SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Classical finite simple groups

av

Seuri Basilio Kuosmanen

2020 - No K31

Classical finite simple groups

Seuri Basilio Kuosmanen

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Sven Raum

2020

1 Abstract

This paper aims to prove the simplicity of the projective special linear groups and the projective symplectic groups, which both belong to the family of six classical simple finite groups. To do this, we first give intuition and motivation for studying simple groups and give some prerequisite knowledge about group theory. We then proceed to prove Jordan-Hölder Theorem, by applying, Schreier's Refinements Theorem. For the main result of this thesis, we use Iwasawa's Lemma.

Acknowledgment

I would like to thank my advisor Sven Raum for suggesting the topic and for helping me in my journey of becoming a mathematician. I am thankful for the inspiring and motivating meetings we have had and especially thankful for his advice and patients during this process. I would also like to thank my family and friends, in particular, my sister Susse Basilio for giving my moral support and perspective during this period. Finally, I would like to thank the late great Kobe Bean Bryant for always being a source of inspiration.

Contents

2 Introduction

The theory of groups can be dated back to the nineteenth century and is born from number theory and the theory of equations. Galois introduced groups to study the symmetry of polynomials and their set of roots. In his studies, he was able to use groups, and in some cases, simple groups, to show that certain polynomials were not solvable by radicals. Group theory is the study of these groups, and groups are a recurring theme in mathematics. It has many applications outside of the world of mathematics, for example, physics, and chemistry. From the study of these algebraic structures, the question of what type of underlying structure is present in these groups arises. One may draw simplified comparisons to the study of integers and the fact that an integer is either a prime number or the product of prime numbers. In other words, there is an interest in understanding what type of underlying structures are present in groups. From that line of questioning, it is possible to get an intuition of the simple groups. One way to look at simple groups is to think of them as building blocks for all groups. In the same way, one may study and construct the integers via prime numbers and more precis prime number composition to get a deeper understanding of integers. So in a sense, there is an interest in wanting to understand if a group is a finite simple group. Or if a group can be reduced to simple pieces, and if there is a uniqueness for which this can be done. Two mathematicians Camille Jordan and Otto Hölder stated and proved a theorem that is known as The Jordan-Hölder theorem that answers these questions. The field of simple finite groups has enjoyed a range of contributions during the twentieth century. The most groundbreaking was the Classification of finite simple groups theorem, which states that every finite simple group belongs to one of the broader classes of simple finite groups, the cyclic groups of prime order, the alternating groups of degree at least 5, the groups of Lie type, sporadic groups, and Tits group. This paper will focus on a specific class of groups of Lie type, namely the classical groups defined as matrices over fields. We start by giving introducing some basic concepts in group theory and proceed to stat and prove Jordan-Hölder theorem. We then continue by stating and proving Iwasawa's Lemma, which we then use to prove the simplicity of two of the classical groups.

3 Basics

In the introduction, we mentioned that Galois introduced the concept of a group to solve polynomial equations of degree higher then four. This led to the development of abstract algebra, which incorporates a wide range of abstract objects, for which the group is one of thous objects. The subject of group theory is living and rich, and has enjoyed a wide range of important results from many known mathematicians. Group theory, is in some ways, interested in studying symmetry, and for example, the platonic solids can be expressed using groups. This section is structured to give sufficient collections of definitions and examples for the upcoming sections. We will introduce relevant definitions paired with explanatory examples. Furthermore, we will state and prove the necessary theorems for the succeeding sections. As stated in the title of this paper, we are focusing on the classical groups, which are subgroups of the general linear groups. They were first recorded in one of three manuscripts that Galois sent to Chevalier in 1832. But Joseph Louis Lagrange and Niels Henrik Abel were also early contributors to the field of group theory.

Definition 3.0.1. A group is a nonempty set G equipped with a binary operation $\star : G \times G \to G$ such that

(i) The operation is associative $(a \star b) \star c = a \star (b \star c)$ for all a, b, c in G

(ii) There exist an identity element e_g in G such that $e_G \star a = a = a \star e_G$ for all a in G.

(iii) For all a in G there exist an inverse $a^{-1} = b$ in G such that $a \star b = e = b \star a$

Remark. A group is called abelian if $a \star b = b \star a$ for all a, b in G. One example of an abelian group is the set $\mathbb{R}^{\times}$ equipped with multiplication.

It might not seem clear from this definition but groups are a recurring theme in mathematics. Many of the sets that we have encountered in elementary mathematics are groups when equipped with a suitable binary operation. We consider a set from linear algebra of invertible square matrices with entries from a field and we will show that the set is in fact a fact a group.

Example 3.0.2. The set $GL_n(q) = \{A \in M_n(\mathbb{F}_q) |\ A \text{ is invertible}\}$ is a group when equipped with matrix multiplication is a group. The set is preserved under matrix multiplication since

$$(AB)^{-1} = B^{-1}A^{-1} \qquad \text{for } A, B \in GL_n(q).$$

We verify the conditions of Definition 4.1. Since matrix multiplication is associative it is also associative in $GL_n(q)$. The condition of the existence of an identity is satisfied since the identity matrix I_n is in $GL_n(q)$. The definition of $GL_n(q)$ satisfies the last condition. So we conclude that $GL_n(q)$ is a group.

Remark. It is the general linear group over a finite field mentioned in the introduction of this section.

There is always an interest in understating the cardinality of a set, and so we introduce a definition for groups, then proceed to calculate the cardinality of the general linear group.

Definition 3.0.3. A group G is finite if the cardinality of the set G is finite. The **order** of the group G is the cardinality of the set G and is denoted $|G|$.

Remark. A group that is not finite is called infinite.

Example 3.0.4. Consider the group $GL_n(q)$ and with entries from $\mathbb{F}_q$. Then the order of the group is

$$|GL_n(q)| = \prod_{k=1}^{n-1}(q^n - q^k)$$

Proof. An element A is in $GL_n(q)$ if and only if it is invertible. Which is equivalent to its row vectors forming a basis of $\mathbb{F}_q^n$. So then we want to count how many n-tuples of vector in $\mathbb{F}_q^n$ for which are linear independent. There are $q^n - 1$ different non-zero vectors in $\mathbb{F}_n^q$. Hence there are $q^n - 1$ possibilities for which we can chose the first vector. If we have chosen k vectors such that they span a k-dimensional subspace of $\mathbb{F}_q^n$ whose cardinality is q^k. Then there are $q^n - q^k$ possible choices for the $k+1$ vector. By the rule of product, there are

$$(q^n - 1)(q^n - q)\dots(q^n - q^{n-1}) = \prod_{k=1}^{n-1}(q^n - q^k)$$

many basis in $\mathbb{F}_q^n$ which equals the order of $GL_n(q)$. □

The order of the group gives arise to questions regarding the elements of the group. Thus for clarity we will give a definition of the the order of the elements of a group.

Definition 3.0.5. Let G be a group and let g be in G. Define the order of g by $\text{ord}(g) = n$ where n is the smallest positive integer such that $x^n = 1$ if such n exist and if not $ord(x) = \infty$.

We started by defining a group from the notion of a set. So naturally, the question of the existence of subgroups arises. Hence we introduce a new definition.

Definition 3.0.6. Let G be a group and let H be a subset of G then H is a subgroup of G denoted $H \leq G$ if and only if $H \neq \emptyset$ and H is closed under products and taking inverse.

Remark. To determine of a set H is a subgroup one simply verifies this conditions from the definition. If H is non-empty and finite the problem is reduced to show that it is closed under the binary operation.

In the next example, we will prove that the subset of invertible matrices whit determinant 1 in $GL_n(q)$ is a subgroup.

Example 3.0.7. The subset

$$SL_n(q) = \{A \in M_n(\mathbb{F}_q) |\ \det(A) = 1\} \leq GL_n(q)$$

is a group since the determinant is multiplicative. It is called the special linear group.

Remark. It will be needed in Section 6 to define the projective special linear group.

Definition 3.0.8. A (left) group action of a group G on a set X denoted by $G \curvearrowright X$ is a mapping

$$G \times X \to X \ (g,x) \mapsto gx,$$

such that the following condition are satisfied

(i) $e_G x = x$ for all x in X

(ii) $(gh)x = g(hx)$ for all x in X and all g,h in G.

Remark. A group action can be thought of as providing for ever element in G a bijective mapping of X to itself. Let us for g in G define the mapping $\alpha_g : X \to X$ by $x \mapsto gx$. Then $\alpha_e = id_X$. So for g in G every α_g has an inverse $(\alpha_g^{-1}) = \alpha_g^{-1}$. Indeed as the action is associative

$$\begin{aligned} \alpha_g \alpha_g^{-1} = \alpha_{gg^{-1}} = \alpha_e = id_x \qquad & \text{associativity of the action} \\ \alpha_g^{-1} \alpha_g = \alpha_{g^{-1}g} = id_x \qquad & \text{analogously.} \end{aligned}$$

This proves that the mapping is invertible and thus bijective.

We will give a concrete example of an group action. To do so we consider a basic concept from linear algebra and show that it can be described using group theory.

Example 3.0.9. The mapping

$$GL_n(q) \times \mathbb{F}_q^n \to \mathbb{F}_q^n$$

defined by matrix multiplication is a group action.

Proof. We need to verify that the conditions of a group action are satisfied. The neutral element of the mapping is the identity matrix I_n since it satisfies $I_n v = v$ for all v in $\mathbb{F}_q^n$. Then the first condition is satisfied. The mapping is associative, since it is defined by matrix multiplication just as the group law of $GL_n(q)$. □

We continue with group actions and introduce some interesting subset. We will see that we are given a more detailed understanding of the action when we take those sets in consideration.

Definition 3.0.10. The *kernel* of an action is the set $\{g \in G |\ gx = x \ \forall x \in X\}$. The elements in the kernel act trivially on every element of X. An action is *faithful* if its kernel contains only the identity element of G.
The *stabilizer* of x in X is the set $G_x = \{g \in G \mid gx = x\}$.

Remark. The kernel and stabilizer are a subgroup of G.

We now proceed to show by a proposition that the group action in Example 3.0.9 is a faithful action.

Proposition 3.0.11. The action $GL_n(q) \curvearrowright \mathbb{F}_q^n$ is faithful.

Proof. Consider the action $GL_n(q) \curvearrowright \mathbb{F}_q^n$, we claim that it is faithful. We need to prove that its kernel consists of only the identity matrix. So consider the row vector e_k in F_q^n with 1 in the k^{th} entry and zero everywhere else. If A is to be in the kernel of the action, then the equality $Ae_k = e_k$ needs to hold for all $k \in \{1,...,n\}$. But for this to be true for $e_1,...,e_n$ in $\mathbb{F}_q^n$, such an A has to have entry 1 on the diagonal, and zero everywhere else, thus $A = I_n$. Hence our claim that the action is faithfully is justified. □

Definition 3.0.12. The *orbit* of a point x in X under a group action $G \curvearrowright X$ is the set $Gx = \{gx \in X |\ g \in G\}$. If there is only one orbit, the action is called *transitive*.

