1. GİRİŞ

Sonlu gruplarda, en temel problem grupların altgruplarını bulmaktır. Aynı mertebeye sahip farklı gruplar vardır. Lagrange Teoremi; sonlu gruplarda alt grubun mertebesinin grubun mertebesini böldüğünü söyler ancak bir grubun alt grupları hakkında fazla bir şey söylemez. Örneğin mertebesi 12 olan ikisi değişmeli, üçü değişmeli olmayan 5 farklı grup vardır. Grupları sınıflandırırken, grupların hangi tür altgruplarının olduğunu bilmek önemlidir. Burada Sylow teoremleri önemli rol oynarlar. Örneğin, Alterne grup A_4 ün mertebesi 6 olan bir altgrubu yoktur.

İlk bölümde bazı temel kavramlar ve önemli teoremler verilmiştir. Sylow teoremleri ayrıntılı olarak ispat edilmiştir. Sylow teoremlerinden yararlanılarak mertebesi 30 dan küçük olan grupların sınıflandırılması yapılmıştır. Daha sonra yeni gruplar oluşturmak için bazı teknikler verilmiştir. Bunlar gruplarda yarı direk çarpım ve wreath çarpımlardır.

Sonlu gruplarda genel lineer gruplar önemli bir yer tutmaktadırlar. Her grup bir permütasyon grubunun altgrubuna izomorf olduğunu Cayley teoreminden biliyoruz. Her satır ve sütununda yalnız 1 olan kare matrislere permütasyon matris denir. n x n boyutlu permütasyon matrislerin oluşturduğu grup Sym(n) ye izomorftur. Dolayısıyla bütün sonlu grupları genel lineer grupların içine gömelebiliriz. Genel lineer grupların p-sylow altgruplarının yapısını bulmak için aşağıdaki aşamaları izleyeceğiz. P sayısı a doğal sayısını bölmeyen bir asal sayı olmak üzere; *val (N) yi* $N = p^{val(N)} \cdot a$ olacak şekilde tanımlayalım.

$\mathbb{F}_q$ mertebesi *q* olan bir cisim ve $\mathbb{F}_q$ üzerinde tanımlı boyutu *n* ***x*** *n* olan tersinir kare matrislerin kümesini $GL_n(\mathbb{F}_q)$ ile gösteririz. Buradan yola çıkarak, $\ell = \left\lfloor \frac{n}{k} \right\rfloor$ ve $r \in \mathbb{N}$ olmak üzere $val(|GL_n(\mathbb{F}_q)|) = \ell r + val(\ell !)$ olduğunu gösterdik.

$\mathbb{F}^*_{q^k}$ dan $GL_n(\mathbb{F}_q)$ ya bir homomorfizma kurulabileceğinden $\mathbb{F}^*_{q^k}$ ın bir kopyasını $GL_n(\mathbb{F}_q)$ içerisine gömebiliriz.

$GL_n(\mathbb{F}_q)$ içerisindeki $GL_n(\mathbb{F}_q)$ nın kopyasını her x$\in \mathbb{F}_{q^k}^*$ için M_x matrislerinin kümesiyle gösterelim. Ayrıca her x_i Î $Sylow_p$ $(\mathbb{F}_{q^k}^*)$ için köşegenleri M_{x_i} ve 1 olan matrislerin kümesini de *P* ile gösterelim. Buradaki *P* kümesi $GL_n(\mathbb{F}_q)$ nun bir *p*-altgrubudur. Ayrıca 5. bölümde simetrik grupların *p*-sylow altgruplarının nasıl bulunabileceği hakkında bilgi vermiştir.

Sonuç olarak $GL_n(\mathbb{F}_q)$ nun *p*-sylow altgruplarından biri P grubu ile Sym (ℓ) nin *p*-sylow altgrubunun yarı direk çarpımına izomorftur.

2. TEMEL TANIMLAR VE BAZI TEOREMLER

Bu bölümde, bu çalışmada sıkça kullanılan bazı temel tanım ve teoremler verilecektir.

Tanım 2.1 (G, o) ve (H, $*$) grup olsun. $\forall$ a, b $\in$ G için;

$$\varphi(a \circ b) = \varphi(a) * \varphi(b)$$

koºulunu saðlayan φ: G $\to$H dönüþümüne grup homomorfizması denir.

Eğer φ bire-bir grup homomorfizması ise grup monomorfizması, örten grup homomorfizması ise grup epimorfizması, bire-bir ve örten grup homomorfizması ise grup izomorfizması adını alır.

Tanım 2.2 (*G, o) ve (H,* $*$*)* iki grup ve $\varphi : G \to H$ bir grup homomorfizması olsun.

$$\ker\varphi = \{a \in G \mid \varphi(a) = e_H\}$$

ile tanımlanan kümeye φ homomorfizmasının çekirdeği denir.

Teorem 2.3 (Lagrange Teoremi) G bir grup ve H < G olsun. O zaman

$|G| = |G : H|\,|H|$ dır. Özet olarak; eğer G grubu sonlu ise a $\in$ G elemanının mertebesi grubun mertebesini böler.

Teorem 2.4 Mertebesi asal sayı olan her grup devirlidir.

İspat. $|G| = p$ olsun. H, G grubunun $H \neq \langle e \rangle$ ifadesini sağlayan bir altgrubu olsun. $|H| \neq 1$ dir. Diğer taraftan Lagrange Teoreminden $|H| \mid |G| = p$ olur. p asal ve $|H| \neq 1$ olduğundan $|H| = p$ dir. Böylece $H = G$ bulunur. G grubunun birimden farklı bir a elemanı için $< a > < G$ ve $|< a >| = p$ olduğundan $< a >= G$ bulunur. Bu ise G grubunun devirli olduğunu gösterir.

Teorem 2.5 G bir grup olsun. H ve K, G grubunun sonlu altgrupları olsun. Bu takdirde $|HK| = \dfrac{|H|.|K|}{|H \cap K|}$ dir.

Teorem 2.6 *N, G* grubunun altgrubu olsun. O zaman aşağıdakiler denktir.

(N1) Modulo *N* ye göre sağ denk ve sol denk olma aynı denklik bağıntısını tanımlar.

(N2) N alt grubunun her sol denklik sınıfı, *N* alt grubunun bir sağ denklik sınıfıdır.

(N3) $\forall a \in G$ için, $aN=Na$

(N4) $\forall a \in G$ için, $aNa^{-1} = \{ana^{-1} \mid n \in N\}$ olmak üzere $ana^{-1} \subset N$ dir.

(N5) $\forall a \in G$ için, $aNa^{-1} = N$ dir.

Tanım 2.7 Yukarıdaki denk olma koşullarından herhangi birini sağlayan *N* alt grubuna, *G* grubunun normal alt grubu denir ve $N \lhd G$ ile gösterilir.

Teorem 2.8 (I. İzomorfizma Teoremi) Eğer $\varphi: G \rightarrow H$ bir grup homomorfizması ise o zaman $G/(\ker\varphi) \cong \varphi(G)$ dir.

Teorem 2.9 (II. Ýzomorfizma Teoremi) G bir grup olsun. Eðer $K< G$ ve $N \lhd G$ ise o zaman $K/(N \cap K) \cong NK/N$ dir.

Teorem 2.10 (III.Ýzomorfizma Teoremi) G bir grup, $K \lhd G, N \lhd G$ ve $K \lhd N$ olsun. O zaman $(G/K)/(N/K) \cong G/N$ dir.

Tanım 2.11 $H<G$ olsun. Eğer $H \neq \{e_G\}$ ise o zaman H altgrubuna G grubunun özaltgrubu denir.

Tanım 2.12 Bir G grubun hiç bir öz normal alt grubu yoksa G grubuna basit grup denir.

Tanım 2.13 $C_G(x) = \{g \in G \mid gx = xg\}$ kümesine *x* elemanının *G* içindeki merkezleyeni denir.

Tanım 2.14 $Cl(x)=\{gxg^{-1} \mid \forall g \in G\}$ kümesine x elemanının eşlenik sınıfı denir.

Tanım 2.15 $C_G(H)=\{g \in G \mid gh = hg \ \forall h \in H\}$ kümesine H nin G deki merkezleyeni denir.

Tanım 2.16 $Z_G(x)=\{g \in G \mid gx = xg \ \forall x \in G\}$ kümesine G` nin merkezi denir.

Tanım 2.17 $N_G(H)=\{g \in G \mid gHg^{-1} = H\}$ kümesine H nin G deki normalleyeni denir.

2.1 Genel Lineer Gruplar

$\mathbb{F}$ herhangi bir cisim olmak üzere ve $n \in \mathbb{N}$ için;

$$GL(n,\mathbb{F})=\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = A \mid aij \in \mathbb{F}, \ \det A \neq 0\}$$

kümesine genel lineer gruplar kümesi denir. Basitçe görülebileceği gibi GL(n,$\mathbb{F}$)

değişmeli olmayan bir gruptur.

Önerme 2.18 Sonlu bir cismin eleman sayısı, p bir asal sayı olmak üzere p nin bir kuvvetidir.

İspat. $\mathbb{F}$ sonlu bir cisim olsun. O halde bu cismin karakteristiği bir p asal sayıdır.

Buradan $\mathbb{F}$ cismi $\mathbb{Z}_p$ ye izomorf bir alt cisim kapsar. Yani $\mathbb{F}$ cismini $\mathbb{Z}_p$ cisminin bir genişlemesi olarak görebiliriz. $\mathbb{F}$ sonlu bir cisim olduğundan

$[\mathbb{F}:\mathbb{Z}_p]=n$ kümesinde sonludur. Eğer $\mathbb{F}$ cisminin $\mathbb{Z}_p$ üzerindeki bir tabanı, $\{\alpha_1,\alpha_2,\dots,\alpha_n\}$ ise $\forall\alpha \in \mathbb{F}$ ve $a_i \in \mathbb{Z}_p$ için $\alpha=a_1\alpha_1+a_2\alpha_2+\dots+a_n\alpha_n$ şeklinde yazılabilir. Buradaki a_i ler için p seçenek mevcuttur. O halde elde edilebilecek α ların sayısı, yani $\mathbb{F}$ nin eleman sayısı da p^n olur.

Önerme 2.19 $n \in \mathbb{N}$ ve $\mathbb{F}$ cisminin karakteristiği q olmak üzere;

$$\left|GL_n(\mathbb{F}_q)\right| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1) \text{ dir.}$$

İspat. İlk satırının seçimini $q^n - 1$ farklı şekilde seçebiliriz. Eğer satırın tüm elemanlarını sıfır seçersek determinant sıfır olur. İkinci satırın elemanlarını seçerken dikkat etmemiz gereken determinantın sıfır olmaması durumudur. Bu mantıkla ikinci satır birinci satırın bir katı olmamalıdır. Bu seçim ise $q^n - q$ kadardır. Bu şekilde devam edersek;

$$\left|GL_n(\mathbb{F}_q)\right| = (q^n - 1)(q^n - q)\ldots(q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1) \text{ dir.}$$

2.2. Gruplarda Etki

Tanım 2.20 G sonlu bir grup X' de bir küme olmak üzere;

$$\varphi : G \times X \to X$$
$$(g, x) \mapsto gx$$

$\forall x \in X$ ve $\forall g_1, g_2 \in G$ için $(g_1 g_2)x = g_1(g_2 x)$ ve $ex = x$
ºartlarýsaðlanýrsa G grubu X kümesi üzerine etki eder denir.

Örnek 2.21 $(\mathbb{Z}, +)$ grubunun $\mathbb{R}$ kümesi üzerine etkisini araştıralım.

$$\varphi : \mathbb{Z} \times \mathbb{R} \to \mathbb{R}$$
$$(n, x) \mapsto x + n$$

$n_1, n_2 \in \mathbb{Z}$ ve $x \in \mathbb{R}$ için

$n_1(n_2x) = n_1(x+n_2) = x+n_2+n_1 = (n_1+n_2)x = (n_1n_2)x$

$0x = x+0 = x$

şartları sağlandığından $(\mathbb{Z}, +)$ grubu $\mathbb{R}$ kümesi üzerine etki eder. Burada öteleme bir etkidir.

Lemma 2.22 G grubunun X kümesi üzerine etki etmesi için gerek ve yeterli şart $\varphi : G \to \text{Sym}(X)$ (Sym(X) tüm permütasyon gruplarının kümesi) ile tanımlanan φ nin homomorfizma olmasıdır.

Ýspat.$\Rightarrow$:G grubu X kümesine üzerine etki etsin.

$$\begin{aligned} \varphi &: G \to \text{Sym}(X) \\ g &\mapsto \varphi_g \\ \varphi_g &: X \to X \\ x &\mapsto gx \end{aligned}$$

$\varphi_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) = \varphi_{g_1}\varphi_{g_2}(x)$

olduðundan dönüþüm bir homomorfizmadýr.

$\Leftarrow$: φ:G $\to$ Sym(x) dönüþüm bir homomorfizma olsun.

$\varphi_{g_1 g_2}(x)=\varphi_{g_1}\varphi_{g_2}(x)$ yani $(g_1 g_2)x = g_1(g_2 x)$

$\varphi : G \to \text{Sym}(x)$ dönüþümü bir homomorfizma olduðunda n birimi birime götürür.

Yani $\varphi_e(x) = 1(x)$'dir.

$\varphi_e(x) = ex = 1(x) = x$ olduðundan G grubu Sym(x) kümesi üzerine etki eder.

Örnek 2.23 S_n permütasyon grubu $\Omega=\{1, 2, ... ,n\}$ kümesi üzerine etki eder.

$$\varphi : S_n \times \Omega \to \Omega$$
$$(\sigma, x) \mapsto \sigma(x)$$
$$\sigma, \tau \in S_n \; ve \; x \in \Omega$$
$$(\sigma\tau)(x) = \sigma(\tau(x)),\; I(x) = x$$

Örnek 2.24 G bir grup H<G ve S kümesi H nin G içindeki sol yan kümeleri olsun.

$S = \{xH \mid x \in G\}$. G grubunun S kümesine etkisini gösterelim.

İspat.

$$\begin{aligned} \varphi &: G \to Sym(S) \\ g &\mapsto \varphi_g \\ \varphi_g &: S \to S \\ xH &\mapsto gxH \end{aligned}$$

Dönüşümlerini ele alalım. Şimdi $\varphi_{g_1g_2} = \varphi_{g_1}\varphi_{g_2}$ eşitliğinin gösterelim.

$$\varphi_{g_1g_2}(xH) = g_1g_2(xH)$$
$$\varphi_{g_1}\varphi_{g_2}(xH) = g_1(g_2xH) = (g_1g_2)xH$$

olduğundan, $\varphi_{g_1g_2}(xH) = \varphi_{g_1}\varphi_{g_2}(xH)$ eşitliği sağlanır bu da bize dönüşümün homomorfizma olduğunu verir.

