

HALL HIGMAN TİPİ TEOREMLER

YÜKSEK LİSANS TEZİ
(MATEMATİK)

Aynur YALINCAKLIOĞLU

Ocak 1990

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

T. C.
Yükseköğretim Kurulu
Dokümantasyon Merkezi

8644

Bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

A. O. Asar

Danışman

Prof.Dr.Ali Osman ASAR :

Sınav Jürisi

Başkan : Prof.Dr. Ali Osman ASAR A.O. Asar

Üye : Prof.Dr. Muhsin MERT

Üye : Doç.Dr. Erdoğan ESİN Esin

Bu Tez Gazi Üniversitesi Fen Bilimleri Enstitüsü
Tez Yazım Esaslarına uygundur. Ali Osman Asar

İÇİNDEKİLER

	<u>Sayfa</u>
ÖZ	ii
ABSTRACT	iii
TEŞEKKÜR	iv
SEMBOLLER	v
GİRİŞ	1
BÖLÜM 1	
KULLANILAN BAZI TANIM VE TEOREMLER	5
BÖLÜM 2	
SAYILAR TEORİSİNE AİT ELEMANTER ÖZELLİKLER	28
BÖLÜM 3	
GRUP TEORİK İNCELEMELER	33
BÖLÜM 4	
MİNİMAL HALİN BELİRLENMESİ	78
BÖLÜM 5	
TEOREMİN İFADESİ	92
BÖLÜM 6	
BERGER'İN REGÜLER YÖRÜNGE TEOREMİ	95
KAYNAKLAR	98
ÖZGEÇMİŞ	-

HALL HIGMAN TİPİ TEOREMLER
(Yüksek Lisans Tezi)

Aynur YALINCAKLIOĞLU
GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Ocak 1990

ÖZ

Bu çalışmada T.R, Berger'in "Hall Higman type theorems, I" başlıklı makalesi ve "Hall Higman type theorems, VI" başlıklı makalesindeki Teorem 2.2 incelenmiştir (Bak; [1] ve [2]).

Birinci makalede;

1) $G = AB$ bir grup; B, G de normal devirli bir altgrup; A, B nin nilpotent bütünleyeni ve $A \cap B = 1$ dir.

2) r bir asal sayı olmak üzere, $k = GF(r)$ bir cisim ve

3) V sadık indirgenmez $k[G]$ -modül ve her $L \triangleleft G$ için $V|_L$ homojendir.

Bu özel durumda A nın V üzerinde en az üç regüler yörüngesi olması için gerekli şartlar incelenmiştir.

İkinci makaledeki Teorem 2.2 de ise A aşikâr olmayan bir nilpotent gruptur ve her $p \nmid |A|$ asal sayısı için A nın $Z_p \times Z_p$ ye izomorf faktörü yoktur. $r \nmid |A|$ asal sayısı için $k = GF(r)$ ve V sadık $k[A]$ -modül olsun. Bu koşullar altında A nın V üzerinde en az bir regüler yörüngesinin olduğu gösterilmiştir.

Biz bu tezde Berger'in yukarıda sözü edilen çalışmalarını ayrıntılı ve anlaşılabilir bir şekilde ifade ettik. Birçok noktaları açıklığa kavuşturduk ve boşlukları doldurduk.

HALL HIGMAN TYPE THEOREMS

(M.Sc. Thesis)

Aynur YALINCAKLIOĞLU

GAZİ UNIVERSITY

INSTITUTE OF SCIENCE AND TECHNOLOGY

January 1990

ABSTRACT

In this work we studied the paper of T.A. Berger entitled "Hall Higman type theorems, I" and Theorem 2.2 in the paper "Hall Higman Type Theorems, VI" of the same author (See; [1] and [2]).

In the first paper,

- 1) $G = AB$ is a group with normal cyclic subgroup B and nilpotent complement A where $A \cap B = 1$.
- 2) $k = GF(r)$ is a field for a prime r , and
- 3) V is a faithful irreducible $k[G]$ -module such that $V|_L$ is homogeneous for all $L \triangleleft G$.

Under these special cases, the conditions for A to have at least three regular orbits on V have been investigated.

In Theorem 2.2 in the second paper, A is a nontrivial nilpotent $Z_p \sim Z_p$ -free group for all primes $p \mid |A|$ and $k = GF(r)$ for a prime $r \nmid |A|$ and V a faithful $k[A]$ module. Under these conditions, it has been shown that A has at least one regular orbit on V .

In this thesis, we have prepared a detailed and readable account of the above mentioned works of Berger, we have clarified many points and filled in many gaps.

TEŞEKKÜR

Yüksek Lisansa başlamamdan itibaren her adımda bilgi ve hoşgörülerinden yararlandığım, Cebir ve Sayılar Teorisi dalında gerekli olan tüm bilgileri vererek yeterli düzeye gelmeme çalışan, ayrıca bu çalışmanın ortaya çıkmasında, başından sonuna kadar her safhasında emeği olan değerli ilgi ve yardımlarını hiç bir zaman esirgemeyen Sayın Hocam Prof.Dr. Ali Osman ASAR'a teşekkürlerimi sunmayı bir borç bilirim.



SEMBOLLER

Sembol	Anlam
$\text{Aut}G$	G nin otomorfizmalarının grubu
$V _H$	V nin H -modülüne kısıtlanmış
$Z_p \sim Z_p$	Z_p ile Z_p nin çelenk çarpımı
$a b$	a böler b
a/b	a bölmez b
$p^m \parallel a$	$p^m a, p^{m+1} \nmid a$
$GF(r)$	Mertebesi r olan cisim
$H \triangleleft G$	H, G nin normal alt grubudur
G/H	G nin H ile bölüm grubu
$G_x, C_G(x)$	x in G içindeki merkezleyeni, G üzerinde x in sabit bıraktığı noktaların grubu
$C_G(A)$	A nın G içindeki merkezleyeni
$N _G(A)$	A nın G içindeki normalleyeni
$Z(G)$	G grubunun merkezi
$[G, G], G'$	G nin komütatör alt grubu
$[x, y]$	x ile y nin komütatörü
$\phi(G)$	G nin Frattini alt grubu
$\exp(G)$	G nin eksponenti
$ G $	G grubunun mertebesi
$[G:H]$	H nın G içindeki farklı kosetlerinin sayısı, H nın G içindeki indeksi ($H \leq G$ olmak üzere)
$o(g)$	g elemanının mertebesi
$G_1 \times G_2$	G_1 ile G_2 nin direkt çarpımı
$\text{kar}(k)$	k cisminin karakteristiği

Q_m	Mertebesi 2^m olan kuaterniyon grubu
D_m	Mertebesi 2^m olan dihedral grup
S_m	Mertebesi 2^m olan yarıdihedral grup
$X \setminus Y$	X de olan fakat Y de bulunmayan elemanların kümesi
$\Omega(H)$	$\langle x \in H : x^p = 1 \rangle$
$U(H)$	$\langle x^p : x \in H \rangle$
$A \cong B$	A ile B izomorftur.
$O_p(G)$	G nin maksimal normal p-altgrubu
$O^p(G)$	$G/O^p(G)$ p-grubu olacak şekilde G nin en küçük normal altgrubu
kerf	f fonksiyonunun çekirdeği
$\text{deng}_G(x)$	x in G deki dengeleyeni, yani G nin x i sabit bırakan elemanları (Burada G, X üzerine etki ediyor ve $x \in X$ dir)
$\langle x \rangle$	x tarafından üretilen devirli grup
$H \text{kar} G$	H, G nin karakteristik altgrubu
$M \otimes_R N$	Sol R-modül N ile sağ R-modül M nin tensör çarpımı
$W _G$	$G \otimes_R W$
$J(A)$	A nin Jacobson radikali
$\bigoplus_{i=1}^r A_i, A_1 \otimes A_2$	A_1 ile A_2 nin direkt toplamı
$\text{Hom}_k(V, V)$	V den V içine k-homomorfizmalarının toplam- sal grubu
$\text{Mat}(n, k)$	Girişleri k da olan $n \times n$ tipinden matris- lerin kümesi
$\text{Gal}(\bar{k}/k)$	$\bar{k}$ nin tüm k-otomorfizmalarının grubu
$Kx_1 H$	K ile H nin G içindeki ikili koseti, $x \in G$
$ G _p$	G nin mertebesini bölen en büyük p-altgrubu- nun mertebesi
G^x	$\langle g^x : g \in G \rangle$
F^{op}	F nin karşıt halkası
x^g	$g x g^{-1}, x, g \in G$

GİRİŞ

Kabul edelim ki, p ve q asal sayılar olmak üzere, Q bir q -grubu ve $C \leq \text{Aut}(Q)$ mertebesi p^e olan bir p -grubu olsun. CQ yarıdirekt çarpımının bir parçalanma cismi k ve $\text{kar}(k) = r \neq q$ olsun. V bir sadık indirgenmez $k[CQ]$ -modülü olsun. Bu şartlar altında V modülünün yapısı geniş biçimde araştırılmıştır. $r = p$ hali Hall-Higman [3] deki Teorem B nin ispatında ve $r \neq p$ hali Shult [4] deki Teorem'in ispatında incelenmiştir. Bütün bu kısıtlı hallerde $V|_C$ nin bir regüler $k[C]$ -direkt bileşeni olmaktadır.

Bu serideki çalışmaların amacı yukarıdaki durumları daha genel bir problem olarak araştırmaktır. G bir sonlu grup, $A \leq \text{Aut}(G)$ bir nilpotent grup ve $(|G|, |A|) = 1$ olsun. k bir cisim ve U bir sadık indirgenmez $k[AG]$ -modülü olsun. SORU : $U|_A$ modülü hakkında ne söylenebilir? Burada $A = C$, $G = Q$, $U = V$ alınırse Hall-Higman'a ait Teorem B deki durum elde edilir. Böylece buradaki soru Hall-Higman'a ait Teorem B deki durumun bir genellemesidir. Teorem B de $C = \langle x \rangle$ ve x in mertebesi p^n ise o zaman x in minimal polinomu ne zaman $(x-1)^{p^n}$ olabileceği araştırılmaktadır. Bu şart varsa x in V üzerinde bir regüler yörüngesi vardır. Teorem B nin ispatında görüldüğü gibi $V|_C$ modülü hemen her zaman bir regüler bileşene sahiptir, yani $k[C]$ -modülü $k[C]$ ye izomorf bir direkt bi-

T. C.

leşeni vardır. Burada da $U|_A$ modülüne benzer cevaplar için bakacağız. Fakat $(|G|, |A|) = 1$ şartını her zaman koymayacağız, bunun sonucu olarak da $U|_A$ nın regüler birekt bileşen içermesi her zaman mümkün olmayacaktır.

Hall-Higman'a ait Teorem B nin ispatına paralel olarak problem iki kısma ayrılacaktır. Teorem B nin ispatında Q , CQ içinde minimal abeliyan hale indirgenmektedir. Bu durumda C , $Q^* = Q \setminus \{1\}$ üzerinde yarı regüler etki etmektedir. Fakat Q^* üzerinde regüler yörüngeler olması $V|_C$ nin regüler direkt bileşeni olması için anahtar rolü oynar. Genel halde biz A nın G nin A -invariant H/K kesimleri üzerinde regüler yörüngelerin varlığını araştıracağız. Burada $K \leq H \leq G$ ve $K, H \triangleleft AG$ dir. Daha kesin olarak aşağıdaki problemi araştıracağız.

(1) $k = GF(r)$ olsun. Ne zaman A , U^* üzerinde regüler yörüngeye sahiptir?

Teorem B nin ikinci halinde Q grubu ekstra-özel, $[C, Z(Q)] = 1$ ve $Q/Z(Q)$ grubu $CQ/Z(Q)$ içinde minimal normaldir. Burada C nin V üzerindeki temsilleri belirlenmiş ve $V|_C$ modülü çalışılmıştır. Biz daha genel olarak şu durumu çalışacağız.

(2) $S \triangleleft AG$, S ekstra-özel, $Z(S) \leq Z(AG)$ ve $SZ(AG)/Z(AG)$, $AG/Z(AG)$ içinde minimal normal ve $A, S/Z(S)$ üzerinde sadık olsun. Hangi şartlar altında $U|_A$ nın regüler direkt bileşeni vardır?

Bu problemin genel çözümleri [2] de verilmiştir.
[Bak. Teorem 2.2 ve Teorem 3.2] Orada görüldüğü gibi eğer

A'nın hiçbir Sylow t -altgrubu $Z_t \sim Z_t$ ye izomorf faktöre sahip değilse ve $(|A|, r) = 1$ ise o zaman A , U^* üzerinde en az bir regüler yörüngeye sahiptir. Aynı hipotez altında $U|_A$ regüler direkt bileşen içerir.

Biz burada (1) durumunun bazı minimal hallerini çalışacağız ve elde edilen sonuçlar yardımıyla [7] deki Teorem 2.2'nin ispatını kolayca yapmak mümkün olacaktır. Daha açık olarak ifade etmek gerekirse aşağıdaki durumlar gözönüne alınacaktır.

- (1) $G = AB$, $B \triangleleft G$, A nilpotent ve $A \cap B = 1$ olsun.
- (2) $k = GF(r)$ bir cisim ve r bir asal sayı olsun.
- (3) V bir sadık indirgenmez $k[G]$ -modül ve her $N \triangleleft G$ için $V|_N$ -homojen olsun.

Bu şartlar altında A 'nın V üzerinde en az üç regüler yörüngesi olması için yeter şartlar belirlenecektir.

Burada takip edilen yol şöyle özetlenebilir. k cisminin öyle bir sonlu genişlemesi $\bar{k}$ vardır ki, eğer $\mathcal{G} = \text{Gal}(\bar{k}/k)$ ise G grubu $\mathcal{T} = \mathcal{G}\bar{k}^x$ yarıdirekt çarpımı içine gömülebilir ve $V = \bar{k}^+$ alınabilir. $\mathcal{T}$ 'nin $\Omega = \bar{k}^+ \setminus \{0\}$ üzerindeki permütasyon temsili $1_{\mathcal{G}}|_{\mathcal{T}}$ oluşturulmuş temsiline izomorftur. Bundan dolayı A , Ω üzerinde

$\sum 1_{\mathcal{G}^{x^{-1}} \cap A} |^A$ 'nın Ω üzerindeki etkisi gibi etki eder. Burada toplam bütün $A \times \mathcal{G}$ çift kosetleri üzerinde değişmektedir. Fakat buradan şu ilginç sonuç elde edilmektedir. Eğer $\mathcal{G}^{x^{-1}} \cap A = 1$ ise yukarıdaki toplam bir regüler A -yörüngesi içerir. Yukarıdaki şartı sağlayan ve farklı çift kosetlere ait olan x için farklı regüler yörüngeler elde

edilecektir. Bu bu x lerin sayısının ikiden fazla olmasını istiyoruz. Bundan sonra her $p \mid |\mathcal{G}|$ için $\bar{k}^x$ in bir J_p altgrubu tanımlanmakta ve $\mathcal{G}^{x^{-1}} \cap A = 1$ olması için her $p \mid |\mathcal{G}|$ için $x \notin J_p$ olması gerektiği gösterilmektedir. Daha sonra $J_p \neq \bar{k}^x$ şartı altında üçten az regüler yörünge olması durumunda B nin mertebesi kısıtlanmakta ve B den yararlanarak $\mathcal{G}$ nin mertebesi belirlenmektedir. Bundan sonra genel hal gözönüne alınarak A nın en çok iki regüler yörüngesi olması halinde B ve $\mathcal{G}$ için bütün muhtemel durumlar belirlenerek, elde edilen bulgular Teorem 5.2 de bir tablo halinde verilmektedir.

T.R. Berger burada sözü edilen durumları bir seri makale halinde incelemiş ve bu sonuçları kullanarak sabit noktasız otomorfizma grubuna sahip olan çözülebilir gruplara ait çok önemli sonuçlar elde etmiştir (Bak. [5]).

BÖLÜM 1

KULLANILAN BAZI TANIM VE TEOREMLER

Bu çalışmada bütün gruplar sonlu olarak alınmıştır.

1.1. TANIM : Ω boştan farklı bir küme, Ω üzerinde tanımlı birebir örten fonksiyonların kümesi S_{Ω} olsun. S_{Ω} kümesi fonksiyon bileşimine göre bir gruptur. Bu gruba Ω üzerinde simetrik grup denir.

S_{Ω} nin herhangi bir altgrubunda S_{Ω} altında bir permütasyon grubu denir.

1.2. TANIM : G, Ω üzerinde bir permütasyon grubu olsun. $\forall a, b \in \Omega$ için $g(a) = b$ olacak şekilde bir $g \in G$ varsa G ye geçişli permütasyon grubu denir.

1.3. TANIM : G, Ω bir permütasyon grubu olsun. $a \in \Omega$ için

$$G_a = \{g \in G : g(a) = a\}$$

altgrubuna a nın G içindeki dengeleyeni (stabilizer) denir.

Ω nın

$$O_{a,G} = \{g(a) : g \in G\}$$

altkümesine de G nin yörüngesi (orbit) denir.

1.4. TANIM : G, Ω üzerindeki geçişli permütasyon grubu olsun. Eğer her $a \in \Omega$ için $G_a = \{e\}$ ise G ye bir regüler permütasyon grubu denir.

Eğer burada permütasyon grubunda geçişlilik şartı yoksa G ye yarı regüler denir.

1.5. TANIM : G bir permütasyon grubu ve $O_{a,G}$, G nin bir yörüngesi olsun. $O_{a,G}$ nin mertebesi G nin mertebesine eşit ise o zaman $O_{a,G}$ ye G nin bir regüler yörüngesi denir. Aşikâr olarak $O_{a,G}$ regüler yörünge ise $G_a = \{e\}$ dir.

1.6. TANIM : G bir grup olsun. $g \in G$ ve her $x \in G$ için

$$\tau_g : x \rightarrow g^{-1}xg$$

biçiminde tanımlı G den G ye τ_g otomorfizmasına iç (inner) otomorfizma denir. G nin iç otomorfizmalarının grubu $\text{inn}G$ ile gösterilir. Ayrıca G nin iç otomorfizmalarının grubu $G/Z(G)$ ye izomorftur.

1.7. TANIM : G bir grup, $H \leq G$ ve A , G nin otomorfizmalarının boş olmayan bir kümesi olsun. Eğer her $h \in H$ ve $\alpha \in A$ için $h^\alpha \in H$ ise H ya G nin A-invariant altgrubu denir. Eğer $A = 1$ ise o zaman aşikâr olarak G nin her altgrubu A-invarianttır.

Eğer H , $\text{Aut } G$ -invariant ise o zaman H ya G nin karakteristik altgrubu denir.

H $\text{inn}G$ -invariant ise H ya G nin normal altgrubu (invariant ya da self-conjugate) denir.

1.8. TANIM : G herhangi bir grup olsun. Her $x \in G$ için

$$C_G(x) = \{g \in G : gx = xg\}$$

biçiminde tanımlanan $C_G(x)$, G nin bir altgrubudur. Bu gruba G içinde x in merkezleyeni denir. Aynı zamanda

$$- \bigcap_{x \in G} C_G(x) = \{g \in G : gx = xg, \text{ her } x \in G\}$$

G nin karakteristik altgrubudur ve G nin merkezi olarak adlandırılır, $Z(G)$ ile gösterilir.

$H \leq G$ için H nin G içindeki merkezleyeni

$$C_G(H) = \{g \in G : gh = hg, \text{ her } h \in H \text{ için}\}$$

olarak tanımlanır. O zaman

$$Z(G) \leq C_G(H) \leq G$$

dır.

1.9. TANIM : $K \triangleleft G$ ve $K \leq H \leq G$ olsun $K \leq J$ ve $J/K = C_{G/K}(H/K)$ olmak üzere G içinde H/K nin merkezleyeni G nin J altgrubu olarak tanımlanır. $J = C_G(H/K)$ yazılır. O zaman

$$C_G(H/K) = \{g \in G : [g, h] \in K, \text{ her } h \in H \text{ için}\}$$

dır. Bununla birlikte eğer $H \triangleleft G$ ise o zaman $C_G(H/K) \triangleleft G$ ve $G/C_G(H/K)$, $\text{Aut}(H/K)$ içine gömülebilir, yani

$$G/C_G(H/K) \tilde{\hookrightarrow} \text{Aut}(H/K)$$

1.10. TANIM : p bir asal sayı olmak üzere G bir p -grubu olsun. Eğer G elementer abeliyan ya da $\Phi(G) = Z(G) = G'$ elementer abeliyan ise G ye özel (special) grup denir. G abeliyan olmayan bir özel grup ve $Z(G)$ devirli ise G ye ekstra-özel (extra-special) grup denir.

1.11. TANIM : R bir halka, M bir toplamsal abeliyan grup olsun. Eğer her $m_1, m_2, m \in M, r_1, r_2, r \in R$ için

$$(i) \quad r(m_1 + m_2) = rm_1 + rm_2$$

$$(ii) \quad (r_1 + r_2)m = r_1m + r_2m$$

$$(iii) \quad (r_1r_2)m = r_1(r_2m)$$

olacak şekilde (her $r \in R, m \in M$ için) bir $rm \in M$ çarpımı tanımlanırsa, o zaman M ye bir sol R-modül denir. Eğer $1_R \in R$ ve her $m \in M$ için $1_R m = m$ ise o zaman M ye birimsel sol R-modül denir. Eğer M bir birimsel sol R-modül ve M , bir R -bazına sahip ise o zaman M ye serbest (free) sol R-modüldür denir.

Eğer R bir cisim ise birimsel serbest R-modülü M ye R üzerinde bir vektör uzayı denir. Bundan sonra R-modül denilince sol R-modül anlaşılacaktır.

1.12. TANIM : R , bir birimsel halka ve M bir sol R-modül olsun. Eğer $M \neq 0$ ise ve M nin sıfırdan farklı hiçbir N öz altmodülü yoksa o zaman M ye bir indirgenmez (basit) sol R-modül denir. Eğer M , indirgenmez sol R-modüllerinin bir direkt toplamı ise, o zaman M ye tam indirgenirdir denir.

1.13. TANIM : M bir $k[G]$ -modül olsun. $\{S_i\}_{i \in I}$, M nin birbirine izomorf indirgenmez altmodüllerinin bir kümesi olsun.

$$M = \sum_{i \in I} S_i$$

şeklinde yazılabilirse M ye bir homojen $k[G]$ -modül denir.

Tam indirgenir $k[G]$ -modül M nin birbirine izomorf olmayan bütün indirgenmez altmodülleri $S_1, \dots, S_n$ olsun. M nin S_1 ye izomorf olan bütün altmodüllerin toplamı M_1 olsun. O zaman $M = M_1 \oplus \dots \oplus M_n$ dir. Burada M_1 ye M nin bir homojen bileşeni denir.

1.14. TANIM : A bir halka, R birimli değişmeli bir halka ve A bir R -modül olsun. Eğer her $a, b \in A, r \in R$ için

$$r(ab) = (ra)b = a(rb)$$

ise o zaman A ya R üzerinde bir cebiri denir. A bir R -cebir olarak da adlandırılır.

1.15. TANIM : G bir grup, k bir cisim olsun. $k[G]$, $\sum_{g \in G} a_g g$ formal toplamlarından oluşan bir küme olsun. Burada sıfırdan farklı a_g lerin sayısı sonludur. Bu küme üzerinde toplama ve çarpma işlemleri sırasıyla

$$\sum_{g \in G} a_g g, \sum_{g \in G} b_g g \in k[G] \quad \text{ için } \sum_{g \in G} a_g g = \sum_{h \in G} a_h h$$

olduğundan

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{g, h \in G} a_g b_h gh$$

şeklinde tanımlanırsa $k[G]$, bir cebir yapılabilir. Bu cebire k üzerinde bir grup cebiri denir.

1.16. TANIM : A ve B iki grup ve kabul edelim ki B den A nın otomorfizmalarının grubu içine, $b \rightarrow \hat{b}$ şeklin-

de tanımlı bir homomorfizma olsun. $\{(a,b) : a \in A, b \in B\}$ sıralı ikililerin kümesi üzerinde çarpma işlemi

$$(a,b)(a_1,b_1) = (a \cdot \hat{b}(a_1), bb_1)$$

şeklinde tanımlanırsa bir grup oluşturur. Bu gruba $b \rightarrow \hat{b}$ homomorfizma yardımıyla elde edilen A ve B nin yarıdirekt çarpımı denir.

Eğer her $b \in B$ için $\hat{b} = 1$ ise, o zaman alışılmış direkt çarpım elde edilir.

G bir grup, A ve B, G nin altgrupları ve $A \triangleleft G$ olsun. Eğer $G = AB$ ve $A \cap B = 1$ ise G ye A nın B ile yarıdirekt çarpımıdır.

1.17. TANIM : $G = HK$ bir grup, H ve K, G nin altgrupları, $H \cap K \leq Z(G)$ ve $H \leq C_G(K)$ şartlarını sağlıyorsa G grubuna H ile K nın merkezi çarpımı denir.

1.18. TANIM : k bir cisim, A, k üzerinde bir cebir olsun. V, k üzerinde sonlu boyutlu bir vektör uzayı olsun.

$$T: A \rightarrow \text{Hom}_k(V, V)$$

bir fonksiyon olsun. Eğer her $a_1, a_2, a \in A$ ve $t \in k$ için

$$(1) \quad T(a_1 + a_2) = T(a_1) + T(a_2)$$

$$(2) \quad T(a_1 a_2) = T(a_1) T(a_2)$$

$$(3) \quad T(ta) = tT(a)$$

$$(4) \quad T(1_A) = I_V$$

ise o zaman T ye A nın V üzerinde bir temsili denir. O zaman her $a \in A$ ve $v \in V$ için

$$a.v = T(a)(v)$$

skaler çarpıma göre V bir sol A -modüldür. Bunun terside doğrudur; yani V bir A -modül ise

$$T : A \rightarrow \text{Hom}_k(V, V)$$

$$T(a)(v) = av$$

şeklinde tanımlı T , A nın bir temsilini tanımlar. Eğer A -modül olarak V , indirgenmez ise T temsiline indirgenmez temsil, eğer tam indirgenir ise T ye tam indirgenir temsil denir.

T_1 ve T_2 , A nın sırasıyla V_1 ve V_2 üzerinde iki temsili olsun. Eğer V_1 ve V_2 A -modül olarak izomorf iseler o zaman T_1 ve T_2 ye eşdeğer temsil denir. Başka bir deyişle eğer

$$S: V_1 \rightarrow V_2$$

tersinir lineer dönüşümü varsa öyle ki $a \in A$, $v \in V$ için

$$S(T_1(a)(v)) = T_2(a)(S(v))$$

ise T_1 ve T_2 eşdeğerdir.

1.19. TANIM : G bir grup, k bir cisim V , k üzerinde sonlu boyutlu bir vektör uzayı olsun. $GL(V, k)$, V üzerinde singüler olmayan (tersinir) lineer dönüşümlerin grubu olsun.

$$T: G \rightarrow GL(V, k)$$

bir grup homomorfizması ise T ye G nin V üzerindeki bir temsili denir. Bu G nin bir grup temsilidir.

$$T: k[G] \rightarrow \text{Hom}_k(V, V)$$

homomorfizması

$$T\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g T(g)$$

ile tanımlanırsa o zaman T , $k[G]$ nin V üzerinde bir temsili olur. Böylece T temsili V üzerinde $k[G]$ -modül yapısını tanımlar. Tersine olarak

$$T: k[G] \rightarrow \text{Hom}_k(V, V)$$

$k[G]$ nin V üzerindeki bir temsili ise o zaman

$$T|_G: G \rightarrow \text{GL}(V, k)$$

homomorfizması da G nin V üzerindeki bir temsilidir. Gerçekten eğer $g \in G$ ise o zaman

$$T(g)T(g^{-1}) = T(gg^{-1}) = T(1_{k[G]}) = I_V$$

dir. Öyle ise $T(g)^{-1}$ vardır. Böylece $T(g) \in \text{GL}(V, k)$ dir.

