FINITE p-SUBGROUPS OF $Sp(n)$

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF
MASTER OF SCIENCE
IN
MATHEMATICS

By
Mustafa Seyyid ÇETİN
September 2021

Finite p-subgroups of $Sp(n)$
x By Mustafa Seyyid ÇETİN
September 2021

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Özgün ÜNLÜ(Advisor)

Müfit SEZER

Şükran GÜL ERDEM

Approved for the Graduate School of Engineering and Science:

Ezhan Karaşan
Director of the Graduate School

ABSTRACT

FINITE p-SUBGROUPS OF $Sp(n)$

Mustafa Seyyid ÇETİN
M.S. in MATHEMATICS
Advisor: Özgün ÜNLÜ
September 2021

Hikari [1] classifies all finite p-subgroups of simple algebras, and Banieqbal [2] classifies the finite subgroups of 2×2 matrices over a division algebra of characteristic zero. In this thesis, we give a new proof for the classification of the finite p-subgroups of 2×2 matrices over the quaternionic algebra. Using this classification, we classify finite p-subgroups of the symplectic group $Sp(2)$. More precisely, for every prime p, we define a denumerable family of p-subgroups of $Sp(2)$ so that every finite p-subgroup of $Sp(2)$ lives inside one of the members of this family. To give this classification, we proved general results for $Sp(n)$ whenever possible.

Keywords: p-group, symplectic group.

ÖZET

$Sp(n)$ İÇİNDEKİ SONLU p-ALTGRUPLAR

Mustafa Seyyid ÇETİN
Matematik, Yüksek Lisans
Tez Danışmanı: Özgün ÜNLÜ
Eylül 2021

Hikari [1] basit cebirlerin tüm sonlu p-altgruplarını sınıflandırır ve Banieqbal [2] 2×2 matrislerinin sonlu altgruplarını karakteristiği sıfır olan bir bölme cebiri üzerinde sınıflandırır. Bu tezde, 2×2 matrislerin sonlu p-altgruplarını kuaterniyonik cebir üzerinden sınıflandırmak için yeni bir kanıt veriyoruz. Bu sınıflandırmayı kullanarak, $Sp(2)$ simplektik grubunun sonlu p-altgruplarını sınıflandıracağız. Daha doğrusu, her asal p için, $Sp(2)$'nin sayılabilir bir p-altgrupları ailesi tanımlarız, böylece $Sp(2)$'nin her sonlu p-altgrubu bu ailenin üyelerinden birinin içinde yaşar. Mümkün olduğu durumlarda $Sp(n)$ için genel sonuçlar kanıtlayarak bu özel sınıflandırmayı verdik.

Anahtar sözcükler: p-grup, simplektik grup.

Acknowledgement

I am grateful to my advisor, Özgün ÜNLÜ, for his patience, help and the many ways he has shown. I would like to thank to Müfit SEZER and Şükran GÜL ERDEM for accept to be my jury. I would like to give special thanks to my Bilkent graduate friends who did not spare their help in this process and my family, who always supported me.

Contents

Chapter 1

Introduction

Representation theory helps to see all finite groups as a subgroup of a matrix group so that finite groups can be studied much better by linear methods. Hence it is crucial to understand the finite subgroups of matrix algebras. Here the matrix group means the multiplicative group of matrix ring, i.e., the group of all invertible $n \times n$ matrices. To clarify, we first introduce the matrix ring over a ring. Most of the time, this ring will be the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$ or the Hamiltonian quaternions $\mathbb{H}$. Let R be a ring. Firstly, $Mat_n(R)$ denotes all $n \times n$ matrices over R and we define $GL_n(R)$ as the general linear group, which is the group of $n \times n$ invertible matrices over a ring R. In this group, there are basic subgroups, and we define some of them now. The special linear group $SL_n(R)$ is the $n \times n$ matrices whose determinant is 1 over a ring R. This group is also a normal subgroup of $GL_n(R)$ because it is the kernel of the determinant as a group homomorphism from $GL_n(R)$ to the multiplicative group of R.

On the real number matrix ring, the orthogonal group $O(n)$ defines the subgroup of $GL_n(\mathbb{R})$ where the transpose of the elements is equal to its inverse. Here the determinant of the orthogonal matrices can be 1 or -1, so we also define the special orthogonal group $SO(n)$ as the group of orthogonal matrices with determinant 1. In $GL_n(\mathbb{C})$, a matrix called unitary if its conjugate transpose is its inverse, and the unitary group $U(n)$ is the group of all unitary matrices. The special unitary group $SU(n)$ is the subgroup of the unitary group with determinant 1. Finally, we define the symplectic group $Sp(n)$ in quaternion matrix ring $GL_n(\mathbb{H})$ with the property $A^*A = I_n$ where $A^* = [a_{ij}]^* = [\overline{a}_{ji}]$ for any matrix $A = [a_{ij}]$ of $Sp(n)$.

Felix Klein [3] firstly started to study the finite subgroups of $SL_n(\mathbb{C})$ by making the relation between geometry and group theory. He classified the finite subgroup of the special linear group for 2×2 matrices over $\mathbb{C}$. Finite subgroups of classical groups have been studied by many authors, and here we give two more examples of such studies.

As an example of finite subgroups of these matrix groups with real entries, we can take the well-known example $SO(3)$, called the rotation group in three dimensions. Artin [4] gives this example in his book, but Armstrong shows this more explicitly in his book [5] by using orbit-stabilizer and counting theorem. It turns out that the conjugacy classes of finite subgroups of $SO(3)$ is equivalent the triples (x, y, z) with $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} > 1$ where $x, y, z \in \mathbb{Z}^+$. Hence, the classification of the finite subgroup of $SO(3)$ has three types: a cyclic group, a dihedral group, and the rotational symmetry group of regular solids. To state clearly, we can think of the cyclic group as a rotation by multiplies of $2\pi/n$ about a line and the dihedral group as symmetries of a regular n-gon with n arbitrary. Also, this includes the rotational symmetry of tetrahedron, octahedron and icosahedron.

In the complex matrix ring, we can give another example: the finite subgroups of SU(2). Klein [3] and Artin [4] show the strong relation between $SU(2)$ and $SO(3)$.

Here Klein proves the important theorem related between $SU(2)$ and $SO(3)$ that there is a double cover from $SU(2)$ to $SO(3)$, i.e., surjective map where the preimage of each element has order 2. Therefore we can find the finite subgroups of $SU(2)$ using the relation with $SO(3)$. Besides, we can consider $\mathbb{S}^3$ as the multiplicative subgroup of quaternions $\mathbb{H}$ that consists of elements whose product of its conjugate is 1. There is an isomorphism showed in, for example, Serrano's paper [6] between $SU(2)$ and $\mathbb{S}^3$. Amitsur [7] classifies the finite subgroups embeddable in a division ring and hence it classifies all subgroups of $\mathbb{S}^3$. Both of these methods show that the subgroups of $SU(2)$ can be listed as follows: a cyclic group, quaternion group Q_8, binary dihedral groups with order $2(n-2)$ where $n \geq 5$ and the binary groups of tetrahedral, octahedral or icosahedral groups.