Örnek 2.25 *G* grup ve $N \lhd G$ olsun.

$$\begin{aligned} \varphi &: G \to \mathrm{Sym}(N) \\ & g \mapsto \varphi_g \\ \varphi_g &: N \to N \\ & x \mapsto gxg^{-1} \end{aligned}$$

Dönüşümleri altındaki etkiyi inceleyelim.

$$\begin{aligned} \varphi_{g_1g_2}(x) &= (g_1g_2)x(g_1g_2)^{-1} \\ &= (g_1g_2)x(g_2^{-1}g_1^{-1}) \\ &= g_1(g_2xg_2^{-1})g_1^{-1} \\ &= \varphi_{g_1}(g_2xg_2^{-1}) \\ &= \varphi_{g_1}\varphi_{g_2}(x) \end{aligned}$$

olduğundan φ dönüşümü bir homomorfizmadır.

$$\begin{aligned} \ker\varphi &= \{g \in G \mid \varphi_g(x) = I(x), \forall x \in N\} \\ &= \{g \in G \mid gxg^{-1} = x, \forall x \in N\} \\ &= C_G(N) \end{aligned}$$

Teorem 2.26 *(*Cayley*)* Her sonlu grup bir simetrik grubun altgrubuna izomorftur.

İspat. Burada amacımız bir φ dönüşümü oluşturmak bu dönüşümün bire-bir ve örten homomorfizma olduğunu göstermek olacaktır.

$$\varphi : G \rightarrow Sym(G)$$
$$g \mapsto \varphi_g$$
$$\varphi_g : G \rightarrow G$$
$$x \mapsto gx$$

$\forall g_1, g_2 \in G$ ve $x \in G$ için;

$\varphi_{g_1 g_2}(x) = (g_1 g_2)(x) = g_1(g_2 x) = \varphi_{g_1}\varphi_{g_2}(x)$

olduğundan dönüşüm bir homomorfizmadır.

$\forall y \in G$ için $\varphi_g(x) = gx = y$ olacak şekilde $x \in G$ bulunabilir .

Gerçekten, $x = g^{-1}y \in G$ alınabilir. Buradan φ_g nin örten olduðu da görülür.

Sonuç olarak $\varphi_g \in S_n$ dir.

$\ker\varphi = \{g \in G \mid \varphi_g(x) = I(x), \forall x \in G\}$

$= \{g \in G \mid gx = x, \forall x \in G\}$

$= \{e_g\}$

olduðundan φ_g dönüþümü bire-bir dir.

O halde 1.Homomorfizma Teoremine göre, $G / \ker\varphi \cong G < S_n$ olduðundan istenilen elde edilir.

Sonuç 2.27 G grubu bir S kümesi üzerine etki etsin.

$x \sim y \Leftrightarrow x = gy$ olacak şekilde $g \in G$ vardır ve bu şekilde tanımlanan ‘ ~ ’ bağıntısı bir denklik bağıntısıdır.

İspat. ~ baðýntýsý yansýmalý; $\forall x \in S$ için $x \sim x$

$x = e_g x$ olduðundan $x \sim x$

~ baðýntýsý simetrik; $\forall x, y \in S$ için $x \sim y$ ise $y \sim x$

$x \sim y \Leftrightarrow x = gy \Leftrightarrow y = g^{-1}x$ olduðundan $y \sim x$

~ baðýntýsý geçiþmeli $\forall\ x,y,z \in S$ için $x \sim y$ ve $y \sim z \Rightarrow x \sim z$

$x \sim y \Rightarrow x = g_1 y$ ve $y \sim z \Rightarrow y = g_2 z$ buradan $x = g_1(g_2 z) = (g_1 g_2)z$ olduðundan $x \sim z$ dir.

~ baðýntýsý yansýma, simetri, geçiþme özeliklerini saðladýðýndan bir denklik baðýntýsýdýr.

Tanım 2.28 G grubu bir X kümesi üzerine etki etsin.

i) $x \in X$ için $G(x) = \{gx \mid g \in G\}$ kümesin x'in G'deki ortibi denir.

ii) $x \in X$ için $G_x = \{g \in G \mid gx = x\}$ kümesine x'in G' deki sabitleºtiricisi denir.

Bundan sonra orbit denilince denklik sınıfları anlayacağız.

$$\tilde{x} = \{y \mid x \sim y\} = \{y \mid y = gx\} = \{gx \mid g \in G\} = G(x)$$

Örnek 2.29 $G = S_3$ permütasyon grubumuz $S = \{1,2,3\}$ kümesi üzerine etki etsin. Biz bu kümedeki elemanlarýn orbit ve sabitleºtiricilerini bulalým.

İspat. $S_3 = \{I, (12), (13), (23), (123), (132)\}$

$$G(1)) = \{g(1) \mid g \in G\} = \{1,2,3\}$$
$$G(2) = \{g(2) \mid g \in G\} = \{1,2,3\}$$
$$G(3) = \{g(3) \mid g \in G\} = \{1,2,3\}$$
$$G_1 = \{g \in G \mid g(1) = 1\} = \{I, (23)\}$$
$$G_2 = \{g \in G \mid g(2) = 2\} = \{I, (13)\}$$
$$G_3 = \{g \in G \mid g(3) = 3\} = \{I, (12)\}$$

Lemma 2.30 G grubu bir X kümesi üzerine etki etsin. O halde $G_x < G$ dir.

İspat. $G_x = \{g \in G \mid g(x) = x\}$, $e_G \in G$ için $e_G x = x$ olduğundan $e_G \in G_x$ ve $G_x \neq \varnothing$ dir.

$g, h \in G_x$ olsun. Yani $gx = x$ ve $hx = x$ dir.

$(gh)x = g(hx) = gx = x$ olduğundan $gh \in Gx$

$g \in Gx$ için $g\,x = x \Leftrightarrow g^{-1}gx = g^{-1}x \Leftrightarrow x = g^{-1}x \Leftrightarrow g^{-1}x = x$

Olduğundan $g^{-1} \in G_x$ şartları sağlandığından $G_x < G$ dır.

Teorem 2.31 G grubu bir X kümesi üzerine etki etsin. X kümesindeki herhangi bir elemanın orbit sayısı o elemanın sabitleştiricisinin G deki indeksine eşittir.

İspat.

$$\begin{aligned} \varphi : G(x) &\to G/G_x \\ gx &\mapsto gG_x \end{aligned}$$

$$\varphi_g(x) = gG_x,\ g_1, g_2 \in G \text{ ve } x \in X \text{ için}$$

$$g_1x = g_2x \Leftrightarrow g_2^{-1}g_1x = x \Leftrightarrow g_2^{-1}g_1 \in G_x \Leftrightarrow g_1G_x = g_2G_x$$

$$\varphi_{g_1}(x) = g_1G_x = g_2G_x = \varphi_{g_2}(x)$$

olduğundan φ iyi tanımlıdır.

$$\begin{aligned} \phi \ : \ G\,|\,G_x &\to G(x) \\ gG_x &\mapsto gx \end{aligned}$$

$$g_1G_x = g_2G_x \Leftrightarrow g_2^{-1}g_1G_x = G_x \Leftrightarrow g_2^{-1}g_1 \in G_x \Leftrightarrow g_2^{-1}g_1x = x$$

$$\Leftrightarrow g_1x = g_2x \Leftrightarrow \phi_{g_1}(G_x) = g_1x = g_2x = \phi_{g_2}(G_x)$$

olduğundan ϕ iyi tanımlıdır. Yani $|G(x)| = [G : G_x]$ şeklindedir.

NOT: Bir G grubu kendi üzerine eşlenik olarak etki ediyorsa;

$$G_x = \{g \in G \mid g(x) = x\} = \{g \in G \mid g^{-1}xg = x\} = \{g \in G \mid gx = xg\} = C_G(x)$$

şeklindedir.

Sonuç 2.32 G sonlu bir grup olsun;

i) x in G deki eşleniklerin sayısı G nin mertebesini böler.

ii) $x_i \in G$ için $G(x_1), G(x_2), \ldots, G(x_n)$, G nin farklı eşlenik sınıfındaki orbitler ise

$$|G| = \sum_{i=1}^{n} [G : C_G(x_i)] \text{ dır.}$$

İspat. i) $[G : C_G(x)] = \dfrac{|G|}{|C_G(x)|}$ Langrange Teoremine göre

$|C_G(x)|$ böler $|G|$ dir.

ii) G grubunun mertebesi ayýk orbitlerin birleþimi ºeklinde yazýlabilir.

$$G = \bigcup_{x \in G} G(x) \Leftrightarrow |G| = \sum_{i=1}^{n} |G(x_i)| = \sum_{i=1}^{n} |G : G_{x_i}| = \sum_{i=1}^{n} |G : C_G(x_i)|$$

Tanım 2.33 (Sınıf Denklemi) G sonlu bir grup ise o zaman;

$$|G| = \sum_{i=1}^{n} |G : C_G(x_i)|$$

şeklindedir.

NOT: G sonlu bir grup; $x \in C(G)$ ise $[G : C_G(x)] = 1$

$$|G| = \sum_{i=1}^{n} |G(x_i)| = \sum_{i=1}^{n} |G : G_{x_i}| = |C(G)\boxed{}| + \sum_{x_i \neq C(G)} |G(x)|$$

Sınıf denklemi bu şekilde yazılabilir.

Örnek 2.34 $G = S_3$ permütasyon grubunu elemanlal

S_3'ün elemanlarý $\{I, (12), (13), (23), (123), (1\ \ 32)\}$ ºeklindedir.

$C(G) = C(S_3) = \{I\}$

G nin farklý eþlenik sýnýflarý $\{I, (12), (13), (23)\}$ ve $\{(123), (132)\}$ ºeklindedir.
Bu kümedeki herhangi bir eleman almamýz yeter lidir. Bunlarýn merkezleyenleri;
$C_G((12)) = \{I, (12)\}$ ve $C_G((123)) = \{I, (123), (132)\}$ bunula beraber;

$$|C(S_3)| + (S_3 : C_G((12))) + (S_3 : C_G((123))) = 1 + 3 + 2 = |S_3|$$

Tanım 2.35 (Otomorfizma) G grubunun kendi üzerine bir izomorfizmasýna otomorfizma denir. Aut G ile gösterilir.

$$\mathrm{Aut}G = \{\varphi : G \to G \mid \varphi \text{ izomorfizma}\}$$

Tanım 2.36 (Ýç Otomorfizma) G bir grup ve $\varphi_g(x) = g^{-1}xg$ ile tanımlanan bir otomorfizmaya iç otomorfizma denir. İç otomorfizmaların kümesi Inn G ile gösterilir.

Lemma 2.37 $\mathrm{Inn}G \lhd \mathrm{Aut}G$

İspat. Ýlk önce $\mathrm{Inn}G < \mathrm{Aut}G$ olduðunu göstermemiz gerekir.

$e_G = i_1 \in \mathrm{Inn}G$, yani $\mathrm{Inn}G \neq \varnothing$.

$i_g, i_h \in \mathrm{Inn}G$ ve $(i_h)^{-1} = i_{h^{-1}}$ alalým.

$$i_g(i_h)^{-1}(x) = i_g(i_{h^{-1}}(x)) = g(i_{h^{-1}}(x))g^{-1} = g(h^{-1}xh)g^{-1} = i_{gh^{-1}}(x)$$

Bununla beraber $i_g(i_h)^{-1} = i_{gh^{-1}} \in \mathrm{Inn}G$ olduðundan $\mathrm{Inn}G < \mathrm{Aut}G$ dýr.

Þimdi $g \in G$ ve $\varphi \in \mathrm{Aut}G$ alalým.

$$\varphi i_g \varphi^{-1}(x) = \varphi(g\varphi^{-1}(x)g^{-1}) = \varphi(g)x\varphi(g^{-1}) = \varphi(g)x\varphi(g)^{-1} = i_{\varphi(g)}(x)$$

olduğundan $\varphi i_g \varphi^{-1}(x) = i_{\varphi(g)} \in InnG$;

$\mathrm{Inn}G \lhd \mathrm{Aut}G$ bulunmuþ olur.

Lemma 2.38 G bir grup olsun.

i) $\forall g \in G$ için g ile eþlenikleri G nin bir otomorfizmasýný belirler

ii) G den Aut (G) *ye* bir homomorfizma vardır ve bunun çekirdeği

$$C(G) = \{g \in G \mid gx = xg, \forall x \in G\} \text{ dir.}$$

İspat. i) G grubu kendi üzerine eşlenik olarak etki etsin. Bu etkiyi şu şekilde tanımlayalım.

$$\varphi : G \to G$$
$$x \mapsto gxg^{-1}$$

$\varphi_{g_1}\varphi_{g_2}(x) = \varphi_{g_1}(g_2 x g_2^{-1}) = g_1(g_2 x g_2^{-1}) = (g_1 g_2)x(g_1 g_2)^{-1} = \varphi_{g_1 g_2}(x)$

φ bire birdir; $\forall x, y \in G$ için $\varphi(x) = \varphi(y) \Rightarrow x = y$,

$\varphi(x) = \varphi(y) \Leftrightarrow gxg^{-1} = gyg^{-1} \Leftrightarrow gx = gy \Leftrightarrow x = y$

olduðundan $\varphi : G \to G$ dönüþümü bire bir örten homorfizmadýr.

ii)

$$\varphi : G \to \mathrm{Aut}G$$
$$g \mapsto \varphi_g$$
$$\varphi_g : G \to G$$
$$x \mapsto gxg^{-1}$$

φ nin bir homomorfizma olduğunu ilk şıkta göstermiştik.
ª imdi dönüºümün çekirdðini bulalým.

$$\begin{aligned} \ker\varphi &= \{g \in G \mid \varphi_g(x) = I(x), \forall x \in G\} \\ &= \{g \in G \mid gxg^{-1} = x, \forall x \in G\} \\ &= \{g \in G \mid gx = xg, \forall x \in G\} \\ &= C(G) \end{aligned}$$

Lemma 2.39 $H < G$ ve G grubu S kümesi üzerine sol çarp mý ile etki etsin. S kümesi H nin G içindeki sol yan kümelerinden oluşsun.
$G \to Aut\ (S)$ dönüşümünün çekirdeği H nin içine düşer.

İspat.

$$\varphi : G \to \mathrm{Aut}(S)$$
$$g \mapsto \varphi_g$$
$$\varphi_g : \quad S \to S$$
$$xH \mapsto gxH$$

etkisini göstermiştik. Şimdi dönüşümün çekirdeğini gösterelim.

$$\ker\varphi = \{g \in G \mid \varphi_g(xH) = I(xH), \forall xH \in S\}$$
$$= \{g \in G \mid gxH = xH, \forall xH \in S\}$$
$$= \{g \in G \mid g \in H\}$$
$$= g \in H$$

Lemma 2.40 $H < G$ ve G sonlu bir grup olsun **.** H nin G içindeki indeksi p ve $[G:H] = p$ olmak üzere p sayısı G nin mertebesini bölen en küçük asal sayı *i*se $H \lhd G$ dir.

İspat. S kümesi H nin G içindeki sol yan kümelerinden oluºsun. $S = \{xH \mid h \in H\}$ $[G:H] = p$ ve $A(S) \cong S_p$ dir. K, $G \to A(S)$ dönüºümünün çekirdeði olsun.

$$\begin{array}{rcccl} \varphi & : & G & \to & A(S) \\ & & g & \mapsto & \varphi_g \\ \varphi_g & : & S & \to & S \\ & & xH & \mapsto & gxH \end{array}$$

etkisini tanımlayalım. $G \to A(S)$ dönüşümünün çekirdeğinin H *n*in içine düştüğünü lemma 2.39 da göstermiştik.

$\forall g \in G$ ve $\forall x \in \mathrm{Ker}\varphi$ için $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)e\varphi(g)^{-1} = e$

olduğundan $\mathrm{Ker}\varphi \lhd G$ yani $K \lhd G$ dir. $K \lhd G$ yani K grubu G de normal olduğundan G/K bölüm grubundan söz edebiliriz.