Aynı zamanda her $g_1, g_2 \in G$ için

$$T(g_1 g_2) = T(g_1)T(g_2)$$

dir.

$$T: G \rightarrow \text{GL}(V, k)$$

G nin bir temsili olsun. Eğer $k[G]$ - modül olarak V indirgenmez ise veya tam indirgenir ise T temsili sırasıyla G nin indirgenmez temsili veya tam indirgenir temsili denir.

Eğer T bir monomorfizma ise T temsiline sadık (faithful) denir. Eğer her $g \in G$ için $T(g) = I_V$ ise T ye aşık (trivial) temsil denir.

$\dim_k V$ ile gösterilen V nin boyutuna temsilin derecesi denir. Derecesi 1 olan temsil lineer temsil olarak adlandırılır.

$k[G]$ bir cebir olduğundan doğal olarak bir sol $k[G]$ -modüldür. Böylece $k[G]$ nin $k[G]$ üzerinde tanımlı olan temsiline $k[G]$ nin sol regüler temsili denir. Burada $g \in G$ ve $b \in k[G]$ için

$$T(g)(b) = gb$$

dır. $T|_G$ temsili de G nin bir sol regüler temsilidir.

1.20. TANIM : G sonlu bir grup, k bir cisim, $GL(n,k)$ k üzerinde $n \times n$ tipinde bütün tersinir matrislerinin grubu olsun.

$$T:G \rightarrow GL(n,k)$$

grup homomorfizmasına k üzerinde G nin bir matris temsili denir. Eğer

$$\text{Ker}(T) = \{g \in G : T(g) = I_n\} = \{e\}$$

ise o zaman T temsiline sadık (faithful) temsil denir. k üzerinde iki matris temsili T_1 ve T_2 nin denk olması için gerek ve yeter şart en az bir $M \in GL(n,k)$ için

$$T_2(G) = M^{-1}T_1(G)M$$

olmasıdır.

1.21. TANIM : $\chi:G \rightarrow k$, $\chi(g) = \text{tr}(T(g))$ ile tanımlı fonksiyona T temsilin karakteri denir.

Eğer χ , bir $k[G]$ -modülü olan V nin karakteri ve H , G nin bir altgrubu ise o zaman V_H nin karakteri $\chi|_H$ ile gösterilir. Buna χ nin H ya kısıtlanmış (restriction) denir.

G sonlu bir grup, H , G nin altgrubu, k bir cisim ol-

sun. $\{g_1 = 1, g_2, \dots, g_r\}$ H'nin G içindeki sol koset temsilcilerinin bir tam kümesi olsun. V sonlu boyutlu $k[G]$ -modülü olsun. $k[H]$, $k[G]$ nin alt cebiridir. Bu durumda V bir $k[H]$ -modülü olur ve V_H ile gösterilir. Buna V'nin $k[H]$ ya kısıtlanmış (restriction) denir.

$$T : G \rightarrow GL(V, k)$$

G'nin V üzerinde bir temsiliken $T_H = T|_H$, V üzerinde H'nin bir temsilini gösterir.

1.22. TANIM : G bir grup ve $H \leq G$ olsun.

$\{1 = x_1, x_2, \dots, x_n\}$ H'nin G içindeki sol koset temsilcilerinin bir tam kümesi ve k bir cisim olsun. O zaman $k[G]$ grup cebiri sağ $k[H]$ -modülü olarak

$$k[G] = k[H] \otimes k[x_2H] \otimes \dots \otimes k[x_nH]$$

şeklinde yazılabilir. Burada her $k[x_iH] = x_i k[H]$ bir sağ $k[H]$ -modülüdür. Şimdi V bir sol $k[H]$ -modülü olsun.

$$V|_H^G = k[G] \otimes_{k[H]} V$$

tensör çarpımına V den oluşturulan modül denir.

$k[G] = \bigoplus_{i=1}^n k[x_iH] = \bigoplus_{i=1}^n x_i k[H]$ değeri yerine konursa

$$\begin{aligned} V|_H^G &= k[G] \otimes_{k[H]} V \\ &= \bigoplus_{i=1}^n x_i (k[H]) \otimes_{k[H]} V \\ &= \bigoplus_{i=1}^n x_i \otimes V \end{aligned}$$

elde edilir. $V|_H^G$ bir sol $k[G]$ modülüdür. Gerçekten $g \in G$ ve $v \in V$ için $gx_i = x_j h$ ise

$$g(x_i \otimes v) = gx_i \otimes v = x_j \otimes hv \text{ dır [6].}$$

1.23. TANIM : H nin V üzerindeki temsili T olsun. O zaman G nin $V|G$ üzerindeki temsiline T den oluşturulmuş temsil denir ve T^G ile gösterilir. Eğer T nin karakteri θ ise o zaman T^G nin karakteri θ^G ile gösterilir ve buna θ dan oluşturulmuş karakter denir. Eğer $\text{kar}(k) \nmid |G|$ ise her $g \in G$ için

$$\theta^G(g) = \frac{1}{|H|} \sum_{y \in G} \theta(y^{-1}gy)$$

formülü sağlanır. $\theta^G(1) = [G:H] \dot{\theta}(1)$ dir. Bu formül

$$\theta^G(g) = \sum_{i=1} \dot{\theta}(x_i^{-1}gx_i)$$

olarak da yazılabilir. Burada, eğer $x \in H$ ise $\dot{\theta}(x) = \theta(x)$ ve $x \notin H$ ise $\dot{\theta}(x) = 0$ şeklinde tanımlıdır.

1.24. TANIM : G bir grup ve Ω bir sonlu küme olsun. G grubu Ω üzerinde etki etsin, yani her $x \in \Omega$ ve $g, h \in G$ için $gx \in \Omega$ tanımlı olsun ve

$$1.x = x, (gh)x = g(hx)$$

şartı sağlansın o zaman Ω üzerinde $\bar{g}(x) = gx$ şeklinde tanımlı $\bar{g}$ fonksiyonu bir permütasyondur ve $g \rightarrow \bar{g}$ eşlemesi G den $\text{Sim}(\Omega)$ içine bir grup homomorfizmasıdır.

Şimdi k bir cisim ve V bir k -uzayı olsun, öyle ki $\{v_x : x \in \Omega\}$, V nin bir bazı olsun. O zaman her $g \in G$ için

$$T(g)(v_x) = v_{gx}$$

olarak tanımlanırsa ve lineerlik yardımıyla V nin hepsine genişletilirse $T(g)$ bir lineer transformasyondur ve T, G nin V üzerinde bir temsilidir. T ye G nin permütasyon temsili ve V ye G nin Ω kümesine karşılık gelen

permütasyon modülü denir. T nin tanımladığı karaktere, G nin Ω üzerindeki permütasyon karakteri denir. $\theta(g)$ değeri $gx = x$ olan x lerin sayısıdır.

Şimdi G nin permütasyon temsili ile oluşturulmuş temsiller arasındaki yakın ilişkiyi gösterelim. (10),
10.4.Example

$H \leq G$ ve H nin aşıkâr temsili l_H olsun. $W = kv$, l_H tensilinin tanımladığı aşıkâr $k[H]$ - modülü olsun. Böylece her $w \in W$ ve $h \in H$ için $hw = w$ olur. $V = W^G$ olsun. $\{1 = g_1, \dots, g_n\}$ H nin G içindeki koset temsilcilerinin bir tam kümesi ise

$$V = \bigoplus_{i=1}^n g_i \otimes W$$

olur. Burada $g \in G$ için $gg_i = g_j h$ ($h \in H$) ise

$$g(g_i \otimes v) = g_j \otimes v$$

olarak tanımlıdır. Buradan görüldüğü gibi G nin $\{g_i h : 1 \leq i \leq n\}$ üzerindeki permütasyon etkisi $\{g_i \otimes W : 1 \leq i \leq n\}$ üzerindeki permütasyon etkisinin aynıdır. Bundan dolayı V modülü G nin gH kosetleri üzerindeki permütasyon modülüne izomorftur. Öyleyse G nin $l_H|_G$ temsili G nin gH üzerindeki permütasyon temsiline eşdeğerdir. Özel olarak $H = \langle 1 \rangle$ alınırsa $k[G]$ -üzerindeki regüler temsili $\langle 1 \rangle$ grubunun aşıkâr temsilinden oluştuğu görülür.

Burada yukarıdaki özellik şu şekilde uygulanacaktır. G, Ω üzerinde bir geçişli permütasyon grubu ve $a \in \Omega$ nin dengeleyeni H olsun. O zaman G nin Ω üzerin-

deki permütasyon temsili $1_H|^G$ ye eşdeğerdir. Bunu Teorem 1.15 den görmek kolaydır (Burada R birimli ve değişmeli bir halkadır) [6].

1.25. TANIM : k bir cisim, A bir k cebiri, V indirgenmez bir A -modül olsun. Eğer k nın her L genişlemesi $V|^L$ bir indirgenmez $A|^L$ -modül ise, o zaman V ye bir mutlak indirgenmez A -modül (absolutely irreducible A -module) denir. Eğer her indirgenmez A -modül mutlak indirgenmez ise o zaman k ya A için bir parçalanma cismi (splitting field) denir. k cebiri cebirsel kapalı ise parçalanma cismidir. Eğer k , $k[G]$ grup cebiri için parçalanma cismi ise, o zaman k , G grubu için bir parçalanma cismidir.

1.26. TANIM : A bir halka, M bir A -modül olsun. M nin tüm maksimal altmodüllerinin arakesitine A -modül radikali denir ve $\text{rad}M$ ile gösterilir. Eğer M nin maksimal altmodülü yoksa $\text{rad}M = M$ olarak tanımlanır.

Her sonlu üreteçli A -modül M için $\text{rad}M \subseteq M$ dir.

Sol regüler modül ${}_A A$ nın radikali ise A nın Jacobson radikali denir ve $J(A)$ ile gösterilir.

1.27. TANIM : A bir halka ve $e \in A$ olsun. Eğer $e^2 = e \neq 0$ ise e ye idempotent eleman denir. $e_1, e_2 \in A$ idempotentleri $e_1 e_2 = e_2 e_1 = 0$ şartını sağlıyorsa e_1, e_2 ye birbirine ortogonal idempotentler denir. Bir $e \in A$ idempotentini iki ortogonal idempotentin toplamı olarak yazılıyorsa e ye ilkel (primitive) idempotent denir.

$e \in Z(A)$ ilkel idempotentine ise merkezi ilkel idempotent eleman denir.

1.28. TANIM G bir grup olsun. Eğer H ve K , $K \triangleleft H$ olacak şekilde G nin iki altgrubu ise o zaman H/K grubuna G nin bir faktörü denir.

1.1. TEOREM : p bir asal sayı, P bir p -grubu olsun. Eğer P nin bütün karakteristik abeliyan altgrupları devirli ise o zaman

(i) p tek olmak üzere, P eksponenti p olan bir ekstra-özel p -grubu ile devirli bir p -grubunun merkezi çarpımıdır.

Ya da

(ii) $p = 2$ olmak üzere $P = E \times C$, bir ekstra-özel 2-grubu E ile devirli, $|C| \geq 16$ olan dihedral veya yarıdihedral ya da genel quaterniyan grubu C nin merkezi çarpımıdır.

İSPAT: (7) Teorem 5.4.9.

1.2. TEOREM : G , karakteristiği p olan bir cisim üzerinde tanımlı bir vektör uzayının sadık indirgenmez bir temsiline sahipse, o zaman G grubunun aşıkâr olmayan normal p -grupları yoktur.

İSPAT : (7) Teorem 3.1.3.

1.3. TEOREM : p bir asal sayı, P bir abeliyan p -grubu ve A da P nin otomorfizmalarının bir p' -grubu olsun. O zaman

$$P = C_P(A) \times [P, A]$$

dir.

İSPAT: (7) Teorem 5.2.3.

1.4. TEOREM : G bir grup olsun. Eğer G nin sadık indirgenmez bir temsili varsa, o zaman $Z(G)$ devirlidir.

İSPAT : (7) III. Teorem 2.2.

Bu teoremin bir uygulaması olarak aşağıdaki Lemmayı verelim. Aynı zamanda bu çalışmanın sonraki kısmında bu lemmadan özel bir durum için yararlanılacaktır.

1.5. LEMMA : G bir grup, V bir indirgenmez sadık $k[G]$ -modül olsun. N, G nin bir normal abelyan altgrubu olsun. O zaman $V|_N$ homojen ise N devirlidir.

İSPAT : $V|_N$ homojen olduğundan $V|_N$ nin öyle indirgenmez $X_1, X_2, \dots, X_s$ altmodülleri vardır ki

$$X|_N = X_1 + X_2 + \dots + X_s$$

ve $1 \leq i, j \leq s$ için $X_i \cong X_j$ dir. Şimdi Teorem (1.5) den dolayı N nin X_1 üzerindeki temsiline çekirdeği K ise N/K devirlidir. Fakat $X_1 \cong X_i$ olduğundan her $i \geq 1$ için X_i üzerindeki temsiline çekirdeği K dir. Bundan dolayı N nin V üzerindeki temsiline çekirdeği K dir. Fakat V sadık $k[G]$ -modülü olduğundan $K = \langle 1 \rangle$ dir. Bundan dolayı $N/K = N$ devirlidir.

1.6. TEOREM : V bir indirgenmez $k[G]$ -modül ve L, K üzerinde bir Galois genişlemesi olsun. O zaman $V' = \bar{k} \otimes_k V$

tam indirgenir $k[G]$ -modülüdür.

İSPAT : (8) V. 13.3 Satz.

Şimdi de çok iyi bilinen bir lemmayı aşağıda ispatıyla birlikte verelim.

1.7. LEMMA : G bir grup, k bir cisim ve k üzerinde sonlu boyutlu $k[G]$ -modül V olsun. $\bar{k}, k$ nın herhangi bir cisim genişlemesi ve $\bar{V} = \bar{k} \otimes_k V$ ise aşağıdakiler sağlanır.

- (i) $U \leq G$ için $C_{\bar{V}}(U) = \bar{k} \otimes_k C_V(U)$ dır.
- (ii) Eğer V sadık $k[G]$ -modül ise o zaman $\bar{V}$ sadık $k[G]$ -modülüdür.

İSPAT :

- (i) $\bar{V} = \bar{k} \otimes_k V$ sol $k[G]$ -modül

$$\varphi : G \times \bar{V} \rightarrow \bar{V},$$

$$(g, \bar{v}) \rightarrow g\bar{v} = g(x \otimes v) = xgv$$

olsun. k cismi üzerinde V için $\{v_1, v_2, \dots, v_n\}$. $\bar{k}/k$ nın bir bazı olsun ve k üzerinde $\bar{k}$ için bir baz Ω olsun.

$$\bar{V} = \left(\bigoplus_{w \in \Omega} wk \right) \otimes_k V = \bigoplus_{w \in \Omega} (wk \otimes_k V) = \bigoplus_{w \in \Omega} (w \otimes_k V)$$

dır. O zaman $\bar{V} = \bigoplus_{w \in \Omega} (w \otimes_k V)$ şeklinde yazılabilir.

O halde $\bar{v} \in C_{\bar{V}}(U)$ olsun. $\bar{v} = \sum_{i=1}^s w_i \otimes x_i$, $x_i \in V$ ve

$$\text{her } u \in U \text{ için } u(\bar{v}) = \sum_{i=1}^s w_i \otimes u(x_i) = \sum_{i=1}^s w_i \otimes x_i \text{ dır.}$$

Burada $\bar{V} = \bigoplus_{w \in \Omega} (w \otimes_k V)$ direkt toplam ve $u(V) \subseteq V$ ol-

duğundan her $1 \leq i \leq s$ için $w_i \otimes u(x_i) = w_i \otimes x_i$ dır.

$w_i(1 \circ u(x_i)) = w_i(1 \circ x_i)$ ve $w_i \neq 0$ olduğundan

$1 \circ u(x_i) = 1 \circ x_i$ dır. $x_i = x$ olsun. O halde $u(x) = x$ olduğunu göstermek yeter. $x \in V$,

$$x = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$$

olsun.

$$u(v_j) = \sum_{i=1}^n t_{ij} v_i \text{ ve}$$

$$u(x) = \sum_{i=1}^n a_j u(v_j) = \sum_{j=1}^n a_j \sum_{i=1}^n t_{ij} v_i = \sum_{i=1}^n \left(\sum_{j=1}^n a_j t_{ij} \right) v_i$$

dır. $1 \circ u(x) = 1 \circ x$ olduğundan

$$1 \circ \sum_{i=1}^n \left(\sum_{j=1}^n a_j t_{ij} \right) v_i = 1 \circ \sum_{i=1}^n a_i v_i$$

$$\sum_{i=1}^n (1 \circ \left(\sum_{j=1}^n a_j t_{ij} \right) v_i) = \sum_{i=1}^n a_i (1 \circ v_i)$$

$$\sum_{i=1}^n \left(\sum_{j=1}^n a_j t_{ij} \right) (1 \circ v_i) = \sum_{i=1}^n a_i (1 \circ v_i)$$

$$\sum_{j=1}^n a_j t_{ij} = a_i$$

elde edilir. Bu değer $u(x)$ ifadesinde yerine konursa

$u(x) = x$ bulunur. Böylece $\bar{v} \in \bar{k} \circ C_V(U)$ dır. Böylece

$C_{\bar{V}}(U) \leq \bar{k} \circ {}_k C_V(U)$ dır. Aşıkarak olarak $\bar{k} \circ {}_k C_V(U) \leq C_{\bar{V}}(U)$

dır. Buradan $C_{\bar{V}}(U) = \bar{k} \circ {}_k C_V(U)$ bulunur.

(ii) Her $w \in \bar{V}$ için $gw = w$ olacak şekilde $g \in G$ ol-

sun. k cisimi üzerinde V için bir baz $\{v_i : i=1, 2, \dots, n\}$

olsun. O zaman k üzerinde $\bar{V}$ için bir baz $\{1 \circ v_i : i=1, 2, \dots, n\}$

dır. Şimdi her $1 \leq i \leq n$ için

$$g(1 \circ v_i) = 1 \circ gv_i = 1 \circ v_i$$

dır. $gv_i = \sum_{j=1}^n a_{ji} v_j$ olsun. Bu değeri yukarıda yerine koyarsak. O zaman

$$\begin{aligned} 1 \otimes gv_i &= 1 \otimes \sum_{j=1}^n a_{ji} v_j = \sum_{j=1}^n (1 \otimes a_{ji} v_j) \\ &= \sum_{j=1}^n a_{ji} (1 \otimes v_j) = 1 \otimes v_i \end{aligned}$$

elde edilir. Fakat $\{1 \otimes v_j : 1 \leq j \leq n\}$, $\bar{k}$ üzerinde lineer bağımsız olduğundan $j \neq i$ için $a_{ji} = 0$ ve $a_{ii} = 1$ dir. O zaman her $i=1,2,\dots,n$ için $gv_i = v_i$ dir. Böylece g , V üzerinde birimseldir. Fakat V sadık $k[G]$ -modül olduğundan $g = 1$ dir. Bundan dolayı $\bar{V}$ sadık $\bar{k}[G]$ -modülüdür.

1.8. TEOREM : (Maschke Teoremi) G sonlu bir grup, k bir cisim $\text{kar}(k) \nmid |G|$ olsun. O zaman $k[G]$ grup cebiri bir yarıbasit halkadır.

İSPAT : (9) Teorem 3.1.

1.9. TEOREM : (Brauer'in parçalanma cisimleri üzerindeki teoremi) G mertebesi n olan sonlu bir grup olsun. 1 in n inci ilkel kökü w_n nin $\mathbb{Q}$ ya katılmasıyla elde edilen $\mathbb{Q}(w_n)$ dairesel genişlemesi G için bir parçalanma cismidir.

İSPAT : (10) Teorem 15.16.

1.10. TEOREM : (Clifford Teoremi) k herhangi bir cisim, V indirgenmez $k[G]$ -modül, $N \trianglelefteq G$ olsun. Bu durumda $g \in G$ için W , V nin bir $k[N]$ -altmodül olmak üzere

$$gW = \{gw : w \in W\} \subseteq V$$

olarak tanımlanır.

(1) Eğer $W \neq 0$ olmak üzere W, V nin bir $k[N]$ -alt-modülü ise o zaman $V = \sum_{g \in G} gW$ dir. Eğer W indirgenmez ise o zaman her gW da indirgenmezdir ve $V|_N$ bir tam indirgenir $k[N]$ -modülüdür.

(2) $W_1, \dots, W_m$ ler V nin indirgenmez $k[N]$ -altmodüllerinin izomorfik sınıflarının temsilcileri olsun. W_i ye izomorf olan V nin bütün $k[N]$ -altmodüllerinin toplamı V_i ile gösterilsin. O zaman $V = V_1 \oplus \dots \oplus V_m$ dir. (V_i ler V nin homojen komponentleridir).

(3) Eğer $g \in G$ ise o zaman her $gV_i = V_j$ dir. $G, \{V_1, \dots, V_m\}$ üzerinde geçişli (transitive) permütasyon grubudur.

(4) Eğer $H_1 = \{g \in G : gV_1 = V_1\}$ ise o zaman V_1 indirgenmez $k[H_1]$ -modülüdür ve

$$V \cong V_1|_G = k[G] \otimes_{k[H_1]} V_1$$

dir.

(5) Bir $e \geq 1$ tamsayısı için

$$V|_N \cong e(W_1 \oplus \dots \oplus W_m)$$

(yani $W_1 \oplus \dots \oplus W_m$ nin e kopyasının direkt toplamıdır).

(6) V ye karşılık gelen G nin karakteri θ ve W_i ye karşılık gelen N nin karakteri χ_i olsun. O zaman en az $g_i \in G$ için $W_i \cong g_i W_1$ ve $\chi_i = \chi_1^{g_i}$ olmak üzere

$$\theta|_N = e(\chi_1 + \dots + \chi_m)$$

dir, her $x \in N$ için $\chi_1^{g_i}, \chi_i^{g_i}(x) = \chi_1(x^{g_i})$ ile tanımlıdır.

İSPAT : (8) V. 17.3 Satz.

1.11. LEMMA: (Schur Lemma) A bir halka, V ve W indirgenmez A-modüller olsunlar. O zaman

$$V \cong W \text{ ise } \text{Hom}_A(V, W) = \{0\}$$

$$V = W \text{ ise } \text{Hom}_A(V, W) = \text{ bir bölme halkasıdır.}$$

İSPAT : (9) Lemma 2.2.

1.12. LEMMA : A bir yarıbasit halka olsun. O zaman

(i) A'nın sonlu sayıda birbirine izomorf olmayan $L_1, L_2, \dots, L_s$ basit sol idealleri vardır.

(ii) Eğer A'nın L_i ye izomorf olan bütün sol basit ideallerinin toplamı A_i ise o zaman A_i A'da 2-yanlı idealdir ve bir basit halkadır.

$$(iii) A = \bigoplus_{i=1}^s A_i$$

(iv) Eğer A_i nin birim elemanları e_i ise o zaman

$$1 = e_1 + e_2 + \dots + e_n$$

ve $A_i = A_{e_i}$ dır. Eğer $i \neq j$ ise $A_i A_j = 0$ dır.

İSPAT : (9) Lemma 2.9.

1.13. TEOREM : A bir basit halka, V bir indirgenmez A-modülü ve $D = \text{End}_A(V)$ olsun. O zaman

$$A \cong \text{End}_D(V) \cong \text{Mat}_n(D^{\text{op}}) \quad (n \in \mathbb{N})$$

İSPAT : (9) Teorem 2.16.

1.14. TEOREM : (Frobenius Recipracity Teoremi)

θ, H nin ve χ, G nin bir sınıf fonksiyonu olsun.

$$(\theta^G, \chi)_G \neq (\theta, \chi_H)_H$$

dır.

İSPAT : (11) Teorem 38.8.

1.15. TEOREM : M bir sol $R[G]$ -modülü olsun. $H \leq G$ ve $\{1 = g_1, \dots, g_n\}$ H nın G içindeki sol kosetlerinin bir tam kümesi olsun. M_H nın öyle bir altmodülü L vardır ki

$$M = \bigoplus_{i=1}^n g_i L$$

olsun. O zaman $R[G]$ -modülü olarak $M \cong L^G$ dir.

İSPAT :

$$t : R[G] \times L \rightarrow M$$

$$t(g, l) = gl$$

olarak tanımlı t fonksiyonu R -bilineer ve $R[H]$ -dengeli-dir. O zaman bir abeliyan grup homomorfizması

$$\varphi : R[G] \otimes L \rightarrow M$$

vardır, öyle ki

$$\varphi(g \otimes l) = t(g, l) = gl$$

dır. Üstelik, t R -bilineer olduğundan φ bir R -homomorfiz-

masıdır. Aynı zamanda $M = \bigoplus_{i=1}^n g_i L$ olduğundan φ örten-

dir. Diğer yandan

$$\psi : \bigoplus_{i=1}^n g_i L \rightarrow R[G] \otimes L$$

$$\psi\left(\sum_{i=1}^n g_i l_i\right) = \sum_{i=1}^n g_i \otimes l_i$$

bir R -epimorfizmasıdır ve φ nin tersidir. Bundan dolayı

φ bir R -izomorfizmasıdır. Fakat tanımdan dolayı R bir

$R[G]$ -homomorfizmasıdır. Bundan dolayı R bir $R[G]$ -izomorfizmasıdır. Yani,

$$M \cong L^G \quad \text{dır.}$$

1.16. TEOREM : (Mackey Altgrup Teoremi) X ve Y , G nin altgrupları ve L bir sol $R[X]$ -modül olsun.

$$G = \bigcup_{i=1}^k X a_i Y$$

G nin (X, Y) ikili kosetlerine göre G nin bir ayrışımı olsun. O zaman

$$(a) \quad L^G|_Y = \bigoplus_{i=1}^k (a_i \circ L)_{a_i X a_i^{-1}} \cap Y|_Y$$

(b) Eğer χ , X in L üzerinde karakteri ise o zaman

$$\chi^G|_Y = \sum_{i=1}^k [(\chi^{a_i^{-1}})_{a_i X a_i^{-1}} \cap Y|_Y]$$

Burada $\chi^{a_i^{-1}}$ karakteri her $x \in X$ için $\chi^{a_i^{-1}}(x^{a_i^{-1}}) = \chi(x)$ dır.

İSPAT : (8) V, 16.9. Satz, (10) Teorem 10.13.,

(11) Teorem 44.2.

1.17. TEOREM : (Wedderburn Teoremi) A bir birimli yarıbasit halka olsun. O zaman

$$A = A_1 \oplus A_2 \oplus \dots \oplus A_r$$

A_i halkaları $i \neq j$ olduğu zaman $A_i A_j = 0$ şeklinde yazılabilir. Bundan başka V_i ler birer indirgenmez A -modül, $D_i = \text{End}_A(V_i)$ olmak üzere

$$A_i \cong \text{Mat}_{n_i}(D_i^{\text{op}})$$

dır. Her indirgenmez A -modül bir tek V_i ye izomorftur ve $i \neq j$ ise $A_i V_j = \{0\}$, $A_i V_i = V_i$, $\dim_{D_i}(V_i) = n_i$ dır.

İSPAT : (9) Teorem 2.17.

1.18. TEOREM : A bir sonlu boyutlu k-cebiri V bir indirgenmez A-modülü olsun. O zaman V mutlak indirgenmez olması için gerek ve yeter şart

$$\text{End}_A(V) = k$$

olmasıdır.

İSPAT : (9), Teorem 4.2

1.19. TEOREM : (Hilbert'in 90 Teoremi) k nın derecesi n olan devirli bir cisim genişlemesi F, Aut_k^F nin bir üretici σ ve $u \in F$ olsun. O zaman $N_k^F(u) = 1_k$ olması için gerek ve yeter şart bir $v \in F$ için $u = v\sigma(v)^{-1}$ olmasıdır.