Remark. If the action is transitive then for every x, y in X we have that $x = gy$ for some g in G.

Definition 3.0.13. Two element a, b in G are said to be *conjugate* in G if $gag^{-1} = b$ for some g in G. The orbits of G by conjugation are called the *conjugacy classes of* G.

We continue with mappings and consider the mapping of a group onto another group.

Definition 3.0.14. Given two groups G, H the mapping $\gamma : G \to H$ is called a *homomorphism* if and only

$$\gamma(ab) = \gamma(a)\gamma(b) \quad \text{for all } a, b \in G.$$

A homomorphism that is bijective is called an *isomorphism*. Then G and H are *isomorphic* which is denoted by $G \cong H$.

Remark. If $G \cong H$ then $|G| = |H|$ and G is abelien if and only if H is abelien. The order of group elements is preserved under isomorphism.

At the end of this section, we will stat and prove an isomorphism theorem. We begin by stating and proving some propositions and introducing some definition

Proposition 3.0.15. If $\gamma : G \to H$ is a homomorphism, then $\gamma(e_G) = e_H$ and $\gamma(g^{-1}) = \gamma(g)^{-1}$ for all g in G.

Proof. Let $\gamma : G \to H$ be a homomorphism. We claim that $\gamma(e_G) = e_H$. Indeed γ is a homomorphism

$$\gamma(e_G) = \gamma(e_G e_G) = \gamma(e_G)\gamma(e_G),$$

then it follows that

$$e_H = \gamma(e_G)^{-1}\gamma(e_G) = \gamma(e_G)^{-1}\gamma(e_G)\gamma(e_G) = \gamma(e_G^{-1}e_G)\gamma(e_G) = \gamma(e_G).$$

This justifies our claim. We want to show that $\gamma(g)^{-1} = \gamma(g^{-1})$ for all g in G. We first observe that for all g in G, then

$$\gamma(g)^{-1}\gamma(g) = \gamma(e_G) = e_H \tag{1}$$

which proves that $\gamma(g^{-1}) = \gamma(g)^{-1})$ holds for all g in G. Hence our claim is justified. □

Definition 3.0.16. The *kernel* of a homomorphism $\gamma : G \to H$ is the set

$$\ker(\gamma) = \{g \in G \mid \gamma(g) = e_H\}.$$

Proposition 3.0.17. If $\ker(\gamma)$ is the kernel of a homomorphism $\gamma : G \to H$, then $\ker(\gamma)$ is a subgroup of G.

Proof. Observe that Proposition 3.2 implies that e_G is in $\ker(\gamma)$. We claim that $\ker(\gamma)$ is a subgroup of G. Suppose that g_1 and g_2 are in $\ker(\gamma)$, then

$$\gamma(g_1 g_2^{-1}) = \gamma(g_1)\gamma(g_2^{-1}) = \gamma(g_1)\gamma(g_2)^{-1} = e_H e_H^{-1} = e_H.$$

Thus proving that $\ker(\gamma)$ is closed under taking inverses and group products. Hence our claim that $\ker(\gamma)$ is a subgroup of G is satisfied. □

We will now give a concrete example of a homomorphism. We will consider the general linear group for the example. We will also see that the special linear group is the kernel of that homomorphism.

Example 3.0.18. Consider the determinant $\det : GL_n(F_q) \to F_q^x$. It is a homomorphism, and its kernel is $SL_n(q)$.

At the end of this section, we will stat and prove two theorems. We begin by introducing some definitions and proceed from there.

Definition 3.0.19. A *left coset* of N in G is a subset of the form $gN = \{gn \mid n \in N\}$ for some g in G. Similarly a *right coset* is a subset $Ng = \{ng \mid n \in N\}$ for some g in G.

Definition 3.0.20. If a subgroup N of G is invariant under conjugation by any element of G, then N is a *normal subgroup*, denoted by $N \trianglelefteq G$.

Remark. If $N \leq G$ is a normal subgroup, then all left N-coset are right N-cosets and vice versa. Indeed $gN = gN(g^{-1}g) = (gNg^{-1})g = Ng$ for all g in G. If N is a normal subgroup of G and $N \neq G$, then N is a proper normal subgroup, denoted by $N \triangleleft G$.

To prove the isomorphism theorem, we must first introduce and verify the following statement.

Theorem 3.0.21. If G is a group with normal subgroup N, then the set of cosets G/N is a group.

Proof. We claim that the set of cosets G/N is a group. To verify this, we first defined the product $(g_1N)(g_2N) = g_1g_2N$ on G/N. We need to show that the product is well-defined. If $gN = hN$ for g, h in G, then there is n in N such that $g = ge = hn$. So we have to prove that for g_1, g_2 in G and n_1, n_2 in N the following the equality holds

$$(g_1n_2)(g_2n_2)N = g_1g_2N.$$

But N is normal in G, so

$$g_1n_1g_2n_2 = g_1g_2(g_2^{-1}n_1g_2)n_2 = g_1g_2nn_2,$$

thus

$$(g_1n_1)(g_2n_2)N = g_1g_2nn_2N = g_1g_2N,$$

and the equality holds. From our definition of the product of G/N associativity follows. Furthermore eN is the identity element and $g^{-1}N$ is the inverse of gN. Hence our claim that G/N is a group is justified. □

Definition 3.0.22. If N is a normal subgroup of G, then the group of cosets G/N is called the *quotient group*.

Theorem 3.0.23. Let G and H groups and let $\gamma : G \to H$ be a homomorphism, then the kernel K is a normal subgroup of G, and G/K is isomorphic to the image $\gamma(G)$.

Proof. We claim that $K \triangleleft G$ and that G/K is isomorphic to the image of γ. Observe that K is a subgroup of G. If K is a normal subgroup G, then this verifies the existence of G/K. To prove that K is normal in G, we need only show that K is invariant under conjugation by any g in G. Let k be in K and g in G, then

$$\gamma(gkg^{-1}) = \gamma(g)\gamma(k)\gamma(g^{-1}) = \gamma(g)\gamma(g^{-1}) = \gamma(gg^{-1}) = \gamma(e_G) \in K,$$

thus verifying that K is normal, and the existence of G/K. We claim that G/K is isomorphic to $\gamma(G)$. We first show that there exists a well-defined mapping, then that the mapping is a homomorphism and bijective. Suppose that $\omega : G/K \to H$, defined by $\omega(gK) = \gamma(g)$ for all g in G and some $\gamma(g)$ in H. We need ω to a well-defined mapping. Suppose that $gK = g'K$, then $g = g'k$ for some k in K, and

$$\omega(gK) = \gamma(g) = \gamma(g'k) = \gamma(g')\gamma(k) = \omega(g'K),$$

thus ω is well-defined. Observe that ω maps G/K to the image $\gamma(G)$, since K is the kernel of γ, it follows that

$$\omega(gKg'K) = \omega(gg'K) = \gamma(gg') = \gamma(g)\gamma(g') = \omega(gK)\omega(g'K)$$

for any gK in G/K. This proves that ω is a homomorphism. The statement holds if ω is bijective, which is equivalent to ω being surjective and injective. We first check subjectivity. If $\gamma(g_1)$ in $\gamma(G)$, then g_1K is in G/K, which implies that $\omega(g_1K) = \gamma(g_1)$, thus ω is surjective. We proceed to check that ω is invective. Let g, g' be in G/K, such that $\omega(gK) = \omega(g'K)$, then

$$\omega(gK)\omega(g'K)^{-1} = \omega(gg'^{-1}K) = \gamma(g)\gamma(g^{-1}) = \gamma(e),$$

which implies that $\gamma(g) = \gamma(g')$ and injective, thus concluding that ω is bijective. Hence our claim that $G/K \cong \gamma(G)$ is satisfied. □

We complete this section by defining the simple group.

Definition 3.0.24. If G is a group, such that the only normal subgroups are the trivial group and G, then G is called a *simple group*.

4 Composition series

4.1 Zassenhaus' Lemm

In this subsection, we will state and prove Zassenhaus' Lemma, which is a statement regarding isomorphisms between quotient groups, the quotients are products of subgroups and intersections, thus before proving the Zassenhaus' Lemma, we need to give some statements and proofs which will convince us that the products are in fact subgroups and that we can have isomorphic subgroup quotients. We start by stating a lemma about subgroup products.

Lemma 4.1.1. If N and H are subgroups of G and $N \trianglelefteq G$, then NH is a subgroup of G. If N and H are normal subgroups of G, then $NH \trianglelefteq G$.

Proof. Let $NH = \{nh \in G \mid n \in N,\ H \in H\}$ we claim that NH is a subgroup of G. Observe that NH is clearly non-empty.To verify that NH is closed under products, one simply uses that N is normal in G and some algebraic manipulation. Suppose that n_1h_1 and n_2h_2 are in NH, then by writing $n_3 = h_1n_2h_1^{-1}$ we obtain,

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1n_3h_1h_2 \in NH,$$

thus verifying that NH is closed under products. It remains to show that NH is closed under taking inverses. Suppose that (nh) is in NH, then from $N \trianglelefteq G$, it follows that

$$(nh)^{-1} = h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1} = n'h^{-1} \in NH,$$

thus proving closedness taking inverses. Hence NH is a subgroup. We proceed to verify the second statement. Suppose that N and H are normal in G and consider any element nh in NH and g in G, then

$$g(nh)g^{-1} = g(ng^{-1}gh)g^{-1} = (gng^{-1})(ghg^{-1}) = n'h' \in NH.$$

Hence NH is a normal subgroup of G. □

Remark. Observe that N is normal in all of G, thus N is normal in NH.

Definition 4.1.2. The intersection of subgroups H,N in G is the set $\{x : x \in H \wedge x \in N\}$. The set is called the *intersection of subgroups* H and N, denoted $H \cap N$,

Lemma 4.1.3. The intersection of subgroups H and N in G is a subgroup of G. If N is normal in G, then $H \cap N$ is a normal subgroup of H.