Cayley Teoremi gereğince her sonlu grup bir simetrik grubun altgrubuna izomorftur yani $G/K \cong S_p$ dir.

Lagrange Teoremi gereğince; G/K nın mertebesi S_p'nin mertebesini böler, o halde $|S_p| = p!$, $|G/K|$ böler.

$|G/K| = [G:K]$ ve $|G| = |K|[G:K]$

Hipotezden p, G'nin mertebesini bölen en küçük asal sayıydı.

$|G:K| = p$ veya $|G:K| = 1$ olmalıdır

$|G/K| = [G:K] = [G:H][H:K] = p[H:K] \geq p$

$[G:K] = p$ ve $[H:K] = 1$ olmak zorundadır.

$[H:K] = 1$ ise $H = K$ ve $K \lhd G$ olduğundan $H \lhd G$ olur. $\lhd$

Örnek 2.41 G grubunun bir elemanı iki tane eşleniğine sahipse G nin birimden farklı normal alt grubu vardır.

İspat. $|G(x)| = [G : G_x(a)] = [G : C_G(a)] = 2$ ise $C_G(a) \lhd G$.

Teorem 2.42 G / C(G) devirliyse G grubu değişmelidir.

İspat. *C(G)* $\lhd G$

Hipotezden; $G / C(G) = < C(G)g >, \ g \in G$

$$\forall x \in G \text{ için } C(G)x = (C(G)g)^m = C(G)g^m, \ m \in \mathbb{Z}$$
$$x, y \in G \text{ için } x \in g^m(G), \ y \in g^n(G) \text{ ve } \exists m, n \in \mathbb{Z}$$
$$x = hg^m, \ y = kg^n \text{ ve } h, k \in C(G)$$
$$xy = (hg^m)(kg^n) = h(g^m k)g^n = h(kg^m)g^n = (hk)(g^m g^n)$$
$$(hk)(g^{m+n}) = (hk)(g^{n+m}) = (kh)(g^n g^m) = k(hg^n)g^m$$
$$(kg^n)(hg^m) = yx$$

olduğundan G grubu değişmelidir.

2.3 Sylow Teoremleri

Lemma 2.43 Mertebesi p^n (p asal) olan H grubu sonlu S kümesine etki etsin ve

$S_0 = \{x \in S \mid hx = x, \ \forall h \in H\}$ ise $|S| \equiv |S_0| \ (\bmod\, p)$ dir.

İspat. Bir H(x) orbitinin bir eleman içermesi için gerek ve yeterli °art

$x \in S_0$ olmasıdır. $S = S_0 \cup H(x_1) \cup H(x_2) \cup \ldots \cup H(x_n)$ dir. Bileşimlerin hepsi ayrık olduğu için S kümesi $|S| = |S_0| + |H(x_1)| + |H(x_2)| + \ldots + |H(x_n)|$ şeklinde yazılabilir. $|H(x_i)| = [H : H_{x_i}]$ olduğundan Lagrange Teoremi gereğince $|H(x_i)| \, \big| \, |H| = p^n$ dir. O halde $p \, \big| \, |H(x_i)|$ bununla beraber $|S| \equiv |S_0| (\bmod\, p)$ dir.

Teorem 2.44 $\left(\text{Cauchy}\right)$ p asal sayýsý G sonlu grubunun mertebesini bölüyorsa G içinde mertebesi p olan en az bir eleman vardır.

İspat. $S=\{(a_1,a_2,\ldots,a_{p-1},a_p) \mid a_i \in G$ ve $a_1a_2\ldots a_p = e\}$ kümesini alalım.

a_p elemaný, $(a_1a_2\ldots a_{p-1})^{-1}$ ile tek türlü bellidir. G nin mertebesi n olsun. Bu durumda $|S| = n^{p-1}$ olur. p | $|G|$ kabul etmiştik o halde $p|n$ olur. Bu durumda $|S| \equiv 0 \pmod p$ olur. $\mathbb{Z}_p$ grubu S kümesi üzerine aşağıdaki dönüşüm ile etki eder.

$$\varphi : \quad \mathbb{Z}_p \times S \to S$$
$$(k,(a_1,a_2,\ldots,a_p)) \mapsto (a_{k+1},a_{k+2},\ldots,a_p,a_1,\ldots,a_k)$$

φ dönüºümü iyi tanýmlýdýr.

$a_1a_2...a_ka_{k+1}a_{k+2}...a_{p-1}a_p = e$ olduðunu biliyoruz.

$(a_1a_2...a_k)^{-1}(a_1a_2...a_k)(a_{k+1}a_{k+2}...a_{p-1}a_pa_1a_2...a_k)$

$(a_1a_2...a_k)^{-1}\left[(a_1a_2...a_k)(a_{k+1}a_{k+2}...a_{p-1}a_p)\right](a_1a_2...a_k)$

$(a_1a_2...a_k)^{-1}(a_1a_2...a_k) = e$ olduðundan $a_{k+1}a_{k+2}...a_pa_1...a_k = e$ olur ve

$\left(a_{k+1},a_{k+2},...,a_p,a_1...a_k\right) \in S$ olduðu gösterilmiþ

ªimdi φ dönüºümün homomorfizma olduðu gösterilmeye çalýþalým

$$\varphi_{k_1}\varphi_{k_2}(a_1,a_2,...,a_p) = \varphi_{k_1}(a_{k_2+1},a_{k_2+2},...,a_p,...,a_{k_2})$$
$$= (a_{k_1+k_2+1},a_{k_1+k_2+2},...,a_p,a_1,...,a_{k_1+k_2})$$
$$= \varphi_{k_1+k_2}(a_1a_2...a_p)$$

olduðundan φ dönüþümü bir homomorfizmadýr.

$(a_1,a_2,...,a_p) \in S_0$ olmasý için gerek ve yeter ºart $a_1 = a_2 = \ldots = a_p$ olmasýdýr.

$(a_1,a_2,\ldots,a_p) \in S_0$ ise $\forall k \in Z$ için $(k(a_1,a_2,\ldots,a_p)) = (a_1,a_2,\ldots,a_p)$ buradan $(a_{k+1},a_{k+2},\ldots,a_p,a_1,\ldots,a_k) = (a_1,a_2,\ldots,a_p)$ dır.

$a_{k+1} = a_1, a_{k+2} = a_2,\ldots,a_p = a_k$ örnek olarak;

$k=1$ için; $(a_2,a_3,a_4,a_5,a_1) = (a_1,a_2,a_3,a_4,a_5)$ buradan

$a_1 = a_2, a_2 = a_3, a_3 = a_4, a_4 = a_5, a_5 = a_1$

$(a,a,\ldots,a)\in S_0$ dır. $aaa\ldots a=e$ buradan $a^p=e$ ve $|a|=p$ dir. O halde $0\equiv|S|\equiv|S_0|(\text{mod } p)$ dır.

Tanım 2.45 G grubunda her elemanın mertebesi bir p asal sayısının kuvveti ise G grubu p-gruptur denir.

Tanım 2.46 H, G nin bir alt grubu ve H bir p-grup ise H grubuna G grubunun bir p-altgrubudur denir.

Tanım 2.47 p bir asal sayı olmak üzere bir G grubu mertebesi p olan devirli grupların direkt çarpımı şeklinde yazılabiliyorsa bu gruba elemanter değişmeli p-grup denir.

Sonuç 2.48 G sonlu grubunun p-grup olması için gerek ve yeterli şart G nin mertebesinin p nin kuvveti şeklinde yazılmasıdır.

İspat. *G* sonlu bir grup q bir asal sayı ve q| |G| olsun.

Buradan $q\,|\,p^n$, p *ve* q nun asallığından p = q dur. Dolayısıyla G nin mertebesi p asal sayısının kuvveti şeklinde yazılır.

Örnek 2.49 $N\lhd G$ olsun. N ve G / N her ikisi birden bir p-grupsa G de bir p-gruptur.

İspat. $N\lhd G$ olduğundan G / N bölüm grubundan bahsedebiliriz. Bu bölüm grubunu G / N= $\{gN\,|\,g\in G\}$ şeklinde tanımlayabiliriz. Şimdi G / N p-grup ise buradaki her elemanın mertebesini bir $p_1=p^k$ asal sayısının kuvveti şeklinde yazabiliriz. Yani $(gN)^{p_1}=N$ ve $g^{p_1}N$ = N buradan da $g^{p_1}\in N$ olur. N grubu bir *p*-grup olduğundan aynı mantıkla $(g^{p_1})^{p_2}=e_G$ olacak şekilde $p_2=p^m$ asal sayısı vardır. Yani $g\in G$ için $g^{p_1p_2}=e_G$ olduğundan G grubu bir *p*-gruptur.

Sonuç 2.50 Aşikar olmayan sonlu her p-grubun merkezi birimden farklıdır.

İspat. G bir p-grup olsun. Sınıf denkleminden; $|G|=|C(G)|+\sum[G:C_G(x_i)]$

dir. Burada $[G:C_G(x_i)]>1$ olduğunu biliyoruz.

G bir p-grup olduğundan $|G| = \mathrm{p}^{\mathrm{n}}$ ve $n \geq 1$ şeklinde yazabiliriz. Ayrıca $[G : C_G(x_i)]$in G grubunun mertebesini böldüğünü de biliyoruz. Buradan $p \mid [G : C_G(x_i)]$ ve $p \mid |G|$ olduğundan $p \mid |C(G)|$ dir. Cauchy teoreminden $C(G)$ içinde en az bir p mertebeli eleman vardır. Dolayısıyla $C(G) \neq 1$ dir.

Teorem 2.51 p bir asal sayı olmak üzere $|G| = p^2$ ise G değişmelidir.

İspat. $C(G) = G$ olduğunu gösterirsek işimiz biter. $C(G) \lhd G$ olduğundan Lagrange teoremi gereğince; $|\mathrm{C(G)}| = 1, \mathrm{p}$ veya p^2 olabilir. Sonuç 2.50 den

$|C(G)| \neq 1$ dir. Şimdi G grubu değişmeli olmasın ve $|C(G)| = p$ olduğunu kabul edelim. $C(G) \lhd G$ olduğundan $G / C(G)$ bölüm grubundan bahsedebiliriz. Bu grubun mertebesi $p^2 / p = p$ dir. Mertebesi p asal sayı olan grup devirlidir.

$G / C(G)$ devirli ise G grubu değişmelidir. Böylelikle kabulümüzle çelişki elde edilmiş oldu. O halde $|C(G)| = p$ olamaz. $|C(G)| = p^2$ dir yani $C(G) = G$ olduğundan G grubu değişmelidir.

Lemma 2.52 H grubu G nin bir p-altgrubu olsun. O zaman $[N_G(H) : H] \equiv [G : H] \pmod{p}$ dir.

İspat. S kümesi H nın G içinde sol yan kümeleri olsun. H grubu S kümesi üzerine Örnek 2.24 deki gibi etki etsin.

$$xH \in S_0 \Leftrightarrow hxH = xH, \forall h \in H \Leftrightarrow x^{-1}hxH = H, \forall h \in H \Leftrightarrow x^{-1}hx \in H,$$
$$\forall h \in H \Leftrightarrow x^{-1}Hx = H \Leftrightarrow xHx^{-1} = H \Leftrightarrow x \in N_G(H)$$

Buradan $|S_0|$, $N_G(H)$ da H nin yan kümelerinin sayısına eşittir.

Dolayısıyla $|S_0| = [N_G(H) : H]$ dir. Lemma 2.43 den;

$$[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \pmod{p} \text{ dir.}$$

Lemma 2.53 H grubu G nin sonlu bir p-altgrubu olsun. Eğer $\mathrm{p} \mid [\mathrm{G} : \mathrm{H}]$ ise $N_G(H) \neq H$ dır.

İspat. $[N_G(H):H]=|S_0|\equiv|S|=[G:H]\ (\text{mod}\ p)$ ve $p \mid [G:H]$ olduğundan

$[G:H]\ (\text{mod}\ p)\equiv 0$ dır.

$0\equiv[G:H]\equiv[N_G(H):H]\ (\text{mod}\ p)$ ise o halde $[N_G(H):H]<1$ dir. Buradan $N_G(H)\neq H$ *dır.*

Sonuç 2.54 G bir grup ve $N \lhd G$ olsun. O zaman G/N grubunun her alt grubu K, N normal alt grubunu kapsayan G grubunun bir alt grubu olmak üzere K/N

biçimindedir. Üstelik $K/N \lhd G/N \Leftrightarrow K \lhd G$ dir.

Teorem 2.55 (I. Sylow Teoremi) G, $p^n m$ mertebeli bir grup olsun.

$n\geq 1, p$ *asal ve* $(p,m)=1$ olsun. O zaman her bir $1\leq i\leq n$ için, G mertebesi p^i

olan bir altgrup içerir. Ayrıca G de mertebesi p^i olan her altgrup mertebesi p^{i+1} olan altgrupta normaldir.

İspat. $p \mid |G|$ olduğunda*,* Cauchy teoremi gereğince G içinde p mertebeli bir eleman vardır. Bu eleman ile üretilen grubu $<a>$ ile gösterelim. Şimdi G grubunu mertebesi üzerinden tümevarım uygulayalım. H altgrubu mertebesi p^i

$1\leq i\leq n$*,* olan G nin bir altgrubu olsun. O zaman $p \mid [G:H]$ ve H altgrubu $N_G(H)$ da normaldir. Lemma 2.52 ve Lemma 2.59 dan;

$H\neq N_G(H)$ ve $1<|N_G(H)/H|=|N_G(H):H|=|G:H|=0\ (\text{mod}\ p)$

Bundan dolayı $p \mid |N_G(H)/H|$ ve Cauchy teoremi gereğince $|N_G(H)/H|$ mertebesi p olan bir altgrup içerir. Bu altgrup H_1/H formundadır. Burada $H_1<G$ dir. $H, N_G(H)$ da normal olduğundan H de H_1 de normal olması gerekir. Sonuçta; $|H_1|=|H||H_1/H|=p^i p=p^{i+1}$ bu da ispatımızı bitirir.

Tanım 2.56 G sonlu bir grup ve p asal sayı olmak üzere, G nin maksimum p-alt grubuna G nin Sylow p-altgrubu denir. G içinde bir maksimal p-altgrup ise Sylow p-altgruptur denir.

Örnek 2.57 S_3 ün Sylow altgruplarını bulalım.

$H = \{I,(12)\} < G$ ve $|H| = 2$ olduğundan H grubu G nin 2-Sylow alt grubudur.
H nin eşleniği olan;

$(13)^{-1}H(13) = \{I,(23)\}$ ve $(23)^{-1}H(23) = \{I,(13)\}$ altgrupları da 2-Sylow

altgruplarıdır.

$K = \{I,(123),(132)\}$ grubu 3-Sylow altgruptur. Eşlenikleri kendisine eşittir.

Sonuç 2.58 G mertebesi $p^n m$ olan p asal $n \geq 1$ ve $(m,p) = 1$ olacak şekilde bir grup olsun. H, G nin p-altgrubu olsun.

(i) H grubu G nin bir Sylow p-altgrubu olması için gerek şart $|H| = p^n$.

(ii) G nin her Sylow p-altgrubunun eşleniği bir Sylow p-altgruptur.