İSPAT : (13) Chapter V, Teorem 7.6.

BÖLÜM 2

SAYILAR TEORİSİNE AİT ELEMANTER ÖZELLİKLER

Bu bölümde makalede geçen sayılar teorisiyle ilgili bazı elemanter özellikler ispat edilecektir.

2.1. LEMMA : r ve s asal sayılar ve r tek olsun. n, e pozitif tamsayılar ve $x = r^n$ olmak üzere;

$$\frac{x^s - 1}{x - 1} = s^e$$

olsun. O zaman $s = 2, 2 \nmid (x-1), n = 1$ ve $r \equiv -1 \pmod{4}$ tür.

İSPAT : $s \neq r$ olduğu açıktır. Mümkünse s tek ve $e > 1$ olsun.

$$\frac{x^s - 1}{x - 1} = \frac{x^s - x}{x - 1} + 1 = s^e$$

olduğundan $\frac{x^s - x}{x - 1}$ bir tamsayıdır. Eğer $\frac{x^s - x}{x - 1}$, s ile bölünürse $s \mid 1$ olur ki, bu bir çelişkidir. Buradan $s \nmid x^s - x$ olduğundan $s \nmid x - n$ dir. Esasen s nin $(x^s - x)$ ve $(x - 1)$ i bölen kuvvetleri eşittir.

$$\begin{aligned} s^e &= \frac{x^s - 1}{x - 1} = \frac{[(x - 1) + 1]^s - 1}{(x - 1)} \\ &= \frac{(x - 1)^s \binom{s}{1} (x - 1)^{s-1} + \dots + \binom{s}{k} (x - 1)^{s-k} + \dots + \binom{s}{s-1} (x - 1) + 1 - 1}{(x - 1)} \\ &= (x - 1)^{s-1} + \binom{s}{1} (x - 1)^{s-2} + \dots + \binom{s}{k} (x - 1)^{s-k-1} + \dots + \frac{s(s-1)}{2} (x - 1) + s \\ s > 2 \text{ tek sayı ve } s \mid (x - 1) \text{ olduğundan } s^2 \mid (x - 1)^{s-1} \text{ dir. Ayrıca} \end{aligned}$$

$) = \frac{s!}{k!(s-k)!}$ katsayıları da s ile bölündüğünde

$|(s)_k(x-1)$ dir. Bundan dolayı

$$-1)^{s-1} + (s)_1(x-1)^{s-1} + \dots + (s)_k(x-1)^{s-k-1} + \dots + (s)_2(x-1)$$

ğeri s^2 ile bölünür. Fakat $s^2 | s^e$ olduğundan $s^2 | s$ çeliş-
si elde edilir. Bundan dolayı $e = 1$ olmalıdır. O halde

$$x^{s-1} + x^{s-2} + \dots + x + 1 = s$$

lunur. Sol tarafta s tane terim olduğundan eşitlikten
layı, bu ancak her terimin 1 e eşit olmasıyla mümkün-
r. O zaman

$$x^{s-1} = 1 \Rightarrow s-1 = 0 \Rightarrow s = 1$$

r. Bu bir çelişkidir. Bundan dolayı $s = 2$ dir. O zaman

$$\frac{x^{s-1}}{x-1} = x + 1 = 2^e$$

lunur. $x = r^n > 2$ olduğundan $e > 1$ dir. Bu durumda
($x + 1$) = ($r^n + 1$) dir. Bundan dolayı $n = 1$ dir. Bu
ağıdaki şekilde gösterilebilir.

Kabul edelim ki $n = 2^k \cdot v$, v tek sayı olsun. Mümkün-
v > 1 ve $b = r^{2^k}$ olsun.

$$r^n + 1 = b^v + 1 = (b + 1)(b^{v-1} - b^{v-2} + b^{v-3} - \dots + 1) \text{ dir.}$$

$$b^{v-1} - b^{v-2} + b^{v-3} - \dots + 1) \text{ de } v \text{ adet terim var ve her}$$

, $0 \leq i \leq v-1$, bir tek sayıdır. Bundan dolayı paran-
zdeki ifade bir tek sayıdır. O halde bu sayı 1 e eşit
malı. Böylece

$$v-1 = 0 \Rightarrow v = 1 \Rightarrow n = 2^k$$

r. Mümkünse $k \geq 1$ olsun. Bu durumda ;

$$r^{2^k} + 1 = r^{2^k} - 1 + 2 = 2^e \text{ dir.}$$

Fakat $4 \mid r^{2^k} - 1$ ve $4 \mid 2^e$ olduğundan $4 \mid 2$ dir. Bir bir çelişkidir. O halde $k = 0$ dir. Bundan dolayı

$$n=1 \Rightarrow x=r \Rightarrow x+1=r+1 \Rightarrow 4 \mid r+1 \Rightarrow r \equiv -1 \pmod{4} \text{ dir.}$$

2.2. LEMMA : $x > 1$ ve $y > 2$ den herbiri birer asal sayının kuvveti olmak üzere, aşağıdaki haller dışında daima

$$(x^y - 1)/(x - 1) > 2y^2 + y$$

dir.

<u>x</u>	<u>y</u>
2	3,4,5
3	3
4	3

İSPAT : $y = 3$ ise

$$\frac{(x^3 - 1)}{(x - 1)} = x^2 + x + 1 \leq 2 \cdot 3^2 + 3 = 21$$

olması halinde; işaret incelemesi yapılırsa

$$x^2 + x - 20 = 0 \Rightarrow (x-4)(x+5) = 0$$

		-5	1	4	
$x^2 + x - 20 = 0$	+	-	-	+	

↗ ↘ ↘ ↘ ↗

tablodan dolayı $x > 1$ ve $y = 3$ için $x = 2, 3, 4$ değerleri elde edilir.

$$y = 4 \Rightarrow \frac{x^4 - 1}{x - 1} = x^3 + x^2 + x + 1 > 2 \cdot 16 + 4 = 36$$

olması için $x \neq 2$ olmalıdır. Eğer $x = 2$ ise $x^3 + x^2 + x < 35$ dir. Eğer $x > 2$ ise o zaman $x^3 + x^2 + x + 1 > 36$ dir.

$x = 3$ için

$$x^3 + x^2 + x = 39 > 35 \quad \text{dir.}$$

$f(x) = x^3 + x^2 + x$ olsun. $f(x)$ artan olduğundan $x > 3$ için $f(x) > f(3) = 39$ dur. $y = 5$ için benzer inceleme yapılır. x ve y asal kuvvetler olduğu için $y = 6$ alınamaz. O halde $y = 7$ ve $x > 2$ için iddianın doğru olduğunu gösterelim.

$x = 2 \Rightarrow \frac{x^7 - 1}{x - 1} = 125 > 105$ dır ve $f(x) = \frac{x^7 - 1}{x - 1}$ artan olduğundan her $x > 2$ ise $f(x) > f(2) > 105$ dir. Şimdi de $y \geq 7$ için iddianın doğru olduğunu gösterelim. y için doğruluğu kabul edilsin. O zaman

$$x^{y-1} + \dots + x + 1 > 2y^2 + y$$

dir. O halde

$$x^y + x^{y-1} + \dots + x + 1 > x^y + 2y^2 + y$$

elde edilir.

Eğer $x^y \geq 4y + 3$ olduğunu gösterirsek induksiyon hipotezimiz ve ispatımız tamamdır.

$$\frac{x^y - 1}{x - 1} > 2y^2 + y \Rightarrow x^{y-1} > (2y^2 + y)(x - 1)$$

$$\Rightarrow x^{y-1} > 2y^2x - 2y^2 + yx - y$$

$$\Rightarrow x^y > 2y^2x - 2y^2 + yx - y + 1$$

$$\Rightarrow x^y > 2y(x-1)y + y(x-1) + 1$$

$$\geq 2y^2 + y + 1 \geq 2 \cdot 7 \cdot y + 7 + 1 = 14y + 8 > 4y + 3 \quad \text{ve}$$

$x > 1$ dır. O halde $x^y > 4y + 3$ elde edilir.

2.3. LEMMA : $x > 1$ ve $y > 2$ asal kuvvetten olmak üzere $x = 2$ ve $y = 3$ olmadığı zaman, daima

$$\frac{x^y - 1}{x - 1} > 2y + 1$$

dir.

İSPAT : Lemma 1.2. deki tabloda verilen değerler dışında daima

$$\frac{x^y - 1}{x-1} > 2y^2 + y$$

dir; yani

$$\frac{x^y - 1}{x-1} > (2y + 1)y > 2y + 1$$

$$\frac{x^y - 1}{x-1} > 2y + n$$

dir.

Bu durumda $x = 2$ ve $y = 3$ değerleri dışında, tablodaki değerlerin $\frac{x^y - 1}{x-1} > 2y + 1$ ifadesini sağladığını göstermek yeter.

$x = 2$ ve $y = 3$ için

$$2^2 + 2 + 1 = 3 \cdot 2 + 1$$

dir, yani $\frac{x^y - 1}{x-1} > 2y + 1$ ifadesini sağlamaz

$y = 4$ ve $x = 2$ için

$$x^3 + x^2 + x + 1 = 15 > 2 \cdot 4 + 1 = 9$$

dir.

$y = 3$ ve $x = 3$ için

$$x^2 + x + 1 = 13 > 2 \cdot 3 + 1 = 7$$

dir.

$y = 3$ ve $x = 4$ için

$$x^2 + x + 1 = 21 > 2 \cdot 3 + 1 = 7$$

dir. Böylece ispat tamamdır.

BÖLÜM 3

GRUP TEORİK İNCELEMELER

Bu makalede [2] deki Teorem 2.2. de ortaya çıkan minimal gruptan bilinen bir grup yapısı içine bir monomorfizma tanımlanacak ve daha sonra üçten az regüler yörünge olması durumunda bu grubun mertebesi belirlenecektir.

Çalışmanın geri kalan kısmı boyunca aşağıdaki kabulleri kullanacağız.

3.1. HİPOTEZ :

(1) $G = AB$ bir grup, B , G nin bir normal devirli altgrubu; A , B nin nilpotent bütünleyicisi ve $A \cap B = 1$ dir.

(2) $k = GF(r)$, r asal sayı

(3) V bir indirgenmez sadık $k[G]$ - modülü ve her $L \triangleleft G$ için $V|_L$ homojendir.

$\bar{k} \geq \hat{k} \geq k$, k nın sonlu genişlemesi $\mathcal{G} = \text{Aut}(\bar{k}/\hat{k})$ $\hat{k}$ üzerinde $\bar{k}$ nin Galois grubu olsun. $\mathcal{T} = \mathcal{T}(\bar{k}/\hat{k}) = \mathcal{G}\bar{k}^x$, $\bar{k}$ nin çarpımsal grubu $\bar{k}^x$ olmak üzere, $\bar{k}^x$ ile $\mathcal{G}$ nin yarıdirekt çarpımı olsun. $\bar{k}$ ve $\hat{k}$ bilindiğinde, bu grup daha basit olarak $\mathcal{T}$ ile gösterilir.

Şimdi $\sigma \in \mathcal{T}$, $\mu \in \bar{k}^x$ olmak üzere $\sigma\mu \in \mathcal{T}$ için $\bar{k}^+$ üzerinde etkisi

$$\sigma\mu \cdot v = \sigma(\mu v)$$

olarak tanımlansın. Bu çarpıma göre $\bar{k}^+$ sadık indirgenmez sol $\mathcal{J}$ -altmodülüdür.

Bu bölümde G nin $\mathcal{J}$ nun bir altgrubu ile ve de V nin $\bar{k}^{+-}$ ile özdeş kılınabileceğini göstereceğiz. Daha sonra G nin $\mathcal{J}$ nin altgrubu olarak sağlaması gereken birkaç şartı araştıracağız.

Önce bazı grup teorik sonuçlar verelim.

3.2. LEMMA : P bir p -grubu, $P_0 \triangleleft P$ ve P_0 in P de normal olan, her abeliyan altgrubu N devirli olsun.

O zaman;

- (a) p tek ise, P_0 devirli;
- (b) $p = 2$ ise, o zaman P_0 devirli ya da P_0 içindeki indeksi 2 ve merkezliyen kendisi olan, P de normal, devirli bir C_0 altgrubu vardır.

İSPAT : N, P_0 in karakteristik abeliyan altgrubu olsun. O zaman $N \triangleleft P$ dir. Ayrıca hipotezden dolayı N devirlidir. Böylece Teorem (1.1) den dolayı P_0 devirli bir grup ile ekstra-özel bir grubun merkezi çarpımı ya da $p = 2$ ve P_0 devirli, yarıdihedral, genel kuaterniyon veya mertebesi ≥ 16 olan dihedral grup ile bir ekstra-özel grubun merkezi çarpımıdır.

$P'_0 = [P_0, P_0] = D$ devirlidir. Şimdi $C_{P_0}(D) = E$, P_0 da karakteristik olduğundan $E \triangleleft P$ dir. E, P_0 in ekstra-özel kısmını içerir ve ekstra-özel grup ile devirli grubun merkezi çarpımıdır.

Şimdi de E nin bir maksimal abeliyan altgrubunun P tarafından normallendiğini gösterelim. B, P tarafından

normallenen E nin abeliyan altgrupları içinde maksimali olsun. Kabul edelim ki B , E de maksimal abeliyan olmasın. O zaman $C_E(B) > B$ ve $C_E(B) \leq C_P(B) \leq N_P(B)$ olduğundan $C_E(B) \triangleleft P$ dir.

$\bar{P} = P/B$ olsun. $1 \neq C_E(\bar{B}) \triangleleft \bar{P}$ olduğundan $Z(\bar{P}) \cap C_E(\bar{B}) \neq \langle 1 \rangle$ dir. Böylece öyle bir $x \in C_E(B)$ vardır ki $\bar{x} \in Z(\bar{P})$ dir. O zaman $\langle \bar{x} \rangle \triangleleft P$ olduğundan, bunun ters görüntüsü $B\langle x \rangle = \langle B, x \rangle \triangleleft P$ dir. $B_1 = \langle x, B \rangle$ olsun. $x \in C_E(B)$ olduğundan $[x, B] = 1$ dir. Böylece $B_1 > B$ abeliyan ve $B_1 \triangleleft P$ dir. Bu B nin maksimal olmasıyla çelişir. $B \leq P_0$ olduğundan hipotezden B devirlidir.

$P_0 = KC$, K ekstra-özel olsun. $K \leq E$ olduğundan $E = K(E \cap C)$ dir. $|Z(E)| \neq p$ olsun. O zaman $|E \cap C| > p$ ve $\exp(E \cap C) > p$ dir. Aynı zamanda $E \cap C \leq Z(E)$ dir. Buradan $\exp(Z(E)) = \exp(E \cap C) = \exp(E)$ dir. Aynı zamanda $Z(E) \leq B$ olduğundan $\exp(Z(E)) = \exp(B)$ dir. Aynı zamanda B devirli olduğundan $Z(E) = B$ dir. Fakat B , E içinde maksimal abeliyan olduğundan $B = E$ olmalıdır. O zaman E devirlidir. $K \leq E$ olduğundan $P_0 = C$ dir. Böylece $p \neq 2$ ise P_0 devirlidir. Öyleyse $p = 2$ olsun. O zaman C devirli veya indeksi 2 olan bir maksimal altgrup içerdiğinden $E = C$ veya $[C:E] = 2$ dir. Şimdi $|Z(P_0)| \neq p$ olsun. $C \leq Z(P_0) \leq Z(E)$ olduğundan $|C| = p$ dir. O zaman ya $P_0 = C$ devirli veya $P_0 = K$ ve P_0 ekstra-özeldir. Eğer $p \neq 2$ ise $\exp(P_0) = p$ olduğundan $\exp(B) = p$ ve buradan $|B| = p$ dir. O zaman $B = Z(P_0)$ dir. $C_{P_0}(B) = B$ olduğundan bu bir çelişkidir. Böylece $p \neq 2$ ve o zaman $[P:B] = 2$ dir.

3.3. LEMMA : Hipotez (3.1)(1) sağlansın, G nin her normal abeliyan altgrubu devirli olsun. O zaman G , $C_G(M) = M \geq B$ olan bir devirli M altgrubu içerir.

Bundan başka

$$(a) \quad C_G(B) = (A \cap C_G(B)) \times B$$

$$(b) \quad (|A \cap C_G(B)|, |B|) = 1$$

(c) $M = C_G(B)$ ya da $[C_G(B):M] = 2$ ve $C_G(B)$ nin bir S -altgrubu quaterniyon, genel quarteniyon, dihedral ya da yarıdihedraldir.

Özel olarak, bu Lemma (3.1) sağlandığı zamanda geçerlidir.

İSPAT : G nin B yi içeren normal abeliyan altgrupların içinde M maksimal altgrubunu seçelim. $M \triangleleft G$ olduğundan hipotezden devirlidir. $M \geq B$ ve A nilpotent olduğundan G/M nilpotenttir.

Kabul edelim ki $C_G(M) > M$ olsun. D/M asal mertebeden ve $D/M \leq C_G(M)/M \cap Z(G/M)$ olsun. O zaman $D \triangleleft G$, $D > M$ ve D abeliyandır. Fakat bu M nin maksimal seçimiyle çelişir. Böylece $C_G(M) = M$ elde edilir. $C = C_G(B)$ olsun. B abeliyan ve $AB = G$ olduğundan $C = (A \cap C)B$ dir. Bundan başka $A \cap C \leq C_G(B)$ olduğundan, $A \cap C$, B yi merkezler ve $A \cap C \cap B \leq A \cap B = 1$ dir. Bundan dolayı

$$C = (A \cap C) \times B$$

dir. Böylece (a) nın ispatı tamamdır.

$Z(A \cap C) \triangleleft G$ ve $B \triangleleft G$ olduğundan $Z(A \cap C)B \triangleleft G$ dir. Ayrıca $Z(A \cap C)B$ abeliyan olduğundan, hipotezden dolayı devirlidir. O zaman $(|Z(A \cap C)|, |B|) = 1$ dir. Ayrıca A

nilpotent olduğundan, $C \cap A \leq A$ da nilpotenttir. Bundan dolayı $|A \cap C|$ yi bölen asal sayılar $|Z(A \cap C)|$ yi de böler. Fakat $(|Z(A \cap C)|, |B|) = 1$ olduğundan $(|A \cap C|, |B|) = 1$ dir.

Şimdi kabul edelim ki $C > M$ olsun. P_0 , C nin abeliyan olmayan S_p -altgrubu, öyleki $P_0 \leq A \cap C$ olsun. P de P_0 ı içeren A nın S_p -altgrubu olsun. O zaman P , G nin bir S_p -altgrubudur. N , P_0 ın P de normal olan herhangi bir abeliyan altgrubu olsun. B ile A nın p' -kısımı P_0 ı merkezlediğinden ve $N \triangleleft P$ olduğundan $N \triangleleft G$ dir. O zaman hipotezden N devirlidir. P_0 abeliyan olduğundan Lemma 3.2 den dolayı $p = 2$ ve P_0, P de normal ve P_0 içinde indeksi 2 olan ve $C_{P_0}(C_0) = C_0$ olan devirli bir C_0 altgrubunu içerir. O zaman $C_0 \text{ kar } P_0 \triangleleft G$ olduğundan, $C_0 \triangleleft G$ dir. (a) dan dolayı C nilpotent olduğundan

$$C = P_0 \times O_2'(C)$$

dir. Yukarıdan görüldüğü gibi $O_2'(C)$ abeliyandır. Şimdi $M_0 = C_0 \times O_2'(C)$ olsun. O zaman $[C: M_0] = 2$ ve $M_0 \triangleleft G$ dir. Aynı zamanda $C_G(M_0) \leq C_G(B) = C$ dir. Buradan $C_G(M_0) = C_C(M_0) = M_0$ dir. Böylece M_0, G nin B yi içeren bir normal maksimal abeliyan altgrubudur. Eğer $M \neq M_0$ ise $[C: M_0] = 2$ olduğundan $MM_0 = C$ dir. Her iki halde $|M| = |M_0|$ dir. Bunun için $MM_0 = C$ haline bakmak yeter. $M \neq M_0$ olduğundan öyle bir $c \in P_0 \setminus M_0$ vardır ki $c \in M$ dir. Aynı zamanda $P_0 = C_0 \langle c \rangle$ dir. P_0 abeliyan olmadığından c, C_0 üzerinde mertebesi 2 olan bir atomorfizma tanımlar. O zaman $C_0 = \langle t \rangle$ olmak üzere $P_0' = \langle t^2 \rangle = [C_0, c]$ olduğu açıktır. $c \in M \triangleleft G$ olduğundan $t^2 \in M$ dir. Böylece

$\langle t^2 \rangle \langle c \rangle \leq M$ dir. Aşıkarak $[P_0 : \langle t^2 \rangle \langle c \rangle] = 2$ dir. Ayrıca $O_2(C) \leq M$ dir. $[C:M] = 2$ ve $|M| = |M_0|$ dir. $p = 2$ için, P_0 in her karakteristik altgrubu G de normal olduğundan hipotezden dolayı devirlidir. Ayrıca P_0 , indeksi 2 olan devirli bir $M \cap P_0$ altgrubuna sahiptir. Teorem 1.1 (ii) den dolayı $P_0 = E \rtimes D$, bir ekstra-özel 2-grubu E ile devirli veya $|D| \geq 16$ olan dihedral veya yarıdihedral ya da quaterniyon altgrubu D nin merkezi çarpıdır. Mümkünse $E \neq 1$ olsun. Önce D devirli olsun. O zaman $D \leq C_C(C_0) \leq C_0$ olduğundan $D \leq C_0$ dir. Eğer $|D| \leq 2$ ise $D \leq E$ olduğundan $C_0 \leq E = P_0$ dir. O zaman $|C_0| = 4$ ve $[E:C_0] = 2$ olduğundan $|E| = 8$ ve böylece E quaterniyon veya dihedraldir.

Şimdi $|D| \geq 4$ olsun. O zaman $D \leq C_0$ ve $\exp(C_0) = \exp(D)$ olduğundan $D \leq C_0$ olmalıdır. Fakat o zaman $E \leq C_0$ olur. Bu çelişkidir.

Şimdi D devirli olmasın. O zaman $[D:D \cap C_0] = 2$ dir. Aynı zamanda $\exp(E) = 4 \leq \exp(D)$ olduğundan $\exp(C_0) = \exp(D \cap C_0)$ dir. O zaman $D \cap C_0 = C_0$ olmalıdır. Fakat şimdi $E \leq C_0$ olduğundan bu bir çelişkidir. Bundan dolayı $E = 1$ dir.

Şimdi de özel duruma bakalım. Hipotez 3.1 sağlansın. O zaman Lemma 1.5 den dolayı G nin her normal abeliyen altgrubu devirlidir. Böylece Lemma 3.3 ün bütün şartları sağlanmış olur.

Şimdi Hipotez 3.1 sağlansın Lemma 3.3 den dolayı G nin merkezleyeni kendisi olan bir devirli M altgrubu vardır ve $B \leq M$ dir.

Bu bölümün geri kalan kısmında $M \neq G$ olduğunu kabul edeceğiz.

3.4. LEMMA : $\text{kar}(k) \nmid |M|$ olsun. Eğer k ya 1 in $|M|$ inci ilkel kökünün katılmasıyla elde edilen cisim $\bar{k}$ ise $\bar{k} \otimes V$, $\bar{k}[G]$ -modülü olarak parçalanır. Bundan başka mutlak indirgenmez bir direkt teriminin boyutu $[G:M]$ dir.

İSPAT : Hipotez 3.1 den dolayı $V|_M$ homojen ve sadık olduğundan M her bir indirgenmez altmodül üzerinde sadıktır. Buradan $\text{kar}(k) = r$ olduğundan Teorem 1.2 den $O_r(M) = 1$ dir. M devirli olduğundan $r \nmid M$ dir.

$\bar{k}$ cismi k nin bir normal genişlemesidir. Bundan dolayı Teorem 1.4 gereğince $\bar{k} \otimes V = \bar{V}$ tam indirgenir $\bar{k}[G]$ -modülüdür.

U bir indirgenmez direkt terim olsun. U nun sadık ve mutlak indirgenmez $\bar{k}[G]$ -modülü olduğunu göstermeliyiz. Önce sadık olduğunu gösterelim.

G nin U üzerinde temsilinin çekirdeği K ve $K \neq \langle 1 \rangle$ olsun. $D = K \cap M$ olsun. $U = C_U(D)$ olduğundan $C_{\bar{V}}(D) \neq \{0\}$ dir. O zaman, Lemma 1.7 den dolayı $C_{\bar{V}}(D) = \bar{k} \otimes C_V(D)$ olduğundan $C_V(D) \neq \{0\}$ dir. Fakat $D \triangleleft G$ olduğundan $C_V(D)$, bir $k[G]$ -modülüdür. Gerçekten $v \in C_V(D)$, $g \in G$ ve $d \in D$ ise $d(gv) = g(g^{-1}dg v) = gv$ olduğundan $gv \in C_V(D)$ dir. Fakat V bir indirgenmez $k[G]$ -modülü olduğundan $C_V(D) = V$ olmalıdır. Fakat V sadık $k[G]$ -modülü olduğundan bu imkansızdır. Bundan dolayı $D = \langle 1 \rangle$ dir. Böylece $K \cap M = \langle 1 \rangle$ dir. Fakat şimdi $K \leq C_G(M) \leq M$ olduğundan $K = \langle 1 \rangle$ bulunur.

Böylece U bir sadık indirgenmez $k[G]$ -modüldür.

Şimdi $U|_H$ sadık ve tam indirgenir $k[M]$ -modüldür. Gerçekten $\text{kar}(\bar{k}) \nmid |M|$ olduğundan Maschke teoreminden tam indirgenirdir.

$U|_M$ nin bir indirgenmez altmodülü W olsun. $\bar{k}$, Brauer'ın parçalanma cisimleri üzerindeki teoreminden dolayı, M için bir parçalanma cismidir. Böylece W mutlak indirgenmez $k[G]$ -modüldür. $0 \neq w \in W$ olsun. O zaman $W = Mw$ dir. $M = \langle c \rangle$ olsun. $\bar{k}$ nin tanımından dolayı c nin $\bar{k}$ içinde bir karakteristik değeri λ vardır. O zaman her $i \geq 0$ için $c^i(w) = \lambda^i w$ olduğundan

$$W = \{c^i(w) : 0 \leq i < m\} = \{\lambda^i w : 0 \leq i < m\} \subseteq \bar{k}w$$

dur. Buradan $W = \bar{k}w$ ve böylece $\dim_{\bar{k}} W = 1$ bulunur.

