Two Generation of The Classical Groups

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Yash Arora

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

May, 2019

Supervisor: Dr. Anupam Kumar Singh

Certificate

This is to certify that this dissertation entitled Two Generation of The Classical Groups towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Yash Arora at Indian Institute of Science Education and Research under the supervision of Dr. Anupam Kumar Singh, Associate Professor, Department of Mathematics , during the academic year 2018-2019.

Dr. Anupam Kumar Singh

Committee:

Dr. Anupam Kumar Singh

Dr. Supriya Pisolkar

This thesis is dedicated to My Grandmother.

Declaration

I hereby declare that the matter embodied in the report entitled Two Generation of The Classical Groups are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Dr. Anupam Kumar Singh and the same has not been submitted elsewhere for any other degree.

yash arora

Yash Arora

Acknowledgments

First of all, I thank my thesis supervisor, Dr. Anupam Kumar Singh for his support and motivation throughout this project. He encouraged me a lot during this project. I would like to thank my thesis advisory committee member Dr. Supriya Pisolkar for her valuable discussions with me which helped me to solve some problems which I was facing in my project. I would also like to thank Dr. Dilpreet Kaur for her support.

I would like to thank Dr.Kaneenika Sinha, I did my first summer project under her guidance and learnt how to present my work. I am grateful to the Department of Science and Technology for giving me INSPIRE research fellowship.

I would also like to thank the mathematics department of IISER PUNE for their continuous support. I am grateful to the Institute and their non-Teaching staff for their support.

At the last, but not least, I would like to thank my parents, my grandmother for their unconditional support and motivation to me.

Abstract

In this thesis, we study the two generation problem for special linear groups and symplectic groups. Let k denote a finite field of characteristic not equal to 2 and $\mathbb{Z}$ denote the ring of rational integers. In this thesis, we study that special linear groups $SL_n(k)$ and symplectic groups $Sp_{2n}(k)$ defined over k, are generated by two elements. We study that special linear groups $SL_n(\mathbb{Z})$ defined over $\mathbb{Z}$, are generated by two elements.

Contents

Introduction

Classical groups are defined as certain subgroups of matrix groups. In this thesis, we study the two generation problem of classical groups. In particular, the two generation of the special linear groups and symplectic groups. The elementary matrices of special linear groups and symplectic groups are helpful in solving two generation problem for these groups.

Groups defined by generators and relations

A group can be defined in many different ways, one of the ways is to define a group by its generators and relations. Generators of a group are those elements of the group which will generate the group which means that every element of the group can be written as a product of powers of these generators and relations are defined among these generators. Defining a group by its generators and relations is called Presentation of a group.

In general, a presentation $P =< T \mid R >$, contains a set T which is called generators and a set R of words on the set T which are called relators. A word defined on a set T has the form $b_1^{r_1} b_2^{r_2} .....b_i^{r_i}$, where $r_i \in \mathbb{Z}$ and $b_i \in T$. A group can be defined by the presentation P. For example a cyclic group of finite order n can be defined as follows:

$$G =< g \mid g^n = 1 >$$

where the set $\{g\}$ is the set of generator for G and $g^n = 1$ is the defined relation.

The two generation problem for finite simple groups

Generation of a group by two elements is called two generation of a group. If we classify all the finite simple groups then they are isomorphic to one of the following groups:

- Cyclic group of prime order
- Alternating group A_n, where $n \geq 5$
- Groups of Lie type
- One of 26 sporadic groups

Groups of Lie type are subgroups of matrix groups when matrices are defined over a finite field $\mathbb{F}_q$. Examples of groups of Lie type are : Projective Special linear groups $PSL_n(\mathbb{F}_q)$, Projective Symplectic groups $PSp_{2n}(\mathbb{F}_q)$, which we define in the chapter 1. In [6] , Guralnick, Kantor, Kassabov and Lubotzky proved the following result about two generation of simple groups of Lie type:

Theorem 0.0.1. *[6, Guralnick] All non abelian finite simple groups of Lie type, except the Ree groups, are two generated with at most* 80 *relations.*

In [14] , R. Steinberg proved that the groups $PSL_n(\mathbb{F}_q), PSp_{2n}(\mathbb{F}_q)$ can be generated by two elements. In this thesis, we study two generation for $SL_n(\mathbb{F}_q)$ and $Sp_{2n}(\mathbb{F}_q)$. In [11] , Macbeath proved that the group $PSL_2(\mathbb{F}_q)$ is two-generated for certain values of q.

Now, we discuss the significance of the two-generation problem in computational group theory. Computational group theory is the study of groups through computers, it is used to gather information about groups. There are a lot of groups of large orders for which we can't do the calculations by hand, so to study them we have to use computers. So, if we can generate these groups by just two elements and some relations then it is very easy to study these groups using computers.

Two generation problem for some groups

If a group is generated by an element of order 2 and an element of order 3 , then this generation of the group is called $(2,3)$-generation. Besides the two generation of the finite simple groups , in [13], M.A.Pellegrini proved that the group $SL_{12}(\mathbb{F}_q)$ is $(2,3)$-generated. Now we also find some examples of two generation , where the matrices are not defined on a finite field. In [5] , Gow, Tamburini proved that the special linear groups $SL_n(\mathbb{Z})$ defined over the ring of rational integers $\mathbb{Z}$ are generated by a unipotent matrix and its transpose. This gives us the two generation of $SL_n(\mathbb{Z})$.

A Chapter-wise description

- In chapter 1, we define classical groups, and give some examples of classical groups and classical simple groups.
- In chapter 2, we give brief survey of results in the area of two generations of classical groups.
- In chapter 3, we study the two generation of $SL_n(\mathbb{F}_q)$ from the paper of Steinberg ([14]).
- In chapter 4, we study the two generation of the group $SL_n(\mathbb{Z})$ from the paper of Gow, Tamburini ([5]).
- In chapter 5, from the paper of Bhunia, Ayan Mahalanobis, Pralhad Shinde and Anupam Singh ([1]), and Steinberg ([14]), we study the two generation of the symplectic groups using the elementary matrices of the group.

In [14], Steinberg proved the two generation for all finite simple groups of Lie type. In the thesis we study the two generation of special linear groups and symplectic groups.

Chapter 1

Classical Groups

In this chapter we define classical groups, discuss examples of classical groups and related definitions to these groups and further properties.

1.1 Bilinear Forms and Classical Groups

Definition 1.1.1. ***Bilinear Forms :*** *Let V be a d dimensional vector space over a finite field k. A map*

$$\beta : V \times V \to k$$

is called bilinear form if it satisfies

1. $\beta(v_1 + sv_2, v_3) = \beta(v_1, v_3) + s\beta(v_2, v_3)$
2. $\beta(v_1, v_2 + sv_3) = \beta(v_1, v_2) + s\beta(v_1, v_3)$

for all $v_1, v_2, v_3 \in V$ and $s \in k$.

Definition 1.1.2. ***Matrix associated to a bilinear form:*** *If we fix a basis of a vector space V over k then for any bilinear form, we define a matrix associated to it. Let $dim(V) = d$ and $\{u_1, u_2, ...u_d\}$ be the basis of V then matrix associated to a bilinear form β is $B = [(\beta(u_i, u_j))]$.*

Definition 1.1.3. ***Symmetric bilinear form:*** *A bilinear form β is called symmetric if $\beta(v_1, v_2) = \beta(v_2, v_1)$ for all $v_1, v_2 \in V$. In this case if we fix a basis of V then matrix B associated to the symmetric bilinear form β satisfies $B^\intercal = B$, where $B^\intercal$ denotes the transpose of matrix B.*

Definition 1.1.4. ***Skew symmetric bilinear form:*** *A Bilinear form β is called skew symmetric if $\beta(v_1, v_2) = -\beta(v_2, v_1)$ for all $v_1, v_2 \in V$. In this case if we fix a basis of V then matrix B associated to this skew symmetric bilinear form β satisfies $B^\intercal = -B$, where $B^\intercal$ matrix is the transpose matrix of B.*

Definition 1.1.5. ***Non-degenerate bilinear form:*** *A bilinear form β is called Non-degenerate bilinear form if its associated matrix B has non-zero determinant.*

Definition 1.1.6. ***Degenerate bilinear form:*** *A bilinear form β is called Degenerate bilinear form if determinant of associated matrix B is equal to zero.*

Definition 1.1.7. ***Classical Group:*** *Let V be a finite dimensional vector space defined over the field of real numbers $\mathbb{R}$, or the field of complex numbers $\mathbb{C}$. A classical group is a group which preserves a bilinear form defined over vector space V.*

Now let β be a non-degenerate bilinear form defined on a vector space V, and M is the matrix associated to the bilinear form β, then the Classical group G is defined as follows:

$$G := \left\{ A \in M_n(k) \;\mid\; A^\intercal M A = M \right\}$$

where $M_n(k)$ denotes the set of $n \times n$ invertible matrices defined over finite field k.

1.2 Examples of Classical Groups

Let k be a finite field with $char(k) \neq 2$. The following groups are some examples of classical groups.

Definition 1.2.1. ***General Linear Group*** $GL_n(k)$***:*** *The set of $n \times n$ invertible matrices $M_n(k)$ forms a group under the operation of matrix multiplication. This group is called General Linear group $GL_n(k)$. This means if $A \in GL_n(k)$ then $det(A) \neq 0$.*

Definition 1.2.2. ***Special Linear Group*** $SL_n(k)$: *Special Linear Group* $SL_n(k)$ *is a subgroup of* $GL_n(k)$ *which contains all* $n \times n$ *invertible matrices which have determinant equal to 1.*

$$SL_n(k) := \{A \in GL_n(k) \mid det(A) = 1\}$$

$SL_n(k)$ is a normal Subgroup of $GL_n(k)$. As $\forall M \in GL_n(k), \forall N \in SL_n(k)$ we can see that $det(MNM^{-1}) = det(M)det(N)det(M^{-1}) = det(M)det(N)det(M)^{-1} = det(N) = 1$. This shows that $MNM^{-1} \in SL_n(k)$.

Definition 1.2.3. ***Symplectic Group*** $Sp_n(k)$***:*** *Let* B *be a matrix associated to the non-degenerate skew-symmetric bilinear form* β*. A matrix* $A \in GL_n(k)$ *is called symplectic matrix if* $A^\intercal BA = B$*. The group formed by symplectic matrices is called symplectic Group.*

Definition 1.2.4. ***Orthogonal Group*** $O_n(k)$***:*** *Let* B *be a matrix associated to the non-degenerate symmetric bilinear form* β*. A matrix* $A \in Gl_n(k)$ *is called Orthogonal if* $A^\intercal BA = B$*. The group formed by orthogonal matrices is called orthogonal group.*

One can see that if $A \in O_n(k)$ then $det(A) = \pm 1$.

Definition 1.2.5. ***Special Orthogonal Group*** $SO_n(k)$***:*** *The subgroup of Orthogonal Group* $O_n(k)$ *containing matrices of determinant* 1 *is called special orthogonal group. The group* $SO_n(k)$ *is a normal subgroup of* $O_n(k)$*.*

1.3 Classical Simple Groups

Definition 1.3.1. ***Commutator:*** *Let* $A, B \in GL_n(k)$*, then commutator of* A *and* B *is defined as follows:* $[A, B] = A^{-1}B^{-1}AB$*.*

Definition 1.3.2. ***Simple Group:*** *A group which has no non-trivial normal subgroup is called a simple group.*

Definition 1.3.3. ***Centre of a Group:*** *Centre of a group* G*, is the subgroup of* G *which is defined as follows:*

$$\mathscr{Z}(G) = \{z \in G \mid \forall\ g \in G\ ;\ zg = gz\}$$

Now following are some examples of Classical Simple Groups:

Definition 1.3.4. ***Projective Special Linear Group*** $PSL_n(k)$***:*** *The Quotient group* $SL_n(k)/\mathscr{Z}(SL_n(k))$ *is known as Projective special linear Group* $PSL_n(k)$*, where* $\mathscr{Z}(SL_n(k))$ *is the centre of the Special Linear Group* $SL_n(k)$*.*

Projective special linear Group $PSL_n(k)$ is a simple group for $n \geq 2$ except for the groups $PSL_2(\mathbb{F}_2)$ and $PSL_2(\mathbb{F}_3)$.

Definition 1.3.5. ***Projective Symplectic Group*** $PSp_n(k)$***:*** *The Quotient group* $Sp_n(k)/\mathscr{Z}(Sp_n(k))$ *is known as Projective symplectic group* $PSp_n(k)$*, where* $\mathscr{Z}(Sp_n(k))$ *is the centre of the symplectic group* $Sp_n(k)$*.*

Projective Symplectic Group $PSp_n(k)$ are simple groups except for the groups $PSp_2(\mathbb{F}_2)$, $PSp_2(\mathbb{F}_3)$ and $PSp_4(\mathbb{F}_2)$.

Definition 1.3.6. ***Commutator Subgroup of Orthogonal Group*** $\Omega_n(k)$***:*** *The Commutator Subgroup of Orthogonal Group* $\Omega_n(k)$ *is simply defined as* $\Omega_n(k) = [O_n(k), O_n(k)]$*.*

Now the corresponding projective group $P\Omega_n(k)$ are usually simple groups.

Chapter 2

History of The Problem

The main problem we are studying is Two generation of classical groups. If a group can be generated by 2 elements, then the group is called two generated and this generation of the group is known as Two-generation.

The aim of this chapter is to give a brief survey of results in the area of two generation of classical groups.

Notation: In this chapter, we denote $q = p^n$, where p is a prime number and $n \in \mathbb{N}$.

- $\mathbb{F}_q$: Finite field containing q elements.
- $\mathbb{F}_q^*$: Multiplicative group of the finite field $\mathbb{F}_q$.

2.1 Two generation of finite simple group of Lie type

Groups of Lie type are the subgroups of general linear groups when matrices are taken over a finite field $\mathbb{F}_q$. Example of Groups of Lie type are $PSL_n(\mathbb{F}_q), PSp_{2n}(\mathbb{F}_q)$, and $PSU_n(\mathbb{F}_q)$ etc.

In [6], Guralnick, Kantor, Kassabov, and Lubotzky proved the following result about finite simple groups of Lie type :

Theorem 2.1.1. *[6, Theorem A] All non abelian finite simple groups of Lie type, except the Ree groups are two generated with at most* 80 *relations.*

2.2 Two generation of Symmetric Group

Definition 2.2.1. ***Permutation:*** *A permutation is a bijective map from a set to itself.*

Example 1. *We take a set containing* 3 *elements namely* $\{1, 2, 3\}$ *then all the permutations on this set are:* $(1), (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)$.

Example 2. *For a set containing* n *elements has* $n!$ *number of permutations.*

Definition 2.2.2. ***Symmetric Group :*** *Let* X *be a set. The group of all the permutations of set* X *is called symmetric group. If* $|X| = n$ *then* $|S_n| = n!$*, where* S_n *denotes symmetric group defined on the set* X*.*

Now onwards, S_n denotes the symmetric group of degree n.

Definition 2.2.3. ***Cycle :*** *A cycle of length* k *is a permutation in* S_n *which permutes* k *elements cyclically, where* $2 \leq k \leq n$.

Example 3. *Permutation* $(1, 2, 3)$ *in* S_n*, is a cycle of length* 3.

Definition 2.2.4. ***Transposition:*** *In the symmetric group* S_n*, a transposition is a cycle of length* 2.

Definition 2.2.5. ***Even Permutation :*** *An even permutation is a permutation in* S_n*, which is product of even number of transpositions.*

Example 4. $(1, 2, 3) = (1, 3)(1, 2)$*, so* $(1, 2, 3)$ *is an even permutation.*

Definition 2.2.6. ***Odd Permutation :*** *An odd permutation is a permutation in* S_n*, which is product of odd number of transpositions.*

Example 5. $(1, 2, 3, 4) = (1, 4)(1, 3)(1, 2)$*, so* $(1, 2, 3, 4)$ *is an odd permutation.*

Now, we study two generation of the symmetric Group ([3]).

Theorem 2.2.1. *[3, Theorem 2.5] Let S_n be a symmetric group defined on the finite set containing n elements and the 2-cycle $(1,2)$ and the n-cycle $(1,2,.....,n) \in S_n$. Then S_n is generated by cycles $(1,2)$ and $(1,2,....,n)$.*

Proof. We know that all the permutations in S_n are product of disjoint cycles. Let $(v_1, v_2, ...v_j)$ be a cycle in S_n of length j , then we can write $(v_1, v_2, ...v_j) = (v_1, v_j)(v_1, v_{j-1})......(v_1, v_2)$. This gives that every element of S_n is product of transpositions.

Now take any arbitrary transposition (i, j) in S_n. Now we prove that S_n can be generated by the set $\{(1,2),(2,3),.....(n-1,n)\}$. To prove this we will use induction on the difference between i and j , where $1 \leq i \neq j \leq n$. We consider $j - i = 1$, then $(i, j) = (i, i+1)$, which proves the statement. Now assume it's true for $j - i = k - 1$. We further consider the case when $j - i = k$, then $(i, j) = ((i+1, i)(i+1, j)(i, i+1)$, as $j - i = k$, we have $j - (i+1) = k - 1$, by induction hypothesis, we get $(i+1, j)$ can be written in product of elements of type $(u, u+1)$, Therefore from induction we proved that S_n can be generated by the set $\{(1,2),(2,3),.....(n-1,n)\}$. We know that , if we have a cycle $(u_1, u_2, ...u_j)$ and an arbitrary permutation τ in S_n, then we have $\tau(u_1, u_2, ...u_j)\tau^{-1} = (\tau(u_1), \tau(u_2), ...\tau(u_j))$.

Let $\tau = (1, 2, ..., n)$ then

$$\tau(1,2)\tau^{-1} = (\tau(1), \tau(2)) = (2,3)$$

so now take $r = 1, 2, ..., n-2$ then,

$$\tau^r(1,2)\tau^{-r} = (\tau^r(1), \tau^r(2)) = (r+1, r+2)$$

This proves that the symmetric group S_n is generated by the 2-cycle $(1,2)$ and the n-cycle $(1,2,...,n)$. □

2.3 Two generation of Special Linear Group

In this section we will provide some results of two-generation of Special Linear group:

2.3.1 $(2,3)$- generation of the group $SL_{12}(\mathbb{F}_q)$

Definition 2.3.1. $(2,3)$***-generation of a group:*** *A group is called* $(2,3)$*-generated if it is generated by an element of order 2 and an element of order 3.*

In [13], Marco Antonio Pellegrini proved the following result:

Theorem 2.3.1. *[13, Prop 2.3, Corollary 2.5] For a prime number* p *and* $n \in \mathbb{N}$*, the group* $SL_{12}(\mathbb{F}_{p^n})$ *is* $(2,3)$*-generated.*

Let V be a 12-dimensional vector space over $\mathbb{F}_q$, we consider the standard basis $\mathscr{B} = \{u_1, u_2, ..., u_{12}\}$ of V over $\mathbb{F}_q$. To give sketch of proof of Theorem 2.2.1 , we define Alternating group.

Definition 2.3.2. ***Alternating Group:*** *The group of even permutations of a finite set, is known as Alternating group.*

Let $Alt(\mathscr{B})$ be Alternating group defined on the set $\mathscr{B}$. We know that the matrix τ corresponding to an element in $Alt(\mathscr{B})$ has determinant equal to 1, so we get that $Alt(\mathscr{B}) \leqslant SL_{12}(\mathbb{F}_q)$.

We define $\omega = (u_1, u_2, u_3)(u_4, u_5, u_6)(u_7, u_8, u_9)(u_{10}, u_{11}, u_{12}) \in Alt(\mathscr{B}) \leqslant SL_{12}(\mathbb{F}_q)$, then we compute that $\omega^2 = (u_1, u_3, u_2)(u_4, u_6, u_5)(u_7, u_9, u_8)(u_{10}, u_{12}, u_{11})$ and $\omega^3 = (u_1) \implies \omega$ is an element of order 3. If $p \neq 5$, then we define a matrix ϕ of $SL_{12}(\mathbb{F}_q)$ with respect to the basis $\mathscr{B}$ as following:

- $\phi u_1 = u_8, \phi u_8 = u_1, \phi u_2 = -u_2, \phi u_5 = u_5$
- $\phi u_3 = u_4, \phi u_6 = u_7, \phi u_4 = u_3, \phi u_7 = u_6$
- $\phi u_9 = u_{10}, \phi u_{10} = u_9, \phi u_{11} = u_{11} + t u_{12}, \phi u_{12} = -u_{12};\ t \in \mathbb{F}_q.$

It is easy to check that ϕ has order 2 , and group $K =< \phi, \omega > \leqslant SL_{12}(\mathbb{F}_q)$. In [13] authors showed that $K = SL_{12}(\mathbb{F}_q)$.