All finite subgroup of $SU(2)$ freely act on $\mathbb{S}^3$ since $SU(2)$ is isomorphic to $\mathbb{S}^3$. Furthermore, Milnor [8] studied the finite group acting on $\mathbb{S}^n$ without fixed points, and he classifies all finite groups acting on $\mathbb{S}^3$ as the trivial group, the quaternion group of order 8n, the octahedral and icosahedral group and also, $D_{2^n(2k+1)} =< a, b : a^{2^n} = 1, b^{2k+1} = 1, ab = b^{-1}a >$ where $2 \leq n, 1 \leq k$, $P'_{8.3^n} =< a, b, c : a^2 = (ab)^2 = b^2, ca = bc, cb = abc, c^{3^n} = 1 >$ where $1 \leq n$ and the groups of direct product of $P \times \prod G_\alpha$ where G_α is one of above groups and C is cyclic with $(ord(G_\alpha), ord(C)) = 1$.

In this thesis, we classify all finite p-subgroups of $Sp(2)$. For p odd, a finite p-subgroup of $Sp(2)$ is isomorphic to a subgroup of $C_{p^n} \times C_{p^n}$ for some natural number n. For $p = 2$, every finite p-subgroup of $Sp(2)$ is a subgroup of a semidirect product of the direct product of two generalized quaternion 2-groups of order 2^n and the cyclic group of order 2 for some natural number n (i.e., a split extension of $Q_{2^n} \times Q_{2^n}$ by $\mathbb{Z}_2$ as $(Q_{2^n} \times Q_{2^n}) \rtimes \mathbb{Z}_2$).

Chapter 2

Preliminaries in Group Theory

We give some definition and notation in group theory which will be used later.

Let G be a finite group, then the *normalizer* in G of $X \subset G$ is defined as

$$N_G(X) = \{g \in G : g^{-1}xg \in X \text{ for all } x \in X\}$$

and the *centralizer* in G of X is

$$C_G(X) = \{g \in G : xg = gx \text{ for all } x \in G\}$$

We denote $\mathrm{Aut}(G)$ as the set of all automorphism of a group G. A *characteristic* subgroup in a group G is an $\mathrm{Aut}(G)$-invariant subgroup of G where we consider the natural action of $\mathrm{Aut}(G)$ on G. If H is a characteristic subgroup of G, then we write H char G.

We also define the rank of a group G by

$rank(G) := min\{r :$ there exist an elementary abelian subgroup of G whose rank is r$\}$.

Let P be a partially ordered set(poset) with respect to $\leq$. Then an *ascending chain* in P is the infinite sequence $a_1, a_2, ...,$ of element of P such that

$$a_1 \leq a_2 \leq ... \leq a_n \leq ...$$

and an *descending chain* in P is the infinite sequence $a_1, a_2, ...,$ of element of P such that

$$a_1 \geq a_2 \geq ... \geq a_n \geq ...$$

We say P satisfies the *ascending chain condition ACC* (respectively *descending chain condition DCC*) if every ascending (descending) sequence eventually stabilizes, i.e., there exist $n \in \mathbb{Z}$ such that $a_n = a_{n+1} = ...$

When we think the subgroup relation, any group G becomes a set of subgroups of poset. Hence if a group G satisfies the ACC, then we said G is a *noetherian* group, and if it satisfies the DCC, we said G is an *artinian*.

Let n be in $\mathbb{Z}$. If a group G has a finite series of subgroups $H_0, H_1, ..., H_n$ such that $1 = H_0 \lhd H_1 \lhd H_2 \lhd ... \lhd H_{n-1} \lhd H_n = G$ (without equality) where each subgroup is maximal normal in the next, or equivalently, the factor groups $H_1/H_0, H_2/H_1, ..., H_n/H_{n-1}$ are simple, then this series is called a *composition series* and these factors are called *composition factors*. Also, n is the *length of this composition series*.

Given groups N and H, a group G is called an *extension* of H by N if there is a short exact sequence

$$0 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 0.$$

It means there is a monomorphism $i : N \to G$ and an epimorphism $\pi : G \to H$ such that $Im(i) = Ker(\pi)$. Therefore, if G is an extension of H by N, $i(N)$ is a normal subgroup of G, and the quotient group $G/i(N)$ is isomorphic to the group H.

Let p be a prime, G be a finite p-group and $n \in \mathbb{Z}^+$, then

$$\Omega_n(G) :=< x \in G : x^{p^n} = 1 >$$

and

$$\mho^n(G) :=< x^{p^n} : x \in G >$$

Now we also give some finite groups with their presentations which we use in this paper later:

The *cyclic group* with order n considered here the rotation naturally with the generator $2\pi/n$ rotation:

$$C_n :=< g : g^n = 1 > \ \textit{where } 1 \textit{ is the group identity}$$

The *dihedral group* with order $2n$ is the group of the rotation and reflection of regular n-gon.

$$D_{2n} :=< g, h : g^n = h^2 = 1, gh = h^{-1}g^{-1} >$$

Besides these group, we give the presentation of another group which is the *generalized quaternion 2-group* with order 2^n:

$$Q_{2^n} :=< g, h : g^{2^{n-1}} = h^4 = 1,\ g^{2^{n-2}} = h^2,\ gh = hg^{-1} >$$

.

For $n \geq 4$, the *semidihedral* group with order 2^n denoted by SD_{2^n} is defined by

$$SD_{2^n} :=< g, h : g^{2^{n-1}} = h^2 = 1, hgh = g^{2^{n-2}-1} >$$

.

The *elementary abelian* group with order p^n denoted by E_{p^n} is defined by

$$E_{p^n} :=< x_1, x_2, ..., x_n : x_1^p = x_2^p = ... = x_n^p = 1,\ x_i x_j = x_j x_i \text{ for all i,j} >$$

The *modular* $p-group\ Mod_{p^n}$ of order p^n is the split extension of $C_{p^{n-1}} =< g >$ by a subgroup $H =< h >$ of order p with $h^{-1}gh = g^{p^{n-2}+1}$

$$Mod_{p^n} :=< g, h : g^{p^{n-1}} = 1, h^p = 1, h^{-1}gh = g^{p^{n-2}+1} >$$

We start with the set of matrices. Let n be a positive integer then we will denote $Mat_n(R)$ the set of all $n \times n$ matrices with entries in a ring R and a matrix A in $Mat_n(R)$ will be represented as $[a_{ij}]$ such that $a_{ij} \in R$ where i,j are positive integers between 1 and n. $Mat_n(R)$ is a ring, and we are interested in the multiplicative group of this ring and subgroups. The multiplicative group of the matrix ring is called the matrix group.

Now we give some definitions of the classical lie groups. For more information, you can see Baker's book "Matrix groups"[9].

We define the *general linear group* in $Mat_n(R)$ where any element has a multiplicative inverse, equivalently, the determinant of any element is not equal to 0 and it denotes by

$$Mat_n(R)^{\times} = GL_n(R) := \{A \in Mat_n(R) : detA \neq 0\}$$

and the *special linear group* define as the set of n×n matrices with determinant 1 and we will show by

$$SL_n(R) := \{A \in Mat_n(R) : detA = 1\}.$$

Here we generally interest in the real number $\mathbb{R}$ or the complex number $\mathbb{C}$ fields, the quaternion number $\mathbb{H}$ as the ring.