(iii) P, G nin tek Sylow p-altgrubu ise $P \lhd G$ dir.

İspat. (i) : H grubu G nin bir Sylow p-altgrubu olsun. O halde H grubu G nin maksimal p-altgrubudur. Buradan H nin mertebesi p^n şeklindedir.

(ii) : P, G nin bir Sylow p-altgrubu $\Leftrightarrow |P| = p^n$ dir.

$x^{-1}Px < G$ $|x^{-1}Px| = |P| = p^n \Rightarrow x^{-1}Px$, G nin bir Sylow p-altgrubudur.

(iii) : P, G nin tek Sylow p-altgrubu ve $x^{-1}Px$ de G nin bir Sylow p-altgrubu ise $\forall x \in G$ için $x^{-1}Px = P$ olur. Böylece $P \lhd G$ olur.

Teorem 2.59 (II.Sylow Teoremi) H grubu sonlu G grubunun bir p-altgrubu ve P G nin Sylow p-altgrubu ise $x \in G$ vardır ki $H < xPx^{-1}$. Üstelik G grubunun bütün Sylow p-altgrupları eşleniktir.

İspat. $S = \{xP \mid x \in G\}$ ve H grubu S kümesi üzerine sol çarpımla etki etsin. Bu etkiyi daha önce göstermiştik.

$$|S_0| \equiv |S| = [G:P] \pmod{p}$$

$|G| = [G : P]|P|$ buradan $p^n m = [G : P]p^n$

p bölmez m buradan p bölmez $[G : P]$. O halde $|S_0| \neq 0$

Sonuçta S_0 ın en az bir xP yan kümesi vardır.

$xP \in S_0 \Leftrightarrow hxP = xP,\ \forall h \in H \Leftrightarrow x^{-1}hxP = P, \forall h \in H \Leftrightarrow x^{-1}Hx < P$

$\Leftrightarrow H < xPx^{-1}$

H bir Sylow p-sylow altgrup ise $|H| = |P| = |xPx^{-1}|$ ve buradan $H = xPx^{-1}$

Teorem 2.60 (III.Sylow Teoremi) G sonlu bir grup p bir asal sayı olsun. O zaman Sylow p-alt gruplarının sayısı $|G|$ yi böler ve $k \in \{0\} \cup Z^+$ için Sylow p-alt gruplarının sayısı $kp+1$ formundadır.

İspat. II. Sylow teoreminden Sylow p-altgruplarının sayısı herhangi birinin eşleniklerinin sayısıdır. Bu sayı $[G : N_G(P)]$ dir ve $|G|$ nin bir bölenidir. Bu arada $N_G(P) = \{x \in G \mid xPx^{-1} = P\}$ şeklinde tanımlarız.

S, G nin tüm Sylow p-altgruplarının bir kümesi olsun ve P , S kümesi üzerine eşlenik ile etki etsin.

$$\begin{array}{cccc} \varphi & : P & \rightarrow & Aut(S) \\ & x & \mapsto & \varphi_x \\ \varphi_x & S & \rightarrow & S \\ & Q & \mapsto & xQx^{-1} \end{array}$$

$Q \in S_0 \Leftrightarrow xQ = Q,\ \forall x \in P \Leftrightarrow xQx^{-1} = Q,\ \forall x \in P$ *o halde* $P < N_G(Q)$ *dur.*

P ve Q her ikisi birden $N_G(Q)$ nun altgruplarý olduðundan G nin Sylow p altgrubudur ve bu altgruplar $N_G(Q)$ da eşleniktirler. Ancak $Q \triangleleft N_G(Q)$ dur.
$Q = P$ olursa $S_0 = \{P\}$ gerçekleşir.
$|S| = |S_0| = 1 \pmod p$ bundan dolayı $|S| = kp+1$ dir.+

Lemma 2.61 p bir asal sayı ve m yi bölmüyorsa o zaman $\forall n \geq 1$ için $\binom{p^a m}{p^a}$ sayısı p ile bölünemez.

İspat. n elemanlı bir kümenin k elemanlı alt kümelerinin k elemanlı alt kümelerinin sayısı;

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad \text{şeklindedir.}$$

Eğer $n = p^a m$ *,* p asal sayı ve $p^r \mid m$ ancak p^{r+1} bölmez m ise;

$$\binom{p^a m}{p^a} = \frac{(p^a)!}{(p^a)!(p^a m - p^a)!} = \frac{p^a m(p^a m-1)\ldots(p^a m-i)\ldots(p^a m - p^a + 1)}{p^a(p^a-1)\ldots(p^a-i)\ldots(p^a-p^a+1)}$$

Paydaki m terimi hariç $(p^a m - i)$ yi bölen p nin kuvveti ile $(p^a - i)$ yi bölen p nin kuvveti aynıdır. Böylece m yi bölen p nin kuvvetleri dışında diğer tüm kuvvetler gözardı edilebilir.

Böylece $p^r \mid \binom{p^a m}{p^a}$ dır ancak p^{r+1} bölmez $\binom{p^a m}{p^a}$ dır.

Teorem 2.62 (Sylow Teoreminin Diğer Bir İspatı) p bir asal sayı ve $p^a \mid |G|$ ise G mertebesi p^a olan bir alt gruba sahiptir.

İspat. $\mathcal{M}$, G de p^a elemanlı tüm alt kümelerinin küme si olsun . Bu durumda $\mathcal{M}$ *nin* eleman sayısı $\binom{p^a m}{p^a}$ dır. Verilen $M_1, M_2 \in \mathcal{M}$ için $M_1 \sim M_2$ yi

$M_1 = M_2 g$ olacak şekilde $g \in G$ olarak tanımlayalım. (M_1, G de p^a elemanına sahip bir alt küme dolayısıyla M_2 de p^a elemanına sahip bir alt kümedir.)

Burada $\sim$ bağıntısı $\mathcal{M}$ kümesi üzerinde bir denklik bağıntısıdır.

$\sim$ bağıntısı yansımalıdır. $M_1 = M_1 e_G$ olacak şekilde e_G G de olduğundan $M_1 \sim M_1$ dir.

$\sim$ bağıntısı simetriktir. $M_1 \sim M_1$, $M_1 = M_2 g$ olacak °ekilde $g \in G$ vardır. Buradan $M_1 g^{-1} = M_2$ olacak şekilde $g^{-1} \in G$ olduğundan $M_1 \sim M_2$ dır.

$\sim$ bağıntısı geçişmelidir. $M_1 \sim M_2$ ve $M_2 \sim M_3$ ise $\mathrm{M_1 = M_2 g_1}$ ve $\mathrm{M_2 = M_3 g_2}$ olacak şekilde $g_1, g_2 \in G$ vard. Buradan $M_1 = (M_3 g_2) g_1$ ve $M_1 = M_3(g_2 g_1)$ olduğundan $M_1 \sim M_3$ dür. M nin denlik sınıfından en az birisinin eleman sayısı p^{r+1} in katı değildir. Hepsi p^{r+1} in katı o zaman p^{r+1} sayısı $\begin{pmatrix} p^a m \\ p^a \end{pmatrix}$ yı bölerdi.

M, $\begin{pmatrix} p^a m \\ p^a \end{pmatrix}$ tane elemana sahip olduğundan ve $\mathrm{p^{r+1}}$ bölmez $\begin{pmatrix} \mathrm{p^a m} \\ \mathrm{p^a} \end{pmatrix}$ olduğundan bu durum olamaz. $\{M_1, M_2, \ldots, M_n\}$ kümesi yukarıdaki koşulu sağlayan denklik sınıfı olsun ve dolayısıyla $\mathrm{p^{r+1}}$ bölmez n dir. M deki denklik tanımımızdan, $g \in G$ olmak üzere her bir $i = 1, \ldots, n$ için $M_i g = M_j$ olacak şekilde $\exists\ 1 \le j \le n$ için yazýlabilir.

$\mathrm{H = \{g \in G \mid M_1 g = M_1\}}$ grubunu alal $a, b \in H$ için $M_1 a = M_1$ ve $M_1 b = M_1$ olduğunda $M_1 ab = (M_1 a)b = M_1 b = M_1$ ile H grubu G de bir alt gruptur. Bizim için önemli olan H altgruplarının mertebesini bulabilmek. H grubunun mertebesi G nin mertebesine eşit olmasın.

H<G olduğundan ve Lagrange teoremi gereğince $|\mathrm{H}| \mid |\mathrm{G}|$ yani $\mathrm{n} \cdot |\mathrm{H}| = |\mathrm{G}|$ dir.

$n.|H| = |G| = p^a m, p^{r+1}$ bölmez $n, p^r \mid m$ ve $p^{a+r} \mid p^a m = n.|H|$ dır. O halde $p^a \mid$ |H| dır ve buradan $|H| \ge p^a$ dır.

Eğer $\mathrm{m_1 \in M_1}$ ise $\forall \mathrm{h \in H}$ için $\mathrm{m_1 h \in M_1}$ dir. Dolayısıyla M_1 en az H nın mertebesi kadar farklı elemana sahip olur. M_1,G nin p^a elemanını kapsayan alt kümesiydi. O halde $p^a \ge |H|$ dır. Bir $|H| \ge p^a$ ve $p^a \ge |H|$ ise $|H| = p^a$ yı elde ederiz. Böylece H grubu G nin p^a elemanı olan elemanı olan alt grubu olur. Böylece ispatımız tamamlanır.

2.4. Sylow Teoremlerinin Uygulamaları

Şimdi mertebeleri küçük olan bazı sonlu grupların Sylow teoremleri yardımıyla basit olup olmadıklarını inceleyeceğiz.

Örnek 2.63 Mertebesi 20 olan grubun basit olamayacağını gösteriniz.

İspat. 20 nin asal bölenleri 2 ve 5 olduğundan G nin Sylow 2 ve 5 altgrupları vardır. Sylow 5-altgruplarının sayısı III. Sylow teoremine göre, 20 yi böler ve $5k+1$ tanedir. 20 nin bölenleri; 1, 2, 4, 5, 10 ve 20 arasında bu özellikteki sayı ancak 1 olabilir. Şu halde bir tek Sylow 5-alt grup vardır ve bu yine Sylow teoreminden aynı zamanda normal bir alt gruptur. O halde böyle bir grup basit olamaz.

Örnek 2.64 Mertebesi 30 olan bir grubun basit olmadığını gösteriniz.

İspat. 30 un bölenleri 1, 2, 3, 5, 6, 10, 15 ve 30 dur. III. Sylow teoremine göre , 5-Sylow altgruplarının sayısı 1 veya 6 olabilir. Bu sayı 6 olsaydı farklı Sylow 5-alt gruplarının kesişimleri $\{e\}$ den ibarettir çünkü 5 asaldır, bu Sylow 5-alt gruplarında birimden farklı 4.6=24 eleman bulunurdu.

Diğer taraftan, Sylow 3-altgruplarının sayısı, benzer düşünce ile 1 veya 10 olabilir. Bu sayı 10 olsaydı, farklı Sylow 3-alt gruplarının kesişimleri de $\{e\}$ den ibaret olacağından, bu Sylow 3-alt gruplarında da birimden farklı 2.10 = 20 eleman bulunurdu.

Halbuki Sylow-3 ve Sylow-5 altgruplarının da kesişimleri birimden ibaret olduğundan, grupta birim elemanla birlikte en az 24+20+1 = 45 eleman olması gerekirdi. Ancak grubumuzun mertebesi 30 olduğundan bu da imkansız bir durum. O halde, Sylow 3 veya 5 altgruplarından birinin sayısı 1 olmak zorundadır. Tek olan Sylow altgrubu da normal olacağından grubun basit olmadığı anlaşılır.

Örnek 2.65 Mertebesi 42 olan bir grubun , Sylow 7-alt grubunun bir normal alt grup olduğunu gösteriniz.

İspat. 42 nin bölenleri 1,2,3,6,7,14,21 ve 42 dir. Üçüncü Sylow teoremine göre Sylow 7-altgruplarının sayısı 1 ve bu alt grubun mertebesi 7 ve normaldir.

Örnek 2.66 Mertebesi 28 olan bir grubun 7. mertebeden bir normal alt grubun varlığını gösteriniz. Eğer bu grubun 4. mertebeden bir normal alt grubu varsa, grubun değişmeli olacağını gösteriniz.

İspat. *28* in bölenleri 1, 2, 4, 7, 14 ve 28 dir. Üçüncü Sylow teoremine göre , Sylow 7-altgruplarının sayısı 1 tane olup 7. mertebeden ve normaldir. Grubun Sylow 7-altgrubunu H ile gösterelim.

Eğer 4. mertebeden bir normal altgrubu varsa, bu Sylow 2-altgruptur ve mertebesi bir asal sayının karesi olduğundan değişmelidir. Bu alt grubu da K ile gösterelim.

| H | = *7* ve | K | = *4* olduğundan, $H \cap K = \{e_G\}$ olduğu açıktır.

$\mathrm{H,K} \lhd \mathrm{G} \Rightarrow \mathrm{HK} < \mathrm{G}$ ve $\mathrm{H} \cap \mathrm{K} = \{\mathrm{e_G}\}$ olduğundan $|\ \mathrm{H\ K}\ | = 28 \Rightarrow \mathrm{HK} = \mathrm{G}$ bulunur. O halde $\mathrm{G} \cong \mathrm{H} \times \mathrm{K}$ olup, H ve K değişmeli olduklarından G nin de değişmeli grup olduğu anlaşılır.

2.5 Sonlu Grupların Sınıflandırılması

Önerme 2.67 Mertebesi p asal sayısı olan bir grup basit gruptur.

İspat. Lagrange teoreminden sonlu bir grubun her altgrubunun mertebesi grubun mertebesini böleceğinden bu grup basit gruptur. Çünkü p asal sayıdır.

Önerme 2.68 p, q asal sayılar p > q ve q bölmez p-1 olsun. Mertebesi pq olan her grup Z_{pq} devirli grubuna izomorftur. Eğer q | p-1 ise mertebesi pq olan iki farklı grup vardır. Bunlar Z_{pq} devirli grubu ve değişmeli olmayan aşağıdaki özellikleri gerçekleyen bir K grubuna izomorftur. K grubu c ve d elemanlarından oluşur öyle ki ; | c |= p ; | d |= q ; dc=$c^s d$, $s \not\equiv 1\ (mod\, \mathrm{p})$ ve $s^q \equiv 1\ (mod\, \mathrm{p})$.

İspat. | G | = pq p, q asal sayılar ve p > q olsun. Cauchy teoremi gereğince G içinde mertebesi p ve q olan iki eleman vardır. Bunlar a, b olsunlar öyle ki | a | = p ve | b |= q şeklindedir. Mertebesi asal sayı olan grup devirlidir.

S = < a > devirli grubu Sylow p-altgrubudur. Lemma 2.40 dan [G : S] = q ve q sayısı G nin mertebesini bölen en küçük asal sayı olduğundan $S = < a > \lhd G$ dir.

