MAKSİMAL DEVİRLİ ALT GRUPLARA SAHİP SONLU P-GRUPLARIN SINIFLANDIRILMASI

Sait TAŞ

Yüksek Lisans Tezi
Matematik Anabilim Dalı
Doç. Dr. Erdal KARADUMAN
2010

ATATÜRK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

MAKSİMAL DEVİRLİ ALT GRUPLARA SAHİP SONLU P-GRUPLARIN SINIFLANDIRILMASI

Sait TAŞ

MATEMATİK ANABİLİM DALI

ERZURUM
2010

Doç. Dr. Erdal KARADUMAN danışmanlığında, Sait TAŞ tarafından hazırlanan bu çalışma 17.08.2010 tarihinde aşağıdaki jüri tarafından Matematik Anabilim Dalı'nda Yüksek lisans tezi olarak kabul edilmiştir.

Başkan: Prof. Dr. Hüseyin AYDIN imza:

Üye: Prof. Dr. Ramazan DİKİCİ imza:

Üye: Doç. Dr. Erdal KARADUMAN imza:

Yukarıdaki sonucu onaylarım.

(imza)

Prof. Dr. Ömer AKBULUT

Enstitü Müdürü

ÖZET

Yüksek Lisans Tezi

MAKSİMAL DEVİRLİ ALT GRUPLARA SAHİP SONLU P-GRUPLARIN SINIFLANDIRILMASI

Sait TAŞ

Atatürk Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Doç. Dr. Erdal KARADUMAN

Bu tezde, maksimal devirli alt gruplara sahip sonlu p-gruplar sınıflandırıldı ve bu grupların izomorf olduğu gruplar hakkında bilgi verildi. Ayrıca grup matrisleri yardımıyla bazı grupların izomorf olup olmadıkları araştırıldı.

2010, 64 sayfa

Anahtar Kelimeler: p-grup, Sonlu p-grup, Güçlü p - grup

ABSTRACT

MS Thesis

CLASSIFICATION OF FINITE P -GROUPS WITH THE MAXIMAL CYCLIC SUBGROUPS

Sait TAS

Ataturk University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Assoc. Prof. Dr. Erdal KARADUMAN

In this thesis, we classified finite p -groups with maximal cyclic subgroups and gave information about groups which are isomorphism to these groups. It is also investigated whether some groups are isomorphism or not with the help of the group matrices.

2010, 64 pages

Keywords: p -group, Finite p -group, Powerful p - group

TEŞEKKÜR

Yüksek lisans tezi olarak sunduğum bu çalışma, Atatürk üniversitesi Fen Fakültesi Matematik Bölümü'nde yapılmıştır.

Bu tez konusunu çalışmamı sağlayan, çalışmalarımda ve tezin hazırlanışında yakın ilgi gösteren ve yardımlarını esirgemeyen hocam Sayın Doç. Dr. Erdal KARADUMAN'a ve çalışmalarım boyunca kendilerinden görmüş olduğum destekten dolayı başta bölüm başkanımız Sayın Prof. Dr. Hüseyin AYDIN olmak üzere bölümdeki bütün hocalarıma ve araştırma görevlisi arkadaşlarıma en içten teşekkürlerimi arz ederim.

Çalışmalarım boyunca kendilerinden görmüş olduğum maddi-manevi destekten ve sonsuz güvenden dolayı anne-babama, kardeşlerime ve eşime teşekkür etmeyi bir borç bilirim.

Yine bu tezde yapmış olduğu maddi ve manevi destekten dolayı TÜBİTAK'a teşekkürlerimi sunarım.

Sait TAŞ
Ağustos 2010

SİMGELER DİZİNİ

$\leq$	Alt grup
e	Birim eleman
$\cup$	Birleşim
G/H	Bölüm grubu
$\equiv$	Denktir
$[\ :\ ]$	İndeks
$\cong$	İzomorf
$\cap$	Kesişim
$[x, y]$	Komutatör
$\vert\ \vert$	Mertebe
$\lhd$	Normal alt grup
$p \vert n$	p böler n yi

ÇİZELGE DİZİNİ

ŞEKİLLER DİZİNİ

İÇİNDEKİLER

1. GİRİŞ

Grup kavramı modern cebirin en temel kavramlarından biridir. Geometrik şekillerin simetri özelliklerinin araştırılmasında ve cebirsel denklemlerin köklerinin belirlenmesinde ortaya çıkmıştır. Grup kavramının ilk izleri Lagrange'ın cebirsel denklemler üzerindeki çalışmalarına kadar gider. Lagrange [1736-1813] bir cebirsel denklemin köklerini belirleyebilmek amacıyla kökler üzerinde tanımlı permütasyonların özelliklerinin araştırılmasını başlatmış ve bu yöndeki çalışmalarla köklerin belirlenebileceğini tahmin etmiştir. Galois [1811-1832] ilk kez grup terimlerini permütasyon grubu anlamında kullanmıştır. Galois'nın çalışmaları Liouville tarafından 1846 da yayınlandıktan sonra grup kavramı yayılmaya başlamıştır. Cauchy [1789-1857] ilk kez permütasyon gruplarını bağımsız bir konu olarak çalışmış ve bir çok özelliklerini elde etmiştir. (Örneğin, sonlu bir permütasyon grubunun mertebesini bölen her asal sayı için mertebesi bu asal sayıya eşit olan bir elemanının olduğunu göstermiştir.)

İlk sonlu grup tanımı A.Cayley [1821-1895] tarafından 1854 de verilmiştir. "Birbirinden farklı elemanları $1,\alpha,\beta,...$ olan bir kümenin herhangi iki elemanının çarpımı ve bir elemanın kendisiyle çarpımı tekrar kümeye ait ise bu kümeye bir grup denir." İlk genel soyut grup tanımı Wolter Von Dyck [1856-1934] tarafından 1882 de verilmiştir. İlk kez burada grubun her elemanının tersinin olduğu belirtilmektedir.

p-gruplar kavramı, sonlu gruplar teorisinde çok önemlidir. Bu kavramın önemi, şu iki nedenden kaynaklanmaktadır. Bunlardan biri; p- gruplar, sonlu gruplarda kapsamlı çalışmaya imkan veren pek çok özelliğe sahip olması, diğeri ise; her hangi bir sonlu G grubu, p- grup olan ve G grubunun yapısıyla yakından ilgili olan, Sylow p-alt gruplar diye adlandırılan alt gruplar içermesidir.

Gruplar teorisi tarihinde ilk olarak $0 \leq n \leq 4$ için, p^n mertebeli gruplar sınıflandırılmıştır (Burnside 1897). Daha sonra, p^7 sayısını bölen mertebeli gruplara kadar genişlemiştir. Sonlu bir grubun yapısı, onun lokal alt gruplar diye adlandırılan, birimden farklı p -alt gruplarının normalleştircilerinin yapısı ile elde edilir.

Braver, Sylow 2-alt grupları olan bütün grupları sınıflandırmıştır. Daha sonra Walter, Govenstein, Bender, Suzuki, Glauberman ve diğerleri, bu basit grupları abelyen, dihedral, semidihedral veya quaternion grup diye sınıflandırmışlardır.

Sonlu gruplarda belli mertebeden bazı alt grupların olduğunu ifade eden bazı teoremler vardır. Bunların başında gelen ve çok kullanılan teoremler Norveçli matematikçi Sylow'a aittir. Sylow teoremleri, $n \| G|$ ise G grubunun n. mertebeden ne zaman bir alt grubunun bulunacağını ifade eder.

Yine Sylow teoremleri abelyen olmayan sonlu grupların yapısının anlaşılmasında önemli rol oynar. Özellikle verilen bir mertebeden bir grubun basit olup olmadığı bu teoremler yardımıyla belirlenebilir.

Lagrange teoremine göre, sonlu bir grubun alt grubunun mertebesi grubun mertebesinin bir bölenidir. Ancak bunun tersi her zaman doğru olmayabilir.

2. KURAMSAL TEMELLER

Bu bölümde sonraki bölümlerde kullanılacak olan temel tanım ve kavramlar verilecektir.

2.1. İkili İşlem

Tanım 2. 1. 1: A ve B iki küme olsun. $a \in A$ ve $b \in B$ olmak üzere

$$(a,b) = \{\{a\},\{a,b\}\}$$

kümesine (a,b) **sıralı ikilisi** denir.

Tanım 2.1.2: $f : A \times A \to A$ fonksiyonuna A da bir **ikili işlem** denir. İşlemler $\oplus, \otimes, \square, *, \ldots$ gibi sembollerle gösterilir. Grup teorisi konusunda bizi ilgilendiren ikili işlemdir.

Tanım 2.1.3: Üzerinde en az bir ikili işlem tanımlı yapıya cebirsel yapı denir. Yani $A \neq \varnothing$ kümesi üzerinde $*$ ikili işlemi tanımlansın. $(A,*)$ ikilisine **cebirsel yapı** denir.

Teorem 2.1.1: (Fermat teoremi) p asal bir sayı ve $(a,p)=1$, $a \in Z^+$ olsun. Bu durumda

$$a^{p-1} \equiv 1 \pmod{p}$$

yazılır (Bayraktar 1988).

Teorem 2.1.2: (**Binom Teoremi**) Her a , b reel sayısı ve her n doğal sayısı için

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

dir.

2.2. Grup Kavramı

Tanım 2.2.1: G boştan farklı bir küme $*$ da G kümesi üzerinde tanımlı bir ikili işlem olsun. $(G,*)$ cebirsel yapısı aşağıdaki şartları sağlıyorsa bu cebirsel yapıya **grup** denir.

G.1 $\forall a,b,c \in G$ için $(a*b)*c = a*(b*c)$ olmalıdır. (Birleşme özelliği)

G.2 $\forall a \in G$ için $a*e = a = e*a$ olacak şekilde $e \in G$ olmalıdır. (Özdeş(birim) elemanın varlığı)

G.3 $\forall a \in G$ için $a*a^{-1} = e = a^{-1}*a$ olacak şekilde $a^{-1} \in G$ olmalıdır. (Ters elemanın varlığı)

Örnek 2.2.1: $\forall \overline{x}, \overline{y} \in Z_n$ için $\overline{x} + \overline{y} = \overline{x+y}$ şeklinde tanımlanan işleme göre Z_n bir gruptur.

Tanım 2.2.2: $(G,*)$ grubu $\forall a,b \in G$ için $a*b = b*a$ şartını sağlıyorsa $(G,*)$ grubuna **değişmeli (abel veya komutatif) grup** denir.

Örnek 2.2.2: $(Z,+)$ değişmeli bir gruptur.

Tanım 2.2.3: G sonlu bir küme ise $(G,*)$ grubuna **sonlu bir grup** denir ve eleman sayısına da **grubun mertebesi** denir. $|G|$ ile gösterilir.

Tanım 2.2.4: G bir grup ve $a \in G$ olsun. Eğer $a^t = e$ olacak biçimde bir t pozitif tam sayısı varsa bu pozitif t tamsayılarının en küçüğüne a **elemanın mertebesi** denir. $|a|$ ile gösterilir.

Tanım 2.2.5: $(G,*)$ bir grup, H da G grubunun boştan farklı bir alt kümesi olsun. Eğer H kümesi $*$ işlemine göre grup şartlarını sağlıyorsa $(H,*)$ grubuna $(G,*)$ grubunun bir **alt grubu** denir. $H \leq G$ ile gösterilir.

Örnek 2.2.3: Çift tamsayılar kümesi $2Z$, $(Z,+)$ grubunun bir alt grubudur.

Tanım 2.2.6: G ve $\{e\}$ gruplarına G grubunun **aşikar (trivial) alt grupları** denir.

Tanım 2.2.7: Bir grubun aşikar alt grupları hariç diğer bütün alt gruplarına **has alt grup** denir.

Tanım 2.2.8: Bir has alt grup, hiçbir has alt grubun has alt grubu değilse bu has alt gruba **maksimal alt grup** denir.

Tanım 2.2.9: $x, y \in G$ olsun. $x^{-1}y^{-1}xy$ ifadesine x ve y nin **komutatörü** denir. $[x, y]$ ile gösterilir. G de tanımlanan bütün komutatörler tarafından gerilen G grubunun alt grubuna **türetilmiş** veya **komutatör alt grup** denir.

Tanım 2.2.10: M , bir G grubunun bir alt kümesi olsun. M kümesini kapsayan, G grubunun bütün alt gruplarının arakesitine M kümesinin **ürettiği(doğurduğu) alt grup** denir ve $\langle M \rangle$ ile gösterilir. M kümesinin elemanlarına da $\langle M \rangle$ **grubunun üreteçleri** denir.

Tanım 2.2.11: Bir G grubu için, $G = \langle M \rangle$ olacak şekilde bir $M \subset G$ alt kümesi bulunabiliyorsa, G grubuna M ile **üretilmiş grup** denir. Eğer M kümesi sonlu ise G grubuna **sonlu üretilmiş grup** ve $M = \{a\}$ şeklinde tek elemanlı bir küme ise G grubuna a ile üretilmiş **devirli grup** denir.

Örnek 2.2.4: Z **,** 1 ile üretilmiş sonsuz devirli bir gruptur.

Örnek 2.2.5: $G=\{i,-i,1,-1\}$ grubu i ile üretilmiş 4. mertebeden sonlu devirli bir gruptur.

Tanım 2.2.12: G bir grup, H kümesi de G grubunun bir alt kümesi olsun.

$$Ha=\{ha : h\in H, a\in G\} \text{ ve } aH=\{ah : h\in H, a\in G\}$$

kümelerine sırasıyla H kümesinin G grubundaki **sağ yan** ve **sol yan kümeleri** denir.

Teorem 2.2.1: $N\le G$ olsun. Bu takdirde aşağıda verilen ifadeler birbirine denktir.

N1. $\forall a\in G, \forall x\in N$ için $axa^{-1}\in N$ dir

N2. $\forall a\in G$ için $aNa^{-1}\subset N$ dir.

N3. $\forall a\in G$ için $aNa^{-1}=N$ dir.

N4. $\forall a\in G$ için $aN=Na$ dır

Tanım 2.2.13: Teorem 2.2.1. in denk koşullarından birini sağlayan G grubunun bir N alt grubuna **normal alt grup** denir ve $N\lhd G$ ile gösterilir.

Teorem 2.2.2: G bir grup ve H,G grubunun bir alt grubu olsun. Her $a,b\in G$ için $(aH)(bH)=abH$ olması için gerek ve yeter şart H nın G grubunun bir normal alt grubu olmasıdır.

İspat: Önce $H\lhd G$ olsun. $x\in(aH)(bH)$ olsun. O zaman $x=(ah_1)(bh_2)$ olacak biçimde $h_1,h_2\in H$ vardır.

$$x=(ah_1)(bh_2)=a(h_1b)h_2=ab(b^{-1}h_1b)h_2\in abH$$

olduğundan $x\in abH$ ve buradan $(aH)(bH)\subseteq abH$ dır. Şimdi ise $y\in abH$ olsun. O zaman $y=abh$ olacak biçimde $h\in H$ vardır. $y=(ae)(bh)\in(aH)(bH)$ olduğundan $y\in(aH)(bH)$ ve buradan $abH\subseteq(aH)(bH)$ bulunur. Böylece eşitlik gösterilmiş olur.

Karşıt olarak her $a,b \in G$ için $(aH)(bH) = abH$ olsun. $h \in H$ ve $g \in G$ olsun. $ghg^{-1} \in H$ olduğunu göstermek yeter. Fakat

$$ghg^{-1} = (gh)(g^{-1}e) \in (gH)(g^{-1}H)$$

olduğundan $ghg^{-1} \in (gg^{-1})H = H$ bulunur.

G bir grup ve H, G grubunun bir alt grubu olsun. Eğer H, G grubunda normal ise Teorem 2.2.1 den dolayı, her $g \in G$ için $gH = Hg$ olduğundan H normal alt grubunun sol yan kümesi sağ yan kümesine eşittir. Bu küme G/H ile gösterilir. Böylece

$$G/H = \{gH : g \in G\} = \{Hg : g \in G\}$$

dir. Aşağıda görüldüğü gibi G/H bir grup yapılabilir.

Teorem 2.2.3: G bir grup ve H, G grubunun bir normal alt grubu olsun. G/H üzerinde bir çarpma işlemi şöyle tanımlansın. Her $aH, bH \in G/H$ için

$$(aH)(bH) = abH$$

olsun. Bu işleme göre G/H bir gruptur.

