

SIMPLE FINITE GROUPS OF LIE TYPE

RAYHAAN PATEL

ABSTRACT. This paper discusses three of the simple finite groups of Lie type: the Projective Special Linear groups, the Projective Symplectic Groups and the Projective Special Unitary groups. We construct all of these, and prove the simplicity of the Projective Special Linear groups, and we discuss other related groups of Lie type, like the General Linear and Projective General Linear Groups.

1. INTRODUCTION

Definition 1.1. A group, $(G; *)$ is non-empty a set G with a binary operation, $*$: $G \times G \rightarrow G$ satisfying the following axioms:

- G0 *Closure*: For all $a, b \in G$, $a * b \in G$ (this is implied by $*$: $G \times G \rightarrow G$ but is included for clarity).
- G1 *Associativity*: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
- G2 *Identity*: There exists an element $e \in G$ such that for all $a \in G$, $a * e = e * a = a$ (sometimes we denote the identity with 1 or 0 instead of e .)
- G3 *Inverses*: For all $a \in G$, there exists some $a^{-1} \in G$ called the *inverse* of a such that $a * a^{-1} = a^{-1} * a = e$.

We often abbreviate $(G; *)$ as G , and write the group operation as multiplication, so $g * h$ where $g, h \in G$ becomes gh .

Some examples of groups include:

- (1) The integers, \mathbb{Z} under addition.
- (2) The rationals excluding 0, \mathbb{Q}^\times under multiplication.
- (3) The integers modulo some natural number n , $\mathbb{Z}/n\mathbb{Z}$ under addition.¹
- (4) The integers modulo some prime p and excluding 0, $\mathbb{Z}/p\mathbb{Z}^\times$, under multiplication.
- (5) The complex numbers with magnitude 1 under multiplication.
- (6) The symmetric groups, S_n , which contains all permutations of n elements, and the group operation is composition of those permutations.
- (7) The alternating groups, A_n , which consists of all even permutations of n elements, and the group operation is composition of those permutations.

Definition 1.2. We call a group, $(G; *)$ *abelian* if $*$ is commutative. That is for all $a, b \in G$, $a * b = b * a$.

A *finite group* is a group with a finite number of elements, and we call the number of elements in a finite group the *order* of a group denoted by $|G|$. Also, the subset $\mathbb{Q} \subset \mathbb{R}$ is still a group under the same operation as \mathbb{R} . Similarly, $A_n \subset S_n$ and is a group under the same operation as A_n . This motivates:

Date: June 2025.

¹Notice that this notation looks like we are dividing the set of integers by the integers times some number, n , keep this in mind when we deal with quotient groups; it has a meaningful interpretation.

Definition 1.3. Let $(G; *)$ be a group, and H a nonempty subset of G . Then H is a subgroup of G if and only if $(H; *)$ is also a group.

Definition 1.4. A subgroup, $H \leq G$ is a *normal* subgroup if for all $g \in G$ and $h \in H$, $ghg^{-1} \in H$.

When we have ghg^{-1} , we say that h is *conjugated* by g . If $gh_2g^{-1} = h_1$, we say h_1 and h_2 are *conjugate*. As an example, similar matrices, A and B are conjugate, since there exists some S such that $SAS^{-1} = B$. Any subgroup of an abelian group is normal, since $ghg^{-1} = gg^{-1}h = h \in H$. Normal subgroups can be thought of as a generalization of commutativity; instead of having $gh = hg$, we get $gh = h'g$, where $h' \in H$, and if we take gH to be the set $\{gh : h \in H\}$, and Hg to be $\{hg : h \in H\}$, then $gH = Hg$.

We can learn more about groups and their relations to each other by studying structure preserving maps between groups. For example, notice that the function $f : \mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$ such that $f(n) \mapsto n \pmod{3}$ seems to preserve some of the relations set by addition on \mathbb{Z} ; $f(a + b) = f(a) + f(b)$ for all $a, b \in \mathbb{Z}$. In number theory, we regularly use functions like this, taking the integers modulo some integer to study properties of the integers.

We call a function like this a *homomorphism*, or more formally:

Definition 1.5. A *homomorphism* is a function $f : G \rightarrow H$ where G and H are groups, such that for all $a, b \in G$, $f(ab) = f(a)f(b)$.

Definition 1.6. Similarly, an *isomorphism* is a bijective homomorphism.

If there exists an isomorphism between two groups, G and H , then we say $G \cong H$, or G is isomorphic to H . An isomorphism from a group to itself is called an *automorphism*. For example, $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $\phi(n) = -n$ is an automorphism.

Given a subset S of a group G , we call the smallest subgroup H containing S the subgroup *generated* by S . We say that S generates H or H is generated by S , or write this as $H = \langle S \rangle$. This smallest subgroup must contain all elements of G that are a product of elements of S and their inverses by closure, and no others in order to stay the smallest. We say that S generates H or H is generated by S , or write this as $H = \langle S \rangle$. Knowing generators for a group makes working with the group easier, since we can write all the elements of the group in terms of the generators.

Example. The symmetric groups are generated by transpositions, and the alternating groups are generated by 3-cycles.

Definition 1.7. We call a group *cyclic* if it can be generated by one element.

Both \mathbb{Z} and $\mathbb{Z}/n\mathbb{Z}$ are generated by 1, and therefore cyclic.

We can combine two groups to get a new one by taking the direct product of the groups.

Definition 1.8. The *direct product* of two groups, $(G; *)$ and $(H; +)$ is a group, where the underlying set is $G \times H$ with and the binary operation is defined component wise:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 + h_2).$$

A group is *simple* if it does not contain any proper normal subgroups (we exclude the group itself and the subgroup consisting of the identity).

In the context of finite group theory, simple groups behave somewhat like prime numbers, in the sense that a simple group G cannot be “factored” into a normal subgroup N and the

quotient group (covered in the next section) G/N . Because of this, we can classify all finite groups, by classifying all simple finite groups, then finding all possible ways of combining them to form the finite groups. One such way of combining simple groups is through the direct product, however, it is far from the only way and does not allow us to produce all finite groups from the simple groups. These two problems form the *Hölder Program*, and are central problems in finite group theory.