Şimdi M nin W üzerindeki temsilinin karakteri λ ve bir $x \in G$ için $\lambda^x = \lambda$ olsun. $m \in M$ ise

$$\lambda^x (xmx^{-1}) = \lambda (xmx^{-1}) = \lambda (m)$$

dir. O zaman $\dim_{\bar{k}} W = 1$ olduğundan, her $w \in W$ için

$$xmx^{-1}.w = mw$$

oldüğundan

$$m^{-1}xmx^{-1}.w = w$$

buradan $[M, x]$, W üzerinde aşıkardır. Fakat $W|_M$ sadık olduğundan $[M, x] = 1$ ve $x \in C_G(M) = M$ dir. Böylece $\text{deng}_G(W) = M$ dir. O zaman Teorem 1.10 (5) den dolayı

$$k[G] \otimes k[M]W = U$$

$$W|_G = U$$

dir. O zaman U mutlak indirgenmez $\bar{k}[G]$ -modüldür. Ger-

çekten $\bar{k} \leq L$ bir cisim genişlemesi olsun $k[G] \mid^L = L(G)$ modülü $U \mid^L$ yi göz önüne alalım. U' , $U \mid^L$ nin bir indirgenmez altmodülü olsun. O zaman $U \mid_M$ halinde olduğu gibi Teorem 1.7 den dolayı $U' \mid^M$ nin bir homojen bileşeni W' ise $\dim_L W' = 1$ ve $U' = W' \mid^L [G]$ dir. Fakat $\dim_L U' = (\dim_L W) [G:M] = [G:M] = \dim_{\bar{k}} U = \dim_L U \mid^L$ olduğundan $U' = U \mid^L$ olur. Böylece $U \mid^L$ indirgenmezdir. Bundan dolayı U mutlak indirgenmez $\bar{k}[G]$ -modülüdür. Ayrıca

$$\dim_{\bar{k}} U = \dim_{\bar{k}} \bar{k}[G] \otimes \bar{k}[M]^W$$

dir.

$$\bar{k}[G] \otimes \bar{k}[M]^W = \bigoplus_{i=1}^r x_i \otimes W$$

burada $\dim(x_i \otimes w) = 1$ ve de $G = \bigcup_{i=1}^r x_i M$ olduğundan

$$\dim_{\bar{k}} U = [G:M] \text{ dir.}$$

3.5. LEMMA : Hipotez 3.1, (1), (2) sağlansın. $M \triangleleft G$ ve $C_G(M) = M$ olsun. V bir indirgenmez $k[G]$ -modülü ve $V \mid_M$ homojen olsun.

$\bar{k}$, k ya 1 in bir $|M|$ inci ilkel kökünün katılmasıyla elde edilen cisim olsun. O zaman $\bar{k}$ nın öyle bir altcismi $\hat{k}$ ve öyle

$$\phi : G \rightarrow \mathcal{J}(\bar{k}/\hat{k})$$

$$\Phi : V \rightarrow \bar{k}^+ \quad (\text{izomorfizma})$$

monomorfizmaları vardır ki

$$(a) \quad \phi(x)\Phi(v) = \Phi(xv), \quad x \in G, \quad v \in V$$

$$(b) \quad \phi(M) = \langle w \rangle \text{ ve } \bar{k} = k(w)$$

$$(c) \quad \phi(G)\bar{k}^x = \text{Gal}(\bar{k}/\hat{k})\bar{k}^x, \text{ ve}$$

$$(d) \quad \phi(G) \cap \bar{k}^x = \phi(M)$$

dir.

İSPAT : $A = k[G] / J(k[G])$ olsun. $J(k[G])V = \{0\}$ olduğundan V bir A -modülüdür. V , $k[G]$ -modülü olarak indirgenmez olduğundan A -modülü olarak da indirgenmezdir. Schur Lemma'dan dolayı $F = \text{Hom}_A(V, V)$ bir bölme halkasıdır. Şimdi A yarıbasit olduğundan dolayı [(9) Teorem 2.17] den dolayı halka olarak

$$A = \bigoplus_{i=1}^r A_i$$

yazılabilir. Burada her A_i bir (iki yanlı) idealdir ve $i \neq j$ için $A_i A_j = 0$ dır. Ayrıca her $1 \leq i \leq r$ için öyle bir ilkel merkez idenpotenti e_i vardır ki

$$A_i = e_i A e_i = A e_i$$

dır. Öte yandan bir $1 \leq j \leq r$ için $A_j V \neq \{0\}$ dır. Fakat her $i \neq j$ için $A_i V = 0$ dır. Bundan dolayı

$$A e_j = A_j \cong \text{Hom}_F(V, V) \cong \text{Mat}(n_j, F^{\text{op}})$$

dır. k sonlu olduğundan F sonludur ve F bir bölme halkası olduğundan sonlu bölme halkalarına ait Wedderburn Teoreminden dolayı F bir cisimdir, yani k nın sonlu cisim genişlemesidir. Böylece $A_e \cong \text{Mat}(m, F)$ dir. Burada $e = e_j$ ve $m = n_j$ dir. Buradan $F \cong Z(A_e)$ elde edilir. Böylece F yi $Z(A_e)$ ile özdeş kılabiliriz. Şimdi

$$\text{Hom}_{A_e}(V, V) = \text{Hom}_A(V, V) \cong F$$

oldüğundan (9), Teorem 4.2 den dolayı F -uzayı olarak V , mutlak indirgenmez A_e -modülüdür. Fakat F nin hiç bir özalt cismi için V , mutlak indirgenmez değildir. V üzerinde G için herhangi bir parçalanma cismi K olsun. Şim-

di (9), Teorem 4.2 den dolayı

$$\text{Hom}_{(eA)K}(V^K, V)^K \cong K$$

olduğundan $Z(Ae) \tilde{C} K$ dır. Buradan $F \tilde{C} K$ bulunur. Lemma 3.4 den dolayı $\bar{k}$, G için parçalanma cismi olduğundan $F \tilde{C} \bar{k}$ dır. $\bar{k}$ nın $\hat{k}$ altcismi $\hat{k} \cong F$ olarak tanımlansın. Böylece

$$(1) \quad \bar{k} \geq \hat{k} \cong F \text{ dır.}$$

$[eA : F] = m^2$ olsun. O zaman $\dim_F V = m$ ve buradan $\dim_k V = (\dim_k \hat{k})(\dim_{\hat{k}} V) = [\hat{k} : k]m$ dır. Ayrıca Lemma 3.4 ten dolayı $[G : M] = m$ dır. Böylece

$$(2) \quad \dim_k V = m[\hat{k} : k], \quad m = [G : M]$$

elde edilir.

Şimdi $k[M]$ nin eA içindeki görüntüsü B olsun. $k[M]$ abeliyan olduğundan B abeliyandır. Öte yandan eA basit halka ve her basit sol ideali ($\neq 0$) V ye izomorftur (Teorem 1.13 ten). Ayrıca hipotezden dolayı $V|_M$ homojen olduğundan $A|_M$ homojendir. Özel olarak $B|_M$ homojendir, yani B , izomorf indirgenmez $k[M]$ -modüllerinin direkt toplamıdır. Fakat $k[M]$ yarıbasit halka olduğundan B halkası $k[M]$ nin bir basit bileşenine izomorftur, yani basit halkadır. O zaman Ae nin durumunda olduğu gibi $B = Z(B)$, k nın bir cisim genişlemesidir.

Eğer $M = \langle y \rangle$ ise ve y nin eA içindeki görüntüsü $\bar{y}$ ise $k[M] = k[\langle y \rangle]$ nin eA içindeki görüntüsünün $k[\langle \bar{y} \rangle]$ olduğu açıktır. $B = k[\langle \bar{y} \rangle]$ cisim olduğundan ve $o(\bar{y}) = o(y) = |M|$ olduğundan B , k ya 1 in $|M|$ yinci ilkel kökünün katılmasıyla elde edilen cisim genişlemesidir.

Böylece $\bar{k}$ nin tanımından dolayı $B = \bar{k}$ dir.

Şimdi $V|_M$ indirgenmez altmodülün direkt toplamı olsun. O zaman $\dim_B V = t$ dir. Bundan

$$\dim_k V = t[B:k] = t[\bar{k} : k]$$

elde edilir.

Şimdi $x \in G$ nin eA içindeki görüntüsü $\bar{x}$ olsun.

$\Psi_x : eA \rightarrow eA$, $\Psi_x(y) = \bar{x}y\bar{x}^{-1}$ olarak tanımlansın Ψ_x , eA nin bir otomorfizmasıdır. Aynı zamanda $M \triangleleft G$ olduğundan $\Psi_x|_B$, B cisminin bir otomorfizmasıdır. Şimdi $x \rightarrow \Psi_x|_B$ eşlemesi G den $\text{Aut}(B)$ içine bir grup homomorfizmasıdır. G nin görüntüsü G_1 olsun. Bu homomorfizmanın çekirdeği $C_G(M) = M$ olduğundan $G/M \cong G_1 \subseteq \text{Aut}(B)$ dir. O zaman (2) den dolayı $|G_1| = m$ dir. Öte yandan $\bar{k}$ bir sonlu cisim olduğundan $\text{Aut}(B) = \text{Gal}(\bar{k}/k)$ grubu devirlidir. O nedenle öyle bir $x \in G$ vardır ki $G_1 = \langle \Psi_x \rangle$ dir. Burada $\Psi_x = \Psi_x|_B$ alınmıştır. $o(\Psi_x) = m$ olduğundan $x^m \in M$ dir. O zaman $\bar{x}^m \in B$ dir. Bundan başka $\langle x, M \rangle = G$ olduğundan Ψ_x ile B birlikte eA basit cebirini üretir. Esasen $G_1 = \langle \Psi_x \rangle$ olduğundan $G = \langle x, M \rangle = \langle x \rangle M$ dir. Böylece $G = \bigcup_{i=0}^{m-1} Mx^i$

yazılabilir. Buradan $k[G] = \bigcup_{i=0}^{m-1} k[M]x^i$ olduğundan

$eA = \bigcup_{i=0}^{m-1} B\bar{x}^i$ yazılabilir. $\bar{x}$, x in eA içindeki görüntüsüdür.

Ψ_x in B içindeki merkezleyeni (sabit cismi) R olsun.

O zaman B abeliyan olduğundan R , B ve $\bar{x}$ tarafından merkezlenir.

Buradan $R \subseteq Z(eA)$ bulunur. Şimdi $z \in Z(eA)$ olsun.

$z = b\bar{x}^i$ olacak şekilde $b \in B$ ve $0 \leq i < m$ vardır. O

zaman $bx = xb$ ve B abeliyan olduğundan $b \in Z(eA)$ dir.

Buradan $\bar{x}^i \in Z(eA)$ olur. O zaman $\bar{x}^i$ B yı merkezlediğinden

x^i , M yi merkezlemelidir. Bu ise ancak $i = 0$ ise mümkündür. Böylece $z = b \in B$ bulunur. O zaman $Z(eA) \subseteq B$ olduğundan $Z(eA) \subseteq R$ dir. Buradan $Z(eA) = R$ bulunur. Böylece

$$(4) \quad [G:M] = [B:F] = [\bar{k}:\hat{k}]$$

elde edilir.

Şimdi (2), (3) ve (4) ten

$$t[\bar{k}:k] = m[\hat{k}:k] = [\bar{k}:\hat{k}][\hat{k}:k] = [\bar{k}:k]$$

olduğundan

$$(5) \quad t = 1$$

elde edilir.

(5) den dolayı $\dim_B V = 1$ olduğundan V bir indirgenmez B-modülüdür ve eğer $0 \neq v \in V$ ise $V = Bv$ yazılabilir.

Şimdi $\Phi: V \rightarrow \bar{k}^+$ ve $\phi: G \rightarrow \text{Gal}(\bar{k}/\hat{k})\bar{k}^X$ şöyle tanımlansınlar: $\Phi(bv) = b$, $\phi(x) = \Psi_x b_2$ Burada $b, b_2 \in B$ ve b_2 elemanı $xv = \Psi_x(b)v$ olacak şekilde tanımlıdır.

$$(a) \quad \phi(x)\Phi(v) = \phi(x).1 = \phi(x)$$

$$\Phi(xv) = \Phi(\Psi_x(b_2)v) = \Psi_x(b_2) = \phi(x)$$

olduğundan (a) sağlanır.

(b) $M = \langle y \rangle$ olsun. V bir sadık $k[M]$ -modülü olduğundan y nin B içindeki görüntüsü w ise yani $yv = wv$ ise o zaman $o(y) = o(w)$ olur. Bundan dolayı w, 1 in bir |M| yinci ilkel köküdür. Böylece $B = k(w)$ olur.

(c) $\phi(x) = \Psi_x b_2 \in \text{Gal}(\bar{k}/\hat{k})\bar{k}^X$ olduğundan $\Psi_x \in \phi(G)\bar{k}^X$ dir. Ayrıca $\langle \Psi_x \rangle = G_1 = \text{Gal}(\bar{k}/\hat{k})$ olduğundan $\phi(G)\bar{k}^X = \text{Gal}(\bar{k}/\hat{k})\bar{k}^X$ dir.

(d) $a \in \phi(G) \cap \bar{k}^X$ olsun. O zaman $a = \phi(x)$ olacak

şekilde $x \in G$ vardır. Eğer $x.v = \Psi_x(b_2)v$ ise $\phi(x) = \Psi_x b_2$ dir. Buradan $a = \Psi_x b_2$ bulunur. Böylece $\Psi_x b_2 \in \bar{k}^x$ dir. Fakat $\Psi_x \in \text{Gal}(\bar{k}/k)$ ve $\text{Gal}(\bar{k}/k) \cap \bar{k} = I$ olduğundan $\Psi_x = I$ dir. Buradan $x \in C_G(M) = M$ bulunur. Bundan dolayı $a = b_2 \in \phi(G) \cap B = \phi(M)$ dir.

Tanımdan dolayı $\phi: V \rightarrow B$ bir k -izomorfizması ve $B \cong \bar{k}$ olduğundan $\bar{V} \cong \bar{k}^+$ dir. Bundan dolayı $V = \bar{k}^+$ alabiliriz.

Şimdi $x, y \in G$ olsun. $xv = \Psi_x(b_2)v$ ve $yv = \Psi_y(b'_2)v$ olsun. O zaman $\phi(x) = \Psi_x b_2$ ve $\phi(y) = \Psi_y b'_2$ dir.

$$\phi(x)\phi(y) = \Psi_x b_2 \Psi_y b'_2 = \Psi_x \Psi_y \Psi_y^{-1}(b_2)b'_2 = \Psi_{xy} \Psi_y^{-1}(b_2)b'_2$$

$$\begin{aligned} (xy)v &= x(yv) = x(\Psi_y(b'_2)v) = \Psi_x(\Psi_y(b'_2)\Psi_x(b_2))x \\ &= \Psi_x \Psi_y(b'_2 \Psi_y^{-1}(b_2))v = \Psi_{xy}(b'_2 \Psi_y^{-1}(b_2))v \end{aligned}$$

Bundan dolayı

$$\phi(xy) = \Psi_{xy} b'_2 \Psi_y^{-1}(b_2)$$

ve böylece $\phi(xy) = \phi(x)\phi(y)$ dir.

Şimdi $G \cong \phi(G)$ olduğundan G yi $\phi(G)$ ile özdeş kılarsak $G = \phi(G)$ alabiliriz. O zaman $G \leq \mathcal{T}$ ve $G \cap \bar{k}^x = M$ dir.

3.6. TEOREM : $\mathcal{T} = \mathcal{G}\bar{k}^x$ grubu $\Omega = \bar{k}^+ \setminus \{0\}$ üzerinde bir permütasyon grubu olarak göz önüne alınsın. O zaman $\mathcal{T}$ nin Ω üzerindeki permütasyon temsili $1_{\mathcal{G}}|_{\mathcal{T}}$ temsiline izomorftur. Böylece A, Ω üzerinde $\Sigma(1_{\mathcal{G}^{x-1}} \cap A |_{\mathcal{T}})^A$ üzerindeki gibi etki eder. Burada toplam bütün $Ax\mathcal{G}$ çift kosetleri üzerinde değişir.

İSPAT : $W = \bigoplus_{x \in \bar{k}} km_x, \mathcal{T}$ nin permütasyon modülü olsun. $\mathcal{T}$ nin V üzerindeki temsili T ise T ye $\mathcal{T}$ nin Ω üzerindeki permütasyon temsili denir. Biz $T = 1_{\mathcal{G}}|_{\mathcal{T}}$ olduğunu göstereceğiz. Burada $1_{\mathcal{G}}, \mathcal{G}$ nin aşikar temsilidir.

$\sigma \in \mathcal{G}$ ve $\mu \in \bar{k}^x$ olsun. $(\sigma\mu).1 = 1$ ise $\sigma(\mu) = 1$ olduğundan $\mu = 1$ olmalıdır. Yani 1 in $\mathcal{T}$ içindeki dengeleyicisi $\mathcal{G}$ dir. O zaman km_1 altmodülünün dengeleyeni de $\mathcal{G}$ dir. Öte yandan $r, s \in \bar{k}$ olsun.

$$s.(rm_x) \neq rm_{sx}$$

olarak tanımlı olduğundan, buradan

$$rm_x = x(rm_1)$$

olduğu görülür. Böylece

$$W = \bigoplus_{x \in \bar{k}^x} x(km_1)$$

olarak yazılabilir. Ayrıca $\bar{k}^x, \mathcal{G}$ nin $\mathcal{T}$ içindeki sol kosetlerinin bir tam kümesidir. Şimdi Teorem 1.15 den dolayı $W \cong km_1|_{\mathcal{T}}$ dir. km_1 aşikar $\mathcal{G}$ modülü olduğundan T ile $1_{\mathcal{G}}|_{\mathcal{T}}$ eşdeğerdir. Böylece özel olarak A nın üzerindeki etkisi yani W_A üzerindeki etkisi $\bar{k}m_1|_{\mathcal{T}}|_A$ üzerindeki etkisinin aynıdır. Fakat Mackey altgrup Teoreminden dolayı

$$km_1|_{\mathcal{T}}|_A = \bigoplus ((km_1)_{C^{x^{-1}} \cap A})|_A$$

oldüğundan iddianın ikinci kısmı da gösterilmiş olur.

Burada toplam $A \rtimes \mathcal{G}$ çift kosetleri üzerinde değişir.

Yukarıdaki teoremden görüldüğü gibi A nın Ω üzerindeki etkisi

$$km_1|_{\mathcal{T}}|_A = \bigoplus ((km_1)_{\mathcal{G}^{x^{-1}} \cap A})|_A$$

üzerindeki etkisinin aynıdır. Şimdi $A, \bar{k}m_1|_{\mathcal{T}}|_A$ üzerinde soldan çarpma şeklinde etki eder.

Kabul edelim ki bir $x \in \bar{k}^+ \setminus \{0\}$ için $\mathcal{G}^{x^{-1}} \cap A = \langle 1 \rangle$ olsun. O zaman

$$(k m_1)_{\langle 1 \rangle} |^A = k[A] \otimes_k (k m_1) \cong k[A] \otimes_k k = k[A]$$

olduğundan regüler $\bar{k}[A]$ modülüne izomorftur. O zaman $k[A]$ modülü regüler A yörüngesi içerdiğinden A nın Ω üzerinde bir regüler yörüngesi olacaktır. Burada yukarıdaki şekilde ikiden fazla x olmayacak şekilde $\mathcal{J}$ ve $\mathcal{G}$ yi belirlemek istiyoruz.

Şimdi bir genişleme Lemması ispat edeceğiz. A nın $A \cap \bar{k}^x = A \cap M = A_0$ üzerinde parçalandığını göstereceğiz. Bunun için A yı biraz genişleteceğiz.

3.7. LEMMA : $|A_0|$ sayısını bölen asal sayıların kümesi π olsun. O zaman $\bar{k}^x$ in öyle bir π -altgrubu $\bar{A}_0$ vardır ki $A_0 \leq \bar{A}_0$, $\bar{A} = A\bar{A}_0$ ve $\bar{G} = \bar{A}\bar{B}$ dir. Böylece $\bar{G}$ Hipotez 3.1 i sağlar ve $\bar{A}$, $\bar{A} \cap \bar{k}^x = \bar{A}_0$ in bir parçalanma genişlemesidir. Yani; $\bar{A} = \bar{A}_0 Y$ ve $\bar{A}_0 \cap Y = 1$ olacak şekilde $Y \subseteq \bar{A}$ vardır.

İSPAT : A nın bir Sylow q -altgrubu Q olsun. Eğer her q için Q , $Q \cap \bar{k}^x = Q \cap A_0$ üzerinde parçalanır ise o zaman A nilpotent olduğundan, A_0 üzerinde de parçalanır. Bu durumda $\bar{G} = G$ alınabilir.

Kabul edelim ki $Q_0 = Q \cap A_0 \neq 1$ olsun. $\bar{k}^x$ in Sylow q -altgrubu Q_1 olsun. Q_1 devirlidir ve A , Q_1 üzerinde $\mathcal{G}$ gibi yani eşlenikleme şeklinde etki eder. Fakat A nilpotent olduğundan A nın her q' -altgrubu Q_0 ı merkezler. $1 \neq Q_0 \leq Q_1$ dir. Ayrıca Q_1 devirlidir. Şimdi A nın q' -altgrupları $Q_0 \neq \langle 1 \rangle$ i merkezlediğinden Q_1 i de merkezler.

$$|\mathcal{G}|_q = |G\bar{k}^x : \bar{k}^x|_q = |G : G \cap \bar{k}^x|_q = |AM : AM \cap \bar{k}^x|_q = |AM : M|_q$$

$$= |A : A \cap M|_q = |Q : Q \cap M| = |Q : Q \cap A_0| = |Q : Q_0| = |QQ_1 : Q_1|$$

$$\Rightarrow |\mathcal{G}\bar{k}^x|_q = |\mathcal{G}|_q |\bar{k}^x|_q = |QQ_1|$$

olduğundan $QQ_1, \mathcal{G}\bar{k}^x = \mathcal{J}$ grubunun bir Sylow q -altgrubudur. O zaman $\mathcal{J} = \mathcal{G}\bar{k}^x$, $\bar{k}^x$ in parçalanma genişlemesi olduğundan QQ_1 de Q_1 in parçalanma genişlemesidir. Ayrıca A nın q' -elemanları Q_1 i merkezlediğinden AQ_1 nilpotenttir.

Şimdi A nın her parçalanmış olmayan Sylow altgrubu Q için Q_1 , yukarıdaki gibi tanımlansın. Bu Q_1 ler tarafından üretilen altgrup A_1 olsun. $A_1 \leq \bar{k}^x$ ve $A_1 \triangle \mathcal{J}$ dir. $\bar{A}_0 = A_0 A_1$ olsun. O zaman $\bar{A} = A\bar{A}_0$ nilpotenttir ve de parçalanmış Sylow altgruplarına sahiptir.

$\bar{G} = \bar{A}B$ ise $\bar{G}$ nin Hipotez 3.1 i sağladığı kolayca görülür.

Bundan sonra $A = CA_0$ ve $C \cap A_0 = 1$ olduğu halleri, yani; A nın A_0 in parçalanmış genişlemesi olduğu halleri gözönüne alacağız.

3.8. LEMMA : Eğer $A \in CA_0, A_0$ ise C nin bir parçalanmış genişlemesi ise o zaman bir $w \in \bar{k}^x$ için $wCw^{-1} = \mathcal{G}$ dir.

İSPAT : $\sigma \in \mathcal{G}, \mu \in \bar{k}^x$ olmak üzere $\sigma\mu$, C nin üreteci olsun. Eğer $o(\sigma) = n$ ise o zaman $o(\sigma\mu) = n$ dir. Çünkü;

$$(\sigma\mu)^n = (\sigma\mu)(\sigma\mu) \dots (\sigma\mu)$$

$$= \sigma^n \mu (\sigma^{-1} \mu \sigma) \dots (\sigma^{-(n-1)} \mu \sigma^{n-1})$$

$$= \mu (\sigma^{-1} \mu \sigma) \dots (\sigma^{-(n-1)} \mu \sigma^{n-1})$$

olduğundan $(\sigma\mu)^n \in C \cap \bar{k}^x \subseteq A \cap \bar{k}^x = A_0$ dir. O zaman

$(\sigma\mu)^n \in C \cap A_0 = 1$ olduğundan $(\sigma\mu)^n = 1$ dir. Ayrıca $n | o(\sigma\mu)$ olduğu aşikardır. Buradan $n = o(\sigma\mu)$ elde edilir. Böylece

$$1 = (\sigma\mu)^n = (\sigma^{-1}\mu\sigma) \dots (\sigma^{-(n-1)}\mu\sigma^{n-1})$$

bulunur. Diğer yandan $\mathcal{G}\bar{k}^x = G\bar{k}^x$ olduğundan

$$\begin{aligned} G\bar{k}^x / \bar{k}^x &\cong G / (G \cap \bar{k}^x) = AM / M \cong A / (A \cap M) = A / (A \cap \bar{k}^x) \\ &= A / A_0 = CA_0 / A_0 \cong C / (C \cap A_0) \cong C \end{aligned}$$

yani;

$$\mathcal{G}\bar{k}^x / \bar{k}^x \cong C$$

dir. Fakat $\mathcal{G}\bar{k}^x / \bar{k}^x \cong \mathcal{G}$ olduğundan $\mathcal{G} \cong C$ dir. Bundan dolayı $\mathcal{G} = \langle \sigma \rangle$ dir.

Şimdi $N = N_{\bar{k}} \rightarrow \hat{k}$ norm fonksiyonunu gözönüne alalım. $N(\mu) = \prod_{\alpha \in \mathcal{G}} \alpha(\mu) = \prod_{i=1} \alpha^i(\mu) = \mu\sigma(\mu) \dots \sigma^{n-1}(\mu) = 1$ dir.

O zaman Hilbertin 90. teoreminden dolayı, öyle bir $w \in \bar{k}^x$ vardırki $\sigma^{-1}(w^{-1})w = \mu$ dir. O zaman

$w(\sigma w)w^{-1} = \sigma(\sigma^{-1}w\sigma)\mu w^{-1} = \sigma(\sigma^{-1}(w))\mu w^{-1} = \sigma(\mu^{-1}w)\mu w^{-1} = \sigma$ elde edilir. Bundan dolayı

$$wCw^{-1} = \mathcal{G}$$

dir.

Şimdi $\bar{k}^x \triangleleft \mathcal{T}$ olduğundan G nin $\bar{k}^x$ üzerindeki yörüngeleri G nin $\mathcal{T}$ içindeki herhangi bir eşleniğinin yörüngesinin aynıdır. Bundan dolayı parçalanmış genişleme halinde $G = \mathcal{G}M$ ve $A = \mathcal{G}A_0$ alabiliriz. Bundan başka parçalanmış olmayan genişleme halinde ise Lemma 3.7 den dolayı $\bar{G} = \mathcal{G}\bar{M}$ ve $\bar{A} = \mathcal{G}\bar{A}_0$ olarak tanımlayıp, $G \leq \bar{G}$ olduğunu kabul ederiz.

3.9. LEMMA : $A = \mathcal{G}A_0$ olsun. Her $p \mid |\mathcal{G}|$ için $\sigma_p \in \mathcal{G}$ mertebesi p olan elemanı olsun. $\sigma_p^{-1}(w)w^{-1} \in A_0$ olan her $w \in \bar{k}^X$ elemanlarının oluşturduğu altgrup J_p olsun. $x \in \bar{k}^X$ olsun. O zaman $\mathcal{G}^x \cap A = 1$ olması için gerek ve yeter şart her $p \mid |\mathcal{G}|$ için $x \notin J_p$ olmasıdır.

İSPAT : $x \in J_p$ olsun. O zaman $\sigma_p^{-1}(x^{-1})x = \mu \in A_0$ dır. Fakat

$x^{-1}\sigma_p x = \sigma_p[\sigma_p^{-1}(x^{-1})]x = \sigma_p \mu \in \mathcal{G}A_0 = A$ olduğundan olduğundan $\sigma_p \mu \in \mathcal{G}^x \cap A$ dır. Bundan dolayı $x \notin J_p$ dir.

Şimdi ise $\mathcal{G}^x \cap A \neq 1$ ve $p \mid |\mathcal{G}^x \cap A|$ olsun. Bu kesişimin mertebesi p olan bir elemanı $\sigma_p \mu$ olsun. O zaman $\mathcal{G}$ devirli olduğundan $\sigma_p \mu = (x^{-1}\sigma_p x)^i = x^{-1}\sigma_p^i x$ şeklinde yazılabilir. Buradan $\sigma_p^{-i} x^{-1}\sigma_p^i x = \sigma_p^{-i+1} \mu \in \bar{k}^X$ olduğundan $\sigma_p^{-i+1} = 1$ ve $i = 1$ bulunur. Böylece $x^{-1}\sigma_p x = \sigma_p \mu$ dır. Buradan $\mu = \sigma_p^{-1} x^{-1}\sigma_p x = \sigma_p^{-1}(x^{-1})x \in A_0$ olduğundan $x \in J_p$ olmalıdır.