İspat: Önce çapma işleminin iyi tanımlı olduğunu gösterelim. $aH, bH \in G/H$ ve $x \in aH, y \in bH$ olsun.

$$(ab)H = (xy)H$$

olduğunu göstermeliyiz. $x = ah_1$ ve $y = bh_2$ olacak biçimde $h_1, h_2 \in H$ vardır. Şimdi $H \lhd G$ olduğundan

$$(xy)H = (ah_1bh_2)H = \left[ab\underbrace{(b^{-1}h_1b)}_{\in H}h_2 \right]H = abH$$

ve böylece iddia gösterilmiştir. Şimdi $aH, bH, cH \in G/H$ olsun. O zaman Teorem 2.2.2. den dolayı

$$[(aH)(bH)](cH) = [(ab)c]H = [a(bc)]H = (aH)[(bh)(cH)]$$

olduğundan birleşme özelliği sağlanır. Bundan başka

$$(aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH)$$

ve

$$(aH)(a^{-1}H) = (aa^{-1})H = eH = (a^{-1}a)H(a^{-1}H)(aH)$$

olduğundan eH birim eleman ve $(aH)^{-1} = a^{-1}H$ dir. Dolayısıyla G/H bir gruptur.

Tanım 2.2.14: Yukarıdaki G/H grubuna **bölüm (faktör)** grubu denir.

Örnek 2.2.6: $N = \langle 4 \rangle = 4Z$ alt grubuna göre Z/N bölüm grubu $\{N, 1+N, 2+N, 3+N\}$ şeklindedir. Çünkü herhangi bir $n \in Z$ alındığında, $n = 4q + r, 0 \le r < 4$ olacak şekilde $\exists q, r \in Z$ bulunabilir. Böylece n tam sayısı bu 4 sınıftan birine ait olur. Şu halde $Z/N \cong Z_4$ olur.

Tanım 2.2.15: $(G, \bullet)$ ve $(H, *)$ iki grup ve $f: G \to H$ bir fonksiyon olsun. $\forall a, b \in G$ için

$$f(a \bullet b) = f(a) * f(b)$$

ise f ye G den H ya bir **homomorfizma** denir.

Tanım 2.2.16: 1-1, örten bir homomorfizmaya **izomorfizm** denir.

Tanım 2.2.17: A, G grubunda boş olmayan bir küme olsun. $g \in G$ elemanı için

$$g^{-1}Ag = \{g^{-1}ag : a \in A\}$$

olarak tanımlanır. Ayrıca,

$$N_H(A) = \{h : h^{-1}Ah = A,\ h \in H\}$$

kümesine, A kümesinin H grubunda **normalleştirilmesi** denir.

Tanım 2.2.18: Bir G grubunun, aşikar olmayan Sylow p-alt grubunun normalleştiricisine **lokal (yerel)** alt grup denir.

Teorem 2.2.4: $A \neq \varnothing$ bir küme ve $H \leq G$ olsun. Bu takdirde, $N_H(A) \leq G$ olur.

Tanım 2.2.19: A ve B, bir G grubunun boş olmayan iki alt kümesi olsun. Bazı $h \in H$ elemanları için , $h^{-1}Ah = B$ oluşuyorsa, B kümesine A kümesinin H **eşleniği** denir. Eğer A ve B, G grubunun birer alt grubu, $g \in G$ için $g^{-1}Ag = B$ oluyorsa, A ve B alt gruplarına G grubunda **eşleniktirler** denir.

Tanım 2.2.20: Bir elemanın tüm eşleniklerinin (konjuge) kümesine, o elemanın **eşlenik (konjuge)** sınıfı denir. Yani $C(a) = \{xax^{-1} : x \in G\}$ dır.

Tanım 2.2.21: G bir grup olsun. G grubunun, bütün elemanları ile değişmeli olan elemanların oluşturduğu kümeye G grubunun **merkezi** denir ve $Z(G)$ ile gösterilir. Yani, $Z(G) = \{x \in G : xg = gx,\ \forall g \in G\}$ kümesine G grubunun **merkezi** denir.

Tanım 2.2.22: Bir G grubu, eğer bazı m tamsayısı için $Z_m(G) = G$ ise nilpotenttir. Bu durumda $Z_c(G) = G$ olacak şekilde en küçük c tamsayısına G grubunun **nilpotent sınıfı** denir.

Bu tanıma göre Abelyen grupların nilpotent sınıfı 1 dir.

Teorem 2.2.5: G bir grup olsun.

$$|a| = m \text{ ve } |b| = n,\ (m,n) = 1 \qquad ab = ba$$

ise, o zaman $|ab| = mn$ olur.

Tanım 2.2.23: $(G,\bullet)$ bir grup ve S bir küme olsun. $f : G \times S \to S,\ f(g,s) \to gs$ yazıldığında $\forall s \in S$ ve $g_1, g_2 \in G$ için

i. $es = s$, (e, G grubunun birim elemanı)

ii. $g_1(g_2 s) = (g_1 g_2) s$

şartlarını sağlayan bir f dönüşümü varsa G, S kümesine **etki** ediyor denir. G, S kümesine etki ediyorsa S kümesine $G-$**küme** adı verilir.

Tanım 2.2.24: G bir grup ve $X \subseteq F$ olmak üzere $\beta : X \to G$ fonksiyonu verilsin. Eğer β fonksiyonunun genişlemesi olacak şekilde tek bir $\beta^{'} : F \to G$ homomorfizmi varsa F, X üzerinde **serbesttir** denir.

Burada $\beta^{'}$ nün β fonksiyonunun genişlemesi olması demek, $\forall x \in X$ için $\beta^{'}(x) = \beta(x)$ olması demektir.

Tanım 2.2.25: X bir küme olsun. $F = F(X)$ ile X üzerinde serbest grubu, R de F nin bir alt kümesini göstersin. Bu takdirde $G = \langle X | R \rangle$ ye G grubunun bir **temsili** denir. X kümesine gerenlerin kümesi ve R kümesine de bağıntıların kümesi denir.

Tanım 2.2.26: Bir G grubu $|a| = n, |b| = 2$ ve $ba = a^{-1}b$ bağıntılarını sağlayacak şekilde a, b elemanları tarafından geriliyorsa bu G grubuna $2n.$ mertebeden bir **dihedral grup** denir ve

$$D_n = \langle a, b | \ a^n = e, b^2 = e, ba = a^{-1}b \rangle$$

ile temsil edilir.

Tanım 2.2.27: Bir G grubu $|a| = 4, a^2 = b^2$ ve $ba = a^3 b$ bağıntılarını sağlayacak şekilde a, b elemanları tarafından geriliyorsa bu G grubuna **quaternion grup** denir ve

$$Q = \langle a, b | \ a^4 = e, a^2 = b^2, ba = a^3 b \rangle$$

ile temsil edilir.

Genelleştirilmiş Quaternion grubu ise

$$Q_{2^n} = \left\langle a,b \middle| \ a^{2^{n-1}} = e, b^2 = a^{2^{n-2}}, aba = b \right\rangle$$

ile temsil edilir.

3. MATERYAL ve YÖNTEMLER

Bu bölümde maksimal devirli alt gruplara sahip sonlu p - grupların sınıflandırılması ile ilgili bazı tanım, teorem ve ispatlar verilecektir.

3. 1. P – Gruplar

Tanım 3.1.1: G bir grup ve p sabit bir asal sayı olmak üzere G grubunun her elemanının mertebesi p asal sayısının bir kuvveti ise G grubuna p **- grup** denir.

Tanım 3.1.2: H **,** her hangi bir G grubunun bir alt grubu olsun. Eğer H alt grubundaki her elemanın mertebesi p asal sayısının bir kuvveti ise H alt grubuna G grubunun p **-alt grubu** denir.

Tanım 3.1.3: $|G| = |Z(G)| + \sum_{x \in C} [G : N(x)]$ ifadesine G grubunun **sınıf denklemi** adı verilir.

Teorem 3.1.1 (Lagrange): Sonlu bir grubun her alt grubunun mertebesi, grubun mertebesini böler (Bayraktar 1988).

Teorem 3.1.2: Sonlu bir G grubunun bir p**-** grup olması için gerek ve yeter şart $|G| = p^{\alpha}$, $\alpha \geq 0$ olmalıdır.

İspat: G bir p**-** grup ve q, G grubunun mertebesini bölen asal bir sayı olsun. Bu takdirde Cauchy Teoreminden dolayı G grubunun, mertebesi q olan bir elemanı vardır. G bir p**-** grup olduğundan, G grubunun her bir elemanının mertebesi p asal sayısının bir kuvveti şeklinde olur. Bu durumda $p = q$ olmak zorundadır. Böylece

$|G| = p^{\alpha}$ olur. Tersine olarak $|G| = p^{\alpha}$ olsun. Bu takdirde Lagrange Teoreminden dolayı her hangi bir $b \in G$ elemanın gerdiği $\langle b \rangle$ devir grubunun mertebesi p^{α} sayısını böler.

Halbuki $\langle b \rangle$ devir grubunun mertebesi b elemanın mertebesi olduğundan $|b| = p^{i}$, $(i \leq \alpha)$ şeklindedir.

Teorem 3.1.3: $G \neq \{e\}$ olmak üzere G sonlu bir p**-** grup olsun. Bu takdirde G grubunun merkezi birden fazla eleman ihtiva eder.

İspat: $|G| = |Z(G)| + \sum_{i=1}^{m} [G : Z_G(x_i)]$ sınıf denklemi ele alınsın. Her i için $[G : Z_G(x_i)] > 1$ olup bu sayı $|G| = p^{\alpha}$ yı böler $(\alpha \geq 1)$. G bir p-grup olduğundan p, $[G : Z_G(x_i)]$ ve $|G|$ yi böler. Dolayısıyla p, $|Z(G)|$ yi de böler. $|Z(G)| \geq 1$ olduğundan $Z(G)$ en az p eleman ihtiva eder.

Teorem 3.1.4: p asal bir sayı olmak üzere H grubunun mertebesi p^{n} ve S sonlu bir H - kümesi olsun. Üstelik kabul edelim ki

$$S_0 = \{ x \in S : hx = x, \ \forall h \in H \}$$

şeklindedir.

Bu takdirde

$$|S| \equiv |S_0| (\mathrm{mod}\ p)$$

olur (Bayraktar 1988).

İspat: $x \in S$ olsun. $\overline{x}$ in bir tek eleman ihtiva etmesi için gerek ve yeter şart $x \in S_0$ olmasıdır. Gerçekten $\overline{x} = \{hx\}$ ise $x \in \overline{x}$ olacağından $hx = \overline{x}$ dir. Bu ise $x \in S_0$

olduğunu ifade eder. Tersine $x \in S_0$ ise $h \in H$ için $hx = x$ olacağından $\overline{x} = \{x\}$ dir. O halde $i = 1,2,...,n$ için $\left|\overline{x_i}\right| > 1$ olmak üzere

$$S = S_0 \cup \overline{x_1} \cup ... \cup \overline{x_n}$$

yazılabilir. Buradan

$$|S| = |S_0| + \left|\overline{x_1}\right| + ... + \left|\overline{x_n}\right|$$

elde edilir. Yine S bir H-küme olduğundan $\left|\overline{x_i}\right| = \left[H : H_{x_i}\right]$ yazılabilir. Buradan $\left|\overline{x_i}\right| \big| |H| = p^n$ olduğundan $p \big| \left|\overline{x_i}\right|$ elde edilir. Böylece $p \big| |S| - |S_0|$ olur. Yani

$$|S| \equiv |S_0| (\mathrm{mod}\, p)$$

dir.

Teorem 3.1.5: H **,** sonlu bir G grubunun bir p **-** alt grubu ise

$$\left[N_G(H) : H\right] \equiv \left[G : H\right] (\mathrm{mod}\, p)$$

olur (Bayraktar 1988).

İspat: H nın G grubundaki sol yan kümelerinin kümesine S denilsin. Bu takdirde

$$|S| = [G : H]$$

olur. $S_0 = \{xH \in S : hxH = xH, \forall h \in H\}$ ise

$$\begin{aligned} xH \in S_0 &\Leftrightarrow hxH = xH \\ &\Leftrightarrow x^{-1}hxH = H \\ &\Leftrightarrow x^{-1}hx \in H \\ &\Leftrightarrow x^{-1}Hx = H \\ &\Leftrightarrow xHx^{-1} = H \\ &\Leftrightarrow x \in N_G(H) \end{aligned}$$

yazılabilir. Buradan anlaşılır ki, S_0 kümesinin mertebesi, $x \in N_G(H)$ olmak üzere xH yan kümelerinin sayısına eşittir. Yani $|S_0| = [N_G(H) : H]$ dır. Teorem 3.1.4 ten dolayı

$$\left[N_G\left(H\right):H\right] \equiv \left[G:H\right]\left(\text{mod } p\right)$$

olur.

Teorem 3.1.6: G sonlu bir grup olsun. H **,** G grubunun bir p **-** alt grubu ve $p \| [G:H]$ ise $N_G(H) \neq H$ olur.

İspat: $p \| [G:H]$ olsun. Teorem 3.1.5 ten

$$0 \equiv [G:H] \equiv \left[N_G\left(H\right):H\right] (\text{mod } p)$$

yazılabilir. Buradan $\left[N_G\left(H\right):H\right] > 1$ olur. Böylece $N_G(H) \neq H$ olur.

Tanım 3.1.4: G sonlu bir grup, p $|G|$ yi bölen bir asal sayı, p nin $|G|$ yi bölen en büyük kuvveti p^n ise G nin p^n inci mertebeden H alt grubuna G nin bir **Sylow** $p-$ **alt grubu** denir.

Sonlu gruplarda belli mertebeden bazı alt grupların olduğunu ifade eden bazı teoremler vardır. Bunların başında gelen ve çok kullanılan teoremler Norveçli Matematikçi Sylow'a aittir. Sylow Teoremleri, $n \mid |G|$ ise G grubunun n. mertebeden ne zaman bir alt grubu bulunacağını ifade eder.

Yine Sylow teoremleri abelyen olmayan sonlu grupların yapısının anlaşılmasında önemli rol oynar. Özellikle verilen mertebeden bir grubun basit olup olmadığı bu teoremler yardımıyla belirlenebilir.

Lagrange teoremine göre, sonlu bir grubun bir alt grubunun mertebesi, grubun mertebesinin bir bölenidir. Ancak tersine m sayısı, n sayısının bir böleni ise n mertebeli bir grup, m mertebeli bir alt gruba sahip olmayabilir.

Örnek 3.1.1: Mertebesi 12 olan bir alterne grubunun, mertebesi 6 olan bir alt grubu yoktur.

$$A_4 = \begin{Bmatrix} I,(12)(34),(13)(24),(14)(23),(123),(132), \\ (234),(134),(124),(142),(143),(243) \end{Bmatrix}$$

Buna göre $m|n$ ise, n mertebeli bir grubun, m mertebeli bir alt grubunun olacağını kesinlikle söylemeyiz. Ancak m bir asal sayı veya bir asal sayının kuvveti ise o zaman böyle alt gruplar mevcuttur.

İşte böyle grupların varlığı ve sayısı Sylow Teoremlerinin konusudur.

Teorem 3.1.7 (Cauchy): G bir grup ve p bir asal sayı olsun. Eğer $p||G|$ ise, G grubunun mertebesi p olan bir elemanı vardır.

İspat: $a_i \in G$ ve $a_1a_2a_3...a_p = e$ olmak üzere G grubunun elemanlarının $(a_1, a_2, a_3, ..., a_p)$ p -lilerinin kümesini S ile gösterelim. Yani

$$S = \{(a_1, a_2, a_3, ..., a_p) : a_i \in G \;\; ve \;\; a_1a_2a_3...a_p = e\}$$

olsun. $|G| = n$ olsun. $a_1a_2a_3...a_p = e$ eşitliğinden $a_p = (a_1a_2...a_{p-1})^{-1}$ bir tek olarak tesbit edilebileceğinden $|S| = n^{p-1}$ olur. $p|n$ olduğundan $|S| \equiv 0 (\text{mod}\, p)$ olur. Şimdi iddia ediyoruz ki Z_p grubu, S kümesine bir devir permütasyonu ile etki eder. Yani $\forall k \in Z_p$ ve $\forall x = (a_1, a_2, a_3, ..., a_p) \in S$ için

$$\begin{aligned} \Phi(k, x) = kx &= k(a_1, a_2, a_3, ..., a_p) \\ &= (a_{k+1}, a_{k+2}, ..., a_p, a_1, a_2, ..., a_k) \end{aligned}$$

olarak tarif edilirse, S bir Z_p-kümesidir. Her şeyden önce gruplarda $ab = e$ olması $ba = e$ olmasını gerektirdiğinden $(a_{k+1}, a_{k+2}, ..., a_p, a_1, a_2, ..., a_k) \in S$ olur. Çünkü

$$\begin{aligned} a_1a_2a_3...a_p = e &\Rightarrow a_pa_1a_2a_3...a_{p-1} = e \\ &\Rightarrow a_{p-1}a_pa_1a_2a_3...a_{p-2} = e \\ &\vdots \\ &\Rightarrow a_{k+1}a_{k+2}...a_pa_1a_2...a_k = e \end{aligned}$$

şeklindedir. Diğer taraftan $0 \in Z_p$ özdeş eleman ise $\forall x \in S$ için $0x = x$ olur. Ayrıca $k, k' \in Z_p$ olmak üzere

$$\begin{aligned} (k+k')(a_1, a_2, a_3, ..., a_p) &= (a_{k+k'+1}, a_{k+k'+2}, ..., a_{k+k'}) \\ &= k(a_{k'+1}, a_{k'+2}, ..., a_{k'}) \\ &= k(k'(a_1, a_2, ..., a_p)) \end{aligned}$$

olduğundan $\forall x \in S$ için $(k+k')x = k(k'x)$ olur. O halde Z_p nin S kümesi üzerine etkisi iyi tanımlıdır.

