m = xa^{-1}$ dersek $m \in N$ olur. O halde $x = xa^{-1}a = ma \in Na$ olup

$$aN \subset Na \ \ldots (1)$$

olur. Herhangi $x \in Na$ alalım. $x \in Na$ olduğundan $x = na$ olacak şekilde $\exists n \in N$ vardır. $x = na$ olduğundan $xa^{-1} = n \in N = aNa^{-1}$ olup $xa^{-1} = ama^{-1}$ olacak şekilde $\exists m \in N$ vardır. $xa^{-1} = ama^{-1}$ olduğundan kısaltma özelliğinden $x = am \in aN$ olup

$$Na \subset aN \ \ldots (2)$$

olur. (1) ve (2) den $aN = Na$ olup istenen elde edilir.

$(iv) \Rightarrow (i)$ $\forall a \in G$ için $aN = Na$ olsun. Herhangi $a \in G$ ve herhangi $x \in N$ alalım. Hipotezden $aN = Na$ olur. $a \in G$ ve $x \in N$ olduğundan $ax \in aN = Na$ olup $ax = na$ olacak şekilde $\exists n \in N$ vardır. $ax = na$ olduğundan $axa^{-1} = n \in N$ olur. Yani $\forall a \in G$ ve $\forall x \in N$ için $axa^{-1} \in N$ olup istenen elde edilir.

Tanım 3.4.9. Teoremin denk koşullarından birini sağlayan G nin bir N alt grubuna **bir normal alt grup** denir ve $\boldsymbol{N \lhd G}$ ile ifade edilir.

Not: G bir grup ise $G \lhd G$ ve $\{e\} \lhd G$ olur. (Nedeni ÖDEV)

Not: G bir değişmeli grup ise G nin her alt grubu normaldir. (Nedeni ÖDEV)

Not: $N \lhd G$ ise N ye göre tanımlanan sağ ve sol denklik sınıfları aynıdır.

Teorem 3.4.10. G bir grup olsun. G nin birtakım normal alt gruplarının kesişimi de bir normal alt gruptur.

İspat: $\{N_i\}_{i\in I}$, G nin normal alt gruplarının bir ailesi olsun. $\bigcap_{i\in I} N_i \lhd G$ olduğunu gösterirsek istenen elde edilir. $\forall i \in I$ için $N_i \lhd G$ olduğundan $N_i < G$ olup ilgili teoremden $\bigcap_{i\in I} N_i < G$ olur. Herhangi $a \in G$ ve herhangi $x \in \bigcap_{i\in I} N_i$ alalım. $x \in \bigcap_{i\in I} N_i$ olduğundan $\forall i \in I$ için $x \in N_i$ olup $N_i \lhd G$ olduğundan tanımdan $axa^{-1} \in N_i$ olur. $\forall i \in I$ için $axa^{-1} \in N_i$ olduğundan $axa^{-1} \in \bigcap_{i\in I} N_i$ olur. Yani $\forall a \in G$ ve $\forall x \in \bigcap_{i\in I} N_i$ için $axa^{-1} \in \bigcap_{i\in I} N_i$ olup tanımdan $\bigcap_{i\in I} N_i \lhd G$ olur.

Not: $N \lhd G$ olsun. G de N ye göre sol (veya sağ) denklik sınıflarının kümesi G/N ile gösterilir. Yani $G/N = \{aN \,|\, a \in G\} = \{Na \,|\, a \in G\}$ olarak tanımlanır.

Teorem 3.4.11. $N \lhd G$ ise $a,b \in G$ olmak üzere $\forall aN, bN \in G/N$ için

$$(aN)(bN) = (ab)N$$

olur.