Böylece bS sol yan kümelerinin sayısı q dur . $S \triangleleft G$ olduğundan G / S bölüm grubundan söz edebiliriz. Bu bölüm grubunun mertebesi q asal sayısıdır. Mertebesi asal sayı olan grup devirlidir. O halde G / S bölüm grubu bS ile üretilen devirli bir gruptur. Yani G / S =< bS > dir. Bu nedenle G nin elemanları $b^i a^j$ ve G = < a , b > şeklinde yazılabilir.

| G |=pq ve q asal sayı olduğundan III. Sylow teoremine göre sylow – q alt gruplarının sayısı | G | = pq yu böler ve bazı k$\geq$ 0 için bu sayı kq+1 şeklindedir. Bu yüzden bu sayı 1 veya p dir. q bölmez p -1 olduğundan bu sayı 1 olur. Yani < b > ile üretilen sylow – q alt grupları 1 tanedir ve aynı zamanda G de normaldir.

Lagrange teoremi gösterir ki $<a> \cap <b> = \{e\}$ dir. Özet olarak $<b> \triangleleft G$ ve $<a> \cap <b> = \{e\}$ olduğundan $|G| = \dfrac{|a| \cdot |b|}{|<a> \cap <b>|}$ dir.

$G = <a> \times <b> \cong Z_p \oplus Z_q \cong Z_{pq}$.

p | q-1 ve $<a> \triangleleft G$ olduğundan $bab^{-1} = a^r$ ve $r \not\equiv 1$ (mod p) . Eğer $r \equiv 1$ (mod p) olursa G grubu değişmeli olur. G tek sylow q-alt grubuna sahiptir. Bu yüzden $bab^{-1} = a^r$ tümevarımla $b^j a b^{-j} = a^{r^j}$, $j = q$.

$a = a^{r^q}$ ve $r^q \equiv 1$ (mod p) . q| p-1 olduğunda G nin değişmeli olamayacağını söyledik. $x^q \equiv 1$ (mod p) olunca x in $r^k \equiv 1$(mod p) ye göre q tane farklı çözüm vardır. Eğer r bir çözüm ve $r^k \equiv 1$ (mod p) yi gerçekleyen en küçük pozitif tam sayı k ise k | p dur. $r \not\equiv 1$ (mod p) ise k=q dur. Bununla beraber $1, r, r^2, \ldots, r^{q-1}$ bunların hepsi $x^q \equiv 1$ (mod p) denkleminin farklı çözümleridir.

Sonuç olarak $s \equiv r^t (\mathrm{mod}\, p)$ ve $1 \leq t \leq q-1$ şeklindeki t ler için $b_1 = b^t \in G$ ise $|b_1| = q$ dur.

G=< a , b_1 > olduğundan G deki her eleman $b_1^i a^j$ şeklinde yazılabilir. | a | = p ve $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$ böylece $b_1 a = a^s b_1$ dir. $G \to K$ eşleme $a \to c$ ve $b_1 \to d$ bir izomorfizmadır.

Sonuç 2.69 p asal sayı ve mertebesi 2p olan her grup ya devirli bir Z_{2p} grubuna ya da dihedral gruba izomorftur.

İspat. q=2 ve s$\equiv$-1 (mod p) ise G grubu devirli değildir. Bundan dolayı

G=< c , d > , |d| = 2, | c | = p ve dc=$c^{-1}d$ şeklindedir. Böylelikle $G \cong D_P$ elde edilir.

Önerme 2.70 Mertebesi 8 olan ve değişmeli olmayan iki farklı grup vardır. Bunlar quaternion grup Q_8 ve D_4 dür.

İspat. $D_4 \not\cong Q_8$ dir çünkü Q_8 de mertebesi iki olan eleman D_4 e göre daha fazladır. Mertebesi 8 olan ve değişmeli olmayan bir G grubu, mertebesi 8 olan eleman ve G deki birimden farklı her elemanın mertebesi 2 olan eleman içermeyebilir. Eğer içerirse G grubu değişmeli olur. Bundan dolayı G mertebesi 4 olan eleman içerir. Bu eleman a olsun. < a > nın G içindeki indeksi 2 olduğundan G de normaldir. $b \notin < a >$ ve $b^2 \in < a >$ seçelim.

$b^2 = a^2$ veya $b^2 = e$ olabilir. $< a > \lhd G$ normal olduğundan $bab^{-1} \in < a >$ şeklindedir. Buradan $bab^{-1} = a^3 = a^{-1}$ dir. Böylelikle biz G nin her elemanını $b^i a^i$ şeklinde yazabiliriz. Yani G=< a , b > şeklindedir.

Eğer |a| = 4 , $b^2 = a^2$, $ba = a^{-1}b$ şeklindedir ve bu da $G \cong Q_8$ olduğunu gösterir.

Diğer durumda | a | = 4 , | b | = 2 , ba = $a^{-1}b$ şeklinde ise de $G \cong D_4$ olduğunu gösterir.

Önerme 2.71 Değişmeli olmayan izomorfik olma koşuluyla mertebesi 12 olan üç tane grup vardır. Bunlar dihedral grup D_6, alterne grup A_4 ve a,b elemanları tarafından üretilen ve | a |= 6 , $b^2 = a^3$ ve $ba = a^{-1}b$ eşitliklerini gerçekleyen T grubudur.

İspat. D_6, A_4, T gruplarından herhangi iki tanesi izomorf değildir. G mertebesi 12 olan değişmeli olmayan grup olsun. | G | = $2^2 \cdot 3$ şeklindedir. P grubu G nin Sylow 3-alt grubu olsun. | P | = 3 ve $[G:P] = 4$ tür. $\varphi : G \to S_4$ dönüşümünün ve çekirdeği olan K grubu Lemma 2.39 dan P nin içine düşer.

K=P veya < e > dir. K= < e > ise φ bire-bir homomorfizmadır. Bu yüzden G $\cong$ A_4 olur.

K = P ve P , G nin tek Sylow 3-altgrubu ise P $\lhd$ G dir. Bu yüzden G mertebesi 3 olan sadece iki eleman içerir. Bunlardan birisi c olsun. c nin tüm eşleniklerinin mertebesi üç tür. $[G : C_G(c)]$=1 veya 2 dir. Bu yüzden $C_G(c)$ grubunun mertebesi 12 veya 6 dır. d $\in$ $C_G(c)$ ve mertebesi iki ise |cd| = 6 dır.

a = cd ve < a > $\lhd G$ olduğundan | G/< a > | = 2 dir. b $\in$ G ve b $\notin$ < a > olsun. b $\neq$ e, $b^2 \in <a>$ ve $bab^{-1} \in <a>$. G değişmeli değil ve |a|=6 ise $bab^{-1} = a^5 = a^{-1}$ tek seçenektir. Yani $ba = a^{-1}b$ olur. $b^2 \in <a>$ olduğundan $b^2 = a^2$ veya $b^2 = a^4$ olamaz. $b^2 = a$ veya $b^2 = a^5$ olması | b | = 12 olmasını ve dolayısıyla G nin değişmeli olmasını gerektirir.

Sonuç olarak;

| a | = 6 ; $b^2 = e$, ba=$a^{-1}b$ olduğundan G$\cong D_6$ dır.

| a | = 6 ; $b^2 = a^3$, $ba = a^{-1}b$ olduğundan G$\cong T$ dır.

3. YARIDİREK ÇARPIM

Tanım 3.1 H ve Q iki grup ve $\varphi : Q \to Aut(H)$ bir grup homomorfizması olsun. Elemanları $H \times Q$ da olan ve $(h,q)(h',q') = (h\varphi_q(h'), qq')$ ile tanımlanan yapıya H ve Q nun yarıdirek çarpımı denir ve $H \rtimes_\varphi Q$ ile gösterilir.

Lemma 3.2 $G = H \rtimes_\varphi Q$ olsun. G yukarıdaki ikili işlemle bir grup yapısıdır.

İspat. $[(a,x)(b,y)](c,z) = (a\varphi_x(b), xy)(c,z) = (a\varphi_x(b)\varphi_{xy}(c), xyz) =$
$(a,x)[(b,y)(c,z)] = (a,x)(b\varphi_y(c), yz) = (a\varphi_x(b\varphi_y(c)), xyz) = (a\varphi_x(b)\varphi_{xy}(c), xyz)$
olduğundan birleşme özelliği sağlanır.

$$(1_H, 1_Q)(a,x) = ((1_H)\varphi_{1_Q}(a), 1_Q\ x) = (a,x)\ (1_H, 1_Q)$$

olduğundan $(1_H, 1_Q)$ ikilisi G nin birim elemanıdır.

$$(\varphi_{x^{-1}}(a^{-1}), x^{-1})(a,x) = (\varphi_{x^{-1}}(a^{-1})\varphi_{x^{-1}}(a), x^{-1}x) = (\varphi_{x^{-1}}(a^{-1}a)1_Q) = (1_H, 1_Q)$$

olduğundan $(\varphi_{x^{-1}}(a^{-1}), x^{-1})$ ikilisi G nin ters elemanıdır.

G kümesi birleşme özelliği, birim eleman ve her elemanın tersi bulunabildiği için bir gruptur.

Lemma 3.3 $K \trianglelefteq G$ olsun. Eğer $G = KQ$, $K \cap Q = 1_G$ olacak şekilde Q altgrubu varsa G grubu K ve Q gruplarının yarıdirek çarpımı şeklinde yazılabilir. Yani $G = K \rtimes Q$ dir.

İspat.
$$\psi : K \to K \rtimes Q$$
$$k \mapsto (k, 1_Q)$$
$$\varphi : Q \to K \rtimes Q$$
$$q \mapsto (1_K, q)$$

şeklinde tanımlı fonksiyonlar birer monomorfizmalardır. Bu fonksiyonların görüntülerini K^* ve Q^* ile gösterirsek, $K \cong K^*$ ve $Q \cong Q^*$ eşitliklerini elde ederiz.

$$\pi : K \rtimes Q \to Q$$
$$(k, q) \mapsto q$$

ile tanımlı π fonksiyonu bir homomorfizmadır. Buna göre π homomorfizmasının çekirdeği,

$$Ker\pi = \{(k, q) \in K \rtimes Q \mid \text{her } x \in Q \text{ için } \pi(k, q) = q\}$$
$$= \{(k, 1_Q) \mid \text{her } k \in K\} = K$$

olur. Buradan $Ker\pi \trianglelefteq G$ yani $K \trianglelefteq G$ dır. $\forall (k, q) \in G$ için $(k, q) = (k, 1_Q)(1_K, q)$ dur. O halde $KQ = G$ dir ve $K \cap Q = (1_K, 1_Q)$ olur.

Lemma 3.4 G bir grup H ve Q da altgrupları olsunlar. $G = HQ$ ve $H \cap Q = 1_G$ ise $\forall g \in G$ için $g = hq, h \in H$ ve $q \in Q$ şeklinde tek türlü yazılabilir.

İspat. $G = HQ$ olsun. Bir $g \in G$ için $g = hq$ ve $g = h^{'}q^{'}$, $\forall h, h^{'} \in H$ ve $q, q^{'} \in Q$ olacak şekilde tek türlü yazılmasın. $hq = h^{'}q^{'}$ ve

$h^{'-1}h = q^{'}q \in H \cap Q = 1_G$ ise $h = h^{'}$ ve $q = q^{'}$ olduğundan $\forall g \in G$ için $g = hq$ yazımı tek türlü bellidir.

Lemma 3.5 S_n simetrik grubu A_n ile $\mathbb{Z}_2$ gruplarının semidirekt çarpımıdır.

İspat. $\left[S_n : A_n\right] = 2$ olduğundan $A_n \trianglelefteq S_n$ dir. Yani $S_n / A_n \cong <(12)>$

$Q = <(12)> \cong \mathbb{Z}_2, A_n \cap Q = \{id\}$ olduğundan $S_n = A_n \rtimes \mathbb{Z}_2$ dir.

Lemma 3.6 D_n dihedral grubu $\mathbb{Z}_n$ ile $\mathbb{Z}_2$ gruplarının semidirekt çarpımıdır.

İspat. $D_n = \{a, b \mid a^2 = b^n = 1, a^{-1}ba = b^{-1}\}$ dihedral grubu olsun. $\mathbb{Z}_n = <r>$ ve $\mathbb{Z}_2 = <s>$ olsun.

$$\theta : \mathbb{Z}_2 \rightarrow Aut(\mathbb{Z}_n)$$

$$s \mapsto \theta_s$$

$$\theta_s : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

$$r^i \mapsto r^{-i}$$

ile tanımlı θ fonksiyonu bir homomorfizmadır. Buradan

$D_n = <r> \rtimes_\theta <s> \cong \mathbb{Z}_n \rtimes_\theta \mathbb{Z}_2$ olur.

Lemma 3.7 Quaternion grup herhangi iki grubun semidirekt çarpımı şeklinde yazılamaz.

İspat. $Q_8 = \{<a, b> \mid a^4 = b^4 = 1, a^2 = b^2, bab^{-1} = a^3\}$ şeklinde quaternion grubu tanımlayalım. Üreteçler aşağıdaki gibi olsunlar. $a = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ ve $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$H = \{1, a^2\}$ kümesi Q_8 in iki elemanlı tek altgrubudur. $Q_8 / H = Q$ buradan da $|Q| = 4$ ve $H \cap Q \neq 1$ olduğundan her $Q < Q_8$ için $Q_8 \neq Q \rtimes H$ dir.

Lemma 3.8 p bir asal sayı olmak üzere mertebesi p^2 olan devirli bir grup herhangi iki grubun yarıdirek çarpımı şeklinde yazılamaz.

İspat. Mertebesi p^2 olan grubun mertebesi p olan sadece bir tek alt grubu vardır. O yüzden herhangi iki grubun yarıdirek çarpımı şeklinde yazılamaz.

Lemma 3.9 Hem S_3 hem de $\mathbb{Z}_6$ grupları farklı homomorfizmalar altında ve $\mathbb{Z}_2$ ve $\mathbb{Z}_3$ gruplarının yarıdirek çarpımı şeklinde yazılabilirler.

İspat. $\phi_1 : Z_2 \;\rightarrow\; Aut(Z_3) \cong Z_2$

$$x \mapsto -x$$

$$\phi_2 : Z_2 \;\rightarrow\; Aut(Z_3) \cong Z_2$$

$$x \mapsto x$$

Şeklinde verilen ϕ_1 ve ϕ_2 fonksiyonları birer homomorfizmadır. Buradan $S_3 = Z_3 \rtimes_{\phi_1} Z_2$.

ϕ_2 fonksiyonu aşikar homomorfizma olduğundan yarıdirek çarpım bir direkt çarpımdır. Yani $Z_6 = Z_3 \times Z_2$ dir.

Lemma 3.10 Mertebesi 12 olan grup Z_3 ve Z_4 gruplarının yarıdirek çarpımı şeklinde yazılabilir.

İspat. $Z_3 = \langle a \rangle$ ve $Z_4 = \langle x \rangle$ olsun.

$$\theta : \mathbb{Z}_4 \rightarrow Aut(\mathbb{Z}_3) \cong \mathbb{Z}_2$$

$$x \mapsto \theta_x$$

$$\theta_x : Z_3 \rightarrow Z_3$$

$$a \mapsto a^2$$

ile tanımlanan dönüşüm bir homomorfizmadır. Burada $\theta_x(a) = a^2$ ve $\theta_x(a^2) = a^4 = \mathrm{a}$, $\theta_{x^2}(a) = \theta_x\theta_x(\mathrm{a}) = \theta_x(a^2) = \mathrm{a}$ yani $x^2, \langle a \rangle$ üzerine trivial etki eder. Buradan $G = Z_3 \rtimes_\theta Z_4$ ayrýca $|G| =$ 12 dir. Şimdi G grubunun üreteçleri arasında nasıl bir bağlantı olduğunu gösterelim.