Now we consider the case $p = 5$, in this case we define a matrix ϕ' of $SL_{12}(\mathbb{F}_{5^n})$ with respect to the basis $\mathscr{B}$ as following:

- $\phi' u_1 = -u_1, \phi' u_5 = u_5, \phi' u_8 = u_8$
- $\phi' u_6 = u_7, \phi' u_7 = u_6, \phi' u_9 = u_{10}, \phi' u_{10} = u_9$
- $\phi' u_2 = 3u_2 + 2u_3 + 3u_4, \phi' u_3 = 3u_2 + 3u_3 + u_4, \phi' u_4 = 2u_2 + u_3 + 3u_4$
- $\phi' u_{11} = u_{11} + tu_{12}, \phi' u_{12} = -u_{12};\ t \in \mathbb{F}_{5^n}$

Here again ϕ' has order 2. In [13] authors proved that $SL_{12}(\mathbb{F}_{5^n}) =< \omega, \phi' >$.

2.3.2 $(2,3,7)$-generation of the groups $SL_n(\mathbb{F}_q)$ and $SL_n(\mathbb{Z})$

Recall that $q = p^n$,

Definition 2.3.3. ***Hurwitz Groups:*** *A $(2,3,7)$-generated group is a group generated by an element of order 2 and an element of order 3, such that order of product of these two elements is 7. A finite $(2,3,7)$-generated group is called Hurwitz Groups.*

In [10] , Lucchini, M.C.Tamburini and J.S.Wilson proved the following results:

Theorem 2.3.2. *[10, Corollary 1] For all $n \geq 287$, $SL_n(\mathbb{F}_q)$ is Hurwitz Group.*

Theorem 2.3.3. *[10, Corollary 1] For all $n \geq 287$, $SL_n(\mathbb{Z})$ is $(2,3,7)$-generated.*

2.4 Two generation of Symplectic Group

In this section we will provide some results of two-generation of Symplectic group :

2.4.1 $(2,3)$-generation of $Sp_6(\mathbb{F}_q)$ for q even

In [12] , Marco Antonio Pellegrini proved that the group $Sp_6(\mathbb{F}_q)$, where q is an even number, is $(2,3)$-generated.

Let $t \in \mathbb{F}_q$, from now onwards in this chapter , $x_{ij}(t)$ denotes the matrix, whose $(i,j)^{th}$ entry is equal to t and all other entries are 0.

Let θ, ζ be 6×6 matrix defined as follows: $\theta = x_{13}(1) + x_{24}(1) + x_{31}(1) + x_{42}(1) + x_{55}(1) + x_{66}(1) + x_{65}(g)$, and

$\zeta = x_{11}(1) + x_{14}(1) + x_{15}(1) + x_{22}(1) + x_{34}(1) + x_{43}(1) + x_{44}(1) + x_{52}(g) + x_{53}(1) + x_{54}(1) + x_{55}(1) + x_{56}(1) + x_{62}(g) + x_{63}(1) + x_{65}(1)$, where $g \in \mathbb{F}_q^*$. We observe that $\theta^2 = \zeta^3 = I_6$ and $\theta, \zeta \in Sp_6(\mathbb{F}_q)$.

In [12], author proved the following result :

Theorem 2.4.1. *[12, Theorem 2.5] Let q be an even number and $g \in \mathbb{F}_q^*$, such that $\mathbb{F}_q = \mathbb{F}_p[g]$ then θ, ζ defined above generates the group $Sp_6(\mathbb{F}_q)$ i.e. $Sp_6(\mathbb{F}_q) =< \theta, \zeta >$.*

The above result proves that the group $Sp_6(\mathbb{F}_q)$, where q is an even number, is $(2, 3)$-generated.

2.4.2 $(2, 3)$-generation of $Sp_{10}(\mathbb{Z})$

In [15] , Vsemirnov and vasilyev proved the following theorem :

Theorem 2.4.2. *[15, Theorem 2.1] The group $Sp_{10}(\mathbb{Z})$ is $(2, 3)$-generated.*

2.4.3 Two generation of $Sp_{2n}(\mathbb{F}_q)$ for large n

In [9], Lucchini and M.C.Tamburini proved the following result:

Theorem 2.4.3. *[9, Theorem 1] For $n \geq 371$, the group $Sp_{2n}(\mathbb{F}_q)$ is Hurwitz group.*

2.5 Two generation of Special Unitary Group

2.5.1 $(2, 3)$-generation of $SU_7(\mathbb{F}_{q^2})$

Let θ' and ζ' be 7×7 matrices defined as follows:

$\theta' = x_{12}(1) + x_{21}(1) + x_{17}(h) + x_{27}(h) + x_{34}(1) + x_{43}(1) + x_{56}(1) + x_{57}(-1) + x_{65}(1) + x_{67}(-1) + x_{77}(-1)$, and

$\zeta' = x_{11}(1) + x_{13}(-1) + x_{15}(-1) + x_{17}(h+i-1) + x_{23}(-1) + x_{32}(1) + x_{33}(-1) + x_{45}(-1) + x_{54}(1) + x_{55}(-1) + x_{67}(-1) + x_{76}(1) + x_{77}(-1)$, where either $h = i \in \mathbb{F}_q$ or $i = h^q \in \mathbb{F}_{q^2}$.

Theorem 2.5.1. *[12, Theorem 3.8] Let $h \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and it satisfies*

- $h^{2q} - h^{q+1} + h^2 + 2h^q + 2h + 4 \neq 0$;
- $(h + h^q)^3 - 8(h + h^q - 2)^2 - 8h^{q+1} \neq 0$, *when p is odd ;*
- $\mathbb{F}_{q^2} = \mathbb{F}_p[h^7]$

Then the group $SU_7(\mathbb{F}_{q^2})$ is generated by θ', ζ' i.e. $SU_7(\mathbb{F}_{q^2}) =< \theta', \zeta' >$.

This proves the $(2, 3)$-generation of the group $SU_7(\mathbb{F}_{q^2})$.

2.5.2 Two generation of $SU_{2n+7}(\mathbb{F}_q)$ for large n

In [9], Lucchini and M.C.Tamburini also proved the following result:

Theorem 2.5.2. *[9, Theorem 2] The group $SU_{2n+7}(\mathbb{F}_q)$ is Hurwitz group, when q is an odd number and $n \geq 371$.*

2.6 $(2, 3, 7)$-generation of Alternating Group

In [2] , Conder proved the following theorem :

Theorem 2.6.1. *[2] For $n > 167$, the Alternating Group is a Hurwitz Group.*

2.7 $(2,3,7)$-Generation of Projective Special Linear Group $PSL_2(\mathbb{F}_q)$

In [11], Macbeath gives the values of q, for which $PSL_2(\mathbb{F}_q)$ is $(2,3,7)$-generated group.

Theorem 2.7.1. *[11, Theorem 8] The group $PSL_2(\mathbb{F}_q)$ is a Hurwitz Group if :*

- $q = 7$
- $q = p$ *where* p *is a prime and* $p \equiv 1$ *or* 6 (mod 7)
- $q = p^3$ *where* p *is a prime and* $p \equiv 2, 3, 4$ *or* 5 (mod 7)

2.8 Probabilistic methods for $(2,3)$ generation problem

In [8], Martin W. Liebeck and Aner Shalev proved the following result related to $(2,3)$ generation problem:

Theorem 2.8.1. *[8, Theorem 1.4] Let H be a finite simple classical group where $H \neq PSp_4(\mathbb{F}_q)$. If we randomly choose an element of order 2 of H and an element of order 3 of H, then the probability that these elements generate the group H goes to 1 as cardinality of the group tends to infinity.*

2.9 Some Negative results towards Two Generation of Classical Groups

In [4], Di Martino, M.C.Tamburini proved that the following classical groups are not Hurwitz Groups:

Theorem 2.9.1. *[4, Theorem 3] If J is one of the following groups:*

1. *When $n = 8, 9, 11$ then*

(a) $Sp_n(\mathbb{F}_q)$, *where* q *is an odd number.*

(b) $SU_n(\mathbb{F}_{q^2})$, *where* $q \neq 27$.

2. $SL_{12}(\mathbb{F}_q)$, *if* $q \not\equiv 1(\mod 7)$.

3. $Sp_{12}(\mathbb{F}_q)$, *where* q *is an odd number.*

Then J *is not a Hurwitz group.*

Chapter 3

Steinberg Generators for Special linear group $SL_n(k)$

In this chapter we will prove that the Special linear groups defined over a finite field $k = \mathbb{F}_q$, $SL_n(k)$ (taking the field k which has $char(k) \neq 2$) can be generated by 2 of its elements. To prove this we will first prove that the special linear group $SL_n(k)$ can be generated by its elementary matrices defined in the section 3.1. Then we will prove that we can generate all the elementary matrices from those 2 elements of $SL_n(k)$, which will prove the Two Generation of $SL_n(k)$. We follow the paper of Steinberg ([14]) here.

Notation: $k = \mathbb{F}_q$; a finite field with q elements.

3.1 Elementary Matrices in $SL_n(k)$

Definition 3.1.1. *Elementary matrix of $SL_n(k)$ is defined as follows : $\lambda \in k$, $i \neq j$, $e_{ij}(\lambda) = I_n + x_{ij}(\lambda)$ where $x_{ij}(\lambda)$ matrix has the following form : $x_{ij}(\lambda) = \begin{cases} \lambda & \text{at ijth postion} \\ 0 & \text{otherwise} \end{cases}$*

In this chapter we are taking $e_{ij}(\lambda)$ as elementary matrices of $SL_n(k)$. (In chapter 5, e_{ij} are defined in a different manner for the symplectic groups)

Definition 3.1.2. *Commutator of 2 matrices A and B is defined as: $[A, B] = A^{-1}B^{-1}AB$.*

Theorem 3.1.1. *$SL_n(k)$ is generated by the following set of Elementary matrices : $\{e_{ij}(\lambda)$, for $i \neq j, 1 \leq i \leq n, 1 \leq j \leq n$ and $\lambda \in k$ $\}$.*

Proof. The idea of the proof is to start with a matrix $A \in SL_n(k)$ and multiply it with the matrices $e_{ij}(\lambda)$. We notice that it amounts to the row-column operations of first kind. So now to prove this theorem we will use induction on n.

first case when $n = 2$:

Define $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(k)$ now if **(i)** $c \neq 0$ then we can simply say that c^{-1} will exist and $A \in SL_2(k)$ so $det(A) = 1$ and the way matrix A is defined, $det(A) = ad - bc = 1 \implies b = (ad-1)c^{-1}$ so now $A = \begin{bmatrix} a & (ad-1)c^{-1}) \\ c & d \end{bmatrix}$ so now multiply A with the matrix $\begin{bmatrix} 1 & -(a-1)c^{-1} \\ 0 & 1 \end{bmatrix}$ then we will have:

$\begin{bmatrix} 1 & -(a-1)c^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & (ad-1)c^{-1} \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & (d-1)c^{-1} \\ c & d \end{bmatrix}$ then multiply with the matrix

$\begin{bmatrix} 1 & 0 \\ -c & 1 \end{bmatrix}$ we will get $\begin{bmatrix} 1 & 0 \\ -c & 1 \end{bmatrix} \begin{bmatrix} 1 & (d-1)c^{-1} \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & (d-1)c^{-1} \\ 0 & 1 \end{bmatrix}$ which proves that

$A = \begin{bmatrix} 1 & (a-1)c^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -c & 1 \end{bmatrix} \begin{bmatrix} 1 & (d-1)c^{-1} \\ 0 & 1 \end{bmatrix}$

which shows that A is a product of elementary matrices of $SL_2(k)$

(ii) if $b \neq 0$ it will proceed in the same way just that now b^{-1} will exist so

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ (d-1)b^{-1} & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ (a-1)b^{-1} & 1 \end{bmatrix}$

(iii) now if $b = c = 0$ then we have $A = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$. We first multiply A with the matrix

$\begin{bmatrix} 1 & 0 \\ 1-a^{-1} & 1 \end{bmatrix}$ to get,

$$\begin{bmatrix} 1 & 0 \\ 1-a^{-1} & 1 \end{bmatrix} A = \begin{bmatrix} a & 0 \\ a-1 & a^{-1} \end{bmatrix}$$

We further compute,

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ a-1 & a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & -a^{-1} \\ a-1 & a^{-1} \end{bmatrix}$$

Now we multiply $\begin{bmatrix} 1 & 0 \\ 1-a & 1 \end{bmatrix}$ with the matrix $\begin{bmatrix} 1 & -a^{-1} \\ a-1 & a^{-1} \end{bmatrix}$ and the computation shows that,

$$\begin{bmatrix} 1 & 0 \\ 1-a & 1 \end{bmatrix} \begin{bmatrix} 1 & -a^{-1} \\ a-1 & a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & -a^{-1} \\ 0 & 1 \end{bmatrix}$$

which eventually gives us,

$$A = \begin{bmatrix} 1 & 0 \\ a^{-1}-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a^{-1} \\ 0 & 1 \end{bmatrix}$$

So the theorem is true for $n = 2$. Now assume that theorem is true for $n = m$ and now we prove that the theorem is true for $n = m + 1$.

Let's take an $(m + 1) \times (m + 1)$ matrix C,

$$C = \begin{bmatrix} a_1 & b_1 & \cdots & b_m \\ a_2 & c_1 & \cdots & c_m \\ \vdots & \vdots & \ddots & \vdots \\ a_{m+1} & d_1 & \cdots & d_m \end{bmatrix}$$

The following cases are possible:

Case 1: $a_1 \neq 0, a_i \neq 0$ **for some** i

In this case we will multiply row i to $(1 - a_1)/a_i$ and then add row i to row 1, that will make the first entry one and after that we will multiply a_j to row 1 and subtract it from row j to make other entries zero of column 1 for $2 \leq j \leq m + 1$.

Case 2: $a_1 = 0, a_i \neq 0$ **for some** i

In this case first we will add row i to row 1 and then follow the case 1.

Case 3: $a_1 \neq 0, a_i = 0$ **for** $2 \leq i \leq m+1$**,**$b_j \neq 0$ **for some** j

In this case we will multiply column j to $(1 - a_1)/b_j$ and then add column j to column 1, that will make the first entry 1 in the place of a_1.

Case 4: $a_1 \neq 0, a_i = 0$ **for** $2 \leq i \leq m+1$**,**$b_j = 0$ **for** $1 \leq j \leq m$

In this case because $C \in SL_{m+1}(k)$, $a_1 = 1$.

Now from all these possible cases we will get a matrix which will have the form:

$$D = \begin{bmatrix} 1 & b'_1 & \cdots & b'_m \\ 0 & c'_1 & \cdots & c'_m \\ \vdots & \vdots & \ddots & \vdots \\ 0 & d'_1 & \cdots & d'_m \end{bmatrix}$$

in all these cases whatever elementary matrices we used they are in $SL_{m+1}(k)$ so if we define $A = \begin{bmatrix} c'_1 & \cdots & c'_m \\ \vdots & \ddots & \vdots \\ d'_1 & \cdots & d'_m \end{bmatrix}$ it will be a $m \times m$ matrix and it will be in $SL_m(k)$. So from our induction hypothesis A can be written in product of elementary matrices so now $D = (\prod e_{ij})E$. Where e_{ij} are elementary matrices in $SL_{m+1}(k)$ defined initially in the chapter and $E = \begin{bmatrix} 1 & b'_1 & \cdots & b'_m \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$. Now we just have to multiply b'_k to $(k+1)$-th row and subtract it from row 1 for each $k = 1, 2, 3...., m$ which reduces E to identity matrix. This proves C can be written as product of elementary matrices in $SL_{m+1}(k)$ which proves the theorem for $n = m + 1$.

So in this way by induction our theorem is proved. □

3.2 Two Generation of $SL_n(k)$

Reference for following theorem is [14, 3.11]:

Theorem 3.2.1. *$SL_n(k)$ is generated by following two elements:*

$$\gamma_m = I_n - x_{11}(1) - x_{22}(1) + x_{11}(m) + x_{22}(m^{-1})$$

and

$$s = e_{12}(1)\delta$$

*, where $x_{ij}(\lambda)$ are the matrices defined in **Definition 3.1.1** and m is the generator of the multiplicative group of the finite field k such that $m \neq 1$, $e_{12}(1)$ is the usual elementary matrix in $SL_n(k)$ and* $\delta = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & (-1)^{n+1} \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & & \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$.

Proof. So $s = e_{12}(1)\delta = (I_n + x_{12}(1))((-1)^{n+1}x_{1n}(1) + x_{21}(1) + x_{32}(1) + ... + x_{n,n-1}(1))$

$s = x_{11}(1) + (-1)^{n+1}x_{1n}(1) + x_{21}(1) + x_{32}(1) + ... + x_{n,n-1}(1)$ in this way we can easily calculate s^{-1} and $s^{-1} = (-1)^{n+1}x_{n1}(1) - x_{n2}(1) + x_{12}(1) + x_{23}(1) + ... + x_{n-1,n}(1)$.

Now we will conjugate γ_m from s and this will define as follows:

$\beta = s\gamma_m s^{-1} = (x_{11}(1) + (-1)^{n+1}x_{1\mathrm{n}}(1) + x_{21}(1) + x_{32}(1) + ... + x_{\mathrm{n,n\text{-}1}}(1))(I_{\mathrm{n}} - x_{11}(1) - x_{22}(1) + x_{11}(m) + x_{22}(m^{-1}))((-1)^{n+1}x_{\mathrm{n1}}(1) - x_{\mathrm{n2}}(1) + x_{12}(1) + x_{23}(1) + ... + x_{\mathrm{n\text{-}1,n}}(1))$.

$\beta = x_{11}(1) + x_{12}(m-1) + x_{22}(m) + x_{33}(m^{-1}) + x_{44}(1) + x_{55}(1) + ... + x_{\mathrm{nn}}(1)$.

Now take commutator of matrices β and γ_m ;

$[\beta, \gamma_m] = \beta^{-1}\gamma_m^{-1}\beta\gamma_m$; we can easily see that $\gamma_m^{-1} = I_{\mathrm{n}} - x_{11}(1) - x_{22}(1) + x_{11}(m^{-1}) + x_{22}(m)$ and $\beta^{-1} = x_{11}(1) + x_{12}(m^{-1} - 1) + x_{22}(m^{-1}) + x_{33}(m) + x_{44}(1) + x_{55}(1) + ... + x_{nn}(1)$.

so now $[\beta, \gamma_m] = (x_{11}(1) + x_{12}(m^{-1} - 1) + x_{22}(m^{-1}) + x_{33}(m) + x_{44}(1) + x_{55}(1) + ... + x_{nn}(1))(I_n - x_{11}(1) - x_{22}(1) + x_{11}(m^{-1}) + x_{22}(m))(x_{11}(1) + x_{12}(m-1) + x_{22}(m) + x_{33}(m^{-1}) +$

$x_{44}(1) + x_{55}(1) + ... + x_{nn}(1))(I_n - x_{11}(1) - x_{22}(1) + x_{11}(m) + x_{22}(m^{-1}))$.

By calculating this matrix multiplication we eventually get $[\beta, \gamma_m] = I_n + x_{12}(g)$=$e_{12}(g)$.

where $e_{12}(g)$ is the usual elementary matrix in $SL_n(k)$ and $g = (1-m)(1-m^{-2})$ and in the theorem we stated that $m \neq 1$ which implies $g \neq 0$.