On the real matrix ring, the *orthogonal group* includes the element $A = [a_{ij}]$ with the property $A^t A = I_n$ where $A^t = [a_{ij}]^t := [a_{ji}]$ is the transpose of A. We will denote by

$$O(n) := \{A \in Mat_n(\mathbb{R}) : A^t A = I_n\}$$

and the *special orthogonal group* is

$$SO(n) := \{A \in O(n) : detA = 1\}$$

For the orthogonality on $Mat_n(\mathbb{C})$ (respectively $Mat_n(\mathbb{H})$), we use the conjugation on $\mathbb{C}$ (respectively $\mathbb{H}$) with the transpose of matrix. On the matrix ring over $\mathbb{C}$ (respectively $\mathbb{H}$), we define the conjugation transpose of matrix $A = [a_{ij}]$ as $A^* = [a_{ij}]^* = [\overline{a}_{ij}]^t = [\overline{a}_{ji}]$. Besides, we also define the standard hermitian(respectively quaternionic) inner product by this conjugation on $\mathbb{C}^n$ (respectively $\mathbb{H}^n$) by

$$< v, w >= v^* w = \sum_{i=1}^{n} \overline{v}_i w_i, \qquad where \;\; v = [v_i], w = [w_i] \in \mathbb{C}^n (\text{respectively } \mathbb{H}^n)$$

In general, we can define a hermitian inner product as a function $<,>: V \times V \to \mathbb{C}$ on a vector space V over $\mathbb{C}$ with the following conditions:
1)$< u + v, w >=< u, w > + < v, w >$
2)$< u, v + w >=< u, v > + < u, w >$
3)$< u\lambda, v >= \overline{\lambda} < u, v >$
4)$< u, v\lambda >=< u, v > \lambda$
5)$< u, v >= \overline{< v, u >}$
6)$< u, u > \geq 0$
7)$< u, u >= 0 \iff u = 0$
for all $u, v, w \in V$ and $\lambda \in \mathbb{C}$

The conjugate transpose also gives the subgroups of matrix group: The *unitary group* in $Mat_n(\mathbb{C})$ is

$$U(n) := \{A \in Mat_n(\mathbb{C}) : A^* A = I_n\}$$

and the *special unitary group* is

$$SU(n) := \{A \in U(n) : detA = 1\}.$$

The *symplectic group* in $Mat_n(\mathbb{H})$ is

$$Sp(n) := \{A \in Mat_n(\mathbb{H}) : A^*A = I_n\}.$$

Let R be a ring, then R^n is an R-module. When R is a division ring, it becomes vector space (see [10]). Matrix ring over R always act naturally on R^n, and these matrix groups have geometric inspiration. Geometrically the action of the orthogonal groups preserves the distance, inner and dot product,and this is another way to define equivalently, so, in particular, these matrices include rotation, reflection and their combination. Hence we can think of the finite rotation and reflection groups in orthogonal groups.

Chapter 3

Preliminaries of Module and Representation Theory

In this thesis, we only consider fields characteristic zero.

Given an F-vector space and a ring R, then we say R is an *algebra* over F if it satisfies the condition

$$\lambda.(ab) = (\lambda.a)b = a(\lambda.b) \; for \; all \; \lambda \in F, \; a, b \in R$$

A *division algebra* D is an algebra (over a field F) where all non-zero elements of D are invertible.

Let R be an algebra over a field F. A non-zero R-module V is called *simple* (or *irreducible*) if V does not have any R-submodules except for 0 and V. An F-algebra R is called semisimple if it is the direct sum of simple submodules, that is, there exist simple submodules S_i, for $i \in I$ an index set, such that $R = \bigoplus_{i \in I} S_i$.

When we think the submodule relation, the set of submodules of a module V becomes poset. Hence if a module V satisfies the ACC, then we said V is *noetherian*, and if it satisfies the DCC, we said V is *artinian*.

Let n be in $\mathbb{Z}$. If a module V has a finite series of submodules $M_0, M_1, ..., M_n$ such that $1 = M_0 < M_1 < M_2 < ... < M_{n-1} < M_n = V$ (without equality) where each subgroup is maximal submodule in the next, or equivalently, the factor groups $M_1/M_0, M_2/M_1, ..., M_n/M_{n-1}$ are simple, then this series is called a *composition series* and these factors are called $composition\ factors$. Also, n is the $length\ of\ this\ composition\ series$.

Let A and B be vector spaces over a field F with bases $a_1, a_2, ..., a_m$ and $b_1, b_2, ..., b_n$, respectively. Now we define $A \otimes_F B$ as the mn-dimensional vector space over F with a basis the set of $a_i \otimes_F b_j$ where $i \in 1, ..., m$ and $j \in 1, ..., n$. For any $a \in A$ and $b \in B$ with $a = \sum_{i=1}^{m} \lambda_i a_i$ and $b = \sum_{j=1}^{n} \gamma_j a_j$ where $\lambda_i, \gamma_j \in F$ for each i, j , the product is defined by

$$a \otimes_F b = \sum_{i,j} \lambda_i \gamma_j (a_i \otimes_F b_j)$$

Let V be an n-dimensional vector space over a division algebra D with a chosen basis. A *representation* of a group G is a homomorphism ρ from G to $Mat_n(D)$ and the *character* of the representation is the trace of the matrix representation. Here, G can act on D-module V with $g.v := \rho(g)v$ for all $g \in G$ and $v \in V$. We can also similarly define *irreducible* representation as an irreducible G-invariant module. A $faithful$ representation is an injective representation. Also, if a module V cannot be written as the direct sum of some of its submodules permuted by G, then we say this module and representation is *primitive*. Otherwise V is called *imprimitive*.

Let $Rep(G, K)$ denote the set of all representations of G on K-vector space where $K = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$. If $\rho \in Rep(G, \mathbb{H})$ can be seen also in $Rep(G, \mathbb{C})$ or $Rep(G, \mathbb{R})$

(similarly complex representation can be seen as real representation) so we can define the restriction maps by

$$r^{\mathbb{H}}_{\mathbb{C}} : Rep(G, \mathbb{H}) \to Rep(G, \mathbb{C})$$

$$r^{\mathbb{H}}_{\mathbb{R}} : Rep(G, \mathbb{H}) \to Rep(G, \mathbb{R})$$

$$r^{\mathbb{C}}_{\mathbb{R}} : Rep(G, \mathbb{C}) \to Rep(G, \mathbb{R})$$

And also, we define the extension maps

$$e^{\mathbb{H}}_{\mathbb{C}} : Rep(G, \mathbb{C}) \to Rep(G, \mathbb{H}) \text{ by } U \mapsto \mathbb{H} \otimes_{\mathbb{C}} U$$

$$e^{\mathbb{H}}_{\mathbb{R}} : Rep(G, \mathbb{R}) \to Rep(G, \mathbb{H}) \text{ by } U \mapsto \mathbb{H} \otimes_{\mathbb{R}} U$$

$$e^{\mathbb{C}}_{\mathbb{R}} : Rep(G, \mathbb{R}) \to Rep(G, \mathbb{C}) \text{ by } U \mapsto \mathbb{C} \otimes_{\mathbb{R}} U$$

$Irr(G, K)$ denotes the set of all irreducible G-invariant modules over K.