Teorem 3.1.4. deki gibi $S_0 = \{x \in S : kx = x, \forall k \in Z_p\}$ olarak tanımlanırsa $(e, e, ..., e) \in S_0$ olduğundan $S_0 \neq \varnothing$ dır. Bu durumda $|S_0| \neq 0$ olur. Dolayısıyla S_0 kümesinde en az p eleman bulunmalıdır. O halde $(a, a, a, ..., a) \in S_0$ olacak şekilde bir $a \neq e$ vardır. Böylece $a^p = e$ olur. p asal olduğundan $|a| = p$ olur.

Teorem 3.1.8 (I. Sylow Teoremi): p asal bir sayı ve $(p, m) = 1$ olmak üzere G grubunun mertebesi $p^n m$ olsun $(n \geq 1)$. Bu takdirde $1 \leq i \leq n$ şartını sağlayan her bir i için G grubunun, mertebesi p^i olan bir alt grubu vardır. Üstelik G grubunun p^i mertebeli $(i < n)$ her alt grubu, p^{i+1} mertebeli alt grubunda normaldir.

İspat: $p \| G|$ olduğundan Cauchy Teoremine göre G grubunun, mertebesi p olan bir a elemanı ve dolayısıyla mertebesi p olan $\langle a \rangle$ alt grubu vardır.

Şimdi varsayalım ki H, G grubunun p^i mertebeli alt grubudur ($1 \leq i \leq n$). Bu durumda $p \| [G : H]$ olur. Diğer taraftan $H, N_G(H)$ da normaldir. Teorem 3.1.6 ya göre $N_G(H) \neq H$ ve Teorem 3.1.5 e göre de

$$1 < \left| N_G(H)/H \right| = \left[N_G(H) : H \right] \equiv \left[G : H \right] \equiv 0 (\mathrm{mod}\, p)$$

olur. Yani $p \| N_G(H)/H|$ olur. O halde yine Cauchy Teoremine göre $N_G(H)/H$ grubunun, mertebesi p olan bir alt grubu vardır. Bu grup, $H < H_1 < N_G(H)$ olmak üzere H_1/H şeklindedir. $H \lhd N_G(H)$ olduğundan H, H_1 de de normaldir.

$$|H_1| = |H|,\ |H_1/H| = p^i p = p^{i+1}$$

olur.

Teorem 3.1.9 (II. Sylow Teoremi): $|G| < \infty$ bir grup, $H \leq G$ herhangi bir p - alt grubu ve K da herhangi bir $p-$Sylow alt grubu olsun. Bu takdirde $H \leq xKx^{-1}$ olacak şekilde $x \in G$ vardır. Özellikle G grubunun herhangi iki Sylow p - alt grubu eşleniktir.

İspat: $S = \{xK : x \in G\}$ olsun. $S_0 = \{x \in S : hxK = xK,\ \forall h \in H\}$ ise Teorem 3.1.5 ten $|S_0| \equiv |S| = [G : K] (\mathrm{mod}\, p)$ olur. p, $[G : K]$ indeksini bölmediğinden $|S_0| \neq 0$ olur. O halde $xK \in S_0$ vardır. Bu takdirde

$$\begin{aligned} xK \in S_0 &\Leftrightarrow hxK = xK, \quad \forall h \in H \\ &\Leftrightarrow x^{-1}hxK = K, \quad \forall h \in H \\ &\Leftrightarrow x^{-1}Hx < K, \\ &\Leftrightarrow H < xKx^{-1} \end{aligned}$$

olur.

Şimdi K ve K', G grubunun herhangi iki Sylow p - alt grubu olsun. Teoremin birinci kısmının ispatından dolayı K' bir p - alt grubu olarak K alt grubunun bir xKx^{-1} konjügesinde ihtiva edilir. $|K| = |K'| = |xKx^{-1}|$ olduğundan $K' = xKx^{-1}$ olur.

Teorem 3.1.10 (III. Sylow Teoremi): $|G| < \infty$ bir grup ve p asal sayı olsun. G grubunun Sylow p-alt grublarının sayısını S_p ile gösterilirse, $S_p \mid |G|$ ve $S_p \equiv 1 (\mathrm{mod}\, p)$ dir.

İspat: İkinci Sylow Teoreminden dolayı G grubunun Sylow p - alt gruplarının sayısı bunlardan her hangi birinin, örneğin P nin eşleniklerinin sayısına eşittir. Bu sayı $[G : N_G(P)]$ olup , $|G|$ yi böler. G grubunun bütün Sylow p - alt gruplarının kümesini S ile gösterelim. Bu takdirde $P \times S \to S, (g, Q) \to gQg^{-1}$ eşlenik olma etkisi ile S bir P - kümesidir. $S_0 = \{Q \in s : xQx^{-1}, \forall x \in P\}$ denirse $Q \in S_0$ olması için gerek ve yeter şart her $x \in P$ için $xQx^{-1} = Q$ olmasıdır. Halbuki $xQx^{-1} = Q$ olması için gerek ve yeter $P < N_G(Q)$ olmasıdır. P ve Q nun her ikisi de G grubunun ve böylece $N_G(Q)$ nun Sylow p - alt grupları olduğu için onlar $N_G(Q)$ da eşleniktir. $Q, N_G(Q)$ da normal olduğu için bu durum $P = Q$ olması ile mümkündür. Dolayısıyla $S_0 = \{P\}$ yani $|S_0| = 1$ dir. Teorem 3.1.6 dan dolayı $|S| \equiv 1(\operatorname{mod} p)$ ve buradan $|S| = s_p = kp + 1$ elde edilir.

Örnek 3.1.2: Mertebesi 15 olan bir grubun basit olup olmadığını araştıralım.
Bunun için önce 15 sayısının asal çarpanlarını bulmalıyız. 3 ve 5, 15 sayısın asal çarpanlarıdır. Buna göre Sylow 3 ve Sylow 5- alt grupları vardır. $S_3 \equiv 1(\operatorname{mod} 3)$ ve $S_5 \equiv 1(\operatorname{mod} 5)$ olduğundan Sylow 3 ve Sylow 5- alt gruplarının sayısı 1 er tanedir. Dolayısıyla bunlar normaldir. Öyle ise 15. mertebeden verilen bu grup basit değildir.

Tanım 3.1.5: G bir p - grup olsun. Her bir n doğal sayısı için

$$\Omega_n(G) = \left\langle x : x \in G, x^{p^n} = e \right\rangle, \quad \mho_n(G) = \left\langle y^{p^n} : y \in G \right\rangle$$

olarak tanımlanır. $\mho_n(G)$ alt grubu G grubunun **agemo alt grubu** olarak adlandırılır (Suzuki 1985).

Tanım 3.1.6: G bir p - grup olsun. Eğer herhangi iki $x, y \in G$ elemanları için

$$x^p y^p = (xy)^p c$$

olacak şekilde $\mho_1(H')$ $\left(H = \langle x, y \rangle\right)$ nün bir c elemanı varsa G ye **regüler p - grup** denir (Suzuki 1985).

Örnek 3.1.3: $D_4=\left\{e,x,x^2,x^3,y,xy,x^2y,x^3y\right\}$ $\left(x^4=e=y^2, yx=x^3y\right)$ ve $H=\left\{e,x^2,y,x^2y\right\}$ olacak şekilde $H\leq G$ olsun. Bu durumda

$$\left[e,x^2\right]=e,\ \left[e,y\right]=e,\ \left[e,x^2y\right]=e$$

$$\left[x^2,x^2\right]=e, \left[y,y\right]=e,\ \left[x^2y,x^2y\right]=e$$

$$\begin{aligned}\left[x^2,y\right]&=x^{-2}y^{-1}x^2y\\ &=x^{-2}\underline{yx}xy\\ &=x^{-2}x^3\underline{yx}y\\ &=xx^3yy\\ &=e\end{aligned}$$

$$\begin{aligned}\left[x^2,x^2y\right]&=x^{-2}y^{-1}x^{-2}x^2x^2y\\ &=x^{-2}\underline{yx}xy\\ &=x^{-2}x^3\underline{yx}y\\ &=xx^3yy\\ &=e\end{aligned}$$

$$\begin{aligned}\left[y,x^2y\right]&=y^{-1}y^{-1}x^{-2}yx^2y\\ &=x^{-2}\underline{yx}xy\\ &=x^{-2}x^3\underline{yx}y\\ &=xx^3yy\\ &=e\end{aligned}$$

olur. Yani $H^{'}=\left\{e\right\}$ komutatör alt grubu elde edilir. $\mho_1\left(H^{'}\right)=\left\langle a^2 : a\in H^{'}\right\rangle$ grubunun

$$\begin{aligned}x^2y^2&=x\underline{xy}y\\ &=xyx^3y\\ &=xyx^2\underline{xy}\\ &=xyx^2yx^3\\ &=xyx\underline{xy}x^3\\ &=xyxyx^3x^3\\ &=\left(xy\right)^2x^2\\ &=\left(xy\right)^2\left[x,y\right]\end{aligned}$$

olacak şekilde $\left[x, y\right] \in \mho_1\left(H^{'}\right)$ bulunur. Böylece D_4 grubu bir regüler p - gruptur.

Teorem 3.1.11: G bir regüler p - grup olsun. $x, y \in G$ için

$$x^{p^n} = y^{p^n} \Leftrightarrow \left(x^{-1}y\right)^{p^n} = e$$

dir (Suzuki 1985).

İspat: İspat tümevarımla yapılacaktır. $\left(R_n\right)$ önermesi

$$\left(R_n\right): x^{p^n} = y^{p^n} \Rightarrow \left(x^{-1}y\right)^{p^n} = e$$

olsun.

a) $\left(R_1\right)$ sağlar.

İspat: $x^p = y^p$ olsun. $G = \left\langle x, y\right\rangle$ ve abelyen olmayan bir grup olsun. M de G grubunun maksimal bir alt grubu olsun. $x^p = y^p$ olduğundan

$$e = y^{-p}y^{-1}y^{p}y = x^{-p}y^{-1}x^{p}y = x^{-p}\left(x^{p}\right)^{y} = x^{-p}\left(x^{y}\right)^{p}$$

yazılabilir. Böylece

$$e = x^{-p}\left(x^{y}\right)^{p} \Rightarrow x^{p} = \left(x^{y}\right)^{p}$$

olacak şekilde x ve x^y, M nin iki elemanıdır. $\left(R_1\right), M$ de sağlar. Bundan dolayı

$$\left(x^{-1}x^{y}\right)^{p} = e$$

yazılır. Bu bize $\left\|\left[x, y\right]\right\| = p$ olduğunu gösterir. $G = \left\langle x, y\right\rangle$ olduğundan, $G^{'}$ türetilmiş grubu, $\left[x, y\right]$ ve onun konjugeleri tarafından gerilir. Üstelik $\left(R_1\right), M$ de sağlandığından $G^{'}$ grubunun her elemanın mertebesi p dir. Özellikle $\mho_1\left(G^{'}\right) = \left\{e\right\}$ dir. G regüler olduğundan

$$x^{-p}y^{p} = \left(x^{-1}y\right)^{p}.c,\ c \in \mho_1\left(G^{'}\right)$$

yazılır. O zaman $c=e$ ve $\left(x^{-1}y\right)^{p}=x^{-p}y^{p}=e$ olur. Bu $\left(R_1\right)$ in G grubunda sağlandığını gösterir.

b) $\left(R_{n-1}\right)+\left(R_1\right)\Rightarrow\left(R_n\right)$

İspat: $x^{p^n}=y^{p^n}$ olsun. $\left(R_{n-1}\right)$ den $\left(x^{-p}y^{p}\right)^{p^{n-1}}=e$ yazılabilir. Bu $x^{-p}y^{p}$ elemanının $\Omega_{n-1}\left(G\right)$ alt grubuna ait olduğu anlamına gelir. G regüler olduğundan $\left(x^{-1}y\right)^{p}\in\Omega_{n-1}$ yazılır. $\left(R_{n-1}\right)$ sağlandığından, $\Omega_{n-1}\left(G\right)$ en çok p^{n-1} mertebeli elemanlardan oluşur. Bundan dolayı

$$\left(\left(x^{-1}y\right)^{p}\right)^{p^{n-1}}=\left(x^{-1}y\right)^{p^n}=e$$

elde edilir. Böylece $\left(R_n\right),G$ grubunda sağlanır.

$\left(S_n\right)$ önermesi

$$\left(S_n\right):\left(x^{-1}y\right)^{p^n}=e\Rightarrow x^{p^n}=y^{p^n}$$

olsun. İlk olarak $\left(S_1\right)$ in sağlandığını gösterelim. $\left(x^{-1}y\right)^{p}=e$ olsun.

$$\left(xy^{-1}\right)^{-p}=\left(yy^{-1}xy^{-1}\right)^{-p}=\left(yx^{-1}yy^{-1}\right)^{p}=y\left(x^{-1}y\right)^{p}y^{-1}=e$$

yazılabilir. Bundan dolayı $\left(R_1\right)$ den

$$\left(x^{-1}y\right)^{p}=\left(xy^{-1}\right)^{p}\Rightarrow\left(xy^{-1}x^{-1}y\right)^{p}=\left[x^{-1},y\right]^{p}=e$$

elde edilir. G regüler olduğundan

$$x^{-p}y^{p}=\left(x^{-1}y\right)^{p}=e$$

yazılır. Bu $\left(S_1\right)$ in sağlandığını gösterir.

c) $\left(S_{n-1}\right)+\left(S_1\right)\Rightarrow\left(S_n\right)$

İspat: $\left(x^{-1}y\right)^{p^n}=e$ olsun. O zaman $\left(x^{-1}y\right)^p\in\Omega_{n-1}\left(G\right)$ olur. $\Omega_{n-1}\left(G\right)$ en çok p^{n-1} mertebeli elemanlardan oluşur. Bundan dolayı

$$\left(x^{-p}y^p\right)^{p^{n-1}}=e$$

ve $\left(S_{n-1}\right)$ den

$$\left(x^p\right)^{p^{n-1}}=\left(y^p\right)^{p^{n-1}}$$

yazılır. Böylece $\left(S_n\right)$, G grubunda sağlanır.

Örnek 3.1.4: D_4 bir regüler p-grup olsun. $x,y\in D_4$ için

$$\begin{aligned}
x^4=y^4 &\Leftrightarrow e=x^{-4}y^4\\
&\Leftrightarrow e=x^{-1}\underline{xy}y^3\\
&\Leftrightarrow e=x^{-1}y\underline{x^3y^3}\\
&\Leftrightarrow e=x^{-1}yx^{-1}yy^2\\
&\Leftrightarrow e=x^{-1}yx^{-1}yx^{-1}\underline{xy}y\\
&\Leftrightarrow e=x^{-1}yx^{-1}yx^{-1}y\underline{x^3}y\\
&\Leftrightarrow e=x^{-1}yx^{-1}yx^{-1}yx^{-1}y\\
&\Leftrightarrow e=\left(x^{-1}y\right)^4
\end{aligned}$$

olarak bulunur.

Teorem 3.1.12: G**,** p^n mertebeli sonlu bir grup olsun. (p asal ve $n>0$) Bu durumda

i. G grubunun aşikar olmayan her hangi bir N normal alt grubu için**,** $Z\left(G\right)\cap N$ aşikar değildir.

ii. H,G grubunun bir has alt grubu ise, o zaman H tamamen $N(H)$ da kapsanır. Bu yüzden H , p^{n-1} mertebeli alt grup ise $H\lhd G$ olur.

İspat: i.

$$G = Z(G) \cup \left(\bigcup_{x \in C} C(x) \right), \quad N = G \cap N = Z(G) \cap N \cup \left(\bigcup_{x \in C} C(x) \cap N \right)$$
$$|N| = |Z(G) \cap N| + \sum_{x \in C} |C(x) \cap N| \qquad (1)$$

ve $x \in N$ ise $C(x) \subset N$ olur. $\forall x \in C$ için $C(x) \cap N$ ya boştur ya da $C(x)$ olur. Bu durumda

$$|C(x) \cap N| = 0 \;\; ya\, da \; |C(x) \cap N| = [G : N(x)]$$

olur. Bu yüzden

$$p \Big| \sum_{x \in C} |C(x) \cap N|$$

olur. $p \big| |N|$ olduğundan ve (1) eşitliğinden $p \big| |Z(G) \cap N|$ olur. Bu da $Z(G) \cap N$ nin aşikar olmadığını gösterir.

ii. $K \subset H$ ve K, G grubunun maksimal alt grubu olsun. O zaman G/K bölüm grubu, bazı $r > 0$ için p^r mertebelidir.