Lemma 3.2.2. *[14, 3.9] Let G be the subgroup generated by the elements $\{\gamma_m, s\}$ and we proved above that $e_{12}(g) \in G$ where $g \in k^*$ and k^* is the multiplicative group of the finite field k. Then γ_m and $e_{12}(g)$ will generate $\{e_{12}(t), t \in k\}$.*

Proof. Let's take conjugation by γ_m on the element $e_{12}(g)$ we will get:

$\gamma_m e_{12}(g)\gamma_m^{-1} = (I_n - x_{11}(1) - x_{22}(1) + x_{11}(m) + x_{22}(m^{-1}))(I_n + x_{12}(g))(I_n - x_{11}(1) - x_{22}(1) + x_{11}(m^{-1}) + x_{22}(m)) = I_n + x_{12}(gm^2) = e_{12}(gm^2)$ now if i take

$\gamma_m e_{12}(gm^2)\gamma_m^{-1} = e_{12}(gm^4)$ so by taking repeated conjugation by γ_m we will get element of type $\{e_{12}(gm_i{}^2)\} \subset G$ where i am taking $m_i{}^2 = m^{2i}$ where $i = 1, 2, 3, ...$

now if we multiply all these elements we will get $\{e_{12}(g\sum_i m_i{}^2)\} \subset G$. Now define a subset of the finite field k as $\mathcal{S} = \{g\sum_i m_i{}^2 : e_{12}(g\sum_i m_i{}^2) \in G\} \subseteq k$ which simply says that $\mathcal{S} = \{gm_1{}^2, gm_2{}^2, ..., g(m_1{}^2+m_2{}^2), ...\}$ and $\mathcal{S}$ is closed under addition so that's why it is an additive subgroup of the finite field k. Now we have the finite field which has characteristic not equal to 2 so the multiplicative group k^* which is a cyclic group will have even order and m is a generator of k^* so definitely half the elements of k are in the subgroup $\mathcal{S}$ which are $\{gm_1{}^2, gm_2{}^2, ...gm_i{}^2\}$ now if we showed that there is at least one more element is in $\mathcal{S}$ then because $\mathcal{S}$ is an additive subgroup , by Lagrange's theorem $\mathcal{S}$ will be the whole field k i.e. $\mathcal{S} = k$.

So now assume that the element $gm_1{}^2 + gm_2{}^2 = gm_j{}^2$ for some j but we know that $m_1{}^2 = m^2$,$m_2{}^2 = m^4$ and $m_j{}^2 = m^{2r}$ for some r so from our assumption $gm^2 + gm^4 = gm^{2r} \implies m^2 + m^4 = m^{2r} \implies$

$$1 + m^2 = m^{2(r-1)} \tag{3.1}$$

Now $k = \mathbb{F}_q$ a finite field with q elements where q is a prime power. So then cardinality of $\mathbb{F}_q{}^*$ will be $|\mathbb{F}_q{}^*| = q - 1$ and m is the generator of $\mathbb{F}_q{}^*$, so $m^{q-1} = 1$ so if we take power $(q-1)/2$ both side of the equation 3.1 then $(1+m^2)^{(q-1)/2} = (m^{2(r-1)})^{(q-1)/2}$ then right hand

side will be equal to 1 but LHS will be $(1+m^2)^{(q-1)/2} = 1+1+..... = 2+....$

which is greater than 1 which is a contradiction so our assumption that ${gm_1}^2 + {gm_2}^2 = {gm_j}^2$ for some j is wrong so $({gm_1}^2 + {gm_2}^2)$ is a new element which proves that $\mathcal{S} = k$ and the way $\mathcal{S}$ is defined $\mathcal{S} = k$ shows $\{e_{12}(t) : t \in k\} \subset G$. □

Now $\{e_{12}(t) : t \in k\} \subset G$. Now take $\delta e_{12}(t)\delta^{-1} = ((-1)^{n+1}x_{1n}(1)+x_{21}(1)+x_{32}(1)+.....+x_{n,n-1}(1))(I_n+x_{12}(t))((-1)^{n+1}x_{n1}(1)+x_{12}(1)+x_{23}(1)+.....+x_{n-1,n}(1)) = ((-1)^{n+1}x_{1n}(1)+x_{21}(1)+x_{32}(1)+.....+x_{n,n-1}(1)+x_{22}(t))((-1)^{n+1}x_{n1}(1)+x_{12}(1)+x_{23}(1)+.....+x_{n-1,n}(1)) = x_{11}(1)+x_{22}(1)+x_{33}(1)+.....+x_{n,n}(1)+x_{23}(t) = I_n+x_{23}(t) = e_{23}(t)$. So $\delta e_{12}(t)\delta^{-1} = e_{23}(t) \implies e_{23}(t) \in G$.

So now take $\delta e_{23}(t)\delta^{-1} = ((-1)^{n+1}x_{1n}(1)+x_{21}(1)+x_{32}(1)+.....+x_{n,n-1}(1))(I_n+x_{23}(t))((-1)^{n+1}x_{n1}(1)+x_{12}(1)+x_{23}(1)+.....+x_{n-1,n}(1)) = ((-1)^{n+1}x_{1n}(1)+x_{21}(1)+x_{32}(1)+.....+x_{n,n-1}(1)+x_{33}(t))((-1)^{n+1}x_{n1}(1)+x_{12}(1)+x_{23}(1)+.....+x_{n-1,n}(1)) = I_n+x_{34}(t) = e_{34}(t) \implies \delta e_{23}(t)\delta^{-1} = e_{34}(t) \in G$.

$\delta e_{34}(t)\delta^{-1} = ((-1)^{n+1}x_{1n}(1)+x_{21}(1)+x_{32}(1)+.....+x_{n,n-1}(1))(I_n+x_{34}(t))((-1)^{n+1}x_{n1}(1)+x_{12}(1)+x_{23}(1)+.....+x_{n-1,n}(1)) = ((-1)^{n+1}x_{1n}(1)+x_{21}(1)+x_{32}(1)+.....+x_{n,n-1}(1)+x_{44}(t))((-1)^{n+1}x_{n1}(1)+x_{12}(1)+x_{23}(1)+.....+x_{n-1,n}(1)) = I_n+x_{45}(t) = e_{45}(t) \implies e_{45}(t) \in G$.

in this way if we calculate $\delta e_{i,i+1}(t)\delta^{-1} = e_{i+1,i+2}(t)$ for $i = 1,2,3,....,(n-2) \implies \{e_{12}(t), e_{23}(t), e_{34}(t), ..., e_{n-1,n}(t)\} \subset G$.

Now take commutator of $e_{12}(t)$ and $e_{23}(t')$ where $t, t' \in k$ we will get :

$[e_{12}(t), e_{23}(t')] = {e_{12}}^{-1}(t){e_{23}}^{-1}(t')e_{12}(t)e_{23}(t') = (I_n - x_{12}(t))(I_n - x_{23}(t')(I_n + x_{12}(t))(I_n + x_{23}(t')) = (I_n - x_{12}(t) - x_{23}(t') + x_{13}(tt'))(I_n + x_{12}(t) + x_{23}(t') + x_{13}(tt')) = I_n + x_{13}(tt') = e_{13}(tt') \implies [e_{12}(t), e_{23}(t')] = e_{13}(tt')$ where t and t' are arbitrary elements of the field k and $tt' \in k$ so tt' will vary on all over the field k and we will have $\{e_{13}(\theta), \theta \in k\} \subset G$.

In the same way $[e_{13}(t), e_{34}(t')] = e_{14}(tt')$ so now in general ;

$[e_{1,j-1}(t), e_{j-1,j}(t')] = e_{1j}(tt')$ for $j = 3,4,5,...,n \implies \{e_{1j}(\phi) : \phi \in k; j = 2,3,4,...,n\} \subset G$.

Now if we take $[e_{23}(t), e_{34}(t')] = e_{24}(tt')$ and $[e_{24}(t), e_{45}(t')] = e_{25}(tt')$ and as above we saw in this case we will get that $\{e_{2j}(\phi) : \phi \in k; j = 3, 4, 5, ..., n\} \subset G$. So by taking these conjugation and commutator we will eventually get that $\{e_{ij}(\phi) : \phi \in k; i < j, 1 \leq i \leq n-1, 1 \leq j \leq n\} \subset G$.

Now let's conjugate δ with the element $e_{1n}(t)$ so we will have : $\delta e_{1n}(t)\delta^{-1} = ((-1)^{n+1}x_{1n}(1) + x_{21}(1) + x_{32}(1) + ... + x_{n,n-1}(1))(I_n + x_{1n}(t))((-1)^{n+1}x_{n1}(1) + x_{12}(1) + x_{23}(1) + ... + x_{n-1,n}(1)) = ((-1)^{n+1}x_{1n}(1) + x_{21}(1) + x_{32}(1) + ... + x_{n,n-1}(1) + x_{2n}(t))((-1)^{n+1}x_{n1}(1) + x_{12}(1) + x_{23}(1) + ... + x_{n-1,n}(1)) = I_n + x_{21}(t) = e_{21}(t) \implies e_{21}(t) \in G$.

Now calculate $\delta e_{21}(t)\delta^{-1} = ((-1)^{n+1}x_{1n}(1) + x_{21}(1) + x_{32}(1) + ... + x_{n,n-1}(1))(I_n + x_{21}(t))((-1)^{n+1}x_{n1}(1) + x_{12}(1) + x_{23}(1) + ... + x_{n-1,n}(1)) = ((-1)^{n+1}x_{1n}(1) + x_{21}(1) + x_{32}(1) + ... + x_{n,n-1}(1) + x_{31}(t))((-1)^{n+1}x_{n1}(1) + x_{12}(1) + x_{23}(1) + ... + x_{n-1,n}(1)) = I_n + x_{32}(t) = e_{32}(t)$. So as previously we did, similarly $\delta e_{i+1,i}(t)\delta^{-1} = e_{i+2,i+1}(t)$ for $i = 2, 3, 4, ...n-2. \implies \{e_{21}(t), e_{32}(t), e_{43}(t), ..., e_{n,n-1}(t)\} \subset G$.

Now take commutator of $e_{32}(t)$ and $e_{21}(t')$; $[e_{32}(t), e_{21}(t')] = {e_{32}}^{-1}(t){e_{21}}^{-1}(t')e_{32}(t)e_{21}(t') = (I_n - x_{32}(t))(I_n - x_{21}(t'))(I_n + x_{32}(t))(I_n + x_{21}(t')) = I_n + x_{31}(tt') = e_{31}(tt'); tt' \in k$.

$[e_{43}(t), e_{32}(t')] = e_{42}(tt')$ and $[e_{42}(t), e_{21}(t')] = e_{41}(tt')$.

In this way we can see that $\{e_{3j}(\phi) : \phi \in k; j = 1, 2\} \subset G$, $\{e_{4j}(\phi) : \phi \in k; j = 1, 2, 3\} \subset G$, $\{e_{5j}(\phi) : \phi \in k; j = 1, 2, 3, 4\} \subset G$,....., $\{e_{nj}(\phi) : \phi \in k; j = 1, 2, 3, 4, ...(n-1)\} \subset G$.

This shows that $\{e_{ij}(\phi) : \phi \in k; i > j, 1 \leq i \leq n, 1 \leq j \leq n-1\} \subset G$.

So we showed that $\{e_{ij}(\phi) : \phi \in k; i \neq j, 1 \leq i \leq n, 1 \leq j \leq n\} \subset G$.

From Theorem 3.1.1 we can see that $SL_n(k)$ is generated by the set $\{e_{ij}(\phi) : \phi \in k; i \neq j, 1 \leq i \leq n, 1 \leq j \leq n\}$ so it shows that $SL_n(k) \leqslant G$, but G is a group generated by $\{\gamma_m, s\}$ and γ_m and s both are elements of $SL_n(k)$ which implies that $G =< \gamma_m, s > \leqslant SL_n(k) \implies G =< \gamma_m, s >= SL_n(k)$.

$$\boxed{G =< \gamma_m, s >= SL_n(k)}$$

Which eventually shows that we can generate $SL_n(k)$ group by two elements γ_m and s. $\square$

Chapter 4

Generation of $SL_n(\mathbb{Z})$ by Two Jordan Unipotent Matrices

In this chapter we study the generation of $SL_n(\mathbb{Z})$ by a Unipotent matrix θ and its transpose. To study this generation problem first we will study that for a Euclidean Ring R the set which is generated by elementary matrices of R will generate the whole $SL_n(R)$. Now $\mathbb{Z}$ is also a Euclidean Ring so then we will use all this above information to prove the desired result, which is Two Generation of $SL_n(\mathbb{Z})$.

Notation: $diag(s_1, s_2, ..., s_n)$: means an $n \times n$ diagonal matrix.

Definition 4.0.1. ***Unipotent Matrix:*** *A square matrix M is said to be Unipotent Matrix if $M - I$ is nilpotent, where I is an Identity matrix. That is, $(M - I)^k = 0$ for some positive integer k.*

Let $\mathbb{Z}$ denote the ring of rational integers and $SL_n(\mathbb{Z})$ the group of $n \times n$ invertible matrices with determinant 1 with entries in $\mathbb{Z}$. Let θ denote the Jordan Unipotent $n \times n$ invertible matrix which has determinant 1 , so $\theta \in SL_n(\mathbb{Z})$ and ϕ is its transpose means $\phi = \theta^{\intercal}$ and θ has following matrix form:

$$\theta = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & & \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{bmatrix} = I_{\mathrm{n}} + x_{21}(1) + x_{32}(1) + ... + x_{\mathrm{n,n\text{-}1}}(1).$$

where $x_{\mathrm{ij}}(t)$ is defined as follows: $t \in \mathbb{Z}$, $x_{ij}(t) = \begin{cases} t & \text{at } ijth \text{ postion} \\ 0 & \text{otherwise} \end{cases}$

so θ and ϕ are in $SL_n(\mathbb{Z})$

Theorem 4.0.1. *[5] For $n \geq 2$ and $n \neq 4$ the elements $\{\theta, \phi\}$ generate the group $SL_n(\mathbb{Z})$.*

. We will prove this Theorem in following sections.

4.1 Generation of the Group $SL_n(R)$ by elementary matrices where R is a Euclidean Ring

$GL_n(R)$: The group of $n \times n$ invertible matrices over R.

Definition 4.1.1. *A ring R is said to be Euclidean Ring, if there exists a norm function $N : R \to \mathbb{Z}^{\geq 0}$ such that for each $a, b \in R$ with $b \neq 0$ there exists $q, r \in R$ such that $a = bq + r$ with $r = 0$ or $N(r) < N(b)$.*

Before starting the lemmas we introduce embedding of $GL_n(R)$ as a subgroup of $GL_{n+1}R)$. $GL_n(R)$ sits inside $GL_{n+1}(R)$ as follows :

$$GL_n(R) \to GL_{n+1}(R)$$

$$A \to \begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}$$

and considering $GL_1(R)$ as a subgroup of $GL_n(R)$ it consist of $n \times n$ diagonal matrices

with first entry of the diagonal is a unit and other entries are 1,which means if $a \in R^*$ then

$$a \to diag(a, 1, ..., 1) \in GL_n(R)$$

Definition 4.1.2. ***Unit of a Ring R:*** *An element $a \neq 0 \in R$ is said to be a unit if there exists an element $b \neq 0 \in R$ such that $ab = 1$.*

Lemma 4.1.1. *[7, Theorem 1.2.10, page 24] If R is a Euclidean Commutative Ring ,then for $n \geq 1$, $GL_n(R) = GL_1(R)E_n(R)$, where $E_n(R)$ is the group generated by the set $\{e_{ij}(t), i \neq j, 1 \leq i \leq n, 1 \leq j \leq n, t \in R\}$ where $e_{ij}(t) = I_n + x_{ij}(t)$ the elementary matrices for $SL_n(R)$ as defined in Chapter 3.*

Proof. We will prove this lemma by induction on n.The lemma is simply true for $n = 1$ because $GL_1(R) = GL_1(R)$, now assume the statement is true for $k = n - 1$ which implies that we are assuming that $GL_{n-1}(R) = GL_1(R)E_{n-1}(R)$.Now let $\zeta \in GL_n(R)$ so we have to just prove that $\exists\ \Omega$ and $\delta \in E_n(R)$ such that $\Omega\zeta\delta \in GL_{n-1}(R)$, let's assume that it is true then we know that $GL_1(R)$ normalizes $E_n(R)$ because if we take $diag(s_1, s_2, ..., s_n)$ then $diag(s_1, s_2, ..., s_n)e_{\mathrm{ij}}(t)diag(s_1, s_2, ...s_n)^{-1} = e_{\mathrm{ij}}(s_i t s_j^{-1})$ and $diag(s, 1, 1, ..., 1)$ are the elements of $GL_1(R)$ when considered as subgroup of $GL_n(R)$ so it shows that $GL_1(R)$ normalizes $E_n(R)$.Now we have $\Omega\zeta\delta \in GL_{n-1}(R) = GL_1(R)E_{n-1}(R)$ so let's take that $\Omega\zeta\delta = \sigma\tau$ where $\sigma \in GL_1(R)$ and $\tau \in E_{n-1}(R)$ so $\Omega\zeta = \sigma\tau\delta^{-1}$ so $\tau\delta^{-1} = \tau' \in E_n(R)$ so $\Omega\zeta = \sigma\tau'$ which implies that $\sigma^{-1}\Omega\zeta = \tau'$ and because $GL_1(R)$ normalizes $E_n(R)$ $\sigma^{-1}\Omega = t\sigma^{-1}$ where $t \in E_n(R)$ so $t\sigma^{-1}\zeta = \tau' \implies \zeta = \sigma t^{-1}\tau'$ where $\sigma \in GL_1(R)$ and $t^{-1}\tau' \in E_n(R)$ so $\zeta \in GL_1(R)E_n(R)$ which implies that $GL_n(R) = GL_1(R)E_n(R)$.

Now we have to prove that $\exists\ \Omega$ and $\delta \in E_n(R)$ such that $\Omega\zeta\delta \in GL_{n-1}(R)$.So let's define a double coset $E_n(R)\zeta E_n(R) = \{\Omega\zeta\delta : \Omega, \delta \in E_n(R)\}$.Define a Norm function N as defined in the Definition 4.1.1 and $p \in R$ in such a way so that $N(p)$ is minimum and it is possible in a Euclidean Ring to find such element.If we see the effect of arbitrary g and $g' \in E_n(R)$ on ζ they are just elementary row and column operations so there will be an appropriate g and g' such that matrix $g\zeta g'$ will contain p as an entry.Now if we define a matrix $d_{ij}(t) = e_{ij}(t)e_{ji}(-t^{-1})e_{ij}(t)$ where $e_{ij}(t)$ are usual elementary matrices.Then $d_{ij}(1) = e_{ij}(1)e_{ji}(-1)e_{ij}(1)$ and the effect of $d_{ij}(1)$ on the matrix $g\zeta g'$ will be simply that it will interchange the ith and jth row and multiply by -1 to the new jth row when it multiplied from the left and it will do the same thing to the columns if it multiplied from the right.So if we multiply $g\zeta g'$ by product of these matrices with an appropriate i and j

then $(\prod_{i,j} d_{ij}(1))g\zeta g'(\prod_{u,l} d_{ul}(1))$ will contain p at (n,n) position. and Simply $\prod_{i,j} d_{ij}(1)) \in E_n(R)$,let $b < n$ and in the matrix $(\prod_{i,j} d_{ij}(1))g\zeta g'(\prod_{u,l} d_{ul}(1))$ let's say q is at (b,n) position , then from division algorithm q can be written as $q = ap + r$ where $N(r) < N(p)$.