The classification of simple finite groups, sometimes called the Enormous Theorem, was finished in 1983 ² by over 100 mathematicians across around 10,000 pages across dozens of papers. However, the second part, called the Extension Problem, remains open. The classification of simple finite groups is as follows:

Theorem 1.9 (The Enormous Theorem). *Every simple finite group G is isomorphic to either*

- (1) *A cyclic group of prime order ($G \cong \mathbb{Z}_p$ for prime p).*
- (2) *An alternating group ($G \cong A_n$ for $n \geq 5$).*
- (3) *A group of Lie type.*
- (4) *One of 26 Sporadic groups.*

There is one edge case, called the Tits group that is almost, but not strictly a group of Lie type, so some consider it to be the 27th sporadic group.

Theorem 1.10. *All simple finite groups are generated by 2 of their elements.*

This result follows from the classification theorem, as it was proven case wise on each family of simple finite group. The proof is too technical for this paper, so see [DMT91], which discusses this in-depth.

2. QUOTIENT GROUPS

Quotient groups are a way to decompose a group into smaller groups, that share some properties with the original. We can decompose groups into their simple factors by taking successive quotients of groups, and they are an important tool in constructing the simple finite groups of Lie type. The prototypical example of quotient groups is $\mathbb{Z}/n\mathbb{Z}$; in taking the integers modulo n , we “divide out” by $n\mathbb{Z}$, setting any element of $n\mathbb{Z}$ to the identity, and partition the other elements of \mathbb{Z} into translates of $n\mathbb{Z}$ by adding some constant to $n\mathbb{Z}$. First, we cover some information about homomorphisms that we then use to define quotient groups.

Let $\phi : G \rightarrow H$ be a homomorphism of groups.

Definition 2.1. The *kernel* of a homomorphism, ϕ is defined to be

$$\ker \phi = \{g \in G : \phi(g) = e_H\}$$

Proposition 2.2. *The kernel of ϕ is a normal subgroup of G .*

Proof. First, we show that $\ker \phi$ is a subgroup of G .

Closure: For all $k_1, k_2 \in \ker \phi$, $\phi(k_1 k_2) = \phi(k_1)\phi(k_2) = e_H$.

Inverses: For all $k \in \ker \phi$, $\phi(k) = \phi(k^{-1})$

Identity: For all $g \in G$, $\phi(g)\phi(e_G)\phi(ge_G) = \phi(g)$, so $\phi(e_G) \in \ker \phi$.

²There were some minor gaps in the proof that were filled in by Ashbacher and Smith in 2004, and Harada and Solomon in 2008.

Thus $\ker \phi$ is a subgroup of G . Now, we show that $\ker \phi$ is a normal subgroup. For all $k \in \ker \phi$, we need to show that $gkg^{-1} \in \ker \phi$ for all $g \in G$. We have that

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = e_H,$$

so $gkg^{-1} \in \ker \phi$ as desired. 

Definition 2.3. The *image* of a homomorphism, ϕ is defined to be

$$\text{Im}(\phi) = \{\phi(g) : g \in G\}$$

Proposition 2.4. *The image of a homomorphism is a subgroup of H .*

Proof.

Closure: For all $g_1, g_2 \in G$, $f(g_1)f(g_2) = f(g_1g_2) = f(g_3)$ where $g_3 \in G$, so $f(g_3) \in H$.

Inverses: For all $g \in G$, $f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$ (the same applies to $f(g^{-1})f(g)$).

Identity: $f(e_G) = e_H$. 

Definition 2.5. A *fiber* of ϕ over some $h \in H$ is defined to be the set

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

The kernel of ϕ is the fiber over e_H . We can multiply any elements in the image of ϕ using the group operation on H , which gives us a natural way to multiply fibers above points in the image of H . Suppose X_a is the fiber of a , and X_b is the fiber above b , then $X_aX_b = X_{ab}$. This multiplication is the same as the multiplication in $\text{Im}\phi$.

Definition 2.6. Let $\phi : G \rightarrow H$ be a homomorphism with kernel K . The quotient group G/K or G modulo K , is the group containing the fibers of ϕ and has the operation as described above.

From this definition, $G/K \cong \text{Im}\phi$. Note that the kernel K is a single element, the identity in G/K . We can think of G/K as taking elements of the group modulo K , analogous to how $\mathbb{Z}/n\mathbb{Z}$ is defined, as it is a quotient group. Our definition of G/K requires the map ϕ , however, we can instead define multiplication of fibers by using *representatives* of the fibers, similarly to how $a \in \mathbb{Z}/n\mathbb{Z}$ represents all integers of the form $a + 3n$.


Proposition 2.7. *Given a homomorphism $\phi : G \rightarrow H$ with kernel K , let X be the fiber above a , then we can choose any $x \in X$ and we have $X = \{xk | k \in \ker \phi\}$ and $X = \{kx | k \in \ker \phi\}$.*

Proof. Let $x \in X$, so $\phi(x) = a$, and let $xK = \{xk | k \in K\}$. We will prove that $xK \subseteq X$, then $X \subseteq xk$. First, for all $k \in K$,

$$\phi(xk) = \phi(x)\phi(k) = \phi(x) = a,$$

so $xk \in X$, meaning $xK \subseteq X$. Now, suppose $g \in X$ and we let $k = x^{-1}g$, so

$$\phi(k) = \phi(x^{-1})\phi(g) = \phi(x)^{-1}\phi(g) = aa^{-1} = e_H$$

The proof for $X = \{kx | k \in \ker \phi\}$ is nearly identical. 

Now we can describe a quotient group without having an explicit homomorphism; we can set a normal subgroup, K of G to be the kernel and construct the *cosets* of K ; sets of the form xK as we have seen before. We then define the group operation on G/K by $xK \cdot yK = (xy)K$.

This proof has an interesting consequence:

Corollary 2.8. $|G/K| = \frac{|G|}{|K|}$.

Proof. From the group axioms, the function $A : G \rightarrow G$ defined by $A(g) = ag$ must be a bijection since it has an inverse $A^{-1} : G \rightarrow G$ defined by $A^{-1}(g) = a^{-1}g$, therefore $|xK| = |K|$ since multiplication by x is bijective. Since $|xK| = |K|$ and $X = xK$, we have $|X| = |K|$ for all fibers X ! We have $|G/K||K| = |G|$ since we subdivide G into $|G/K|$ fibers with $|K|$ elements each, giving us $|G/K| = \frac{|G|}{|K|}$ as desired. 🐼

3. VECTOR SPACES

The groups of Lie type we will be exploring involve linear algebra, so we will cover the basics here.