Let V be a finite-dimensional left vector space over $\mathbb{C}$ and ρ be a representation of G on V. Then
i) if V has a map conjugate-linear G-map $f : V \to V$ with $f^2 = 1$ then ρ is called to be of real type
ii) if V has a map conjugate-linear G-map $f : V \to V$ with$f^2 = -1$ then ρ is called to be of quaternionic type
iii) if ρ is neither real nor quaternionic type, then ρ is called to be of complex type

Now, we give more specific definitions on $Irr(G, K)$ which denoted by $Irr(G, K)_L$ where L and K are one of $\mathbb{H}$, $\mathbb{C}$ and $\mathbb{R}$:

$$U \in Irr(G, \mathbb{H})_{\mathbb{H}} :\Longleftrightarrow (\exists V \text{ of quaternionic type, } V = r^{\mathbb{H}}_{\mathbb{C}}(U))$$

$$U \in Irr(G, \mathbb{H})_{\mathbb{C}} :\Longleftrightarrow (\exists V, V \ncong \overline{V} \text{ and } U = e^{\mathbb{H}}_{\mathbb{C}}(V))$$

$$U \in Irr(G, \mathbb{H})_{\mathbb{R}} :\Longleftrightarrow (\exists V \text{ of real type, } U = e^{\mathbb{H}}_{\mathbb{C}}(V))$$

$$U \in Irr(G,\mathbb{C})_{\mathbb{H}} :\Longleftrightarrow U \text{ is of quaternionic type}$$

$$U \in Irr(G,\mathbb{C})_{\mathbb{C}} :\Longleftrightarrow U \ncong \bar{U}$$

$$U \in Irr(G,\mathbb{C})_{\mathbb{R}} :\Longleftrightarrow U \text{ is of real type}$$

$$U \in Irr(G,\mathbb{R})_{\mathbb{H}} :\Longleftrightarrow (\exists V \text{ of quaternionic type, } U = r_{\mathbb{R}}^{\mathbb{C}}(V))$$

$$U \in Irr(G,\mathbb{R})_{\mathbb{C}} :\Longleftrightarrow (\exists V, V \ncong \bar{V} \text{ and } U = r_{\mathbb{R}}^{\mathbb{C}}(V))$$

$$U \in Irr(G,\mathbb{R})_{\mathbb{R}} :\Longleftrightarrow (\exists V \text{ of real type, } V = e_{\mathbb{R}}^{\mathbb{C}}(U))$$

Let $(R,+,.)$ be a ring. An element e of R is called *idempotent* if it satisfies that $e^2 = e$. The idempotent elements e and f are called *orthogonal* if $ef = fe = 0$. And if the idempotent belongs to the center of the ring then, it is called central idempotent.

Let A be an F-algebra, then the *Jacobson radical* $J(A)$ is the intersection of all maximal left ideals of A.

Here are the main theorems on semisimplicity:

Theorem 3.0.1. *(Artin-Weddernburn) Let A a semisimple F-algebra where F is a field. Then*

$$A \cong Mat_{n_1}(D_1) \times ... \times Mat_{n_r}(D_r)$$

for some division algebras D_i over F where n_i's are in $\mathbb{Z}^+$ for all $1 \leq i \leq n$ and r is the number of simple A-submodules.

Theorem 3.0.2. *(Maschke's theorem) Let F be a field and G a finite group. Then the characteristic of F does not divide the order of G if and only if the group algebra FG is semisimple.*

Chapter 4

Some known result about the classification of finite p-subgroups of $Mat_2(\mathbb{H})$

Definition 4.0.1. Let $P_0 =< g >$ be a cyclic group with an order p. Let P, P' be finite p-groups and $P'_1, P'_2, ..., P'_p$ be equal to P'. If P is an extension of $P'_1 \times P'_2 \times ... \times P'_p$ by P_0 such that $P'^g_1 = P'_2$,...,$P'^g_{p-1} = P'_p$, $P'^g_p = P'_1$, then we will say P is a *simple* (1-$fold$) $p-extension$ of P'. We also call P an n-fold p-extension of a finite p-group P', if there exist finite p-groups, $P_0 = P'$, P_1, ..., P_{n-1}, $P_n = P$ where P_{i+1} is a simple p-extension of P_i for all $0 \leq i \leq n-1$

We also define

$$T_p^{(0)} = \begin{Bmatrix} \{all\ generalized\ quaternion\ 2-groups\},\ if\ p = 2 \\ \{all\ cyclic\ p-groups\},\ otherwise \end{Bmatrix}$$

and an element of $T_p^{(0)}$ is called a p-group of 0-type. When a finite p-group P is an

n-fold p-extension of a p-group of 0-type, we will call P is n-type. $T_p^{(n)}$ is also defined as the set of all p-groups of n-type.

The following theorem is the main theorem from Hikari's paper on the Multiplicative p-subgroup of simple algebras.

Theorem 4.0.2. *[1] Let n be a fixed positive integer and let P be a finite p-group. Then following conditions are equivalent:*
1) P is a subgroup of $Mat_n(\mathbb{H})^\times$
2) There is a division algebra D such that $P \subset Mat_n(D)^\times$
3) There exist non-negative integers, t, m_0, ..., m_t with $\sum_{i=0}^{t} p^i m_i \leq n$ and $P_i^{(1)}, ..., P_i^{(m_i)} \in T_p^{(i)}$ for each $0 \leq i \leq t$ such that $P \subset \prod_{i=0}^{t} \prod_{j=1}^{m_i} P_i^{(j)}$.

For 2-groups, we consider $T_2^{(0)}$ as the set of all generalized quaternion 2-groups. Also, when we look at 2-groups in $Mat_2(\mathbb{H})^\times$, the third condition has only three possibilities with $2^0.m_0 + 2^1.m_1 \leq 2$
1) $m_0 = 1$ and $m_1 = 0$ then $P \subset P_0^{(1)}$ for $P_0^{(1)} \in T_2^{(0)}$
2) $m_0 = 2$ and $m_1 = 0$ then $P \subset P_0^{(1)} \times P_0^{(2)}$ for $P_0^1, P_0^{(2)} \in T_2^{(0)}$
3) $m_0 = 0$ and $m_1 = 1$ then $P \subset P_1^{(1)}$ for $P_1^{(1)} \in T_2^{(1)}$

Here the condition 2 includes condition 1, so we only consider conditions 2 and 3. Hence we can rewrite Hikari's theorem when $p = n = 2$;

Theorem 4.0.3. *Let P be a finite 2-group. Then following conditions are equivalent:*
1) P is a subgroup of $Mat_2(\mathbb{H})^\times$
2) There is a division algebra D such that $P \subset Mat_2(D)^\times$
3) P is the subgroup of the direct product of two generalized quaternion 2-groups or 1-fold 2-extension of a generalized quaternion 2-group.