Now let's take $e_{b,n}(-a)$ and multiply $e_{b,n}(-a)(\prod_{i,j} d_{ij}(1))g\zeta g'(\prod_{u,l} d_{ul}(1))$ then this matrix will have r at its (b,n) position but $N(r) < N(p)$. So $r = 0$ so in this way we get a matrix which has 0 at (b,n) position where $b < n$ and b is arbitrary so by varying b and take $(\prod_{b<n} e_{b,n}(-a))(\prod_{i,j} d_{ij}(1))g\zeta g'(\prod_{u,l} d_{ul}(1))$ this matrix will have all entries of nth column as 0 except p at (n,n) position and the same thing we do from right. We will get a matrix which has all entries of nth row as 0 except p at (n,n) position and $p \in R^*$ because the resultant matrix is in $GL_n(R)$. So now if we multiply the resultant matrix with $d_{n-1,n}(p)d_{n-1,n}(-1)$ then we will get a matrix which has all entries of nth row and nth column as 0 except 1 at (n,n) position.So we get a matrix which is in $GL_{n-1}(R)$ and also in the double coset. □

Corollary 4.1.2. *[7, Theorem 1.2.11, page 25] If R is a commutative Euclidean ring then $SL_n(R) = E_n(R)$.*

Proof. In a commutative ring R, $E_n(R) \leq SL_n(R)$ and from Lemma 4.1.1 $SL_n(R) \leq GL_n(R) = GL_1(R)E_n(R) \leq E_n(R)$ which implies $SL_n(R) \leq E_n(R) \implies SL_n(R) = E_n(R)$. □

Corollary 4.1.3. *Because $\mathbb{Z}$ is also a Euclidean Commutative Ring , then from Corollary 4.1.2 $SL_n(\mathbb{Z}) = E_n(\mathbb{Z})$.*

Lemma 4.1.4. *$SL_n(\mathbb{Z})$ is generated by the set $\{e_{ij}(1), i \neq j, 1 \leq i \leq n, 1 \leq j \leq n\}$.*

Proof. From corollary 4.1.3 we have $SL_n(\mathbb{Z}) = E_n(\mathbb{Z})$ which implies that $SL_n(\mathbb{Z})$ is generated by the set $\{e_{\mathrm{ij}}(t), i \neq j, 1 \leq i \leq n, 1 \leq j \leq n, t \in \mathbb{Z}\}$ so now let's take $t \in \mathbb{Z}, i \neq j$ and take $e_{\mathrm{ij}}(t) = e_{\mathrm{ij}}(1)^t$ this simply proves the lemma. □

4.2 Proof Of The Theorem 4.0.1 in the case of $n = 2$

In this case $\theta = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $\phi = \theta^{\intercal} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ Now take an arbitrary element $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2,\mathbb{Z})$. Let's say $c \neq 0$ and also let's assume $|a| \geq |c|$ means the lower left entry has lower

absolute value than the upper left entry then by dividing a by c from divison algorithm $a = cq + r$ where $0 \leq r < |c|$. Now if we multiply ϕ^{-q} to γ from the left side then $\phi^{-q}\gamma = \begin{bmatrix} 1 & -q \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a - cq & b - qd \\ c & d \end{bmatrix}$ but we have $a - cq = r$ so then $\phi^{-q}\gamma = \begin{bmatrix} r & b - qd \\ c & d \end{bmatrix}$ now if we take $\phi\theta^{-1}\phi == \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, define $\phi\theta^{-1}\phi\phi^{-q}\gamma == \begin{bmatrix} c & d \\ -r & qd - b \end{bmatrix}$ in this matrix also we have the lower left entry with lower absolute value than the upper left entry. So multiplying by enough copies of $\phi\theta^{-1}\phi$ and powers of ϕ we will get the lower left entry zero (because of the divison algorithm) and the resultant matrix will be in $SL_2(\mathbb{Z})$ so the determinant of that matrix will be one and the form of the matrix will be as follows: $\begin{bmatrix} \pm 1 & h \\ 0 & \pm 1 \end{bmatrix}$ for some $h \in \mathbb{Z}$ where the diagonal entries will have the same sign. So the matrix is either ϕ^h or $-\phi^{-h}$. Now let's define that H the subgroup of $SL_2(\mathbb{Z})$ generated by θ and ϕ. Then $\exists y \in H$ such that $y\gamma = \pm\phi^j$ for some $j \in \mathbb{Z}$. Define $\phi\theta^{-1}\phi = V$ then $V^2 = -I_2$ which shows that $\gamma = \pm y^{-1}\phi^j \in H$. H is the subgroup generated by θ and ϕ, and γ is an arbitrary element of $SL(2, \mathbb{Z})$ which shows θ and ϕ will generate $SL(2, \mathbb{Z})$. So the theorem is proved for $n = 2$.

Now in further section we will take $n \geq 3$. Before going further let's define some elements: First take H is the subgroup of $SL_n(\mathbb{Z})$ for $n \geq 3$ generated by $\{\theta, \phi\}$

Let $\{u_1, ..., u_n\}$ be the standard generators (written in column vectors) of the free $\mathbb{Z}$-module $\mathbb{Z}^n$ of rank n.which means u_i is a column vector having entry 1 at ith place and other place 0.Now define $\sigma = \theta^{-1}\phi$ and $\omega = \sigma^{-1}\phi\sigma$.

So we can easily see that $\sigma u_1 = \theta^{-1}\phi u_1 = \theta^{-1}u_1 = u_1 - u_2 + ... + (-1)^{n-1}u_n$ and $\sigma u_i = u_{\text{i-1}}$ for $2 \leq i \leq n$.

So $\omega u_1 = u_1 - u_2 + ... + (-1)^{n-1}u_n$, $\omega u_2 = u_2$ and $\omega u_i = u_i + u_{i-1}$ for $3 \leq i \leq n$.

So we can write ω in the matrix form in following way: $\omega = \begin{bmatrix} 1 & 0 \\ f & \phi_1 \end{bmatrix}$ where f is the following column vector:$f = \begin{pmatrix} -1 \\ (-1)^2 \\ \vdots \\ (-1)^{n-1} \end{pmatrix}$ and ϕ_1 is the $(n-1) \times (n-1)$ analogue of ϕ.

4.2.1 The Subgroup $\mathscr{C}_n$ and the map η

Let $\mathscr{C}_n$ be the subgroup of $SL_n(\mathbb{Z})$ consisting of all matrices of the type $\begin{bmatrix} 1 & 0 \\ u & a \end{bmatrix}$ where u runs over all elements (written in column vectors) in $\mathbb{Z}^{n-1}$ and a runs over all elements in $SL_{n-1}(\mathbb{Z})$. Let's define a map η:

$$\eta : \mathscr{C}_n \to SL_{n-1}(\mathbb{Z})$$

$$\begin{bmatrix} 1 & 0 \\ u & a \end{bmatrix} \to a$$

we can easily see that η is a group homomorphism considering them as multiplicative groups because if we identify $\mathscr{C}_n$ with set of all ordered pairs (u, a) where $u \in \mathbb{Z}^{n-1}$ and $a \in SL_{n-1}(\mathbb{Z})$ and the multiplication will be defined in the following way to these ordered pairs:

$$(u, a)(v, b)=(u + av, ab)$$

$$\eta((u + av, ab)) = \eta((u, a)(v, b)) = ab = \eta(u, a)\eta(v, b)$$

and for any arbitrary a in $SL_{n-1}(\mathbb{Z})$ we will always have a matrix $\begin{bmatrix} 1 & 0 \\ u & a \end{bmatrix} \in \mathscr{C}_n$ so η is a surjective group homomorphism. Ker $\eta = \mathscr{J}_n = \{M \in \mathscr{C}_n : \eta(M) = I\}$ so

$\mathscr{J}_n = \{\begin{bmatrix} 1 & 0 \\ u & I \end{bmatrix} : u \in \mathbb{Z}^{n-1}\}$. The elements θ and ω which we defined above clearly we can see that they are in $\mathscr{C}_{\mathrm{n}}$ where $\theta = (s, \theta_1)$ where $s = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ and θ_1 is the $(n-1) \times (n-1)$ analogue of θ and $\omega = (f, \phi_1)$.

Lemma 4.2.1. *[5, Lemma 1] If r and s are integers in such a way that $1 \leq s < r \leq n$ then $\phi^{-1}e_{rs}(q)e_{r+1,s}(q)\phi = e_{r+1,s}(q)e_{r+1,s+1}(q)$, where q is a non-zero integer.*

Proof. $e_{\mathrm{rs}}(q) = I_{\mathrm{n}} + x_{\mathrm{rs}}(q)$ as defined earlier now we have following thing: $x_{\mathrm{rs}}(q)x_{\mathrm{kl}}(t) = 0$ if $s \neq k$, otherwise if $s = k$, then $x_{\mathrm{rs}}(q)x_{\mathrm{sl}}(t) = x_{\mathrm{rl}}(qt)$ and we want to prove

$$e_{\mathrm{rs}}(q)e_{\mathrm{r+1,s}}(q)\phi = \phi e_{\mathrm{r+1,s}}(q)e_{\mathrm{r+1,s+1}}(q) \tag{4.1}$$

and $\phi = I + x_{12}(1) + x_{23}(1) + ... + x_{\mathrm{n\text{-}1,n}}(1)$ so LHS of equation 4.1 is : $e_{\mathrm{rs}}(q)e_{\mathrm{r+1,s}}(q)\phi = (I + x_{\mathrm{rs}}(q))(I + x_{\mathrm{r+1,s}}(q))(I + x_{12}(1) + x_{23}(1) + ... + x_{n-1,n}(1)) = I + x_{12}(1) + x_{23}(1) + ... + x_{n-1,n}(1) + x_{\mathrm{rs}}(q) + x_{\mathrm{r,s+1}}(q) + x_{\mathrm{r+1,s}}(q) + x_{\mathrm{r+1,s+1}}(q)$.

Now if we calculate RHS of equation 4.1 : $\phi e_{\mathrm{r+1,s}}(q)e_{\mathrm{r+1,s+1}}(q) = I + x_{12}(1) + x_{23}(1) + ... + x_{n-1,n}(1) + x_{\mathrm{rs}}(q) + x_{\mathrm{r,s+1}}(q) + x_{\mathrm{r+1,s}}(q) + x_{\mathrm{r+1,s+1}}(q)$ which implies $LHS = RHS$. □

Lemma 4.2.2. *[5, Lemma 2] Let $v = s_1u_1 + s_2u_2 + ... + s_nu_n$ be an element of $\mathbb{Z}^n$,where u_i is the standard basis of $\mathbb{Z}^n$. Then if $s_i \neq 0$ for some i then the sub-module of $\mathbb{Z}^n$ which is generated by the set $\{gu : g \in H\}$, contains $(|s_i|\mathbb{Z})^n$. So if any s_i will have value 1 then the set $\{gu : g \in H\}$ will generate $\mathbb{Z}^n$, where $H =< \theta, \phi >$.*

Proof. Let M be the submodule of $\mathbb{Z}^n$ generated by the set $\{gu : g \in H\}$. We can see that $\theta u_i = u_{\mathrm{i}} + u_{\mathrm{i+1}}$ for $1 \leq i \leq n-1$ and $\theta u_{\mathrm{n}} = u_{\mathrm{n}}$, so if we take $\theta v - v = s_1u_2 + s_2u_3 + ...s_{\mathrm{n\text{-}1}}u_{\mathrm{n}} \in M$ and let's define $\theta v - v = m$ then if we take $\theta m - m = s_1u_3 + s_2u_4 + ...s_{\mathrm{n\text{-}2}}u_{\mathrm{n}} \in M$ this process will occur upto we got $Q = s_1u_{\mathrm{n\text{-}i+1}} + s_2u_{\mathrm{n\text{-}i+2}} + ...s_{\mathrm{i}}u_{\mathrm{n}} \in M$. Now we will take $\phi Q - Q = s_1u_{\mathrm{n\text{-}i}} + s_2u_{\mathrm{n\text{-}i+1}} + ...s_{\mathrm{i}}u_{\mathrm{n\text{-}1}} \in M$ and let's define $\phi Q - Q = Q'$ and take $\phi Q' - Q' = Q'' = s_1u_{\mathrm{n\text{-}i\text{-}1}} + s_2u_{\mathrm{n\text{-}i}} + ...s_{\mathrm{i}}u_{\mathrm{n\text{-}2}}$ so $Q'' \in M$ in this way if we do this process we will eventually get that $s_{\mathrm{i}}u_{\mathrm{i}} \in M\ \forall i$ which means $\{s_1u_1, s_2u_2, ...s_{\mathrm{n}}u_{\mathrm{n}}\} \in M$. Now let's take $\theta s_1u_1 = s_1(u_1 + u_2) \in M$ which simply implies that $s_1u_2 \in M$ in the same way operating θ on these elements will give us that $\{s_1u_{\mathrm{j}} \in M \text{ for } 1 \leq j \leq n\}$. In the same way operating θ on s_2u_2 we will get that $\{s_2u_{\mathrm{j}} \in M \text{ for } 2 \leq j \leq n\}$ and operating ϕ on s_2u_2 we will see that $\phi s_2u_2 = s_2u_1 + s_2u_2 \in M$ but it is proved above that $s_2u_2 \in M$ which implies that $s_2u_1 \in M$. So in this way by operating θ and ϕ we will get $\{s_{\mathrm{i}}u_{\mathrm{j}} \in M \text{ for } 1 \leq i \leq n\ ,\ 1 \leq j \leq n\}$. □

The proof in the following section follows very closely to that of Theorem 1 of [5].

4.3 Proof of Theorem 4.0.1 in the case of $n = 3$ and $n = 5$

Let's take $n = 5$, the way $\mathscr{C}_5$ is defined it is obvious that θ and ω are in the subgroup $\mathscr{C}_5$.Now define $\chi = \theta^{-1}\omega$ then $\chi = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -2 & 1 & 1 & 0 & 0 \\ 3 & -1 & 0 & 1 & 0 \\ -4 & 1 & 0 & 0 & 1 \\ 5 & -1 & 0 & 0 & 0 \end{bmatrix}$ so now $\chi^5 = \begin{bmatrix} 1 & 0 \\ \rho_1 & -I \end{bmatrix}$ where I is a 4×4 identity matrix and ρ_1 is a column vector $\begin{bmatrix} 4 & 4 & 2 & 6 \end{bmatrix}$ Then the commutator $[\theta, \chi^5] = \theta^{-1}\chi^{-5}\theta\chi^5 = \begin{bmatrix} 1 & 0 \\ \rho_2 & I \end{bmatrix}$ where ρ_2 is the column vector $\begin{bmatrix} -2 & -2 & -2 & 0 \end{bmatrix}$. Now we see that from lemma 4.2.2 , if we define the sub-module $\{g\rho_2 : g \in H\}$ of $\mathbb{Z}^4$, then this sub-module will contain $(2\mathbb{Z})^4$, now let's define a subgroup $\left\{k(\rho_2, I)k^{-1} : k \in < \theta, \omega > \leqslant H\right\} \leqslant \mathscr{J}_5$ and this subgroup will contain all the elements of the form (ρ_3, I) where ρ_3 is a column vector in $\mathbb{Z}^4$ which has even integers as its components, this we can see because $\mathscr{J}_5$ is a Normal Subgroup of $\mathscr{C}_5$ so then $\forall g \in \mathscr{C}_5$ and $\forall h \in \mathscr{J}_5$, $ghg^{-1} \in \mathscr{J}_5$ and the components of ρ_3 are even integers because let's take $g = (c_1, a) \in \mathscr{C}_5$ where $a \in SL_4(\mathbb{Z})$ then $g^{-1} = (-a^{-1}c_1, a^{-1})$, then $g[\theta, \chi^5]g^{-1} = (c_1, a)(\rho_2, I)(-a^{-1}c_1, a^{-1}) = (a\rho_2, I)$ and ρ_2 has even integers as components which implies $a\rho_2$ will also have only even integers as components. That's why the components of ρ_3 are even integers and $(\rho_3, I) \in H$. So which shows $e_{\mathrm{i1}}(2) \in H$ for $2 \leq i \leq 5$. Now we will show that $e_{\mathrm{ij}}(2) \in H$ for $j < i$.

We will use induction on j to prove that $e_{\mathrm{ij}}(2) \in H$ for $1 \leq j < i \leq 5$.

For $j = 1$ it is proved above , now assume it is true for $1 \leq j < i \leq 5$ we will prove it for $1 \leq j+1 < i+1 \leq 5$. From lemma 4.2.1 we know that $\phi^{-1}e_{\mathrm{ij}}(2)e_{\mathrm{i+1,j}}(2)\phi = e_{\mathrm{i+1,j}}(2)e_{\mathrm{i+1,j+1}}(2)$, now we know that $\phi^{-1}e_{\mathrm{ij}}(2)e_{\mathrm{i+1,j}}(2)\phi \in H$ from induction hypothesis and $e_{\mathrm{i+1,j}}(2) \in H$ which simply says that $e_{\mathrm{i+1,j+1}}(2) \in H$ which proves our statement from induction. So we proved that $e_{\mathrm{ij}}(2) \in H$ for $j < i$. Now let's take $\theta^4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 4 & 1 & 0 & 0 & 0 \\ 6 & 4 & 1 & 0 & 0 \\ 4 & 6 & 4 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{bmatrix} \in H$. Which

states that $\theta^4 = e_{21}(2)^2e_{31}(2)^3e_{41}(2)^2e_{51}(1)e_{32}(2)^2e_{42}(2)^3e_{52}(2)^2e_{43}(2)^2e_{53}(2)^3e_{54}(2)^2 \in H$, and we proved that $e_{ij}(2), j < i \in H$ which shows that $e_{51}(1) \in H$. Now $e_{51}(1) = \begin{bmatrix} 1 & 0 \\ \rho_4 & I \end{bmatrix}$ where ρ_4 is the column vector $\begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix}$ so from lemma 4.2.2 if we define the sub-module $\{g\rho_4 : g \in H\}$ of $\mathbb{Z}^4$ then this sub-module will generate the whole $\mathbb{Z}^4$ and now define a set $\{g(\rho_4, I)g^{-1} : g \in < \theta, \omega >\}$ and this set will be a subgroup of $\mathscr{J}_5$ and in this case from lemma 4.2.2 $\{g(\rho_4, I)g^{-1} : g \in < \theta, \omega >\} = \mathscr{J}_5$. This implies that $e_{i1}(1) \in H$ for $2 \leq i \leq 5$. Now as above we proved by using lemma 4.2.1 that $e_{ij}(2) \in H$ for $j < i$ similarly we can prove that $e_{ij}(1) \in H$ for $j < i$. So now ϕ is the transpose of θ so if we use ϕ instead of θ in this proof we will get that $e_{ij}(1) \in H$ for $j > i$ because $H =< \theta, \phi >$. This shows that that the set $\{e_{ij}(1), i \neq j, 1 \leq i, j \leq 5\} \in H$ and H is the subgroup of $SL_5(\mathbb{Z})$ but now from Lemma 4.1.4 , $SL_5(\mathbb{Z}) \subseteq H$ which implies that $H =< \theta, \phi >= SL_5(\mathbb{Z})$.

Now take the case for $n = 3$, similarly define $\chi = \theta^{-1}\omega = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 1 \\ 3 & -1 & 0 \end{bmatrix}$ then $\chi^3 = \begin{bmatrix} 1 & 0 & 0 \\ 2 & -1 & 0 \\ 4 & 0 & -1 \end{bmatrix}$ So $[\theta, \chi^3] = \theta^{-1}\chi^{-3}\theta\chi^3 = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = e_{21}(-2)$ which implies $e_{21}(-2) \in H$ which further implies $e_{21}(2) \in H$ because they are inverse of each other and H is a group.we can see that $e_{21}(2) = \begin{bmatrix} 1 & 0 \\ \rho_5 & I \end{bmatrix}$ where I is a 2×2 identity matrix and ρ_5 is a column vector $\begin{bmatrix} 2 & 0 \end{bmatrix}$ so we can use lemma 4.2.2 as we use in the case of $n = 5$ it will give us that $e_{i1}(2) \in H$ for $i = 2, 3$ and similarly using lemma 4.2.1 we will get that $e_{ij}(2) \in H$ for $j < i$. Now $\theta^2 == \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 2 & 1 \end{bmatrix} = e_{21}(2)e_{32}(2)e_{31}(1)$ which implies that $e_{31}(1) \in H$ now use the same argument which we used in the case of $n = 5$ we will eventually get that $e_{ij}(1) \in H$ for $j < i$ and same as in $n = 5$ we will get $\{e_{ij}(1), i \neq j, 1 \leq i, j \leq 3\} \in H$ which shows that $H =< \theta, \phi >= SL_3(\mathbb{Z})$.