3.10. LEMMA : $A = \mathcal{G}A_0$ ve $w, v \in \bar{k}^X$ olsun. O zaman $Aw\mathcal{G} = Av\mathcal{G}$ olması için gerek ve yeter şart bir $\sigma \in \mathcal{G}$ için

$$\sigma(w)A_0 = vA_0$$

olmasıdır.

İSPAT : Kabul edelim ki $Aw\mathcal{G} = Av\mathcal{G}$ olsun. O zaman $\mu \in A_0$ ve $\sigma, \tau \in \mathcal{G}$ olmak üzere;

$$w = (\sigma\mu)\tau = \sigma\tau\tau^{-1}(\mu v)\tau = (\sigma\tau)[\tau^{-1}(\mu v)]$$

olsun. O zaman $w \in \bar{k}^X$ olduğundan

$$\sigma\tau = 1 \Rightarrow \sigma = \tau^{-1}$$

dir. Böylece

$$w = \tau^{-1}(\mu v) = \sigma(\mu v) = \sigma(\mu)\sigma(v) = \sigma(v)\sigma(\mu) \in \sigma(v)A_0$$

$$\Rightarrow w \in \sigma(v)A_0 \Rightarrow wA_0 = \sigma(v)A_0$$

dir.

Tersine olarak $\sigma(w)A_0 = vA_0$ olsun. O zaman $\mu \in A_0$ olmak üzere $v = \sigma(w)\mu$ olarak yazılabilir. Fakat

$$v = \sigma(w)\mu = \sigma w \sigma^{-1} \mu = \mu \sigma w \sigma^{-1} = \sigma(\sigma^{-1} \mu \sigma) w \sigma^{-1} = \sigma[\sigma^{-1}(\mu)w] w \sigma^{-1}$$

olduğundan $v \in Aw\mathcal{G}$ dir. Bundan dolayı

$$Aw\mathcal{G} = Av\mathcal{G}$$

dir.

Ayrıca Lemma 3.3 (b) den dolayı $(|A_0|, |B|) = 1$ dir. Bundan başka eğer $|A_0|$, bölen asalların sayısı π ise o zaman B yi $\bar{k}^x$ in bir Hall π' -altgrubuna genişletmek hipotez 3.1 i etkilemez.

Şimdi aşağıdaki kabulleri yapalım.

3.11. HİPOTEZ : $G < \mathcal{T}$, $G \cap \bar{k}^x = M$ $M \neq G$, $A_0 = A \cap M$
 $M = A_0 \times B$ olsun ve $A = \mathcal{G}A_0$, hipotez 3.1 i sağlasın. Eğer $|A_0|$ 1 bölen asal sayıların kümesi π ise, o zaman B, $\bar{k}^x$ nin bir Hall π' altgrubu olur.

(a) Her $p \mid |\mathcal{G}|$ için $J_p \neq \bar{k}^x$.

(b) $C_G(B) = M$.

3.12. LEMMA : G , Hipotez 3.11 i sağlasın, fakat (a) veya (b) den biri sağlanmasın. O zaman

(a) $\bar{k} = GF(r^2)$

(b) $r \equiv -1 \pmod{4}$

(c) $2^t = r + 1$

(d) $B \leq GF(r)$ dir.

İSPAT : Lemma 3.3 den dolayı $[C_G(B):M] = 1,2$ dir. Önce hipotez 3.11 (a) yanlış olsun. O zaman (b) nin de yanlış olduğunu gösterelim.

Kabul edelim ki bir $p \mid |\mathcal{G}|$ için $J_p = \bar{k}^x$ olsun. $\sigma \in \mathcal{G}$ mertebesi p olsun bir eleman olsun. Eğer $w \in \bar{k}^x$ ise

$$(\sigma-1)w = w^{\sigma-1} = \sigma(w)w^{-1} \in A_0$$

olduğundan

$$(\sigma-1)\bar{k}^x \leq A_0$$

dir. Buradan

$$(\sigma-1)B \leq B \cap A_0 = 1$$

bulunur. O zaman $b \in B$ ise $(\sigma-1)b = \sigma(b)b^{-1} = 1$, yani $\sigma(b) = b$ dir. Bundan dolayı $\sigma \in C_G(B)$ dir. Ayrıca $G = \mathcal{G}M$ ve $\mathcal{G} \cap M = 1$ olduğundan $\sigma \in C_G(B) \setminus M$ dir. Buradan $M < C_G(B)$ ve $[C_G(B):M] = 2$ dir. Bu bir gelişkidir.

Şimdi ise Hipotez 3.11 (b) yanlış olsun. O zaman $[C_G(B):M] = 2$ dir. $\sigma \in \mathcal{G}$ ve $o(\sigma) = 2$ olsun. O zaman $\sigma \in C_G(B)$ dir.

$\bar{k} = GF(r^{2m})$ ve $\bar{\mathcal{G}} = \text{Gal}(\bar{k}/k)$ olsun. O zaman $\bar{\mathcal{G}}$ devirli dir ve $|\bar{\mathcal{G}}| = 2m$ dir. Şimdi $C_G(B)$ nin bir Sylow 2-alt-grubu T olsun. O zaman $T = (M \cap T) \langle \sigma \rangle$ dir.

$(M \cap T) \cap \langle \sigma \rangle = 1$ olduğundan T nin en az iki involosyonu vardır. O zaman Lemma 3.3 den dolayı T dihedral veya yarıdihedraldir. $|T| = 2^n$ olsun. Bu durumda σ bir kare olamaz. Mümkünse $\sigma = \tau^2$ olacak şekilde $\tau \in \mathcal{G}$ olsun. Şimdi

$T \cap M = \langle t \rangle$ olsun. O zaman $o(t) = 2^{n-1}$ dir. T dihedral

ya da yarıdihedral olduğundan $\sigma t \sigma = t^{-1}$ veya $\sigma t \sigma^{-1} = t^{-1+2^{n-2}}$

($n > 3$) dir. $t_1 = t^{2^{n-3}}$ olsun. O zaman $o(t_1) = 2^{n-1}/(2^{n-1}, 2^{n-3}) = 4$

dür. Yukarıdan görüldüğü gibi $\sigma t_1 \sigma \neq t_1$ olduğundan $\sigma t_1 \sigma = t_1^{-1}$ dir. Fakat o zaman $\tau^{-1} t_1 \tau = t_1^{-1}$ olmalıdır. Buradan $\sigma t_1 \sigma = t_1$ elde edilir, bu bir çelişkidir. Bundan dolayı σ bir kare değildir. Şimdi σ , $k = GF(r)$ yi sabit bıraktığından eğer $4 \mid r-1$ ise o zaman σ , mertebesi 4 olan bir elemanı merkezler. Fakat $\sigma^{-1} t \sigma = t^{-1}$ veya $\sigma t \sigma = t^{-1+2^{n-2}}$ olduğundan bu imkansızdır. Bundan dolayı $4 \nmid r-1$ dir. O zaman $4 \mid r+1$, yani $r \equiv -1 \pmod{4}$ olmalıdır. Ayrıca σ kare olmadığından $4 \nmid 2m$ dir. Dolayısıyla m tek sayıdır. Şimdi $2^t \parallel r^m + 1$ ve $s \mid r^m + 1$ bir asal tek sayı olsun. Ayrıca σ yi $\sigma: x \rightarrow x^{r^m}$ olarak tanımlayabiliriz. $w \in \bar{k}^x$ elemanının mertebesi s olsun. O zaman $\sigma(w) = w^{r^m+1-1} = w^{-1}$ $\langle \sigma, w \rangle$ mertebesi $2s$ olan bir dihedral gruptur ve nilpotent olmadığından $s \nmid |A_0|$ dir. B , $\bar{k}^x$ nin Hall π' -altgrubu olduğundan $s \mid |B|$ dir. Buradan $w \in B = C_G(\sigma)$ dir. Bu bir çelişkidir. Bundan dolayı s mevcut değildir. Dolayısıyla $r^m + 1 = 2^t = r + 1$ hiç bir asal tek sayı ile bölünmez ve böylece $m = 1$ dir.

Son olarak $(|B|, |A_0|) = 1$ olduğundan $|B|$ tektir ve $B \leq GF(r)$ dir.

Şimdi hipotez 3.11 sağlansın. Eğer $w, \bar{k}^x$ in bir üretici ise her $p \mid |\mathcal{G}|$ için $w \notin J_p$ dir. $\bar{k}^x/A_0$ grubunun üreticilerinin bir kümesi B olsun. Kabul edelim ki $\sigma \in \mathcal{G}$ nin mertebesi q asal sayısı olsun ve $\sigma, vA_0 \in B$ elemanını sabit bıraksın. O zaman, her $a \in A_0$ için $\sigma(va) = va'$ olacak şekilde $a' \in A_0$ olduğundan $\sigma(v)a = va'$ ve buradan $\sigma(v)v^{-1} \in A_0$ bulunur. Böylece $v \in J_p$ elde edilir. Fakat, eğer $v, \bar{k}^x$ in bir üretici ise Hipotez 3.11 (a) dan dolayı

bu imkansızdır.

Şimdi vA_0 bir üreteç ise $\bar{k}^x$ bir üreticini içerdiğini gösterelim. $\bar{k}^x$ nın bir üretici b olmak üzere $v = b^s$ olsun. $o(b) = n$, $A_0 = \langle b^s \rangle$ olsun. $\bar{k}^x/A_0 = \langle bA_0 \rangle$ ve $(bA_0)^t = b^t A_0 = A_0$ olduğundan $o(\bar{k}^x/A_0) = t$ dir. O zaman $o(b^s A_0) = o(vA_0) = t$ dir. Çünkü vA_0 bir üreteçtir. Ayrıca b yi $\langle b \rangle$ nin uygun bir elemanı ile değiştirerek $t|n$ olduğunu kabul edebiliriz. Şimdi;

$$o(b^s A_0) = o(bA_0)^s = \frac{t}{(t,s)} = t$$

oldüğundan $(t,s) = 1$ dir. $vA_0 = b^s \langle b^t \rangle$ nin elemanları $o \leq i \leq \frac{n}{t}$ olmak üzere b^{s+it} şeklindedir. Eğer $(s,n) = 1$ ise o zaman b^s , $\bar{k}^x$ ın bir üreticidir ve $b^s \in vA_0$ dir. Kabul edelim ki $(s,n) = d > 1$ olsun. Şimdi $n = n_1 n_2$ öyle ki n_1 in asal bölenleri d nin asal bölenleri ve $(n_2, d) = 1$ olsun. Ayrıca $(s + n_2 t, n) = k$ olsun. Eğer $p|k$ ise $p|n$ olduğundan $p|n_2$ veya $p|n_1$ dir. Eğer $p|n_2$ ise $p|s + n_2 t$ olduğundan $p|s$ dir. O zaman $p|d$ dir. Bu ise bir çelişkidir. Öyleyse $p|n_1$ dir. n_1 in asal bölenleri d nin de asal bölenleri olduğundan $p|s$ dir. Fakat $p|s + n_2 t$ ve $p \nmid n_2$ olduğundan $p|t$ dir. Buradan $p|(s,t) = 1$ dir. Bu tekrar bir çelişki verir. O halde $k = 1$ ve $(s + n_2 t, n) = 1$ elde edilir. Bundan dolayı $b^{s+n_2 t} \in vA_0$ bir üreteçtir. Böylece v , $\bar{k}^x$ nın bir üretici olarak alınabildiğinden $\sigma(v)v^{-1} \notin A_0$ dir. Bundan dolayı vA_0, σ tarafından sabit bırakılamaz. Böylece $\mathcal{G}$ nin vA_0 ı içeren yörüngesi regüler yörüngedir. Çünkü Hipotez 3.11 sağlanırsa o zaman her $p \in |\mathcal{G}|$ için $J_p \neq \bar{k}^x$ dir. Öyleyse x , $\bar{k}^x$ ın bir ürete-

ci ise $x \notin J_p$ dir. Böylece Lemma 3.9 dan dolayı $\mathcal{G}^x \cap A = 1$ dir ve Teorem 3.6 nın sonunda yapılan açıklamadan dolayı A nın Ω üzerinde bir regüler yörüngesi vardır. Şimdi eğer $\bar{k}^x/A_0$ nın bir üretici vA_0 ise bu koset $\bar{k}^x$ nın bir üreticini içerir. Bu üretici v olsun. Eğer bir $\sigma_p \in \mathcal{G}$ için $\sigma_p(vA_0) = vA_0$ ise o zaman yukarıda görüldüğü gibi $v \in J_p$ ve $J_p = \bar{k}^x$ olur. Fakat bu imkansızdır. Çünkü Hipotez 3.11 sağlanmaktadır. Bundan dolayı σ_p nin vA_0 üreticileri üzerindeki etkisi regülerdir, yani sabit noktasız etki eder. Böylece $\mathcal{G}$, $\bar{k}^x/A_0$ ın üreticileri üzerinde yarı regülerdir.

Böylece aşağıdaki Lemma ispatlanmış olur.

3.13. LEMMA : Eğer Hipotez 3.11 sağlanırsa $\mathcal{G}$, $\bar{k}^x/A_0$ ın üreticileri üzerinde yarı regülerdir. Yani, her üretici bir regüler yörünge tanımlar.

Artık $\bar{k}^x/A_0$ grubunun yapısını kısıtlayacağız.

3.14. LEMMA : Kabul edelim ki Hipotez 3.11 sağlansın, fakat A nın $\bar{k}^+$ üzerindeki etkisinde üç regüler yörünge bulunmasın. O zaman p ve q asal tek sayılar olmak üzere aşağıdakilerden biri sağlanır.

(a) $|B| = pq$, $|\mathcal{G}| = (p-1)(q-1)/2$ bir tek sayı ve $[\bar{k}^x : BA_0] = 1, 2$ dir.

(b) $|B| = 2p$, $|\mathcal{G}| = (p-1)/2$ tek sayı ve $[\bar{k}^x : BA_0] = 1$ dir.

(c) $|B| = p$ ve $|\mathcal{G}| = (p-1)/\delta$ dir. Burada $[\bar{k}^x : BA_0]$ ve δ değerleri aşağıda verilmiştir.

$[\bar{k}^x : BA_0]$	δ
1	1, 2
2	1, 2
4	1

İSPAT : $x \in \bar{k}^x$ ve $x \neq 0$ olsun. A nın x i içeren yörüngelerinin regüler olması için genel ve yeter koşul $\mathcal{G}$ nin xA_0 1 içeren yörüngeşinin regüler olmasıdır. Bunun için A nın x i sabit bırakan bir eleman varsa, $\mathcal{G}$ nin de xA_0 1, sabit bırakan bir elemanı olduğunu göstermeliyiz.

Kabul edelim ki $\sigma \in \mathcal{G}$ ve $a_0 \in A_0$ olmak üzere

$$\sigma a_0 \cdot x = x \text{ olsun.}$$

O zaman

$$\sigma(a_0 x) = x \Rightarrow a_0 \sigma(x) = x \Rightarrow \sigma^{-1}(x)x = a_0 \in A_0$$

dır.

Şimdi, $x\sigma x^{-1} = \sigma(\sigma^{-1}(x))x^{-1} = \sigma a_0 \in A$ olduğundan $x\sigma x^{-1} \in \mathcal{G}^x \cap A$ dır. Öyleyse x in regüler yörünge tanımlaması için gerek ve yeter şart $\mathcal{G}^x \cap A = 1$ olmasıdır. Şimdi Lemma 3.9 dan dolayı $\mathcal{G}^x \cap A = 1$ olması için gerek ve yeter şart $\sigma(x)x^{-1} \notin A_0$ olduğundan $\sigma(xA_0) \neq xA_0$ olmasıdır. Yani xA_0 ın regüler yörünge tanımlamasıdır.

Bundan dolayı $\mathcal{G}$ nin $\bar{k}^x/A_0$ üzerinde üçten az regüler yörüngeye sahip olduğunu kabul edebiliriz. $\bar{B} = BA_0/A_0$ olsun. $\bar{B} \cong B$ Hall grubu olduğundan $\bar{k}^x/A_0 = \bar{C} \times \bar{B}$ şeklinde yazılabilir. Şimdi $C_G(B) = M \leq \bar{k}^x$ ve $G = \mathcal{G}M$ olduğundan

$$\begin{aligned} G/C_G(B) &\tilde{C} \text{ Aut}(B) \Rightarrow \mathcal{G}M/M \tilde{C} \text{ Aut}(B) \\ &\Rightarrow \mathcal{G} \tilde{C} \text{ Aut}(B) \end{aligned}$$

dır.

Bundan dolayı $\mathcal{G} \leq \text{Aut}(\bar{B})$ olduğunu kabul edebiliriz. O zaman Lemma 3.13 den dolayı $\mathcal{G}$, $\bar{B}$ nin üreteçleri üzerinde yarı regülerlerdir. $\bar{k}^x/A_0 = \bar{C} \times \bar{B}$ üzerindeki regüler yö-

rüngelerinin sayısı; $c = |C|$, $b = |B|$ ve ϕ Euler F_1 -fonksiyonu olmak üzere

$$\frac{\phi(c) \cdot \phi(b)}{|\mathcal{G}|} \leq 2$$

dir. Ayrıca B devirli olduğundan $|\text{Aut}(B)| = \phi(b)$ dir. Bundan dolayı $[\text{Aut}(\bar{B}) : \mathcal{G}] \leq 2$ dir. Şimdi $\bar{B}$ devirli olduğundan $\text{Aut}(\bar{B})$ devirlidir veya $\text{Aut}(\bar{B}) \cong \mathbb{Z} \times \mathcal{G}$ dir.

Şimdi Euler F_1 -fonksiyonunun özelliklerinden aşağıdakiler ifade edilebilir.

(i) $\text{Aut}(\bar{B})$ devirli olsun. Eğer $|B| = b$ ise $\text{Aut}(\bar{B})$, $\mathbb{Z}_b$ nin bilimsellerinin çarpım grubuna izomorf ve $|\text{Aut}(B)| = \phi(b)$ dir. Bundan dolayı eğer $\text{Aut}(B)$ devirli ise o zaman b modülüne göre bir ilkel kök vardır. O zaman $b > 2$ olduğundan $b = 4$ veya p asal teksayı olmak üzere $b = p^e$, $2p^e$ tipindedir.

(ii) Eğer $\text{Aut}(\bar{B}) \cong \mathbb{Z}_2 \times \mathcal{G}$ ve $|\mathcal{G}|$ çift ise o zaman p ve q asal tek sayılar olmak üzere $|\bar{B}| = 2^t$ ($t > 2$), $4p^e$, $p^e q^t$ veya $2p^e q^f$ dir.

$|\mathcal{G}| > 1$ ve $[\text{Aut}(B) : \mathcal{G}] \leq 2$ olduğundan $2 \mid |\mathcal{G}|$ olması için şartlar verebiliriz.

(iii) $\text{Aut}(\bar{B})$ nin devirli olması ve p bir asal tek sayı olmak üzere $|\bar{B}| = p^e$ veya $p \equiv -1 \pmod{4}$ olmak üzere $|\bar{B}| = 2p^e$ olması ve $[\text{Aut}(\bar{B}) : \mathcal{G}] \neq 2$ hali dışında daima $2 \mid |\mathcal{G}|$ dir.

(iv) Eğer $2 \mid |\mathcal{G}|$ ve $2 \mid |B|$ ise $8 \mid |B|$ dir. Bunun için $\bar{k} = \text{GF}(r^m)$ olsun. Kabul edelim ki 2 sayısı $|B|$ ve $|\mathcal{G}|$ ni bölsün. $|\text{Gal}(\bar{k}/k)| = m$ olduğundan $|\mathcal{G}| \mid m$ dir. Buradan $2 \mid m$ dir. Ayrıca $|B| \mid (r^m - 1)$ ve $2 \mid |B|$ olduğundan $2 \mid (r^m - 1)$

dir. Bu durumda r^m sayısı tek olmalıdır. O halde r tek-
tir. $2|m$ olduğu için $m = 2k$ ve ayrıca r tek olduğundan
 $r^k = 2\ell - 1$ şeklinde yazılabilir. O halde

$$\begin{aligned}(r^m - 1) &= (r^{2k} - 1) = (r^k - 1)(r^k + 1) \\ &= (2\ell - 1 - 1)(2\ell - 1 + 1) = 4(\ell - 1)\ell\end{aligned}$$

dir. Fakat $(\ell - 1)$ ile ℓ ardışık olduğundan $2 | (\ell - 1)\ell$ dir.
Bundan dolayı $8 | (r^m - 1)$ dir. Fakat B , $\bar{k}^x$ nin bir Hall alt-
grubu olduğundan $8 || B|$ olmalıdır.

(ii) ve (iv) den dolayı $|B| = 4$, $4p^e$ ve $2p^e q^f$ halle-
ri olamaz. Bu durumlarda $8 \nmid |B|$ olduğundan (iv) den dolayı
 $2 \nmid |\mathcal{G}|$ dir. Çünkü bu hallerde $2 || B|$ ve $2 || \mathcal{G}|$ dir. O zaman
(iv) den dolayı $8 || B|$ dir. Bu çelişkidir. Eğer $|\bar{B}| = 2p^e$
ise tekrar (iii) den dolayı $p \equiv -1 \pmod{4}$ ve $[\text{Aut}(B) : \mathcal{G}] = 2$
dir.

(v) Eğer $\mathcal{G} = \text{Aut}(\bar{B})$ ise $\text{Aut}(\bar{B})$ devirli ve böylece
(i) den dolayı $|\bar{B}| = p^e$, $2p^e$ dir. Eğer $|\bar{B}| = 2p^e$ ise $2 || \bar{B}|$,
 $4 \nmid |\bar{B}|$ dir. Fakat $2 || \mathcal{G}|$ olduğundan (iv) den dolayı $8 || B|$
dir. Bu bir çelişkidir. Böylece $|\bar{B}| = p^e$ dir.

Eğer $[\text{Aut}(\bar{B}) : \mathcal{G}] = 2$ ise o zaman (i), (ii) den ve
yukarıdaki açıklamadan dolayı $|B| = p^e$, $2p^e$ ($p \equiv -1 \pmod{4}$),
 2^t ($t > 2$) ya da $p^e q^f$ olabilir.

(vi) Eğer p tek olmak üzere $p^e || B|$ olduğundan $e = 1$
dir.

Kabul edelim ki $e > 1$ olsun. O zaman $p^{e-1} || \mathcal{G}|$ dir.
 $\sigma \in \mathcal{G}$ mertebesi p olan bir eleman olsun. Eğer q , $|B|$ yi
bölen bir asal sayı ve $p \neq q$ ise o zaman $\mathcal{G}$, biri mertebe-
si $p^{e-1}(p-1)/2$ ve diğerinin mertebesi $q-1$ olan iki devir-

li grubun direkt çarpımını içerir. Fakat $\mathcal{G}$ devirli olduğundan $(p, q-1) = 1$ olmalıdır. O zaman σ , B nin S_q -alt-grubunu merkezler. Çünkü $|S_q| = q^f$ olduğunda $|\text{Aut}(S_q)| = q^{f-1}(q-1)$ dir. Fakat $(p, q(q-1)) = 1$ olduğundan σ , S_q yu merkezlemek zorundadır. Buradan görüldüğü gibi $p \nmid |\text{Aut}(S_q)|$ dur. Böylece $\mathcal{G}$ nin bir Sylow p -altgrubu S_q yu merkezler. Şimdi P , G nin Sylow p -altgrubu olsun. $G = AB = \mathcal{G}M = \mathcal{G}(A_0 \times B)$ olduğundan $P_1 = \mathcal{G} \cap P$ ve $P_2 = M \cap P$ ise $P = P_1 P_2$ dir. $M \trianglelefteq G$ ve $P_2 \trianglelefteq M$ nin karakteristik altgrubu olduğundan $P_2 \trianglelefteq G$ dir. Yukarıda görüldüğü gibi P_1 , B nin p' -kısımını merkezler. Ayrıca $p \mid |A_0|$ ve A_0 nilpotent olduğundan P_1 , A_0 merkezler. O zaman P , M tarafından normallenir. Ayrıca $\mathcal{G}$ tarafından normallenir. Bundan dolayı $P = P_1 P_2 \trianglelefteq G$ dir. Şimdi $\langle \sigma, P \rangle$ bir p -grubu olduğundan $\sigma \in P$ olmalıdır. $M \langle \sigma \rangle \trianglelefteq G$ olduğundan

$$P \cap M \langle \sigma \rangle = \langle \sigma \rangle (P \cap M) = \langle \sigma \rangle P_2 \trianglelefteq G$$

dir. $P_0 = \langle \sigma, U_1(P_2) \rangle$ ise P_0 abeliyandır. Çünkü $P_2 = \langle y \rangle$ ise (3), 5.4.2. (ii) den dolayı y^p yi merkezler. Böylece P_0 abeliyandır. Ayrıca $P_0 \trianglelefteq G$ dir. Gerçekten

$$P_0 \trianglelefteq P_2 \langle \sigma \rangle = \langle y \rangle \langle \sigma \rangle$$

dir. Eğer $y^\sigma = y$ ise durum aşıkardır. Öyleyse σ , $P_2 = \langle y \rangle$ üzerinde mertebesi p olan otomorfizma olsun. O zaman (3). Teorem 5.4.2 (ii) den dolayı $y^\sigma = y^{1+p^{n-1}}$ dir. Buradan $o(y) = p^n$ dir. $[\sigma, y] = y^{p^{n-1}} \in \langle y^p \rangle$ dir. Bundan dolayı $\langle y^p \rangle \langle \sigma \rangle \trianglelefteq \langle y \rangle \langle \sigma \rangle$ dir. Böylece $P_0 \trianglelefteq G$ dir. G nin her normal abeliyan altgrubu devirli olduğundan P_0 devirlidir. O zaman $\sigma \in U_1(P_2)$ olmalıdır. Fakat $\sigma \in \mathcal{G}$ ve $\mathcal{G} \cap M = 1$ olduğundan bu bir çelişkidir. Dolayısıyla $e = 1$ dir.

Şimdi çeşitli halleri ayrı ayrı gözönüne alacağız.
 $[\phi(b):\mathcal{G}] \leq 2$ olduğundan $\phi(c) = 1, 2$ dir. Bundan dolayı
 $c = 1, 2, 3, 4, 6$ olabilir.

(A) $|B| = 2^t$; $t > 2$, bu hal olamaz.

Kabul edelim ki $|B| = 2^t$ olsun. Burada $|\text{Aut}(\bar{B}):\mathcal{G}| = 2$ olduğundan $\phi(c) = 1$ dir. Böylece $c = 1$ veya $c = 2$ dir. Fakat $(|\bar{C}|, |\bar{B}|) = 1$ olduğundan $c = 1$ ve $\bar{c} = 1$ dir. Ayrıca $\phi(b) = 2^{t-1}$ ve $|\text{Aut}(\bar{B}):\mathcal{G}| = 2$ olduğundan $|\mathcal{G}| = 2^{t-2}$ dir.