For p-groups when p is odd, we consider $T_p^{(0)}$ as the set of all cyclic p-groups. When we consider p-groups in $Mat_2(\mathbb{H})^\times$, we only have two possibilities for the

third condition with $p^0.m_0 \leq 2$
1) $m_0 = 1$ then $P \subset P_0^{(1)}$ for $P_0^{(1)} \in T_p^{(0)}$
2) $m_0 = 2$ then $P \subset P_0^{(1)} \times P_0^{(2)}$ for $P_0^1, P_0^{(2)} \in T_p^{(0)}$

Similarly, condition 2 includes condition 1, so we can conclude that:

Theorem 4.0.4. *Let p is odd prime and P be a finite p-group. Then following conditions are equivalent:*
1) P is a subgroup of $Mat_2(\mathbb{H})^\times$
2) There is a division algebra D such that $P \subset Mat_2(D)^\times$
3) P is the subgroup of the direct product of two cyclic p-groups.

Chapter 5

Finite p-subgroups of $Sp(2)$ when p is odd

Theorem 5.0.1. *Given a finite group G and an injective group homomorphism from G to $Mat_n(\mathbb{H})^\times$, there exists an injective group homomorphism from G to $Sp(n)$.*

Proof. Assume that $\alpha : G \to Mat_n(\mathbb{H})^\times$ is an injective group homomorphism. Then this induces a G-action on $\mathbb{H}^n$ as follows $G \times \mathbb{H}^n \to \mathbb{H}^n$ with $(g, x) \mapsto \alpha(g)(x)$ Define a new quaternion Hermition inner product with the usual Quaternion Hermitian inner product

$$< ., . >_m : \mathbb{H}^n \times \mathbb{H}^n \to \mathbb{H}^n \text{ as follows } < x, y >_m = \frac{1}{|G|} \sum_{g \in G} < gx, gy >$$

Let $\{w_1, w_2, ..., w_n\}$ be a orthonormal basis with respect to the new inner product. Define $P = [w_1, w_2, ..., w_n]$ then

$$\frac{1}{|G|} \sum_{g \in G} P^* g^* g P = I, \text{ so } \quad \frac{1}{|G|} \sum_{g \in G} g^* g = (P^*)^{-1} P^{-1}$$

Hence

$$(P^{-1}g_0P)^*(P^{-1}g_0P) = P^*g_0^*(P^{-1})^*P^{-1}g_0P = \star$$
$$\star = P^*g_0^*(P^*)^{-1}P^{-1}g_0P = P^*g_0^*\frac{1}{|G|}\sum_{g\in G} g^*gg_0P$$

then we get

$$\star = \frac{1}{|G|}\sum_{g\in G} P^*(gg_0)^*(gg_0)P = \frac{1}{|G|}\sum_{g\in G} P^*g^*gP = I$$

Then the G-action now with this new inner product induces $G \to Sp(n)$ which is injective because it is just a conjugate.

□

Theorem 5.0.2. *Let R be a ring with $1 \neq 0$. There is a one-to-one correspondence between the following sets:*
i) $\{\{I_1, I_2, ..., I_n\} : R = I_1 \oplus I_2 \oplus ... \oplus I_n$ is a decomposition of R as a direct sum of left ideals $\}$
ii) $\{\{e_1, e_2, ..., e_n\} : e_1, e_2, ...e_n$ are orthogonal idempotents of R such that $e_1 + e_2 + ... + e_n = 1_R\}$
given by the equality $I_i = Re_i$.

Proof. Let $e_1, e_2, ..., e_n$ are orthogonal idempotents, then Re_i is a left ideal. Since $1_R = e_1+e_2+...+e_n$, we get $R = \sum_{i=1}^{n} I_i$. And also, let us take $x \in Re_1\cap(Re_2+...+Re_n)$, then $x = r_1e_1$ for some $r_1 \in R$ and $x = r_2e_2 + ... + r_ne_n$. We get $x = r_1e_1 = r_1e_1^2 = r_2e_2e_1+...+r_ne_ne_1 = 0$ from the orthogonality of $\{x_i\}$. Hence $Re_1\cap(Re_2+...+Re_n) = 0$ and it is also true for all i such that $Re_i \cap (Re_2 + ... + Re_{i-1} + Re_{i+1} + ... + Re_n) = 0$ so $R = \bigoplus_{i=1}^{n} I_i$.

Conversely, given $R = I_1 \oplus I_2 \oplus ... \oplus I_n$ where I_i is a left ideal, we have $1_R = \sum_{i=1}^{n} x_i$ where $x_i \in I_i$. Since R is the direct sum of I_i and $x_ix_j \in I_j$ then $x_i.x_j = 0$ for all i,j

$(i \neq j)$ so x_i's are orthogonal. Since $x_i.x_j = 0$ and $x_i = x_i.1 = \sum_{j=1}^{n} x_i x_j = x_i^2$ for all i then the x_i are orthogonal idempotents. $\square$

Theorem 5.0.3. *If D is a division algebra, then $Mat_n(D)$ is artinian and semisimple.*

Proof. Let $M = Mat_n(D)$. Let i be an integer between 1 and n, and let e_i be the matrix with (i,i) entry is 1_D otherwise 0. Me_i is a left ideal. Here Me_i is a minimal nonzero left ideal and left M-module. To show minimality, if we get any element me_i of Me_i where $m \in M$ then me_i is equal to the matrix with (i,i) entry $a \in D$ otherwise 0. Here if we multiply me_i with the matrix with (i,i) entry is a^{-1}, we get $e_i \in Me_i$ again, so Me_i is minimal ideal. Define $M_0 = 0$ and $M_i = Me_1 + Me_2 + ... + Me_i$ for $1 \leq i$, then $M_i/M_{i-1} \cong Me_i$. Therefore, we get $0 = M_0 \subset M_1 \subset ... \subset M_n = M$, so M has a composition series then M is artinian. For semisimplicity, we use that the artinian ring where the Jacobson radical is zero is semisimple (see Theorem 5.4 page 452 in [10]) . So the Matrix ring is semisimple. $\square$

Theorem 5.0.4. *Let R be a ring with $1 \neq 0$ and S a left-artinian and semisimple ring. Assume that $f : R \to S$ is a unitary ring homomorphism and $1_R = e_1 + e_2 + ... + e_n$ where $e_1, e_2, ..., e_n$ are orthogonal idempotents. Then*

$$|\{i | f(e_i) \neq 0\}| \leq \textit{composition length of } S.$$

Proof. Say $\{i|f(e_i) \neq 0\} = \{i_1, i_2, ..., i_r\}$. Then $1_S = f(e_{i_1}) + f(e_{i_2}) + ... + f(e_{i_r})$ Notice that for each j, $f(e_{i_j})$ is an orthogonal idempotent of S. Hence by Theorem 5.0.2 there exist left ideals $I_1, I_2, ..., I_r$ of S such that $S \cong I_1 \oplus I_2 \oplus ... \oplus I_r$. This means $0 \subseteq I_1 \subseteq I_1 \oplus I_2 \subseteq ... \subseteq I_1 \oplus I_2 \oplus ... \oplus I_r = S$ is a normal series of S. Hence we have $r \leq \textit{composition length of} S$. $\square$

Fact 5.0.5. Composition length of $Mat_n(\mathbb{H})$ is n.