Proof. Observe that for any H and N in G, the intersection of subgroups is non-empty. In the first statement, we claim that the $H \cap N = \{x : x \in H \wedge x \in N\}$ is a subgroup of G. To justify our claim, we need to show that $H \cap N$ is closed under products and taking inverses. Suppose that we have x, y in $H \cap N$, which implies that xy^{-1} is in H and N, since H and N are subgroups of G. But if xy^{-1} is in H,N, then xy^{-1} is also in $H \cap N$. Thus we have verified that $H \cap N$ is nonempty closed under products and taking inverse, and our claim that the intersection of subgroups is a subgroup is justified. Observe that the intersection subgroups $H \cap N$ is contained in N and H, thus a subgroup of H,N.

Furthermore, we claim that if $H, N \leq G$, and N is a normal subgroup of G, then their intersection $N \cap H$ is normal in H. Our claim is justified if we can show that $H \cap N$ is invariant under conjugation by any h in H. Now assume that x is in $H \cap N$, and consider the conjugate of x by any h in H, that is hxh^{-1}. Then the conjugate is clearly an element of $H \cap N$, since H is a subgroup of G and N is normal in G, it follows that $H \cap N$ is invariant under conjugation. Hence $H \cap N$ is a normal subgroup of$H$. □

Remark. Observe that it is not generally the case that $H \cap N$ is normal in all of G, even if H or N is normal in G. For this to be true in general, we need for both N and H to be normal in G. Which implies that for any x in $H \cap N$, the conjugate of x by any g in G. That is gxg^{-1} is an element of N and H. This is clearly true for all x in $H \cap N$, since we have that $H, N \trianglelefteq G$, so it follows that $g(H \cap N)g^{-1}$ is in $H \cap N$ for any g in G. Thus $H \cap N$ is invariant under conjugation by any g in G, so $H \cap N$ is normal in G.

We can now state and prove one of the isomorphism theorems. The proof applies Lemma[4.1.1] and Theorem[3.0.23]. The theorem will then be used in the proof of Zassenhaus' Lemma

Theorem 4.1.4. Let H and N be subgroups of G, and let N be normal in G, then HN/N is isomorphic to $H/(H \cap N)$.

Proof. Observe that by the conditions of our statement, we can apply Lemma[4.1.1], and N is normal in all of G, thus verifying the existence of HN/N. We claim that the quotient groups are isomorphic. If the conditions of Theorem [3.0.23] are satisfied, then $H/H \cap N$ is isomorphic to HN/N. Consider $\gamma : H \to HN/N$ defined by $\gamma(h) = hN$ for h in H. Since γ is the composition mapping of embedding of H into HN with the quotient mapping HN to HN/N, it follows that γ is a homomorphism. Our claim is justified if the kernel of γ is equal to $H \cap N$. We first show that $H \cap N$ is contained in the kernel, then the converse. Suppose that h' is in $H \cap N$, then $\gamma(h') = h'N$. But h' is contained in both H and N, thus $\gamma(h') = h'N = N$, which shows that $(H \cap N)$ is contained in $\ker(\gamma)$. Conversely, if h is any non-trivial element in H, such that h is in the kernel of γ, then we have that $\gamma(h) = N$, which implies that and h is in N and $H \cap N$, thus proving that kernel of γ is contained $H \cap N$. Hence by Theorem[3.0.23] our claims is justified. □

We will offer a final observation about subgroups and intersections of subgroups, which we present in the following proposition.

Proposition 4.1.5. (Dedekind modular law) If X, Y and Z are subgroups of G, and Y is contained in X. Then the intersection $X \cap (YZ)$ is equal to $Y(X \cap Z)$.

Proof. For the subgroups $Y \leq X$ and Z in G, suppose that we have the intersections of subgroups $X \cap Z = \{a : \ a \in X \wedge \ a \in Y\}$, and that we have the following product of groups subset, $YZ = \{yz : y \in Y, \ z \in Z\}$ and $Y(X \cap Z) = \{ya : \ y \in Y \wedge, a \in X \cap Z\}$. We claim have that $X \cap (YZ)$ and $Y(X \cap Z)$ are equivalent, that is we claim that the following equality holds $X \cap (YZ) = Y(X \cap Z)$. For this to be true, we need for the inclusion $X \cap (YZ) \subseteq (X \cap Z)$, and its converse to be true. Note that a subgroup products subset is not necessarily a subgroup of G, and note that $X \cap (YZ)$ and $Y(X \cap Z)$ are both contained in X. Let a be in $X \cap (YZ)$, which implies that there is some yz in YZ, such

that $a = yz$, then $x = yz$ for some x in X. Which is equivalent to $y^{-1}x = z$, since both x, y are in $Y \leq X$, so it follows that z is in X and Z. Hence z is in the intersection of X and Y, and $a = yz$ is in $Y(X \cap Z)$ for any a in $X \cap (YZ)$. Before proving the converse, observe that $Y(X \cap Z) \subseteq X \cap (YZ)$ is just the product of subset with intersection, for which the intersections are subsets of the same set. So we can conclude that

$$Y(X \cap Z) \subseteq (Y \cap X) \cap (Y \cap Z) = X \cap (YZ).$$

Hence the inclusions $X \cap (YZ) \subseteq Y(X \cap Z)$ and its converse have been verified, and the statement that $X \cap (YZ) = Y(X \cap Z)$ is justified. □

Now we have the relevant statements and proofs needed for us to prove Zassenhaus' Lemma.

Theorem 4.1.6. (Zassenhaus' Lemma) Let A and B be subgroups of G, and let N_A be a normal subgroup of A, and let N_B a normal subgroup of B, then the quotient groups are all isomorphic

$$\frac{N_A(A \cap B)}{N_A(A \cap N_B)} \cong \frac{A \cap B}{(N_A \cap B)(A \cap N_B)} \cong \frac{N_B(A \cap B)}{N_B(N_A \cap B)}.$$

Proof. The following proof is based on [[2], Theorem 70]. Since the Theorem's statement is symmetric in both A and B, we need only prove the first two isomorphisms. We will prove the isomorphism statement by applying Theorem[4.1.4]. Before we can do this, we must first verify that the quotient groups in the statement exists. Suppose that $N_A \trianglelefteq A$ and $N_A \trianglelefteq B$, and that $A, B \leq G$. Then the intersection $A \cap B$ is a subgroup of G, with normal subgroups $N_A \cap B$ and $A \cap N_B$, Lemma[4.1.3]. Thus $(N_A \cap B)(A \cap N_B)$ is normal in $A \cap B$, by Lemma[4.1.1]. Which implies the existence of the quotient group

$$\frac{(A \cap B)}{(N_A \cap B)(A \cap N_B)}.$$

We continue with the two remaining quotients it suffices to show the existence of one, and outline the proper steps for its analog. Before we can verify the existence of the quotient group

$$\frac{N_A(A \cap B)}{N_A(A \cap N_B)},$$

we first need to show that $N_A(A \cap B)$ is a subgroup of G, it suffices to show that $N_A(A \cap B)$ is a subgroup of A. We do this by simply checking the assumptions in Lemma[4.1.1], thus we conclude that $N_A \trianglelefteq A'(A \cap B)$ is a subgroup of A. So we have that N_A is a normal subgroup of $N_A(A \cap B)$, we need for $N_A(A \cap N_B)$ to be normal in $N_A(A \cap B)$. To get the desired normal subgroup, we must first show that $(A \cap B')$ is a subgroup of $N_A(A \cap B)$. We use the fact that we have the following inclusion $A \cap B' \subseteq A \cap B$, and that and B, are all subgroups of G, then by applying Proposition[4.1.5] to $N_A(A \cap B)$, we get the following equality,

$$N_A(A \cap B) = N_A(A \cap (A \cap N_B)B) = N_A(A \cap N_B)(A \cap B),$$

which provides the desired result, $(A \cap N_B) \leq N_A(A \cap B)$. Therefore we can now conclude that $N_A(A \cap B')$ is a normal subgroup of $N_A(A \cap B)$, by Lemma[4.1.1]. This implies the existence of the quotient group,

$$\frac{N_A(A \cap B)}{N_A(A \cap N_B)} = \frac{N_A(A \cap N_B)(A \cap B)}{N_A(A \cap N_B)}.$$

To verify the existence of the quotient group $N_B(A \cap B)/N_B(N_A \cap B)$, we simply recall that $N_B \trianglelefteq B$ and that $(A \cap N_B) \leq (A \cap B)$ and N_B are all subgroups of B. Hence the desired results will follow after making the appropriate adjustments to the previous arguments of its analog. Before proving the first isomorphism statement, that is

$$\frac{N_A(A \cap N_B)(A \cap B)}{N_A(A \cap N_B)} \cong \frac{A \cap B}{(N_A \cap B)(A \cap N_B)}.$$

We recall first the assumptions of Theorem[4.1.4], thus we need only show that

$$N_A(A \cap N_B) \cap (A \cap B) = (N_A \cap B)(A \cap N_B).$$

To show that the equality holds, we apply Proposition[4.1.5] to the left hand side and deduce that

$$N_A(A \cap N_B) \cap (A \cap B) = (N_A \cap A \cap B \cap B)(A \cap N_B \cap A \cap B) = (N_A \cap B)(A \cap N_B).$$

We then use the analogous argument for $B(N_A \cap B) \cap (A \cap B)$. Hence the isomorphism claim is justified by Theorem [4.1.4], so from symmetry it follows that

$$\frac{N_A(A \cap B)}{N_A(A \cap N_B)} \cong \frac{A \cap B}{(N_A \cap B)(A \cap N_B)} \cong \frac{N_B(A \cap B)}{N_B(N_A \cap B)},$$

and the statement is verified. □

4.2 Jordan-Hölder theorem

In this section, we will prove one of the main results of the thesis, namely the Jordan-Hölder theorem. The theorem fits into the analogy presented in the introduction regarding viewing simple groups as building blocks of groups. We first give relevant definitions paired with some concrete examples based on [[8], Section 10.1], then continue to prove statements needed for the main result.

Definition 4.2.1. A sequence of subgroups

$$e = 0 \leq H_0 \leq H_1 \leq \cdots \leq H_n = G$$

is called a *subgroup series*, denoted $(H_k)_{k \in [0,n]}$. A sequence of normal subgroups

$$e = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = G$$

is called a *normal series*, denoted $\langle N_k \rangle_{k \in [0,n]}$. The quotient groups N_k/N_{k+1} are called *factor groups*.

We will give an example of a normal series, which will do by considering the quotient group of integers modulo 20.

Example 4.2.2. Let $Z/20$ and let d denote all the d-multiplies of element in $Z/20$. Then $Z/20$ as the following normal series $0 \triangleleft 2Z/20 \triangleleft Z/20$.

In some cases, we can refine a normal series, resulting in a series containing new factor groups. We give a definition then show by an example a refined version of a normal series.