4.4 Generation of $SL_n(\mathbb{Z})$ for $n \geq 6$

Definition 4.4.1. ***Perfect Group:*** *Perfect group is a group in which the commutator subgroup of the group is exactly equal to the group i.e. if G is a Perfect group then $[G, G] = G$.*

Lemma 4.4.1. *$SL_n(\mathbb{Z})$ is a Perfect group for $n \geq 3$.*

Proof. To prove this we will use the commutator relation among elementary matrices of $SL_n(\mathbb{Z})$.If we take i, j, l in such a way that $i \neq j \neq l$ then $[e_{\mathrm{ij}}(1), e_{\mathrm{jl}}(1)] = e_{\mathrm{il}}(1)$ other than this if we have $[e_{\mathrm{ij}}(1), e_{\mathrm{kl}}(1)] = I$ where $j \neq k$. We know that $[SL_n(\mathbb{Z}), SL_n(\mathbb{Z})]$ is always a subgroup of $SL_n(\mathbb{Z})$, so let's take an arbitrary element $\gamma \in SL_n(\mathbb{Z})$ we will prove that $\gamma \in [SL_n(\mathbb{Z}), SL_n(\mathbb{Z})]$ then from lemma 4.1.4 we can write γ as $\gamma = \prod_{i,j} e_{\mathrm{ij}}(1)$ so now for each $e_{\mathrm{ij}}(1)$ i can choose an l in such a way that $i \neq j \neq l$ and $e_{\mathrm{ij}}(1) = [e_{\mathrm{il}}(1), e_{\mathrm{lj}}(1)]$ then each element of product is in the commutator subgroup and $SL_n(\mathbb{Z})$ is a multiplicative group so then it simply proves that $\gamma \in [SL_n(\mathbb{Z}), SL_n(\mathbb{Z})]$ and γ is an arbitrary element of $SL_n(\mathbb{Z})$ so it proves that $SL_n(\mathbb{Z}) = [SL_n(\mathbb{Z}), SL_n(\mathbb{Z})]$ for $n \geq 3$, which at last proves that $SL_n(\mathbb{Z})$ is a perfect group for $n \geq 3$. □

Lemma 4.4.2. *[5, Lemma 3] The group $\mathscr{C}_n$ is perfect for $n \geq 4$.*

Proof. We earlier saw that $\mathscr{C}_n$ contains a Normal subgroup $\mathscr{J}_n$ which simply we can see that it is isomorphic to $\mathbb{Z}^{n-1}$ and $\mathscr{C}_n/\mathscr{J}_n$ is isomorphic to $SL_{n-1}(\mathbb{Z})$ (from first isomorphism Theorem of groups applied on the map η) and we proved the fact that $SL_n(\mathbb{Z})$ is a perfect group for $n \geq 3$ which implies that $SL(n-1, \mathbb{Z})$ is a perfect group for $n \geq 4$. So $\mathscr{C}_{\mathrm{n}}/\mathscr{J}_{\mathrm{n}}$ is a Perfect group for $n \geq 4$. This means that $[\mathscr{C}_{\mathrm{n}}/\mathscr{J}_{\mathrm{n}}, \mathscr{C}_{\mathrm{n}}/\mathscr{J}_{\mathrm{n}}] = \mathscr{C}_{\mathrm{n}}/\mathscr{J}_{\mathrm{n}}$ so now if i take an element $M \in \mathscr{C}_n$ and define $[\mathscr{C}_n, \mathscr{C}_n] = \mathscr{C}'_n$. Now $M \in \mathscr{C}_{\mathrm{n}}$ that's why $M\mathscr{J}_{\mathrm{n}} \in \mathscr{C}_{\mathrm{n}}/\mathscr{J}_{\mathrm{n}}$ and we have the fact that $\mathscr{C}_n/\mathscr{J}_n$ is a perfect group for $n \geq 4$ which means $\exists \;\; P\mathscr{J}_n$ and $Q\mathscr{J}_n$ such that $[P\mathscr{J}_n, Q\mathscr{J}_n] = M\mathscr{J}_n$. This implies that $P^{-1}Q^{-1}PQ\,\mathscr{J}_n = M\mathscr{J}_n$ which means $M^{-1}P^{-1}Q^{-1}PQ \in \mathscr{J}_n$ so we can take an element $j_n \in \mathscr{J}_n$ so that $j_n = M^{-1}P^{-1}Q^{-1}PQ \implies M = P^{-1}Q^{-1}PQj_n^{-1}$ which says $M = [P, Q]j_n^{-1}$ and M was an arbitrary element of $\mathscr{C}_n$ that proves that $\mathscr{C}_n = [\mathscr{C}_n, \mathscr{C}_n]\mathscr{J}_n \implies \mathscr{C}_n = \mathscr{C}'_n\mathscr{J}_n$. Now if we prove that $\mathscr{J}_n$ is a subgroup of $\mathscr{C}'_n$ then we are done. As we previously state that we can write elements of $\mathscr{C}_n$ as ordered pairs (u, a) where $u \in \mathbb{Z}^{n-1}$ and $a \in SL_{n-1}(\mathbb{Z})$. Now we have $(u, I)^{-1}(0, a^{-1})(u, I)(0, a) = (a^{-1}u - u, I)$. So let's take $u_1, u_2, ..., u_{n-1}$ are free generators

of $\mathscr{J}_n$ so let's take u to be u_1 where $u_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ and a^{-1} to be $e_{i1}(1)$ where $2 \leq i \leq n-1$. Then $(u_1, I)^{-1}(0, e_{i1}(1))(u_1, I)(0, e_{i1}(-1)) = (u_i, I)$ for $2 \leq i \leq n-1$ which also shows that $(u_i, I) \in \mathscr{C}'_n$ for $2 \leq i \leq n-1$. Now if we take $u = u_2$ and $a^{-1} = e_{12}(1)$ then it shows that (u_1, I) is also a commutator , but (u_i, I) for $1 \leq i \leq n-1$ generates $\mathscr{J}_n$ and that proves $\mathscr{J}_n$ is a subgroup of $\mathscr{C}'_n$ which states that $\mathscr{C}_n = \mathscr{C}'_n = [\mathscr{C}_n, \mathscr{C}_n]$ which shows that $\mathscr{C}_{\mathrm{n}}$ is a perfect group for $n \geq 4$. □

4.4.1 Proof Of Theorem 4.0.1 when $n \geq 6$

The proof in the following section follows very closely to that of Theorem 2 of [5].

We will proceed by induction on n, so the theorem is true for $n = 5$ by previous section and assume the theorem is true for $k = n-1$. Intially we defined the surjection $\eta : \mathscr{C}_n \to SL_{n-1}(\mathbb{Z})$ given by $\eta(u, a) = a$ and $\ker\eta = \mathscr{J}_n$. Let $\mathscr{K}_n$ be the subgroup of $\mathscr{C}_n$ generated by θ and ω So the way θ and ω are defined in previous sections we can clearly see that $\eta(\theta)$ and $\eta(\omega)$ are the elements of $SL_{n-1}(\mathbb{Z})$ that are the $(n-1) \times (n-1)$ analogue of θ and ϕ. So from induction hypothesis $\eta(\theta)$ and $\eta(\omega)$ will generate $SL_{n-1}(\mathbb{Z})$ and thus $\eta(\mathscr{K}_n) = \eta(\mathscr{C}_n)$. Now we prove the following lemma:

Lemma 4.4.3. $\mathscr{J}_n\mathscr{K}_n = \mathscr{C}_n$

Proof. So we know that $\mathscr{J}_n\mathscr{K}_n \subseteq \mathscr{C}_n$. Now let's take an element $(v, a) \in \mathscr{C}_n$ we will prove that $(v, a) \in \mathscr{J}_n\mathscr{K}_n$ so to prove this we can write $(v, a) = (v_1, I)(v_2, a)$ and the way the multiplication of these ordered pairs are defined we have to choose our v_2 in such a way so that $v_1 + v_2 = v$ and $(v_2, a) \in \mathscr{K}_n$ and we know that $a \in SL_{n-1}(\mathbb{Z})$ and from induction hypothesis $SL_{n-1}(\mathbb{Z})$ is generated by $\eta(\theta)$ and $\eta(\omega)$ so $a = \eta(\theta)^i\eta(\omega)^j$ so $(v_2, a) = (v_2, \eta(\theta)^i\eta(\omega)^j)$ and in section 4.2.1 we saw that $\theta = (s, \theta_1) = (s, \eta(\theta))$ and $\omega = (f, phi_1) = (f, \eta(\omega))$ so let's take the element $\theta^i\omega^j = \prod_{n=1}^{n=i}(s, \eta(\theta)^n)\prod_{m=1}^{m=j}(f, \eta(\omega)^m) = (s + \eta(\theta)s + \eta(\theta)^2 s + ... + \eta(\theta)^{i-1}s, \eta(\theta)^i)(f + \eta(\omega)f + \eta(\omega)^2 f + ... + \eta(\omega)^{j-1}f, \eta(\omega)^j)$.

which implies that $\theta^i\omega^j = (s+\eta(\theta)s+\eta(\theta)^2 s+.....+\eta(\theta)^{i-1}s+\eta(\theta)^i(f+\eta(\omega)f+\eta(\omega)^2 f+$

$..... + \eta(\omega)^{j-1}f), \eta(\theta)^i\eta(\omega)^j)$.

so we will choose our v_2 as $v_2 = s + \eta(\theta)s + \eta(\theta)^2 s + ... + \eta(\theta)^{i-1}s + \eta(\theta)^i(f + \eta(\omega)f + \eta(\omega)^2 f + ... + \eta(\omega)^{j-1}f)$ taking this vector as v_2 it will give us that $(v_2, a) = \theta^i\omega^j$ which implies that $(v_2, a) \in \mathscr{K}_n$ because $\mathscr{K}_n =< \theta, \omega >$ and $v_1 = v - v_2$ and $(v_1, I) \in \mathscr{J}_n \implies (v, a) \in \mathscr{J}_n\mathscr{K}_n$ which implies that $\mathscr{C}_n \subseteq \mathscr{J}_n\mathscr{K}_n$ which ultimately shows that $\mathscr{C}_n = \mathscr{J}_n\mathscr{K}_n$. □

Now Let $\mathscr{C}_{n-1}$ be the subgroup of $SL_{n-1}(\mathbb{Z})$ same as $\mathscr{C}_n$ subgroup of $SL_n(\mathbb{Z})$. Now let $\mathscr{E}_n$ be the preimage of $\mathscr{C}_{n-1}$ in $\mathscr{K}_n$ which implies that $\mathscr{E}_n \leqslant \mathscr{K}_n$, now the preimage of $\mathscr{C}_{n-1}$ under the map η in $\mathscr{C}_n$ will contain in a subgroup $\mathscr{T}$ of $\mathscr{C}_n$ which will have elements of the type $\begin{bmatrix} G(b) & 0 \\ J & R \end{bmatrix}$ where $b \in \mathbb{Z}$, $G(b)$ is a 2×2 matrix and $G(b) = e_{21}(b)$, J is a $(n-2) \times 2$ matrix and $R \in SL_{n-2}(\mathbb{Z})$. Now as we saw earlier that $\eta(\mathscr{K}_n) = \eta(\mathscr{C}_n)$ similarly, the way $\mathscr{E}_n$ and $\mathscr{T}$ defined and because η is onto that's why we will have $\eta(\mathscr{E}_n) = \eta(\mathscr{T}) = \mathscr{C}_{n-1}$. Now if we see the group $\mathscr{J}_n$ is in the group $\mathscr{T}$ means $\mathscr{J}_n \leqslant \mathscr{T}$ with $R = I$. So then from lemma 4.4.3, $\mathscr{T} = \mathscr{J}_n\mathscr{E}_n$.

Now Let's define a map, $\beta : \mathscr{T} \to \mathbb{Z}$

$$\begin{bmatrix} G(b) & 0 \\ J & R \end{bmatrix} \to b$$

the map β is a surjective homomorphism considering $\mathscr{T}$ as a multiplicative group and $\mathbb{Z}$ as an additive group which means $\beta(de) = \beta(d) + \beta(e)$. Now take the commutator $[\mathscr{T}, \mathscr{T}] \leqslant \mathscr{T}$ and let's say $t \in \mathscr{T}$ then we can easily see that $\beta([t, t]) = 0$ and we have that $\mathscr{E}_n \leqslant \mathscr{T}$ so it says that $[\mathscr{E}_n, \mathscr{E}_n] \leqslant [\mathscr{T}, \mathscr{T}] \leqslant ker\beta$ and $\eta([\mathscr{E}_n, \mathscr{E}_n]) = [\eta(\mathscr{E}_n), \eta(\mathscr{E}_n)] = [\mathscr{C}_{n-1}, \mathscr{C}_{n-1}]$ but from lemma 4.4.2 we have that $\mathscr{C}_n$ is a perfect group for $n \geq 4$ so $[\mathscr{C}_{n-1}, \mathscr{C}_{n-1}] = \mathscr{C}_{n-1}$. Let's denote $[\mathscr{C}_n, \mathscr{C}_n] = \mathscr{C}'_n$ then $\eta(\mathscr{E}'_n) = \mathscr{C}_{n-1}$ and then it follows that $\mathscr{T} = \mathscr{J}_n\mathscr{E}'_n$.

Now $\theta \in \mathscr{T}$ with $b = 1$ so $\beta(\theta) = 1$ and let's say $\exists y \in \mathscr{J}_n$ and $q \in \mathscr{E}'_n$ so that $\theta = yq$ and $\beta(\theta) = \beta(yq) = \beta(y) + \beta(q)$ but $q \in \mathscr{E}'_n$ and that's why $\beta(q) = 0$ which implies $\beta(y) = 1$ and $\theta \in \mathscr{K}_n$ and $q \in \mathscr{E}'_n \leqslant \mathscr{E}_n \leqslant \mathscr{K}_n$, which implies $y \in \mathscr{J}_n \cap \mathscr{K}_n$ so $y \in \mathscr{J}_n$ such that $\beta(y) = 1$ so this says that $y = (z, I)$ where $z \in \mathbb{Z}^{n-1}$ and $z = \begin{bmatrix} 1, ... \end{bmatrix}'$ so from lemma 4.2.2 the sub-module $\{gz : g \in \mathscr{K}_n\}$ will generate module $\mathbb{Z}^n$ and the set $\{gyg^{-1} : g \in \mathscr{K}_n\}$ is a subgroup of $\mathscr{K}_n$ because $y \in \mathscr{K}_n$ and also subgroup of $\mathscr{J}_n$ but because of lemma 4.2.2

this subgroup will generate $\mathscr{J}_n$ so that implies $\mathscr{J}_n \leqslant \mathscr{K}_n$. From the map η and from first isomorphism theorem of groups we have $\mathscr{K}_n/\mathscr{J}_n \cap \mathscr{K}_n \cong SL_{n-1}(\mathbb{Z})$ but $\mathscr{J}_n \cap \mathscr{K}_n = \mathscr{J}_n$ so we have $\mathscr{K}_n/\mathscr{J}_n \cong SL_{n-1}(\mathbb{Z})$ but we also have $\mathscr{C}_n/\mathscr{J}_n \cong SL_{n-1}(\mathbb{Z})$ this implies that $\mathscr{C}_n = \mathscr{K}_n$.

Which says that $\mathscr{C}_n =< \theta, \omega > \leqslant H$. Now the way $\mathscr{C}_n$ is defined it contains all the elementary matrices of the form $e_{i1}(1)$ for $2 \leq i \leq n$ which implies that $e_{i1}(1) \in H$ for $2 \leq i \leq n$ and then from lemma 4.2.1 we can see that $e_{ij}(1) \in H$ for $i > j$. Now $H =< \theta, \phi >$ and we have $\phi = \theta^{\intercal}$, so the group H will contain all the transpose of its elements which implies that $\{e_{ij}(1), 1 \leq i, j \leq n, i \neq j\} \in H$ so from lemma 4.1.4 we can see that $H =< \theta, \phi >= SL_n(\mathbb{Z})$ for $n \geq 6$.

So in this way we proved Theorem 4.0.1.

4.5 The group generated by θ and ϕ when $n = 4$

When we stated Theorem 4.0.1 we stated that θ and ϕ will generate the whole $SL_n(\mathbb{Z})$ except the case of $n = 4$ so in this section we will see which type of subgroup of $SL_4(\mathbb{Z})$, θ and ϕ will generate , what are the properties of that subgroup.

Lemma 4.5.1. *[5, Lemma 4] In the case of $n = 4$,the set $\{e_{ij}(2), 1 \leq i \neq j \leq 4\} \in H$, where H is the subgroup of $SL_4(\mathbb{Z})$ generated by θ and ϕ.*

Proof. In this case also let's define $\chi = \theta^{-1}\omega = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 1 & 0 \\ 3 & -1 & 0 & 1 \\ -4 & 1 & 0 & 0 \end{bmatrix}$ now χ^4 has the form:

$$\chi^4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -6 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 1 \end{bmatrix}$$

$\implies \chi^4 = (v, I) \in \mathscr{C}_4$ where v is the column vector $\begin{bmatrix} -6 & 0 & 6 \end{bmatrix}$ so similarly as we got in section 4.3 using lemma 4.2.2 we will get that $(\rho_6, I) \in H$ where vector ρ_6 will have

integers divisible by 6 as its components.Which implies $e_{i1}(6) \in H$ for $2 \leq i \leq 4$ and then using lemma 4.2.1 , $e_{ij}(6) \in H$ for $i > j$. Now take $\theta^{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 12 & 1 & 0 & 0 \\ 66 & 12 & 1 & 0 \\ 220 & 66 & 12 & 1 \end{bmatrix} \implies$ $\theta^{12} = e_{21}(6)^2 e_{31}(6)^{11} e_{32}(6)^2 e_{41}(6)^{37} e_{41}(-2) e_{42}(6)^{11} e_{43}(6)^2 \in H$. We proved that $e_{ij}(6)$ for $i > j \in H \implies e_{41}(-2) \in H$,then $e_{41}(2) \in H$. Then from lemma 4.2.2, $e_{i1}(2) \in H$ for $2 \leq i \leq 4$ and in the same way as we did in previous sections from lemma 4.2.1, $e_{ij}(2) \in H$ for $i > j$ and $H =< \theta, \phi >$ and $\phi = \theta^{\intercal}$ so if $M \in H$ then $M^{\intercal} \in H$ so it implies that $e_{ij}(2) \in H$ for $i < j$ which implies the set $\{e_{ij}(2), i \neq j, 1 \leq i, j \leq 4\} \in H$. □

Define a map $\psi_2 : SL_4(\mathbb{Z}) \to SL_4(\mathbb{Z}/2\mathbb{Z})$ which is just sending to the matrix of $SL_4(\mathbb{Z})$ to its equivalence class in $SL_4(\mathbb{Z}/2\mathbb{Z})$. This map is clearly surjective so now if we talk about the kernel of this map it will be :

Ker$\psi_2 = \{M \in SL_4(\mathbb{Z}) \mid \psi_2(M) = I\}$ so if $M \in Ker\psi_2$, then M will have following matrix form:

$$M_{ij} = \begin{cases} 1 & \text{when } i = j \\ 2a & \text{otherwise} \end{cases} \text{ where } a \in \mathbb{Z}.$$

So if we take $e_{ij}(2)$ for $i \neq j$ will contain in Kerψ_2 and also if we take any arbitrary element of Kerψ_2 that can be written as product of powers of $e_{ij}(2)$ which simply implies that Ker$\psi_2 =< e_{ij}(2), 1 \leq i \neq j \leq 4 > \implies$ Ker$\psi_2 \leqslant H$. So it means that Kerψ_2 is contained in H which is the subgroup of $SL_4(\mathbb{Z})$ generated by θ and ϕ.

Theorem 4.5.2. *[5, Theorem 3] The subgroup H of $SL_4(\mathbb{Z})$ which is generated by θ and ϕ has index 8 in $SL_4(\mathbb{Z})$.*

Proof. We know that Ker$\psi_2 \leqslant H \leqslant SL_4(\mathbb{Z})$ and from first isomorphism theorem of Groups we have that $SL_4(\mathbb{Z})/Ker\psi_2 \cong SL_4(\mathbb{Z}/2\mathbb{Z})$. So index of Ker$\psi_2$ in $SL_4(\mathbb{Z})$ is the cardinality of $SL_4(\mathbb{Z}/2\mathbb{Z})$ and that will be $(2^4 - 1)(2^4 - 2)(2^4 - 2^2)(2^4 - 2^3)$ and we have a fact that $H/$Ker$\psi_2 \cong A_7$ where A_7 is the alternating group which is the subgroup of symmetric group S_7 and it has cardinality $\frac{7!}{2}$ So $[SL_4(\mathbb{Z}) : H] = \frac{[SL_4(\mathbb{Z}):Ker\psi_2]}{[H:Ker\psi_2]}$

Which implies that $[SL_4(\mathbb{Z}) : H] = \frac{15 \times 14 \times 12 \times 8 \times 2}{7!} = 8$

Which proves that the subgroup H of $SL_4(\mathbb{Z})$ which is generated by θ and ϕ has index 8 in $SL_4(\mathbb{Z})$. $\square$

Chapter 5

Steinberg Generators for Symplectic Group $Sp(2l, k)$

In this chapter we will study two generation of the Symplectic Group $Sp(2l, k)$ ($char(k) \neq 2$). It means that 2 elements can generate $Sp(2l, k)$. For this first we will define all the elementary matrices of $Sp(2l, k)$ and then we will show that those elementary matrices will generate $Sp(2l, k)$. Then we will prove the Two Generation of $Sp(2l, k)$.

Notation: $k = \mathbb{F}_q$; a finite field with q elements.

5.1 Symplectic Group $Sp(2l, k)$

We defined Symplectic Group in Chapter 1 ,so now in this section we will define Symplectic Group with $B = \begin{bmatrix} 0 & I_l \\ -I_l & 0 \end{bmatrix}$ where B is the matrix associated to the non-degenerate skew-symmetric Bilinear form β as defined in Chapter 1.

So now as defined in the Chapter 1, let's take the dimension of the Vector space V , an odd number then the matrix associated to β which is B will also have an odd order and we know that B is skew-symmetric and an odd order skew-symmetric matrix will have determinant 0. So if β is skew-symmetric and non-degenerate then the $dimV$ has to be even ,so let's take $dim(V) = 2l$, then size of the matrix will also be $(2l \times 2l)$ and let's denote the first l rows

and l columns as $\{1, 2, 3, ..., l\}$ and $l+1$ to $2l$ rows and columns as $\{-1, -2, ... - l\}$.