Proof. Firstly, we can easily see that $\mathbb{H}^n$ is simple as a $Mat_n(\mathbb{H})$-module since we have $Mat_n(\mathbb{H}^n).v = \mathbb{H}^n$ for any nonzero element v of $\mathbb{H}^n$. Now, let $N_m := \{[a_{ij}] \in Mat_n(\mathbb{H});\ a_{ij} = 0 \text{ when } j \neq m\}$ for each $m \in 1, 2, ..., n$ then N_m is a $Mat_n(\mathbb{H})$-submodule and $N_m \cong \mathbb{H}^n$, so we can write $Mat_n(\mathbb{H})$ as a sum of these submodules, i.e., $Mat_n(\mathbb{H}) = N_1 \oplus N_2 \oplus ... \oplus N_n$. Then we can get this composition series:

$$0 \subset N_1 \subset N_1 \oplus N_2 \subset ... \subset N_1 \oplus ... \oplus N_n = Mat_n(\mathbb{H})$$

Hence the composition length is n. □

Fact 5.0.6. (2) A group homomorphism $\psi : G \to Mat_n(\mathbb{H})$ can be extended to a $\mathbb{Q} - algebra$ morphism $\mathbb{Q}G \to Mat_n(\mathbb{H})$ by sending $\sum\limits_{g\in G} c_g g \mapsto \sum\limits_{g\in G} c_g \psi(g)$

Theorem 5.0.7. *(Proposition 6.8 in Chapter 2 from Bröcker and Dieck's book [11]) Let G be a group and V be in Rep$(G, \mathbb{C})$ with character $\mathcal{X}_V : G \to \mathbb{C}$. Then*

$$\int \mathcal{X}_V(g^2)dg = \left\{\begin{matrix} 1 \Leftrightarrow V \ is\ of\ \ real\ type \\ 0 \Leftrightarrow V \ is\ of\ \ complex\ type \\ -1 \Leftrightarrow V \ is\ quaternionic\ type, \end{matrix}\right\}$$

Theorem 5.0.8. *(Proposition 6.6 in chapter 2 from Bröcker and Dieck's book [11])*

i) If $W \in Irr(G, \mathbb{H})_{\mathbb{R}}$ then $r^{\mathbb{H}}_{\mathbb{C}} W = V \oplus V$ for $V \in Irr(G, \mathbb{C})_{\mathbb{R}}$
ii) If $W \in Irr(G, \mathbb{H})_{\mathbb{C}}$ then $r^{\mathbb{H}}_{\mathbb{C}} W = V \oplus \overline{V}$ for $V \in Irr(G, \mathbb{C})_{\mathbb{C}}$
iii) If $W \in Irr(G, \mathbb{H})_{\mathbb{H}}$ then $r^{\mathbb{H}}_{\mathbb{C}} W = V$ for $V \in Irr(G, \mathbb{C})_{\mathbb{H}}$

Theorem 5.0.9. *Let G be a finite group. Assume that $|G|$ is odd. Then G is isomorphic to subgroup of $Sp(2)$ if and only if G is isomorphic to subgroup of $\mathbb{Z}_n \times \mathbb{Z}_n$ for some odd natural number n.*

Proof. (⇐) Let n be an odd number. Then

$$\mathbb{Z}_n \times \mathbb{Z}_n \cong < a, b : a^n = b^n = 1,\ ab = ba >$$

Define $\alpha : \mathbb{Z}_n \times \mathbb{Z}_n \to Sp(2)$ by $a \mapsto \begin{bmatrix} e^{\frac{2\pi i}{n}} & 0 \\ 0 & 1 \end{bmatrix}$ $b \mapsto \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{n}} \end{bmatrix}$ Notice that α is injective. So $\mathbb{Z}_n \times \mathbb{Z}_n$ is isomorphic to a subgroup of $Sp(2)$. Hence any subgroup of $\mathbb{Z}_n \times \mathbb{Z}_n$ is isomorphic to a subgroup of $Sp(2)$.

($\Rightarrow$) Now assume G is isomorphic to a subgroup of $Sp(2)$. Then there exist an injection $\alpha : G \to Mat_2(\mathbb{H})$. So we get a 2-dimensional quaternionic representation W of G. If W is not irreducible, then $G < \mathbb{H} \times \mathbb{H}$. Also notice that the group algebra $\mathbb{Q}E_{p^m}$ has the following orthogonal central primitive idempotent: $e_0 = \frac{1}{|G|} \sum\limits_{g \in E_{p^m}} g$, $e_H = \frac{1}{|G|} \sum\limits_{g \in E_{p^m}} c_{H,g} g$ where $c_{H,g} = \left\{ \begin{array}{l} \dfrac{-1}{|G|},\ if\ g \in H \\ \dfrac{p-1}{|G|},\ if\ g \in H \end{array} \right\}$ for $H \leq E_{p^m}$ with $|H| = p^{m-1}$. And notice that H acts trivially on e_H for all $H \leq E_{p^m}$ with $|H| = p^{m-1}$. Hence by Amitsur (Theorem 7 in [7]), G is abelian so by Theorem 5.0.4, $rank(G) \leq 2$. So by Fundamental theorem of abelian groups, $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$. Take $n = lcm(m_1, m_2)$. G is isomorphic to a subgroup of $\mathbb{Z}_n \times \mathbb{Z}_n$. If W is irreducible then by Theorem 5.0.8 (Proposition 6.6 in Bröcker and Dieck's book [11]), either $r_{\mathbb{C}}^{\mathbb{H}} W = V \oplus V$ or $r_{\mathbb{C}}^{\mathbb{H}} W = V \oplus \overline{V}$ or $r_{\mathbb{C}}^{\mathbb{H}} W = V$ for some V in $Irr(G, \mathbb{C})$ In either case, $dim(V)$ is even. This is impossible because the degree of an irreducible representation divides the order of a group.(See [12] and [13]). $\square$

Theorem 5.0.10. *If G is a p-subgroup of $Sp(2)$ and p is an odd prime, then G is isomorphic to a subgroup of $C_{p^n} \times C_{p^n}$ for some n in $\mathbb{N}$.*

Proof. Let G be p-subgroup of $Sp(2)$ and p be an odd prime. Then by Theorem 5.0.9, G is isomorphic to a subgroup of $C_m \times C_m$ for some natural number m. Define $n_0 = max\{n : p^n | m\}$ then G is isomorphic to a subgroup of $C_{p^{n_0}} \times C_{p^{n_0}}$. $\square$

Chapter 6

Classification of the Finite 2-Subgroups of $Sp(2)$

Theorem 6.0.1. *(see [14] and [15]) If a finite group G has a faithful, irreducible, primitive representation module over a field with characteristic zero, then G is isomorphic to one of the following groups:*
a) The cyclic group C_{p^m} where $m \geq 0$
b) The dihedral group D_{2^m} where $m \geq 4$
c) The semidihedral group SD_{2^m} where $m \geq 4$
d) The quaternion group Q_{2^m} where $m \geq 3$

Lemma 6.0.2. *If a finite group G has a faithful, irreducible, primitive representation module, then every abelian normal subgroup of G is cyclic.*

Proof. Assume M is a faithful, irreducible, primitive G-module. Let $N \trianglelefteq G$ so that N is abelian. Since $\mathbb{Q}N$ is a commutative semi-simple algebra, there exist a set of fields F such that $\mathbb{Q}N = \bigoplus_{K \in F} K$. Hence we have $M = \bigoplus_{K \in F} KM$. Notice that for each $K \in F$, KM is a left N-module and a right $End(M)$-module. Since $N \trianglelefteq G$, $\mathbb{Q}N$ is invariant under the G-action by conjugation, so G permutes the components of the direct sum $\mathbb{Q}N = \bigoplus\limits_{K \in F} K$ to each other. Since M is primitive, there exist K_0 in F such that $M = K_0 M$. Let π_0 denote the projection of $\mathbb{Q}N = \bigoplus\limits_{K \in F} K$ to K_0. We have $\forall n \in N$ $\pi_0(n) \neq 0$ because otherwise, the action of n on M is not invertible.