Definition 4.2.3. If for the normal series $\langle N_k \rangle_{k\in[0,n]}$ of G, there exist another normal series $\langle M_l \rangle_{l\in[0,m]}$ of G, such that $\langle N_k \rangle_{k\in[0,n]}$ is contained in $\langle M_l \rangle_{l\in[0,m]}$. Then $\langle M_l \rangle_{l\in[0,m]}$ is a *refinement* of the normal series, that is $\langle N_k \rangle_{k\in[0,n]} \subseteq \langle M_l \rangle_{l\in[0,m]}$. A proper refinement of $\langle N_k \rangle_{k\in[0,n]}$ is a refinement that is not equal to $\langle N_k \rangle_{k\in[0,n]}$.

In Example[4.2.2], we constructed a normal series from the quotient group of the integers module 20. We will now give an example of a refinement of the series.

Example 4.2.4. Indeed the normal series $0 \triangleleft 2Z/20 \triangleleft Z/20$ has the following proper refinement $0 \triangleleft 10Z/20 \triangleleft 2Z/20 \triangleleft Z/20$

We will offer another example of a normal series and proper refinement. Before we can do this, we must first introduce some new groups.

Definition 4.2.5.

- The group of all bijections on the set $\{1,...,n\}$ is called the symmetric group of order n, denoted S_n.
- The group consisting of exactly the permutations that can be expressed as an even product of transpositions is called the alternating group, denoted A_n
- The unique non-cyclic group of order 4, denoted V_4 is called the Klein-4 group. It is unique up to isomorphism.

Remark. Observer that the parity of the number of the decomposition of a permutation in to products of transposition is unique, [[5], Section 3.5].

Example 4.2.6. The following example is based on [[8], Example 10.1.1]. Consider the symmetric group S_4 with has a normal series $e \triangleleft A_4 \triangleleft S_4$. The normal series has following proper refinement $e \triangleleft \mathbb{Z}/\mathbb{Z}_2 \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$. Observe that the factor groups in the refinement have prime order, thus there exists no further refinement.

Remark. The group V_4 is the subgroup of order 4, which is normal in S_4 and A_4.

Definition 4.2.7. Given two normal series $\langle N_k \rangle_{k\in[0,n]}$ and $\langle N'_k \rangle_{l\in[0,n']}$, we denoted their factor groups by $F_k = N_{k+1}/N_k$ and $F'_{k'} = N_{k'+1}/N_k$ for $k > 0$. We say that the normal series are equivalent. If and only if $n = n'$ and there exists a permutation, σ in S_n, such that $F_k \cong F'_{\sigma(k)}$ for all k in $[1,n]$.

Definition 4.2.8. If for two refinements $\langle C_k \rangle_{k\in[0,n]}$ and $\langle C'_l \rangle_{l\in[0,m]}$ of two normal series in G, for which there exists equivalent factor groups. Then the refinements have equivalent refinement terms. If this is true for every distinct term in the refinements, then the normal series have equivalent refinements.

We now have a collection of relevant definitions and statements needed to prove Schreier's Theorem. The proof is constructed by producing two refinements, then applying Zassenhaus' Lemma to the factor groups in the refined normal series.

Theorem 4.2.9. (Schreier's Refinement Theorem) Any two normal series of the same finite group G have equivalent refinements.

Proof. The following proof is based on [[2], Theorem 72] Given two normal series of G, that is

$$e = N_0 \trianglelefteq N_1 \ldots \trianglelefteq N_{n-1} \trianglelefteq N_n = G \quad \text{and} \quad e = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{m-1} \trianglelefteq H_m = G.$$

We want to construct refinements for $\langle N_i \rangle_{i\in[0,n]}$ and $\langle H_j \rangle_{j\in[0,m]}$ in G, such that the their refinements have the same length, and equivalent refinement terms. To construct a refinement, we must first construct a new series,

$$e = \tilde{N}_0 \trianglelefteq \tilde{N}_1 \ldots \trianglelefteq \tilde{N}_{nm-1} \trianglelefteq \tilde{N}_{qm} = G \quad \text{and} \quad \tilde{N}_{in} = N_i$$

We define the terms in the series by $\tilde{N}_k = N_q(N_{q+1} \cap H_r)$, for $k = qm + r$,with $0 \leq q < n$ and $0 \leq r \leq m$. We need to verify that $\tilde{N}_k$ is well-defined, that is that

$$N_q(N_{q+1} \cap H_m) = N_{q+1}(N_{q+2} \cap H_0)$$

Recall that $H_m = G$ and $H_0 = e$, so

$$N_q(N_{q+1} \cap H_m) = N_q(N_{q+1} \cap G) = N_q N_{q+1} = N_{q+1},$$

and

$$N_{q+1}(N_{q+1} \cap H_0) = N_{q+1}(N_{q+2} \cap \{e\}) = N_{q+1}.$$

Hence our $\tilde{N}_k$ is well-defend. Furthermore our construction of $\tilde{N}_k$, implies that each term in $\langle N_i \rangle_{i\in[0,n]}$ is equal to some $\tilde{N}_k$ in the new series. For the new series to be a refinement of the original series $\langle N_i \rangle_{i\in[0,n]}$, we must first show that $\tilde{N}_k$ is normal subgroup in $\tilde{N}_{k+1}$. We first recall that H_j is normal in H_{j+1}. Therefore if we consider the term $\tilde{N}_{k+1} = N_{q+1}(N_{q+2} \cap H_{r+1})$ and $r < m$. Then it follows that

$$\tilde{N}_k = N_q(N_{q+1} \cap H_r) \trianglelefteq N_{q+1}(N_{q+2} \cap H_{r+1}) = \tilde{N}_{q+1},$$

which shows that $\tilde{N}_k$ is normal $\tilde{N}_{k+1}$. Observe that there might exist some numbers k for which $\tilde{N}_k = \tilde{N}_{k+1}$. Therefore we can not yet verify that our new series is in fact a normal series, and thus a refinement of $\langle N_i \rangle_{i\in[0,n]}$. Before we can treat this aspect, we construct the analogue of $(\tilde{N}_k)_k$ for $\langle H_i \rangle_{\in[0,m]}$

$$e = \tilde{H}_0 \trianglelefteq \tilde{H}_1 \ldots \trianglelefteq \tilde{H}_{nm-1} \trianglelefteq \tilde{H}_{nm} = G \quad \text{and} \quad \tilde{H}_{jm} = H_j$$

and setting $\tilde{H}_l = H_q(H_{q+1} \cap N_r)$, for $l = nq + r$, where $0 < q \leq m$ and $0 \leq r \leq n$. The previous arguments hold analogously for $\tilde{H}_k$. Let $k = um + v$ and $l = sn + t$, then the factor groups $\tilde{N}_{k+1}/\tilde{N}_k$ and $\tilde{H}_{l+1}/\tilde{H}_l$ can expressed as

$$\frac{N_{k+1}}{N_k} = \frac{N_u(N_{u+1} \cap H_{v+1})}{N_u(N_{u+1} \cap H_v)} \quad \text{and} \quad \frac{H_{l+1}}{H_l} = \frac{H_s(H_{t+1} \cap N_{t+1})}{H_s(H_{s+1} \cap N_t)}.$$

Thus by applying Zassenhaus' Lemma [4.1.6], we conclude that there exists a permutation, denoted σ, in S_{mn}, such that the factor groups, $\tilde{N}_{k+1}/\tilde{N}_k$ and $\tilde{H}_{l+1}/\tilde{H}_l$ are isomorphic. Now all we have to do is remove any redundant terms of the series. This is done by observing that there is an equal number of trivial inclusions $\tilde{N}_k = \tilde{N}_{k+1}$ and $\tilde{H}_l = \tilde{H}_{l+1}$. Therefore after removing suitable terms from $(\tilde{N}_k)_k$ and $(\tilde{H}_l)_l$, we obtain equivalent refinements, that is $\langle \tilde{N}_k \rangle \cong \langle \tilde{H}_k \rangle$, and our claim is justified. □

We now have acquired the tools needed for the main theorem of this section. Before stating and proving the Jordan-Holders Theorem, we introduce the definition of a normal series consisting of simple factor groups.

Definition 4.2.10. A a normal series in which the factor groups are simple is called a *composition series*.

Remark. It is possible to think of the composition series as a normal series which has no proper refinements.

To prove the main result of this section, we will apply Schreier's theorem and consider the remark made in the definition of the compositions series.

Theorem 4.2.11. (Jordan-Hölder) Let G be a finite group, then any two composition series of G are equivalent to etch other.

Proof. Observe that a composition series, admits no proper refinements of the series. Therefore, Schreier's Theorem applies to a pair of compositions series, providing the desired conclusion. □

5 Classic simple finite groups

5.1 Iwaswa's Lemma

The classic simple groups consist of six families of simple groups, the linear, unitary, symplectic groups and three families of orthogonal groups. In this thesis, we will prove the simplicity of the projective special linear group and the projective symplectic group. Their simplicity will be proven by applying Iwasawa's Lemma on the general cases. This subsection is devoted to stating and proving Iwasawa's Lemma, which uses a stronger form of transitive group actions and a specific type of group property to prove that simplicity of the group. We begin by giving the relevant definitions and statements needed to verify Iwasawa's Lemma.

Definition 5.1.1. A proper subgroup M is a *maximal subgroup* of G if its not contained in any other proper subgroup H in G.

Remark. The term maximal will be used when it is clear from the context that we are referring to a maximal subgroup.

Definition 5.1.2. A *block system* for $G \curvearrowright \Omega$, is a set of partitions of the set Ω preserved by the group G. The partitions are mutually disjointed non-empty subsets, whose unions is Ω, and are referred to as *blocks*.

Definition 5.1.3. The *trivial block system* are the block system consisting of the single block Ω, and the block system of the partition by singletons. A non-trivial block system is called a *system of imprimitivity*. Any group action admitting a system of imprimitivity is called imprimitive.

Remark. The trivial block system is preserved for every group G.

Definition 5.1.4. Any group that is non-empty and not imprimitive is called primitive.

Lemma 5.1.5. A transitive group action is primitive if and only if all point stabilizers are a maximal subgroup.

Proof. The following proof is based on [[9], Proposition 2.1]. Let $G \curvearrowright \Omega$ be transitive and take x in Ω. We claim that the action is primitive if and only if G_x is a maximal subgroup of G. Suppose that the group action is primitive and that $H = G_x$ is not maximal, then there exist K such that $H < K < G$. Observe that there exists a natural bijection between the points in Ω and the cosets gH in G, since $g(xH) = gxH$. But $H < K$ and the cosets of K in G are unions of H-cosets, thus sets can be identified with a partition of Ω, this implies the existence of a non trivial block system, which contradicts the assumption that the action is primitive. Conversely, assume that G acts transitively and imprimitive on Ω, and fix x in Ω. Then x is contained in some imprimitive block, denote the block Ω_x. Since the action is transitive, it follows that the stabilizer of Ω_x acts transitively on itself, and not on Omega. Thus H is contained in the stabilizer of Ω_x, that is G_{Ω_x}. This contradicts the assumption that H is maximal. Hence our claim is justified. □

Before stating Iwasawa's Lemma, we need to formalize a certain type of group property. We do this by first giving a definition, then stating and proving a proposition.