$s = (a^2, x^2)$ ve $t = (1, x)$ alalım. Buradan ;

$$s^2 = (a^2, x^2)(a^2, x^2) = (a^2\theta_x^2(a^2), x^4) = (a,1)$$
$$s^3 = (a^2, x^2)(a,1) = (a^2\theta_x^2(a^2), x^2) = (1, x^2)$$

$s^6 = (1, x^2)(1, x^2) = (1,1)$ olduğundan $|s| = 6$ dır.

$$t^2 = (1,x)(1,x) = (1,x^2) = s^3$$

$$st = (a^2, x^2)(1,x) = (a^2\theta_x^2(1), x^3) = (a^2, x^2)$$

$(st)^2 = (a^2, x^3)(a^2, x^3) = (a^2\theta_x^3(a^2), x^2) = (1, x^2)$ buradan da

$G = Z_3 \rtimes Z_4 = \{< s,t > | s^6 = 1, t^2 = s^2 = (st)^2\}$ şeklindedir.

Lemma 3.11 p tek bir asal sayı olmak üzere $K = |< a >| = p^2$ ve $Q = |< a >| = p$ şeklinde devirli gruplar verilsin. $Aut(K) \cong \mathbb{Z}_p(p-1) \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_p$ dir.

$$\theta \ : \ Q \ \rightarrow \ Aut(K)$$
$$x \ \mapsto \ \theta_x$$
$$\theta_x \ : \ K \ \rightarrow \ K$$
$$a \ \mapsto \ a^{1+p}$$

dönüşümü bir homomorfizmadır.

$$\alpha \ : \ K \ \rightarrow \ K$$
$$a \ \mapsto \ a^{1+p}$$

$\mathbb{Z}_p = < \alpha >$ yani buradan Aut(K) mertebesi p olan bir eleman içerir. $\theta_x = \alpha$ alırsak, G=K $\rtimes Q$ dur ve $|G| = p^3$ dür. G grubu x ve a tarafından üretilir. Burada $x^p = 1, a^{p^2} = 1, xpx^{-1} = \theta_x(a) = a^{1+p}$ dir. Ayrıca G grubu değişmeli değildir.

Lemma 3.12 p bir asal sayı olmak üzere, K=<a,b> ile üretilen mertebesi p^2 olan elemanter değişmeli bir p grup olsun. Yani ;
$|<a>| = p, |<b>| = p \; ve \; Q = |<x>| = p$ olsun.
$Aut(K) \cong |GL(2,p)| = (p^2-1)(p^2-p)$

$$\theta \;:\; Q \;\to\; Aut(K)$$

$$x \;\mapsto\; \theta_x$$

$$\theta_x \;:\; K \;\to\; K$$

$$a \;\mapsto\; ab$$

$$b \;\mapsto\; b$$

Aut(K) mertebesi p olan bir eleman içerir.

$$\theta_x(a) = xax^{-1} = ab, \theta_x(b) = xbx^{-1} = b$$

$$xax^{-1} = ab \Rightarrow a^{-1}x^{-1}ax = b \Rightarrow [x,a] = b$$

$$b = xax^{-1}a^{-1} = b = aba^{-1} \Rightarrow aba^{-1}b^{-1} = 1 \Rightarrow [b,a] = 1$$

$$xbx^{-1} = b \Rightarrow xbx^{-1}b^{-1} = 1 \Rightarrow [b,x] = 1$$

G grubu yukarıdaki bağıntılarla üretilen değişmeli olmayan bir gruptur. Ayrıca G=K $\rtimes_\theta Q$ ve $|G| = p^3$ olacak şekilde belirtebiliriz.

Lemma 3.13 $G = GL_n(\mathbb{F})$ olsun. B de G içinde üst üçgensel matrislerden oluşan bir alt grubu olsun. T de G nin köşegen matrislerinden oluşan bir alt grubu olsun. U da G nin köşegenleri 1 olan üst üçgensel matrislerden oluşan bir alt grubu olsun. Buradan B=U $\rtimes$T dır.

İspat. $\varphi : \quad B \quad \to \quad T$

$$\begin{pmatrix} b_{11} & * \\ 0 & * \end{pmatrix} \mapsto \begin{pmatrix} b_{11} & 0 \\ 0 & b_{22} \end{pmatrix}$$

ile tanımlı φ dönüşümü bir homomorfizmadır. Buna göre φ homomorfizmanın çekirdeği,

$$\text{Ker } \varphi = \left\{ \begin{pmatrix} b_{11} & * \\ 0 & * \end{pmatrix} \middle| \begin{pmatrix} b_{11} & 0 \\ 0 & b_{22} \end{pmatrix} = I \right\} = U$$

olur. Buradan Ker $\varphi \trianglelefteq B$ ve $U \trianglelefteq B$ dir. Ayrıca I.İzomorfizma teoreminden $B / \text{Ker}\varphi \cong T$ ve $U \cap T = I$ olduğundan $B = U \rtimes T$ olur.

3.1 Wreath Çarpım

Şimdi iki grup verildiğinde grupların yarıdirek çarpım yardımıyla Wreath çarpım grubunu tanımlayalım.

Lemma 3.14 A ve B iki grup ve $K = A^{[B]} = \{ f \mid f : B \to A, f \text{ fonksiyon} \}$ olsun. K kümesi $f_1, f_2 \in K$ ve $x \in B$ için $(f_1.f_2)(x) = f_1(x) \cdot f_2(x)$ işlemiyle bir gruptur.

İspat. $(f_1, f_2) = (g_1, g_2)$ olsun. Sıralı ikililerin eşitliğinden $f_1 = g_1$ ve $f_2 = g_2$

olsun. Buradan $\forall x \in B$ için $f_1(x) = g_1(x)$ ve $f_2(x) = g_2(x)$ olur. Böylece $(f_1 f_2)(x) = f_1(x) \cdot f_2(x) = g_1 \cdot g_2(x) = (g_1 g_2)(x)$ olduğundan iyi tanımlılık sağlanır. $\forall x \in B$ ve $\forall f, g, h \in K$ için
$[f(gh)](x) = f(x) \cdot (gh)(x) = f(x) \cdot [g(x) \cdot h(x)] = [f(x) \cdot g(x)] h(x)$
$= (fg)(x) \cdot h(x) = [(fg)h](x)$ olduğundan birleşme özelliği sağlanır.

$1_K : B \to A, 1_K(x) = 1_A$ fonksiyonu için $1_K f(x) = 1_K(x) \cdot f(x) = 1_A \cdot f(x) =$

$f(x) = f(x) \cdot 1_K(x)$ olduğundan 1_K , B den A ya tanımlanan birim fonksiyondur. Son olarak B den A ya tanımlanan herhangi bir f fonksiyonun tersini de $f^{-1}(x) = (f(x))^{-1}$ şeklinde ifade edebiliriz. Böylece K kümesi bir grup olmuş olur.

Lemma 3.15 B grubu K kümesi üzerine aşağıdaki işlemle etki eder.

İspat. B grubunun K kümesi üzerine etkisini tanımlayalım. $b\in B$ için $K\times B\to K,\ \ (f,b)\to f^{b},\ f^{b}(x)=f(xb^{-1})$ şeklinde tanımlanan işlem ile B grubu K kümesine etki eder. Gerçekten de;

i-) $f^{b_1b_2}(x)=f(x(b_1b_2)^{-1})=f(xb_2^{-1}b_1^{-1})=f^{b_1}(xb_2^{-1})=(f^{b_1})^{b_2}(x)$

Buradan; $f^{b_1b_2}=(f^{b_1})^{b_2}$ olur.

ii-) $f^{1_B}(x)=f(x1_B)=f(x)$ olur. Böylece;

θ : B $\to$ Aut(K)

b $\mapsto$ θ_b

θ_b : K $\to$ K

f $\mapsto$ f^{b}

olacak şekilde bir θ homomorfizması vardır.

Lemma 3.16 A ile B gruplarının Wreath çarpımı K ile B nin θ ile tanımlanan homomorfizma altında semi direkt çarpımıdır. Yani;

$W:=A^{[B]}\rtimes$B=K$\rtimes$B=$\{(f,b)|\ f\in K,b\in B\}$ kümesi
$(f_1,b_1)(f_2,b_2)=(f_1f_2^{b_1^{-1}},b_1b_2)$ işlemiyle bir gruptur.

İspat. Verilen herhangi $f_1,f_2,f_3,f_4\in K$ ve $b_1,b_2,b_3,b_4,x\in B$ için;

$((f_1,b_1),(f_2,b_2))=((f_3,b_3),(f_4,b_4))$

$\Rightarrow(f_1,b_1)=(f_3,b_3),(f_2,b_2)=(f_4,b_4)$

$\Rightarrow f_1=f_3,f_2=f_4,b_1=b_3,b_2=b_4$

$\Rightarrow f_1f_2^{b_1^{-1}}(x)=f_1(x)f_2^{b_1^{-1}}(x)=f_1(x)f_2(xb_1)=f_3(x)f_4(xb_3)=f_3(x)f_4^{b_3^{-1}}(x)$ ve $b_1b_2=b_3b_4$ olduğundan $(f_1f_2^{b_1^{-1}},b_1b_2)=(f_3f_4^{b_3^{-1}},b_3b_4)$

eşitliği sağlanır. Bu ise tanımdan, $(f_1,b_1)(f_2,b_2)=(f_3,b_3)(f_4,b_4)$

olmasını gerektirir. Böylece iyi tanımlılık gösterilmiş olur.

G1) $(f_1,f_2)^b(x)=(f_1f_2)(xb^{-1})=f_1(xb^{-1})f_2(xb^{-1})=f_1^b(x)f_2^b(x)=f_1^b f_2^b(x)$

Buradan, $(f_1,f_2)^b(x)=f_1^b f_2^b(x)$ olur.

$$\left[(f_1,b_1),(f_2,b_2)\right](f_3,b_3)=(f_1f_2^{b_1^{-1}},b_1b_2)(f_3,b_3)=(f_1f_2^{b_1^{-1}}f_3^{(b_1b_2)^{-1}},(b_1b_2)b_3)=$$

$$(f_1f_2^{b_1^{-1}}f_3^{b_2^{-1}b_1^{-1}},b_1b_2b_3)=(f_1(f_2f_3^{b_2^{-1}})^{b_1^{-1}},b_1(b_2b_3))=(f_1,b_1)(f_2f_3^{b_2^{-1}},b_2b_3)=$$

$(f_1 b_1)[(f_2 b_2)(f_3 b_3)]$ olduğundan birleşme özelliği sağlanır.

G2) Verilen her $(f,b)\in W$ için $(f,b)(1_K,1_B)=(1_K,1_B)(f,b)=(f,b)$

olduğundan $(1_K,1_B)$, W nin elemanıdır.

G3) Verilen herhangi bir $(f,b)\in W$ için;

$$(f,b)((f^{-1})^b,b^{-1})=(f((f^{-1})^b)^{b^{-1}},bb^{-1})=(f(f^{-1})^{bb^{-1}},1_B)=(1_K,1_B)$$

$$((f^{-1})^b,b^{-1})(f,b)=((f^{-1})^b f^b,b^{-1}b)=((f^{-1}f)^b,1_B)=(1_K^b,1_B)=(1_K,1_B)$$

olduğundan $(f,b)^{-1}=((f^{-1})^b,b^{-1})$ dir. O halde W kümesi verilen ikili işlemle bir gruptur.

Lemma 3.18 Verilen her $f,g\in K$ ve $b\in B$ için;

i) $(1_K,b)^{-1}(f,1_B)(1_K,b)=(f^b,1_B)$

ii) $(f,b)=(g,1_B)(f,b)^{-1}=(fg^{b^{-1}}\ f^1,1_B)$ olur.

İspat.

i) $(1_K,b)^{-1}(f,1_B)(1_K,b)=((1_K^{-1})^b,b^{-1})(f1_K^{1_B},1_Bb)=(1_K,b^{-1})(f,b)=(f^b,1_B)$

ii) $(f,b)(g,1_B)(f,b)^{-1}=(f,b)(g,1_B)((f^{-1})^b,b^{-1})=(f,b)(g(f^{-1})^{b1_B},b^{-1})$

$(f(g(f^{-1})^{b})^{b^{-1}}, 1_B) = (f g^{b^{-1}} f^{1}, 1_B)$

Şimdi $K^* := \{(f, 1_B) \mid f \in K\} \subseteq W$ ve $B^* := \{(1_K, b) \mid b \in B\} \subseteq W$ kümelerini tanımlayalım. Burada $B^* \leq W$ ve Lemma 3.18 (ii) den $K^* \trianglelefteq W$ dır.

Ayrıca $B^* \cap K^* = \{(1_K, 1_B)\}$ ve $W = K^* B^*$ olduğundan W K ile B nin semidirekt çarpımı olur. Yani $W = K^* \rtimes B^*$ şeklinde yazılır.

Bu tanımlar gereği $w \in W$ için $w = fb$ olacak şekilde teklikle belli $f \in K$ ve $b \in B$ vardır. B grubunun $A^{[B]} = K$ kümesi üzerine etkisini f nin eşleniği olarak lemma (i) den $b^{-1} f b = f^{b}$ olarak yazılabilir, çarpmayı da $(fb)(gb_1) = f(bgb^{-1})bb_1 = fg^{b^{-1}}bb_1$ olacak şekilde tanımlayabiliriz.

Tanım 3.19 W ya A ile B gruplarının Wreath çarpım grubu denir. W=AWrB şeklinde gösterilir. Burada B ye Wreath çarpım grubunun üst grubu, $A^{[B]}$ ye Wreath çarpım grubunun temel grubu denir.

Sonuç 3.20 Mertebesi 2 olan grupları $\mathbb{Z}_2$ ile gösterelim. $\mathrm{W} = \mathbb{Z}_2 \mathrm{Wr} \mathbb{Z}_2$

grubunu oluşturmaya çalışalım.

İspat. Mertebesi 2 olan grup $\mathbb{Z}_2 = \{1, a\}$ ve $\mathbb{Z}_2$ den $\mathbb{Z}_2$ ye tanımlanan fonksiyonların kümesi,

$$K = \mathbb{Z}_2^{\mathbb{Z}_2} = \{f_1 = \begin{pmatrix} 1 & a \\ 1 & 1 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & a \\ a & a \end{pmatrix},$$
$$f_3 = \begin{pmatrix} 1 & a \\ 1 & a \end{pmatrix}, f_4 = \begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix}\}$$

olsun. $f_2 f_3 = \begin{pmatrix} 1 & a \\ a & a \end{pmatrix}\begin{pmatrix} 1 & a \\ 1 & a \end{pmatrix} = \begin{pmatrix} 1 & a \\ a & a^2 \end{pmatrix} = \begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix} = f_4$

Benzer şekilde $f_1 f_1 = f_2 f_2 = f_3 f_3 = f_4 f_4 = f_1, f_2 f_4 = f_3, f_3 f_4 = f_2, f_3 f_2 = f_4$ olur. $W = \{(f_1, b), (f_2, a), (f_3, a), (f_4, a), (f_1, 1), (f_2, 1), (f_3, 1), (f_4, 1)\}$

$= \{f_1 a, f_2 a, f_3 a, f_4 a, f_1 1, f_2 1, f_3 1, f_4 1,\}$

$f, g \in \mathbb{Z}_2^{\mathbb{Z}_2}$ ve $b \in \mathbb{Z}_2$ için $(fb)(gb_1) = f(bgb^{-1})bb_1 = fg^{b^{-1}}bb_1$

işlemiyle bir gruptur. Bu grup $\mathbb{Z}_2$ ile $\mathbb{Z}_2$ nin Wreath çarpımıdır.