Then let's fix the basis of V as standard basis $\{u_1, u_2, ...u_l, u_{-1}, u_{-2}, ...u_{-l}\}$ where basis vector u_i is defined as follows:

$$u_i = \begin{cases} 1 & \text{at ith postion} \\ 0 & \text{otherwise} \end{cases}$$

then with respect to this basis we can always find the matrix associated to skew-symmetric and non-degenerate bilinear form β as $B = \begin{bmatrix} 0 & I_l \\ -I_l & 0 \end{bmatrix}$ where B is a $(2l \times 2l)$ matrix and I_l is a $l \times l$ identity matrix.

Definition 5.1.1. ***Symplectic Group*** *$Sp(2l, k)$: Symplectic Group defined with the $B = \begin{bmatrix} 0 & I_l \\ -I_l & 0 \end{bmatrix}$ over a finite field k is denoted as $Sp(2l, k)$.*

In this chapter we will just deal with this Symplectic Group $Sp(2l, k)$.

For section 5.2 and 5.3 Reference is [1].

5.2 Elementary Matrices of $Sp(2l, k)$

We are denoting rows by $1, 2, ..., l, -1, -2, ..., -l$. Now take $l \geq 2, t \in k$

Then in this chapter we are defining $e_{i,j}$ (a $2l \times 2l$ matrix) as follows:

$$e_{i,j} = \begin{cases} 1 & \text{at } ijth \text{ postion} \\ 0 & \text{otherwise} \end{cases}$$

. Now following are the elementary matrices of $Sp(2l, k)$ where, $1 \leq i \leq l,\ 1 \leq j \leq l$:

$$\Psi_{i,j}(t) = I + t(e_{i,j} - e_{-j,-i}),\ i \neq j$$

$$\Psi_{i,-j}(t) = I + t(e_{i,-j} + e_{j,-i}),\ i < j$$

$$\Psi_{-i,j}(t) = I + t(e_{-i,j} + e_{-j,i}),\ i < j$$

$$\Psi_{i,-i}(t) = I + te_{i,-i}$$

$$\Psi_{-i,i}(t) = I + te_{-i,i}$$

So if we write them in matrix form using block diagonal notations , there will be following Elementary matrices :

$Q1 : \begin{bmatrix} S & 0 \\ 0 & (S^\intercal)^{-1} \end{bmatrix}$ where $S = I + te_{ij};\ i \neq j$ and S is a $l \times l$ matrix.

$Q2 : \begin{bmatrix} I & S \\ 0 & I \end{bmatrix}$ where S is either $t(e_{ij} + e_{ji})$; $i < j$ or $te_{i,i}$

$Q3 : \begin{bmatrix} I & 0 \\ S & I \end{bmatrix}$ where S is either $t(e_{ij} + e_{ji})$; $i < j$ or $te_{i,i}$

5.2.1 Elementary Operation for $Sp(2l, k)$

In this section we will see how the above defined elementary matrices of $Sp(2l, k)$ will effect an arbitrary element of $Sp(2l, k)$.

Now let $h = \begin{bmatrix} M & N \\ T & P \end{bmatrix} \in Sp(2l, k)$ where M, N, T, P all are $l \times l$ matrices.Elementary Operations are:

ER1: $\begin{bmatrix} S & 0 \\ 0 & (S^\intercal)^{-1} \end{bmatrix} \begin{bmatrix} M & N \\ T & P \end{bmatrix} = \begin{bmatrix} SM & SN \\ (S^\intercal)^{-1}T & (S^\intercal)^{-1}P \end{bmatrix}$

EC1: $\begin{bmatrix} M & N \\ T & P \end{bmatrix} \begin{bmatrix} S & 0 \\ 0 & (S^\intercal)^{-1} \end{bmatrix} = \begin{bmatrix} MS & N(S^\intercal)^{-1} \\ TS & P(S^\intercal)^{-1} \end{bmatrix}$

ER2: $\begin{bmatrix} I & S \\ 0 & I \end{bmatrix} \begin{bmatrix} M & N \\ T & P \end{bmatrix} = \begin{bmatrix} M + ST & N + SP \\ T & P \end{bmatrix}$

EC2: $\begin{bmatrix} M & N \\ T & P \end{bmatrix} \begin{bmatrix} I & S \\ 0 & I \end{bmatrix} = \begin{bmatrix} M & MS + N \\ T & TS + P \end{bmatrix}$

ER3: $\begin{bmatrix} I & 0 \\ S & I \end{bmatrix} \begin{bmatrix} M & N \\ T & P \end{bmatrix} = \begin{bmatrix} M & N \\ SM+T & SN+P \end{bmatrix}$

EC3: $\begin{bmatrix} M & N \\ T & P \end{bmatrix} \begin{bmatrix} I & 0 \\ S & I \end{bmatrix} = \begin{bmatrix} M+NS & N \\ T+PS & P \end{bmatrix}$

5.3 Generation of $Sp(2l,k)$ by Elementary Matrices:

Theorem 5.3.1. *[1, 4.1] Symplectic Group $Sp(2l,k)$ is generated by the elementary matrices* $\{\Psi_{i,j}(t); i \neq j, \Psi_{i,-j}(t); i < j, \Psi_{-i,j}(t); i < j, \Psi_{i,-i}(t), \Psi_{-i,i}(t) \mid t \in k\}$.

Proof. Now let's take $h = \begin{bmatrix} M & N \\ T & P \end{bmatrix} \in Sp(2l,k)$ so it's a $2l \times 2l$ matrix. We will prove that h which is an arbitrary element of $Sp(2l,k)$ is product of the elementary matrices defined in section 5.1 . We also note that the inverse of an elementary matrix is also an elementary matrix.

First Step: h will be converted into $h_1 = \begin{bmatrix} M_1 & N_1 \\ T_1 & P_1 \end{bmatrix}$ by elementary matrices:

So let's see the effect of ER1 and EC1 on the block M.It changes M to SM where $S = I + te_{ij}$. There are 2 cases , first if M is invertible $l \times l$ matrix and second is that M is not an invertible matrix.So take the first case:

(i)**Block M is Invertible:** In this case we will prove that by multiplying S to M for different i, j we will get a matrix M_1 which will have the following form:$M_1 = diag(1, 1, 1, ..., \mu)$ where $\mu \neq 0$.

Lemma 5.3.2. $\prod_{i,j} SM = M_1$ *where* $M_1 = diag(1, 1, 1, ..., \mu)$.

Proof. We know that M is a $l \times l$ matrix and we will prove the lemma by applying induction on l so let's take $l = 2$, then $M = \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}$ and in this case $S = I + te_{ij}$ where $1 \leq i \leq 2, 1 \leq j \leq 2,\ i \neq j$

so let's take $S_1 = I + (-a_1 b_1^{-1})e_{12}$ then $S_1 M = \begin{bmatrix} 0 & a_2 - a_1 b_2 b_1^{-1} \\ b_1 & b_2 \end{bmatrix}$ we can take $a_2 -$

$a_1 b_2 b_1^{-1} = \mu_1 \in k$ then $S_1 M = \begin{bmatrix} 0 & \mu_1 \\ b_1 & b_2 \end{bmatrix}$.Now take $S_2 = I + (-b_2 \mu_1^{-1}) e_{21}$ then $S_2 S_1 M = \begin{bmatrix} 0 & \mu_1 \\ b_1 & 0 \end{bmatrix}$.Now let's take $S_3 = (I + e_{21})(I - e_{12})(I + e_{21}) = e_{21} - e_{12} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ then $S_3 S_2 S_1 M = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & \mu_1 \\ b_1 & 0 \end{bmatrix} = \begin{bmatrix} -b_1 & 0 \\ 0 & \mu_1 \end{bmatrix}$ Now take $S_4 = (I - b_1^{-1} e_{12})(I + b_1 e_{21})(I - b_1^{-1} e_{21})(I - e_{12})(I + e_{21})(I - e_{12}) = \begin{bmatrix} -b_1^{-1} & 0 \\ 0 & -b_1 \end{bmatrix}$. So now $S_4 S_3 S_2 S_1 M = \begin{bmatrix} 1 & 0 \\ 0 & -b_1 \mu_1 \end{bmatrix}$ and we can take $-b_1 \mu_1 = \mu$, so then; $S_4 S_3 S_2 S_1 M = \begin{bmatrix} 1 & 0 \\ 0 & \mu \end{bmatrix}$

which shows our statement is true for $l = 2$.

Assume the lemma is true for $l - 1$. Now take the case when M is a $l \times l$ matrix then $M = \begin{bmatrix} a_1 & a_2 & \cdots & a_l \\ \vdots & \vdots & \ddots & \vdots \\ l_1 & l_2 & \cdots & l_l \end{bmatrix}$ now if we apply $S = I + te_{ij}$ on M with the condition that $1 \leq i, j \leq l - 1$ then it is equivalent to applying on a $l - 1 \times l - 1$ matrix and then from induction hypothesis these operations will change M to $M' = \begin{bmatrix} 1 & 0 & \cdots & 0 & a_l \\ 0 & 1 & \cdots & 0 & b_l \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & \mu_1 & k_l \\ l_1 & l_2 & \cdots & l_{l-1} & l_l \end{bmatrix}$. Now

Take $S_1 = I - l_1 e_{l,1}$ and $S_1 M' = \begin{bmatrix} 1 & 0 & \cdots & 0 & a_l \\ 0 & 1 & \cdots & 0 & b_l \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & \mu_1 & k_l \\ 0 & l_2 & \cdots & l_{l-1} & l_l - a_l l_1 \end{bmatrix}$

Now take $S_i = I - l_1 e_{l,i}$ for $1 \leq i \leq l - 1$ and

evaluate $\prod_{i=1}^{i=l-1} S_i M' = \begin{bmatrix} 1 & 0 & \cdots & 0 & a_l \\ 0 & 1 & \cdots & 0 & b_l \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & \mu_1 & k_l \\ 0 & 0 & \cdots & 0 & \mu' \end{bmatrix}$ where $\mu' = l_l - a_l l_1 - b_l l_2 - ..... - k_l l_{l-1}$.

In the same way we can make $a_l, b_l, ...k_l$ all entries zero by appropriate elementary operations and we will get:

$$M'' = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & \mu_1 & 0 \\ 0 & 0 & \cdots & 0 & \mu' \end{bmatrix} = diag(1, 1, ..., \mu_1, \mu')$$

now take $S = (I + \mu_1^{-1} e_{l-1,l})(I - \mu_1 e_{l,l-1})(I + \mu_1^{-1} e_{l-1,l})(I - e_{l-1,l})(I + e_{l,l-1})(I - e_{l-1,l}) = diag(1, 1, ..., \mu_1^{-1}, \mu_1)$. So $SM'' = diag(1, 1, ...1, \mu_1\mu')$; so we can take $\mu_1\mu' = \mu \neq 0$ which implies $SM'' = diag(1, 1, ..., \mu) = M_1$ which proved our lemma. □

Now because we are observing the effect of ER1 and EC1 on h so it will also affect the block T because it will change T to $(S^\intercal)^{-1}T$. Now we will prove that these elementary operations will change T to T_1 where $T_1 = \begin{bmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{bmatrix}$ where T_{11} is a $l-1 \times l-1$ symmetric matrix and $T_{12} = \mu T_{21}^\intercal$. To prove this we will prove following lemma:

Lemma 5.3.3. *[1, Lemma 4.1] If $A = diag(1, 1, .., 1, \mu, \mu, ...\mu)$ is a matrix of size l and number of 1s equal to $m < l$ and $\mu \neq 0$. Then let's say we have a matrix X such that AX is symmetric then $X = \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}$ where X_{11} will be a $m \times m$ symmetric matrix and $X_{12} = \mu X_{21}^\intercal$.*

Proof. Now $AX = \begin{bmatrix} X_{11} & X_{12} \\ \mu X_{21} & \mu X_{22} \end{bmatrix}$, but AX is symmetric so $(AX)^\intercal = AX \implies \begin{bmatrix} X_{11}^\intercal & \mu X_{21}^\intercal \\ X_{12}^\intercal & \mu X_{22}^\intercal \end{bmatrix} = \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}$ so $X_{11}^\intercal = X_{11}$ which shows that X_{11} is symmetric

and $X_{12} = \mu X_{21}^\intercal$. □

Now in The first step we wrote that we will get $h_1 = \begin{bmatrix} M_1 & N_1 \\ T_1 & P_1 \end{bmatrix}$ from h and $h_1 \in Sp(2l, k)$ so from the definition of $Sp(2l, k)$ we will have $h_1^\intercal B h_1 = B$ so which implies that $\begin{bmatrix} M_1^\intercal & T_1^\intercal \\ N_1^\intercal & P_1^\intercal \end{bmatrix} \begin{bmatrix} 0 & I_l \\ -I_l & 0 \end{bmatrix} \begin{bmatrix} M_1 & N_1 \\ T_1 & P_1 \end{bmatrix} = \begin{bmatrix} 0 & I_l \\ -I_l & 0 \end{bmatrix}$; after solving this matrix equation

we will get $M_1^\intercal T_1 = T_1^\intercal M_1$ but we get $M_1 = diag(1, 1, ..., \mu)$ so $M_1^\intercal = M_1$ so we will get $M_1T_1 = T_1^\intercal M_1^\intercal \implies M_1T_1 = (M_1T_1)^\intercal$ which shows that M_1T_1 is symmetric and $M_1 = diag(1, 1, ..., \mu)$. So from lemma 5.2.3 we will get that $T_1 = \begin{bmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{bmatrix}$ where T_{11} is a $l-1 \times l-1$ symmetric matrix and $T_{12} = \mu T_{21}^\intercal$.

So in the **First Step** (i) we got $h_1 = \begin{bmatrix} M_1 & N_1 \\ T_1 & P_1 \end{bmatrix}$ where $M_1 = diag(1, 1, ..., \mu)$ where $\mu \neq 0$ and $T_1 = \begin{bmatrix} T_{11} & \mu T_{21}^\intercal \\ T_{21} & T_{22} \end{bmatrix}$ where T_{11} is a $l-1 \times l-1$ symmetric matrix.

(ii) Block M is not invertible: In this case also we will apply ER1 and EC1 on h in the same way as in the case (i) but because M is not invertible so there will be some rows and columns which will be linearly dependent on other rows or columns so when we will apply these elementary operations on M , then that many rows will become zero and that number will depend upon the rank and let's say $rank(M) = m$ then in this case M_1 will be $M_1 = diag(1, 1, ..., 1, 0, 0, ..., 0)$ where no of $1s$ will be $m < l$.

In this case also M_1T_1 is symmetric and let's say $T_1 = \begin{bmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{bmatrix}$ then $M_1T_1 = (M_1T_1)^\intercal \implies \begin{bmatrix} T_{11} & T_{12} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} T_{11}^\intercal & 0 \\ T_{12}^\intercal & 0 \end{bmatrix}$ which says that T_{11} is a $m \times m$ symmetric matrix and $T_{12} = 0$ so $T_1 = \begin{bmatrix} T_{11} & 0 \\ T_{21} & T_{22} \end{bmatrix}$ where T_{11} is a $m \times m$ symmetric matrix.

So in the **First Step** (ii) we got $h_1 = \begin{bmatrix} M_1 & N_1 \\ T_1 & P_1 \end{bmatrix}$ where $M_1 = diag(1, 1, .., 1, 0, 0, ..., 0)$ where no of $1s$ equal to $m < l$ and $T_1 = \begin{bmatrix} T_{11} & 0 \\ T_{21} & T_{22} \end{bmatrix}$ where T_{11} is a $m \times m$ symmetric matrix.

Second Step: h_1 will be converted into $h_2 = \begin{bmatrix} M_2 & N_2 \\ 0 & (M_2^\intercal)^{-1} \end{bmatrix}$ by elementary matrices ; where $M_2 = diag(1, 1, ..., 1, \mu'')$:

(i) When $M_1 = diag(1, 1, ..., \mu)$ and $T_1 = \begin{bmatrix} T_{11} & \mu T_{21}^\intercal \\ T_{21} & T_{22} \end{bmatrix}$ We will observe the effect of

ER3 on the block T_1, because ER3: $\begin{bmatrix} I & 0 \\ S & I \end{bmatrix} \begin{bmatrix} M_1 & N_1 \\ T_1 & P_1 \end{bmatrix} = \begin{bmatrix} M_1 & N_1 \\ SM_1 + T_1 & SN_1 + P_1 \end{bmatrix}$ so let's see the effect on T_1 it changes it into $SM_1 + T_1$ where $S = t(e_{i,j} + e_{j,i})$; $i < j$ or $te_{i,i}$ and $M_1 = diag(1, 1, ..., \mu)$. Let's define $T_{11} = \begin{bmatrix} a_1 & \cdots & a_{l-1} \\ b_1 & \cdots & b_{l-1} \\ \vdots & \ddots & \vdots \\ k_1 & \cdots & k_{l-1} \end{bmatrix}$ a $l-1 \times l-1$ symmetric matrix and $T_{21} = \begin{bmatrix} \lambda_1 & \cdots & \lambda_{l-1} \end{bmatrix}$; then $T_{12} = \mu T_{21}^{\intercal}$ then $T_1 = \begin{bmatrix} a_1 & \cdots & a_{l-1} & \mu\lambda_1 \\ b_1 & \cdots & b_{l-1} & \mu\lambda_2 \\ \vdots & \ddots & \vdots & \vdots \\ k_1 & \cdots & k_{l-1} & \mu\lambda_{l-1} \\ \lambda_1 & \cdots & \lambda_{l-1} & d \end{bmatrix}$ let's take $S = (-a_1)e_{1,1}$ then $SM_1 + T_1 = \begin{bmatrix} 0 & \cdots & a_{l-1} & \mu\lambda_1 \\ b_1 & \cdots & b_{l-1} & \mu\lambda_2 \\ \vdots & \ddots & \vdots & \vdots \\ k_1 & \cdots & k_{l-1} & \mu\lambda_{l-1} \\ \lambda_1 & \cdots & \lambda_{l-1} & d \end{bmatrix}$ so now in this way we can do multiply by these elementary matrices and change T_1 to $T_1' = \begin{bmatrix} 0 & \cdots & 0 & \mu\lambda_1 \\ 0 & \cdots & 0 & \mu\lambda_2 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \mu\lambda_{l-1} \\ 0 & \cdots & 0 & 0 \end{bmatrix}$ now take $S = (-\lambda_1)e_{1,l}$ then $SM_1 + T_1' = \begin{bmatrix} 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & \mu\lambda_2 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \mu\lambda_{l-1} \\ 0 & \cdots & 0 & 0 \end{bmatrix}$

in this way we will eventually change T_1 into zero matrix that means T_1 changes into $T_2 = 0$ so h_1 converted into $h_2 = \begin{bmatrix} M_2 & N_2 \\ 0 & P_2 \end{bmatrix}$ where $M_2 = diag(1, 1, ..., 1, \mu'')$ where in this case $\mu'' = \mu$ and $h_2 \in Sp(2l, k)$ so if we use the fact that $h_2^{\intercal} B h_2 = B$ where $B = \begin{bmatrix} 0 & I_l \\ -I_l & 0 \end{bmatrix}$ where I_l is a $l \times l$ identity matrix.Then we will get that $P_2 = (M_2^{\intercal})^{-1}$

then $h_2 = \begin{bmatrix} M_2 & N_2 \\ 0 & (M_2^{\intercal})^{-1} \end{bmatrix}$.

(ii) When $M_1 = diag(1, 1, ..., 1, 0, ..., 0)$ where no of $1s$ is $m < l$ and $T_1 = \begin{bmatrix} T_{11} & 0 \\ T_{21} & T_{22} \end{bmatrix}$: where T_{11} is a $m \times m$ symmetric matrix. Now in the same way as we did in the **Second Step (i)** we will observe the effect of ER3 on the block T_1 , let's say $T_{11} = \begin{bmatrix} a_1 & \cdots & a_m \\ b_1 & \cdots & b_m \\ \vdots & \ddots & \vdots \\ m_1 & \cdots & m_m \end{bmatrix}$ is a $m \times m$; $m < l$ symmetric matrix and in this case T_{21} is a $l - m \times m$ matrix. So now the way M_1 is defined in this case and by using appropriate $S = t(e_{i,j} + e_{j,i})$; $i < j$ by doing $SM_1 + T_1$ similarly as the case (i) we can easily make T_{11} matrix as zero matrix. Now T_1 changes into $T_1' = \begin{bmatrix} 0 & 0 \\ T_{21} & T_{22} \end{bmatrix}$. So now ER3 will not change M_1 and N_1 so upto now h_1 is changed into $h_1' = \begin{bmatrix} M_1 & N_1 \\ T_1' & P_2' \end{bmatrix}$; h_1' being a $2l \times 2l$ matrix and element of $Sp(2l, k)$. So now in the matrix h_1' the block M_1 has 0 as an entry from $(m+1)th$ row to lth row. and the block T_1' has 0 as an entry from (-1) row to $(-m)th$ row.