Definition 5.1.6. Let G be a group and let x, y be in G. The element $[x,y] = xyx^{-1}y^{-1}$ is called the *commutator* of x and y.

Remark. The commutator is equal to identity if and only if x, y commute.

Definition 5.1.7. The subgroup $\langle [x,y] \mid x,y \in G \rangle$ in G is called the commutator subgroup, denoted G'.

Remark. Observe that the set $G' = e[x,y] \mid x,y \in G\rangle$ is a subgroup by definition.

Proposition 5.1.8. The commutator subgroup $G' \leq G$, is a normal subgroup of G.

Proof. We claim that G' is a normal subgroup of G. To verify this claim, we simply check that G is invariant under conjugation by any g in G. It suffices to show that the conjugate of a commutator is again a commutator. Consider the commutator subgroup of G. Suppose that $[x,y]$ is in G', then the conjugate of $[x,y]$ by any g in G is,

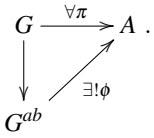
$$\begin{aligned} g[x,y]g^{-1} &= g(xyx^{-1}y^{-1})g^{-1} \\ &= gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} \\ &= (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} \\ &= [gxg^{-1}, gyg^{-1}]. \end{aligned}$$

Thus proving that the conjugate of a commutator $[x,y]$ is another commutator, so the subgroup G' is a normal subgroup of G. □

The commutator subgroup allow us to understand how close a non-commutative group is to being abelian. This is defined and formalist in the next definition and proposition.

Definition 5.1.9. The abelian quotient group of group G by its commutator subgroup G' is called the abelianization of G, denoted G^{ab}.

Proposition 5.1.10. Let G be a group with the non-trivial subgroup G', then for every abelian group A and every homomorphism $\pi : G \to A$, there exists a unique homomorphism $\phi : G^{ab} \to A$, such that the following diagram commutes,



In particular G/N is abelien if and only if $G' \leq N$.

Proof. Let G be a non-commutative group, this means $1 \nleq G' \trianglelefteq G$, and let A be abelian. We claim that for every homomorphism $\pi : G \to A$, there exists a unique homomorphism denoted ϕ, such that $\phi : G^{ab} \to A$, for which the previous diagram commutes. To do verify the claim we simply apply Theorem[3.0.23], we first make the following observation regarding π. Observer that since the homomorphism $\pi : G \to A$ maps any non-commutative group G into an abelian group A, it follows that the image $\pi(G)$ is commutative, this means that for any x,y in G

$$\pi(xy) = \pi(x)\pi(y) = \pi(y)\pi(x) = \pi(yx),$$

thus the kernel $\ker(\pi)$ is contained in $G' \trianglelefteq G$,

$$\pi(xy)\pi(yx)^{-1} = \pi(xyx^{-1}y^{-1}) = \pi([x,y]) = e_A.$$

Observer that the converses inclusion is also true, that is any commutator $[x,y]$ in G' also gets mapped to the identity in A. Thus the kernel $\ker(\pi)$ is equal to the the commutator subgroup in G' in G. So by Theorem[3.0.23] there exists a mapping $\phi : G/G' \to A$ such that ϕ is a isomorphism. But if ϕ is the isomorphism $\phi : G/G' \to A$l, then G/G' is the abelianization of G, and since ϕ it is the composition mapping of the embedding of G into G/G' with the mapping $G/G' \to A$, it follows that ϕ is a unique homomorphism. Hence the diagram commutes and our claim is justified. To prove the last statement, that is that G/N is abelian if and only if the commutator subgroup G' is in $N \trianglelefteq G$. Suppose that G/N is abelian and let x,y be in G, then

$$(xN)(yN) = (yN)(xN) = (xyx^{-1}y^{-1})N = N,$$

which implies that $(xyx^{-1}y^{-1}) = [x,y]$ is in N, thus showing that G' is contained in N. Conversely if $G' \leq N$ and $N \trianglelefteq G$, then $xNyN = xNyN$ and $xyx^{-1}y^{-1}N = eN$, which implies that G/N is abelian. Hence our claim is justified. □

Definition 5.1.11. A group with no non-trivial abelian quotient is called a *perfect group*.

Theorem 5.1.12. (Iwasawa's Lemma) If G is a finite perfect group, acting faithfully and primitively on a set Ω, such that the every point stabilizer has a normal abelian subgroup whose conjugates generate G, then G is simple.

Proof. The following proof is based on [[9], Proposition 2.1]. Let K be a non-trivial subgroup of G. We are going to show that the following equality $K = G$ holds. Since K is non-trivial, there exist some point in Ω, which is not fixed by all of K. We take x in Ω to be such a point, then K is not a subgroup of the stabilizer G_x. We set $H = G_x$ and so $K \nleq H$. Since is H maximal, it follows that $G = HK$, this means that $g = hk$ for any g in G, by h in H and k in K. So every conjugate of A by any g in G can be expressed by

$$g^{-1}Ag = k^{-1}h^{-1}Ahk = k^{-1}Ak \leq AK.$$

Recall that we assume K is normal in G hence the inclusion $k^{-1}Ak \leq AK$ is justified. Since the conjugates of A generate G, it follows that $AK = G$. Thus by Theorem[4.1.4], we find an isomorphism $G/K = K/K \cong A/(A \cap K)$ which implies that G/K is abelian. But G is a perfect group, that is there exists no non-trivial abelianization of G. Therefore the quotient G/K is trivial which proves the desired equality, $K = G$, and so we conclude that G is simple. □

5.2 Projective Special linear groups

In the previous section, we introduced a collection of tools to verify the hypothesis of Iwasawa's Lemma. In this section, and the next one, we will use those tools to show the simplicity of two of the classic finite groups, namely, the projective special linear groups and the projective symplectic group. We do this by first deafening the group as the quotient group of special linear groups. After that, we state and prove a collection of lemmas about the special linear group. This is simply some verification's of the existence of the tools stated in Section 5.1. So that we can apply Iwasawa's Lemma on the projective special linear groups. Besides proving the simplicity of projective special linear groups, we will also derive its order and study two isomorphism cases.

Definition 5.2.1. The set $Z(G) = \{z \in G |\ gz = zg \text{ for all } G\}$ is called the *center* of G.

Remark. Since the identity commutes with ever element it is an element of the center. Thus the center is non-empty.

Proposition 5.2.2. Let G be a group, then $Z(G)$ is a normal abelian subgroup of G.

Proof. We claim that center is a normal abelian subgroup. Let G be a group, and let $Z(G)$ be the center of G. Since associativity of G and the definition of $Z(G)$, ensures closeness under products and taking inverses. It follows that the center is a subgroup of G. Observer that any two elements in $Z(G)$ commute, so it is an abelian subgroup. Since every z in $Z(G)$ commutes with every element g in G, it follows that $Z(G)$ is invariant under conjugation by any element in G. Hence $Z(G)$ is a normal abelian subgroup of G. □

Definition 5.2.3. The **projective special linear groups** denoted $PSL_n(q)$ is defined as the quotient group $SL_n(q)/Z(SL_n(q)$.

Remark. The subgroup $Z(SL_n(q))$ consist of all matrices that commutes with all matrices in $SL_n(q)$. The only matrices that commutes with all of $SL_n(q)$ are the scalar matrices and the identity.

In the previous section, we introduced a stronger form of transitive group action. That is the primitive action. In the next definition, we formulate yet another stronger form of transitivity.

Definition 5.2.4. A group action of G on Ω is called *2-transitive* if for every (x_1,x_2), and (y_1,y_2) in $\Omega\times\Omega$, such that $x_1 \neq x_2$ and $y_1 \neq y_2$. There exists some g in G which satisfies the equality $(gx_1,gx_2) = (y_1,y_2)$.

Remark. This can be reframed by saying that, the action $G,\curvearrowright \Omega$ is 2-transitive if and only if $G \curvearrowright \{(x_1,x_2) \in \Omega^2 \mid x_1 \neq x_2\}$ is transitive.

We give an example of a 2-transitive group action by considering the special linear group and the set of one-dimensional subspaces of of the finite vector space $\mathbb{F}_q^n$. We do this by stating and proving a lemma.

Lemma 5.2.5. The special linear group $SL_n(q)$ acts two transitively on the set of 1-dimensional sub vector spaces of $\mathbb{F}_q^n$, denoted Ω.

Proof. The following proof is based on [[6], Lemma 8.3]. We claim that $SL_n(q) \curvearrowright \Omega$ is two transitive. Let U_1,U_2,V_1,V_2 be one dimensional subspace of $\mathbb{F}_q^n$. We pick a pair of non-zero vectors u_i in U_i and v_i in V_i for i in $\{1,2\}$. To prove this we will directly check the condition spelled out in Definition 5.2.4. This is done by by completing u_1,u_2 and v_1,v_2 respectively, to basis. We will then consider the unique linear invertible map between these basis. In a final step we will modify this map in order to have determinant 1. Recall that given two different one-dimensional subspaces of a vector space, and a non-zero vector in each them, the resulting pair of vectors is linearly independent. Hence, the pairs (u_1,u_2) and (v_1,v_2) are linearly independent. As a consequence, we can complete both to a basis of $\mathbb{F}_q^n$, say $(u_1,...,u_n)$ and $(v_1,...,v_n)$, respectively. Hence we can choose appropriate u_k and v_k so that there exists a unique invertible linear mapping T in $\mathbb{F}_q^n$, described as $T(u_k) = (v_k)$ for all k in $\{1,2,...,n\}$. Note that T is an element of $GL_n(q)$, but not necessarily of $SL_n(q)$. We take c in $\mathbb{F}_q$ to denoted the inverse of $\det(T)$. The tuple $\{cv_1,v_2,...,v_n\}$ is a basis of $\mathbb{F}_q^n$ $\mathbb{F}_q^n$, thus there is a unique invertible linear transformation S, such that $S(cv_1) = v_1$ and $S(v_k) = v_k$, for k in $\{2,3,...,n\}$. It follows that

$$\det(S)\det(T) = c\det(T) = c\lambda = \lambda^{-1}\lambda = 1.$$

This proves that the product ST is in $SL_n(q)$. Since $\mathbb{F}_q^n cv_1 = \mathbb{F}_q^n v_1$, it follows that ST maps the pair of subspace (U_1,U_2) to the pair (V_1,V_2). □

Remark. The kernel of the action is the set of scalar matrices and geometrically the action maps bases to bases up to scalar matrix.

