The $\mathcal{C}_6$ Subgroups of Classical groups

Southern University of Science and Technology

xyl 11930521@mail.sustech.edu.cn

March 8, 2022

The $\mathcal{C}_6$ Subgroups of Classical groups

Southern University of Science and Technology

xyl 11930521@mail.sustech.edu.cn

April 3, 2022

Overview

A subgroup of linear(symplectic/unitary) groups in Aschbacher's class $\mathcal{C}_6$ is **the normalizer of a symplectic type** p **-group of exponent** $p(p,2)$ in linear(symplectic/unitary) groups.

1. Structure and automorphism groups of symplectic type p-groups
   1. Structure and automorphism of extraspecial p-groups
   2. Regular p-groups
   3. Inner automorphisms of extraspecial p-groups.
2. Embedding symplectic type p-groups in linear (Symplectic/unitary) groups
   1. Representation of extraspecial-r groups R (here r is a prime number).
   2. Full normalizer of R in linear groups.
   3. Dimension 2 examples.
   4. Dimension 3 examples.

Symplectic-p group, Extraspecial p-group and Regular p-group

Definition

A p-group P is of **Symplectic type** if every characteristic abelian subgroup of P is cyclic.

Definition

A **special**-p group is a p-group P such that $\Phi(P) = Z(P) = P'$, if moreover $\Phi(P) = Z(P) = P' \cong \mathbb{Z}/p\mathbb{Z}$, then P is called an **extraspecial**-p group.

Definition

A P-group is **regular** if for each $x, y \in P$, $(xy)^p = x^p y^p \prod_i d_i^p$ for some $d_i \in \langle x, y \rangle'$

Definition

Let P be a p-group,

$$\Omega_k(P) := \langle x \mid x \in P, x^{p^k} = e \rangle$$
$$\mho_k(P) := \langle x^{p^k} \mid x \in P \rangle$$

A not very important theorem: If P is a regular p-group, $\Omega_k(P) = \{x \in P \mid x^{p^k} = e\}, \mho_k(P) = \{x^{p^k} \mid x \in P\}, |P/\Omega_k(P)| = |\mho_k(P)|$

Theorem

If $[x, y]$ commutes with both x and y, then

- $[x^a, y] = [x, y]^a$
- $(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}$

Extraspecial-p group

Let P be an Extraspecial-p group,

- $(xy)^p = x^p y^p [y, x]^{\binom{p}{2}}$, therefore, P is regular if $p > 2$.
- P is of exponent p or P is of exponent p^2.
- $P/P' = P/\Phi(P)$ is elementary abelian
- $f : P/\Phi(P) \times P/\Phi(P) \longrightarrow Z(P)$, $f(\bar{x}, \bar{y}) = [x, y]$ is a symplectic form on $P/\Phi(P)$ if $p > 2$. • Therefore $|P/Z(P)| = p^{2m}$ for some integer m.
- If $p = 2$, $(xy)^2 = x^2 y^2 [y, x]$, $Q : P/\Phi(P) \longrightarrow Z(P)$, $\quad Q(x) = x^2$ is a quadratic form on $P/\Phi(P)$.

Minimal example of Extraspecial-p Groups

- $E(p^3) = p_+^{1+2} \cong (\mathbb{Z}/p\mathbb{Z})^2{:}(\mathbb{Z}/p\mathbb{Z})$
- $M(p^3) = p_-^{1+2} \cong (\mathbb{Z}/p^2\mathbb{Z}){:}(\mathbb{Z}/p\mathbb{Z})$
- $Q_8 = 2_-^{1+2} = \langle x, y \mid x^4 = e, x^2 = y^2, x^y = x^{-1} \rangle$
- $D_8 = 2_+^{1+2} = \langle x, y \mid x^4 = y^2 = e, x^y = x^{-1} \rangle$

Inner automorphism of Extraspecial-p group

Theorem

Let P be an extraspecial-p group and let $\sigma \in \mathrm{Aut}(P)$. If σ leaves every element of $P/Z(P)$ fixed, then $\sigma \in \mathrm{Inn}(P)$.

Proof.

Let $A = \{\sigma \in \mathrm{Aut}(P) \mid \sigma$ leaves every element of $P/Z(P)$ fixed$\}$

$\mathrm{Inn}(P) \subseteq A$ since $P/Z(P) \cong \mathrm{Inn}(P)$ is elementray - abelian.