Definition 3.1. A *field* is a set \mathbb{F} with *two* binary operations, addition and multiplication, that satisfies the following axioms:

Addition Axioms:

- A0 *Closure:* For all $a, b \in \mathbb{F}$, $a + b \in \mathbb{F}$.
- A1 *Associativity:* $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{F}$.
- A2 *Commutativity:* For all $a, b \in \mathbb{F}$, $a + b = b + a$
- A3 *Identity:* There exists an element $0 \in \mathbb{F}$ such that for all $a \in \mathbb{F}$, $a + 0 = 0 + a = a$.
- A4 *Inverses:* For all $a \in \mathbb{F}$ there exists some $-a$ called the *additive inverse* of a such that $a + -a = -a + a = 0$

Multiplication Axioms:

- M0 *Closure:* For all $a, b \in \mathbb{F}$, $ab \in \mathbb{F}$.
- M1 *Associativity:* $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{F}$.
- M2 *Commutativity:* For all $a, b \in \mathbb{F}$, $ab = ba$
- M3 *Identity:* There exists an element $1 \in \mathbb{F}$ such that for all $a \in \mathbb{F}$, $a1 = 1a = a$.
- M4 *Inverses:* For all $a \in \mathbb{F}$ there exists some a^{-1} called the *multiplicative inverse* of a such that $aa^{-1} = a^{-1}a = 1$.

Distributivity:

- D1 *Distributivity:* For all $a, b, c \in \mathbb{F}$, $a(b + c) = ab + ac$.

A finite field is a field with a finite number of elements. We write \mathbb{F}^\times when we refer to just the multiplicative group of \mathbb{F} (which does not contain 0).

Definition 3.2. The smallest natural number n such that n times the multiplicative identity is 0 is called the *characteristic* of a finite field. For an infinite field, like \mathbb{Q} , there may be no such n , in which case we say it has characteristic 0.

Example. In $\mathbb{Z}/p\mathbb{Z}$, the characteristic is p ; $1p = 0$, while \mathbb{Q}, \mathbb{R} and \mathbb{C} are all characteristic 0.

Definition 3.3. A *vector space* is an abelian group $(V; +)$ under *vector addition*. Elements of the vector space are called *vectors*. Vector spaces are also paired with a field \mathbb{F} and have a

binary operation from $\cdot : \mathbb{F} \times V \rightarrow V$ called scalar multiplication. We say that V is a vector space *over* \mathbb{F} when it is paired with \mathbb{F} . These satisfy the following axioms:

- (1) $1 \cdot v = v$ for all $v \in V$.
- (2) For all $a, b \in \mathbb{F}$, $a \cdot (b \cdot v) = (ab) \cdot v$.
- (3) For all $a \in \mathbb{F}$, $a \cdot (u + v) = a \cdot u + a \cdot v$.
- (4) For all $a, b \in \mathbb{F}$, $(a + b) \cdot v = a \cdot v + b \cdot v$.

Definition 3.4. A *subspace* is a subset of a vector space that is also a vector space under the same vector addition and scalar multiplication.

Definition 3.5. A *linear combination* of vectors in a subset W of a vector space V is an expression written in the form

$$\sum \lambda w$$

for scalars λ and $w \in W$.

Definition 3.6. The *span* of a subset W of V is the subspace of all vectors that can be written as a linear combination of elements of W . If the span of W is V , we say W spans V . If a vector v is in the span of W , then v is spanned by W .

Definition 3.7. A set of vectors, $W = \{v_1, \dots, v_n\}$ in V is *linearly independent* if each v_i is not spanned by $W \setminus v_i$.

This also means $a_1v_1 + \dots + a_nv_n = 0$ if and only if all $a_i = 0$, where v_1, \dots, v_n is linearly independent. Otherwise, suppose $a_1v_1 + \dots + a_nv_n = 0$ and there are nonzero a_i , then $\frac{a_1}{a_n}v_1 + \dots + \frac{a_{n-1}}{a_n}v_{n-1} = -v_n$. Also, if v_1, \dots, v_n are not linearly independent, which means there exists a_i such that $a_1v_1 + \dots + a_{n-1}v_{n-1} = v_n$, then $a_1v_1 + \dots + a_{n-1}v_{n-1} - v_n = 0$.

Definition 3.8. We call a subset $W \subseteq V$ a *basis* if it spans V and is linearly independent.

A basis gives us a sort of coordinate system of the vector space in terms of its elements, and since all bases of a vector space have the same number of elements as shown in [DF04, Chapter 11] we have:

Definition 3.9. The unique number of elements of a basis in a vector space V is called the *dimension* of V , also written as $\dim(V)$ or $\dim V$.

Definition 3.10. A *linear transformation* is a function $T : V \rightarrow W$ where V and W are vector spaces over the same field \mathbb{F} that satisfies the following properties:

- (1) *Additivity*: For all $u, v \in V$, $T(u + v) = T(u) + T(v)$.
- (2) *Homogeneity*: For all $\lambda \in \mathbb{F}$ and $v \in V$, $T(\lambda v) = \lambda T(v)$.


Linear transformations are the analogue of a homomorphism for groups; they are group homomorphisms that also satisfy homogeneity.

Proposition 3.11. Let $T : V \rightarrow W$ be a linear transformation, and let B be a basis of V . Then $T(B)$ spans $T(V)$ and if T is injective, then $T(B)$ is a basis of $T(V)$.

Proof. We assume T does not map everything to 0, as this becomes trivial otherwise. Let $w \in L(V)$ where $w \neq 0$, then there exists some $v \in V$ such that $L(v) = w$. We now write v as $a_1v_1 + \dots + a_nv_n$ where v_1, \dots, v_n is a basis of V and $a_1, \dots, a_n \in \mathbb{F}$. This gives us

$w = a_1T(v_1) + \cdots + a_nT(v_n)$, which means $T(v_1), \dots, T(v_n)$ spans $T(V)$ as desired. If T is injective, $\ker T = \{0\}$, so

$$a_1T(v_1) + \cdots + a_nT(v_n) = T(a_1v_1 + \cdots + a_nv_n) = 0$$

implies that $a_1v_1 + \cdots + a_nv_n = 0$, which means each $a_i = 0$ since v_i form a basis. This implies that $T(v_i)$ forms a basis as well. 