We leave the special linear group for a moment to formulate and prove a statement regarding the 2-transitive action and point stabilizers subgroup.

Lemma 5.2.6. If G acts 2-transitive on the set Ω, then the stabilizer is a maximal subgroup of G, for all x in Ω.

Proof. Suppose that $G \curvearrowright \Omega$ is 2-transitive. We claim that the stabilizer G_x is a maximal subgroup of G for all x in Ω. Recall that 2-transitivity is a stronger form of transitivity. So if we can prove that 2-transitive implies primitive, then all point stabilizers are a maximal subgroup by Lemma[5.1.5]. We need to show that the action is primitive, that is that there exists no non-trivial block systems. Assume that there exists a block containing more than one element of Ω. Since the action is 2-transitive, that it has two orbits, it follows that the block is the partition of Ω into Ω. Thus any non-singleton partition of Ω must be equal to all of Ω. This means that we have no imperative block systems, so G is 2-transitive and primitive. Hence our claim that the stabilizer G_x is a maximal subgroup of G for all x in Ω is justified. □

Remark. Observe that the proof also shows that 2-transitive implies primitive.

We will prove simplicity of projective special linear groups by applying Iwasawa's Lemma.

Theorem 5.2.7. The projective special linear group $PSL_n(q)$ is simple for $(n,q) \neq (2,2)$ and $(n,q) \neq (2,3)$.

Proof. The following proof is based on [[9], Section 3.2.2]. We claim that $PSL_n(q)$ is a simple group, when $(2,2) \neq (n,q) \neq (2,3)$. Let $SL_n(q)$ with $n > 2$ and $q > 3$, and let that Ω denote the set of one-dimensional subspace of $\mathbb{F}_q^n$. We will prove the claim by applying Iwasawa's Lemma[5.1.12]. Consider the action $SL_n(q)$ on Ω and take a point $\langle(1,0,...,0)\rangle$ in Ω, so that H is the stabilizers of that point. Then the action is 2-transitive by Lemma[5.2.6], which implies that the action is primitive. Thus the stabilizers H is a maximal subgroup of $SL_n(q)$. So it suffices to show that there exists a normal abelain subgroup in H, whose conjugates generated $SL_n(q)$. We first prove the existence of a normal abelian subgroup. Since H stabilize the point $\langle(1,0,...,0)\rangle$ in Ω, if follows that H consist of all matrices, so that the first row is $(\lambda,0,...,0)$ for some $\lambda \neq 0$ in $\mathbb{F}_q$. This implies that there exists a subset A in H defined as

$$A = \{\begin{pmatrix} 1 & 0_{n-1} \\ v_{n-1} & I_{n-1} \end{pmatrix} \in M_n(\mathbb{F}_q) \mid v_n \in \mathbb{F}_q^{n-1}\}.$$

Since A satisfies the condition of a subgroup and any non-trivial element in A is an invertible lower triangular matrix, it follows that any two elements in A commute and that A is invariant under conjugation by any element in H, thus A is a normal abelian subgroup of H. Observe that any non-trivial elements of A is a transvection, that is any non-trivial M in A is a shear matrix with $\det(M) = 1$ and rank $(M - I_n) = 1$ and $(M - I_n)^2 = 0$, so all transvections are contained in A. Note that transvections are elementary matrices whose conjugate is still a elementary matrices. We also recall that any matrix with determinant one can be reduced into a sequence of elementary row and column matrices $E(\lambda_{i,j})$ in $\mathbb{F}_q^n$, for λ in $\mathbb{F}_q$ and some $i, j \leq n$, since any such elementary matrix is a transvection, it follows that $E(\lambda_{i,j})$ is in A. Thus every transvection is

contained in some conjugate of A. But if $SL_n(q)$ consists of exactly the matrices with determinant one, then $SL_n(q)$ is contained in some conjugate of A. Hence $SL_n(q)$ is generated by transvections. This part of the proof is based on [[7], Theorem 9.2]. We need to show that $SL_n(q)$ is perfect for $n \geq 2$ and $q > 3$, that is that $SL'_n(q) = SL_n(q)$ when $n \geq 2$ and $q > 3$. It suffices to show that when $n \geq 3$ and $k \neq i, j$ any elementary metrics $E_{i,j}(\lambda)$ is in some commutator $[E_{i,k}(\lambda), E_{k,j}(1)]$ in $SL'_n(q)$. To verify that any elementary matrixs in $SL_n(q)$ for $n > 2$ and $q > 3$ is equal to some commutator of $SL'_n(q)$, we start with $n = 3$ and $q > 3$. We take the commutator $[E_{21}(\lambda), E_{32}(1)]$ in the commutator subgroup $SL'_3(q)$,

$$\left[\begin{pmatrix} 1 & 0 & 0 \\ \lambda & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \right]$$
$$= \begin{pmatrix} 1 & 0 & 0 \\ \lambda & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -\lambda & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\lambda & 0 & 1 \end{pmatrix}$$

Thus the commutator $[E_{21}(\lambda), E_{32}(1)]$ is the elementary matrix $E_{31}(-\lambda)$ in $SL_3(q)$. Since $SL_n(q)$ is generated by transvections, that is a elementary matrices, it follows that after a subtitle choice of basis every transvections is contained in $SL'_n(q)$ whenever $n \geq 3$. Thus is $SL_n(q)$ is a perfect when $n \geq 3$. Furthermore elementary matrices of the kind previously describe do not exist in $SL_2(q)$. This means that the previous augment do not apply for $SL_2(q)$ and $q > 3$. Instead we simply show that there are elements of the normal abelian subgroup A that appears as commutator in $SL'_2(q)$, since the commutator subgroup is a normal subgroup, it immediately follows $SL'_2(q) = SL_2(q)$. This part of the proofs is based on [[1], Lemma 2.8]. Hence conjugates of A generate $SL_2(q)$. Consider the commutator subgroup $SL'_2(q)$, and supposes that $q > 3$. We take a arbitrary commutator in $SL'_2(q)$. Since $q > 3$, there is a non-zero element γ in $\mathbb{F}_q$ such that $\gamma^2 \neq 1$. Fix such an element. Let $\lambda = (1-\gamma^2)^{-1}$. Then $[E_{21}(\lambda), D(\gamma^{-1}, \gamma)]$ is in $SL'_2(q)$, that is

$$\left[\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}, \begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix} \right]$$
$$= \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix} \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \lambda(1-\gamma^2) & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Observe that for $SL_2(q)$, we need for $q > 3$ otherwise $\lambda^2 = 1$ for a non-zero λ in $\mathbb{F}_q$, then we obtain the desired result, that is that there are arbitrary commutators in $SL'_2(q)$ that are also present in A. So by normality of the commutator subgroup $SL'_2(q)$, it follows that $SL_2(q)$ is perfect when $q > 3$. Now before we continue, recall the remark given in Lemma[5.2.5], and since the quotient group of a perfect group is again perfect, it follows that the quotient group $SL_n(q)/Z(SLn(q))$ is perfect. Hence our claim that $PSL_n(q)$ is a simple group whenever $n > 2$ or $q > 3$, is justified by Iwasawa's by lemma[5.1.12]. □

The remaining part of the section will be devoted to deriving the order of the special linear group, and the projective linear group, as well as studying the two cases $PSL_2(2)$ and $PSL_2(3)$. We will see that they are two special cases for when the projective linear group is not simple.

Proposition 5.2.8. The order of $SL_n(q)$ is

$$|SL_n(q)| = \frac{1}{q-1}\prod_{k=1}^{n-1}(q^n - q^k).$$

Proof. We recall that the $\det : GL_n(q) \to F_q$ is a surjective homomorphism. Its kernel is the special linear group as every A in $SL_n(q)$ have determinant 1. The image of the homomorphism is the quotient group and its order is $|GL_n(q)|/|SL_(q)| = q-1$. Thus the order of the special linear group is equal to $|GL_n(q)|/q-1$ as stated.

$$|SL_(q)| = \frac{1}{1-q}\prod_{k=1}^{n-1}(q^n - q^k) = \frac{GL_n(q)}{q-1}.$$

□

Proposition 5.2.9. The order of $PSL_n(q)$ is

$$|PSL_n(q)| = \frac{1}{\gcd(n,q-1)}q^{n(n-1)/2}\prod_{k=2}^{n}(q^i - 1)$$

Proof. We recall that $PSL_n(q) = SL_n(q)/Z(SL_n(q)$ and as the order of $SL_n(q)$ is already known so the problem is reduced to finding the order of $Z(SL_n(q)$. Recall that center of $SL_(q)$ only contains I_n and λI_n. So it suffices to find the number of solutions to $\det(\lambda I_n) = \lambda^n = 1$ for λ $\mathbb{F}_q$. But this equal to the greatest common divisor of $(n, q-1)$, that is $\gcd(n, q-1)$. Therefore the order of the quotient is

$$|SL_n(q)|/(Z(SL_n(q)| = \frac{1}{(n,q-1)}\frac{1}{q-1}\prod_{k=1}^{n-1}(q^n - q^k) = \frac{1}{(n,q-1)}q^{n(n-1)/2}\prod_{k=2}^{n}(q^i - 1)$$

□

Example 5.2.10. The group $PSL_n(q)$ is not simple when (n,q) is equal to $(2,2)$ or $(2,3)$. In particular,

$$PSL_2(2) \cong S_3 \text{ and } PSL_2(3) \cong A_4.$$

Proof. We will verify the statement by considering the two cases separately.

Case 1: We claim that $PSL_2(2)$ is not simple, and that $PSL_2(2)$ is isomorphic to S_3. Let $PSL_n(q)$ by the protective special linear group of order 6, that is $PSL_2(2)$, and take the projective points space $\mathbb{P}$ over $\mathbb{F}_2^2$, yielding the projective lines $\mathbb{P}^2 = X$. To verify the statements, it suffices to show that $PSL_n(q)$ is isomorphic to any of the two non simple group of order 6. Since $PSL_2(2)$ is non-abelain, it follows that the only possible

isomorphism is $PSL_2(2) \cong S_3$. Recall that a group G acting on a set X induce a a homomorphism from $G \to S_{|x|}$, the kernel of the homomorphism is equivalent to the kernel of the action. Since $PSL_2(2)$ acts on X by left multiplication and $Card(X) = 3$, it suffices to show that $PSL_2(2) \curvearrowright X$ is faithful. That is that the kernel of the action is trivial. Since I_2 is the only element that satisfies the condition the kernel, that is $I_2 p = p$ for any p in $\mathbb{P}^2$, it follows that the kernel is trivial. Hence the action is faithful, and so the homomorphism between $PSL_2(2)$ and S_3 is bijective.