Now let's define a matrix for $1 \leq i \leq l$; $\omega_{i,-i} = \Psi_{i,-i}(1)\Psi_{-i,i}(-1)\Psi_{i,-i}(1) = I_{2l} + e_{i,-i} - e_{-i,i} - e_{i,i} - e_{-i,-i} \in Sp(2l, k)$ where I_{2l} is a $2l \times 2l$ identity matrix. When this matrix $\omega_{i,-i}$ multiplied to the matrix h_1' it will interchange the ith and $(-i)th$ row and it will multiply one of these rows by (-1). So we will use these matrices to interchange the rows of h_1' to make T_1' a zero matrix.

So $\prod_{i=m+1}^{i=l} \omega_{i,-i} h_1' = \begin{bmatrix} M_1' & N_1' \\ 0 & P_1' \end{bmatrix}$. Now all the rows which was zero in the block M_1 is interchanged in h_1' as we saw above so now we can follow the same proof as we did in the case First Step (i) means we can use ER1 and EC1 to make M_1' diagonal so then the block M_1' will change into $M_2 = diag(1, 1, ..., 1, \mu'')$ and $\prod_{i=m+1}^{i=l} \omega_{i,-i} h_1'$ will change into $h_2 = \begin{bmatrix} M_2 & N_2 \\ 0 & P_2 \end{bmatrix}$ and now using the fact that $h_2 \in Sp(2l, k)$ gives us that $P_2 = (M_2^{\intercal})^{-1}$.

So now we got our desired matrix which is $h_2 = \begin{bmatrix} M_2 & N_2 \\ 0 & (M_2^{\intercal})^{-1} \end{bmatrix}$ where $M_2 = diag(1, 1, ..., 1, \mu)$ and $\mu \neq 0$.

Third Step: h_2 will be converted into $h_3 = \begin{bmatrix} M_2 & 0 \\ 0 & (M_2^\intercal)^{-1} \end{bmatrix}$ by elementary matrices ; where $M_2 = diag(1, 1, ..., 1, \mu)$: To prove this we will first prove following lemma:

Lemma 5.3.4. *[1, Corollary 4.3] Let $Q = \begin{bmatrix} C & D \\ 0 & C^{-1} \end{bmatrix} \in Sp(2l, k)$ where $C = diag(1, 1, ..., \mu)$ then D will have following form $D = \begin{bmatrix} D_{11} & \mu^{-1}D_{21}^\intercal \\ D_{21} & D_{22} \end{bmatrix}$ where D_{11} is a $l-1 \times l-1$ symmetric matrix .*

Proof. Now because $Q \in Sp(2l, k)$ then $Q^\intercal BQ = B$

which implies that $\begin{bmatrix} C^\intercal & 0 \\ D^\intercal & (C^{-1})^\intercal \end{bmatrix} \begin{bmatrix} 0 & I_l \\ -I_l & 0 \end{bmatrix} \begin{bmatrix} C & D \\ 0 & C^{-1} \end{bmatrix} = \begin{bmatrix} 0 & I_l \\ -I_l & 0 \end{bmatrix}$ after solving this matrix equation we will get $D^\intercal C^{-1} = (C^{-1})^\intercal D$ but $C^\intercal = C$ so we have $D^\intercal (C^{-1})^\intercal = C^{-1}D \implies (C^{-1}D)^\intercal = C^{-1}D$ which says that $C^{-1}D$ is symmetric.

Now $C^{-1}D = \begin{bmatrix} D_{11} & D_{12} \\ \mu^{-1}D_{21} & \mu^{-1}D_{22} \end{bmatrix} = \begin{bmatrix} D_{11}^\intercal & \mu^{-1}D_{21}^\intercal \\ D_{12}^\intercal & \mu^{-1}D_{22}^\intercal \end{bmatrix}$ which implies that $D_{11}^\intercal = D_{11}$ which says that D_{11} is a symmetric matrix and $D_{12} = \mu^{-1}D_{21}^\intercal$. □

Now in our case $Q = h_2$, $C = M_2$, $D = N_2$ so from Lemma 5.2.4 $N_2 = \begin{bmatrix} N_{11} & \mu^{-1}N_{21}^\intercal \\ N_{21} & N_{22} \end{bmatrix}$ where N_{11} is a $l-1 \times l-1$ symmetric matrix. Now this matrix has the same form as T_1 had in the **First Step** and now if we observe the effect of ER2 on the block N_2 is same as effect of ER3 on the block T_1 in the **Second step** and from that elementary operations we made T_1 into a zero matrix, so similarly here we can make N_2 into a zero matrix.and ER2 doesn't change the block M_2. so we got $h_3 = \begin{bmatrix} M_2 & 0 \\ 0 & (M_2^\intercal)^{-1} \end{bmatrix}$.

Fourth Step: Now $h_3 = diag(1, 1, ..., \mu, 1, 1, ..., \mu^{-1})$ will be converted into $h_4 = I_{2l}$ where I_{2l} is a $2l \times 2l$ identity matrix: To prove this we just have to prove that h_3 is a product of elementary matrices in $Sp(2l, k)$.

earlier we defined the element $\omega_{l,-l}(\mu) = \Psi_{l,-l}(\mu)\Psi_{-l,l}(-\mu^{-1})\Psi_{l,-l}(\mu) = I_{2l} - e_{l,l} - e_{-l,-l} + \mu e_{l,-l} - \mu^{-1}e_{-l,l}$

so now take , $\omega_{l,-l}(\mu)\omega_{l,-l}(-1) = \Psi_{l,-l}(\mu)\Psi_{-l,l}(-\mu^{-1})\Psi_{l,-l}(\mu)\Psi_{l,-l}(-1)\Psi_{-l,l}(1)\Psi_{l,-l}(-1) =$

$(I+\mu e_{l,-l})(I-\mu^{-1}e_{-l,l})(I+\mu e_{l,-l})(I-e_{l,-l})(I+e_{-l,l})(I-e_{l,-l}) = I_{2l} - e_{l,l} - e_{-l,-l} + \mu e_{l,l} + \mu^{-1}e_{-l,-l} = diag(1,1,...,\mu,1,1,...\mu^{-1}) = h_3$

so $\omega_{l,-l}(-1)^{-1}\omega_{l,-l}(\mu)^{-1}h_3 = I_{2l} = h_4$.

So in this way we proved that elementary matrices of $Sp(2l,k)$ will generate $Sp(2l,k)$. $\square$

5.4 Two Generation of $Sp(2l,k)$

Reference for the following theorem is [14, 3.11].

Theorem 5.4.1. *$Sp(2l,k)$ is generated by following two elements:*
$\alpha_j = I_{2l} - e_{1,1} - e_{2,2} - e_{-1,-1} - e_{-2,-2} + je_{1,1} + j^{-1}e_{2,2} + j^{-1}e_{-1,-1} + je_{-2,-2}$ *and* $r = \Psi_{1,2}(1)\Gamma$. *Where j is the generator of the multiplicative group k^* of the finite field k such that $j \neq 1$.* $\Psi_{1,2}(1) = I + e_{1,2} - e_{-2,-1}$ *is an elementary matrix of $Sp(2l,k)$ and* $\Gamma = e_{1,-l} - e_{-1,l} - e_{2,1} - e_{-2,-1} - e_{3,2} - e_{-3,-2} - ..... - e_{l,l-1} - e_{-l,-(l-1)}$.

Proof. To prove that $\{\alpha_j, r\}$ will generate the group $Sp(2l,k)$ we will prove that these two elements will generate the elementary matrices of $Sp(2l,k)$ and then from theorem 5.3.1, we have that the elementary matrices of $Sp(2l,k)$ will generate the group $Sp(2l,k)$. So in this way we will prove that $\{\alpha_j, r\}$ will generate the group $Sp(2l,k)$. Now $r = \Psi_{1,2}(1)\Gamma = (I_{2l} + e_{1,2} - e_{-2,-1})(e_{1,-l} - e_{-1,l} - e_{2,1} - e_{-2,-1} - e_{3,2} - e_{-3,-2} - ..... - e_{l,l-1} - e_{-l,-(l-1)}) = \Gamma - e_{1,1} + e_{-2,l} \implies r = \Gamma - e_{1,1} + e_{-2,1}$. Now define $r^{-1} = e_{-l,1} - e_{-l,2} - e_{1,2} - e_{2,3} - .... - e_{l-1,l} - e_{l,-1} - e_{-1,-1} - e_{-1,-2} - e_{-2,-3} - .... - e_{-(l-1),-l}$.

Now define P be the subgroup of $Sp(2l,k)$ generated by α_j and $r \implies P =< \alpha_j, r > \leqslant Sp(2l,k)$. Now let's take $\rho = r\alpha_j r^{-1} = (\Gamma - e_{1,1} + e_{-2,l})(I_{2l} - e_{1,1} - e_{2,2} - e_{-1,-1} - e_{-2,-2} + je_{1,1} + j^{-1}e_{2,2} + j^{-1}e_{-1,-1} + je_{-2,-2})r^{-1} = (r + e_{2,1} - je_{2,1} + e_{-2,-1} - j^{-1}e_{-2,-1} + e_{3,2} - j^{-1}e_{3,2} + e_{-3,-2} - je_{-3,-2} + e_{1,1} - je_{1,1})r^{-1} = (r + ((1-j)(e_{2,1} + e_{-3,-2} + e_{1,1}) + (1-j^{-1})(e_{-2,-1} + e_{3,2}))r^{-1} = I_{2l} + ((1-j)(e_{2,1} + e_{-3,-2} + e_{1,1}) + (1-j^{-1})(e_{-2,-1} + e_{3,2}))(e_{-l,1} - e_{-l,2} - e_{1,2} - e_{2,3} - .... - e_{l-1,l} - e_{l,-1} - e_{-1,-1} - e_{-1,-2} - e_{-2,-3} - .... - e_{-(l-1),-l}) = I_{2l} - e_{2,2} - e_{3,3} - e_{-2,-2} - e_{-3,3} + (j-1)e_{1,2} + je_{2,2} + j^{-1}e_{3,3} + (j-1)e_{-2,-1} + j^{-1}e_{-2,-2} + je_{-3,-3} \implies \rho = I_{2l} - e_{2,2} - e_{3,3} - e_{-2,-2} - e_{-3,3} + (j-1)e_{1,2} + je_{2,2} + j^{-1}e_{3,3} + (j-1)e_{-2,-1} + j^{-1}e_{-2,-2} + je_{-3,-3}$.

Let's take commutator of ρ and α_j ; $[\rho, \alpha_j] = \rho^{-1}\alpha_j^{-1}\rho\alpha_j = (I_{2l} - e_{2,2} - e_{3,3} - e_{-2,-2} -$

$e_{-3,-3}+(j^{-1}-1)e_{1,2}+j^{-1}e_{2,2}+je_{3,3}+(j-1)e_{-2,-1}+je_{-2,-2}+j^{-1}e_{-3,-3})(I_{2l}-e_{1,1}-e_{2,2}-e_{-1,-1}-e_{-2,-2}+j^{-1}e_{1,1}+je_{2,2}+je_{-1,-1}+j^{-1}e_{-2,-2})(I_{2l}-e_{2,2}-e_{3,3}-e_{-2,-2}-e_{-3,3}+(j-1)e_{1,2}+je_{2,2}+j^{-1}e_{3,3}+(j^{-1}-1)e_{-2,-1}+j^{-1}e_{-2,-2}+je_{-3,-3})(I_{2l}-e_{1,1}-e_{2,2}-e_{-1,-1}-e_{-2,-2}+je_{1,1}+j^{-1}e_{2,2}+j^{-1}e_{-1,-1}+je_{-2,-2}) = (I_{2l}-e_{1,1}-e_{3,3}-e_{-1,-1}-e_{-3,-3}+j^{-1}e_{1,1}+(1-j)e_{1,2}+je_{3,3}+je_{-1,-1}+(j^2-j)e_{-2,-1}+j^{-1}e_{-3,-3})(I_{2l}-e_{1,1}-e_{3,3}-e_{-1,-1}-e_{-3,-3}+je_{1,1}+(1-j^{-1})e_{1,2}+j^{-1}e_{3,3}+j^{-1}e_{-1,-1}+(j^{-2}-j^{-1})e_{-2,-1}+je_{-3,-3}) = I_{2l}+(1-j+j^{-1}-j^{-2})e_{1,2}-(1-j+j^{-1}-j^{-2})e_{-2,-1} = I_{2l}+(j-1)(j^{-2}-1)(e_{1,2}-e_{-2,-1}) = \Psi_{1,2}((j-1)(j^{-2}-1))$.

So we have $[\rho,\alpha_j] = \Psi_{1,2}((j-1)(j^{-2}-1))$, now as in the statement of the theorem we have $j \neq 1 \implies (j-1)(j^{-2}-1) \neq 0$, let's say $(j-1)(j^{-2}-1) = f \neq 0$ then $[\rho,\alpha_j] = \Psi_{1,2}(f) \in P$ where $f \neq 0$ and $\Psi_{1,2}(t)$ is a elementary matrix of $Sp(2l,k)$.

Lemma 5.4.2. *[14, 3.9] We have $P =< \alpha_j, r >$ and $\Psi_{1,2}(f) \in P$ where $f \in k^*$ where k^* is the multiplicative group of the finite field k. Then α_j and $\Psi_{1,2}(f)$ will generate the set $\{\Psi_{1,2}(d);\ d \in k\}$ which will further imply that $\{\Psi_{1,2}(d);\ d \in k\} \subset P$.*

Proof. Let's take conjugate of $\Psi_{1,2}(f)$ with α_j , then $\alpha_j\Psi_{1,2}(f)\alpha_j^{-1} = (I_{2l}-e_{1,1}-e_{2,2}-e_{-1,-1}-e_{-2,-2}+je_{1,1}+j^{-1}e_{2,2}+j^{-1}e_{-1,-1}+je_{-2,-2})(I_{2l}+f(e_{1,2}-e_{-2,-1}))(I_{2l}-e_{1,1}-e_{2,2}-e_{-1,-1}-e_{-2,-2}+j^{-1}e_{1,1}+je_{2,2}+je_{-1,-1}+j^{-1}e_{-2,-2}) = I_{2l}+j^2f(e_{1,2}-e_{-2,-1}) = \Psi_{1,2}(j^2f)$. Now if we take $\alpha_j\Psi_{1,2}(j^2f)\alpha_j^{-1}$ it will be equal to $\Psi_{1,2}(j^4f)$, in this way if we repeatedly do this conjugation we will get that $\{\Psi_{1,2}(j^2f), \Psi_{1,2}(j^4f), \Psi_{1,2}(j^6f), ..., \Psi_{1,2}(j^{2i}f)\} \subset P$ so if we take product of these elements that will also be in the subgroup P which means that $\{\Psi_{1,2}((\sum_i j^{2i})f)\} \subset P$.

So now let's define the subset $\mathscr{Q}$ of the finite field k as follows: $\mathscr{Q} = \{(\sum_i j^{2i})f : \Psi_{1,2}((\sum_i j^{2i})f) \in P\}$ which means $\mathscr{Q} = \{j^2f, j^4f, ..., (j^2+j^4)f, ...\} \subseteq k$ and j is the generator of k^* and $j \neq 1$. Now we can prove that $\mathscr{Q} = k$ by using lemma 3.2.2 in chapter 3, which simply proves that $\{\Psi_{1,2}(d) : d \in k\} \subset P$. □

Now let's take $\Gamma\Psi_{1,2}(d)\Gamma^{-1} = (e_{1,-l}-e_{-1,l}-e_{2,1}-e_{-2,-1}-e_{3,2}-e_{-3,-2}-.....-e_{l,l-1}-e_{-l,-(l-1)})(I_{2l}+d(e_{1,2}-e_{-2,-1}))(e_{-l,1}-e_{l,-1}-e_{1,2}-e_{-1,-2}-e_{2,3}-e_{-2,-3}-.....-e_{l-1,l}-e_{-(l-1),-l}) = (\Gamma - de_{2,2} + de_{-3,-1})\Gamma^{-1} = I_{2l} + de_{2,3} - de_{-3,-2} = I_{2l} + d(e_{2,3}-e_{-3,-2}) = \Psi_{2,3}(d) \implies \Gamma\Psi_{1,2}(d)\Gamma^{-1} = \Psi_{2,3}(d)$. Which simply says that $\Psi_{2,3}(d) \in P$. Now in the same way if we calculate $\Gamma\Psi_{2,3}(d)\Gamma^{-1} = \Psi_{3,4}(d)$. So just following this procedure we will get that for any $d \in k$; $\{\Psi_{2,3}(d), \Psi_{3,4}(d), \Psi_{4,5}(d), ..., \Psi_{l-1,l}(d)\} \subset P$.

Now let's take $d, u \in k$ and calculate commutator of $\Psi_{1,2}(d)$ and $\Psi_{2,3}(u)$, $[\Psi_{1,2}(d), \Psi_{2,3}(u)]$ $= \Psi_{1,2}(d)^{-1}\Psi_{2,3}(u)^{-1}\Psi_{1,2}(d)\Psi_{2,3}(u) = (I_{2l}-d(e_{1,2}-e_{-2,-1}))(I_{2l}-u(e_{2,3}-e_{-3,-2}))(I_{2l}+d(e_{1,2}-e_{-2,-1}))(I_{2l}+u(e_{2,3}-e_{-3,-2})) = (I_{2l}-ue_{2,3}+ue_{-3,-2}-de_{1,2}+due_{1,3}+de_{-2,-1})(I_{2l}+ue_{2,3}-ue_{-3,-2}+de_{1,2}+due_{1,3}-de_{-2,-1}) = I_{2l}+(du)(e_{1,3}-e_{-3,-1}) = \Psi_{1,3}(du) \implies [\Psi_{1,2}(d), \Psi_{2,3}(u)] = \Psi_{1,3}(du)$ and du will vary over all the elements of the field k so which says that for any $t \in k; \{\Psi_{1,3}(t)\} \subset P$. So in general let's take $2 \leq i \leq l-1$ then $[\Psi_{1,i}(d), \Psi_{i,i+1}(u)] = \Psi_{1,i}(d)^{-1}\Psi_{i,i+1}(u)^{-1}\Psi_{1,i}(d)\Psi_{i,i+1}(u) = \Psi_{1,i+1}(du)$ which implies that $\{\Psi_{1,i+1}(t)\} \subset P$ for $3 \leq i+1 \leq l \implies \{\Psi_{1,3}(t), \Psi_{1,4}(t), ..., \Psi_{1,l}(t)\} \subset P; \forall t \in k$. Now in the same way if we calculate for $3 \leq i \leq l-1$, $[\Psi_{2,i}(d), \Psi_{i,i+1}(u)] = \Psi_{2,i}(d)^{-1}\Psi_{i,i+1}(u)^{-1}\Psi_{2,i}(d)\Psi_{i,i+1}(u) = I_{2l}+(du)(e_{2,i+1}-e_{-(i+1),-2}) = \Psi_{2,i+1}(du) \implies \{\Psi_{2,4}(t), \Psi_{2,5}(t), ..., \Psi_{2,l}(t)\} \subset P; \ \forall t \in k.$

So in this way , we can do this calculation and we will get that $\{\Psi_{3,i}(t);\ 3 < i\}$, $\{\Psi_{4,i}(t); 4 < i\}, ..., \{\Psi_{l-1,i}(t); l-1 < i\}$ will contain in the group P. So it shows that $\{\Psi_{i,j}(t);\ i < j; t \in k\} \subset P$.

$$\boxed{\{\Psi_{i,j}(t);\ i < j; t \in k\} \subset P =< \alpha_j, r >}$$

Now we have that $\Psi_{l-1,l}(d) \in P$; so let's take $\Gamma\Psi_{l-1,l}(d)\Gamma^{-1} = (e_{1,-l}-e_{-1,l}-e_{2,1}-e_{-2,-1}-e_{3,2}-e_{-3,-2}-.....-e_{l,l-1}-e_{-l,-(l-1)})(I_{2l}+d(e_{l-1,l}-e_{-l,(l-1)}))(e_{-l,1}-e_{l,-1}-e_{1,2}-e_{-1,-2}-e_{2,3}-e_{-2,-3}-.....-e_{l-1,l}-e_{-(l-1),-l}) = (\Gamma - de_{1,-(l-1)}-de_{l,l})\Gamma^{-1} = I_{2l}+de_{1,-l}-de_{l,-1} = I_{2l}+d(e_{1,-l}+e_{l,-1}) = \Psi_{1,-l}(d)$; so for any $d \in k; \{\Psi_{1,-l}(d)\} \subset P$.