Because of this, once we specify the image of a basis of V , we define the entire linear transformation.

Definition 3.12. Let V and W be vector spaces of dimensions m and n respectively, and let T be a linear transformation $T : V \rightarrow W$. Let v_1, \dots, v_n and w_1, \dots, w_m be bases of V and W respectively. the *matrix corresponding to T* is an $n \times m$ array, where we write a_{ij} for the entry in the i^{th} row and j^{th} column, defined by: $T(v_j) = a_{1j}w_1 + \cdots + a_{nj}w_n$.

Definition 3.13. Let V be an n -dimensional vector space, and consider the identity map, $1 : V \rightarrow V$ defined by $1v = v$ for all $v \in V$. The matrix corresponding to this transformation, I_n , is called the $n \times n$ identity matrix, which is a matrix of the form:

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

We will only work with linear transformations from a vector space to itself. Given two matrices, A and B , their product, AB is the matrix corresponding to the composition of their corresponding linear transformations.

4. LINEAR GROUPS

4.1. Lie Groups. The groups of Lie type were originally constructed from Lie groups and their closely related Lie algebras, so we will give a brief intuition for what a Lie group and Lie algebra is. A more detailed discussion can be found in [Kir17] Lie theory was initially developed by Sophus Lie in an attempt to use group theory to solve differential equations by studying groups on continuous surfaces after he saw Galois' success with proving the unsolvability of the quintic. This did not work out, though it still produced a valuable theory. Informally, manifolds are like curves or surfaces, though they can be of higher dimension. An n -dimensional manifold locally resembles n -dimensional real space. As an example, 1-dimensional manifolds are curves and lines, like the real line, a circle or a helix. Two-dimensional manifolds are surfaces, like a sphere (mathematicians consider spheres to be spherical *surfaces* rather than a solid ball or a torus. The formal definition of a manifold is too technical to include here, though interested readers can refer to [Lee11].

Definition 4.1. A *Lie group* is a manifold where the points on the manifold also form a group, and applying the group operation and taking inverses are smooth maps of the manifold.

As an example, consider the complex unit circle, \mathbb{T} . It is a 1-dimensional manifold The group operation is complex multiplication, and for all $z, x \in \mathbb{T}$, the maps from $\mathbb{T} \rightarrow \mathbb{T}$, $\phi : x \mapsto zx$ and $\psi : x \mapsto x^{-1}$, which correspond to multiplication by z and taking inverses respectively, are smooth maps.

Complex Lie groups have corresponding Lie algebras over \mathbb{C} , and if the Lie group is simple, then so is the Lie algebra. Simple Lie algebras were classified about 100 years ago, and in 1955 Chevalley constructed analogues of the simple Lie algebras over \mathbb{C} for all finite fields and then constructed simple finite groups from them. These are called the Chevalley groups and account for 9 of the 18 infinite families. Unfortunately this construction is too involved to include here, though [Gec24] covers the construction and the prerequisite Lie theory.

Definition 4.2. The *General Linear Group*, denoted $GL_n(\mathbb{F})$ is the group of $n \times n$ matrices of nonzero determinant over the field \mathbb{F} .

For $\mathbb{F} = \mathbb{R}$, this forms a Lie group that is a submanifold of \mathbb{R}^{n^2} , since we can interpret each matrix as a strange way to write the coordinates for a point in \mathbb{R}^{n^2} space. To get a very rough idea of why matrix multiplication and inversion results in smooth maps, the transformations of two nearby matrices on the manifold would be very similar (here, very similar means “they would look about the same”), so their inversions or result when multiplied by another matrix would again be very similar and therefore nearby. When \mathbb{F} is a finite field, we write $GL_n(q)$ where $q = |\mathbb{F}|$.

Definition 4.3. The *center* of a group G is the subgroup such that for all z in the center, $gz = zg$ for all $g \in G$. The center of a group is a normal subgroup, since $gzg^{-1} = gg^{-1}z = z$.

Let the center of $GL_n(q)$ be Z , which consists of all scalar matrices, which are of the form λI_n where $\lambda \in \mathbb{F}_q^\times$ and I_n is the $n \times n$ identity matrix.


Proposition 4.4. *Given that Z consists of scalar matrices, Z is a cyclic group of order $q - 1$.*

Proof. Consider the isomorphism $\phi : Z \rightarrow \mathbb{F}_q^\times$ defined by $\lambda I_n \mapsto \lambda$. It has inverse $\phi^{-1} : \mathbb{F}_q^\times \rightarrow Z$ defined by $\lambda \mapsto \lambda I_n$, so it is a bijection. Given any $\lambda_1, \lambda_2 \in \mathbb{F}_q^\times$, we have that

$$\phi(\lambda_1 I_n \lambda_2 I_n) = \phi(\lambda_1 \lambda_2 I_n) = \lambda_1 \lambda_2.$$

We also have

$$\phi(\lambda_1 I_n \lambda_2 I_n) = \phi(\lambda_1 I_n) \phi(\lambda_2 I_n) = \lambda_1 \lambda_2.$$

Thus ϕ is an isomorphism. Since \mathbb{F}_q^\times is cyclic and of order $q - 1$, so is Z . 

If we take the quotient $GL_n(q)/Z$, we get the Projective General Linear group, $PGL_n(q)$. We can get another important group by constructing a homomorphism $\phi : GL_n(q) \rightarrow \mathbb{F}_q^\times$ by $\phi(A) \mapsto \det(A)$, since $\det(AB) = \det(A) \det(B)$.

Definition 4.5. The kernel of ϕ as described above, which consists of matrices with determinant 1, is called the *Special Linear Group* $SL_n(q)$.

The center of $SL_n(q)$, which we will call SZ^3 , also consists of scalar matrices. However, $\lambda^n = 1$ so that $\det(\lambda I_n) = 1$.


Definition 4.6. Similar to $GL_n(q)$, we take the quotient $SL_n(q)/SZ$ to get the Projective Special Linear group, $PSL_n(q)$. As we will prove later, $PSL_n(q)$ is simple and is one of the 16 infinite families of simple finite groups of Lie Type.

³This notation is often used for the Suzuki groups rather than the center of $SL_n(q)$.