Bu yüzden (i) den G/K, aşikar olmayan bir merkeze sahiptir. Bu merkez L/K şeklinde olsun. $L/K \lhd G/K$ olduğundan $L \lhd G$ olur. $L \not\subset H, K \subseteq H$ ve K maksimal olduğundan $K \subsetneq L$ olur. $h \in H$ ve $l \in L$ olsun. L/K, G/K bölüm grubun merkezi olduğundan

$$(hK)(lK) = (lK)(hK)$$

olur. Bu yüzden $l^{'}hl \in hK \subset H$ olur. Bu takdirde $L \subset N(H)$ olur. Bu $H \neq N(H)$ olduğunu ifade eder ve $H \subset N(H)$ yazılır. $|H| = p^{n-1}$ ise o zaman

$$|N(H)| = |G| = p^n$$

olmalıdır. Dolayısıyla $H \lhd G$ olur.

Teorem 3.1.13: p asal sayı olmak üzere, p mertebeli sonlu bir grup devirlidir (Bayraktar 1988).

Tanım 3.1.7: G bir grup olsun. G grubunun $\mathrm{Z}_0(G), \mathrm{Z}_1(G), \mathrm{Z}_2(G), \ldots$ biçimindeki alt gruplarının

$$\{e\} = \mathrm{Z}_0(G) \subseteq \mathrm{Z}_1(G) \subseteq \mathrm{Z}_2(G) \subseteq \ldots$$

serisine, G grubunun **üst merkez serileri** adı verilir.

Teorem 3.1.14: G**,** sonlu bir p -grup olsun. Bu durumda G grubu bir nilpotenttir.

İspat: Eğer $G = \{e\}$ ise, G grubunun nilpotent olduğu aşikardır. $G \neq \{e\}$ olsun. Bu durumda Teorem 3.1.3 e göre, $\mathrm{Z}_1(G) = \mathrm{Z}(G) \neq \{e\}$ olur. $G/Z_1(G) \neq \{e\}$ ise, yine Teorem 3.1.3 e göre, $G/Z_1(G) = Z_2(G)/Z_1(G) \neq Z_1(G)/Z_1(G)$ olur. $Z_1(G) \neq G$ ise, $Z_2(G) \neq Z_1(G)$ olur. Benzer olarak, $G \neq Z_2(G)$ ise $Z_3(G) \neq Z_2(G)$ olur. Tüme varımla, $Z_i(G) \neq G$ ise, $Z_{i+1}(G) \neq Z_i(G)$ elde edilir. Böylece

$$\{e\} = \mathrm{Z}_0(G) \subseteq \mathrm{Z}_1(G) \subseteq \ldots \subseteq \mathrm{Z}_i(G) \subseteq \mathrm{Z}_{i+1}(G)$$

yazılır. G grubu sonlu olduğundan, bazı k tam sayıları için, $Z_k(G) = G$ olur.
Buradan

$$\{e\} = \mathrm{Z}_0(G) \subseteq \mathrm{Z}_1(G) \subseteq \ldots \subseteq \mathrm{Z}_k(G) = G$$

yazılır. Yani, G grubu nilpotenttir.

Örnek 3.1.5: p asal bir sayı olsun. G, mertebesi p^3 olan ve abelyen olmayan bir grup ise, $\mathrm{Z}_2(G) = G$ olur.

Çözüm: $|G| = p^3$ olsun. Bu durumda Teorem 3.1.14 e göre, $Z_1(G) = Z(G) \neq \{e\}$ biçimindedir. Böylece $Z_1(G) \neq G$ ise, $G/Z_1(G)$ bölümünün mertebesi p veya p^2 sayılarıdır. Burada " G bir grup ve $S \leq Z(G)$ olsun. G/S devirliyse, G grubu değişmelidir." ifadesine göre, yalnız $Z_1(G) = G$ için $G/Z_1(G)$ bölümü devirli olduğundan, mertebesi p^2 olan
$G/Z_1(G)$ bölüm grubu bulunur. Böylece, $G/Z_1(G)$ bölüm grubu değişmelidir. Bu takdirde, $G/Z_1(G) = Z_2(G)/Z_1(G)$ olup, $Z_2(G) = G$ yazılır.

Örnek 3.1.6: D_n**,** mertebesi $2n$ olan bir dihedral grubu olsun. Eğer n sayısı 2 sayısının bir kuvveti ise, yani $n = 2^r$ şeklindeyse, D_n grubu bir nilpotenttir. Fakat A_4 alterne grubu bir nilpotent değildir.

Çözüm: $|D_n| = 2^r$ şeklinde olsun. Bu durumda D_n grubu bir p-gruptur. Teorem 3.1.14 e göre D_n grubu bir nilpotenttir.
Öte yandan, A_4 alterne grubunda, $Z_1(A_4) = \{e\}$ biçimindedir. Böylece, $Z_1(A_4) = Z_2(A_4) = Z_3(A_4) = \ldots$ olur. Buradan, her n tam sayısı için, $Z_n(A_4) \neq A_4$ olduğu için, A_4 alterne grubu bir nilpotent değildir.

Tanım 3.1.8: $H_i \leq H_{i+1}, H_i \lhd H_{i+1}, H_0 = \{e\}$ ve $H_n = G$ olacak biçimde G grubunun $H_{0,} H_1, \ldots, H_n$ şeklinde sonlu sayıdaki alt gruplarının dizisine, G grubunun **alt normal** veya **alt invaryant serisi** denir. $H_i \leq H_{i+1}, H_0 = \{e\}$ ve $H_n = G$ olacak şekilde G grubunun $H_{0,} H_1, \ldots, H_n$ şeklinde sonlu sayıdaki alt gruplarının dizisine, G grubunun **normal serisi** adı verilir.

Örneğin; Z tam sayılar kümesinin normal iki serisi

$$\{0\} \leq 8Z \leq 4Z \leq 2Z \leq Z \text{ ve } \{0\} \leq 9Z \leq Z$$

biçimindedir. Öte yandan, karenin tüm simetrilerinden oluşan D_4 dihedral grubunun

$$I=\begin{pmatrix}1234\\1234\end{pmatrix}, d_1=\begin{pmatrix}1234\\3412\end{pmatrix}, d_2=\begin{pmatrix}1234\\2143\end{pmatrix} \text{ ve } d_3=\begin{pmatrix}1234\\4321\end{pmatrix}$$

elemanları için, $\{I\}\leq\{I,d_2\}\leq\{I,d_1,d_2,d_3\}\leq D_4$ dizisi, alt normal bir seridir. $\{I,d_2\}$ alt grubu D_4 dihedral grubunda normal olmadığı için, bu dizi normal bir seri değildir.

Tanım 3.1.9: Eğer her bir H_i grubu K_j gruplarının birinde ise, yani $\{H_i\}\subseteq\{K_j\}$ ise, $\{K_j\}$ alt normal (veya normal) serisine, G grubunun $\{H_i\}$ alt normal (veya normal) serisinin bir **incesidir** denir.

Tanım 3.1.10: Tüm H_{i+1}/H_i bölüm grupları basit olan G grubunun $\{H_i\}$ alt normal serisine **bileşim serisi** denir. Tüm H_{i+1}/H_i bölüm grupları basit olan G grubunun $\{H_i\}$ normal serisine de **baş seri** adı verilir.

Tanım 3.1.11: Tüm H_{i+1}/H_i bölüm grupları abelyen olan G grubunun $\{H_i\}$ bileşim serisi varsa, G grubuna **çözülebilirdir** denir.

Örnek 3.1.7: p ve q asal sayıları için, mertebeleri p^2, pq veya p^2q olan tüm G grupları çözülebilir.

Çözüm: $|G|=p^2$ ise, G grubu abelyendir. Her sonlu abelyen grup çözülebilir olduğundan, G grubu çözülebilir.
$|G|=pq$ ise, $p<q$ için G grubunun q mertebeli sadece bir tane H alt grubu vardır. Bu alt grup tek olduğundan G grubunun normal alt grubu olur. Buna göre $|G/H|=p$ olur. Böylece G/H bölüm grubu abelyendir. $|H|=q$ olduğundan H grubu da abelyen olur. Böylece, bölüm grupları abelyen olan alt normal seri,

$$\{e\} \subseteq H \subseteq G$$

biçimindedir. Bu da, G grubunun çözülebilir olmasını verir.

$|G| = p^2 q$ ise, $s_p = (1+kp) \mid p^2 q$ olur. Buna göre $1+kp=1$ veya $1+kp=q$ olmalıdır. $1+kp=1$ ise, $H \lhd G$ olur. Buradan, G/H ve $H/\{e\}$ bölüm grupları abelyen olan alt normal serisi, $\{e\} \subseteq H \subseteq G$ biçiminde olduğu için, G grubu çözülebilir.

4. ARAŞTIRMA ve BULGULAR

Bu bölümde p - grupların sınıflandırılması üzerinde duruldu.

4.1. Bazı Teoremler

Teorem 4.1.1: G, $g = p^n$ mertebeden bir p - grup olsun. G grubunun abelyen olmadığını ve bir M maksimal devirli alt gruba sahip olduğunu varsayalım. $n \geq 3$ ve p tek ise, G grubu, aşağıda takdimi verilen $M\left(p^n\right)$ grubuna izomorftur.

$$M\left(p^n\right) = \left\langle x, y : x^{pq} = y^p = e, y^{-1}xy = x^{1+q} \right\rangle, \qquad q = p^{n-2}$$

Eğer $p = 2$ ise;

$$G \cong M(2^n) = \left\langle x, y : x^{2q} = y^2 = e, y^{-1}xy = x^{1+q} \right\rangle, \qquad q = 2^{n-2}$$

veya

$$G \cong Q_{2^n} = \left\langle x, y : x^{2^{n-1}} = e, y^2 = x^{2^{n-2}}, y^{-1}xy = x^{-1} \right\rangle$$

veya

$$G \cong D_{2^{n-1}}\,(Dihedral\ \ grup) = \left\langle x, y : x^{2^{n-1}} = y^2 = e, y^{-1}xy = x^{-1} \right\rangle$$

veya takdimi aşağıda verilen S_g grubuna izomorftur.

$$S_g = \left\langle x, y : x^{2a} = y^2 = e,\ y^{-1}xy = x^{-1+a} \right\rangle, \quad a = 2^{n-2}\ , \quad n \geq 4$$

İspat: (a) x, M devirli grubunun bir gereni ve y, $G = \langle x, y \rangle$ olacak şekilde bir eleman olsun. M, G grubunun maksimal alt grubu olduğundan M, G grubunun Sylow p - alt grubudur. Böylece I.Sylow teoreminden $M \lhd G$ dir ve $|G : M| = p$ dir.

$$\left|G:M\right| = p \Rightarrow \ \left|G:M\right| = \frac{|G|}{|M|} = p$$
$$\Rightarrow \ \frac{p^n}{|M|} = p$$
$$\Rightarrow \ |M| = p^{n-1}$$

Bu durumda

$$x^{pq} = e \qquad \left(q = p^{n-2}\right), \ y^{-1}xy = x^r, \quad y^p \in M$$

olur. G abelyen olmadığından yani; $xy = yx$ olmadığından r ,

$$r \not\equiv 1(\text{mod } p^{n-1})$$

denkliğini sağlar.

Gerçekten eğer $r \equiv 1(\text{mod } p^{n-1})$ olsaydı o zaman ; $r = \alpha p^{n-1} + 1$ olarak yazılabilir.

Buna göre;

$$y^{-1}xy = x^{\alpha p^{n-1}+1} = x \Rightarrow xy = yx$$

olurdu. Bu G grubunun abelyen olmaması ile çelişkilidir. Bu çelişki $r \equiv 1(\text{mod } p^{n-1})$ alınmasından kaynaklandı. Dolayısıyla

$$r \not\equiv 1(\text{mod } p^{n-1})$$

dir. y^p , M nin bir gereni olmadığından

$$y^p = x^{sp}$$

dir. Şimdi x^{r^i} yi bulalım.

$$\begin{aligned} x^{r^i} = \left(x^r\right)^{r^{i-1}} = \left(y^{-1}xy\right)^{r^{i-1}} &= \underbrace{y^{-1}xyy^{-1}xy...y^{-1}xy}_{r^{i-1}} \\ &= y^{-1}x^{r^{i-1}}y \\ &= y^{-1}(y^{-1}xy)^{r^{i-2}}y \\ &= y^{-1}\underbrace{y^{-1}xyy^{-1}xy...y^{-1}xy}_{r^{i-2}}y \\ &= y^{-2}x^{r^{i-2}}y^2 \\ &\ \vdots \\ &= y^{-i}xy^i \end{aligned}$$

olarak bulunur.

Buna göre

$$x^{r^p} = y^{-p}xy^p = x^{-sp}xx^{sp} = x \Rightarrow r^p = \alpha p^{n-1} + 1$$
$$\Rightarrow r^p \equiv 1(\text{mod } p^{n-1})$$

olarak bulunur.

(b) p tek olsun. Fermat teoreminden

$$r^{p-1}r = 1 + \alpha p^{n-1} \quad \text{ve} \quad r^{p-1} = 1 + \beta p$$
$$r = 1 + kp^{\lambda} \qquad \left(k, p\right) = 1, \quad \lambda \geq 1$$

yazılır.

Binom teoreminden

$$r^p = \left(1 + kp^{\lambda}\right)^p = \binom{p}{0}(kp^{\lambda})^0 + \binom{p}{1}(kp^{\lambda}) + \binom{p}{2}(kp^{\lambda})^2 + \ldots + \binom{p}{p}(kp^{\lambda})^p$$
$$\Rightarrow r^p \equiv 1 + kp^{\lambda+1}(\text{mod } p^{\lambda+2})$$

olarak yazılır. $r^p \equiv 1 \not\equiv r(\text{mod } p^{n-1})$ olduğundan $\lambda = n-2$ dir. $ik \equiv 1(\text{mod } p)$ olacak şekilde bir i tam sayısı ve y^i yerine y seçilir. Bu takdirde

$$y^{-1}xy = x^r \ , \quad r = 1 + p^{n-2} = 1 + q$$

olur.

Böylece

$$y^{-1}xy = x^{1+p^{n-2}} \Rightarrow x^{-1}y^{-1}xy = x^{p^{n-2}}$$

olacak şekilde $\left[x, y\right]$ komutatörü vardır. Dolayısıyla reguler p-grubun tanımından G bir reguler p - gruptur.

Bu durumda

$$y^p = x^{sp} \Rightarrow (x^{-s}y)^p = e$$

olur. Son olarak $x^{-s}y$ nin yerine y seçilirse

$$G \cong M(p^n) = \left\langle x, y : x^{pq} = y^p = e, \ y^{-1}xy = x^{1+q} \right\rangle$$

elde edilir.

(c) $p=2$ olsun. $g=2m=2^n$ dir. İlk olarak, eğer $G-M$ mertebesi 2 olmayan eleman içeriyorsa $G\cong Q_{2^n}$ olduğunu ispatlayacağız. (a) daki bağıntılardan

$$x^{2s}=y^2=y^{-1}x^{2s}y=x^{2sr}$$

yazılır. Bu takdirde

$$\begin{aligned} x^{2s}=x^{2sr} \quad &\Rightarrow x^{2sr-2s}=e=x^{2^{n-1}}=x^m \\ &\Rightarrow 2(r-1)s\equiv 0(\mathrm{mod}\, m) \qquad (2) \end{aligned}$$

olarak bulunur. $M\lhd G$ olduğundan $x^{\lambda}y\not\in M$ dir.

$$\begin{aligned} \left(x^{\lambda}y\right)^2 &= x^{\lambda}y^2(y^{-1}x^{\lambda}y) \\ &= x^{\lambda}x^{2s}x^{r\lambda} \\ &= x^{\lambda(r+1)+2s} \end{aligned}$$

olur. $G-M$ nin mertebesi 2 olan elmanı olmadığını kabul ettiğimizden $x^{\lambda(r+1)+2s}\neq e$ olur.

Böylece

$$(r+1)\lambda+2s\equiv 0(\mathrm{mod}\, m) \qquad (3)$$

nin λ ya bağlı çözümü yoktur.

$$r+1=2^e r', \quad 2s=2^f s' \qquad (r'\,ve\;\; s'\;\; tek)$$

yazılır.