On the otherhand, Let $\{x_1, \cdots x_n\}$ be a generator of P of minimal cardinality. $\bar{x}_1 \cdots \bar{x}_n$ is a basis of $P/Z(P) = P/\Phi(P)$

$\sigma \in A$ is determined by $x_1^\sigma, \cdots x_n^\sigma$. x_i^σ has p-choices,

Therefore, σ has $p^n = |P/Z(P)|$ choices. Hence

$|\mathrm{Inn}(P)| \leq |A| \leq |P/Z(P)| = |\mathrm{Inn}(P)|$ ------ $(*)$

In $(*)$ all "=" holds and hence $A = \mathrm{Inn}(P)$.

□

Corollary of Inner automorphism of extraspecial p-group

Theorem

Suppose $E \leq G$ and E is an extraspecial-p group, and $[E, G] \leq Z(E)$, then $G = E \circ C_G(E)$

Proof.

One notes that i $E \lhd G$
ii the action of G on E by conjugation is Inner automorphism.

□

Structure of Extraspecial-p group $p > 2$

Theorem

Let P be an extraspecial-p group of exponent p where $p > 2$, then

- *If P is of exponent p, then $P \cong E(p^3) \circ E(p^3) \circ \dots E(p^3) = p_+^{1+2m}$*
- *If P is of exponent p^2, then $P \cong M(p^3) \circ E(p^3) \circ \dots \circ E(p^3) = p_-^{1+2m}$*

Proof.

- the trick is to write P as $E \circ C_G(E)$.

We show the second one and the first one is easier.

Since P is regular. and It's easy that $\mho_1(P) = Z(P) \cong \mathbb{Z}/p\mathbb{Z}$ $|\Omega_1(P)| = |P/\mho_1(P)| = p^{2m}$ hence $\Omega_1(P)$ is not extraspecial.

Hence $Z(\Omega_1(P)) \neq Z(P)$

- take $x \in P$ such that $|\langle x \rangle| = p^2$
  take $y \in Z(\Omega_1(P)) \setminus Z(P)$ then $\Omega_1(P) \leq C_P(y) < P$ comparing the order, $\Omega_1(P) = C_P(y)$ and $x \notin \Omega_1(P) = C_P(y)$

Let $E = \langle x, y \rangle \cong M(p^3)$

$[E, P] \leq P' = Z(P) = Z(E)$ Hence $P = E \circ C_P(E)$

$Z(C_P(E)) \leq C_P(E) \cap C_P(C_P(E)) = C_P(E, C_P(E)) = Z(P)$

$1 < C_P(E)' \leq P' = Z(P)$ comparing the order $C_P(E)' = Z(P) = Z(C_P(E))$

Since $C_P(E)/C_P(E)' = C_P(E)/Z(P)$ is elementary abelian. $C_P(E)' = \Phi(C_P(E)) = Z(C_P(E))$

$C_P(E)$ is an extraspecial p-group, and $C_P(E) \leq C_P(y) = \Omega_1(P)$,

$C_P(E)$ is of exponential p.

□

Structure of Extraspecial 2-group

Let P be an extraspecial 2-group, then

- Either $P \cong D_8 \circ D_8 \circ \dots D_8 = 2_+^{1+2m}$
- Or $P \cong Q_8 \circ D_8 \circ \cdots \circ D_8 = 2_-^{1+2m}$

Proof.

- $Q_8 \circ Q_8 \cong D_8 \circ D_8 \not\cong D_8 \circ Q_8$

Let $(Q_8)_i = \langle x_i, y_i \rangle$, where $i \in \{1, 2\}$, $x_i^4 = e$, $x_i^2 = y_i^2$ $x_i^{y_i} = x_i^{-1}$

And $(D_8)_i = \langle x_i', y_i' \rangle$, where $i \in \{1, 2\}$ $(x_i')^4 = e$ $(y_i')^2 = e$ $(x_i')^{y_i'} = (x_i')^{-1}$

Let $\varphi: Q_8 \circ Q_8 \longrightarrow D_8 \circ D_8$

$(x_1, 1) \longrightarrow (x_1, 1)$

$(y_1, 1) \longrightarrow (y_1, x_2)$

$(1, x_2) \longrightarrow (1, x_2)$

$(1, y_2) \longrightarrow (x_1, y_2)$

Then φ induces an isomorphism from $Q_8 \circ Q_8$ to $D_8 \circ D_8$

By counting the number of eltments of order 4, one gets $Q_8 \circ Q_8 \not\cong D_8 \circ Q_8$

□

Let P be a symplectic-type p group, then P is a central product of E and S where

- E is trivial or E is an extraspecial p-group, and
- S is cyclic or isomorphic to D_{2^n}, Q_{2^n}, SD_{2^n}.
- If $p > 2$ then $\exp(E) = p$.