Case 2: We claim that $PSL_2(3)$ is not simple, and that $PSL_2(3)$ is isomorphic to A_4. Let $PSL_n(q)$ is by the protective special linear group, and $(n,q) = (2,3)$. To verify the claim, we first need to show that there is non-trivial proper normal subgroup contained in $PSL_2(3)$. So if $PSL_2(3)$ is not simple, then there exists at least one non-trivial normal subgroup in $PSL(2,3)$. Since 12 is the product of distinct prime numbers, it follows by Sylow's Theorem [[7], Section 4.5 Theorem 18] and some direct computations that there exists a unique 2-Sylow normal subgroup in $PSL_2(3)$. Hence $PSL_2(3)$ is not simple. We recall that group structures are preserved under isomorphisms, since $PSL_2(3)$ is a non-commutative group order 12, with a unique 2-Sylow normal, it follows that the only possible isomorphism is $PSL_2(3) \cong A_4$. To verify this, we apply Cayley's Theorem [[5], Section 4.2 Corollary 4], that states that any group G is isomorphic to some subgroup of the symmetric group S_n, we recall the definition of S_n and A_n and choose $n = 4$. If $PSL_2(3) = G$ and S_4, then $PSL_2(3)$ is isomorphic the subgroup of order 12 in S_4, which is the alternating group A_4. Thus our claim that $PSL_2(3) \cong A_4$ is justified by Cayley's Theorem.

□

5.3 Projective symplectic group

In this section, we will prove the simplicity of the projective symplectic group. To do so, we must first introduce the symplectic group. We start by formalizing a definition for the mapping, that is linear in both its arguments and the symplectic basis.

Definition 5.3.1. Let V be a vector space over a field F the map $f : V \times V \to F$ is a *bilinear* mapping if it satisfies the following laws

$$f(\lambda u + v, w) = \lambda f(u,w) + f(v,w)$$

$$f(u, \lambda v + w) = \lambda f(u,v) + f(u,w),$$

for all u, v in V and λ in $\mathbb{F}$. For the bilinear mapping f, we say that

- if $f(u,v) = f(v,u)$, then f is *symmetric*,
- if $f(u,v) = -f(v,u)$, then f is *skew-symmetric*,
- if $f(v,v) = 0$, then f is *alternating*.

We say that f is *non-singular*, if and only if $f(u,v) = 0$ for all v in V implies that $u = 0$.

Remark. The alternating bilinear form is always skew-symmetric, [[9], Definition 3.4.1].

Definition 5.3.2. A *symplectic bilinear mapping* is a alternating non singular bilinear mapping.

Definition 5.3.3. A *symplectic basis* is a ordered pair of vectors $e_1,...,e_m,f_1,...,f_m$ contained in a vector space V paired with symplectic bilinear mapping, such that

- $f(e_i,e_i) = f(f_i,f_i) = 0$
- $f(e_i,f_i) = -f(f_i,e_i) = \lambda \neq 0$,

where f is the *symplectic form* and λ is in $\mathbb{F}_q^{2m}$.

We now have acquired the necessary tools to formalize the definition of the symplectic group. We do this in the next definition.

Definition 5.3.4. Fix a symplectic basis, the *symplectic group* $Sp_{2m}(q)$ is the group of $2m$ squared matrices which preserve the symplectic form f on $V \cong F_q^{2m}$ where V is the symplectic basis.

Before verifying the hypothesis of Iwasawa's lemma for the general case of the symplectic group, we consider the case for $Sp_2(q)$. This is done in the following lemma.

Lemma 5.3.5. The group $Sp_2(q)$ is equal to $SL_2(q)$.

Proof. The following proof is based on [[4], Theorem 2.2.9]. We claim that $Sp_2(q)$ is equal to $SL_2(q)$. Let $Sp_2(q)$ be the symplectic group, and let $V = \mathbb{F}_q^2$ denote the symplectic basis. To verify the claim, we need to show that $Sp_2(q)$ consists of precisely all invariable 2×2 matrices with determinant one. Recall that $Sp_2(q)$ consists of the ordered pair of the symplectic basis V, that preserves the non-singular alternating form. So it suffices to show that the form

$$\det : V \times V \to \mathbb{F}_q$$

$$(u,v) \mapsto \det(u,v)$$

is a symplectic form on V. Since $\det(u,u) = 0$ and $\det(u,v) = -\det(v,u) = \lambda \neq 0$ for any u,v in V and λ in $\mathbb{F}_q$, it follows that det is an alternating bilinear form on the symplectic basis V. Thus $Sp_2(q)$ consist of precisely all invariable 2×2 matrices with determinant one. Hence our claim that $Sp_2(q)$ is equal to $SL_n(q)$ is justified. □

Remark. Observer that this implies that $Sp_2(q)$ is generated by transvections.

The symplectic group is also generated by a type of transvection. We formalize this in the next definition and lemma.

Definition 5.3.6. A *symplectic transvection* is a linear map T such that

$$T_v(\lambda) : x \mapsto x + \lambda f(x,v)v,$$

where f is the symplectic form on V, for which v is a non-zero vector and λ is a non-zero scalar in $\mathbb{F}$.

Lemma 5.3.7. $Sp_{2m}(q)$ is generated by symplectic transvections. In particular $Sp_{2m}(q)$ is a subgroup of $SL_{2m}(q)$.

Proof. The following proof is based on [[9], Theorem 3.5.1]. We claim that $Sp_{2m}(q)$ is generated by symplectic transvections, and that the determinant of a symplectic transvection is equal to one. Let $Sp_{2m}(q)$ be the symplectic group, and let V be the set of ordered symplectic basis of $\mathbb{F}_q^{2m}$. Suppose that $S \leq Sp_{2m}(q)$ is the subgroup generated by symplectic transvection, and let u, v, w be in V, so that v, w are non zero vectors. To verify the claim, we need to show that the subgroup generated by symplectic transvection is equal to the symplectic group. It suffices to show that the subgroup S acts transitively on V. Observer that any such action will induce trivial point stabilizers, and the desired result will follow. We will prove that S is transitive by way of induction. We start by verifying three cases.

Case 3: Suppose that $f(v,w) = \lambda \neq 0$, then the symplectic transvection $T_{v-w}(\lambda^{-1})$ is

$$\begin{aligned} T_{v-w}(\lambda^{-1}) : v &\mapsto v + \lambda^{-1} f(v, v-w)(v-w) \\ &= v + \frac{f(v, -w+v)}{f(v,w)}(v-w) \\ &= v + \frac{-f(v,w) + f(v,v)}{f(v,w)}(v-w) \\ &= v - (v-w) \\ &= w \end{aligned}$$

Thus $T_{v-w}(\lambda^{-1})$ maps v to w in V. If this is not the case, then we choose an x in V, such that $f(v,x)$ and $f(w,x)$ are not equal to zero. This is possible since f is a non-singular form on a symplectic basis V. That is, if $f(v,x) = 0 = f(w,x)$, then there exists y and z in V, such that $f(v,y)$ and $f(w,z)$ are not equal to zero, which implies the existence of a map $v \mapsto x$ and a map $x \mapsto w$. Thus S acts transitively non-zero vectors in V.

But we have not yet convinced ourselves that S acts transitively on order symplectic pairs in V. Fix u in V and suppose that $f(u,v) = f(u,w) = 1$ for v, w in V, such that $f(v,w) = \lambda$ for a non-zero λ in $\mathbb{F}_q$, otherwise $f(v,w) = 0$. So we need to show that there exists transvections that map $v \mapsto w$ and fixes u, we do this by considering the $f(v,w) \neq 0$ and $f(v,w) = 0$ separately.

Case 4: If $f(v,w) = \lambda \neq 0$, then the symplectic transvection

$$\begin{aligned} T_{v-w}(\lambda^{-1}) : v &\mapsto v + \lambda^{-1} f(v, v-w)(v-w) \\ &= v + \frac{f(v, -w+v)}{f(v,w)}(v-w) \\ &= v - (v-w) \\ &= w, \end{aligned}$$

thus $T_{v-w}(\lambda^{-1})$ maps v to w while u is fix.

For the case $f(v,w) = 0$ we consider a mortification of the argument in Case 3.

Case 5: Let $f(v,w)=0$, and $x=u+v$ in V, so that $f(u,x)=1$ and $f(v,x)=-1$ and $f(w,x)=-1$. Then the symplectic transvection

$$\begin{aligned} T_{v-x}(\lambda) : v &\mapsto v+\lambda f(v,v-x)(v-x) \\ &= v+\lambda f(v,\lambda x+v)(v-x) \\ &= v+\lambda(\lambda f(v,x)+f(v,v))(v-x) \\ &= v-(v-x) \\ &= x, \end{aligned}$$

which implies that $x \mapsto v$. Similarly the symplectic transvection

$$\begin{aligned} T_{x-w}(\lambda) : x &\mapsto x+\lambda f(x,x-w)(x-w) \\ &= x+\lambda f(x,\lambda w+x)(v-x) \\ &= x+\lambda(\lambda f(x,w)+f(x,x))(v-w) \\ &= x-(x-w) \\ &= w. \end{aligned}$$

Hence we have convinced ourselves that v maps to w via x whiles u is fix.

Therefor by induction the subgroup of symplectic transvections $S \leq Sp_{2m}(q)$ acts transitively on the ordered symplectic basis, and $S = Sp_{2m}(q)$. Observe that symplectic transvections have determinant one, Lemma[5.3.8], thus $Sp_{2m}(q)$ is contained in $SL_{2m}(q)$. □

We have no acquired the necessary definition and statements to prove that the symplectic group is perfect and primitive. This is done in the following two lemmas.