$f\geq 1$ dir. r' tek olduğundan,

$$r'\lambda'+s'\equiv 0(\mathrm{mod}\, m)$$

bir λ' çözüme sahiptir. Eğer $e\leq f$ ise, o zaman $2^{f-e}\lambda'=\lambda$ (3) yi sağlayacaktır. Bu bir çelişkidir. Bu çelişki $e\leq f$ alınmasından kaynaklandı. Öyle ise $e>f\geq 1$ dir. $4\,|\,r+1$ dir. Ancak $4\nmid r-1$ dir. (1) den $m\,|\,2(r-1)s$ olduğunu görmüştük. Buradan $f\geq n-2$ dir. $y^2\neq e$ kabul edilmesinden $f=n-2$ ve

$$y^2=x^{2s}=x^a \qquad (a=2^{n-2}),$$

dir. $r+1=2^e r'\equiv 0(\mathrm{mod}\, m)$ olduğundan $r=-1$ alınmalıdır. Böylece

$$G\cong Q_{2^n}=\left\langle x,y: x^{2^{n-1}}=e, y^2=x^{2^{n-2}}, y^{-1}xy=x^{-1}\right\rangle$$

olur.

(d) $y \notin M$ olacak şekilde $y^2 = e$ olsun. Buna göre

$$r \not\equiv 1(\bmod 2^{n-1}) \text{ ve } r^2 \equiv 1(\bmod 2^{n-1})$$

denklemlerinin çözümlerine bakılır. (a) dan hatırlanacağı gibi

$$r = 1 + 2^{\lambda} k \qquad (k \quad tek) \qquad \lambda \geq 2$$

idi. Bu takdirde

$$r^2 \equiv 1 + 2^{\lambda+1} k + 2^{2\lambda} k^2 \equiv 1(\bmod 2^{n-1})$$

olur. Buradan $\lambda + 1 \geq n - 1$ olur. Eğer $\lambda \geq n-1$ ise o zaman $r = -1$ dir ve

$$G \cong D_{2^{n-1}} = \left\langle x, y : x^{2^{n-1}} = y^2 = e, y^{-1}xy = x^{-1} \right\rangle$$

olur.Eğer $\lambda = n-2$ ise

$$r = -1 + 2^{n-2} \qquad n \geq 4$$

alınır ve böylece

$$G \cong S_g = \left\langle x, y : x^{2a} = y^2 = e,\ y^{-1}xy = x^{-1+a} \right\rangle, \quad a = 2^{n-2}$$

olur. Böylece ispat tamamlanmış olur.

Şimdi de $D_{2^{n-1}}$ grubu ile Q_{2^n} grubunun birbirlerine izomorf olmadıkları grup matrisleri yardımıyla gösterilecektir. Bunun için grup matrisleri ile ilgili bazı tanım ve teoremler verilecektir.

Tanım 4.1.1: G, n. mertebeden bir grup ve e, G grubunun birim elemanı olsun. g_k ile G grubundaki k mertebeli elemanları, g_{kj} ile de G grubundaki k mertebeli j. elemanı tanımlansın. Eğer $\theta = \left\{a_{ij}\right\}_{n \times n}$ matrisi

$$a_{11} = e,\ a_{12} = a_{13} = a_{14} = \ldots = a_{1n} = a_{21} = a_{31} = \ldots = a_{n1} = 0$$

ve

$$g_{kj} = a_{k(j+1)},\ 1 \leq j \leq n-1, 2 \leq k \leq n$$

elemanlarından oluşuyorsa, o zaman θ matrisine G grubunun **grup matrisi** denir ve θ_G ile gösterilir.

Örnek 4.1.1: Klein 4-grubu verilsin.

$$V = \{e, x, y, xy\}, x^2 = y^2 = (xy)^2 = e$$

için tanım 4.1.1 uygulanırsa

$$\begin{array}{lll} a_{11} = e, a_{12} = a_{13} = a_{14} = a_{21} = a_{31} = a_{41} = 0 & & \\ g_{21} = a_{22} = x & g_{22} = a_{23} = y & g_{23} = a_{24} = xy \\ g_{31} = a_{32} = 0 & g_{32} = a_{33} = 0 & g_{33} = a_{34} = 0 \\ g_{41} = a_{42} = 0 & g_{42} = a_{43} = 0 & g_{43} = a_{44} = 0 \end{array}$$

elemanlar elde edilir. Böylece

$$\theta_V = \begin{bmatrix} e & 0 & 0 & 0 \\ 0 & x & y & xy \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{4\times 4}$$

şeklinde Klein 4-grubunun grup matrisi elde edilir.

Tanım 4.1.2: G ve H, *n.* mertebeden iki grup olsun. θ_G ve θ_H sırasıyla G ve H gruplarının grup matrisleri olsun. Eğer her $1 \le i \le n$ için θ_G ve θ_H grup matrislerinin *i.* satırları aynı sayıda sıfırdan farklı elemanlara sahip ise, o zaman bu **matrisler denktir** denir ve $\theta_G \approx \theta_H$ ile gösterilir

Örnek 4.1.2: $\mathrm{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ grubu verilsin.

$$\begin{array}{lll} a_{11} = \overline{0}, a_{12} = a_{13} = a_{14} = a_{21} = a_{31} = a_{41} = 0 & & \\ g_{21} = a_{22} = \overline{2} & g_{22} = a_{23} = 0 & g_{23} = a_{24} = 0 \\ g_{31} = a_{32} = 0 & g_{32} = a_{33} = 0 & g_{33} = a_{34} = 0 \\ g_{41} = a_{42} = \overline{1} & g_{42} = a_{43} = \overline{3} & g_{43} = a_{44} = 0 \end{array}$$

elemanları elde edilir. Böylece

$$\theta_{Z_4} = \begin{bmatrix} \bar{0} & 0 & 0 & 0 \\ 0 & \bar{2} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \bar{1} & \bar{3} & 0 \end{bmatrix}_{4\times 4}$$

grup matrisi elde edilir. Bu durumda örnek 4.1.1 deki θ_V ile θ_{Z_4} grup matrisleri denk matrisler değildir. Yani $\theta_V \not\approx \theta_{Z_4}$ olur.

Örnek 4.1.3: $K = \{1, -1, i, -i\}$ grubu verilsin.

$$\begin{aligned} &a_{11} = 1, a_{12} = a_{13} = a_{14} = a_{21} = a_{31} = a_{41} = 0 \\ &g_{21} = a_{22} = -1 \quad g_{22} = a_{23} = 0 \quad g_{23} = a_{24} = 0 \\ &g_{31} = a_{32} = 0 \quad g_{32} = a_{33} = 0 \quad g_{33} = a_{34} = 0 \\ &g_{41} = a_{42} = i \quad g_{42} = a_{43} = -i \quad g_{43} = a_{44} = 0 \end{aligned}$$

elemanları elde edilir. Böylece

$$\theta_K = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & i & -i & 0 \end{bmatrix}_{4\times 4}$$

grup matrisi elde edilir. Buna göre örnek 4.1.2 de bulunan θ_{Z_4} matrisi ile θ_K matrisi birbirlerine denktirler. Yani $\theta_{Z_4} \approx \theta_K$ olur.

Teorem 4.1.2: G ve H, n. mertebeden iki grup olsun. θ_G ve θ_H da bu grupların grup matrisleri olsun. Bu durumda $G \cong H$ olması için gerek ve yeter şart $\theta_G \approx \theta_H$ olmasıdır.(Atagün,2005)

İspat: Eğer $G \cong H$ ise, o zaman bu grupların her ikisi de sayıları eşit olan, aynı mertebeden elemanlara sahiptirler. Böylece tanım 4.1.2 ye göre $\theta_G \approx \theta_H$ olur. Tersine eğer $\theta_G \approx \theta_H$ ise, o zaman elemanların mertebeleri kullanılarak G ve H nın elemanları arasında 1-1 benzerlik tanımlanabilir. Aynı sonlu mertebeden iki grubun arasında 1-1 homomorfizma olduğundan aynı zamanda örtendir. Böylece G ve H arasında 1-1 ve örten bir homomorfizma olduğundan $G \cong H$ yazılır.

Şimdi, $n \geq 3$ için

$$D_{2^{n-1}} = \left\langle r, s : r^{2^{n-1}} = s^2 = e, srs^{-1} = r^{-1} \right\rangle \text{ve}\, Q_{2^n} = \left\langle x, y : x^{2^{n-1}} = y^4 = e, yxy^{-1} = x^{-1}, x^{2^{n-2}} = y^2 \right\rangle$$

gruplarının birbirine izomorf olmadıklarını grup matrisleri yardımıyla aşağıdaki gibi gösterebiliriz.

$n = 3$ için;

$$D_4 = \left\{e, r, r^2, r^3, s, rs, r^2s, r^3s\right\}$$
$$Q_8 = \left\{e, x, x^2, x^3, y, xy, x^2y, x^3y\right\}$$

şeklinde yazılır. Buna göre

$$|r| = 4, \left|r^2\right| = 2, \left|r^3\right| = 4, |s| = 2, |rs| = 2, \left|r^2s\right| = 2, \left|r^3s\right| = 2$$
$$|x| = 4, \left|x^2\right| = 2, \left|x^3\right| = 4, |y| = 4, |xy| = 4, \left|x^2y\right| = 4, \left|x^3y\right| = 4$$

elde edilir. Böylece

$$\theta_{D_4}=\begin{bmatrix} e & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & r^2 & s & rs & r^2s & r^3s & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & r & r^3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{2^3\times 2^3},\theta_{Q_8}=\begin{bmatrix} e & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x & x^3 & y & xy & x^2y & x^3y & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{2^3\times 2^3}$$

grup matrisleri bulunur. Buradan $\theta_{D_4} \not\approx \theta_{Q_8}$ olduğundan $D_4 \not\cong Q_8$ olduğu görülür.

$n=4$ için;

$$D_8=\{e,r,r^2,r^3,r^4,r^5,r^6,r^7,s,rs,r^2s,r^3s,r^4s,r^5s,r^6s,r^7s\}$$
$$Q_{16}=\{e,x,x^2,x^3,x^4,x^5,x^6,x^7,y,xy,x^2y,x^3y,x^4y,x^5y,x^6y,x^7y\}$$

şeklinde yazılır. Buna göre

$$|r|=8,|r^2|=4,|r^3|=8,|r^4|=2,|r^5|=8,|r^6|=4,|r^7|=8,|s|=2,|rs|=2,|r^2s|=2,|r^3s|=2,$$
$$|r^4s|=2,|r^5s|=2,|r^6s|=2,|r^7s|=2$$
$$|x|=8,|x^2|=4,|x^3|=8,|x^4|=2,|x^5|=8,|x^6|=4,|x^7|=8,|y|=4,|xy|=4,|x^2y|=4,|x^3y|=4$$
$$|x^4y|=4,|x^5y|=4,|x^6y|=4,|x^7y|=4$$

elde edilir. Böylece

$$\theta_{D_8}=\begin{bmatrix} e&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&r^4&s&rs&r^2s&r^3s&r^4s&r^5s&r^6s&r^7s&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&r^2&r^6&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&r&r^3&r^5&r^7&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{bmatrix}_{2^4\times 2^4}$$

ve

$$\theta_{Q_{16}}=\begin{bmatrix} e&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&x^4&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&x^2&x^6&y&xy&x^2y&x^3y&x^4y&x^5y&x^6y&x^7y&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&x&x^3&x^5&x^7&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{bmatrix}_{2^4\times 2^4}$$

şeklinde grup matrisleri bulunur. Buradan $\theta_{D_8} \not\approx \theta_{Q_{16}}$ olduğundan $D_8 \not\cong Q_{16}$ olduğu görülür. Bu şekilde devam edilirse

$$\theta_{D_{2^{n-1}}} = \begin{bmatrix}
e & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & r^{2^{n-2}} & s & rs & r^2 s & . & . & . & r^{2^{n-1}-1}s & 0 & . & . & . & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & r^{2^{n-3}} & r^{3.2^{n-3}} & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
0 & r & r^3 & r^5 & r^7 & . & . & . & r^{2^{n-1}-1} & 0 & . & . & . & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}_{2^n \times 2^n}$$

ve

$$\theta_{Q_{2^n}} = \begin{bmatrix} e & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x^{2^{n-2}} & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & . & . & . & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & . & . & . & 0 \\ 0 & x^{2^{n-3}} & x^{3.2^{n-3}} & y & xy & x^2y & . & . & . & x^{2^{n-1}-1}y & 0 & 0 & . & . & . & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ 0 & x & x^3 & x^5 & x^7 & . & . & . & x^{2^{n-1}-1} & 0 & 0 & 0 & . & . & . & 0 \\ 0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{2^n \times 2^n}$$

şeklinde grup matrisler bulunur. Buradan $\theta_{D_{2^{n-1}}} \not\approx \theta_{Q_{2^n}}$ olduğundan $D_{2^{n-1}} \ncong Q_{2^n}$ olduğu görülür.

Teorem 4.1.3: İndeksi p olan devirli bir alt grup içeren, p^n mertebeli gruplar aşağıda verilen tiplerden biridir.

Abelyen olanlar;

$n \geq 1$, devirli;

1) $a^{p^n} = e$

$n \geq 2$;

2) $a^{p^{n-1}} = e$, $b^p = e$, $ba = ab$

Abelyen olmayanlar;

p tek asal sayı, $n \geq 3$;

3) $a^{p^{n-1}} = e$, $b^p = e$, $ba = a^{1+p^{n-2}}b$

$p = 2$, $n \geq 3$;

4) Genelleştirilmiş Quaternion grup

$a^{2^{n-1}} = e$, $b^2 = a^{2^{n-2}}$, $ba = a^{-1}b$

$p = 2$, $n \geq 3$;

5) Dihedral grup

$a^{2^{n-1}} = e$, $b^2 = e$, $ba = a^{-1}b$

$p = 2$, $n \geq 4$;

6) $a^{2^{n-1}} = e$, $b^2 = e$, $ba = a^{1+2^{n-2}}b$

$p = 2$, $n \geq 4$;

7) $a^{2^{n-1}} = e$, $b^2 = e$, $ba = a^{-1+2^{n-2}}b$

İspat: p^{n-1} mertebeli bir eleman içeren, p^n mertebeli abelyen bir grup, p^n veya p^{n-1} mertebeli bir elemana sahip olmalıdır. Bu takdirde teoremdeki 1) ve 2) tipleri sağlanır. Şimdi p^{n-1} mertebeli bir eleman içeren p^n mertebeli abelyen olmayan grupları ele alalım. İlk olarak p tek asal sayı olsun. $a^{p^{n-1}} = e$ ise, o zaman $\langle a \rangle$, indeksi p olan normal bir alt gruptur. $b \notin \langle a \rangle$ için

$$r \not\equiv 1(\bmod p^{n-1}) \quad , \quad bab^{-1} = a^r$$

yazılır. Çünkü grubumuz abelyen değildir.

Şimdi de a^{r^i} yi araştıralım.

$$
\begin{aligned}
a^{r^i} = \left(a^r\right)^{r^{i-1}} = \left(bab^{-1}\right)^{r^{i-1}} = \underbrace{bab^{-1}bab^{-1}...bab^{-1}bab^{-1}}_{r^{i-1}} = ba^{r^{i-1}}b^{-1} = b\left(a^r\right)^{r^{i-2}}b^{-1} = b\left(bab^{-1}\right)^{r^{i-2}}b^{-1} \\
= b\,\underbrace{bab^{-1}bab^{-1}...bab^{-1}bab^{-1}}_{r^{i-2}}\,b^{-1} = b^2a^{r^{i-2}}b^{-2} \\
\vdots \\
= b^iab^{-i}
\end{aligned}
$$

olarak bulunur. $b^p \in \langle a \rangle$ için

$$a^{r^p} = b^pab^{-p} = a^{sp}aa^{-sp} = a \quad \text{ve} \quad r^p \equiv 1(\text{mod } p^{n-1})$$

yazılır. p asal sayısı tek olduğundan

$$r \equiv 1 + kp^{n-2}\left(\text{mod } p^{n-1}\right), \quad k \not\equiv 0(\text{mod } p) \;\; , \quad r \not\equiv 1(\text{mod } p^{n-1})$$

şeklinde yazılır. $ik \equiv 1(\text{mod } p)$ olacak şekilde $b_1 = b^i$ alınırsa

$$r^i \equiv (1+kp^{n-2})^i = 1 + ikp^{n-2} \equiv 1 + p^{n-2}(\text{mod } p^{n-1})$$

elde edilir. Bu durumda

$$b_1ab_1^{-1} = b^iab^{-i} = a^{r^i} = a^{1+p^{n-2}} \qquad (4)$$

olur. $h = 1 + p^{n-2}$ olsun. O zaman

$$
\begin{aligned}
(a^ib_1)^2 &= a^ib_1a^ib_1 \\
&= a^i(b_1a^ib_1^{-1})b_1^2
\end{aligned}
$$

olarak bulunur. (4) deki ifadeden

$$
\begin{aligned}
(a^ib_1)^2 &= a^ib_1a^ib_1 \\
&= a^i(b_1a^ib_1^{-1})b_1^2 \\
&= a^ia^{ir^i}b_1^2 \\
&= a^ia^{i(1+p^{n-2})}b_1^2 \\
&= a^ia^{ih}b_1^2
\end{aligned}
$$

elde edilir.