Since M is faithful otherwise, the action of n on M must be trivial.

Therefore π_0 sends the group N injectively into the multiplicative group of the field K_0. Hence N is cyclic. □

Lemma 6.0.3. *If every abelian normal subgroup of a p-group G is cyclic and G is not abelian, then G contains a cyclic normal subgroup U with $C_G(U) = U$.*

Proof. Assume that G is a p-group which is not abelian such that every abelian normal subgroup of G is cyclic. Then take a maximal normal cyclic subgroup M of G. Since G is not abelian $M \neq G$. So G/M is a nontrivial group. Now notice that M is normal in G and M is abelian so G/M acts by conjugation on M. Let K denote the kernel of this action. Assume $K = \overline{K}/M$ then $\overline{K} \neq M$. Notice $Z(K) \neq 1$ since K is a p-group so there exists $\overline{Z}$ such that $\overline{Z}/M = Z(K)$, $M \ntrianglelefteq \overline{Z} \trianglelefteq \overline{K} \trianglelefteq G$. Notice $\overline{Z}$ is abelian and $\overline{Z} \trianglelefteq G$ then $\overline{Z}$ is cyclic. This is contradiction. So $\overline{K} = M$ then $C_G(M) = M$. Hence we take $U = M$. □

Lemma 6.0.4. *(Aschbacher (23.5) [16]) Let G be a nonabelian p-group. Suppose that G contains such a normal subgroup U of order p^n such that U is cyclic and $C_G(U) = U$ then one of the followings is true:*
a) G is isomorphic to $D_{2^{n+1}}$, $Q_{2^{n+1}}$ or $SD_{2^{n+1}}$
b) $M = C_G(\mho_1(U)) = Mod_{p^{n+1}}$ and $E_{p^2} = \Omega_1(M) char\, G$

Proof. (of Theorem 6.0.1) By Lemma 1, Lemma 2 and the condition (23.5) from Aschbacher, we only have the cyclic group, the quaternion group Q_{2^m}, the dihedral group, and the semidihedral group SD_{2^m}. We do not consider part b in Aschbacher lemma. If every abelian normal subgroup of G is cyclic, then it is not a group that satisfies the condition (2) in (23,5) by Aschbacher because H char G is true and there is a subgroup H isomorphic to E_{p^2} in G. So $H \trianglelefteq G$ since every characteristic subgroup is also normal. But H is not cyclic. Also notice that we have $\mathbb{Q}D_8 = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus L$ where $L = \mathbb{Q}(i)[u : iu = -ui,\ u^2 = 1]$. Hence L acts nontrivially on an irreducible faithful representation of D_8. However, all irreducible faithful representations of D_8 on which L acts nontrivially are isomorphic to the representation given by the map $D_8 \to Mat_2(\mathbb{Q})$ where $h \mapsto \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $g \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Hence these representations are not primitive. □

Theorem 6.0.5. *(Banieqbal, Lemma 2, [2]) Let D be a division ring and let $G < Mat_2(D)^\times$ be finite. Assume that G is imprimitive then there exist $H \leq G$ with $[G : H] = 2$ and $N \trianglelefteq H$ with the property if $G = H \cup Hg$ for some $g \in G$ then $N \cap N^g = 1$, $[N : N^g] = 1$ and H/N maps injectively into D. Conversely, assume that the groups H and N exist as above and ρ be a representation of H on D with $ker(\rho) = N$. Then we define a representation of G in $Mat_2(D)$*

$$g \to \begin{bmatrix} 0 & \rho(g^2) \\ 1 & 0 \end{bmatrix}, \qquad h \to \begin{bmatrix} \rho(h) & 0 \\ 0 & \rho(g^{-1}hg) \end{bmatrix}$$

for $h \in H$ and this representation is a faithful.

Proof. $G < Mat_2(D)^\times$ is an imprimitive finite groups means there exist subspace W_1, W_2 of $D \oplus D$ such that $D \oplus D = W_1 \oplus W_2$ and G permutes W_1 and W_2. Let v_i be a vector that spans W_i then conjugate each element of G by the matrix $[v_1, v_2]$. Consider G as the new subgroup of $Mat_2(D)^\times$, then H is the kernel of the permutation action. Since G is irreducible $[G : H] = 2$. By the choice of v_1 and v_2, the group H is the diagonal matrices in $Mat_2(D)$. Also notice that the elements of N have the form $\begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix}$. □

Because of Theorem 6.0.5, it is important to understand the structure of 1-fold 2-extension of 2-group. Here, we give the theorem of the presentation of the extension from D. L. Johnson's book [17], so it helps to understand what kind of group we have.

Let N be a group with a presentation $< X : R >$ and let H be a group with presentation $< Y : S >$ where X, Y are the generator sets and R, S are the relation sets.

Let G be an extension of H by N then we have the short exact sequence

$$0 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 0$$

where i is a monomorphism and π is epimorphism with $Im(i) = Ker(\pi)$. Remember $Im(i) \trianglelefteq G$ since $ker(\pi) \trianglelefteq G$ and $G/im(i) \cong H$.

Firstly, since i is monomorphism, we can see the N as a subgroup of G. Now we define the set $\tilde{X} = \{\tilde{x} = i(x) : x \in X\}$ with the relation $\tilde{R} = \{\tilde{r} : r \in R\}$ which is the same relation just changing a element x of X with element $\tilde{x}$ of $\tilde{X}$.

Next, define $\tilde{Y} = \{\tilde{y} \mid y \in Y \; and \; v(\tilde{y}) = y\}$ and for each $s \in S$, let $\tilde{s}$ be the word in $\tilde{Y}$ obtained from s by replacing each y by $\tilde{y}$. Now annihilates each $\tilde{s}$, and so far $s \in S$, $\tilde{s} \in Ker \; v = Im \; i$ and since $Im \; i$ is generated by the set $\tilde{Y}$, each $\tilde{s}$ can be written as a word - say v_s- in the $\tilde{y}$. Then let

$$\tilde{S} = \{\tilde{s}v_s^{-1} | s \in S\}.$$

And also, since $Imi \trianglelefteq G$, each conjugate $\tilde{y}^{-1}\tilde{x}\tilde{y}$, $\tilde{y} \in \tilde{Y}$, $\tilde{x} \in \tilde{X}$, belongs to Imi, and so is a word -$w_{x,y}$- in the $\tilde{x}$. Putting

$$\tilde{T} = \tilde{y}^{-1}\tilde{x}\tilde{y}w_{x,y}^{-1} : x \in X, y \in Y$$

Theorem 6.0.6. *[17] [page 138-139, Proposition 1]*

$\tilde{G}$ *can be presented by* $< \tilde{X}, \tilde{Y} : \tilde{R}, \tilde{S}, \tilde{T} >$.