İspat: $N \lhd G$ olsun. $a,b \in G$ olmak üzere herhangi $aN, bN \in G/N$ alalım. $(aN)(bN) = (ab)N$ olduğunu gösterirsek istenen elde edilir. Herhangi $x \in (aN)(bN)$ alalım. $x \in (aN)(bN)$ olduğundan $x = x_1 x_2$ olacak şekilde $\exists x_1 \in aN$ ve $\exists x_2 \in bN$ vardır. $x_1 \in aN$ ve $x_2 \in bN$ olduğundan $x_1 = an_1$ ve $x_2 = bn_2$ olacak şekilde $\exists n_1, n_2 \in N$ vardır. Burada $x = x_1 x_2 = an_1 bn_2$ olur. $n_1 \in N$ olduğundan $n_1 b \in Nb$ olur. $N \lhd G$ olduğundan $Nb = bN$ olup $n_1 b \in Nb = bN$ olur. O halde $n_1 b = bn_3$ olacak şekilde $\exists n_3 \in N$ vardır. Bu durumda $x = an_1 bn_2 = abn_3 n_2$ olur. Burada $n_3, n_2 \in N$ ve $N < G$ olduğundan $n_3 n_2 \in N$ olup $x = abn_3 n_2 \in (ab)N$ olur. Yani $\forall x \in (aN)(bN)$ için $x \in (ab)N$ olup

$$(aN)(bN) \subset (ab)N \quad \ldots (1)$$

olur. Herhangi $x \in (ab)N$ alalım. $x \in (ab)N$ olduğundan $x = abn$ olacak şekilde $\exists n \in N$ vardır. Burada $x = abn = aebn$ olur. $e, n \in N$ olduğundan $ae \in aN$ ve $bn \in bN$ olur. O halde $x = aebn \in (aN)(bN)$ olup

$$(ab)N \subset (aN)(bN) \quad \ldots (2)$$

olur. (1) ve (2) den $(aN)(bN) = (ab)N$ olup istenen elde edilir.

Teorem 3.4.12. $N \lhd G$ ise G/N, $a,b \in G$ olmak üzere $\forall aN, bN \in G/N$ için

$$(aN)*(bN) = (aN)(bN)$$

ile tanımlı $*$ işlemine göre bir gruptur.

İspat: $N \lhd G$ olsun. $G \neq \emptyset$ olduğundan $G/N \neq \emptyset$ olur. Bir önceki teoremden $a,b \in G$ olmak üzere $\forall aN, bN \in G/N$ için $(aN)*(bN) = (aN)(bN) = (ab)N \in G/N$ olup $*$ işlemi G/N de bir iç işlem olur.

$*$ işleminin tanımı ve bir önceki teoremden $a,b,c \in G$ olmak üzere $\forall aN, bN, cN \in G/N$ için

$$(aN)*\left[(bN)*(cN)\right] = (aN)*\left[(bc)N\right] = \left(a(bc)\right)N = \left((ab)c\right)N = \left[(ab)N\right]*(cN) = \left[(aN)*(bN)\right]*(cN)$$

olup $*$ işleminin G/N de birleşme özelliği vardır.

G/N nin $eN = N$ elemanını alalım. $*$ işleminin tanımı ve bir önceki teoremden $a \in G$ olmak üzere $\forall aN \in G/N$ için $(aN)*(eN) = (ae)N = aN$ ve $(eN)*(aN) = (ea)N = aN$ olup $eN = N$ elemanı G/N nin $*$ işlemine göre birim elemanı olur.

$a \in G$ olmak üzere herhangi $aN \in G/N$ alalım. G/N nin $a^{-1}N$ elemanını alırsak $*$ işleminin tanımı ve bir önceki teoremden $(aN)*(a^{-1}N) = (aa^{-1})N = eN = N$ ve $(a^{-1}N)*(aN) = (a^{-1}a)N = eN = N$ olup $a^{-1}N$ elemanı aN elemanının G/N de $*$ işlemine göre tersi olur. Yani G/N deki her elemanın G/N de $*$ işlemine göre tersi vardır.

Böylece G/N kümesi $*$ işlemine göre bir grup olup istenen elde edilir.

Not: Teoremdeki $*$ sembolü yerine de genellikle $\cdot$ sembolü kullanılacaktır. Ayrıca $(aN)(bN)$ ve $(ab)N$ gibi ifadelerde parantezler konulmayacaktır.

Tanım 3.4.13. $N \lhd G$ ise G/N grubuna, G nin N ye göre **bölüm grubu** denir.

Teorem: G bir sonlu grup ve $N \lhd G$ olsun. Bu durumda G/N de bir sonlu gruptur ve $\circ(G/N) = \circ(G)/\circ(N)$ olur.

İspat: $G/N = \{aN \mid a \in G\}$ ve G sonlu elemanlı olduğundan G/N de sonlu elemanlı olur. Ayrıca G/N nin tanımı ve ilgili teoremden $\circ(G/N) = (G:N) = \circ(G)/\circ(N)$ olup istenen elde edilir.