$\mathcal{G}$ nin bir üretici σ olsun. $(|A_0|, |B|) = 1$ olduğundan σ, A_0 1 merkezler. Çünkü $\sigma \in \mathcal{G}$ ve $|\mathcal{G}| = 2^{t-2}$ olduğundan $o(\sigma) = 2^{t-2}$ şeklinde yazılabilir. Ayrıca $A = \mathcal{G}A_0$ ve $(|B|, |A_0|) = 1$ olduğundan $2 \nmid |B|$ fakat $2 \nmid |A_0|$ dir. Ayrıca A nilpotent olduğundan $A = A_2 \times Q_2'(A)$ dir. Aşıkarak olarak $\sigma, Q_2'(A)$ yı merkezler. Fakat $2 \nmid |A_0|$ olduğundan $A_0 \leq Q_2'(A)$ dir. Bundan dolayı σ, A_0 1 merkezler. O zaman $G = \mathcal{G}(B \times A_0) = \langle \sigma, B \rangle \times A_0$ dir. Şimdi $\langle \sigma, B \rangle$ nin bir Sylow 2-altgrubu ve $G = \langle \sigma, B \rangle \times A_0$ olduğundan $\langle \sigma, B \rangle$ nin her normal altgrubu G de normaldir. Böylece Hipotez 3.1 den dolayı $\langle \sigma, B \rangle$ nin her normal ameliyan altgrubu devirlidir. O zaman (3), 5.4.10 ve 5.4.2, (ii) den dolayı bu altgrup yarıdihedraldir. Buradan $o(\sigma) = 2$ olduğundan $2 = |\mathcal{G}| = 2^{t-2}$ ve $t = 3$ bulunur. Böylece $|B| = 2^t = 2^3 = 8$ dir. Burada $\bar{k}^x = \text{GF}(r^{2n})$, σ, A_0 merkezlediğinden $A_0 \leq \text{GF}(r^n)$ ve $\text{GF}(r^n)^x B = \bar{k}^x$ dir.

$$|\bar{k}^x| = (r^{2n}-1) = (r^n-1)(r^n+1) = \frac{(r^n-1)8}{|\text{GF}(r^n)^x \cap B|}$$

olduğundan $r^n + 1 = \frac{8}{|GF(r^n)^x \cap B|}$ dir. Fakat

$|GF(r^n)^x \cap B| \geq 2$ olduğundan $(r^n + 1) | 4$ dir. Bundan dolayı $n = 1$, $r = 3$ dür. Ayrıca $A_0 \leq GF(g)$, $|A_0| \leq 3 - 1 = 2$ ve A_0 ın mertebesi tek olduğundan $|A_0| = 1$ dir.

Şimdi $\mathcal{G} = \langle \sigma \rangle$ ın sabit cismi $GF(3)$ olduğundan $GF(9) \setminus GF(3)$ kümesinin hiçbir elemanı σ tarafından sabit bırakılmaz. Bundan dolayı $\mathcal{G} = \langle \sigma \rangle$ ın $GF(9)$ modülü içinde $(9-3)/2 = 3$ tane regüler yörüngesi vardır. Bu bir ilişkidir. Bundan dolayı $|B| = 2^t$ olamaz.

(B) $|B| = 2p^e$ olsun (vi) den dolayı $e = 1$ dir.

(v) den dolayı $[Aut(\bar{B}) : \mathcal{G}] = 2$ ve $p \equiv -1 \pmod{4}$ tür. Burada $\phi(c) = 1$ olduğundan $c = 1, 2$ olmalı, ayrıca $(c, b) = 1$ olduğundan $c = 2$ olamaz. Bundan dolayı $c = 1$ dir. Böylece $|\bar{C}| = 1$ dir. Fakat $\bar{k}^x/A_0 = \bar{C} \times \bar{B}$ olduğundan $\bar{k}^x = A_0 B$ dir. Bundan dolayı $[\bar{k}^x : BA_0] = 1$ dir. Ayrıca $|\mathcal{G}| = \frac{1}{2}(p-1)$ ve $p \equiv -1 \pmod{4}$ olduğundan $4 | (p-1)$ dir. Böylece (b) sağlanır.

(C) $|B| = p^e q^f$ olsun. (vi) den dolayı $e = f = 1$ dir. Bundan dolayı $Aut(\bar{B}) = (p-1)(q-1)$ dir. $\mathcal{G}$ devirli olduğundan $(p-1, q-1) = 2$ olmalıdır. O zaman $4 \nmid p-1$ veya $4 \nmid q-1$ dir. Eğer $4 \nmid q-1$ ise $(p-1, (q-1)/2) = 1$ olduğundan mertebesi $(p-1)\frac{q-1}{2}$ olan devirli bir altgrup vardır. Böylece $|\mathcal{G}| = \frac{(p-1)(q-1)}{2}$ dir. Diğer halde de aynı sonuç elde edilir. Bundan başka $\phi(c) = 1$ olduğundan $c = 1$ dir. Dolayısıyla (a) sağlanır.

(D) $|B| = p^e$ olsun. (vi) den dolayı $e = 1$ ve $|B| = p$ dir. Bu durumda $[\bar{k}^x : BA_0] = c = 1, 2, 3, 4, 6$ olabilir. Aynı

zamanda $|\mathcal{C}| = \frac{p-1}{\delta}$, $\delta = 1, 2$ dir. Eğer $\delta = 2$ ise $|\text{Aut}(B) : \mathcal{C}| = 2$ dir. Bundan dolayı $\phi(c) = 1$ olduğundan $c = 1, 2$ dir. Eğer $3 \nmid c$ olduğu gösterilirse (c) ispatlanmış olur.

Kabul edelim ki $3 \nmid |C|$ olsun. C nin üretici σ olsun. $\bar{C}$ nin Sylow 3-altgrubu $\bar{D}$ olsun. O zaman $|\bar{D}| = 3$ tür. $3 \nmid |\bar{B}|$ olduğundan $3 \nmid |A_0|$ dir. σ otomorfizması $\bar{D}$ üzerine etki ettiğinde ya aşikâr veya mertebesi 2 dir. Fakat $3 \nmid |A_0|$ ve $A = \mathcal{C}A_0$ nilpotent olduğundan 2 olması mümkün değildir. Böylece σ , D üzerinde aşikâr etki eder. Esasen $|\bar{C}| = 3, 6$ olduğundan $\bar{C} = \bar{D}$ veya $\bar{C}$ nin mertebesi 2 olan bir altgrubu $\bar{Y}$ olmak üzere $\bar{C} = \bar{D} \times \bar{Y}$ dir. Fakat σ , $\bar{Y}$ yi merkezler. Bundan dolayı σ , $\bar{C}$ yi merkezler. Böylece $\bar{C}$ nin $\bar{k}^x$ içindeki ters görüntüsü C ise $[\sigma, C] \leq A_0$ olduğundan, her $s \in \mathcal{C}$ için $C \leq J_s$ dir. Fakat σ , $\bar{k}^x/A_0 = \bar{C} \times \bar{B}$ nin üreticileri üzerinde regülerdir. $\bar{B} \cong B$ olduğundan σ , B nin üreticileri üzerinde de regülerdir. Böyle bir üretic wA_0 olsun. O zaman her $s \in \mathcal{C}$ için $w \notin J_s$ dir.

Şimdi $\mu, \nu \in \bar{D} = D/A_0$ in farklı iki kosetinin temsilcisi olsun. O zaman μwA_0 , νwA_0 ve wA_0 in hiçbirisi J_s/A_0 içinde değildir. Şöyleki Hipotez 3.11 sağlandığından ve wA_0 bir üretic olduğundan $\sigma(w)w^{-1} \notin A_0$ dir. Mümkünse $\sigma(\mu w)(\mu w)^{-1} = a \in A_0$ olsun. O zaman $\sigma(\mu)\mu^{-1}\sigma(w)w^{-1} = a$ dir. σ , $\bar{D}$ aşikâr olduğundan $\sigma(\mu)\mu^{-1} \in A_0$ dir. O zaman $\sigma(w)w^{-1} \in A_0$ dir. Bu bir çelişkidir. Benzer şekilde $\sigma(\nu w)(\nu w)^{-1} \notin A_0$ dir. Fakat o zaman μwA_0 , νwA_0 ve wA_0 , $\mathcal{C}$ nin $\bar{k}^x/A_0$ üzerindeki üç farklı regüler yörüngesini üretir. Bu bir çelişkidir. Böylece (c) ispatlanmıştır.

Artık B nin yapısı oldukça açıktır. Amacımız $|\mathcal{G}|$ sayısını daha yakın olarak belirlemektir. Bütün muhakeme biçimleri, esas olarak aynıdır. Kabul edelim ki H/K , $\mathcal{G}$ nin mertebesi s asal sayısı olan bir kesmi olsun. $|H| = x$ olsun. x , r nin bir kuvvetidir. $[K^x : H^x] = (x^s - 1)/(x - 1)$ dir. Bu indeksi ikinci bir yolla hesaplayıp sonuçları karşılaştıracacağız. Muhakemelerin esası budur.

3.15. LEMMA : Kabul edelim ki Hipotez 3.11 sağlansın ve A , $\bar{k}^+$ üzerinde en çok iki regüler yörüngeye sahip olsun. s asal olmak üzere, σ mertebesi s^t olan $\mathcal{G}$ nin bir elemanı ve σ nin sabit cismi F olsun. O zaman

- (a) s tek ise $t < 2$ dir.
- (b) $s = 2$ ise $t < 3$ dür.
- (c) $s = 2$ ve $t = 2$ ise o zaman $4 \mid |F^x|$ veya $|B| = pq$ ve σ, B üzerinde sabit noktasıdır.

İSPAT : Teoremin ispatı için aşağıdaki adımları izleyeceğiz.

(i) σ , B üzerinde sabit noktasız, $s = 2$ ve $|B| = pq$ halleri dışında bir $e \geq 1$ tamsayısı ve bir asal tek sayı $p \mid |B|$ için $[\bar{k}^x : F^x]$ indeksi $s^e p$ yi böler.

$|A_0|$ sayısını bölen asal sayıların kümesi π olsun. O zaman B , $\bar{k}^x$ nin bir Hall π' -alt grubudur. $A = \mathcal{G}A_0$ nilpotent ve $\bar{k}^x/B$ devirli bir π -grubu olduğundan $\mathcal{G}\bar{k}^x/B$ nilpotenttir. Çünkü her $q \in \pi$ için $\mathcal{G}\bar{k}^x/B$ grubunun mertebesi q olan alt grubu A_0 içinde olduğundan $\mathcal{G}$ nin q' -alt grubu tarafından merkezlenir. Böylece (3), 5.2.4 den dolayı σ her $q \in \pi$ ve $q \neq s$ için $\bar{k}^x$ nin Sylow q -alt grubunu mer-

kezler. Bundan dolayı $\bar{k}^x/F^x_B$ bir s-grubudur. Böylece bir $e \geq 1$ tamsayısı için $|\bar{k}^x/F^x_B| = s^e$ dir. Şimdi

$$[\bar{k}^x:F^x] = [\bar{k}^x:F^x_B][F^x_B:F^x] = s^e[F^x_B:F^x]$$

olduğundan $[\bar{k}^x : F^x]$ inteksi $s^e |B|$ sayısını böler.

Şimdi Lemma 3.14 ün hallerini inceleyelim. Öncelikle (c) halinde $|B| = p$ bir asal tek sayı olduğundan iddia gerçekleşir.

(b) halinde ise p asal tek sayı olmak üzere $|B| = p$ dir. Bu durumda $-1 \in \bar{k}^x$ ve $\bar{k}^x$ nin tek invazyonu olduğundan $-1 \in B \cap F^x$ dir. Böylece $2 \mid |B \cap F^x|$ dir. Fakat $[F^x_B:F^x] = |F^x_B/F^x| = |B/B \cap F^x|$ olduğundan $[\bar{k}^x:F^x]$ indeksi $s^e p$ sayısını böler.

Son olarak (a) sağlansın. O zaman $|B| = pq$; p ve q asal tek sayılar ve $(p-1, q-1) = 2$ ve $|G| = (p-1)(q-1)/2$ dir. Eğer s asal tek sayı ise $s^e \mid p-1$ olduğunu kabul edebiliriz. Bu durumda $s \nmid (q-1)$ olduğundan σ , Sylow q-alt grubunu merkezler. Böylece $[\bar{k}^x:F^x]$ indeksi $s^e \frac{|B|}{q} = s^e p$ sayısını böler.

Şimdi $s = 2$ olsun. Eğer σ , B üzerinde sabit noktasız değilse, o zaman mertebesi p veya q olan alt grubunu merkezler. O zaman (3), 5.2.4 den dolayı σ , B nin Sylow p-alt grubunu veya Sylow q-alt grubunu merkezler. Kabul edelim ki σ , Sylow q-alt grubunu merkezlesin. O zaman yukarıda görüldüğü $[\bar{k}^x : F^x]$ indeksi $s^e p$ sayısını böler.

(ii) Eğer $s = 2$ σ , B üzerinde sabit noktasız ve $|B| = pq$ ise $[\bar{k}^x : F^x]$ indeksi $2^e pq$ sayısını böler ve $[\bar{k}^x : F^x_1]$ indeksi $2^e p$ sayısını böler. Burada F_1 σ^2 nin

sabit cismidir ve $t > 1$ dir. (i) nin ispatında olduğu gibi $[\bar{k}^x : F^x]$ indeksi $s^e | B|$ yi böler. Burada $s = 2$ ve $|B| = p q$ olduğundan bu indeks $2^e p q$ sayısını böler. Şimdi B nin Sylow p -altgrubu S_p ve Sylow q -altgrubu S_q ise

$$\text{Aut}(B) \cong \text{Aut}(S_p) \times \text{Aut}(S_q)$$

dur ve $|\text{Aut}(S_p)| = p - 1$ $|\text{Aut}(S_q)| = q - 1$ dir. $\text{Aut}(S_p)$ ve $\text{Aut}(S_q)$ nun Sylow 2-altgruplarının birer üretici τ γ ise (τ, γ) elemanı $\text{Aut}(B)$ nin Sylow 2-altgrubunu üretir. Fakat Lemma 3.14 (a) dan dolayı $(p-1, q-1) = 2$ olduğundan ya $o(\tau) = 2$ veya $o(\gamma) = 2$ dir. $o(\gamma) = 2$ olduğunu kabul edebiliriz. Şimdi σ , (τ, γ) nin bir kuvveti olduğundan σ^2 , $(\tau, \gamma)^2 = (\tau^2, 1)$ in bir kuvveti olmalıdır. Fakat $(\tau^2, 1)$, S_q yu merkezlediğinden σ^2 de B_q yi merkezler. Buradan $B_q \leq F_1$ dir. Aynı zamanda $[\bar{k}^x : F_1^x] | 2^e p q$ ve $B_q \leq F_1$ olduğundan $[\bar{k}^x : F_1^x] | 2^e p$ dir. Böylece (ii) gösterilmiş olur.

Şimdi her $i \geq 0$ için $\sigma^{s^i} = \sigma_i$ ve σ_i $\bar{k}^x$ içindeki sabit cismi, F_i olsun. O zaman $F_0 = F$ dir. Bu durumda (i) ve (ii) den görüldüğü gibi $p || B|$ asal tek sayısı için S_p Sylow p -altgrubu her $0 \leq i < t$ için σ_i tarafından sabit noktası bırakılır. Bundan dolayı $p || [\bar{k}^x : F^x]$ dir.

(iii) Her $0 \leq i \leq t-1$ için

$$[F_{i+1}^x : F_i^x] = \frac{[k^x : F_i^x]}{[\bar{k}^x : F_{i+1}^x]}$$

olduğu açıktır. (i) halinde sağ taraf s^e yi böldüğünden sol taraf s nin bir kuvvetidir.

(iv) (ii) halinde ise yukarıdaki eşitlikte $i \geq 1$ için sağ taraf 2^e yi böldüğünden sol taraf 2 nin bir kuvvetidir.

Şimdi x, r nin bir kuvveti olmak üzere $\frac{x^s-1}{x-1} = s^e$ olsun. O zaman Lemma 2.1 den dolayı $s = 2, 2 \parallel (x-1)$ ve $x+1 = 2^e$ dir. Aynı zamanda $x = r^n$ olduğundan $r^n+1 = 2^e$ ve bu eşitliğin sağlanması için de $n = 1$ olmalıdır. Buradan $r+1 = 2^e$ ve $r > 2$ olduğundan $r \equiv -1 \pmod{4}$ olmalıdır.

Şimdi habul edelim ki s tek olsun. Eğer $t \geq 2$ ise o zaman $0 \leq i < t-1$ için (iii) den dolayı $[F_{i+1}^x : F_i^x] = s^e$ yazılabilir. $|F_i| = x = r^n$ olsun. Ayrıca $[F_{i+1} : F_i] = s$ olduğundan $|F_{i+1}| = x^s$ dir. Buradan

$$\frac{|F_{i+1}^x|}{|F_i^x|} = \frac{x^s - 1}{x-1} = s^e$$

bulunur. Fakat bu durumda yukarıda gösterildiği gibi $s = 2$ olmalıdır. Bu bir çelişkidir. Bundan dolayı s tek ise $t < 2$ dir.

Şimdi ise $s = 2$ olsun. Eğer $t \geq 3$ ise o zaman (iv) den dolayı $[F_2 : F_1]$, 2 nin bir kuvveti olduğundan $x+1 = r^n+1 = 2^e$ yazılabilir. Yukarıda görüldüğü gibi bunun için $n = 1$ ve $r \equiv -1 \pmod{4}$ tür. Fakat şimdi $|F_1| = x = r$ olur. Bu imkânsızdır, çünkü; $F_1 > F_0$ ve $|F_0| \geq r$ dir. Bundan dolayı $t \leq 2$ olmalıdır. Kabul edelim ki $t = 2$ olsun ve $|B| \neq pq$ olmasın. O zaman Lemma 3.14 den dolayı $|B| = p$ ve her $0 \leq i < t$ için σ_i , B üzerinde sabit noktasızdır. Yani $p \nmid [\bar{k}^x : F_i]$ dir. Bundan dolayı $[F_1 : F_0]$ indeksi 2 nin bir kuvvetidir. O zaman

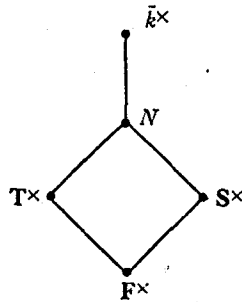
yukarıda olduğu gibi $|F_0| = r$ ve $2 \parallel (r-1)$ dir. $|F_0^X| = r-1$ olduğundan $4 \nmid |F_0^X|$ dir.

Yukardaki Lemma $|\mathcal{G}|$ sayısının asal bölenlerinin üstlerini sınırlamaktır. Şimdi de $|\mathcal{G}|$ sayısının asal bölenlerinin sayısını sınırlayacağız. Bunun ispatı önceki ispata benzerdir.

3.16. LEMMA : Kabul edelimki Hipotez 3.11 sağlansın ve en çok iki regüler yörüngeye sahip olsun. $p \mid |B|$ bir asal tek sayı ve B , B nin bir S_p -altgrubu olsun. $\mathcal{G}$ nin B ye kısıtlanmasıyla elde edilen otomorfizma grubu $\mathcal{G}^*$ olsun. O zaman $|\mathcal{G}^*|$ sayısı bir asal kuvvettir.

İSPAT : Kabul edelim ki s ve $t, |\mathcal{G}^*|$ sayısının iki asal böleni ve $t > s$ olsun. O zaman t tek sayıdır. $\tau \in C$ ve $o(\tau) = t^e > 1$ olsun. O zaman Lemma 3.15 (a) dan dolayı $o(\tau) = t$ dir. Aynı zamanda $t \mid |\mathcal{G}^*|$ olduğundan τ, B üzerinde mertebesi t olan bir otomorfizma tanımlar. Bunu tekrar τ ile gösterelim. Bundan başka $\mathcal{G}$ nin mertebesi s^e olan öyle bir elemanı vardır ki bu eleman B üzerinde mertebesi s olan bir otomorfizma tanımlar. Bu otomorfizmayı σ ile gösterelim.

σ nin sabit cismi S ve τ nin sabit cismi T olsun. O zaman $F = S \cap T, \sigma\tau$ nun sabit cismidir. $N = S^X T^X$ olsun. Böylece aşağıdaki kafes diyağramı elde edilir.



Şimdi $t \neq 2$ olduğundan Lemma 3.15 in ispatının (i) kısmından dolayı $[\bar{k}^x : T^x] | t^f_p$ ve aynı ispatın (i) ve (ii) kısmından $[\bar{k}^x : S^x] | s^g_{pq}$ veya $[\bar{k}^x : S^x] | s^g_p$ dir. B_0 $\bar{k}^x$ nın bir Sylow p -altgrubu olduğundan $|B_0| = p$ dir. Aynı zamanda σ ve τ, B nın aşikar olmayan otomorfizması olduğundan

$$B_0 \cap T^x = B_0 \cap S^x = \langle 1 \rangle$$

dir. Bundan dolayı $p \nmid N$ dir ve böylece $p | [\bar{k}^x : N]$ dir. Buradan $[N : T^x] = [S^x : F^x] = t^h$ elde edilir. Gerçekten $[k : T] | t^t_p$ ve $p | [\bar{k}^x : N]$ olduğundan $[N : T^x] = t^h$ olacak şekilde bir h vardır. Ayrıca

$$[S^x : F^x] = \frac{|S^x|}{|F^x|} = \frac{|S^x|}{|T^x \cap S^x|} = \frac{|S^x T^x|}{|T^x|} = \frac{|N|}{|T^x|} = t^h$$

dir. $|F| = x$ olsun, x, r nin bir kuvvetidir. O zaman

$$[S^x : F^x] = \frac{x^t - 1}{x - 1} = t^h$$

dir. Fakat t tek olduğundan Lemma 2.1 den dolayı $\frac{x^t - 1}{x - 1} = t^h$ denkleminin çözümü yoktur. Bu bir çelişkidir. Yani; $|G^*|$ sayısı bir asal sayının kuvvetidir.

Artık Lemma 3.14, Lemma 3.15 ve Lemma 3.16 yı uygulayarak bazı değerler elde edebiliriz.

3.17. LEMMA : Kabul edelim ki Hipotez 3.11 sağlansın ve A nın $\bar{k}^x$ üzerindeki etkisinin en çok iki regüler yörüngesi olsun. O zaman s bir asal tek sayı olmak üzere $|B|$ için aşağıdaki olasılıklar elde edilir.

	$ B $	$(p-1)$	$(q-1)/2$	$ G $
(1)	3,6	2	-	2
(2)	5,10	4	-	2,4
(3)	$2s+1, 4s+2$	$2s$	-	s
(4)	$3(2s+1)$	2	0	$2s$
(5)	$5(2s+1)$	4	s	$4s$
(6)	3.5	4	1	4

İSPAT : Lemma 3.16 dan B nin yapısı bilinmektedir.
Buna göre $|B| = p, 2p, pq$ olabilir.

(A) $|B| = p, 2p$ olsun.

$\mathcal{G}$ grubu B üzerinde sadık olduğundan B nin S_p -altgrubu üzerinde de sadıktır. Böylece Lemma 3.16 dan dolayı $|\mathcal{G}|$ bir asal sayının kuvvetidir. O zaman Lemma 3.15 den dolayı ya $|\mathcal{G}| = 2^t$, $t < 3$ veya s bir tek asal sayı olmak üzere $|\mathcal{G}| = s$ dir. Lemma 3.14 den dolayı $(p-1) = |\mathcal{G}|$ veya $(p-1) = 2|\mathcal{G}|$ dir.

Kabul edelim ki $|\mathcal{G}| = 2^t \leq 4$ olsun. O zaman $2|\mathcal{G}| = p-1$ olduğundan $(p-1) = 2 \cdot 2^t \leq 8$ dir. Buradan $p = 3$ veya $p = 5$ sonucu çıkar. $p = 3$ ise $|\mathcal{G}| = 2$ dir. Eğer $p = 5$ ise $|\mathcal{G}| = 2, 4$ tür. Böylece (1) ve (2) halleri gösterilmiş olur.

Şimdi de $|\mathcal{G}| = s$ olsun. O zaman $p-1 = s$ veya $p-1 = 2s$ dir. Buradan $p = s + 1$ veya $p = 2s + 1$ elde edilir. Böylece (3) gösterilmiş olur.

(B) $|B| = pq$ olsun. Bu durumda Lemma 3.14 (b) den dolayı $|C| = (p-1)(q-1)/2$ ve $(p-1, p-1) = 2$ dir. Şimdi q yu öyle seçebilirizki $2 \parallel (q-1)$ dir.

B nin Sylow p-altgrubu üzerine, $\mathcal{G}$ nin kısıtlanması $\mathcal{G}^*$ ve Sylow q-altgrubu üzerine kısıtlanması $\mathcal{G}^{**}$ olsun. Lemma 3.16 dan dolayı $\mathcal{G}^*$ ve $\mathcal{G}^{**}$ nin mertebeleri birer asal sayının kuvvetidir. Bu mertebelerden biri çifttir. p ve q öyle seçilebilir ki $\mathcal{G}^*$ nin mertebesi çifttir. Buradan $p-1 = 2^t$ elde edilir. O zaman Lemma 3.15 den dolayı $t < 3$ ve $s = 1$ veya bir asal tek sayı olmak üze-

re $(q-1)/2 = s$ bulunur. Böylece $q = 2s + 1$ elde edilir. Eğer $t = 1$ ise $p = 2$, $q = 2s + 1$ ve $|G| = 2s$ dir. Böylece (4) şartı elde edilir.

Eğer $t = 2$ ve tekrar s , asal tek sayı ise $p = 5$ ve $q = 2s + 1$ dir. Ayrıca $|G| = 4s$ dir. Bu ise (5) şartını sağlar.

$s = 1$ ise $|G| = 4s = 4$, $q = 2s + 1 = 3$ ve $p = 5$ elde edilir. Buda son olarak (6) yı sağlar. Böylece ispat tamamdır.

3.18. LEMMA : Lemma 3.17 de $|B| \neq pq$ dur.

İSPAT : Lemma 3.17 de $|B| = pq$ iken (4), (5) ve (6) hallerini elde etmiştir. Önce (4) ve (5) hallerine bakalım.

G içinde σ nun mertebesi s ve τ nun mertebesi 2 olsun. σ nun sabit cismi S ve τ nun sabit cismi T olsun. $F = S \cap T$ olsun. O zaman $F, \sigma\tau$ nun sabit cismidir. Şimdi Lemma 3.18 de ki şekile bakalım. $|F| = x$, r nin bir kuvvetidir. Şimdi $[S:F] = o(\tau) = 2$ ve $[\bar{k}:S] = o(\sigma) = s$ olduğundan

$$[\bar{k}^x:S^x] = \frac{x^{2s}-1}{x^2-1} = s^e_p$$

dir. Benzer şekilde

$$[\bar{k}^x:T^x] = \frac{x^{2s}-1}{x^s-1} = 2^f_q$$

elde edilir. Bu iki indeks aralarında asal olduğundan $[\bar{k}^x:N][N:S^x]$ ile $[\bar{k}^x:N][N:T^x]$ aralarında asaldır. Bundan dolayı $[\bar{k}^x:N] = 1$ ve $N = S^x T^x = \bar{k}^x$ elde edilir. Böylece

$$\frac{(x^{2s}-1)}{(x^2-1)} = [N:S^X] = [T^X:F^X] = \frac{(x-1)}{(x-1)} \text{ dir. Fakat}$$

$$\frac{x^{2s}-1}{x^2-1} > \frac{x^s-1}{x-1}$$

olduğundan bu bir çelişkidir.

Son olarak (6) yı gözönüne alalım. Burada birkaç çeşit yol var. Biz aşağıdakini seçeceğiz. $\sigma \in \mathcal{G}$, $\mathcal{G}$ yi üretsin $o(\sigma) = 4$ tür. σ nın sabit cismi S ve σ^2 nin sabit cismi F olsun. İki olasılık vardır. Birincisi σ , B nin bir S_q -altgrubunu sabit bırakabilir. Bu durumda $p \nmid [k:F^X]$ dir. Bundan dolayı $[F^X:S^X]$, 2 nin bir kuvvetidir. Burada $p = 5$ ve $q = 3$ tür.