Lemma 5.3.8. *$Sp_{2m}(q)$ is perfect for $m=2$ and $q>3$, and $m>3$ $q>2$*

Proof. The following proof is based on [[3], Proposition 7.3]. We claim that $Sp_{2m}(q)$ is perfect, that is $Sp'_{2m}(q) = Sp_{2m}(q)$. Let V denoted be the symplectic basis $\mathbb{F}_q^{2m}$, and let $Sp'_{2m}(q)$ be the commutator subgroup in $Sp_{2m}(q)$. To verify this, we need to show that every symplectic transvection is in $Sp'_{2m}(q)$. Since $Sp_{2m}(q)$ is generated by symplectic transvections, Lemma[5.3.7], it suffices to show that given any v in V and λ in $\mathbb{F}_q$ the transvection $T_v(\lambda)$ is in $Sp'_{2m}(q)$. Suppose that λ is in $\mathbb{F}_q$, and that v is in V. Then λv is also in V. Since $Sp_{2m}(q)$ acts transitively on the symplectic basis, Lemma[5.3.7], we can find g in $Sp_{2m}(q)$ and v in V, so that $gv = \lambda v$ for any λ in $\mathbb{F}_q$. Thus for any λ in $\mathbb{F}_q$, the commutator $[g, T_v(\lambda)]$ is an element of $Sp'_{2m}(q)$. Observe that product of the commutator $[g, T_v(\lambda)]$ is equal to

$$\begin{aligned} [g, T_v(\lambda)] &= gT_v(\lambda)g^{-1}T_v(\lambda^{-1}) \\ &= T_{gv}(\lambda)T_{g^{-1}v}(-\lambda) \\ &= T_{\lambda v}(\lambda)T_{\lambda^{-1}v}(-\lambda) \\ &= T_v(\lambda^2)T_v(-1) \\ &= T_v(\lambda^2-1), \end{aligned}$$

and $T_v(\lambda^2-1)$ is just another symplectic transvection. If $q>3$ we can choose λ^2 not equal to 1, then $\lambda^2-1\neq 0$ is in $\mathbb{F}_q$, which implies that every transvection is contained in the commutator subgroup $Sp'_{2m}(q)$. Thus $Sp_{2m}(q)$ is equal to its commutator subgroup, for $q>3$. To complete the argument, we need for $Sp_{2m}(q)$ to be equal to $Sp'_{2m}(q)$. This part of the proof is based on [[1], Lemma 4.9]. Let $Sp'_{2m}(q)$ be the commutator subgroup of $Sp'_{2m}(q)$. Suppose that A is any invertible 3×3, and B any symmetric matrix 3×3, both with entries in $\mathbb{F}_q$. Since the symplectic group is generated by symplectic transvections, it suffices to show the an arbitrary commutator is equal to a symplectic matrix. We do this by considering the commutator of two two-block matrices

$$\left[\begin{pmatrix} A^{-1} & 0 \\ 0 & A^T \end{pmatrix},\begin{pmatrix} I & 0 \\ B & I \end{pmatrix}\right]$$
$$=\begin{pmatrix} A^{-1} & 0 \\ 0 & A^T \end{pmatrix}\begin{pmatrix} I & 0 \\ B & I \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & (A^T)^{-1} \end{pmatrix}\begin{pmatrix} I & 0 \\ -B & I \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ BA^{T+1}-B & 1 \end{pmatrix}$$

Thus by suitable choice of A,B, we get that $BA^{T+1}-B1$ has rank 1. So we can conclude that the commutator is equal to a symplectic matrix in $Sp_6(q)$. Hence our claim that $Sp_2m(q)$ is perfect, is justified. □

Before stating and proving the primitively for the symplectic group, we derive the order of the symplectic group.

Proposition 5.3.9. The order of $Sp_2m(q)$ is

$$|Sp_{2m}(q)|=q^{k^2}\prod_{k=1}^{l}(q^{2k}-1)$$

Proof. This proof is based on [[9], Section 3.5]. We want to deduce the order of $Sp_{2m}(q)$. That is want to compute the number of ways to choose an order symplectic basis. We start by selecting the first vector e_1 in V. This can be done in $q^{2m}-1$ ways. There are q^{2m-1} ways of selecting the perpendicular complete $e_1^{\perp}$ in V. We recall that, $u=e_m$ and $v=\lambda f_m$ and observe that for every pair $f(u,v)$. There are $q-1$ possible scalar multiples λ in $\mathbb{F}_q$. So the vector f_1 can be selected in $q^{2m}-q^{2m-1}/(q-1)$ ways. Therefore the first vector pair e_1,f_1 can be selected in $q^{m^2}(q^{2m}-1)$ possibilities. The order is derive the order by induction.

$$|Sp_{2m}(q)|=q^{k^2}\prod_{k=1}^{m}(q^{2k}-1)$$

□

Remark. All matrices in $M\in Sp_2m(q)$ have linearly independent vectors as it is a subgroup of $GL_2m(q)$. This allows us to reduce the problem to finding linearly independent vectors in a symplectic basis.

Lemma 5.3.10. The special symplectic group $Sp_m(q)$ acts primitively on the set of 1-dimensional subspace of $\mathbb{F}_q^{2m}$, denoted Ω.

Proof. The proof is based on [[9], Section 3.5.2]. We want to prove that $Sp_2m(q)$ acts primitively on Ω. We first recall that a primitive action has only two block-systems. That is, the block consisting of the partition of Ω into Ω, and the blocks of the partition of all of Ω into singletons. To verify the claim, we assume the converse. Suppose that the action $Sp_2m(q) \curvearrowright \Omega$ is imprimitive, then there exists some non-trivial block systems. We know that the action is transitive, Lemma[5.3.7]. So if p is a point in Ω. Then the stabilizer G_p acts transitively one the (q^{2m-1}) points not orthogonal to the fixed point. Recall that for any symplectic form $f(u,v) \neq 0$, there exists $q-1$ possible scalars, Proposition[5.3.9]. This means that the stabilizer of p also acts transitively on the $(q^{2m-1}-1)/(q-1)-1$ points that are orthogonal but not equal to p, this is simply a consequence of the fact that if given three vectors u,v,w in $\mathbb{F}_q^{2m}$, so that both the vectors v and w are orthogonal to u, there exist two possible values for the symmetric form of u,v, either $f(v,w) = \lambda \neq 0$ or $f(v,w) = 0$. If for v,w we have that $f(w,v) = \lambda \neq 0$, then there exists a transvection $T_{v-u}(\lambda^{-1}) : v \mapsto w$ while u gets fix, Lemma[5.3.7]. If $f(w,v) = 0$, then there exists a suitable vectors x for which $f(v,x)$ and $f(w,x)$ are non-zero, which implies that we can map v to w via x while u gets fix. Hence the only blocks systems are the partitions which has cardinality $1+q^{2m-1}$ and $1+(q^{2m-1}-1)/(q-1)$. But non of the possible blocks is divisible with $(q^{2m-1}-1)/(q-1)$, then the only block systems are the trivial one, this contradicting our assumption that $Sp_2m(q)$ is imprimitive. Therefore, the claim that the action $Sp_2m(q) \curvearrowright \Omega$ is primitive is justified. □

Definition 5.3.11. The **projective symplectic group** denoted $PSp_{2m}(q)$, is the group defined as the quotient of $Sp_{2m}(q)$ by the set of scalar matrices in $Sp_{2m}(q)$, denoted $PSp_{2m}(q)$.

Remark. Recall that for the definition of $PSL_n(q)$ in Section[5.2], we used the center of the special linear group, which consists of the scalar matrices in $SL_n(q)$. Observe that this is also what we did for $Sp_{2m}(q)$. But, since we are restricted to the symplectic form, any λ in $\mathbb{F}_q$ must satisfy $f(\lambda u, \lambda v) = \lambda^2 f(u,v)$, it follows that any the only possible scalars are $\lambda \pm 1$. This observation will be used when deriving the order of the projective symplectic group.

In the next theorem, we state and prove the simplicity projective symplectic group. This is done by simply verifying the hypothesis of Iwasawa's lemma.

Theorem 5.3.12. The group $PSp_{2m}(q)$ is simple for all $m > 2$, and $m = 2$ and $q > 2$.

Proof. The fallowing proof is based on [[9], Section 3.5.2]. We claim that the group $PSp_{2m}(q)$ is simple for $m > 2$, and for $m = 2, q > 2$. Let $Sp_{2m}(q)$ and $m \geq 2$ and when $m = 2$, take $q > 2$. Now suppose that $Sp_{2m}(q)$ acts on the set of one-dimensional subspace of $\mathbb{F}_q^{2m}$, denoted Ω. To prove the statement, we simply need to verify the hypothesis of Iwasawa's Lemma[5.1.12]. We first recall that $Sp_{2m}(q)$ is perfect, Lemma[5.3.8]. Furthermore the action $Sp_{2m}(q) \curvearrowright \Omega$ is primitive, Lemma[5.3.10], and the point stabilizer are maximal subgroups, Lemma[5.1.5]. Therefore, it suffices to show that any arbitrary point stabilizer have a normal abelian subgroup whose conjugates generate $Sp_{2m}(q)/Z(Sp_{2m}(q))$. To show this, we fix vector v in Ω, and consider the stabilizer $H = Sp_{2m}(q)_{\langle v \rangle}$. Since the stabilizer H fixes $\langle v \rangle$ and its perpendicular complement

$\langle v \rangle^{\perp}$, it follows that the transvections $T_v(\lambda)$ that fix $\langle v, v^{\perp} \rangle$ form a subset A of H, defined as

$$A = \left\{ \begin{pmatrix} 1 & 0 & \mathbf{0} \\ \lambda & 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I_{2m-1} \end{pmatrix} \mid \lambda \in \mathbb{F}_q \right\}.$$

Observe A satisfies the condition of a subgroup and any non-trivial element in A is an invertible lower triangular matrix, so any two elements in A commute. But $Sp_{2m}(q)$ is generated by symplectic transvections, Lemma[5.3.7], and every non-trivial element in A is an symplectic matrix and thus invariant under transpose conjugation, it follows that A is an abelain normal subgroup whose conjugates generate $PSp_{2m}(q)$. Hence the claim that the projective symplectic group $PSp_{2m}(q)$ is simple for $m > 2$ and $m = 2$,$q > 2$, is justified by Iwasawa's Lemma.

□

6 References

References

[1] Peter J Cameron. "Notes on classical groups". In: (2000).

[2] Allan Clark. *Elements of abstract algebra*. Courier Corporation, 1984.

[3] James Cruickshank and Fernando Szechtman. "Generators and relations for the unitary group of a skew hermitian form over a local ring". In: *Linear Algebra and its Applications* 552 (2018), pp. 1–28.

[4] Adrien Deloro. *A First Encounter with Classical groups*. 2014.

[5] David Steven Dummit and Richard M Foote. *Abstract algebra*. Vol. 3. Wiley Hoboken, 2004.

[6] I Martin Isaacs. *Finite group theory*. Vol. 92. American Mathematical Soc., 2008.

[7] Serge Lang. *Graduate Texts in Mathematics: Algebra*. Springer, 2002.

[8] Derek JS Robinson. *Abstract Algebra: An Introduction with Applications*. Walter de Gruyter GmbH & Co KG, 2015.

[9] Robert Wilson. *The finite simple groups*. Vol. 251. Springer Science & Business Media, 2009.