Proof.

(Only show the case $p > 2$) Still write P as $E \circ C_P(E)$

$Z(P')$ char P' char P and $Z(P')$ is cyclic, while $P' \leq \Phi(P)$ hence P' is cyclic and $p \geq 3$. therefore

P is regular and $\Omega_1(P) = \{x \in P \mid x^p = 1\}$.

Let $E = \Omega_1(P)$ E/E' is elementary abelian hence $\Phi(E) \leq E'$ and $\Phi(E) = E'$ $Z(E)$ is abelian $Z(E)$ char E char P therefore. $Z(E)$

is cyclic and $Z(E) \cong \mathbb{Z}/p\mathbb{Z}$ $Z(\Phi(E))$ char $\Phi(E)$ char E char P hence $Z(\Phi(E))$ is cyclic and hence $\Phi(E)$ is cyclic $\Phi(E) \cong \mathbb{Z}/p\mathbb{Z}$.

hence $E' = Z(E) = \Phi(E)$ is cyclic of order p. And hence E is extraspecial.

$P = E \circ C_P(E)$ Let $S = C_P(E)$ while $\Omega_1(S) \leq Z(E)$ is cyclic of order p.

Hence S is cyclic.

□

Structure of $\mathcal{C}_6$ subgroups

Kleidman-Liebeck p149("We will be concerned only with symplectic-type r-groups with minimal exponent")

structure	R,$\lvert Z(R)\rvert$	notation	$C_{Aut(R)}(Z(R))$
$E(r^3)\circ\cdots\circ E(r^3)$	r^{1+2m} ,r	r^{1+2m}	$r^{2m}.Sp_{2m}(r)$
$D_8\circ\cdots\circ D_8$	$2^{1+2m}, 2$	2_+^{1+2m}	$2^{2m}.O_{2m}^+(2)$
$D_8\circ\cdots\circ D_8\circ Q_8$	$2^{1+2m}, 2$	2_-^{1+2m}	$2^{2m}.O_{2m}^-(2)$
$\mathbb{Z}/4\mathbb{Z}\circ D_8\circ\ldots D_8$	$2^{1+2m}, 4$	$4\circ 2^{1+2m}$	$2^{2m}.Sp_{2m}(2)$

Automorphism of those groups above

Theorem

Automorphisms induced on $Z(R)$ Let R be an extraspecial r-group, $\mathrm{Aut}(R)$ induces full automorphism on $Z(R)$.

Proof.

Assume $Z(R) = \langle z \rangle$, take $\{x_1, y_1, x_2, y_2, \dots x_m, y_m\}$ to be a generator of R such that $[x_i, y_j] = e$ if $i \neq j$, $[x_i, y_i] = z, [x_i, x_j] = [y_i, y_j] = e$ for each $i, j \in [m]$. Let $\theta : R \longrightarrow R$ such that θ is defined by $(\theta(x_i), \theta(y_i)) = (x_i^s, y_i)$ where s is a generator of $\mathbb{F}_p^\times$, then $\langle \theta \rangle$ induces full automorphism on $Z(R)$. □

Theorem

Let $H \subseteq \mathrm{Aut}(R)$ be the set of automorphisms of R that induces trivial automorphism on $Z(R)$, that is $H = C_{\mathrm{Aut}(R)}(Z(R))$. Then $H \trianglelefteq \mathrm{Aut}(R)$ and $\mathrm{Aut}(R) = \langle \theta \rangle H$

We use the same notation $H = C_{\mathrm{Aut}(R)}(Z(R))$ as last page.

Theorem

Let R be an extraspecial r-group, then

- *If* $p > 2$, *then* $H/\operatorname{Inn}(R) \cong \mathrm{Sp}_{2m}(p)$
- *If* $R = 2_{+}^{1+2m}$, *then* $H/\operatorname{Inn}(R) \cong O_{2m}(2)^{+}$.
- *If* $R = 2_{-}^{1+2m}$, *then* $H/\operatorname{Inn}(R) \cong O_{2m}(2)^{-}$.

Proof.

In all cases, there is a symplectic or quadratic form on $R/Z(R)$, $\sigma \in H$ preserves those forms. Let $T \in \mathrm{Sp}_{2m}(r)$ (or $O_{2m}^{+}(2)$ or $O_{2m}^{-}(2)$), such that T induces $[t_{i,j}]$ on standard basis (with respect to that formed spaces). □

Proof.