4.2. Orders of the Linear Groups. Knowing the orders of groups is important for understanding their structure; Lagrange's theorem and the Sylow theorems provide us information about subgroups of a group based on just the factorization of a group's order. In the case of the linear groups we discussed above, we can write the orders with nice formulas with combinatorial proofs.

Theorem 4.7. *The order of $GL_n(q)$ is as follows:*

$$|GL_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Proof. Since the matrix is invertible, its columns must be linearly independent (which requires all columns to have at least 1 nonzero entry). We have n entries in the first column, so there are q^n total possibilities, but we must subtract 1 to avoid the case where all entries are 0. The second column cannot be one of the q multiples of the first, so there are $q^n - q$ possibilities. In general, the first i (linearly independent) columns form the basis of an i -dimensional subspace, which contains q^i elements, so we must subtract these from our q^n possibility for the $i + 1^{\text{th}}$ column, resulting in the above formula. 

Corollary 4.8. *The order of $PGL_n(q)$ follows easily as $|PGL_n(q)| = \frac{1}{q-1}|GL_n(q)|$.*

Proof. Since $PGL_n(q) = GL_n(q)/Z$, we have $|PGL_n(q)| = \frac{1}{|Z|}|GL_n(q)|$ by Corollary 2.8, which is equal to $|\frac{1}{q-1}|GL_n(q)|$, as desired. 

Theorem 4.9. *The order of $SL_n(q)$ is as follows:*

$$|SL_n(q)| = \frac{1}{q}|GL_n(q)|.$$

Proof. To show this, we show that each set

$$G_m = \{A \in GL_n(q) : \det(A) = m\}$$

has the same order for all $m \in \mathbb{F}_q^\times$. Note that $G_1 = SL_n(q)$. We create a bijection

$$\phi_m : SL_n(q) \rightarrow G_m$$

where $\phi_m(A)$ multiplies the first column of A by m , so that $\phi_m(A)$ has determinant m . We have

$$\phi_m^{-1} : G_m \rightarrow SL_n(q)$$

where $\phi_m^{-1}(A)$ multiplies the first column of A by m^{-1} so ϕ is invertible and therefore a bijection. We simultaneously bijected $SL_n(q) = G_1$ to all $q - 1$ sets G_m , which partition $GL_n(q)$. Thus,

$$|SL_n(q)| = \frac{1}{q}|GL_n(q)|.$$



We can also define analogues of the linear groups that contain linear transformations as elements rather than matrices.

Definition 4.10. Given a vector space V , we define:

- (1) $GL(V)$ is the group of all linear transformations of V with nonzero determinant.
- (2) $PGL(V)$ is $GL(V)/Z(GL(V))$.

- (3) $SL(V)$ is the group of all linear transformations with determinant 1, and can also be defined as the kernel of the linear functional $\det : GL(V) \rightarrow \mathbb{F}^\times$, where \mathbb{F} is the base field of V .
- (4) $PSL(V)$ is $SL(V)/SZ(V)$, where $SZ(V)$ is the center of $SL(V)$.

All of these are isomorphic to their matrix analogues; we can define the isomorphism by choosing a basis of V and writing each linear transformation as a matrix relative to this basis. This allows us to work directly with linear transformations to prove properties about the linear groups; we can (and we will) prove that $PSL(V)$ is simple, and since $PSL_n(q) \cong PSL(V)$, $PSL_n(q)$ is simple.

4.3. Simplicity of $PSL_n(q)$.

Definition 4.11. A *hyperplane* H of an n -dimensional vector space is an $n - 1$ dimensional subspace.

Definition 4.12. Given two subspaces G, H of a vector space V , $H + G$ is the span of $G \cup H$.

Lemma 4.13. Given two hyperplanes, H_1, H_2 of a vector space V of dimension n where $n \geq 3$, $H_1 \cap H_2 \neq \{0\}$.

Proof. We prove this by showing that $\dim(H_1 \cap H_2) = n - 2$, which is not $\{0\}$ as long as $n \geq 3$. First, let $K = \{h_1, \dots, h_k\}$ be a basis of $H_1 \cap H_2$ (we leave this basis empty if $H \cap G = \{0\}$). We can extend this basis to bases of H_1 and H_2 , respectively by adjoining $n - 1 - \dim(H_1 \cap H_2)$ (non-arbitrary) vectors to K . Call these bases K_1 and K_2 , where K_i is a basis of H_i . If we take $\{v \in K_1 : v \notin K\} \cup \{v \in K_2 : v \notin K\} \cup K$, we get a basis of $H_1 + H_2 = V$, which must have n elements. This gives us

$$\begin{aligned} n &= 2(n - 1 - \dim(H_1 \cap H_2)) + \dim(H_1 \cap H_2) \\ n &= 2n - 2 - \dim(H_1 \cap H_2) \\ \dim(H_1 \cap H_2) &= n - 2, \end{aligned}$$

as desired. 

Definition 4.14. A *transvection* T is a linear transformation of a vector space V that fixes a hyperplane H of V , has determinant 1 and is not the identity. A *transvection matrix* is a matrix that corresponds to some transvection.

Lemma 4.15. Any transvection T of an $n \geq 2$ -dimensional vector space V can be written as a matrix of the following form:

$$J_n = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots & 0 \\ \vdots & \vdots & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Proof. Since T is a transvection, some hyperplane, H must be fixed. For any $w \notin H$, we can write Tw as $\mu w + h$, where $h \in H$ and $\mu \in \mathbb{F}_q^\times$, since we can create a basis of V by adding w to a basis of H . We then write Tw as a linear combination of this basis, which gives us μw plus some linear combination of a basis of H , which must be an element of H . Now, consider the matrix of T over the ordered basis $(w, h, h_3, h_4, \dots, h_n)$ where $h = Tw - \mu w$. Only the

first column would differ from the identity matrix, since w is the only basis element that is not preserved by T , and since $Tw = \mu w + h$, the first row would contain μ and the second row would contain 1. We know that T has determinant 1, so μ must be 1.



Since our proof used arbitrary $w \notin H$, we have that for all $w \notin H$, $Tw = w + h$ for some $h \in H$, since $\mu = \det(T) = 1$.