Now take $\Gamma\Psi_{1,-l}(d)\Gamma^{-1} = (e_{1,-l}-e_{-1,l}-e_{2,1}-e_{-2,-1}-e_{3,2}-e_{-3,-2}-.....-e_{l,l-1}-e_{-l,-(l-1)})(I_{2l}+d(e_{1,-l}+e_{l,-1}))(e_{-l,1}-e_{l,-1}-e_{1,2}-e_{-1,-2}-e_{2,3}-e_{-2,-3}-.....-e_{l-1,l}-e_{-(l-1),-l}) = (\Gamma - de_{2,-l}-de_{-1,-1})\Gamma^{-1} = I_{2l}-de_{2,1}+de_{-1,-2} = I_{2l}-d(e_{2,1}-e_{-1,-2}) = \Psi_{2,1}(-d) \implies \Psi_{2,1}(-d) \in P$. Now $\Psi_{2,1}(d)$ is inverse of $\Psi_{2,1}(-d) \implies \Psi_{2,1}(d) \in P$. Now $\Gamma\Psi_{2,1}(d)\Gamma^{-1} = (e_{1,-l}-e_{-1,l}-e_{2,1}-e_{-2,-1}-e_{3,2}-e_{-3,-2}-.....-e_{l,l-1}-e_{-l,-(l-1)})(I_{2l}+d(e_{2,1}-e_{-1,-2}))(e_{-l,1}-e_{l,-1}-e_{1,2}-e_{-1,-2}-e_{2,3}-e_{-2,-3}-.....-e_{l-1,l}-e_{-(l-1),-l}) = I_{2l}+d(e_{3,2}-e_{-2,-3}) = \Psi_{3,2}(d) \implies \Gamma\Psi_{2,1}(d)\Gamma^{-1} = \Psi_{3,2}(d)$. So as previously we did, in the same way we will get that $\{\Psi_{3,2}(d), \Psi_{4,3}(d), ..., \Psi_{l,l-1}(d)\} \subset P$. Now $[\Psi_{3,2}(d), \Psi_{2,1}(u)] = \Psi_{3,2}(d)^{-1}\Psi_{2,1}(u)^{-1}\Psi_{3,2}(d)\Psi_{2,1}(u) = (I_{2l}-d(e_{3,2}-e_{-2,-3}))(I_{2l}-u(e_{2,1}-e_{-1,-2}))(I_{2l}+d(e_{3,2}-e_{-2,-3}))(I_{2l}+u(e_{2,1}-e_{-1,-2}) = (I_{2l}-ue_{2,1}+ue_{-1,-2}-de_{3,2}+due_{3,1}+de_{-2,-3})(I_{2l}+ue_{2,1}-ue_{-1,-2}+de_{3,2}+due_{3,1}-de_{-2,-3}) = I_{2l}+(du)(e_{3,1}-e_{-1,-3}) = \Psi_{3,1}(du) \implies \Psi_{3,1}(du) \in P$ and du will vary over all the elements of the field k; so $\Psi_{3,1}(t) \in P$. Now as we previously did , we will have $\{\Psi_{i,j}(t);\ i > j;\ t \in k\} \subset P$. We previously proved that $\{\Psi_{i,j}(t);\ i <$

$j;\ t \in k\} \subset P \implies \{\Psi_{i,j}(t);\ i \neq j;\ t \in k\} \subset P$

$$\boxed{\{\Psi_{i,j}(t);\ i \neq j;\ t \in k\} \subset P}$$

Now calculate $\Gamma\Psi_{l,1}(d)\Gamma^{-1} = (e_{1,-l} - e_{-1,l} - e_{2,1} - e_{-2,-1} - e_{3,2} - e_{-3,-2} - ..... - e_{l,l-1} - e_{-l,-(l-1)})(I_{2l} + d(e_{l,1} - e_{-1,-l}))(e_{-l,1} - e_{l,-1} - e_{1,2} - e_{-1,-2} - e_{2,3} - e_{-2,-3} - ..... - e_{l-1,l} - e_{-(l-1),-l}) = (\Gamma - de_{-1,1} + de_{-2,-l})\Gamma^{-1} = I_{2l} + d(e_{-1,2} + e_{-2,1}) = \Psi_{-1,2}(d)$, which implies that $\Psi_{-1,2}(d) \in P$. Now take $\Gamma\Psi_{1,l}(d)\Gamma^{-1} = (e_{1,-l} - e_{-1,l} - e_{2,1} - e_{-2,-1} - e_{3,2} - e_{-3,-2} - ..... - e_{l,l-1} - e_{-l,-(l-1)})(I_{2l} + d(e_{1,l} - e_{-l,-1}))(e_{-l,1} - e_{l,-1} - e_{1,2} - e_{-1,-2} - e_{2,3} - e_{-2,-3} - ..... - e_{l-1,l} - e_{-(l-1),-l}) = (\Gamma - de_{2,l} - de_{1,-1})\Gamma^{-1} = I_{2l} + d(e_{1,-2} + e_{2,-1}) = \Psi_{1,-2}(d) \implies \Psi_{1,-2}(d) \in P.$

Now let's take $\Gamma\Psi_{1,-2}(d)\Gamma^{-1} = (e_{1,-l} - e_{-1,l} - e_{2,1} - e_{-2,-1} - e_{3,2} - e_{-3,-2} - ..... - e_{l,l-1} - e_{-l,-(l-1)})(I_{2l} + d(e_{1,-2} + e_{2,-1}))(e_{-l,1} - e_{l,-1} - e_{1,2} - e_{-1,-2} - e_{2,3} - e_{-2,-3} - ..... - e_{l-1,l} - e_{-(l-1),-l}) = (\Gamma - de_{2,-2} - de_{3,-1})\Gamma^{-1} = I_{2l} + d(e_{2,-3} + e_{3,-2}) = \Psi_{2,-3}(d)$. Now if we follow this procedure as we did previously we will get that $\{\Psi_{2,-3}(d), \Psi_{3,-4}(d), \Psi_{4,-5}(d), ..., \Psi_{l-1,-l}(d);\ d \in k\} \subset P$. Now take the commutator of $\Psi_{1,2}(d)$ and $\Psi_{2,-3}(u)$; $[\Psi_{1,2}(d), \Psi_{2,-3}(u)] = \Psi_{1,2}(d)^{-1}\Psi_{2,-3}(u)^{-1}$ $\Psi_{1,2}(d)\Psi_{2,-3}(u) = (I_{2l} - d(e_{1,2} - e_{-2,-1}))(I_{2l} - u(e_{2,-3} + e_{3,-2}))(I_{2l} + d(e_{1,2} - e_{-2,-1}))(I_{2l} + u(e_{2,-3} + e_{3,-2})) = I_{2l} + (du)(e_{1,-3} + e_{3,-1}) = \Psi_{1,-3}(du)$ so this says that $\Psi_{1,-3}(t) \in P$. Now we can see $[\Psi_{1,3}(d), \Psi_{3,-4}(u)] = \Psi_{1,-4}(du)$; in this way if we calculate $[\Psi_{1,3}(d), \Psi_{3,-4}(u)]$, $[\Psi_{1,4}(d), \Psi_{4,-5}(u)], ..., [\Psi_{1,l-1}(d), \Psi_{l-1,-l}(u)]$ we will get that $\{\Psi_{1,-4}(t), \Psi_{1,-5}(t), ..., \Psi_{1,-l}(t)$ $;\ t \in k\} \subset P$. In the same way if we calculate for $3 \leq i \leq l-1$; $[\Psi_{2,i}(d), \Psi_{i,-(i+1)}(u)]$ it will be equal to $\Psi_{2,-(i+1)}(du) \implies \{\Psi_{2,-4}(t), \Psi_{2,-5}(t), ..., \Psi_{2,-l}(t); t \in k\} \subset P$. Similarly if we take $[\Psi_{3,i}(d), \Psi_{i,-(i+1)}(u)] = \Psi_{3,-(i+1)}(du)$ for $4 \leq i \leq l-1$. Then we get that $\{\Psi_{3,-5}(t), \Psi_{3,-6}(t), ..., \Psi_{3,-l}(t); t \in k\} \subset P$. Now just following this procedure we will get that $\{\Psi_{i,-j}(d);\ i < j; d \in k\} \subset P$.

$$\boxed{\{\Psi_{i,-j}(d);\ i < j; d \in k\} \subset P}$$

Now let's take conjugate of $\Psi_{-1,2}(d)$ with Γ ; $\Gamma\Psi_{-1,2}(d)\Gamma^{-1} = (e_{1,-l} - e_{-1,l} - e_{2,1} - e_{-2,-1} - e_{3,2} - e_{-3,-2} - ..... - e_{l,l-1} - e_{-l,-(l-1)})(I_{2l} + d(e_{-1,2} + e_{-2,1}))(e_{-l,1} - e_{l,-1} - e_{1,2} - e_{-1,-2} - e_{2,3} - e_{-2,-3} - ..... - e_{l-1,l} - e_{-(l-1),-l}) = (\Gamma - de_{-2,2} - de_{-3,1})\Gamma^{-1} = I_{2l} + d(e_{-2,3} + e_{-3,2}) = \Psi_{-2,3}(d)$. Now in general let's take $1 \leq i \leq l-2$, and evaluate $\Gamma\Psi_{-i,i+1}(d)\Gamma^{-1} = (e_{1,-l} - e_{-1,l} - e_{2,1} - e_{-2,-1} - e_{3,2} - e_{-3,-2} - ..... - e_{l,l-1} - e_{-l,-(l-1)})(I_{2l} + d(e_{-i,i+1} + e_{-(i+1),i}))(e_{-l,1} - e_{l,-1} - e_{1,2} - e_{-1,-2} - e_{2,3} - e_{-2,-3} - ..... - e_{l-1,l} - e_{-(l-1),-l}) = (\Gamma - de_{-(i+1),i+1} - de_{-(i+2),i})\Gamma^{-1} = I_{2l} + d(e_{-(i+1),(i+2)} + e_{-(i+2),(i+1)}) = \Psi_{-(i+1),(i+2)}(d)$. Which shows that $\{\Psi_{-2,3}(d), \Psi_{-3,4}(d), ...,$

$\Psi_{-(l-1),l}(d)\} \subset P$. Now $[\Psi_{-1,2}(d), \Psi_{2,3}(u)] = \Psi_{-1,2}(d)^{-1}\Psi_{2,3}(u)^{-1}\Psi_{-1,2}(d)\Psi_{2,3}(u) = (I_{2l} - d(e_{-1,2} + e_{-2,1}))(I_{2l} - u(e_{2,3} - e_{-3,-2}))(I_{2l} + d(e_{-1,2} + e_{-2,1}))(I_{2l} + u(e_{2,3} - e_{-3,-2})) = (I_{2l} - ue_{2,3} + ue_{-3,-2} - de_{-1,2} + due_{-1,3} - de_{-2,1})(I_{2l} + ue_{2,3} - ue_{-3,-2} + de_{-1,2} + due_{-1,3} + de_{-2,1}) = I_{2l} + du(e_{-1,3} + e_{-3,1}) = \Psi_{-1,3}(du) \implies \Psi_{-1,3}(t) \in P$. Now $[\Psi_{-1,3}(d), \Psi_{3,4}(u)] = \Psi_{-1,4}(du), ...,$ $[\Psi_{-1,l-1}(d), \Psi_{l-1,l}(u)] = \Psi_{-1,l}(du) \implies \{\Psi_{-1,4}(t), \Psi_{-1,5}(t), ..., \Psi_{-1,l}(t); t \in k\} \subset P$.

Now if we take $[\Psi_{-2,i}(d), \Psi_{i,i+1}(u)]$ for $3 \leq i \leq l-1$; it will be equal to $\Psi_{-2,i+1}(du)$, which states that $\{\Psi_{-2,4}(t), \Psi_{-2,5}(t), ..., \Psi_{-2,l}(t)\} \subset P$. We can repeat this procedure for $j = 3, ..., l-1$ and we will get that $\{\Psi_{-i,j}(d); i < j; d \in k\} \subset P$.

$$\boxed{\{\Psi_{-i,j}(d); i < j; d \in k\} \subset P}$$

We earlier proved that $\Psi_{-1,l}(d), \Psi_{l,1}(d) \in P$, now $[\Psi_{-1,l}(d), \Psi_{l,1}(u)] = \Psi_{-1,l}(d)^{-1}\Psi_{l,1}(u)^{-1}$ $\Psi_{-1,l}(d)\Psi_{l,1}(u) = (I_{2l} - d(e_{-1,l} + e_{-l,1}))(I_{2l} - u(e_{l,1} - e_{-1,-l}))(I_{2l} + d(e_{-1,l} + e_{-l,1}))(I_{2l} + u(e_{l,1} - e_{-1,-l})) = (I_{2l} - u(e_{l,1} - e_{-1,-l}) - de_{-1,l} + due_{-1,1} - de_{-l,1})(I_{2l} + u(e_{l,1} - e_{-1,-l}) + de_{-1,l} + due_{-1,1} + de_{-l,1}) = I_{2l} + (2du)e_{-1,1} = \Psi_{-1,1}(2du) \implies [\Psi_{-1,l}(d), \Psi_{l,1}(u)] = \Psi_{-1,1}(2du)$. Because du vary over all the elements of the finite field k so we proved that for any $t \in k, \Psi_{-1,1}(2t) \in P$. To prove that $\{\Psi_{-1,1}(t); t \in k\} \in P$, we will prove the following lemma:

Lemma 5.4.3. *If k is a finite field with characteristic not equal to 2 then the following map:*

$$g : k \to k$$

$$t \to 2t$$

is a bijective map.

Proof. k is a finite set so if i prove that g is injective then that will imply it is surjective which implies that g is bijective. So we will show that g is injective,let's take $t_1, t_2 \in k$ such that $g(t_1) = g(t_2) \implies 2t_1 = 2t_2 \implies 2(t_1 - t_2) = 0$ and let's say $t_1 - t_2 = t'$ then $2t' = 0$ and t' is arbitrary and field k has characteristic not equal to 2 which implies $t' = 0 \implies t_1 - t_2 = 0 \implies t_1 = t_2$ which shows that g is an injective map which further implies that g is bijective,because k is a finite set. □

So from lemma 5.4.3 if we have that $\Psi_{-1,1}(2t) \in P \implies \{\Psi_{-1,1}(t'); t' \in k\} \subset P$. So now let's take $1 \leq i \leq l-1$ and calculate $\Gamma\Psi_{-i,i}(t)\Gamma^{-1} = (e_{1,-l} - e_{-1,l} - e_{2,1} - e_{-2,-1} - e_{3,2} -$

$e_{-3,-2} - ..... - e_{l,l-1} - e_{-l,-(l-1)})(I_{2l} + te_{-i,i})(e_{-l,1} - e_{l,-1} - e_{1,2} - e_{-1,-2} - e_{2,3} - e_{-2,-3} - ..... - e_{l-1,l} - e_{-(l-1),-l}) = (\Gamma - te_{-(i+1),i})\Gamma^{-1} = I_{2l} + te_{-(i+1),i+1} = \Psi_{-(i+1),i+1}(t)$, and we proved that $\Psi_{-1,1}(t) \in P \implies \{\Psi_{-2,2}(t), \Psi_{-3,3}(t), ...\Psi_{-l,l}(t)\} \subset P$. So which shows that

$$\boxed{\{\Psi_{-i,i}(t); 1 \leq i \leq l; t \in k\} \subset P}$$

We have that $\Psi_{-l,l}(t) \in P$, so now take $\Gamma\Psi_{-l,l}(t)\Gamma^{-1} = (e_{1,-l} - e_{-1,l} - e_{2,1} - e_{-2,-1} - e_{3,2} - e_{-3,-2} - ..... - e_{l,l-1} - e_{-l,-(l-1)})(I_{2l} + te_{-l,l})(e_{-l,1} - e_{l,-1} - e_{1,2} - e_{-1,-2} - e_{2,3} - e_{-2,-3} - ..... - e_{l-1,l} - e_{-(l-1),-l}) = (\Gamma + te_{1,l})\Gamma^{-1} = I_{2l} - te_{1,-1} = \Psi_{1,-1}(-t) = \Psi_{1,-1}(t)^{-1} \implies \Gamma\Psi_{-l,l}(t)\Gamma^{-1} = \Psi_{-1,1}(t)^{-1} \implies \Psi_{1,-1}(t) \in P$. Now for $1 \leq i \leq l-1$, $\Gamma\Psi_{i,-i}(t)\Gamma^{-1} = \Psi_{i+1,-(i+1)}(t) \implies \{\Psi_{2,-2}(t), \Psi_{3,-3}(t), ...\Psi_{l,-l}(t)\} \subset P$. We also proved that $\Psi_{1,-1}(t) \in P \implies$

$$\boxed{\{\Psi_{i,-i}(t); 1 \leq i \leq l; t \in k\} \subset P}$$

$P =< \alpha_j, r > \leqslant Sp(2l, k)$ and we showed that all the elementary matrices of $Sp(2l, k)$ defined in the section 5.2,will contain in the subgroup P. But from theorem 5.3.1 the group $Sp(2l, k)$ is generated by the elementary matrices of $Sp(2l, k)$ which shows that $Sp(2l, k) \leqslant P \implies P = Sp(2l, k)$.

$$\boxed{P =< \alpha_j, r >= Sp(2l, k)}$$

It proves the two generation of $Sp(2l, k)$ i.e. $Sp(2l, k)$ is generated by 2 elements $\{\alpha_j, r\}$. $\square$

Bibliography

[1] Sushil Bhunia, Ayan Mahalanobis, Pralhad Shinde, and Anupam Singh. Gaussian elimination in symplectic and split orthogonal groups. *arXiv preprint arXiv:1504.03794*, 2015.

[2] Marston DE Conder. Generators for alternating and symmetric groups. *Journal of the London Mathematical Society*, 2(1):75–86, 1980.

[3] Keith Conrad. Generating sets. *Unpublished manuscript. Available at http://www. math. uconn. edu/˜ kconrad/blurbs/grouptheory/genset. pdf*, 2013.

[4] L Di Martino, MC Tamburini, and AE Zalesskii. On hurwitz groups of low rank. *Communications in Algebra*, 28(11):5383–5404, 2000.

[5] Roderick Gow and Maria Chiara Tamburini. Generation of $\mathrm{SL}(n, \mathbb{Z})$ by a jordan unipotent matrix and its transpose. *Linear algebra and its applications*, 181:63–71, 1993.

[6] Robert M Guralnick, William M Kantor, Martin Kassabov, and Alexander Lubotzky. Presentations of finite simple groups: a computational approach. *arXiv preprint arXiv:0804.1396*, 2008.

[7] Alexander J. Hahn and O. Timothy O'Meara. *The classical groups and K-theory*, volume 291 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1989. With a foreword by J. Dieudonné.

[8] Martin W. Liebeck and Aner Shalev. Classical groups, probabilistic methods, and the $(2, 3)$-generation problem. *Ann. of Math. (2)*, 144(1):77–125, 1996.

[9] A Lucchini and MC Tamburini. Classical groups of large rank as hurwitz groups. *Journal of Algebra*, 219(2):531–546, 1999.

[10] A Lucchini, MC Tamburini, and JS Wilson. Hurwitz groups of large rank. *Journal of the London Mathematical Society*, 61(1):81–92, 2000.

[11] Alexander M Macbeath. Generators of the linear fractional groups. In *Proc. Symp. Pure Math*, volume 12, pages 14–32, 1969.

[12] Marco Antonio Pellegrini. The (2, 3)-generation of the classical simple groups of dimensions 6 and 7. *Bulletin of the Australian Mathematical Society*, 93(1):61–72, 2016.

[13] Marco Antonio Pellegrini. The $(2, 3)$-generation of the special linear groups over finite fields. *Bulletin of the Australian Mathematical Society*, 95(1):48–53, 2017.

[14] Robert Steinberg. Generators for simple groups. *Canadian Journal of Mathematics*, 14:277–283, 1962.

[15] Vadim Vasilyev and Maxim Vsemirnov. The group $\mathrm{Sp}_{10}(\mathbb{Z})$ is (2,3)-generated. *Cent. Eur. J. Math.*, 9(1):36–49, 2011.