Now we are back to 1-fold 2-extension of a generalized quaternion 2-group.

$$Q_{2^n} =< x, y : x^{2^{n-1}} = y^4 = 1, x^{2^{n-2}} = y^2, y^{-1}xy = x^{-1} >$$

$$A = Q_{2^n} \times Q_{2^n} = \left\langle x_1, y_1, x_2, y_2 : \begin{array}{c} x_1^{2^{n-1}} = y_1^4 = 1,\ x_1^{2^{n-2}} = y_1^2,\ y_1^{-1}x_1y_1 = x_1^{-1}, \\ x_2^{2^{n-1}} = y_2^4 = 1,\ x_2^{2^{n-2}} = y_2^2,\ y_2^{-1}x_2y_2 = x_2^{-1}, \\ x_1x_2 = x_2x_1,\ x_2y_1 = y_1x_2, \\ x_1y_2 = y_2x_1,\ y_1y_2 = y_2y_1 \end{array} \right\rangle$$

$$G = \mathbb{Z}_2 =< t : t^2 = 1 >$$

Assume $1 \to A \xrightarrow{i} \tilde{G} \xrightarrow{v} G \to 1$ is a group extension such that the action of G on A is given by $A \times G \to G$ where $(x_1, t) \mapsto x_2$, $(y_1, t) \mapsto y_2$, $(x_2, t) \mapsto x_1$, $(y_2, t) \mapsto y_1$

Lemma 6.0.7. $\tilde{G} \cong A \rtimes G$

Proof. Now, let $\tilde{x}_i = i(x_i)$ and $\tilde{y}_i = i(y_i)$ and $\tilde{t} \in \tilde{G}$ such that $v(\tilde{t}) = t$. Then v_{t^2} is a word in $\tilde{x}_1, \tilde{x}_2, \tilde{y}_1, \tilde{y}_2$ such that $\tilde{t}^2 = v_{t^2}$. Notice v_{t^2} is in $Z(i(A))$ and $\tilde{t}v_{t^2} = v_{t^2}\tilde{t}$, so $v_{t^2} = y_1^2y_2^2$ or $v_{t^2} = 1$. In case $v_{t^2} = 1$ we are done because $v_{t^2} = 1$ means $\tilde{G} = A \rtimes G$. In case $v_{t^2} = y_1^2y_2^2$. We have an isomorphism as follows

$$\psi : A \rtimes G \to \tilde{G}$$

by $x_1 \mapsto x_1$, $y_1 \mapsto y_1$, $x_2 \mapsto x_2^{-1}$, $y_2 \mapsto y_2$, $\tilde{t} \mapsto \tilde{t}y_1y_2$

□

Notice that $A \rtimes G \cong (Q_{2^n} \times Q_{2^n}) \rtimes_\varphi C_2$ where $\varphi : C_2 \to \mathrm{Aut}(Q_{2^n} \times Q_{2^n})$ is defined by $\alpha(t)(a,b) = (b,a)$. Let say $A \rtimes G := \Gamma_n$. We have $Q_{2^n} \times 1 =< x_1, y_1 >$, in other words, the group generated by x_1, y_1 and we also have $1 \times Q_{2^n} =< x_2, y_2 >$, in other words, the group generated by x_2, y_2.

Theorem 6.0.8. *If G is a 2-subgroup of $Sp(2)$, then G is isomorphic to a subgroup of Γ_n for some n in $\mathbb{N}$.*

Proof. i) Case G is a primitive subgroup of $Sp(2)$. By Theorem 6.0.1, G is isomorphic to C_{2^m}, Q_{2^m}, D_{2^m} or SD_{2^m} for some m.
C_{2^m} is isomorphic to $< x_1 >$ in Γ_{m+1}
Q_{2^m} is isomorphic to $< x_1, y_1 >$ in Γ_m
D_{2^m} is isomorphic to $< x_1 x_2^{-1}, t >$ in Γ_m
SD_{2^m} is isomorphic to $< x_1 x_2^{2^{m-1}}, t >$ in Γ_m

ii) Case G is an imprimitive subgroup of $Sp(2)$. Then by Theorem 6.0.5, we have an extension $1 \to \underbrace{N \times N}_{=H} \to G \to \underbrace{G/H}_{=C_2} \to 1$, $G = H \cup gH$ and $N < \mathbb{H}$. So $N < Q_{2^m}$ for some m. Hence proof is done by Lemma 6.0.7. $\square$

Bibliography

[1] M. Hikari, “Multiplicative P-subgroups of simple algebras,” *Osaka Math. J.*, vol. 10, pp. 369–374, 1973.

[2] B. Banieqbal, “Classification of finite subgroups of 2×2 matrices over a division algebra of characteristic zero,” *J. Algebra*, vol. 119, no. 2, pp. 449–512, 1988.

[3] F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade.* Birkhäuser Verlag, Basel; B. G. Teubner, Stuttgart, 1993. Reprint of the 1884 original, Edited, with an introduction and commentary by Peter Slodowy.

[4] M. Artin, *Algebra.* Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[5] M. A. Armstrong, *Groups and symmetry.* Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1988.

[6] J. C. Serrano, “Finite subgroups of $sl(2, \mathbf{C})$ and $sl(3, \mathbf{C})$,” 2014.

[7] S. A. Amitsur, “Finite subgroups of division rings,” *Trans. Amer. Math. Soc.*, vol. 80, pp. 361–386, 1955.

[8] J. Milnor, “Groups which act on S^n without fixed points,” *Amer. J. Math.*, vol. 79, pp. 623–630, 1957.

[9] A. Baker, *Matrix groups*. Springer Undergraduate Mathematics Series, Springer-Verlag London, Ltd., London, 2002. An introduction to Lie group theory.

[10] T. W. Hungerford, *Algebra*, vol. 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[11] T. Bröcker and T. tom Dieck, *Representations of compact Lie groups*, vol. 98 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1985.

[12] W. Fulton and J. Harris, *Representation theory*, vol. 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[13] J.-P. Serre, *Linear representations of finite groups*. Graduate Texts in Mathematics, Vol. 42, Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott.

[14] L. Barker, "Genotypes of irreducible representations of finite p-groups," *J. Algebra*, vol. 306, no. 2, pp. 655–681, 2006.

[15] P. Roquette, "Realisierung von Darstellungen endlicher nilpotenter Gruppen," *Arch. Math. (Basel)*, vol. 9, pp. 241–250, 1958.

[16] M. Aschbacher, *Finite group theory*, vol. 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second ed., 2000.

[17] D. L. Johnson, *Presentations of groups*, vol. 15 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, second ed., 1997.