Let T be a transvection that fixes the hyperplane H in the vector space V , then for all $w \notin H$, $T(w) = w + h$ for some $h \in H$. For all $v \in V$, then $v = \lambda w + h'$ for some $\lambda \in \mathbb{F}_q$ and $h' \in H$, since $H \cup \{w\}$ spans V . Since T fixes H

$$T(v) = \lambda T(w) + T(h') = \lambda(w + h) + h' = \lambda w + h' + \lambda h = v + \lambda h.$$

The function $\phi : V \rightarrow \mathbb{F}_q$ defined by $\phi(v) = \phi(\lambda w + h) = \lambda$ is a linear functional.

Definition 4.16. A linear functional is a function $f : V \rightarrow \mathbb{F}$ that satisfies the following properties:

- (1) $f(v + w) = f(v) + f(w)$ for all $v, w \in V$, and
- (2) $f(\alpha v) = \alpha f(v)$ for all $v \in V$ and all $\alpha \in \mathbb{F}$

The function ϕ is a linear functional since

$$\phi(\mu(\lambda w + h)) = \phi(\mu\lambda w + \mu h) = \mu\lambda$$

since $\mu h \in H$, and

$$\phi(\lambda w + h + \mu w + h') = \phi((\mu + \lambda)w + h'') = \mu + \lambda.$$

We can construct such a linear functional ϕ and find a vector $h \in \ker \phi = H$ for all transvections T , allowing us to write $T(v) = v + \phi(v)h$ for all $v \in V$.

This gives us an alternate way to write transvections; we can write them as $\{\phi, h\} : V \rightarrow V$ defined by

$$\{\phi, h\} : v \mapsto v + \phi(v)h.$$

Corollary 4.17. All transvection matrices in $GL_n(q)$ are conjugate, or equivalently, all transvection matrices are similar.

Proof. Since all transvections can be written as some J_n , all transvection matrices must be similar to some J_n , and therefore all transvection matrices are conjugate in $GL_n(q)$.



Lemma 4.18. All transvections in $SL(V)$ are conjugate if the $n \geq 3$.

Proof. We start by proving the equivalent statement for linear transformations rather than matrices, then choosing a basis of V to convert back to matrices. Let $T_H = \{\phi, h\}$ and $T_L = \{\psi, l\}$ be transvections that fix the hyperplanes $H = \ker \phi$ and $L = \ker \psi$, respectively. Now, we can choose vectors $v, u \in V$ where $\phi(v) = 1$ and $\psi(u) = 1$ (so $v \notin H$ and $u \notin L$). We can create the bases

$$\{h, h_2, \dots, h_{n-1}\}$$

of H , and

$$\{l, l_2, \dots, l_{n-1}\}$$

for L , then adjoin v and u to create the bases of V :

$$\{v, h, h_2, \dots, h_{n-1}\}$$

and

$$\{u, l, l_2, \dots, l_{n-1}\}$$

We define S to be a linear transformation that maps the first of these ordered bases of V to the second, which means $S(v) = u$, $S(H) = L$ and $S(h) = l$.

We call the determinate of S d , and we now will create a new matrix S_1 that has determinant 1 and shares other properties with S . Our first basis of V has some vector, say h_{n-1} , that is not v or h , since $n \geq 3$. We construct S_1 the same we we construct S , except we have $S_1(h_{n-1}) = d^{-1}l_{n-1}$. If we consider the matrices of S_1 and S relative to $\{v, h, h_2, \dots, h_{n-1}\}$, we obtain S_1 by multiplying the last column of S by d^{-1} , which means $\det(S_1) = 1$.


Now, consider the linear transformation $S_1 T_H S_1^{-1}$ on the basis $\{u, l, l_2, \dots, l_{n-1}\}$. First applying S_1^{-1} , we get the basis $\{v, h, h_2, \dots, dh_{n-1}\}$. Applying T_H to this result preserves all elements of the basis except for v , and we know

$$T_H(v) = v + \phi(v)h = v + h,$$


so

$$S(T_H(v)) = S_1(v) + \phi(v)S_1(h) = S_1(v) + S_1(h) = u + l.$$

Taking S_1 of $\{h, h_2, \dots, dh_{n-1}\}$ results in $\{l, l_2, \dots, l_{n-1}\}$, so $S_1 T_H S_1^{-1}$ preserves L and maps u to $u + l$. Now, we apply T_L to the basis $\{u, l, l_2, \dots, l_{n-1}\}$, which also preserves L , and we know $\psi(u) = 1$ so $T_L(u) = u + \psi(u)l = u + l$. The result of applying $S_1 T_H S_1^{-1}$ is identical to T_2 on the basis $\{u, l, l_2, \dots, l_{n-1}\}$, so, they must be equal.

Now, we consider these transformations as matrices relative to an arbitrary basis of V ; since S_1 as a transformation has determinant 1, the matrix corresponding to S_1 is in $SL_n(q)$ (the same is true for S_1^{-1}). Thus, the transvection matrices corresponding to T_1 and T_2 relative to a (fixed) arbitrary basis are conjugate in $SL_n(q)$, so all transvection matrices are conjugate in $SL_n(q)$. 

Lemma 4.19. *The group $SL_n(q)$ is generated by transvection matrices.*

Proof. We show that all matrices generated by taking the identity matrix, and replacing one of the zero entries with some non-zero entry $\lambda \in \mathbb{F}_q^\times$ are transvection matrices, then show that these generate $SL_n(q)$. Suppose λ is in row r , column c of the matrix. Then, we can modify the construction in the proof of lemma 4.15. Take the basis we constructed, $(w, h, h_3, h_4, \dots, h_n)$, and replace h with $h' = h/\lambda$. We get $Tw = w + h = w + \lambda h'$, so instead of a 1 in the second row of the first column, we have a λ . Now, we reorder this basis so that w is in the c^{th} position and h' is in the r^{th} position, which moves λ to column c , row r , as desired. We call a matrix of this form an *elementary* transvection matrix. Multiplying some $A \in GL_n(q)$ by an elementary transvection matrix with λ in column c and row r Multiplication by each elementary transvection matrix corresponds to taking some row r_i and adding λr_j to it, where r_j is another row. This means we can decompose a matrix $A \in SL_n(q)$ into elementary transvections by reducing it to the identity and using the row operations needed to do so to construct a product of transvections. *Gauss - Jordan Elimination* states that all invertible matrices of determinant 1 can be reduced only using these operations, and invertible matrices of determinant $\neq 1$ require a row scaling operation as well. For the proof of Gauss-Jordan Elimination, see [Rot95, Lemmas 8.7 and 8.8]. Since all $A \in SL_n(q)$ can be reduced, we can write each A as a product of elementary transvection matrices, as desired. 