Bu ifade genelleştirilerek

$$(a^ib_1)^t = a^{iT}b^t \qquad , \quad T = 1 + h + ... + h^{t-1}$$

şeklinde yazılır. $t = p$ alınırsa

$$\begin{aligned} 1+h+\ldots+h^{p-1} &= 1+1+p^{n-2}+\ldots+(1+p^{n-2})^{p-1} \\ &\equiv p+p^{n-2}\left[1+2+3+\ldots+(p-1)\right](\operatorname{mod} p^{n-1}) \\ &\equiv p+p^{n-1}\frac{(p-1)}{2} \equiv p(\operatorname{mod} p^{n-1}) \end{aligned}$$

olarak bulunur. Böylece

$$\left(a^i b_1\right)^p = a^{ip} b_1{}^p$$

olur. $b_1{}^p = a^u \in \langle a \rangle$, $u = pv$ olsun. $b_2 = a^{-v} b_1$ ise, o zaman

$$\begin{aligned} b_2{}^p = \left(a^{-v} b_1\right)^p &= a^{-vp} b_1{}^p \\ &= a^{-vp} a^{vp} \\ &= e \end{aligned}$$

ve

$$\begin{aligned} b_2 a b_2{}^{-1} &= (a^{-v} b_1) a (a^{-v} b_1)^{-1} \\ &= a^{-v} (b_1 a b_1{}^{-1}) a^v \\ &= a^{-v} a^{1+p^{n-2}} a^v \\ &= a^{1+p^{n-2}} \end{aligned}$$

olarak bulunur. a ve b_2 elemanları, teoremin 3). maddesindeki durumu sağlamış olur.

Şimdi $p = 2$ ve $a^{2^{n-1}} = e,\ b \notin \langle a \rangle$ olsun. O zaman

$$bab^{-1} = a^r, \quad r^2 \equiv 1(\operatorname{mod} 2^{n-1}),\ r \not\equiv 1(\operatorname{mod} 2^{n-1})$$

olur. Buna göre $r = -1,\ r = 1 + 2^{n-2},\ \ r = -1 + 2^{n-2}$ olur.

$b^2 = a^w \in \langle a \rangle$ olsun. O zaman

$$\begin{aligned} b^2 &= b(b^2)b^{-1} \\ &= ba^w b^{-1} \\ &= a^{rw} \end{aligned}$$

olduğundan $a^{rw} = a^w$ veya $wr \equiv w(\operatorname{mod} 2^{n-1})$ elde edilir.

$r = -1$ için

$$-w \equiv w(\operatorname{mod} 2^{n-1}), \quad a^w = 1 \text{ veya } a^w = a^{2^{n-2}}$$

olur. Bu durumda grubumuz ya

$$a^{2^{n-1}} = e, b^2 = e, ba = a^{-1}b \ (\textit{Dihedral grup})$$

ya da

$$a^{2^{n-1}}=1, b^2=a^{2^{n-2}}, ba=a^{-1}b \ (Genel\ Quaternion\ grup)$$

olur. Böylece teoremin 4). ve 5). maddeleri sağlanmış olur.

Şimdi $n \geq 4$, $ba=a^r b$ ve $r=1+2^{n-2}$ olsun. $b^2=a^w$ ise,

$$wr \equiv w(\mathrm{mod}\, 2^{n-2})$$

olur. Buna göre

$$2^{n-2}w \equiv 0(\mathrm{mod}\, 2^{n-1}) \text{ veya } w=2w_1$$

olur.

$i\left(1+2^{n-3}\right)+w_1 \equiv 0(\mathrm{mod}\, 2^{n-2})$ olacak şekilde bir i tanımlansın. Bu durumda $b_1=a^i b$ için

$$\begin{aligned} b_1^{\,2} &= a^i b a^i b \\ &= a^i(ba^i)b \\ &= a^i(a^{ir}b)b \\ &= a^{i(1+r)}b^2 \\ &= a^{i(2+2^{n-2})}a^{2w_1} \\ &= a^{2\left[i\left(1+2^{n-3}\right)+w_1\right]} \\ &= a^{2^{n-1}} \\ &= e \end{aligned}$$

olarak bulunur.

Böylece $b_1 a = a^{1+2^{n-2}} b_1, a$ ve b_1 elemanları teoremin 6). maddesini sağlamış olur.

Son olarak,

$$n \geq 4,\ ba=a^r b,\ r=-1+2^{n-2}$$

olsun.

$b^2=a^w$ ise $w \equiv wr(\mathrm{mod}\, 2^{n-2})$ olur.

Buna göre

$$\left(2+2^{n-2}\right)w \equiv 0\left(\mathrm{mod}\, 2^{n-1}\right) \text{ ya da } w \equiv 0\left(\mathrm{mod}\, 2^{n-2}\right)$$

olur. Bu durumda $b^2=e$ veya $b^2=a^{2^{n-2}}$ olarak bulunur. $b^2=a^{2^{n-2}}$ ve $b_1=ab$ ise

$$
\begin{aligned}
b_1^2 &= abab \\
&= a(bab^{-1})b^2 \\
&= aa^r b^2 \\
&= aa^{-1+2^{n-2}} a^{2^{n-2}} \\
&= a^{2^{n-1}} \\
&= e
\end{aligned}
$$

şeklinde bulunur. Böylece teoremin 7). maddesi de sağlanmış oldu.

Teorem 4.1.4: G**,** mertebesi p^{n+1} olan bir grup ve indeksi p olan devirli bir alt gruba sahip olsun. O zaman G ya devirli bir gruptur ya da $x^{p^n} = e$ ve aşağıda verilen gruplardan birini sağlayan x ve y tarafından gerilir.

i. $y^p = e,\ y^{-1}xy = x$ (abelyen grup)

ii. $p > 2$ veya $p = 2, n \geq 3$: $y^p = e,\ y^{-1}xy = x^{1+p^{n-1}}$ (ordinary abelyen olmayan grup)

iii. $p = 2$, $y^2 = e,\ y^{-1}xy = x^{-1}$ (dihedral grup)

iv. $p = 2$, $y^2 = e,\ y^{-1}xy = x^{-1+2^{n-1}}$ (semidihedral grup)

v. $p = 2$, $y^2 = x^{2^{n-1}}$, $y^{-1}xy = x^{-1}$ (quaternion grup)(Passman 1968)

Teorem 4.1.5: p mertebeli sadece bir alt grup içeren bir p - grup devirli veya genelleştirilmiş quaternion gruptur.

İspat: G**,** p^n mertebeli bir grup ve p mertebeden sadece bir alt gruba sahip olsun. İlk olarak, p asal sayısı tek olsun. O zaman indeksi p olan bir H alt grubu devirlidir. Böylece teorem 4.1.3. den G**,** 1. 2. veya 3. maddelerden biridir ve bu maddelerden 2. ve 3. maddeler en az bir tane p mertebeli alt grup içerir. Böylece G devirlidir. $p = 2$ olduğu zaman , G**,** indeksi 2 olan bir H devirli alt grubu içeriyorsa, o zaman teorem 4.1.3 den G, 1. 2. 3. 4. 5. 6. veya 7. maddelerden biridir ve bu tiplerden her biri mertebesi 2 olan en az bir alt grup içerir. Bu takdirde G, devirli veya genelleştirilmiş quaternion gruptur.

Geriye kalan durumlarda indeksi 2 olan her H alt grubu genelleştirilmiş quaternion gruptur. Burada $n \geq 4$ tür. İlk olarak $n = 4$ ve indeksi 2 olan bir Q quaternion grup olsun. $c \notin Q$ olsun. Q,

$$a^4 = b^4 = e, a^2 = b^2, ba = a^{-1}b$$

ile verilsin. $G = Q + Qc$ olsun. Mertebesi 2 nin kuvveti olan c elemanı Q daki mertebesi 4 olan $\langle a \rangle, \langle b \rangle, \langle ab \rangle$ alt gruplarının en az birine kendisini dönüştürmelidir. Yeniden adlandırmak gerekirse bunu $\langle a \rangle$ olarak alabiliriz. O zaman $c^{-1}ac = a$ veya $c^{-1}ac = a^{-1}$ olur. Eğer $c^{-1}ac = a$ ise o zaman $\langle a, c \rangle$ indeksi 2 olan abelyen alt gruptur. Bu bir çelişkidir. Eğer $c^{-1}ac = a^{-1}$ ise, o zaman

$$(cb)^{-1} a (cb) = a$$

olur. Bu durumda $\langle a, cb \rangle$, indeksi 2 olan abelyen bir alt gruptur. Bu da bir çelişkidir.

Son olarak $n \geq 5$ ve H, indeksi 2 olan genelleştirilmiş quaternion grup olsun. O zaman H,

$$a^{2^{n-2}} = e, \; b^2 = a^{2^{n-3}}, \; ba = a^{-1}b$$

ile verilir. Burada $\{a\}$, 2^{n-2} mertebeli H grubunun bir tek alt grubudur. H grubunun bütün elemanları, 4. mertebeden olan $\langle a \rangle$ grubunun içinde değildir. Bu yüzden

$$c^{-1}ac = a^r, c^2 = a^i b \text{ veya } c^2 = a^i$$

olur. $c^2 = a^i b$ ise, o zaman

$$c^{-2}ac^2 = a^{-1} \text{ ve } r^2 \equiv -1 (\mathrm{mod}\, 2^{n-2})$$

olur. Ancak bu imkansızdır. $c^2 = a^i$ ise, o zaman $\langle a, c \rangle$, indeksi 2 olan bir al gruptur ve varsayımdan genelleştirilmiş quaternion gruptur. Bu takdirde

$$c^{-1}ac = a^{-1}, (cb)^{-1} a (cb) = a$$

ve $\langle cb, a \rangle$, indeksi 2 olan abelyen bir alt gruptur. Bu bir çelişkidir. Böylece ispat tamamlanmış olur.

Teorem 4.1.6: $1 < m < n$, p^m mertebeli tek bir alt grup içeren p^n mertebeli grup devirlidir.

İspat: $m = n-1$ ise, o zaman p^n mertebeli bir H grubu ile sadece p^{n-1} mertebeli tek bir alt grup, her hangi bir x elemanı tarafından gerilir. Çünkü $\langle x \rangle$ tek bir maksimal alt grupta kapsanmaz ve böylece $\langle x \rangle = H$ ve H devirlidir. Şimdi $m < n-1$ olsun. H_1, p^m mertebeli tek bir alt grup olsun. H_1, p^{n-1} mertebeli maksimal bir alt grup olan A da kapsansın $1 < m < n-1$ olduğundan A devirlidir. Böylece aynı zamanda H_1 alt grubu da A nın bir alt grubu olarak devirlidir. p veya p^2 mertebeli her alt grup, p^m mertebeli bir alt grupta kapsanır ($m \geq 2$). Devirli olan H_1 alt grubu, p , p^2 mertebeli yalnız birer alt grup içerir. Bu takdirde teorem 4.1.5 den H devirli veya genelleştirilmiş quaternion gruptur. Ancak quaternion grup, 4. mertebeden en az bir grup içerir. Dolayısıyla H devirli bir grup olmalıdır.

Teorem 4.1.7: p^n mertebeli bir grubun, maksimal devirli bir alt gruba sahip olması için gerek ve yeter şart, bu grubun aşağıda verilen tiplerden biri gibi olmasıdır.

i. p^n mertebeli devirli bir grup

ii. Mertebesi p^{n-1} olan bir devirli grup ve birinin mertebesi p olan grubun direkt çarpımı

iii. $\left\langle x, a : x^p = e = a^{p^{n-1}},\ a^x = a^{1+p^{n-2}} \right\rangle$, $n \geq 3$

iv. Dihedral grup D_{2^n} , $n \geq 3$

v. Genelleştirilmiş quaternion grup Q_{2^n} , $n \geq 3$

vi. Semidihedral grup $\left\langle x, a : x^2 = e = a^{2^{n-1}},\ a^x = a^{2^{n-2}-1} \right\rangle$, $n \geq 3$

İspat: G grubunun mertebesi p^n olsun. $N=\langle a\rangle$ maksimal devirli bir alt grup olsun. O zaman I. Sylow Teoreminden $N \lhd G$ ve $[G:N]=p$ olur. $G/N=\langle xN\rangle$ yazılır. $G=\langle x,a\rangle$, $|a|=p^{n-1}$ ve $x^p\in N$ olur. Eğer G grubu abelyen ve $x^p=b^p$, $b\in N$ ise o zaman $\left(xb^{-1}\right)^p=e$ olarak elde edilir. Aksi takdirde $x^p=a^i$, $(i,p)=1$ ve $G=\langle x\rangle$ olur. Bu yüzden G grubu abelyen ise, G grubu (**i**) tipinde veya (**ii**) tipinde olur.

Bundan sonra $n>2$ olacak şekilde G grubunun abelyen olmadığı kabul edilecektir. x elemanı, mertebesi p olan , N normal alt grubunda bir otomorfizma oluşturur. Böylece $m^p\equiv 1(\bmod p^{n-1})$ ve $1<m<p^{n-1}$ için $a^x=a^m$ olur. Fermat Teoreminden $m^{p-1}\equiv 1(\bmod p)$ olur. Böylece $m\equiv 1(\bmod p)$ olur. Bir an için p asal sayısı tek olsun. $(p,k)=1$ için $m=1+kp^i$, $0<i<n-1$ yazılır. Buna göre

$$\begin{aligned} m^p &= \left(1+kp^i\right)^p = 1+kp^{i+1}+\frac{(p-1)}{2}k^2p^{2i+1}+\frac{(p-1)(p-2)}{6}k^3p^{3i+1}+\cdots \\ m^p &\equiv 1+kp^{i+1}\left(\bmod p^{i+2}\right) \end{aligned}$$

elde edilir. $kp^{i+1}+lp^{i+2}=l'p^{n-1}$ için $m^p=1\left(\bmod p^{n-2}\right)$ olur. $i+1\le n-1$ ve $(p,k)=1$ olduğundan $i+1=n-1$ ve $i=n-2$ elde edilir. Bu yüzden $m=1+kp^{n-2}$ olur. $kk'\equiv 1(\bmod p)$ olacak şekilde bir k' vardır ve $a^{x^{k'}}=a^{\left(1+kp^{n-1}\right)^{k'}}=a^{1+p^{n-2}}$ olur. $\left(x^p\right)^x=x^p$, $x^p\in\langle a^p\rangle$ ve $x^p=b^p, b\in N$ olsun. $[a,x]=a^{p^{n-2}}$ olduğundan G grubu sınıfı 2 olan nilpotenttir. Böylece $\left[b^{-1},x\right]^p=e$ olduğundan

$$\left(xb^{-1}\right)^p=x^pb^{-1}=e$$

olur. xb^{-1} elemanının yerine x alınarak $x^p=1$ elde edilir. Bu takdirde G grubu (**iii**) deki gibi olur.

$p=2$ ve $m=2k+1$ olsun. $m^2\equiv 1(\bmod 2^{n-1})$ ifadesinden $k(k+1)\equiv 0(\bmod 2^{n-3})$ ve $k\equiv 0(\bmod 2^{n-3})$ veya $k\equiv -1(\bmod 2^{n-3})$ elde edilir. Bu yüzden iki durum söz konusu olur. Bunlar $m = 2^{n-2} l + 1$ ve $m = 2^{n-2} l - 1$ dir. İlk durumda $m = 2^{n-2} l + 1$ alınır. İkinci durumda ya l çifttir ve $m = 2^{n-1} - 1$ ya da l tektir ve $m = 2^{n-2} - 1$ olarak alınır. $a^x = a^{-1}$ ve $m = 2^{n-1} - 1$ olsun. $\left(x^2\right)^x = x^2$ olduğundan, $x^2 = e$ veya $x^2 = a^{2n-2}$ olur. Bu takdirde $G \cong D_{2^n}$ veya $G \cong Q_{2^n}$ olur. Son olarak $m = 2^{n-2} - 1$ olsun.

$x^2 = a^{2r}$ ise, o zaman

$$a^{2r} = \left(a^{2r}\right)^x = a^{2r\left(2^{n-2}-1\right)}$$

olur. $2r \equiv 0(\bmod 2^{n-2})$ ve $x^2 = 1$ veya $x^2 = a^{2^{n-2}}$ olur. $x^2 \neq 1$ ise o zaman

$$\begin{aligned}\left(xa^{-1}\right)^2 &= xa^{-1}xa^{-1} \\ &= a^{2^{n-2}} a^{-2} a^{2-2^{n-2}} \\ &= e\end{aligned}$$

olup G grubu (**vi**) tipinde olur.