Contiuning We take $\{x_1, x_2, x_3, y_4, \ldots x_{2m-1}, x_{2m}\}$ to be a generator of R such that $[x_i, x_j] = e$ and $[x_i, x_j] = z$ if and only if $(i, j) = (2k-1, 2k)$ for $k \in [m]$. (For 2_-^{1+2m}) we take another generator respectively.

- Let
$$\phi : R \longrightarrow R, \quad \prod_{i=1}^{2m} x_i^{a_i} z^c \mapsto \prod_{i=1}^{2m} (\prod_{j=1}^{2m} (x_j)^{t_{i,j}})^{a_i} z^c$$
- $\phi(x_i^{a_i}) = (\phi(x_i))^{a_i}$
-
$$\phi([\prod_{i=1}^{2m} x_i^{a_i}] z^c) = [\prod_{i=1}^{2m} \phi(x_i)^{a_i}] z^c$$
- $[\phi(x), \phi(y)] = [x, y]$ for all $x, y \in R$
- $\phi \in \mathrm{Aut}(P)$ if and only if $\phi(x_i^p) = x_i^p$ for each $i \in [2m]$

□

More about $C_{\mathrm{Aut}(R)}(Z(R))$

This is essential later since "$\overline{H} \cong C_{\mathrm{Aut}(R)}(Z(R))$ "Kleidman-Liebeck p151

- By previous page , $r > 2$ then $C_{\mathrm{Aut}(R)}(Z(R)) \cong r^{2m}.\mathrm{Sp}_{2m}(r)$
- Take $\phi \in C_{\mathrm{Aut}(R)}(Z(R))$ such that ϕ induce $-\mathcal{I}$ on $R/Z(R)$, Let $H_1 = C_{C_{\mathrm{Aut}(R)}(Z(R))}(\phi)$, then
- $H_1 \operatorname{Inn}(R)/\operatorname{Inn}(R) \cong \mathrm{Sp}_{2m}(r)$,
- $H_1 \cap \operatorname{Inn}(R) = e(\mathrm{Aut}(R))$.
- $\mathrm{Sp}_{2m}(r) \cong H_1 \operatorname{Inn}(R)/\operatorname{Inn}(R) \cong H_1/H_1 \cap \operatorname{Inn}(R) \cong H_1$.
- $C_{\mathrm{Aut}(R)}(Z(R)) = \operatorname{Inn}(R){:}H_1 \cong r^{2m}{:}\mathrm{Sp}_{2m}(r)$

Representation of those groups above

Theorem

Assume R is a symplectic-type r group of exponent $r(2,r)$ as in table above, and that $r \neq p$. Then

1. *R has precisely $|Z(R)| - 1$ inequivalent faithful absolutely irreducible representations over an algebraically closed field of characteristic p. Denote those representation by $\rho_1, \dots \rho_k$, $k = |Z(R)| - 1$.*
2. *The ρ_i are quasiequivalent of degree R^m, the smallest field over which they can be realized is $\mathbb{F}_{p^e}$, where e is the smallest integer for which $p^e \equiv 1 \pmod{|Z(R)|}$*
3. *If $i \neq j$, then ρ_i and ρ_j differ on $Z(R)$.*

Proof.

First representation over $\mathbb{C}$, then by $(|G|, p) = (r, p) = 1$ and ... □

Proof of Representations of R over $\mathbb{C}$

We only show the case when R is an extraspecial $-r$ group. Let $R \cong r^{1+2m}$

Since $|\mathrm{Inn}\, R| = |R/Z(R)|$ is just those automorphisms of R that leaves every points of $R/Z(R)$ fixed.

the orbits of $\mathrm{Inn}\, R$ = the conjugacy classes of R are: $\bigsqcup_{x \in Z(R)} x$, $\bigsqcup_{\bar{y} \in R/Z(R)}$ preimage of $\bar{y}$; $r + r^{2m} - 1 = r^{2m} + r - 1$ classes

Since $R/R' \cong r^{2m}$ there are r^{2m} linear characters.