Definition 4.20. Let H be a hyperplane of the vector space V , then

$$\mathcal{T}(H) = \{\text{all transvections fixing } H\} \cup \{I_V\}.$$

Lemma 4.21. *The set of transformations in $SL(V)$ that commute with all elements of $\mathcal{T}(H)$ is $\{sT : s \in SZ(V), T \in \mathcal{T}(H)\}$.*

The proof of this can be found in [Rot95, Lemma 8.22]

Theorem 4.22 (Jordan-Dickson). *If V is vector space of dimension $n \geq 3$ over a field \mathbb{F} , then $PSL(V)$ is simple.*

Proof. Suppose N is a normal subgroup of $SL(V)$ that contains a transformation $A \notin SZ(V)$, then we will show that $N = SL(V)$. This implies that there are no normal subgroups of $SL(V)$ that are not contained in $SZ(V)$, or is $SL(V)$ itself, which by the fourth isomorphism theorem implies that $PSL(V)$ is simple. A proof of the fourth isomorphism theorem can be found in [DF04].

Since all transvections are conjugate in $SL(V)$, any normal subgroup of $SL(V)$ containing a transvection must contain all transvections. Transvections generate $SL(V)$, so the only normal subgroup of $SL(V)$ that contains a transvection is $SL(V)$. This means we only need to show that N containing $A \notin SZ(V)$ implies N contains a transvection.

We claim there must be a transvection T that does not commute with A . Suppose all transvections commuted with A , then given any $g \in SL(V)$, we can decompose g into a product of transvections $t_1 t_2 \dots t_x$ and get that $t_1 t_2 \dots t_x A = t_1 t_2 \dots t_{x-1} A t_1$. We can continue this process to commute each t_i getting that $t_1 t_2 \dots t_x A = A t_1 t_2 \dots t_x$. This implies $A \in SZ(V)$, which is a contradiction.

Therefore, we have that

$$B = T^{-1} A^{-1} T A \neq 1,$$

and since

$$B A^{-1} = T^{-1} A^{-1} T \in N,$$

$B \in N$ given that N is a normal subgroup of $SL(V)$. Also,

$$B = T^{-1} (A^{-1} T A) = T_1 T_2,$$

where each T_i is a transvection. Let $T_i = \{\phi_i, h_i\}$, where $h_i \in H_i = \ker \phi_i$ for $i = 1, 2$, so

$$T_i(v) = v + \phi_i(v) h_i$$

for all $v \in V$.

Let $W = \langle h_1, h_2 \rangle \leq V$, so the dimension of $\dim W \leq 2$. There must be a hyperplane, L of V that contains W since $\dim V \geq 3$. Now, we will show that $B(L)$ is a subspace of L . Let $l \in L$, then

$$\begin{aligned} B(l) &= T_1 T_2(l) = T_2(l) + \phi_1(T_2(l)) h_2 \\ &= l + \phi_2(l) h_2 + \phi_1(T_2(l)) h_1 = l + \lambda_1 h_2 + \lambda_2 h_2 \in L \end{aligned}$$

where $\lambda_1, \lambda_2 \in \mathbb{F}^\times$, so we have a linear combination of elements of L , which must be in L . Now, we show that $H_1 \cap H_2 \neq 0$. By lemma 4.13, $\dim(H_1 \cap H_2) = n - 2 \geq 1$. Let $z \in H_1 \cap H_2$ such that $z \neq 0$, then we have

$$B(z) = T_1 T_2(z) = z.$$

We assume B is not a transvection (otherwise we would be done), so $B \notin \mathcal{T}(L)$, which contains only transvections and the identity. Suppose $B = \alpha S$ where α is a scalar and

$S \in \mathcal{T}(L)$. We have that $\alpha Sz = Bz = z$, so $Sz = \alpha^{-1}z$, and since $Sz = z + \phi_S(z)l = \alpha^{-1}z$ for some $l \in L$, $\phi_S(z)l$ and therefore l must be a multiple of z or $\phi_S(z) = 0$. Both cases imply $z \in L$, which means $\alpha = 1$ so $S = B$, which is a contradiction.

By lemma 4.21, there exists some element $U \in \mathcal{T}(L)$ that does not commute with B . Let


$$C = UBU^{-1}B^{-1} \neq 1.$$

Then $UBU^{-1} \in N$, so

$$C = (UBU^{-1})B^{-1} \in N.$$

Now, we show that C is a transvection. Let $l \in L$ be arbitrary, then

$$C(l) = UBU^{-1}B(l) = UBB^{-1}(l) = l,$$

since $B^{-1}(l) \in L$, and U^{-1} fixes L , which means C fixes L . Since $B, U \in SL(V)$, $\det(C) = \det(UBU^{-1}B) = 1$, so C is a transvection. Therefore $N = SL(V)$, which completes our proof. 

5. OTHER CLASSICAL GROUPS

We will briefly construct two other families of groups of lie type; the Symplectic and Unitary groups, however we will not go over their simplicity proofs. For more details, about the classical groups, see [Rot95, Chapter 8].

Definition 5.1. Let V be a vector space over \mathbb{F} , then we call a function $f : V \times V \rightarrow \mathbb{F}$ a *bilinear form* if it satisfies the following properties:

- (1) $f(u + v, w) = f(u, w) + f(v, w)$
- (2) $f(u, v + w) = f(u, v) + f(u, w)$
- (3) $f(\alpha u, v) = f(u, \alpha v) = \alpha f(u, v)$.

An equivalent definition is that $f(v, _) : V \rightarrow \mathbb{F}$ and $f(_, v) : V \rightarrow \mathbb{F}$ are both linear functionals. We call a bilinear form f *symmetric* if $f(v, u) = f(u, v)$ for all $u, v \in V$, and we call it *alternating* if $f(v, v) = 0$ for all $v \in V$.