Not: G bir toplamsal grup ise değişmeli olacağından her alt grubu normal olur. Şu halde G nin her alt grubuna göre bölüm grubu tanımlanabilir. Burada bölüm grubundaki işlem de genellikle + ile ifade edilir. $N < G$ ve $a \in G$ ise a nın denklik sınıfı $\overline{a} = a + N = \{a + x \,|\, x \in N\}$ olur.

Teorem 3.4.14. Bir grubun indeksi 2 olan her alt grubu normaldir.
İspat: G bir grup ve N, G nin G içindeki indeksi 2 olan bir alt grubu olsun. $N \lhd G$ olduğunu gösterirsek istenen elde edilir. $x \in G$ olmak üzere

$$x \in N \Leftrightarrow e^{-1}x \in N \Leftrightarrow e \equiv_L x \pmod{N} \Leftrightarrow N = eN = xN$$

ve

$$x \in N \Leftrightarrow xe^{-1} \in N \Leftrightarrow x \equiv e \pmod{N} \Leftrightarrow Nx = Ne = N$$

denklikleri vardır. Herhangi $a \in G$ alalım. Eğer $a \in N$ ise yukarıdaki denkliklerden $aN = N$ ve $Na = N$ olup $aN = Na$ olur. Kabul edelim ki $a \notin N$ olsun. Bu durumda yine yukarıdaki denkliklerden $aN \neq N$ ve $Na \neq N$ olur. $aN \neq N$ ve $(G:N) = 2$ olduğundan G de N ye göre sol denklik sınıflarının ailesi $\{aN, N\}$ olup bu aile G nin bir ayrışımı olduğundan $G = aN \cup N$ ve $aN \cap N = \varnothing$ olur. Bu durumda $aN = G - N$ olur. $Na \neq N$ ve $(G:N) = 2$

olduğundan G de N ye göre sağ denklik sınıflarının ailesi $\{Na, N\}$ olup bu aile G nin bir ayrışımı olduğundan $G = Na \cup N$ ve $Na \cap N = \varnothing$ olur. Bu durumda da $Na = G - N$ olur. $aN = G - N$ ve $Na = G - N$ olduğundan $aN = Na$ olur. Yani $\forall a \in G$ için $aN = Na$ olup tanımdan $N \lhd G$ olur.

Teorem 3.4.15. $N \lhd G$ olsun. $N < K < G$ ise $N \lhd K$ ve $K/N < G/N$ olur. Eğer ayrıca $N < K \lhd G$ ise $K/N \lhd G/N$ olur. Tersine, G/N nin alt grupları $N < T < G$ olmak üzere T/N şeklinde ve normal alt grupları da $N < T \lhd G$ olmak üzere T/N şeklindedir.

İspat: $N < K < G$ olsun. Herhangi $a \in K$ ve herhangi $x \in N$ alalım. $a \in K$ ve $K < G$ olduğundan $a \in G$ olup ayrıca $x \in N$ ve $N \lhd G$ olduğundan $axa^{-1} \in N$ olur. Yani $\forall a \in K$ ve $\forall x \in N$ için $axa^{-1} \in N$ olup ayrıca $N < K$ olduğundan tanımdan $N \lhd K$ olur. $N \lhd K$ olduğundan K/N bölüm grubu tanımlıdır. Ayrıca $K/N \subset G/N$ ve K/N bölüm grubundaki işlem G/N grubundaki işlem olduğundan $K/N < G/N$ olur. Şimdi kabul edelim ki $N < K \lhd G$ olsun. Herhangi $aN \in G/N \ (a \in G)$ ve herhangi $xN \in K/N \ (x \in K)$ alalım. $a \in G$, $x \in K$ ve $K \lhd G$ olduğundan tanımdan $axa^{-1} \in K$ olup $aNxN(aN)^{-1} = axNa^{-1}N = axa^{-1}N \in K/N$ olur. Yani $\forall aN \in G/N \ (a \in G)$ ve

$\forall xN \in K/N \ (x \in K)$ için $aNxN(aN)^{-1} \in K/N$ olup ayrıca $K/N < G/N$ olduğundan tanımdan $K/N \lhd G/N$ olur.