Ayrıca $f^b(x) = f(xb^{-1})$ için $f_1^a(1) = f_1(1a) = 1$ ve $f_1^a(a) = f_1(aa) = 1$

olduğundan $f_1^a = f_1$ dir. Benzer şekilde, $f_2^a = f_2, f_3^a = f_4, f_4^a = f_3$ olur.

$x = f_1 a$ ve $y = f_3 a$ için;

$x^2 = (f_1 a)^2 = (f_1^a)(f_1^a) = f_1 f_1^a 1 = f_1 1 = 1$ dir.

$y^2 = (f_3 a)^2 = (f_3 a)(f_3 a) = f_3 f_3^a 1 = f_3 f_4 1 = f_2 1$

$y^3 = (f_3 a)^3 = (f_3 a)(f_2 1) = f_3 f_2^a a = f_4 a$

$y^4 = (f_3 a)^4 = (f_3 a)(f_4 a) = f_3 f_4^a 1 = f_3 f_3 1 = f_1(1) = 1,\ xy = (f_1 a)(f_3 a) = f_1 f_3^a 1$

$= f_1 f_4 1 = f_4 1 y^{-1} x = (f_3^a)^{-1}(f_1 a) = ((f_3^{-1})^a a^{-1}) = (f_3^a a)(f_1 a) = (f_4 a)(f_1 a) =$

$f_4 f_1^a 1 = f_4 f_1 1 = f_4 1$

Böylece, $x^2 = y^4 = 1,\ \ xy = y^{-1}x$ koşullarını sağladığından $W \cong D_8$ olur.

4. GENEL LİNEER GRUPLARDA SYLOW P-ALTGRUPLARININ BULUNMASI

p , 2 den farklı bir asal sayı olsun. Amacımız $|GL_n(\mathbb{F}_q)|$ nun mertebesini bölen p asal sayısının en büyük kuvvetini aramak olacaktır. Buradaki bulacağımız p nin kuvveti bizim için $|GL_n(\mathbb{F}_q)|$ nun p-sylow altgruplarının mertebesi olacaktır. $GL_n(\mathbb{F}_q)$ nun mertebesi ;

$$|GL_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i-1)$$

dir. Eğer $p|q$ ise p-sylow altgruplarının mertebesi $q^{\frac{n(n-1)}{2}}$ dir. Bu durumda p-sylow altgruplardan bir tanesi köşegeni bir olan n × n lik üst üçgensel matrislerden oluşur. Bu altgrubu aşağıdaki gibi görebiliriz.

$$\mathbf{Q} = \left\{ \begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \,\middle|\, * \in \mathbb{F}_q \right\}$$

şeklindedir. Açıkça görülebileceği gibi Q grubunun mertebesi $|Q| = 1 \cdot q \cdot q^2 \cdot q^3 \cdots q^{n-1} = q^{\frac{n(n-1)}{2}}$ kadardır.

Eğer p bölmez q ise iki durum vardır. Ya p-sylow altgrup yoktur ya da $p | \prod_{i=1}^{n}\left(q^i-1\right)$ dir. Doğal olarak biz burada ikinci durumla ilgileneceğiz. k modulo-p ye göre q nun çarpımsal mertebesi olsun. Yani $q^a \equiv 1$ (mod p) için $k|a$ dır. İkinci durum gereği bazı $i \in [1,n]$ için $p | (q^i-1)$ olsun. Buradan $k \le n$ dir.

$\ell = \left[\dfrac{n}{k}\right]$ alırsak, $q^a \equiv 1(\text{mod p})$ gereği $(q^k-1)\,(q^{2k}-1)\ldots(q^{\ell k}-1)$ şeklinde yazılan çarpanlar p asal sayısına bölünürler.

Bazı $r,s \in \mathbb{N}$ için $q^k = 1 + p^r s$ öyle ki p bölmez s olsun. Buradan;

$$(q^k-1) = p^r s$$
$$(q^{2k}-1) = (1+p^r s)^2 - 1 = 2p^r s + p^{2r}s^2 = p^r(2s + p^r s^2)$$
$$\vdots$$
$$(q^{\ell k}-1) = (1+p^r s)^{\ell} - 1 = \sum_{i=1}^{\ell}\binom{\ell}{i}\left(p^{ri}s^i\right) = p^r\sum_{i=1}^{\ell}\binom{\ell}{i}p^{r(i-1)}s^i$$

eşitliklerini taraf tarafa çarparsak;

$$\prod_{j=1}^{\ell}\left(q^{jk}-1\right) = p^{r\ell}\prod_{j=1}^{\ell}\left(\sum_{i=1}^{j}\binom{j}{i}\left(p^{r(i-1)}s^i\right)\right)$$ eşitliği elde edilir.

Bu eşitlikten de görüldüğü gibi p-sylow altgrupları en az $p^{r\ell}$ tane elemana sahiptir. Ancak biz bunun $p^{r\ell}$ den daha fazla olduğunu göstereceğiz.

Şimdi bu bölümde çok fazla kullanacağımız valuation kavramıyla alakalı tanım ve özellik verelim.

val(N)$\in \mathbb{N}$ olsun. N= $p^{val(N)} \cdot a$ olacak şekilde p bölmez $a \in \mathbb{N}$ vardır. Ayrıca $a,b \in \mathbb{N}$ olmak üzere $val(a \cdot b) = val(a) + val(b)$ dir. Şimdi de

$$val\left(\sum_{i=1}^{j}\binom{j}{i}\left(p^{r(i-1)}s^i\right)\right) = val(j) \quad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

eşitliğini kabul edelim.

$$val(|GL_n(\mathbb{F}_q)|) = val\left(\prod_{j=1}^{\ell}(q^{jk-1})\right) = val\left(p^{r\ell}\prod_{j=1}^{\ell}\left(\sum_{i=1}^{j}\binom{j}{i}\left(p^{r(i-1)}s^i\right)\right)\right)$$

$$= val(p^{r\ell}) + val(\prod_{j=1}^{\ell}(\sum_{i=1}^{j}\binom{j}{i}(p^{r(i-1)}s^i)))$$

$$= \ell r + \sum_{j=1}^{\ell} val(\sum_{i=1}^{j}\binom{j}{i}(p^{r(i-1)}s^i)) = \ell r + \sum_{j=1}^{\ell} val(j)$$

$$= \ell r + val(1) + val(2) + \ldots + val(\ell) = \ell r + val(1\cdot 2\ldots \ell) = \ell r + val(\ell !)$$

Sonuç olarak; $val(|GL_n(\mathbb{F}_q)|) = \ell r + val(\ell !)$ eşitliğini elde ederiz.

Şimdi de binom açılımından gelecek p asal sayısının kuvvetini bulalım.

p bölmez q $\Rightarrow val(\sum_{i=1}^{j}\binom{j}{i}(p^{r(i-1)}s^i)) = val(j)$

eşitliğinin gerçeklendiğini gösterelim.

$$val(\sum_{i=1}^{j}\binom{j}{i}(p^{r(i-1)}s^i)) = val(\binom{j}{1}p^0 s + \binom{j}{2}p^r s^2 + \binom{j}{3}p^{2r}s^3 \ldots + \binom{j}{j}p^{r(j-1)}s^j)$$

$$= val(j\,s + \binom{j}{2}p^r s^2 + \binom{j}{3}p^{2r}s^3 \ldots + \binom{j}{j}p^{r(j-1)}s^j)$$

O zaman $\forall i \in (1, j]$ için $val(j) < val(\binom{j}{i}p^{r(i-1)}s^i)$ olduğunu gösterirsek ispatımız tamamlanmış olur.

Eğer $val(j) < val(\binom{j}{i}) + val(p^{r(i-1)}) + val(s^i) = val(\binom{j}{i}) + r(i-1)$ öyle ki $i-1 \le r(i-1)$ olduğundan $val(j) < val(\binom{j}{i}) + i - 1$ eşitsizliğini göstermek ispatımızı tamamlamaya yeterli olacaktır.

Hipotezimizi i üzerinden tümevarımla kanıtlayacağız.

İlk olarak p bölmez j ise $val(j) < val(\binom{j}{i}) + i - 1$ dir. O halde $p \mid j$ olsun. $i = 2$ için tümevarımımızı başlatalım.

$$val(j) \overset{?}{<} val(\tbinom{j}{2}) + i - 1$$

$$\Leftrightarrow val(j) < val(\frac{j(j-1)}{2!}) + 1$$

$$\Leftrightarrow val(j) < val(j) + \underbrace{val(j-1) - val}_{0}(2) + 1$$

$\Leftrightarrow 0 < 1 - val(2)$ ve $p \neq 2$ olduğundan $val(2) = 0$ dır. O halde $0 < 1$ olur yani $i = 2$ için hipotezimiz doğru olur.

Şimdi de i için hipotezimiz doğru olsun $i+1$ için doğru olacağını görelim.

$$val(j) < val((\tbinom{j}{i})) + (i-1) = val(j!) - val((j-i)!) - val(i!) + (i-1)$$

$$\Leftrightarrow val(j) < val(j!) - val((j-i)!) - val(i!) + (i-1)$$

$$\Leftrightarrow val(j) < val(j) + val((j-1)!) - val((j-i)!) - val(i!) + (i-1)$$

$$\Leftrightarrow 0 < val((j-1)!) - val((j-i)!) - val(i!) + (i-1) \text{..........................}(*)$$

bizim göstermek istediğimiz eşitsizliğin $i+1$ için doğru olacağıdır. Yani;

$$val(j) \overset{?}{<} val((\tbinom{j}{i+1})) + i = val(j!) + val((j-i-1)!) - val((i+1)!) + i$$

$$\Leftrightarrow 0 \overset{?}{<} val((j-1)!) - val((j-i-1)!) - val((i+1)!) + i \text{......................}(**)$$

Eğer; $val((j-i)) - val((i+1)) + 1 \geq 0$ ise bu ifadeyi $(*)$ eşitliğine eklediğimiz zaman $(**)$ eşitliğini elde ederiz. Yani;

$$0 < val((j-1)!) - val((j-i)!) - val(i!) + (i-1) + val((j-i)) - val((i+1)) + 1$$

$0 < val((j-1)!) - val((j-i-1)!) - val((i+1)!) + i$ olur. Yani $(**)$ eşitlik sağlanmış olur.

Kabul edelim ki; $val((j-i)) - val((i+1)) + 1 < 0$ olsun. Bu eşitsizlik ancak, $i \equiv -1 \pmod p$ olması durumunda sağlanır. Eğer ;

$$\left| val((j-i)) - val((i+1)+1) \right|$$
$$< val((j-1)!) - val((j-i)!) - val(i!) + (i-1) \text{..............}(2)$$

olduğunu gösterirsek $val((j-1))-val((i+1))+1$ ifadesini $(*)$ ın sağ tarafına eklersek $(**)$ ın doğruluğunu göstermiş oluruz.

$i \equiv -1 \pmod p$ ve p | j olduğunda $\left|val((j-i))-val((i+1))+1\right| = val(i+1)-1$

ifadesi gerçeklenir.

$$val(j!) = \sum_{n=1}^{\infty} \left\lfloor \frac{j}{p^n} \right\rfloor$$

$$val(i+1)-1 \overset{?}{<} val((j-1)!)-val((j-i)!)-val(i!)+(i-1)$$

$$val(i+1) < \sum_{n=1}^{\infty} \left\lfloor \frac{j-1}{p^n} \right\rfloor - \sum_{n=1}^{\infty} \left\lfloor \frac{j-i}{p^n} \right\rfloor - \sum_{n=1}^{\infty} \left\lfloor \frac{i}{p^n} \right\rfloor + i$$

$$val(i+1) < \sum_{n=1}^{\infty} (\left\lfloor \frac{j-1}{p^n} \right\rfloor - \left\lfloor \frac{j-i}{p^n} \right\rfloor - \left\lfloor \frac{i}{p^n} \right\rfloor) + i$$

$$x \geq y \Rightarrow \left\lfloor \frac{x-y}{a} \right\rfloor \leq \left\lfloor \frac{x}{a} \right\rfloor - \left\lfloor \frac{y}{a} \right\rfloor$$

Yukarıda ki eşitliği; $j-1 \geq j-i$ için $\left\lfloor \frac{i-1}{p^n} \right\rfloor \leq \left\lfloor \frac{j-1}{p^n} \right\rfloor - \left\lfloor \frac{j-i}{p^n} \right\rfloor$ olacak şekilde uygulayabiliriz. Bu sonucu kullanarak;

$$\sum_{n=1}^{\infty} (\left\lfloor \frac{i-1}{p^n} \right\rfloor - \left\lfloor \frac{i}{p^n} \right\rfloor) + i \leq \sum_{n=1}^{\infty} (\left\lfloor \frac{j-1}{p^n} \right\rfloor - \left\lfloor \frac{j-i}{p^n} \right\rfloor - \left\lfloor \frac{i}{p^n} \right\rfloor) + i$$

$i \equiv -1 \pmod p$ olduğundan $\left\lfloor \frac{i-1}{p^n} \right\rfloor = \left\lfloor \frac{i}{p^n} \right\rfloor$ dir. O halde

$\sum_{n=1}^{\infty} (\left\lfloor \frac{i-1}{p^n} \right\rfloor - \left\lfloor \frac{i}{p^n} \right\rfloor) = 0$ ve $\forall i \in (1, j]$ için $val(i+1) < i$ dir.

$$val(i+1) < i \leq \sum_{n=1}^{\infty} (\left\lfloor \frac{j-1}{p^n} \right\rfloor - \left\lfloor \frac{j-i}{p^n} \right\rfloor - \left\lfloor \frac{i}{p^n} \right\rfloor) + i$$

$$\Leftrightarrow val(i+1) < \sum_{n=1}^{\infty}\left(\left\lfloor \frac{j-1}{p^n} \right\rfloor - \left\lfloor \frac{j-i}{p^n} \right\rfloor - \left\lfloor \frac{i}{p^n} \right\rfloor\right) + i$$

Böylece (2) numaralı eşitsizlik ispatlanmış olur. Oradan da $(**)$ ispatlanır ve sonuç olarak (1) numaralı kabulümüzü ispatlamış oluruz.

5. SİMETRİK GRUPLARIN SYLOW P-ALTGRUPLARI

p bir asal sayı olmak üzere, $Sym(n)$ nin p-sylow alt gruplarını n üzerinden tümevarımla göstereceğiz.

$n=1$ için trivial.

Şimdi n den küçük bütün doğal sayılar için $Sym(n)$ nin tüm p-sylow alt gruplarını biliyor kabul edelim. n için bulunabileceğini gösterelim.

p bölmez n için $val(n!) = val(n) + val((n-1)!) = val((n-1)!)$ olduğundan $Sym(n)$ nin p-sylow alt gruplarıyla $Sym(n-1)$ in p-sylow alt grupları aynı kardinaliteye sahiptir.

$Sym(n-1) \leq Sym(n)$ olduğundan ve $Sym(n-1)$ in p-sylow alt gruplarını tümevarımla bildiğimiz için $Sym(n)$ nin de p-sylow alt gruplarını biliyoruz.