Let $\tau_1, \cdots \tau_{r^{2m}}$ be the linear-characters of R and $\rho_1, \cdots \rho_{r-1}$ be the non-linear characters of R. Take $x \in R \setminus Z(R)$

By column-orthogonality we have

$$r^{2m} + \sum_{k=1}^{r-1} |\chi_{\rho_k}(x)|^2 = \sum_{i=1}^{r^{2m}} |\chi_{\tau_i}(x)|^2 + \sum_{k=1}^{r-1} |\chi_{\rho_k}(x)|^2 = |C_R(x)| \le r^{2m}$$

Therefore, we get $|C_R(x)| = r^{2m}$ and $\rho_i(x) = 0$ for each $i \in \{1, 2, \cdots r-1\}$

"ρ_i vanishes outside $Z(R)$" It's clear that $\rho_i|_{Z(R)} \cong \mathbb{Z}/r\mathbb{Z}$ are scalars, therefore, ρ_i $i \in \{1, \cdots r-1\}$ differs on $Z(R)$

- We then calculate the degree of ρ_i $i \in [r-1]$

By row-orthogonality

$$|R| = \sum_{x \in R} |\chi_{\rho_i}(x)|^2 = \sum_{x \in Z(R)} |\chi_{\rho_i}(x)|^2 = |\chi_{\rho_i}(e)|^2 \cdot r \Rightarrow \deg \rho_i = \chi_{\rho_i}(e) = r^m$$

(↑) this is because $\rho|_{Z(R)}$ are scalar matrices

- Construction of representations. Let $\omega = e^{\frac{2\pi i}{r}}$ ω is a primitive r-th root of unity over $\mathbb{C}$

$m = 1$ $\rho(R) = \langle x, y \rangle$ $x = \begin{bmatrix} 1 & & & \\ & \omega & & \\ & & \ddots & \\ & & & \omega^{r-1} \end{bmatrix}$ $y = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{bmatrix}$ $\rho(R) \le GL_r(\mathbb{C})$

Let $\rho(\underbrace{R \circ R \circ R \cdots \circ R}_{m \text{ ones}}) = \underbrace{\rho(R) \otimes \rho(R) \otimes \cdots \otimes \rho(R)}_{m \text{ ones}} \le \underbrace{GL_r(\mathbb{C}) \otimes \cdots \otimes GL_r(\mathbb{C})}_{m \text{ - ones}} \le GL_{r^m}(\mathbb{C})$.

Proof of Representations of R over a Finite field.

Structure of normalizer of R

Let π be an representation equivalent to ρ_1,
$N_{\mathrm{GL}(V)}(R\pi)/C_{\mathrm{GL}(V)}(R\pi) \lesssim \mathrm{Aut}(R)$, $C_{\mathrm{GL}(V)}(R\pi) \leq \mathrm{End}_{\mathbb{F}_{p^e}R}(V) = \mathbb{F}_{p^e}^{\times}$

$\pi : R \longrightarrow GL(V)$ — π induces an isomorphisms from $Aut(R)$ to $Aut(R\pi)$

$\pi^* : Aut(R) \xrightarrow{\sim} Aut(R\pi)$

$\beta \longrightarrow \pi \circ \beta \circ \pi^{-1}$

Let $R(R, V)$ be the set of embeddings of R to $GL(V)$ where $\dim(V) = r^m$

We show that $Aut(R)$ acts on $R(R,V)$

Let $Aut(R) \times R(R,V) \longrightarrow R(R,V)$

$(\beta, \pi) \longrightarrow \pi^\beta : R \to GL(V)$, $r \mapsto \pi(\beta r)$

the orbits of the actions of $Aut(R)$ are called the semi-equivalence class of representations of R

Since $Aut(R)$ induces the full-automorphisms on $Z(R)$ and $\rho_1, \dots, \rho_{r-1}$ differs on $Z(R)$

$Aut(R)$ acts transitively on the equivalence classes of representations of R

the stabilizer of a equivalence class say ρ_1 is.

Let π be a representation in the equivalence class ρ_1

Stabilizer of ρ_1: $\{\beta \mid \pi^\beta \sim \pi\}$

$= (\pi^*)^{-1}\left(N_{GL(V)}(R)/C_{GL(V)}(R)\right)$

↑ this is because they are induced by conjugation of Normalizer of $R\pi$ in $Aut(R\pi)$.

On the other hand, $\{\beta \mid \pi^\beta \sim \pi\}$ are those automorphisms of R that leaves every element of $Z(R)$ fixed since ρ_i $i \in \{1, \cdots, r-1\}$ differs on $Z(R)$

Hence $\{\beta \mid \pi^\beta \sim \pi\} = C_{Z(R)}(Aut(R))$

and $N_{GL(V)}(R)/C_{GL(V)}(R) \cong C_{Z(R)}(Aut(R))$

References

David Smith 1972
The Automorphism Group Of An Extraspecial p-group
JORNAL OF MATHEMATICS

M.Aschbacher
Finite Group Theory

M. Aschbacher
On the maximal subgroups of the finite classical groups
Inventiones mathematicae 76,469-514

Peter Kleidman, Martin Liebeck
The subgroup structure of the classical groups