Tersine, G/N nin herhangi $\overline{T}$ alt grubunu alalım. $T = \left\{ c \in G \middle| cN \in \overline{T} \right\}$ kümesini tanımlayalım. $\forall x \in N$ için $e^{-1}x = x \in N$ olduğundan $e \equiv_L x \pmod N$ olup $xN = eN = N = e_{G/N} \in \overline{T}$ ve buradan da $x \in T$ elde edilir. O halde $N \subset T$ olur. Burada $N \neq \varnothing$ olduğundan $T \neq \varnothing$ olur. Ayrıca $T \subset G$ olduğu da açıktır. Yani $\varnothing \neq T \subset G$ olur. Herhangi $a,b \in T$ alalım. $a,b \in T$ olduğundan $aN, bN \in \overline{T}$ olup $\overline{T} < G/N$ olduğundan $ab^{-1}N = aNb^{-1}N = aN(bN)^{-1} \in \overline{T}$ olur. O halde T nin tanımından $ab^{-1} \in T$ olup ilgili teoremden $T < G$ olur. Ayrıca $N \subset T$ olduğundan $N < T < G$ olur. $N \lhd G$ ve $N < T < G$ olduğundan $N \lhd T$ ve $T/N < G/N$ olur. Herhangi $\overline{x} \in T/N$ alalım. $\overline{x} \in T/N$ olduğundan $\overline{x} = xN$ olacak şekilde $\exists x \in T$ vardır. $x \in T$ ve $T = \left\{ c \in G \middle| cN \in \overline{T} \right\}$ olduğundan $\overline{x} = xN \in \overline{T}$ olur. Yani $\forall \overline{x} \in T/N$ için $\overline{x} \in \overline{T}$ olup

$$T/N \subset \overline{T} \ \ldots (1)$$

olur. Herhangi $\bar{x} \in \bar{T}$ alalım. $\bar{x} \in \bar{T}$ ve $\bar{T} < G/N$ olduğundan $\bar{x} \in G/N$ olup $\bar{x} = xN$ olacak şekilde $\exists x \in G$ vardır. $xN = \bar{x} \in \bar{T}$ olduğundan T nin tanımından $x \in T$ olup $\bar{x} = xN \in T/N$ olur. Yani $\forall \bar{x} \in \bar{T}$ için $\bar{x} \in T/N$ olup

$$\bar{T} \subset T/N \ \ldots (2)$$

olur. (1) ve (2) den $\bar{T} = T/N$ elde edilir. Son olarak, kabul edelim ki $\bar{T} \lhd G/N$ olsun. $T \lhd G$ olduğunu gösterirsek istenen elde edilir. Herhangi $a \in G$ ve herhangi $x \in T$ alalım. $a \in G$ ve $x \in T$ olduğundan $aN \in G/N$ ve $xN \in T/N = \bar{T}$ olup $\bar{T} \lhd G/N$ olduğundan $axa^{-1}N = aNxNa^{-1}N = aNxN\left(aN\right)^{-1} \in \bar{T}$ olur. $axa^{-1}N \in \bar{T}$ olduğundan T nin tanımından $axa^{-1} \in T$ olur. Yani $\forall a \in G$ ve $\forall x \in T$ için $axa^{-1} \in T$ olup ayrıca $T < G$ olduğundan tanımdan $T \lhd G$ olur.

Teorem 3.4.16. G bir grup, $N \lhd G$, $N < K < G$ ve $N < T < G$ olsun. Bu durumda $K/N = T/N$ olması için gerek ve yeter koşul $K = T$ olmasıdır.

Tanım 3.4.17. Bir G grubunun $\{e\}$ ve G den başka hiçbir normal alt grubu yoksa G ye **bir basit grup** denir.

ÖRNEK: Mertebesi asal olan grup basittir.

Tanım 3.4.18. G bir grup, $M \lhd G$ ve $M \neq G$ olsun. G nin M yi kapsayan M ve G den başka hiçbir normal alt grubu yoksa M ye G nin **bir maksimal normal** alt grubu denir.

Teorem 3.4.19. G bir grup, $M \lhd G$ ve $M \neq G$ olsun. Bu takdirde M nin maksimal olması için gerek ve yeter koşul G/M nin basit olmasıdır.