Şimdi de $p \mid n$ olsun. Buradan $n = kp$ olacak şekilde $k \in \mathbb{N}$ vardır.

$$val(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots = k + \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \ldots = k + val(k!)$$

$\forall i \in [1,k]$ için $\sigma_i = ((i-1)p+1, \ldots, ip)$ olacak şekilde bir permütasyon tanımlayalım. Buradan;

$$\sigma_1 = (1, \ldots, p)$$

$$\sigma_2 = (p+1, \ldots, 2p)$$

$$\vdots$$

$$\sigma_k = ((k-1)p+1, \ldots, n)$$

Burada tanımladığımız permütasyonların mertebeleri p dir. Yani $\forall i \in [1,k]$ için $|\sigma_i| = p$ dir.

G_i grubu σ_i ler tarafından üretilen ve mertebesi p asal sayısı olan grup olarak tanımlayalım. Yani $G_i = <\sigma_i>, |G_i| = p$ ve $G_i \cap G_j = \{id\}$ dir.

$<\sigma_1, \sigma_2, \ldots, \sigma_k>$ değişmeli bir gruptur. Ayrıca değişmeli grubun her alt grubu normal olduğundan $G_i \trianglelefteq <\sigma_1, \sigma_2, \ldots, \sigma_k>$ dir. O halde

$G_1 \oplus G_2 \oplus \ldots \oplus G_k = <\sigma_1, \sigma_2, \ldots, \sigma_k> \leq Sym(n)$ şeklinde yazabiliriz. Ayrıca;

$|G_1 \oplus G_2 \oplus \ldots \oplus G_k| = p^k$ dir.

Şimdi de $Sym(k)$ nın $Sym(n)$ üzerine etkisini gösterelim.

$$\begin{aligned} \varphi : \quad & Sym(k) \to Sym(n) \\ & \sigma \mapsto \varphi_\sigma \end{aligned}$$

$$\begin{aligned} \varphi_\sigma \quad : \quad \{1, \ldots, n\} \quad & \to \quad \{1, \ldots, n\} \\ ip \quad & \mapsto \quad \sigma(i)p \\ ip - \ell \quad & \mapsto \quad \sigma(i)p - \ell \end{aligned}$$

$i \in [1, k]$ ve $\ell \in [1, p)$ olmak üzere yukarıdaki gibi tanımlansın φ dönüşümünün bir grup homomorfizması olduğunu gösterelim.

$\forall \sigma, \tau \in Sym(k)$ olmak üzere; ve

$$\varphi_{(\sigma\tau)}(ip) = ((\sigma\tau)(i))p = \varphi_\sigma(\tau(i)p) = \varphi_\sigma(\varphi_\tau(ip))$$

$$\varphi_{(\sigma\tau)}(ip - \ell) = \sigma(\tau(i))p - \ell = \varphi_\sigma(\tau(i)p) - \ell = \varphi_\sigma(\tau(i)p - \ell) = \varphi_\sigma(\varphi_\tau(ip - \ell))$$

olduğundan φ dönüşümünün bir grup homomorfizmasıdır. Buna göre φ homomorfizmasının çekirdeği,

$$Ker\varphi \;=\; \{\sigma \in Sym(k) \;|\forall\, i \in [1, k] \text{ için } \varphi_\sigma(ip) = ip\}$$

$$= \{\sigma \in Sym(k) \mid \forall i \in [1, k], \sigma(i) = i\} = \{id\}$$

olduğundan φ dönüşümü bir 1-1 homomorfizmadır. Ayrıca φ dönüşümü örten değildir. O halde, 1. izomorfizma teoremine göre;

$$Sym(k)/Ker\varphi \cong \varphi(Sym(k))$$

$$Sym(k) \cong \{\sigma \mid \forall i \in [1, k], \sigma(ip) = \sigma(i)p \text{ ve } \sigma(ip - \ell) = \sigma(ip) - \ell, \forall \ell \in [1, p)\}$$

Şeklinde ifade edebiliriz. Ayrıca;

$(\mathbb{Z}/p\mathbb{Z})^k \cong <\sigma(1),\ldots,\sigma(k)> = <\sigma(1)> \oplus \ldots \oplus <\sigma(k)> = G_1 \oplus \ldots \oplus G_k$ dir.

$Sym(n)$ nin p-sylow altgrubu;

$\bigoplus_{i=1}^{k} G_i \rtimes Sylow(\varphi(Sym(k))) \cong \bigoplus_{i=1}^{k} (\mathbb{Z}/p\mathbb{Z})^i \rtimes Sylow(Sym(k))$ formundadır.

Örnek 5.1 Yukarıdaki tanımladığımız yapı ile $Sym(4)$ ün 2-sylow alt gruplarını bulalım.

İspat. $n = 4,\ p = 2,\ k = 2$ ve $\ell = 1$ için $\forall i \in [1,2]$ için $\sigma_i = ((i-1)p+1,\ldots,ip)$

olacak şekilde tanımlanan permütasyonlar $\sigma_1 = (12),\ \sigma_2 = (34)$ şeklinde yazılabilen 2-devirlerdir. Bu devirlerin ürettikleri gruplar;

$\langle \sigma_1 \rangle = \{I, (12)\}$ ve $\langle \sigma_2 \rangle = \{I, (34)\}$ şeklindedir. Ayrıca σ_1 ve σ_2 permütasyonlarının birlikte ürettikleri grup;

$\langle \sigma_1, \sigma_2 \rangle = \{I, (12), (34), (12)(34)\}$ şeklindedir.

Şimdi $Sym(2)$ nin $Sym(4)$ üzerine etkisini tanımlayıp $Sym(2)$ nin 2-sylow altgruplarının yapısını oluşturalım.

$$\begin{aligned} \varphi : Sym(2) &\to Sym(4) \\ \sigma &\mapsto \varphi_\sigma : \{1,2,3,4\} \to \{1,2,3,4\} \end{aligned}$$

$2i \quad \mapsto \quad \sigma(\mathrm{i})2$

$2i-1 \quad \mapsto \quad \sigma(i)2\text{ - }1$

Yukarıdaki gibi tanımlanan φ dönüşümü bir grup homomorfizmasıdır.

Ayrıca ; $Sym(2) \cong \{\sigma \mid \forall i = 1,2, \sigma(2i) = \sigma(i)\cdot 2 \text{ ve } \sigma(2i-1) = \sigma(2i)-1,\ \ell = 1\}$

olduğundan ; $Sym(2) \cong \{I, (13)(24)\}$dir.

$Sym(2)$ nin 2-sylow altgrubu kendisine eşit olduğundan;

$Sylow(Sym(2)) = \{I, (13)(24)\}$dir. O halde $Sym(4)$ ün 2-sylow altgruplarından biri;

$\{\mathrm{I}, (12), (34), (12)(34)\} \rtimes \{\mathrm{I}, (13)(24)\}$

Yarıdirek çarpımına izomorftur. Bu yarıdirek çarpımının ürettiği grup;

$\{I, (12), (34), (12)(34), (14)(23), (13)(24), (1324), (1423)\}$şeklindedir. Bu grupta $Sym(4)$ ün 2-sylow altgruplarından biridir.

6. GENEL LİNEER GRUPLARIN SYLOW P-ALT GRUPLARININ SINIFLANDIRILMASI

$\mathbb{F}_{q^k}$ cismi $\mathbb{F}_q$ üzerine k-boyutlu bir vektör uzayıdır. O zaman; $\varphi : \mathbb{F}^*_{q^k} \to GL_k(\mathbb{F}_q)$ $\quad \forall x \in \mathbb{F}^*_{q^k}$, $g \in \mathbb{F}_{q^k}$ ve $\varphi(x)(g) = xg$ olacak şekilde bir homomorfizma vardır. O halde $\mathbb{F}^*_{q^k}$ nın bir kopyası $GL_k(\mathbb{F}_q)$ içindedir.

$\forall x \in \mathbb{F}^*_{q^k}$ için bu kopya matrise M_x diyelim. Ayrıca $\mathbb{F}^*_{q^k}$ nın p-sylow altgrubu da $Sylow_p(\mathbb{F}^*_{q^k})$ şeklinde tanımlayalım.

$$
\mathrm{P} = \left\{ \begin{pmatrix} (M_{x_1}) & 0 & & \cdots & & 0 \\ 0 & (M_{x_2}) & & & & \\ \vdots & & \ddots & & & \vdots \\ & & & (M_{x_\ell}) & & \\ & & & & 1 & \\ & & & & & \ddots \\ 0 & & \cdots & & 0 & 1 \end{pmatrix} \;\middle|\; x_i \in Sylow_p(\mathbb{F}^*_{q^k}) \right\}
$$

Bu şekilde yazılan P kümesi $GL_n(\mathbb{F}_q)$ nun bir alt grubudur. Bu alt grubun mertebesi; $\left|Sylow_p(\mathbb{F}^*_{q^k})\right|^{\ell} = (p^{val(q^k-1)})^{\ell} = p^{r\ell}$ dir. Aynı zamanda P bir p-altgruptur. Şimdi $Sym(\ell)$ nin P grubu üzerine eşlenik etkisini tanımlayalım. Verilen bir $\sigma \in Sym(\ell)$ için;

$$\sigma \begin{pmatrix} (M_{x_1}) & 0 & & \cdots & & & 0 \\ 0 & (M_{x_2}) & & & & & \\ \vdots & & \ddots & & & & \vdots \\ & & & (M_{x_\ell}) & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & \cdots & & 0 & 1 \end{pmatrix} \sigma^{-1}$$

$$= \begin{pmatrix} (M_{x_{\sigma(1)}}) & 0 & & \cdots & & & 0 \\ 0 & (M_{x_{\sigma(2)}}) & & & & & \\ \vdots & & \ddots & & & & \vdots \\ & & & (M_{x_{\sigma(\ell)}}) & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & \cdots & & 0 & 1 \end{pmatrix}$$

Aynı zamanda;

$$\begin{aligned} \varphi : Sym(\ell) &\rightarrow GL_\ell(\mathbb{F}_q) \\ \sigma &\mapsto \varphi_\sigma \\ \varphi_\sigma : \mathbb{F}_q^\ell &\rightarrow \mathbb{F}_q^\ell \\ e_i &\mapsto e_{\sigma(i)} \end{aligned}$$

φ dönüşümü bir homomorfizmadır. Burada dönüşüm tabanı başka bir tabana götüren dönüşümdür. Bununla birlikte $Sym(\ell)$ nin izomorfik kopyası $GL_\ell(\mathbb{F}_q)$ içindedir ve P grubu üzerine de yukarıda verildiği gibi eşlenik olarak etki eder. Bu izomorfik kopyanın oluşturulma yöntemini özet olarak verecek olursak;

1.) $Sym(\ell)$ nin doğal kopyası $GL_\ell(\mathbb{F}_q)$ içerisindedir. Bu alt grup matrislerin tabanlarının değişmesiyle oluşuyor. Ayrıca bu matrislerin her satır ve sütununda yalnızca bir tane 1 vardır.

2.) Verilen bir M elemanının izomorfik görüntüsünde 1 gördüğümüz her yeri $Id_{k\times k}$ ve 0 gördüğümüz her yeri de $0_{k\times k}$ matrisleriyle değiştiririz. Böylece bizim taban matrisimiz $k\ell \times k\ell$ boyutlu bir matris içerir.

3.) Köşegenlerin sonuna $n-k\ell$ sayıda 1 ve 0 eklersek $n\times n$ boyutlu bir matris elde ederiz. $GL_n(\mathbb{F}_q)$ nun bu alt grubuna S_ℓ diyelim. S_ℓ grubu $Sym(\ell)$ simetrik grubuna izomorftur ve ayrıca P grubu üzerine eşlenik olarak etki eder. Buradan;

P $\rtimes$ $Sylow_p(S_\ell)$ grubu $GL_n(\mathbb{F}_q)$ nun bir alt grubudur ve $P \cong (Sylow_p(\mathbb{F}^*_{q^k}))^\ell$ dır.

P $\rtimes$ $Sylow_p(S_\ell) \cong (Sylow_p(\mathbb{F}^*_{q^k}))^\ell \rtimes Sylow_p(Sym(\ell))$

Bununla birlikte;

$$\left|(Sylow_p(\mathbb{F}^*_{q^k}))^\ell \times Sylow_p(Sym(\ell))\right| = \left|(Sylow_p(\mathbb{F}^*_{q^k}))\right|^\ell \cdot \left|Sylow_p(Sym(\ell))\right| = p^{r\ell + val(\ell!)}$$

Böylece $(Sylow_p(\mathbb{F}^*_{q^k}))^\ell \rtimes Sylow_p(Sym(\ell))$ grubu $GL_n(\mathbb{F}_q)$ nun bir p-sylow altgrubuna izomorftur.

7. SONUÇ

Sonlu gruplarda Sylow p-altgruplarını bulmak mertebe arttıkça zorlaşmaktadır. Bu çalışmamızda Genel Lineer gruplar ve Simetrik grupların Sylow p-altgruplarının yapısı hakkında çalıştık. Bu çalışmanın ileri aşaması olarak Sonlu basit grupların sınıflandırılmasından yola çıkılarak sonsuz yerel sonlu grupların merkezleyenleri üzerinde çalışılabilir.

KAYNAKLAR

Alperin J. L. 1995. Groups and Representations. x+194 pp Springer-Verlag New York Berlin Heidelberg.

Dixon, J. D. And Mortimer, B.1996. Permutation Groups. Springer-Verlag, p. 346, New York.

Dixon, M. R. Evans, M. J., Obraztsov, V. N. And Wiegold, J. 2000. Groups that are covered by non-abelian simple groups, **Journal of Algebra, 223:** 511-526.

Feit, W. and Thompson, J. G. 1963. Solvability of groups of odd order, **Pacific J. Math., 13:** 775-1029. scructure of H_p-groups, **Pacific J. Math., 9:** 1097-1101. permutation groups, **Arch. Math., 27:** 3-17.

Herstein, I.N. 1990. Abstract Algebra. xix+292 pp., Berlin.

Hungerford, T.W., 1974. Algebra. xxiii+500 pp. Heidelberg, Berlin.

Robinson, D. J. S. 1995. A Course in the Theory of Groups. Springer-Verlag, p. 499, New York.

Rotman, Joseph J. 1994. An İntroduction to the Theory of Groups. xiv+513 pp. Springer-Verlag New York Berlin Heidelberg,

William Findlay, 1904. The Sylow Subgroups of the Symmetric Group, Transaction of the American Mathematical Society, Vol.5 No. 3 pp. 263-278.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı	:	Koray KARATAŞ
Doğum Yeri ve Tarihi	:	İzmir 18–11–1986

EĞİTİM DURUMU

Lisans Öğrenimi	:	Adnan Menderes Üniversitesi
Yüksek Lisans Öğrenimi	:	Adnan Menderes Üniversitesi
Bildiği Yabancı Diller	:	İngilizce

BİLİMSEL FAALİYETLERİ

a) Yayınlar
   -SCI
   -Diğer
b) Bildiriler
   -Uluslararası
   -Ulusal
c) Katıldığı Projeler

İŞ DENEYİMİ

Çalıştığı Kurumlar ve Yıl :

İLETİŞİM

E-posta Adresi : koraykaratas_35@hotmail.com

Tarih :