4.2. p, p^2, pq, p^3 Mertebeli Gruplar

p, p^2, pq, p^3 mertebeli grupların durumunu inceleyelim.

p bir asal sayı olmak üzere, p mertebeli bir grup, bir has alt gruba sahip olmayabilir. Bu durumda bu grup devirli bir grup olmalıdır. Birimden farklı herhangi bir eleman tarafından gerilir. Burada, “ G , sadece birimden oluşmayan bir grup olsun. O zaman G grubunun, kendisinden ve birimden başka alt grubu olmaması için gerek ve yeter şart G grubunun asal mertebeli sonlu devirli bir grup olmasıdır.” ifadesine bakılarak p mertebeli grup devirlidir.

p^2, mertebeli bir G grubu, devirli değil ise p mertebeli ayrık iki alt grup içerecektir. $\langle a \rangle$ ve $\langle b \rangle$ için $a^p = e, b^p = e$ ve $\langle a \rangle \cap \langle b \rangle = e$ olur. (p^m mertebeli bir grubun, her alt grubu, p^{m-1} mertebeli bir maksimal alt grubunda kapsanır.)

Bunların her ikisi de maksimal olduğundan her ikisi de normal olabileceklerdir. $G = \langle a \rangle \times \langle b \rangle$ olup, G abelyen bir gruptur.

p^3 mertebeli gruplar için $p = 2$ ve p asal sayısının tek olması durumlarını ayrı ayrı ele alacağız. İlk olarak $p = 2$ olsun ve mertebesi 8 olan abelyen olmayan gruplara bakalım. Böyle grupların mertebesi 8 olan elemanı olmayabilir. O zaman grup devirli olacaktır.
Eğer bütün elemanların mertebesi 2 ise, o zaman

$$(ab)^2 = e \text{ veya } abab = e$$

için

$$\begin{aligned} ba = a^2bab^2 &= a(abab)b \\ &= ab \end{aligned}$$

olup grup abelyen olur. Bu bir çelişkidir. Bu burumda mertebesi 4 olan bir eleman olmalıdır. $a^4 = e$. Eğer $b \notin \{a\} = A$ ise, o zaman $G = A + Ab$ ve $b^2 \in A$ olur. Eğer

$$b^2 = a \text{ veya } b^2 = a^3$$

ise o zaman b elemanın mertebesi 8 ve G grubu devirli olur. Bu durumda $b^2 = e$ veya $b^2 = a^2$ olur. A normal olduğundan $b^{-1}ab \in A$ için

$$b^{-1}ab = a \text{ veya } b^{-1}ab = a^3$$

olur. Çünkü A alt grubunun elemanlarının mertebesi 4 tür. $b^{-1}ab = a$ olduğunda G grubu abelyen olacağından $b^{-1}ab = a^3$ olur. Böylece abelyen olmayan iki grup elde edilmiş olur. Bunlar;
i. Dihedral grup
$a^4 = e,\ b^2 = e,\ b^{-1}ab = a^3$
ii. Quaternion grup
$a^4 = e,\ b^2 = a^2,\ b^{-1}ab = a^3$
şeklindedir.

Şimdi p^3 mertebeli abelyen olmayan grupları ele alalım. p asal sayısı tek ve G grubu devirli olmadığından, mertebesi p^3 olan elemanları içermez. G grubu mertebesi

p^2, $a^{p^2}=e$ olan bir elemana sahip olsun. O zaman $\langle a\rangle = A$ bir maksimal alt gruptur ve normaldir. $b\notin A$ olsun. Bu durumda

$$G = A + Ab + \cdots + Ab^{p-1} \text{ ve } b^p \in A,\ b^{-1}ab = a^r$$

olur.

G abelyen olmadığından $r\neq 1$ olur. Daha önceden $b^{-i}ab^i = a^{r^i}$ olduğunu görmüştük. $a = b^{-p}ab^p = a^{r^p}$ olup buradan aşağıdaki eşitlik elde edilir.

$$\begin{aligned} r^p \equiv 1(\text{mod } p^2) &\Rightarrow r \equiv 1(\text{mod } p)\\ &\Rightarrow r = 1 + sp \end{aligned}$$

$is \equiv 1(\text{mod } p)$ olacak şekilde i sayısı seçilirse

$$b^{-i}ab^i = a^{(1+sp)i} = a^{1+isp} = a^{1+p}$$

elde edilir. $(i,p)=1,\ b^i \notin A$ olduğundan b^i ile b elemanı yer değiştirilirse

$$G = A + Ab + \cdots + Ab^{p-1}, \quad b^{-1}ab = a^{p+1}$$

olur. $b^p \in A$ olup, $b^p = a^t$ olur. Burada b elemanının mertebesi p^3 olmadığından t, p nin bir çarpanı olmalıdır. $b^p = a^{up}$ yazılır. O zaman $a^i b = ba^{i(1+p)}$ kuralı kullanılarak

$$\begin{aligned} \left(ba^{-u}\right)^2 &= ba^{-u}ba^{-u} = b(a^{-u}b)a^{-u}\\ &= b(ba^{-u(1+p)})a^{-u}\\ &= b^2a^{-u(1+p)}a^{-u} \end{aligned}$$

$$\begin{aligned} \left(ba^{-u}\right)^3 &= ba^{-u}ba^{-u}ba^{-u} = b(a^{-u}b)(a^{-u}b)a^{-u}\\ &= b(ba^{-u(1+p)})(ba^{-u(1+p)})a^{-u}\\ &= b^2a^{-u(1+p)}ba^{-u(1+p)}a^{-u}\\ &= b^3a^{-u(1+p)(1+p)}a^{-u(1+p)}a^{-u} \end{aligned}$$

$$\vdots$$

$$\begin{aligned} \left(ba^{-u}\right)^p &= \underbrace{ba^{-u}ba^{-u}\ldots ba^{-u}}_{p} = b\underbrace{(a^{-u}b)(a^{-u}b)\ldots(a^{-u}b)}_{p-1}a^{-u}\\ &= b^pa^{-u(1+p)^{p-1}}\ldots a^{-u(1+p)}a^{-u} \end{aligned}$$

elde edilir. Buna göre

$$\begin{aligned}
\left(ba^{-u}\right)^{p} &= b^{p}a^{-u\left[1+(1+p)+(1+p)^{2}+\cdots+(1+p)^{p-1}\right]} \\
&= b^{p}a^{-u\left[1+1+p+1+2p+\cdots+1+(p-1)p\right]} && \left(a^{p^{2}}=e\right) \\
&= b^{p}a^{-up-up\left[1+2+\cdots+(p-1)\right]} \\
&= b^{p}a^{-up}a^{-up\left[1+2+\cdots+(p-1)\right]} \\
&= b^{p}a^{-up}a^{-up^{2}\frac{(p-1)}{2}} && \left(a^{p^{2}}=e\right) \\
&= b^{p}a^{-up} && \left(b^{p}=a^{up}\right) \\
&= e
\end{aligned}$$

olarak bulunur. $b_1 = ba^{-u}$ olarak alınırsa, aşağıdaki bağıntılar elde edilir.

$$a^{p^2} = e, b_1^{\,p} = e, b_1^{\,-1}ab_1 = a^{u}\left(b^{-1}ab\right)a^{-u} = a^{u}a^{1+p}a^{-u} = a^{1+p}$$

Son olarak G grubu p^2 mertebeli elemanlara sahip olmasın. $Z(G)$ merkezinin mertebesi p olmalıdır. Çünkü, eğer $Z(G)$ merkezinin mertebesi p^2 olsaydı, G grubu abelyen olacaktı. $G/Z(G)$ bölüm grubu,

$$x^p = e, y^p = e, yx = xy$$

olacaktır. O zaman $G \to G/Z(G)$ bir homomorfizm ise $a \to x, b \to y$ olur. Bu takdirde

$$a^p = e, b^p = e, a^{-1}b^{-1}ab = c \in \mathrm{Z}$$

olur. $a^{-1}b^{-1}ab = e$ ise, bu durumda G grubu abelyen olacaktı. Bu yüzden $c \neq 1$, $Z(G)$ merkezi için bir gerendir ve bağıntılar aşağıdaki gibi olur.

$$a^p = e, b^p = e, c^p = e, ab = abc, ac = ca, bc = cb$$

G, grubunun mertebesi pq olsun. Burada $p < q$ asal sayıdırlar. 3. Sylow Teoreminden q mertebeli alt grupların sayısı $1+kq$ tanedir ve qp sayısını böler. Bu durumda bu sayı 1 olmalıdır. q mertebeli Sylow alt grup 1 tane olduğundan bu alt grup normal alt grup olur. $\langle b\rangle, b^q = e$. p mertebeli Sylow alt grupların sayısı $1+kp$ tanedir ve qp sayısını böler. Bu nedenle bu sayı ya 1 dir ya da q dur. Eğer sayı 1 ise, bu alt grup normal alt grup olur. $\langle a\rangle, a^p = e$. $G = \langle a\rangle \times \langle b\rangle$ yazılır. Burada $c = ab$ elemanı pq mertebelidir ve G grubu devirlidir. Eğer sayı q ise, p mertebeli alt grup normal değildir. O zaman

$a^p = e, b^q = e$ ve $\langle b \rangle$ normal olduğundan $a^{-1}ba = a^r$ olarak yazılır. Burada $r = 1$ ise G grubu abelyen ve devirlidir. Bu yüzden $r \neq 1$ olsun. O zaman;

$$\begin{aligned} a^{-1}ba = b^r &\Rightarrow \left(a^{-1}ba\right)\left(a^{-1}ba\right) = \left(b^r\right)^2 \Rightarrow a^{-1}b^2a = b^{2r} \\ &\Rightarrow \left(a^{-1}ba\right)\left(a^{-1}ba\right)\left(a^{-1}ba\right) = \left(b^r\right)^3 \Rightarrow a^{-1}b^3a = b^{3r} \\ &\vdots \\ &\Rightarrow \underbrace{\left(a^{-1}ba\right)\left(a^{-1}ba\right)\ldots\left(a^{-1}ba\right)}_{r} = \left(b^r\right)^r \Rightarrow a^{-1}b^ra = b^{r^2} \end{aligned}$$

olarak yazılır. Bu son eşitlikte b^r yerine yazılırsa

$$\begin{aligned} a^{-1}b^ra = b^{r^2} &\Rightarrow a^{-1}\left(a^{-1}ba\right)a = b^{r^2} \\ &\Rightarrow a^{-2}ba^2 = b^{r^2} \\ &\Rightarrow a^{-p}ba^p = b^{r^p} \quad \left(a^p = e\right) \\ &\Rightarrow b = b^{r^p} \\ &\Rightarrow r^p = 1 + kq \\ &\Rightarrow r^p \equiv 1 \pmod{q} \end{aligned}$$

olarak bulunur.

Teorem 4.2.1: p^2 mertebeli gruplar abelyendir.

İspat: $|G| = p^2$ olsun. Teorem 3.1.12'den $|Z(G)| = p^s > 1$ olur. Lagrange teoremine göre $|Z(G)|\,\big|\,|G|$ olur. Bu durumda $|Z(G)| = p$ veya $|Z(G)| = p^2$ olur. Eğer $|Z(G)| = p^2$ ise, o zaman $Z(G) = G$ olur. Dolayısıyla G grubu abelyen olur. $|Z(G)| = p$ olsun. $Z(G) \lhd G$ olur. Bu durumda $G/Z(G)$ bölüm grubunun mertebesi p olur. Teorem 3.1.13'den $G/Z(G)$ bölüm grubu devirli olur ve $\bar{g} = gZ(G)$ tarafından gerilir. Bu yüzden

$$G/Z(G) = \left\{\bar{g}, \bar{g}^2, \bar{g}^3, \ldots, \bar{g}^{p-1}, \bar{g}^p = \bar{e}\right\}$$

olur. $\bar{g}^r = \overline{\left(g^r\right)} = g^r Z(G)$ dir. Bu durumda

$$G = gZ(G) \cup g^2 Z(G) \cup \ldots \cup g^{p-1} Z(G) \cup Z(G)$$

olur.

x ve y, G grubunun herhangi iki elemanı olsun. O zaman $x \in g^i Z(G)$ ve $y \in g^j Z(G)$, $1 \le i \le p,\ 1 \le j \le p$ olur. Buradan $x = g^i c_1$ ve $y = g^j c_2$, $c_1, c_2 \in Z(G)$ olur.

$$xy = g^i c_1 g^j c_2 = g^i g^j c_1 c_2 = g^{i+j} c_1 c_2$$
$$yx = g^j c_2 g^i c_1 = g^j g^i c_2 c_1 = g^{i+j} c_1 c_2$$

elde edilir. Böylece $xy = yx$ olup G grubu abelyen olur. O zaman $Z(G) = G$ olur. Dolayısıyla $|Z(G)| = p^2$ olur. Bu yüzden $|Z(G)| = p$ olması bir çelişkidir.

Teorem 4.2.2: $p < q$ olmak üzere, G, pq mertebeli bir grup olsun. O zaman G grubu, q mertebeli tek bir tane alt gruba sahiptir ve bu alt grup G grubunda normaldir. Eğer p asal sayısı, $q-1$ sayısını bölmez ise, o zaman G grubu devirlidir.

İspat: $(1+k_1 p) \mid pq$ ise, $1+k_1 p$ tane Sylow p - alt grup vardır. $(1+k_2 q) \mid pq$ ise, $1+k_2 q$ tane Sylow q-alt grup H vardır. q, $(1+k_2 q)$ sayısını bölmediğinden, $(1+k_2 q) \mid p$ olur. $p < q$ olduğundan $1+k_2 q = 1$ olmalıdır. Bu takdirde sadece bir tane Sylow q- alt grup vardır ve bu alt grup normaldir.

Şimdi p, $q-1$ sayısını bölemez olsun. Yani $q \ne 1+k_1 p$ olsun. Böylece bir tane Sylow p-alt grup K vardır.

$H \cap K$, H ve K nın bir alt grubudur. Bu durumda

$$|H \cap K| \,\big|\, |H| \text{ ve } |H \cap K| \,\big|\, |K|$$

olur. $(p,q) = 1$ olduğundan $|H \cap K| = 1$ olmalıdır. Böylece $H \cap K = \{e\}$ olmalıdır. $G = HK$ olur. $H = \langle h \rangle,\ K = \langle k \rangle$ olsun. O zaman H normal alt grup olduğundan

$$[h,k] = h^{-1}\left(k^{-1} h k\right) \in H$$

olur. Yine K normal alt grup olduğundan

$$[h,k] = \left(h^{-1}k^{-1}h\right)k \in K$$

olur. Böylece $[h,k] \in H \cap K = \{e\}$ olur. Dolayısıyla $hk = kh$ olur. Teorem 2.2.5'ten $|hk| = pq$ olur. Bu durumda $G = \langle (hk) \rangle$ devirlidir.

Şimdi 8. mertebeden olan grupları belirleyelim.

G, mertebesi 8 olan abelyen olmayan bir grup olsun. Lagrange teoremine göre G grubunun elemanlarının mertebeleri 1, 2, 4, veya 8 olmalıdır. Ancak $a \in G$ için $|a| = 8$ ise, o zaman $G = \langle a \rangle$ olup G grubu abelyen olur. Bu durumda G grubunun elemanlarının mertebeleri 1, 2, veya 4 olmalıdır. $\forall e \neq g \in G$ elemanının mertebesi 2 olsun. $a,b \in G$ olsun. O zaman

$$a^2 = b^2 = (ab)^2 = e$$

yazılır. Bu durumda

$$\begin{aligned} abab = e &\Rightarrow a^2bab = a \\ &\Rightarrow bab = a \\ &\Rightarrow b^2ab = ba \\ &\Rightarrow ab = ba \end{aligned}$$

elde edilir. Yani G grubu abelyen olur. Oysaki G grubu abelyen değildi. Bu bir çelişki oluşturdu. Bu çelişki G grubunun bütün elemanlarının mertebesinin 2 alınmasından kaynaklandı. Bu yüzden G grubunun bütün elemanlarının mertebesi 2 olamaz. Böylece $a \in G$ elemanının mertebesi 4 olmalıdır. O zaman

$$H = \langle a \rangle = \{e, a, a^2, a^3\}$$

G grubunda indeksi 2 olan devirli bir alt gruptur. $H \lhd G$ olur.
$b \in G, b \notin H$ olsun. O zaman

$$|G/H| = \frac{|G|}{|H|} = \frac{8}{4} = 2$$

bulunur. Bu durumda

$$|G/H| = \langle \overline{b} \rangle = \left\{ \overline{b}, \overline{b}^2 = \overline{e} \right\}, \qquad \overline{b} \in bH = Hb$$

yazılır. Böylece G grubu H ve Hb kümelerinin bir birleşimden oluşur.

$$H = \left\{ e, a, a^2, a^3 \right\}, \quad Hb = \left\{ b, ab, a^2b, a^3b \right\}$$

olmak üzere,

$$G = \left\{ e, a, a^2, a^3, b, ab, a^2b, a^3b \right\}$$

şeklinde yazılır. $ba \in bH = Hb$ olduğundan ba elemanı b, ab, a^2b, a^3b elemanlarından biri olmalıdır.