Diğer halde ise σ B nin S_q -altgrubu üzerinde sabit noktasız olur. Fakat $q = 3$ olduğundan σ S_q üzerinde mertebesi 2 olan otomorfizma etkisi yapar. Bu durumda $S_q < F$ dir. Bu halde şu sonuç elde edilir.

$$(i) [k^X:F^X] = 2^e p = 2^e 5 \text{ ve } [F^X:S^X] = 2^f q = 2^f . 3$$

$|S| = x$, r nin bir kuvveti olsun. O zaman

$$(ii) [k^X:F^X] = \frac{x^4-1}{x^2-1} = x^2 + 1 = 2^e . 5$$

ve

$$F^X:S^X = \frac{x^2-1}{x-1} = x + 1 = 2^f . 3$$

elde edilir.

$f = 1$ olsun. O zaman $x + 1 = 2.3$ den $x = 5$ elde edilir. Fakat $x^2 + 1 = 2^e . 5$ olduğundan $26 = 2^e . 5$ elde edilirki bu bir çelişkidir. Dolayısıyla $f = 1$ olamaz.

Şimdi ise $f > 1$ olsun. O zaman $4 \mid (x + 1)$ olduğundan $4 \nmid x^2 + 1$ dir. Buradan $e = 1$ ve $x^2 + 1 = 10$ olduğun-

dan $x = 3$ elde edilir. Fakat $x + 1 = 3 + 1 = 4 = 2^f$. 3 olduğundan bu bir çelişkidir. Bundan dolayı f birden büyük olamaz.

$f = 0$ olsun. O zaman $e = 0$ ve $x = 2$ dir.

(iii) Böylece $x = 2$ ve $q = 3$ tür.

Şimdi $A_0 = A \cap \bar{k}^x = A \cap B = \langle 1 \rangle$ olduğundan $A = \mathcal{G}A_0 = \mathcal{G}$ dir. Böylece $|A| = |\mathcal{G}| = o(\sigma) = 4$ tür. Şimdi $\phi(15) = 8$ olduğundan $\mathcal{G}$ nin $\bar{k}^x$ üzerinde $\frac{\phi(B)}{|\mathcal{G}|} = \frac{8}{4} = 2$ regüler yörüngesi vardır.

Fakat $\bar{k}^x = S_3 \times S_5$ olduğundan S_5 in bir üretici üzerinde σ , bir regüler yörünge tanımladığından, $\mathcal{G}$ nin $\bar{k}^+$ üzerinde tam olarak 3 regüler yörüngesi vardır. Bu bir çelişkidir.

3.19. LEMMA : Hipotez 3.11 sağlansın ve A nın $\bar{k}^x$ üzerinde en çok iki regüler yörüngesi bulunsun. O zaman aşağıdakilerden biri sağlanır.

$ \mathcal{G} $	$ \hat{k} $	$ B $	
4	3	5	
3	4	7	
3	2	7	
2	$2^a \cdot 5 - 1$	5	$a \geq 1$
2	$2^a \cdot 5 - 1$	3	$a \geq 1$
2	4	5	
2	2	3	

İSPAT : Önce $x > 1$ ve $y > 2$ den herbiri birer asal sayının kuvveti olsun. Lemma 2.2 den dolayı aşağıdaki özel hallerin dışında daima

$$(x^y - 1)/(x - 1) > 2y^2 + y \quad \text{dir.}$$

x	y
2	3,4,5
3	3
4	3

Ayrıca $x = 2$ ve $y = 3$ hali dışında Lemma 2.3 den dolayı $x^y - 1/x - 1 > 2y + 1$ dir.

Şimdi Lemma 3.18 den dolayı $|B| \neq pq$ olduğu için Lemma 3.12 nin yalnızca (1), (2) ve (3) hallerini incelemek yeter.

$|G| = s$ bir asal tek sayı $|\hat{k}| = x$, r nin bir kuvveti ve $\sigma \in G$ nin mertebesi s olsun. O zaman $\hat{k}$, σ nin sabit cismidir. Bundan dolayı $[\bar{k}^x : \hat{k}^x] = s^e_p$ dir. Böylece $(x^s - 1)/(x - 1) = s^e_p = s^e(2s + 1)$ dir. $s \nmid (x - 1)$ olduğu zaman $e = 0$ dir. Gerçekten $x^s - 1/(x - 1) = s^e_p$ olduğundan $s^e \mid \frac{x^s - x}{x - 1} = 1$ dir. $\frac{x^s - x}{x - 1}$ bir tamsayı olduğundan eğer $s \mid \frac{x^s - x}{x - 1}$ ise $s \mid 1$ dir. Bu bir çelişkidir. O halde $s \nmid \frac{x^s - 1}{x - 1}$ olsun. Fakat o zaman Fermat Teoreminden $s \mid x^s - x$ olduğundan ve de $s \nmid \frac{x^s - x}{x - 1}$ olduğundan $s \mid x - 1$ dir. Bu tekrar bir çelişkidir. Bundan dolayı $e = 0$ olmak zorundadır. O zaman

$$\frac{x^s - 1}{x - 1} = 2s + 1$$

dir.

Eğer $s \mid (x - 1)$ ise Lemma 2.1 den dolayı $e = 1$ olduğunu kabul edebiliriz. Dolayısıyla

$$\frac{x^s - 1}{x - 1} = s(2s + 1) = 2s + s$$

dir. Böylece yukarıdaki tablodan $y = s$ için tek çözüm $x = 4$ ve $y = 3$ olduğu görülür. Buradan $|\hat{k}| = 4$, $|G| = s = 3$ ve $|B| = p = 2.s + 1 = 2.3 + 1 = 7$ veya

$|B| = 4.s + 2 = 4.3 + 2 = 14$ elde edilir. Fakat $|\bar{k}^x| = 4^3 - 1 = 63$ sayısı 14 sayısı tarafından bölünmediğinden $|B| = 14$ olamaz, o halde $|B| = 7$ olmalıdır. Böylece (2) şartı elde edilir.

Şimdi de $e = 0$ ise $\frac{x^s - 1}{x - 1} = p = (2s + 1)$ olmalıdır. Yukarıda $y = s$ için tek çözüm $x = 2$, $y = 3$ olduğu görülür. O zaman $|\hat{k}| = 2$, $|G| = s = 3$ ve $|\bar{k}^x| = 2^3 - 1 = 7$ ve $|B|$, $|\bar{k}^x|$ yi böldüğünden $|B| = 7$ bulunur. Böylece (3) şartı elde edilir.

Şimdi $|G| = 4$ olsun $\sigma \in G$ ve $o(\sigma) = 4$ olsun. σ^2 nin sabit cismi F ve $|\hat{k}| = x$ olsun. O zaman

$$[\bar{k}^x : F^x] = \frac{x^4 - 1}{x^2 - 1}$$

dir. Aynı zamanda Lemma 3.17 satır (2) den dolayı $|B| = 5, 10$ olduğundan Lemma 3.15 in ispatından dolayı $[\bar{k}^x : F^x] = 2^e . 5$ dir. Böylece $(x^4 - 1)/(x^2 - 1) = 2^e . 5$ elde edilir. Buradan $x^2 + 1 = 2^e . 5$ bulunur. Kolayca görüleceği üzere $4 | x^2 + 1$ dir. Buradan $e = 0, 1$ olmalıdır.

Eğer $e = 0$ ise o zaman $x^2 + 1 = 5$ dir. Buradan $x = 2$ elde edilir. O zaman $|\hat{k}| = 2$, $|F| = 4$ ve $|\bar{k}^x| = 2^4 - 1 = 15$ olduğundan $|B| = 5$ bulunur. Fakat $|F^x| = 4 - 1$ olduğundan F^x nin mertebesi 3 olan bir y elemanını içerir. Bu eleman σ tarafından sabit bırakılmaz. Fakat $\langle y, \sigma \rangle$ nilpotent olmadığından $y \notin A_0$ dir. Böylece $3 \nmid |B|$ ve $3 \nmid |A_0|$ dir. Bu bir çelişkidir. Bundan dolayı $e = 1$ olmalıdır. O zaman $x^2 + 1 = 2 . 5 = 10$ dir. Buradan $x = 3$ bulunur. O halde $|\hat{k}| = 3$ ve $|\bar{k}^x| = 3^4 - 1 = 80$ dir. $4 | 80$ fakat $4 \nmid |B|$ olduğundan $2 \nmid |B|$ dir. Çünkü B , $\bar{k}^x$ nin

Bir Hall altgrubudur. Bundan dolayı $|B| = 5$ dir. Böylece (1) şartı elde edilir.

Son olarak $|\mathcal{G}| = 2$ olsun. $\sigma \in \mathcal{G}$ elemanının mertebesi 2 olsun. Böylece

$$[\bar{k}^x, \hat{k}^x] = (x - 1)/x - 1 = x + 1$$

dir. O zaman Lemma 3.17 nin (1) ve (2) şartlarından dolayı $p = 3, 5$ dir. Böylece $x + 1 = 2^e \cdot 3$ veya $x + 1 = 2^e \cdot 5$ dir. Eğer $e \geq 1$ ise $4 | x^2 + 1$ dir. Fakat $4 \nmid |B|$ ve $B, \bar{k}^x$ nin bir Hall altgrubu olduğundan $2 \nmid |B|$ dir. Böylece $|B| = 3, 5$ dir.

Eğer $e = 0$ ise $x + 1 = p$ dir. Burada $p = 3, 5$ olduğundan $x = 2, 4$ dir. $x = 2, 4$ olduğundan $2 \nmid x - 1$ dir. Böylece $|B| = 3, 5$ dir. Buradaki değerlerden (4) ve (7) şartları elde edilir.

Böylece tablo gösterilmiş olur.

3.20. LEMMA : Lemma 3.19 ın (4) ve (5) hallerinde $|\hat{k}| = r$ sayısı, $a = 1$ için $|\hat{k}| = 9$ olması hali dışında r asal sayıdır.

İSPAT : $m > 1$ olmak üzere $|\hat{k}| = r^m$ olsun. O zaman Lemma 3.19 da (4) ve (5) den dolayı $\delta = 3, 5$ olmak üzere $r^m = 2^{a_\delta} - 1 \Rightarrow r^m + 1 = 2^{a_\delta}$ dir. Eğer $a > 1$ ise $4 | r^m + 1$ olduğundan $r^m \equiv -1 \pmod{4}$ ve m tekdir. Böylece $2^a | (r + 1)$ dir. Bundan dolayı $2^a = r + 1$ dir. $2^{a_\delta} = r^m + 1$ ve $2^a = r + 1$ olduğundan $\delta = \frac{r^m + 1}{r + 1}$ dir. Fakat son eşitliğin çözümü yoktur. Çünkü $\delta = \frac{r^m + 1}{r + 1}$ olduğundan $r(r^{m-1} - \delta) = (\delta - 1)$ el-

de edilir. Buradan $r \mid (\delta-1)$ dır. Fakat $\delta = 3,5$ olduğundan r bir çift sayıdır. Bu ise r nin tek olmasıyla çelişir.

Böylece $a > 1$ iken $m = 1$ ve $|\hat{k}| = r$ asal sayıdır.

Şimdi $a = 1$ olsun. O zaman $r^m + 1 = 2\delta$ olduğundan $\delta = 3$ için $|\hat{k}| = r^m = 5$ ve $\delta = 5$ için $|\hat{k}| = r^m = 9$ elde edilir. Bu ise ispatı tamamlar.

BÖLÜM 4

MINİMAL HALİN BELİRLENMESİ

Minimal halde ortaya çıkabilecek bütün durumlar ayrıntılı olarak incelenecektir.

Bu bölümde önceki durumlara devam edeceğiz. A nın $\bar{k}^+ \setminus \{0\}$ üzerinde üç regüler yörüngenin olmadığı halleri ayrıntılı olarak belirleyeceğiz.

Kabul edelim ki A nın en çok regüler yörüngesi bulunsun. Hatırlanacağı üzere

$$G \leq \mathcal{J} = \mathcal{J}(\bar{k}/\hat{k})$$

$$G \cap \bar{k}^x = M = A_0 \times B$$

ve M, G nin kendisinin merkezleyeni olan, maksimal devirli bir altgrubudur. Ayrıca $k(M) = \bar{k} = GF(r^m)$ dir.

$$|g| = g, |\hat{k}| = r^n \text{ olsun.}$$

(I) $M = G$ olsun. Bu durumda $G \leq \bar{k}^x$ olduğundan G nin $\bar{k}^+$ üzerine etkisi regüler permütasyon etkisidir. Bundan dolayı A nın regüler yörünge sayısı

$$[\bar{k}^x : A] = \frac{r^m - 1}{|A|} \geq 3 \text{ veya } \frac{r^m - 1}{|A|} = 1, 2$$

dir. Eğer $\frac{r^m - 1}{|A|} = 1$ ise $|A| = r^m - 1$ olduğundan $|A| = |\bar{k}^x|$

dir. Bundan dolayı $|B| = 1$ dir. Şimdi $\frac{r^m - 1}{|A|} = 2$ olsun.

Eğer $2 \nmid |A|$ ise $A \leq C_G(B)$ ve $(|B|, |C_G(B) \cap A|) = 1$ olduğun-

dan $|B| = 1$ olmalıdır. Eğer $2 \parallel (r^m - 1)$ ise o zaman $2 \nmid |A|$

dir. Buradan $|B| = 1, 2$ olabilir. Ayrıca $A = A_0$ dir. Böy-

lece aşağıdaki tablo elde edilir.

$\frac{r}{r}$	$\frac{g}{1}$	$\frac{n}{n}$	$\frac{ A_0 }{r^{m-1}}$	$\frac{B}{1}$	$\frac{\text{reg}}{1}$	$\frac{\text{diğer}}{0}$
r	1	n	r^{m-1}	1	1	0
r	1	n	$\frac{r^{m-1}}{2}$	$1,2$	2	0

Burada $\bar{k}^+ \setminus \{0\}$ üzerindeki regüler yörünge sayısı "reg" ile diğer yörünge sayısında "diğer" ile gösterilmiştir.

(II) $M < G$

(1) $\mathcal{T}$ nilpotent olsun. O zaman $\bar{k}^x / \hat{k}^x$ bölüm grubu ve buradan $\mathcal{G}$ bir 2-grubu olmak zorundadır. $\bar{k}^x$ nın Sylow 2-altgrubu T olsun $\hat{k}^x$ in maksimal 2'-altgrubu Z olsun. O zaman $\bar{k}^x = T \times Z$ dir. $\mathcal{G} = \langle \sigma \rangle$ olsun. Eğer Hipotez 3.11. sağlanırsa Lemma 3.19 dan dolayı $2 \nmid |B|$ olduğundan $B \leq \hat{k}^x$ dir. Fakat $\mathcal{T} = \mathcal{G}\bar{k}^x$ ve $\mathcal{G} = \text{Gal}(\bar{k}/\hat{k})$ olduğundan $\mathcal{G}$ grubu B yi merkezler. Böylece $C_G(B) = G$ olur. Bu Hipotez 3.11 (b) ile çelişir. Böylece Hipotez 3.11 in sağlandığını kabul edebiliriz. O zaman Lemma 3.12 den dolayı $\bar{k} = GF(r^2)$, $r = 2^a - 1$ ve $B \leq GF(r)$ dir. Bundan başka $|\mathcal{G}| = 2$ ve G nin maksimal seçiminden dolayı $A_0 = T$ dir. $A = \langle \sigma \rangle A_0$, $|A| = 2 \cdot 2^{a+1} = 2^{a+2}$ dir. $(r-1, r+1) = 2$ olduğundan $4 \nmid \hat{k}^x$ dir. Böylece $r-1 = 2|Z|$ ve $|Z| = \frac{r-1}{2}$ dir. Şimdi, $z \in Z$ olsun. T nin z ye uygulanmasıyla

$$z, tz, t^2z, \dots, t^{2^{a+1}-1}z$$

elde edilir. Bu elemanlara σ uygulanırsa, yine bu elemanlar elde edilir. Çünkü T , σ altında invaryanttır ve $\sigma(z) = z$ dir. Böylece $\langle \sigma \rangle T$ nin z ye uygulanmasıyla elde edilen yörünge'nin uzunluğu $|T| = 2^{a+1}$ dir. Şimdi eğer z , Z nin elemanları üzerinde değişirse $|Z| = \frac{r-1}{2}$ adet ayrık yörünge elde edilir. $\frac{r-1}{2} |T| = \frac{r-1}{2} \cdot 2(r+1) = r^2 - 1 = |\bar{k}^x|$

olduğundan başka yörünge yoktur. Özel olarak A'nın regüler yörüngesi yoktur. $T_1 = \mathcal{G}T$ olsun. $|T_1| = 2^{a+2}$ dir.

Şimdi $T_2 = \mathcal{G}T^2$ olsun. $T = \langle t \rangle$ olduğundan $T^2 = \langle t^2 \rangle$ dir. $\sigma(t) = t^r = t^{-1+2^a}$ olduğundan $\sigma(t^2) = t^{-2}$ dir. Ayrıca $\sigma^2 = (t^2)^{2^a} = 1$ dir. Bundan dolayı T_2, T nin bir maksimal dihedral altgrubudur. T_2 nin bütün yörüngeleri T_1 in yörüngelerinden elde edilebilir.

$$\{z, tz, t^2z, \dots, t^{2^{a+1}-1}z\}$$

yörüngesine $T^2 = \langle t^2 \rangle$ uygulanırsa

$$A = \{z, t^2z, t^4z, \dots, t^{2^{a+1}-2}z\}$$

ve

$$B = \{tz, t^3z, \dots, t^{2^{a+1}-1}z\}$$

yörüngeleri elde edilir. Esasen A ve B T_2 nin birer yörüngesidir. Bunun için $\sigma(A) \subseteq A$ ve $\sigma(B) \subseteq B$ olduğunu göstermek yeter.

$$\sigma(t^{2i}z) = t^{2i(-1+2^a)}z = t^{-2i}z \in A$$

dir. Benzer şekilde $\sigma(B) \subseteq B$ dir. Aşıkarak olarak

$|B| = |A| = |T|/2$ dir. Eğer A tipindeki yörüngeleri bir sınıfta ve B tipindeki yörüngeleri başka bir sınıfa ko-nursa, o zaman T_2 nin eşlenik olmayan iki sınıfı elde edilir. Her sınıfta herbirinin uzunluğu $|T|/2$ olan $(r-1)/2$ yörünge vardır. $|T_2| = |\mathcal{G}T^2| = |T|$ olduğundan, bu durumda regüler yörünge yoktur.

Şimdi $T_3 < T_2, T_2$ nin maksimal dihedral altgrubu olsun. $T_3 = \mathcal{G}\langle t^4 \rangle$ alınabilir. Eğer T_3 A yörüngesine uygulanırsa

$$A_1 = \{z, t^4 z, \dots, t^{2^{a+1}-4} z\}$$

$$A_2 = \{t^2 z, t^6 z, \dots, t^{2^{a+1}-2} z\}$$

şeklinde iki yörünge elde edilir ve $|A_1| = |A_2| = |T|/4$ tür. Eğer T_3, B ye uygulanırsa tekrar B elde edilir. Bundan dolayı T_3 ün $\bar{k}^+ \setminus \{0\}$ üzerinde $(r-1)/2$ regüler yörüngesi ve herbirinin uzunluğu $|T|/4 = 2^{a-1}$ olan $(r-1)$ regüler olmayan yörüngesi vardır.

Şimdi $T_4 < T_1, T_1$ in maksimal genel quaterniyon veya quaterniyon altgrubu olsun. $(t^2)^{2^a} = t^{2^{a+1}} = 1 = \sigma(t^2) = t^{-2}$ ve $(\sigma t)^2 = \sigma t \sigma t = \sigma t \sigma^{-1} t = \sigma(t) t = t^{2^a-1} = t^{2^a}$ olduğundan $T_4 = \langle \sigma t, t^2 \rangle$ alınabilir. Eğer T_4 grubu $z \in Z$ ye uygulanırsa

$$z, t^2 z, \dots, t^{2^{a+1}-2} z, t^{2^a-1} z, \dots, t^{1+2^a} z$$

elemanlarından oluşan yörünge elde edilir. Bu yörünge

$$z, tz, \dots, t^{2^{a+1}-1} z$$

elemanların yörüngesidir. Böylece T_4 in $(r-1)/z$ yörüngesi vardır. Yani her yörünge regülerdir.

Eğer $T_5 < T_4$ ün maksimal quaterniyon veya genel quaterniyon altgrubu ise T_5 in $(r-1)$ adet regüler yörüngesi vardır. Eğer $|T_1| = 16$ ise T_5 yoktur.

Şimdi $C, \hat{k}^+ \setminus \{0\}$ in mertebesi tek sayı olan bir altgrubu ve $|C| = (r-1)/2\mu$ olsun. O zaman yukardaki açıklamalardan kolayca aşağıdaki yörünge tablosu elde edilir.

<u>Grup</u>	<u>reg</u>	<u>diğer</u>
T_1C	0	$(2^{a+1} C)^\mu$
T_2C	0	$(2^a C)^{2\mu}$
T_3C	μ	$(2^{a-1} C)^{2\mu}$
T_4C	μ	0
T_5C	2μ	0

Burada $(x)^Y$ nin anlamı herbirinin uzunluğu x olan y tane yörünge demektir.

Yukarıdaki açıklamalardan görüldüğü gibi T_1 in yukarıdaki tablodan görülen altgruplarına izomorf altgrup içermeyen her altgrup en az üç regüler yörünge içerir. Yalnız mertebesi sekiz olan dihedral grubun, devirli olmayan abeliyan altgrubu olduğundan G nin seçiminde bu duruma dikkat edilmelidir.

Şimdi yukarıdaki tablodan yararlanarak A nın üçten az regüler yörüngesinin olması halleri aşağıdaki tabloda gösterilmiştir.

<u>r</u>	<u>g</u>	<u>n</u>	<u>A_0</u>	<u>B</u>	<u>reg</u>	<u>diğer</u>	
2^a-1	2	1	$2^a(r-1)/\mu$	b	0	$(A_0)^\mu$	parçalanmış
2^a-1	2	1	$2^{a-1}(r-1)/\mu$ ($a > 2$)	b	0	$(A_0)^{2\mu}$	parçalanmış
2^a-1	2	1	$2^{a-2}(r-1)$ ($a > 3$)	1	1	$(A_0)^2$	parçalanmış
2^a-1	2	1	$2^{a-1}(r-1)$	1	1	0	parçalanmamış
2^a-1	2	1	$2^{a-2}(r-1)$ ($a > 2$)	1	2	0	parçalanmamış

Burada μ tek olmak üzere $(|A|, b) = 1$ ve $b|\mu$ dür. Son kolon A nın A_0 üzerinde parçalanmış olup olmadığını gösterir.

(ii) $\mathcal{T}$ nilpotent değildir.

Önce A nın A_0 üzerinde parçalanmış olduğu hali inceleyelim. Eğer Hipotez 3.11 sağlanmaz ise Lemma 3.12 den dolayı $B \leq GF(r) \leq \hat{k}$ olduğundan $G = C_G(B)$ dir. $|\bar{k}^x/\hat{k}^x| = r + 1 = 2^a$ olduğundan $\mathcal{G}$ bir 2-grubudur ve $\bar{k}^x$ nin Sylow 2-altgrubu T ise $\bar{k}^x = \hat{T}\hat{k}^x$ ve $|T \cap \hat{k}^x| = 2$ dir. $\mathcal{G}$ grubu $\hat{k}^x$ üzerinde aşikar olduğundan $\mathcal{T} = \mathcal{G}(T\hat{k}^x)$ grubu nilpotenttir. Fakat $\mathcal{T}$ nilpotent olmadığından bu gelişkidir. Bundan dolayı Hipotez 3.11 in sağlandığını kabul edebiliriz. Kabul edelim ki A nın $\bar{k}^x$ üzerindeki yörünge sayısı üçten az olsun. Bu hal Lemma 3.19 ve Lemma 3.20 de tam olarak tablo halinde gösterilmiştir. Şimdi bu tablodan yararlanarak Hipotez 3.1 in şartını sağlayan altgruplar için ayrıntılı bilgiler elde edelim. Bunun için Lemma 3.19 in durumlarını inceleyelim.

$$(1) \quad |\mathcal{G}| = 4, \quad |\hat{k}| = 3, \quad |B| = 5$$

$\bar{k}^x$ in Sylow 2-altgrubu T olsun. $|\mathcal{G}| = 4$ olduğundan $|\bar{k}^x| = 3^4 - 1 = 80 = 5 \cdot 16$ dir. Buradan $|T| = 16$ bulunur. Ayrıca $(|A_0|, |B|) = 1$ olduğundan $A_0 \leq T$ dir. Önce $A_0 = T$ olsun. O zaman $A = \mathcal{G}A_0 = \mathcal{G}T$, $\mathcal{G}$ ile T nin parçalanmış genişlemesidir. $\bar{k}^x = B \times T$ dir. $\mathcal{G} = \langle \sigma \rangle$, $B = \langle b \rangle$ ve $T = \langle t \rangle$ olsun. $\mathcal{G}$, T yi normallediğinden $\mathcal{G}T$ nin $1 \in \bar{k}^x$ elemanından elde edilen yörüngesi

$$\{1, t, t^2, \dots, t^{15}\}$$

olup, $|\mathcal{G}T| = 64$ olduğundan regüler değildir. Şimdi de b den elde edilen yörüngeye bakalım.

$$b, bt, bt^2, \dots, bt^{15} \quad (1)$$

elemanına σ uygulanırsa $\sigma(x) = x^3$ olduğundan,

$$b^3, b^3\sigma(t), \quad b^3\sigma(t^2), \dots, b^3\sigma(t^{15})$$

elde edilir. Fakat σ bir otomorfizma olduğundan bu elemanlar _

$$b^3, b^3t, \quad b^3t^2, \dots, b^3t^{15} \quad (2)$$

elemanlarından ibarettir. Burada σ yerine σ^2, σ^3 alınırsa $\sigma^2(b) = b^9 = b^4$, $\sigma^3(b) = b^2$ olduğundan, sırasıyla

$$b^4, b^4t, \quad b^4t^2, \dots, b^4t^{15} \quad (3)$$

$$b^2, b^2t, \quad b^2t^2, \dots, b^2t^{15} \quad (4)$$

elemanları elde edilir. Bu şekilde $\sigma^4 = I$, σ , σ^2, σ^3 elemanlarına karşılık gelen dört satırdaki bütün elemanlar birbirinden farklı olduğundan b den elde edilen yörünge 4.16 = 64 eleman vardır. Ayrıca $|\mathcal{G}T| = 4.16 = 64$ olduğundan bu yörünge regülerdir. $64 + 16 = 80 = |\bar{k}^X|$ olduğundan, bu durumda A nın bir regüler ve bir de regüler olmayan yörüngesi vardır.

Şimdi $A_0 = T^2$ olsun. O zaman $A = \mathcal{G}T^2$, $\mathcal{G}$ ile T nin parçalanmış genişlemesidir. $|A| = 4.8 = 32$ dir. Şimdi $\langle \sigma \rangle$, T^2 yi sabit bıraktığından

$$1, t, t^2, \dots, t^{15}$$

elemanlarından herbirinin uzunluğu sekiz olan

$$1, t^2, t^4, \dots, t^{14}$$

$$t, t^3, t^5, \dots, t^{15}$$

iki regüler olmayan yörünge elde edilir. $\mathcal{G}T^2$ nin yukarıdaki regüler yörüngeye uygulanmasıyla da,

$$\{b, bt^2, \dots, bt^{14}, b^3, b^3t^2, \dots, b^3t^{14}, b^4, b^4t^2, \dots, b^4t^{14}, b^2, b^2t^2, \dots, b^2t^{14}\}$$

ve

$$\{bt, bt^3, \dots, bt^{15}, b^3t, b^3t^3, \dots, b^3t^{15}, b^4t, b^4t^3, \dots, b^4t^{15}, b^2t, b^2t^3, \dots, b^2t^{15}\}$$

uzunluğu 32 olan yukardaki iki regüler yörünge elde edilir.

$$2 \times 32 + 2 \times 8 = 80 = |\bar{k}^x|$$

olduğundan başka yörünge yoktur.