The vector dot product defined on \mathbb{R}^n is a symmetric form. Let f be an alternating bilinear form and $u, v \in V$, then

$$\begin{aligned} 0 &= f(u + v, u + v) \\ &= f(u, u) + f(u, v) + f(v, u) + f(v, v) \\ &= f(u, v) + f(v, u) \\ f(u, v) &= -f(v, u). \end{aligned}$$

If f is a bilinear form such that $f(v, u) = -f(u, v)$, then if \mathbb{F} has characteristic 2, f is symmetric, since $a + a = 2a = 0$, so $a = -a$ for all $a \in \mathbb{F}$. If \mathbb{F} has characteristic $\neq 2$, then \mathbb{F} is alternating. In both cases, $2f(v, v) = 0$.

Definition 5.2. Suppose \mathbb{F} has an automorphism σ (denoted by $\sigma : \alpha \mapsto \alpha^\sigma$) of order 2, that is $\sigma = \sigma^{-1}$. A *hermitian form* (sometimes called a sesquilinear form) on a vector space V over \mathbb{F} is a function $h : V \times V \rightarrow \mathbb{F}$ that has the following properties for all $u, v \in V$ and all $\alpha \in \mathbb{F}$.

- (1) $h(u, v) = h(v, u)^\sigma$
- (2) $h(\alpha u, v) = \alpha h(u, v)$
- (3) $h(u + v, w) = h(u, w) + h(v, w)$.

If h is hermitian, then

$$h(u, \alpha u) = h(\alpha v, u)^\sigma = (\alpha h(v, u))^\sigma = \alpha^\sigma h(v, u)^\sigma = \alpha^\sigma h(u, v),$$

since σ is its own inverse. Also,

$$h(u, v + w) = h(v + w, u)^\sigma = (h(v, u) + h(w, u))^\sigma = h(v, u)^\sigma + h(w, u)^\sigma = h(u, v) + h(u, w),$$

so h satisfies additivity with its second variable.

Definition 5.3. An *inner product space* (V, f) is a vector space V paired with a function $f : V \times V \rightarrow \mathbb{F}$ that is either a symmetric, alternating or hermitian form.

Definition 5.4. Let (V, f) be an inner product space, and let $\{v_1, \dots, v_n\}$ be a basis of V , then *inner product matrix* of f with respect to this basis is the matrix where the entry on the i^{th} row and j^{th} column is $f(v_i, v_j)$.


Inner product matrices uniquely determine f with a given basis. We call an inner product space *nondegenerate* if its the inner product matrices for that space have nonzero determinant.

Definition 5.5. We call a linear transformation $T : V \rightarrow V$ of a nondegenerate space (V, f) an *isometry* if it preserves the form f , that is for all $u, v \in V$,

$$f(Tu, Tv) = f(u, v).$$

Proposition 5.6. All the isometries of the nondegenerate space (V, f) form a group, $Isom(V, f)$, which is a subgroup of $GL(V)$.

Proof. First, we show that all elements of $Isom(V, f)$ have nonzero determinant. Let T be an isometry; if $Tu = 0$, then we have that $f(u, v) = f(Tu, Tv) = f(0, Tv) = 0$ for all $v \in V$. Now, suppose u is nonzero and we construct a basis of V with u as the first element of it. From the definition of an inner product matrix, the entire first row and first column would be zero, which results in a matrix of determinant 0. This contradicts (V, f) being nondegenerate, so $u \neq 0$, and therefore $\ker T = 0$, which means $V \cong V/\{0\} \cong \text{Im} V$ if we consider V as an abelian group. The isomorphism would be T , and therefore T is a bijection, which means its invertible and has nonzero determinant.

To check closure, let T and M be isometries, then $f(u, v) = f(Tu, Tv) = f(MTu, MTv)$ for all $u, v \in V$, so MT is an isometry. The identity is clearly an isometry, and if $f(u, v) = f(Tu, Tv)$ for all $u, v \in V$, $f(T^{-1}u, T^{-1}v)$ must equal $f(u, v)$ since we can take $f(TT^{-1}u, TT^{-1}v) = f(u, v)$ and applying T preserves f . 

We can obtain more classical groups, and then construct more simple finite groups of Lie type from isometry groups.

Definition 5.7. Given a nondegenerate space (V, f) , there is one isometry group up to isomorphism $Isom(V, f)$ for all alternating forms f , and we call this the *symplectic group* $Sp(V)$ or $Sp_n(q)$.

Definition 5.8. Similarly, the isometry groups for all hermitian forms are isomorphic, and we call $Isom(V, f)$ when f is hermitian the *unitary group*, $U(V)$ or $U_n(q^2)$ (since hermitian forms are only defined on fields where the order is a perfect square).

Each of these classical groups allows us to construct a family of simple groups. We can define

$$PSp_{2l}(q) = Sp_{2l}(q)/Z(Sp_{2l}(q))$$

where $Z(Sp_{2l}(q))$ is the center of $Sp_{2l}(q)$. These are simple with the exceptions: $(2l, q) = (2, 2), (2, 3), (4, 2)$. For the unitary groups, we take $SU_n(q^2)$, which is the subgroup of elements of the unitary group that has determinant 1, and we quotient by its center to get

$$SU_n(q^2)/Z(SU_n(q^2)) = PSU_n(q^2),$$

which are simple groups unless $(n, q^2) = (2, 4), (2, 9), (3, 4)$

ACKNOWLEDGMENTS

I would like to thank Dr. Simon Rubinstein-Salzedo and Faizan Hussaini for guidance in writing this paper.

REFERENCES

- [DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Chichester: Wiley, 3rd ed. edition, 2004.
- [DMT91] L. Di Martino and M. C. Tamburini. 2-generation of finite simple groups and some related topics. Generators and relations in groups and geometries, Proc. NATO/ASI, Castelvechio-Pascoli/Italy 1990, NATO ASI Ser., Ser. C 333, 195-233 (1991)., 1991.
- [Gec24] Meinolf Geck. A Course on Lie algebras and Chevalley groups. Preprint, arXiv:2404.11472 [math.RT] (2024), 2024.
- [Kir17] Alexander jun. Kirillov. *An introduction to Lie groups and Lie algebras*, volume 113 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge University Press, reprint of the 2008 hardback edition edition, 2017.
- [Lee11] John M. Lee. *Introduction to topological manifolds*, volume 202 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed. edition, 2011.
- [Rot95] Joseph J. Rotman. *An introduction to the theory of groups.*, volume 148 of *Grad. Texts Math.* New York, NY: Springer-Verlag, 4th ed. edition, 1995.