$ba = b \Rightarrow a = e$ olur ki, bu mümkün değildir.

$ba = ab \Rightarrow G$ abelyen olur ki, bu da mümkün değildir.

$ba = a^2b \Rightarrow a^2 = e$ olur ki, bu da mümkün değildir.

Buna göre, $ba = a^3b$ olarak yazılır.

Şimdi, $\overline{b^2} = \overline{b}^2 = \overline{e} = H$ olduğundan, $b^2 \in H$ yazılır. Dolayısıyla b^2 elemanı, e, a, a^2, a^3 elemanlarından biri olur.

$b^2 = a$ ise, o zaman b elemanının mertebesi 2 olamaz. Aksi takdirde $e = b^2 = a$ yazılır. Yine b elemanının mertebesi 4 olamaz. Aksi takdirde $e = b^4 = \left(b^2\right)^2 = a^2$ yazılır. Dolayısıyla $b^2 \neq a$ olur.

$b^2 = a^3$ ise, o zaman b elemanının mertebesi 2 olamaz. Aksi takdirde $a^3 = e$ olur. Yine b elemanının mertebesi 4 olamaz. Aksi takdirde $e = \left(b^2\right)^2 = a^6$ yazılır. Oysaki $a^4 = e$ olduğundan $b^2 \neq a^3$ olur.

Geriye $b^2 = e$ ya da $b^2 = a^2$ olması durumları kaldı.

1. Durum

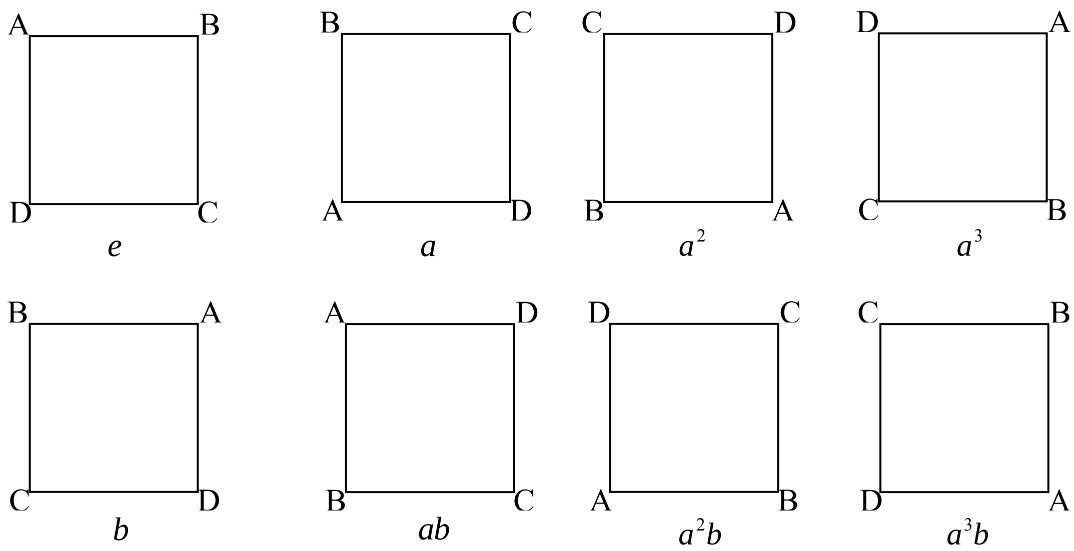
$b^2 = e$ olsun. Buna göre,

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}, \quad a^4 = e, \;\; b^2 = e, ba = a^3b$$

yazılır. Bu durumda aşağıdaki çarpım çizelgesi elde edilir.

Çizelge 4.1 Elemanların çarpımı

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e



Şekil 4.1 Karenin simetrileri

Sonuç olarak 1. durum D_4 dihedral grubu teşkil eder. Çarpım çizelgesinden veya karenin simetriklerinden D_4 dihedral grubu hakkında aşağıdaki bilgiler elde edilir.

Elemanlar : $e \quad a \quad a^2 \quad a^3 \quad b \quad ab \quad a^2b \quad a^3b$

Tersleri : $e \quad a^3 \quad a^2 \quad a \quad b \quad ab \quad a^2b \quad a^3b$

Mertebeler : 1 4 2 4 2 2 2 2

biçiminde yazılır.

Konjuge sınıfları,

$$\{e\},\{a^2\},\{a,a^3\},\{b,a^2b\},\{ab,a^3b\}$$

olarak bulunur. Aynı konjuge sınıflarındaki elemanların mertebeleri aynıdır ve bu sınıflardaki elemanların sayısı grubun mertebesini böler. D_4 dihedral grubunun merkezi tek elemanlardan oluşan konjuge sınıflarının birleşimine eşittir.

Yani, $Z(D_4)=\{e,a^2\}$ olarak yazılır. Komutataör alt grubu ise,

$$D_4' = \left\langle \left\{ x^{-1}y^{-1}xy : x, y \in D_4 \right\} \right\rangle = \{e,a^2\} = Z(D_4)$$

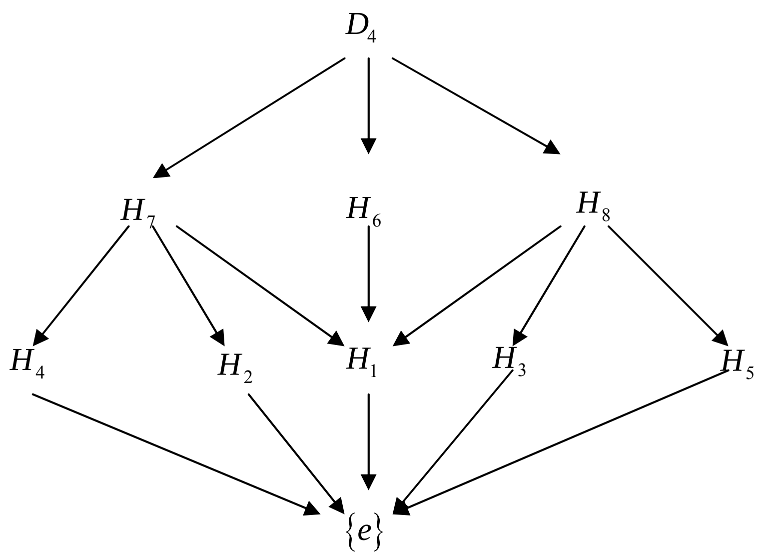
biçimindedir. Şimdi ise D_4 dihedral grubunun alt gruplarını inceleyelim.

$$H_1 = \{e, a^2\} = \langle a^2 \rangle,\ H_2 = \{e, b\} = \langle b \rangle$$
$$H_3 = \{e, ab\} = \langle ab \rangle,\ H_4 = \{e, a^2b\} = \langle a^2b \rangle$$
$$H_5 = \{e, a^3b\}$$

şeklinde mertebesi 2 olan alt grupları mevcuttur. Diğer taraftan mertebesi 4 olan alt gruplar ya devirlidir ya da $|x| = |y| = 2$ olacak şekilde $K_4 = \{e, x, y, xy = yx\}$ Klein 4-grubudurlar.

$$H_6 = \{e, a, a^2, a^3\} = \langle a \rangle, H_7 = \{e, a^2, b, a^2b\} \cong K_4$$
$$\cong H_8 = \{e, a^2, ab, a^3b\}$$

alt gruplarının mertebeleri 4 olduğundan D_4 dihedral grubundaki indisleri 2 olup hepsi normal alt grupturlar. Bu durumda alt grupların diyagramı aşağıdaki gibi olur.



Şekil 4.2 Alt gruplar diyagramı

Buna göre,

$$D_4/H_6 \cong D_4/H_7 \cong D_4/H_8$$

yazılır.

2. Durum

$b^2 = a^2$ olsun. Buna göre,

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}, \quad a^4 = e = b^4, \ \ b^2 = a^2, ba = a^3b$$

elde edilir.

Bu takdirde aşağıdaki çarpım çizelgesi oluşturulabilir.

Çizelge 4.2 Elemanların çarpımı

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

$a = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ ve $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $i^2 = -1$ olsun. O zaman,

$$a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, a^3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, ab = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$
$$a^2b = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}, a^3b = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

şeklinde Q_8 quaternion grubunun elemanları teşkil edilmiş olur. Çizelge 4.2. veya yukarıdaki elemanlardan

$$Q = \langle a, b : a^4 = e, b^2 = a^2, ba = a^3b \rangle$$

yazılır ve bu grup hakkında aşağıdaki bilgiler elde edilir.

Elemanlar :	e	a	a^2	a^3	b	ab	a^2b	a^3b
Tersleri :	e	a^3	a^2	a	a^2b	a^3b	b	ab
Mertebeler :	1	4	2	4	4	4	4	4

Konjuge sınıfları,

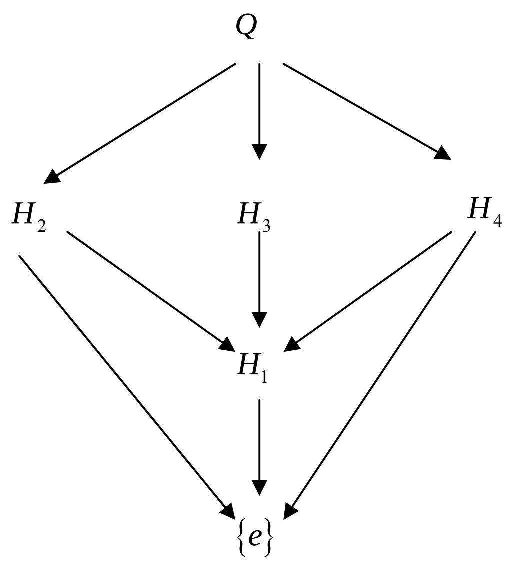
$$\{e\},\{a^2\},\{a,a^3\},\{b,a^2b\},\{ab,a^3b\}$$

biçiminde olur.

$Z(Q)=\{e,a^2\}=Q'$ yazılır. Mertebesi 2 olan alt grup devirlidir ve sadece a^2 elemanı tarafından gerilir. Mertebesi 4 olan alt gruplar ise ya devirlidir ya da Klein 4-grubudurlar.

$$H_2=\{e,a,a^2,a^3\}=\langle a\rangle=\langle a^3\rangle$$
$$H_3=\{e,b,a^2,a^2b\}=\langle b\rangle=\langle a^2b\rangle$$
$$H_4=\{e,ab,a^2,a^3b\}=\langle ab\rangle=\langle a^3b\rangle$$

alt grupları elde edilir. Böylece alt grupların diyagramı aşağıdaki şekildeki gibi olur.



Şekil 4.3 Alt gruplar diyagramı

Bölüm grupları,

$$Q/H_2 \cong Q/H_3 \cong Q/H_4$$

olarak yazılır.

Çizelge 4.3 Genel durum çizelgesi

$\lvert G \rvert = p$	$\lvert G \rvert = p^2$	$\lvert G \rvert = pq, p < q$	$\lvert G \rvert = p^3$
Grup devirlidir. $a^p = 1$	**i.** Grup devirlidir. $a^{p^2} = 1$ **ii.** Grup abelyendir. $a^p = 1, b^p = 1$ $ba = ab$	**i.** Grup devirlidir. $a^{pq} = 1$ **ii.** Abelyen değildir. $a^p = 1, b^q = 1$ $a^{-1}ba = b^r$ $r^p \equiv 1 (\operatorname{mod} q)$ $r \not\equiv 1 (\operatorname{mod} q)$ $p \mid (q-1)$	Abelyen olan **i.** $a^{p^3} = 1$ **ii.** $a^{p^2} = 1, b^p = 1$ $ba = ab$ **iii.** $a^p = b^p = c^p = 1$ $ba = ab$ $ac = ca$ $cb = bc$ 2^3 mertebeli abelyen olmayan **i.** Dihedral $a^4 = 1, b^2 = 1, ba = a^{-1}b$ **ii.** Quaternion $a^4 = 1, b^2 = a^2, ba = a^{-1}b$ p^3 mertebeli abelyen olmayan **i.** $a^{p^2} = 1, b^p = 1$ $b^{-1}ab = a^{1+p}$ **ii.** $a^p = 1, b^p = 1, c^p = 1$ $ab = bac, ca = ac$ $cb = bc$

5. SONUÇ

Yapılan bu çalışmada maksimal devirli alt gruplara sahip sonlu p-gruplar sınıflandırıldı. Bunu yaparken temsili verilen bir p-grup kullanılarak bu grubun izomorf olduğu gruplar bulunmuştur. Grup matrisleri yardımı ile bazı grupların izomorf olup olmadıkları incelenmiştir.

G, sonlu bir p- grup olsun. G grubunun aşağıda verilen gruplardan birine izomorf olduğu gösterildi.

$p > 2$, $n \geq 3$ ve $g = p^n$ için

$$G \cong M\left(p^n\right) = \left\langle x, y : x^{p^{n-1}} = y^p = e, y^{-1}xy = x^{1+p^{n-2}} \right\rangle$$

Eğer $p = 2$ ise;

$$G \cong Q_{2^n} = \left\langle x, y : x^{2^{n-1}} = e, y^2 = x^{2^{n-2}}, y^{-1}xy = x^{-1} \right\rangle$$

veya

$$G \cong D_{2^{n-1}}\,(Dihedral\ \ grup) = \left\langle x, y : x^{2^{n-1}} = y^2 = e, y^{-1}xy = x^{-1} \right\rangle$$

veya

$$G \cong S_g = \left\langle x, y : x^{2^{n-1}} = y^2 = e,\ y^{-1}xy = x^{-1+2^{n-2}} \right\rangle, \quad n \geq 4$$

olur.

Yine ayrıca G, grubu p mertebeli bir grup ise grubun devirli, p^2 mertebeli bir grup ise grubun abelyen, pq $\left(p < q\right)$ mertebeli bir grup ise grubun, q mertebeli tek bir tane alt gruba sahip olduğu ve bu alt grubun G grubunda normal olduğu ve eğer p asal sayısı $q-1$ sayısını bölmez ise G grubunun devirli olduğu gösterildi.

KAYNAKLAR

Asar, O.A & Arıkan, A. & Arıkan, A; Cebir, 2009, ısbn 978-605-4160-22-8, pages:101-102

Atagün, A.O; A New Method To Show Isomorphisms of Finite Groups, SAÜ Fen Bilimleri Enstitüsü Dergisi 9.Cilt, 2.Sayı 2005

Bayraktar, M.; Soyut Cebir ve Sayılar Teorisi, 1988, ısbn 975-442-006-8, pages: 72, 171-178,

Bhattacharya, P. B. & Jain, S. K. & Nagpaul, S. R.; Basic Abstract Algebra, Cambridge London New York New Rochelle Melbourne Sydney, ısbn 0 521 30990 5, pages:111, 140-146,

Çallıalp, F.; Örneklerle Soyut Cebir, 2001, ısbn 975-511-350-9, pages: 65-155,

Dönmez, A.; Cebir ve Sayılar Kuramı, 1984, pages: 154, 155, 258-265, 281,

Gardnier, C.F.; A First Course in Group Theory, ısbn 3-540-90545-6 Springer-Verlag New York Heidelberg Berlin, page: 82,116-126, 134-143,

Johnson, D. L.; Presentations of Groups,1990, ısbn 0 521 37203 8, pages: 168-170,

Hall, M.; The Theory of Groups, 1965, Library of Congress Catalog Card Number:59-5035 pages: 43-53

Passman, D.;Permutation Groups, 1968, Library of Congress Catalog Card Number: 68-55989 pages: 68-71

Scott, W. R.; Group Theory, 1964, Library of Congress Catalog Card Number: 64-14533 pages: 131,139,141,

Suzuki, M.;Group Theory I, ısbn 3-540-10915-3 Springer-Verlag Berlin Heidelberg New York, page:86-115

Suzuki, M.;Group Theory II, ısbn 3-540-10916-1 Springer-Verlag New York Berlin Heidelberg Tokyo, page: 1, 54-100

ÖZGEÇMİŞ

1982 yılında Erzurum'da doğdu. İlk orta öğrenimini ve lise öğrenimini Erzurum'da tamamladı. 2002 yılında Atatürk Üniversitesi Fen Fakültesi Matematik Bölümüne(i.ö) girmeye hak kazanarak 2006 yılında mezun oldu. 2006 da Atatürk Üniversitesi Fen Bilimleri Enstitüsünde yüksek lisans eğitimine başladı. Halen Fen Fakültesi Matematik Bölümünde araştırma görevlisi olarak devam etmektedir. Evlidir.