Şimdi $A = \langle \sigma t, t^2 \rangle$ olsun.

$$\begin{aligned} (\sigma t)^4 &= (\sigma t)(\sigma t)(\sigma^2 t^4) = (\sigma t)(\sigma^3 t^9 t^4) = (\sigma t)(\sigma^3 t^{13}) \\ &= (\sigma^4 \sigma^3(t) t^{13}) = (1 t^{27} t^{13}) = t^8 \end{aligned}$$

olduğundan $o(\sigma t) = 8$ ve $|A| = 32$ dir. 1 elemanından elde edilen yörüngeyi belirleyelim. 1 e $\langle t^2 \rangle$ uygulanırsa

$$1, t^2, t^4, \dots, t^8$$

elde edilir. Bu elemanlara σt uygulanırsa

$$t, t^3, t^5, \dots, t^{15}$$

elde edilir. Böylece $1, t, t^2, \dots, t^{15}$ yörüngeye aittir. Fa-

kat A nın herhangi bir elemanının 1 e uygulanması $\langle t \rangle$

nin bir elemanı olduğundan 1 den elde edilen yörünge

$$1, t, t^2, t^3, \dots, t^{15}$$

den ibarettir. Şimdi de b den elde edilen yörüngeyi belirleyelim.

$$b, t^2b, t^4b, \dots, t^{14}b$$

yörüngeye ait sekiz elemandır. Bu elemanlara σt uygulanırsa

$$tb^3, t^3b^3, t^5b^3, \dots, t^{15}b^3$$

elde edilir. Aynı işlem σt yerine $(\sigma t)^2$ ve $(\sigma t)^3$ ile tekrarlanırsa $(\sigma t)^2 = \sigma t \sigma t = \sigma^2 t^4$ ve

$$(\sigma t)^3 = (\sigma t)(\sigma^2 t^4) = \sigma^3 t^9 t^4 = \sigma^3 t^{13} = \sigma^{-1} t^{-3} \text{ olduğundan}$$

sırasıyla

$$b^4, t^2b^4, t^4b^4, \dots, t^{14}b^4$$

ve

$$tb^2, t^3b^2, t^5b^2, \dots, t^{15}b^2$$

satırları elde edilir. Böylece b den elde edilen yörünge-
de 32 eleman vardır. Dolayısıyla bu yörünge regülerdir.
Burada b yerine bt alınırsa 32 elemanlı bir regüler yörün-
ge daha elde edilir. Bu durumda iki regüler yörünge ile
uzunluğu 16 olan bir regüler olmayan yörünge elde edilir .

$|A_0| \leq 4$ için Hipotez 3.1 şartları sağlanmaz. Böy-
lece aşağıdaki tablo elde edilir. Hipotez 3.1 den dolayı
 $|B| \neq 1$ dir.

r	g	n	$ A_0 $	$ B $	reg	diğer
3	4	1	16	5	1	(16)
3	4	1	8	5	2	(8) ²
3	4	1	8	5	2	(16)

$$(2) \quad |\mathcal{G}| = 3, \quad |\hat{k}| = 4, \quad |B| = 7$$

$|\bar{k}^x| = 4^3 - 1 = 63 = 7 \times 9$ dur. $\bar{k}^x$ in Sylow 3-altgrubu
 T olsun. $A_0 \subseteq T$ dir. $A_0 = T$ olsun. O zaman $A = \mathcal{G}T$ ve
 $\bar{k}^x = T \times B$ dir. $\mathcal{G}$, T yi invaryant bıraktığından $\mathcal{G}T$ nin
1 e uygulanmasıyla

$$1, t, t^2, \dots, t^8$$

yörüngesi elde edilir. Şimdi de $\mathcal{G}T$ yi b ye uygulayalım.
 T nin uygulanmasıyla

$$b, tb, t^2b, \dots, t^8b$$

elde edilir. Bu satıra σ , σ^2 uygulanırsa $\sigma(x) = x^4$ ve
 $\sigma^2(x) = x^2$ olduğundan, b yerine sırasıyla b^4, b^2 gelir.
Böylece b den elde edilen yörüngenin uzunluğu $3 \times 9 = 27 = |A|$

dır. Yani bu yörünge regülerlerdir. Şimdi $\mathcal{G}_T$, b^3 e uygulanırsa bir regüler yörünge daha elde edilir. $27+27+9=63$ olduğundan başka yörünge yoktur.

A'nın bir X altgrubunun A'nın bir regüler yörüngesi üzerinde yarı regüler olduğundan A'nın regüler yörüngesi X'in $[A:X]$ regüler yörüngesinin ayrık bileşimidir. Şimdi eğer $|A_0|=3$ alınırsa, o zaman $\mathcal{G}_{A_0}$ grubunun yukarıda tanımlı A içindeki indeksi 3 olduğundan $\bar{k}^X$ içinde en az üç regüler yörüngesi vardır. Fakat kabulümüzden dolayı A'nın en çok iki regüler yörüngesi olduğundan $A \neq \mathcal{G}_{A_0}$ olmalıdır. Yani $|A_0|=3$ hali olamaz.

Eğer $|B|=1$ ise $G=A=\mathcal{G}_{A_0}$ mertebesi 27 olan bir gruptur, fakat $\langle \sigma, t^3 \rangle \trianglelefteq G$ ve elemanter abeliyan olduğundan ve de Hipotez 3.1 de G'nin her normal abeliyan altgrubu devirli olduğundan, G, Hipotez 3.11 i sağlamaz. Dolayısıyla $|B|=1$ olamaz. Böylece aşağıdaki tablo elde edilir.

$\frac{r}{2}$	$\frac{g}{3}$	$\frac{n}{2}$	$\frac{ A_0 }{9}$	$\frac{ B }{7}$	$\frac{\text{reg}}{2}$	$\frac{\text{diğer}}{(9)}$
2	3	2	9	7	2	(9)

$$(3) \quad |\mathcal{G}| = 3, |\hat{k}| = 2, |B| = 7$$

$|\bar{k}^X| = 2^3 - 1 = 7 = |B|$ olduğundan $|A_0|=1$ dir.

$\sigma(b) = b^2 \neq b$ olduğundan $\langle \sigma \rangle$ nın $\langle b \rangle$ üzerinde iki regüler yörüngesi ve bir aşıkâr yörüngesi vardır.

$|\bar{k}^X| = 2 \times 3 + 1$ olduğundan başka yörünge yoktur.

$|B|=1$ olması Hipotez 3.1 ile çelişmez. Böylece aşağıdaki tablo elde edilir.

<u>r</u>	<u>g</u>	<u>n</u>	<u> A₀ </u>	<u> B </u>	<u>reg</u>	<u>diğer</u>
3	2	2	16	5	2	(16)

$$(4') \quad |\mathcal{G}| = 2 \quad |\hat{k}| = r = 2^a, \quad a > 1, \quad |B| = 5$$

$|\bar{k}^x| = r^2 - 1 = (r-1)(r+1) = (2^{a-1}.5-2)(2^{a-1}.5) = 2^{a+1}.5(2^{a-1}.5-1)$
 dir. $T = \langle t \rangle$, $\bar{k}^x$ in Sylow 2-altgrubu olsun. $\sigma(t) = 2^{a+1}$
 ve $\sigma(t) = t^r = t^{2^{a-1}.5-1} = t^{2^{a+2}} t^{2^{a-1}} = t^{-1+2^a}$ olduğundan
 $\langle \sigma, T \rangle = \langle \sigma \rangle T$ yarı dihedraldir. Şimdi

$|A_0| = 2^{a+1}(2^{a-1}.5-1) = 2^a(2^{a-1}.5-2) = 2^a(r-1)$ ve
 $|B| = 5$ alınırrsa G için maksimum seçenek $G = AB = \langle \sigma \rangle A_0 B$
 elde edilir. $|A| = |\langle \sigma \rangle A_0| = 2^{a+1}(r-1)$ dir. A nın 1'e
 uygulanması $|A| = 2^a(r-1)$ uzunluğunda bir yörünge verir.
 A nın b ye uygulanması bir regüler yörünge verir $\sigma^2 = I$
 ve $\sigma(b) = b^{-1}$ olduğundan b^2 bu yörüngeye ait değildir. A
 nın b^2 ye uygulanması ikinci bir regüler yörünge verir.
 Böylece

$$\begin{aligned}
 |A| + |A| + 2^a(r-1) &= 2^{a+1}(r-1) + 2^{a+1}(r-1) + 2^a(r-1) \\
 &= (r-1)(2^{a+1} + 2^{a+1} + 2^a) \\
 &= (r-1)2^{a+1}.5 \\
 &= (r-1)(r+1) \\
 &= r^2 - 1 \\
 &= |\bar{k}^x|
 \end{aligned}$$

olduğundan başka yörünge yoktur.

$$|\langle \sigma \rangle A_0| = 2^{a+1}(r-1) = 2^{a+2}(2^{a-1}.5-1)$$

olduğundan $\langle \sigma \rangle A_0$ grubu yarıdihedral bir 2-grubu ile
 mertebesi tek olan bir devirli grubun direkt çarpımıdır.
 Bu grup Hipotez 3.1 in şartını sağladığından $G = \langle \sigma \rangle A_0$
 alınabilir. Dolayısıyla $|B| = 1$ hali mümkündür. Böylece

aşağıdaki değerler elde edilir.

r	g	n	$ A_0 $	$ B $	reg	diğer
$5 \cdot 2^a - 1$	2	1	$2^a(r-1)$	1,5	2	$(A_0) \quad a > 1$

$$(5) \quad |G| = 2, \quad |\hat{k}| = r = 5, \quad |B| = 3$$

$|\bar{k}^x| = 5^2 - 1 = 24 = 8 \times 3$ tür. $|A_0| = 8$ ve $|B| = 3$ alınır-
sa, G için maksimum seçenek $G = \langle \sigma \rangle A_0 B$ elde edilir.

$|A_0| = 8$ olduğundan, A nın $1 \in \bar{k}^x$ elemanından elde edilen, uzunluğu 8 olan bir yörüngesi vardır. $o(b) = 3$ olsun. A nın b ye uygulanması bir regüler yörünge verir. $|A| = 16$ olduğundan $16 + 8 = 24$ tür. Dolayısıyla başka yörünge yoktur. $A_0 = \langle t \rangle$ olsun. $o(t) = 8$ dir. $\sigma(t) = t^5 = t^{1+2^2}$ olduğundan $t^{-1}\sigma t\sigma = t^{-1}t^5 = t^4 \in \langle \sigma, t^4 \rangle$ tür. $o(t^4) = 2$ ve $\langle \sigma, t^4 \rangle \triangleleft \langle \sigma \rangle A_0$ olduğundan $|B| = 1$ mümkün değildir. Çünkü G nin normal abeliyan her altgrubu devirli olduğundan Hipotez 3.11 ile gelişir.

Şimdi $|A_0| = 4$ olsun. O zaman $o(t) = 8$ olmak üzere $A_0 = \langle t^2 \rangle$ dir $\sigma(t^2) = t^{10} = t^2$ olduğundan $[\sigma, t^2] = 1$ dir. Dolayısıyla $\langle \sigma, t^2 \rangle$ abeliyandır. Fakat $\sigma(b) = \sigma^{-1}b\sigma \in \langle b \rangle$ olduğundan $b^{-1}\sigma^{-1}b\sigma = [\sigma, b] \in \langle b \rangle$ dir. $\langle \sigma, t^2 \rangle \cap \langle b \rangle = 1$ olduğundan $[\sigma, b] \notin \langle \sigma, t^2 \rangle$ dir. Bundan dolayı $\langle \sigma, t^2 \rangle$ nin σ yı içine alan hiç bir altgrubu b tarafından normallenmez. Dolayısıyla G olarak $\langle \sigma \rangle A_0 B$ alınabilir. Buradan $|B| = 1$ mümkün değildir. Böylece aşağıdaki tablo elde edilir.

r	g	n	$ A_0 $	$ B $	reg	diğer
5	2	1	8	3	1	(8)
5	2	1	4	3	2	(4) ²

$$(5') \quad |\mathcal{G}| = 2, \quad |\hat{k}| = r = 2^a \cdot 3 - 1, \quad a > 1 \quad |B| = 3$$

$$|\bar{k}^x| = r^2 - 1 = (r-1)(r+1) = 2^a \cdot 3(r-1) = 3 \cdot 2^a(r-1) \text{ dir.}$$

$|A_0| = 2^a(r-1)$ ve $|B| = 3$ alınırsa G için maksimum seçenek $G = \langle \sigma \rangle A_0 B$ elde edilir. $|A| = |\langle \sigma \rangle A_0| = 2^{a+1}(r-1)$ dir. (4') de olduğu gibi A nın bir regüler yörüngesi ve uzunluğu $|A_0|$ olan bir yörüngesi vardır.

$$\begin{aligned} |A| + |A_0| &= 2^{a+1}(r-1) + 2^a(r-1) \\ &= (r-1) \cdot 2^a(2+1) \\ &= (r-1) \cdot (2^a \cdot 3 - 1 + 1) \\ &= (r-1) \cdot (r+1) \\ &= r^2 - 1 \\ &= |\bar{k}^x| \end{aligned}$$

olduğundan başka yörüngesi yoktur.

$\bar{k}^x$ in Sylow 2-altgrubu $\langle t \rangle$ olsun. $\sigma(t) = 2^{a+1}$ dir. $\sigma(t) = t^r = t^{2^a \cdot 3 - 1} = t^{2^{a+1} + 2^a - 1} = t^{-1 + 2^a}$ ve $a + 1 > 2$ olduğundan $\langle \sigma, t \rangle$ yarıdihedraldir. O zaman (4') de olduğu gibi $\langle \sigma \rangle A_0$ grubu Hipotez 3.1 in şartını sağlar. Dolayısıyla $|B| = 1$ olması mümkündür.

Şimdi $|A_0| = 2^{a-1}(r-1)$ olsun. A_0 in Sylow 2-altgrubu $\langle t^2 \rangle$ dir. $\sigma(t^2) = t^{2(-1 + 2^a)} = t^{-2} = (t^2)^{-1}$ olduğundan $\langle \sigma, t^2 \rangle$ dihedraldir. Eğer $|B| = 3$ ise $G = \langle \sigma \rangle A_0 B$, Hipotez 3.1 in şartını sağlar. Eğer $|B| = 1$ ise $|\langle \sigma, t^2 \rangle| > 8$ yani $a > 2$ olmalıdır. Böylece aşağıdaki tablo elde edilmiştir.

<u>r</u>	<u>g</u>	<u>n</u>	<u> A₀ </u>		<u> B </u>	<u>reg</u>	<u>diğer</u>
$2^a \cdot 3 - 1$	2	1	$2^a(r-1)$	($a > 1$)	1, 3	1	(A_0)
$2^a \cdot 3 - 1$	2	1	$2^{a-1}(r-1)$	($a > 1$)	1, 3	2	$(A_0)^2$

$$(6) \quad |\mathcal{G}| = 2, \quad |\hat{k}| = 4, \quad |B| = 5$$

$$(7) \quad |\mathcal{G}| = 2, \quad |\hat{k}| = 2, \quad |B| = 3$$

(6) ve (7) hallerine ait tablo aşağıdadır.

<u>r</u>	<u>g</u>	<u>n</u>	<u>A_0</u>	<u>B</u>	<u>reg</u>	<u>diğer</u>
2	2	2	3	5	2	(3)
2	2	1	1	3	1	(1)

Yukardaki halleri kontrol ederken şuna dikkat etmek gerekir. G grubu Hipotez 3.1 in şartlarını sağlamalıdır. Yani G nin her normal abeliyan altgrubu devirli olmalıdır. Bundan başka eğer A nın bir regüler yörüngesi varsa A nın $[A: A_0] = 3$ olan her devirli altgrubunun en az üç regüler yörüngesi olacaktır. Bundan başka A yerine alınacak her X altgrubu için $X/(X \cap \bar{k}^X) \cong \mathcal{G}$ olmalıdır.

BÖLÜM 5

TEOREMİN İFADESİ

Buraya kadar elde ettiğimiz bütün sonuçları teorem halinde ifade edebiliriz.

Önce hipotezimizi tekrar verelim.

5.1. HİPOTEZ :

(1) $G = AB$ bir grup, B , G nin bir normal devirli altgrubu; A , B nin bir nilpotent bütünleyicisi ve $A \cap B = 1$ dir.

(2) $k = GF(r)$, r asal sayı

(3) V bir indirgenmez $k[G]$ -modülü ve her $L \trianglelefteq G$ için $V|_L$ homojendir.

Lemma 3.3 ten dolayı G grubu kendi merkezliyenine eşit bir devirli normal M altgrubu içerir ve $B \leq M$ dir. $A_0 = A \cap M$ olsun. Aşağıdaki sembolleri kullanacağız.

c - G devirlidir

n - G nilpotenttir.

n^* -Eğer $|B| = 1$ ise G nilpotenttir. Quaterniyon c , n veya n^* ile işaretlenmiş her durum nilpotent değildir.

q - Eğer Q , A nın bir Sylow 2-altgrubu ise o zaman Q quaterniyon veya genel quaterniyon olur. Bütün diğer hal-lerde Q , $Q \cap A_0$ üzerinde parçalanır.

$\mu, b - \mu, (r-1)$ in bir tek böleni ve b, μ nun bir böleni öyle ki $(b, |A_0|) = 1$ dir.

reg- A nın V üzerindeki regüler yörüngelerinin sayısı

diğer- uzunluğu e ve sayısı f olan diğer yörüngeler $(e)^f$ ile gösterilir.

5.2 TEOREM : Kabul edelim ki Hipotez 5.1 sağlansın. Aşağıdaki haller dışında A nın V üzerinde daima en az üç regüler yörüngesi vardır.

$$t = \dim V / [A:A_0]$$

olsun. $V \cong \bar{k} = GF(r^m)$ ve $\hat{k} = GF(r^n)$ dir. Ayrıca $\mathcal{G} = \text{Gal}(\bar{k}/\hat{k})$ olduğundan $GF(r^m) = GF(r^{ng})$ dir. Buradan $m = ng$ bulunur. Şimdi $[A:A_0] = g$ ve $\dim_{\bar{k}} V = m$ olduğundan $\frac{m}{g} = n = t$ dir. Daha önce elde ettiğimiz bütün tablolar birleştirilirse aşağıdaki tablo elde edilir.

	<u>r</u>	<u>[A:A₀]</u>	<u>t</u>	<u> A₀ </u>	<u> B </u>	<u>reg</u>	<u>diğer</u>
(1)	2	2	1	1	3	1	(1)
(2)	2	2	2	6	5	2	(3)
(3)	2	3	1	1	7	2	(1)
(4)	2	3	2	9	7	2	(9)
(5)	3	2	2	16	3	2	(16)
(6)	3	4	1	16	5	1	(16)
(7)	3	4	1	8	5	2	(8) ²
(8)	3	4	1	8	5	2	(16)
(9)	5	2	1	8	3	1	(8)
(10)	5	2	1	4	3	2	(4) ²
(11)	r	1	m	(r ^m -1)	1	1	0 c
(12)	r	1	m	(r ^m -1)/2	1,2	2	0 c, (*)
(13)	2 ^a -1	2	1	2 ^a (r-1)/μ	b	0	(A ₀) ^μ n, a > 1
(14)	2 ^a -1	2	1	2 ^{a-1} (r-1)/μ	b	0	(A ₀) ^{2μ} n, a > 2
(15)	2 ^a -1	2	1	2 ^{a-2} (r-1)	1	1	(A ₀) ² n, a > 3
(16)	2 ^a -1	2	1	2 ^{a-1} (r-1)	1	1	0 n, q
(17)	2 ^a -1	2	1	2 ^{a-2} (r-1)	1	2	0 n, q, a > 2
(18)	2 ^{a.3} -1	2	1	2 ^a (r-1)	1,2	1	(A ₀) n [*] , a > 1
(19)	2 ^{a.3} -1	2	1	2 ^{a-1} (r-1)	1,3	2	(A ₀) ² n [*] , a > 1, (**)
(20)	2 ^{a.5} -1	2	1	2 ^a (r-1)	1,5	2	(A ₀) n [*] , a > 1

(*) ve (**) sembolleri şu durumlar için kullanılmıştır.

(*) |B| = 2 hali yalnızca (r-1)/2 tek ise mümkündür.

(**) Eğer |B| = 1 ise o zaman a > 2 dir.

BÖLÜM 6

BERGER'İN REGÜLER YÖRÜNGE TEOREMİ

Bu bölümde Teorem 5.2 yi kullanarak [2] deki regüler yörünge teoremi ispat edilecektir. Yani Berger'in en az bir regüler yörünge olmasına ait Teorem 2.2 nin ispatı verilecektir.

6.1. HİPOTEZ : A aşıkâr olmayan nilpotent grup olsun. Her $p \nmid |A|$ asal sayısı için A nın $Z_p \sim Z_p$ ye izomorf faktörü olmasın. $r \nmid |A|$ asal sayısı için $K = GF(r)$ ve V sadık $K[A]$ -modül olsun.

6.2. TEOREM : Eğer Hipotez 6.1 sağlanıyorsa o zaman A nın V nin elemanları üzerinde permütasyon etkisinin en az bir regüler yörüngesi vardır.

İSPAT : İspatı $\dim V$ üzerine indüksiyon yaparak göstereceğiz.

Kabul edelim ki Teorem 6.2 sağlanmasın ve (A, V) teoremi sağlamayan sıralı ikililer kümesi içinde $\dim V$ en küçük olan bir elemanı olsun.

(i) V indirgenmezdir.

Hipotez gereğince $(|A|, r) = 1$ olduğundan Maschke Teoreminden dolayı V tam indirgenir $K[A]$ -modülüdür. Böylece $1 \leq i \leq t$ için V_i ler indirgenmez $K[A]$ -altmodülleri olmak üzere

$$V = V_1 \dot{+} V_2 \dot{+} \dots \dot{+} V_t$$

şeklinde yazılabilir.

Kabul edelim ki $t > 1$ olsun. A nın V_1 üzerindeki temsilinin çekirdeği A_1 olsun. O zaman her $1 \leq i \leq t$ için $\dim V_i < \dim V$ ve V_i bir sadık indirgenmez $K[A/A_1]$ -modüldür. Böylece $(A/A_1, V_i)$ sıralı ikilisi teoremin hipotezini sağlar. O zaman indüksiyon hipotezinden dolayı A/A_1 nın V_1 üzerinde en az bir regüler yörüngesi vardır. Buradan (14), (1.1) den dolayı A nın V üzerinde en az bir regüler yörüngesi vardır. Bu kabulümüzle çelişir. Bundan dolayı $t = 1$ ve V indirgenmezdir.

(ii) Her $N \triangleleft A$ için $V|_N$ homojendir.

Kabul edelim ki bu doğru olmasın. O zaman öyle bir $N \triangleleft A$ vardır ki $V|_N$ homojen değildir. Bu durumda Clifford Teoreminden dolayı

$$V|_N = V_1 \dot{+} V_2 \dot{+} \dots \dot{+} V_t$$

yazılabilir. Burada V_i ler $V|_N$ nin homojen bileşenleridir. Kabulümüzden dolayı $t > 1$ dir. S, V_1 in A içindeki dengeleyeni olsun. O zaman Teorem 1.7 (c) den dolayı V bir indirgenmez $K[S]$ -modüldür ve $V_1|_S^A \cong V$ dir. S_1, S nin V üzerindeki temsilinin çekirdeği olsun. O zaman $(S/S_1, V_1)$ sıralı ikilisi teoremin hipotezini sağlar ve $\dim V_1 < \dim V$ dir. Böylece indüksiyon hipotezinden dolayı S/S_1 in V_1 üzerinde en az bir regüler yörüngesi vardır. O zaman (14), (4.2) (c) den dolayı A nın V üzerinde en az bir regüler yörüngesi vardır. Kabülden dolayı bu bir çelişkidir. Bun-

dan dolayı $V|_N$ homojendir. Böylece $|B| = 1$ için Teorem 5.2 nin Hipotezi 5.1 sağlanır. Fakat listeden görüldüğü gibi (13) ve (14) numaralı hallerin dışında A'nın V üzerinde en az bir regüler yörüngesi vardır. Fakat (14) nolu halde $a > 2$ olduğundan $|B| > 1$ dir. Bu teoremin hipotezinde ise $|B| = 1$ olduğundan, bu hal ortaya çıkamaz. (13) nolu halde ise $a > 2$ ise tekrar $|B| > 1$ dir. Öyleyse $a = 2$ haline bakalım. Bu durumda $r = 2^2 - 1 = 3$ olduğundan $|\hat{k}| = 3$ dür ve $|\bar{k}| = 3^2 = 9$. Şimdi $\bar{k}^x$ nin Sylow 2-altgrubu T olduğundan $|T| = 8$ dir. $A = \langle \sigma \rangle T$ bir yarıdihedral gruptur. $T = \langle t \rangle$ olsun. O zaman $\sigma(t) = t^3$ dür. Buradan $\sigma(t^2) = (t^2)^{-1} = t^{-2}$ olduğundan $\langle \sigma, t^2 \rangle$ mertebesi 8 olan bir dihedral gruptur. Fakat $\langle \sigma, t^2 \rangle \cong Z_2 \times Z_2$ olduğundan bu teoremin hipoteziyle çelişir.

KAYNAKLAR

1. Berger, T.R., "Hall-Higman Type theorems, I"
Can. J. Math., Vol XXVI 3, 513-531, (1974).
2. Berger, T.R. "Hall-Higman type theorems VI"
J. Algebra 51, 416-424, (1978).
3. Hall, P. and Higman, G., "On the p-length of
p-solvable groups and reduction theorems for
Burnside's problem", Proc. London Math.Soc.,6,
1-42, (1956).
4. Shult, E. "On groups admitting fixed point free
abelian operator groups, Illinois J. Math.9, 701-
720, (1965).
5. Berger, T.R. "Automorphisms of Solvable Groups"
J. Algebra, 27, 311-340, (1973).
6. Asar, A.O. Yayınlanmamış notlar.
7. Gorenstein, D. Finite Groups, Harper and Row,
Publishers, New York-Evanston-London, (1971).
8. Huppert, B., Endliche Gruppen I. Springer-Verlag,
Berlin-New York, (1967).
9. Darnhoff, L., Group Representation Theory Marcel
Dekker, Inc., New York, (1971).
10. Curtis, C.W. and Reiner, I.N., Methods of
Representation Theory Volume I, John Wiley, Sons,
New York-Chichester-Brisbane, Toronto.

11. Curtis, C.W. and Reiner, I.N., Representation Theory of Finite Groups and Associative Abgebras, New York, (1962).
12. Rose J.S., A Course on Group Theory, Combridge University Press, London-New-York. Belmoume (1978).
13. Hungerford, T.W., Algebra, Holt, Rinehart and Winston Company, (1973).
14. Berger, T.R. "Hall-Higman type theorems V" Pacific Journal of Math. Vol 73, 1-62, (1977).

T. C.
Yükseköğretim Kurulu
Dokümantasyon Merkezi

özgeçmiş

ÖZGEÇMİŞ

Aynur Yalincakoğlu 1964 yılında Sivas'ta doğdu.

İlk ve orta öğrenimini Sivas'ta, Devrim İlkokulu, Dört Eylül Ortaokulu ve Sivas Lisesinde tamamladı.

Yüksel öğrenimini Gazi Üniversitesi Gazi Eğitim Fakültesi, Fen Bilimleri Eğitimi Bölümü, Matematik Ana Bilim Dalında tamamladığı 1986 yılında, aynı Üniversitenin Fen Edebiyat Fakültesine araştırma görevlisi olarak atandı. Halen bu görevini sürdürmektedir.

