

Contents

1. S_1: Introduction	1
1.1. Definitions and basics	1
1.2. Classifying characters	4
1.3. Consequences	7
2. S_2: Linear characters	8
2.1. Defining linear characters	8
2.2. The character table	8
2.3. Abelian groups and their duals	9
2.4. Fourier inversion	9
3. A_3: Galois conjugates	10
4. S_3: Permutation characters	11
5. A_4: Quotient characters	12
6. S_4: Products of characters	13
7. S_5: Exterior products	14
8. S_6: Induced characters	15
9. A_5: Restriction	16
10. A_6: Lie type	17
A. Exceptional isomorphisms	18
A.1. Rotational symmetries	18
A.2. Rotations of the cube	20
A.3. Reducing the coordinate ring	22
A.4. Rotations of the tetrahedron	24
A.5. Rotations of the icosahedron	26
A.6. Characters and coordinates	29
A.7. Complexifying	32
A.8. Projective actions	35

Contents

B. Structure of groups of Lie type	38
B.1. Stabilizer subgroups	38
B.2. Tori and coordinates	41
B.3. Conjugacy classes	44
C. Bimodules and adjunction	49
C.1. Tensor product and homomorphisms	49
C.2. Group rings	49
C.3. Trace	50
C.4. Reciprocity	50

1. S_1 : Introduction

The goal of these notes is to introduce some interesting ordinary character theory, by focusing on the characters (and sometimes the representations) of the small-degree symmetric and alternating groups. All our groups will be finite, and all characters will be over $\mathbb{C}$.

1.1. Definitions and basics

What is a character? The easiest explanation is to start with a **representation**, which is a group homomorphism $\phi : G \rightarrow \text{GL}(V)$ for a finite group G and a (positive) finite-dimensional $\mathbb{C}$ -vector space V . Note if we pick a basis for V , then we can treat our homomorphism as ending up in $\text{GL}(n, \mathbb{C})$ instead, but we will often avoid picking explicit bases. We can also think of a representation as defining a linear action of G on V . We call two representations ϕ, ψ **equivalent** if there exists an element $P \in \text{GL}(V)$ such that $P^{-1}\phi(g)P = \psi(g)$ for all $g \in G$ (in particular, P does not depend on specific elements of G).

With this definition of representations, we can then define the **character** afforded by a representation ϕ , often denoted χ_ϕ , as

$$\chi_\phi(g) = \text{Tr}(\phi(g)) \quad (1)$$

Because $\text{Tr}(B^{-1}AB) = \text{Tr}(A)$, traces don't depend on a specific basis, and more generally, equivalent representations yield the same characters. Even more, letting $A = \phi(g)$ and $B = \phi(h)$ for $g, h \in G$, we see that (using ϕ is a homomorphism)

$$\chi_\phi(g) = \chi_\phi(h^{-1}gh) \quad (2)$$

For notational convenience, we'll often drop or adjust the subscript for characters. Because $\phi(e)$ is the identity element of $\text{GL}(V)$ (here $e \in G$ is the notation for the identity element), we see that

$$\chi_\phi(e) = \dim_{\mathbb{C}}(V) \quad (3)$$

Since $g \in G$ has finite order (say k), we know that $\phi(g)^k = 1$, and hence by the Cayley-Hamilton theorem that $\phi(g)$ satisfies $x^k - 1 = 0$. Since every eigenvalue of $\phi(g)$ is a root of

1. S_1 : Introduction

this polynomial, it's a root of unity. Since all roots of this polynomial are distinct, we see $\phi(g)$ is diagonalizable; these two facts imply

$$\chi_\phi(g^{-1}) = \overline{\chi_\phi(g)} \quad (4)$$

Because $\chi_\phi(g)$ is a sum of roots of unity, this also implies that $\chi_\phi(g)$ is an algebraic integer. This fact can be leveraged in many proofs that use Galois theory, because an algebraic integer in $\mathbb{Q}$ is automatically in $\mathbb{Z}$. This is a key ingredient in the character-theoretic proof of Burnside's $p^a q^b$ theorem, for example.

We will work mainly with characters, because they're easier functions to talk about (defined by complex numbers and not complex linear maps/matrices), but they can be a bit more awkward to prove things about, because they in general are **not** homomorphisms. Note that until stated otherwise, a character is **not** just a function $G \rightarrow \mathbb{C}$, but it is attached to a specific representation; later we will remove this restriction and consider characters simply as complex-valued functions satisfying some conditions. But first let's discuss a key way to build new representations from old ones. If V and W are $\mathbb{C}$ -vector spaces, and $\phi : G \rightarrow \text{GL}(V)$ and $\psi : G \rightarrow \text{GL}(W)$ are representations, then we can form a new representation $\phi + \psi : G \rightarrow \text{GL}(V \oplus W)$ from the block diagonal of these two:

$$g \mapsto \begin{pmatrix} \phi(g) & 0 \\ 0 & \psi(g) \end{pmatrix} \quad (5)$$

In terms of characters, note that $\chi_{\phi+\psi} = \chi_\phi + \chi_\psi$. The key take away here is that **the sum of two characters is also a character**. So the set of characters for G is closed under addition, and a natural question is to find a "generating set" for all characters. This is similar to noting that positive integers are closed under multiplication, and thus breaking down all positive integers into their prime constituents, those integers that can't be further subdivided. In that same way, we will now discuss characters that cannot be further broken down as a sum of two other characters. These are called **irreducible characters** and are the prime building blocks for all characters of G : every character is a sum of irreducibles. This sum is finite because $\chi(e) > 0$ for all characters by equation (3).

There is a similar notion, of **irreducible representations**. From the addition formula (5) above, we can make a first pass by defining a representation $\phi : G \rightarrow \text{GL}(W)$ as reducible if we can write $W = U \oplus V$ for G -invariant proper subspaces U and V . Such a decomposition gives a character formula $\chi_W = \chi_U + \chi_V$ where the subscript denotes the restriction of G to that subspace. So in this case χ_W is a reducible character, being the sum of two other characters. If we define W as **irreducible** when it cannot be written as a direct sum of two proper G -invariant subspaces, then the contrapositive of the above says that **an irreducible character is afforded by an irreducible representation**. We have already noted that every character is a sum of irreducibles; it is a wonderful fact that every representation is a sum of irreducibles as well. To prove that, we need (a simple version of) the most fundamental theorem of representation theory.

1. S_1 : Introduction

THEOREM 1.1 (Maschke): *Every representation W is completely reducible: if $U \leq W$ is a G -invariant subspace, then there exists a complementary G -invariant subspace $V \leq W$ with $W = U \oplus V$.*

Note that the theorem says nothing about the *uniqueness* of V ; in general, there are many different choices for a complement.

Proof. We use an averaging trick to construct V . Let V_0 be a $\mathbb{C}$ -linear complement of U in W , which exists because these are all just finite-dimensional vector spaces. The problem is that V_0 is not necessarily G -invariant. Let $P : W \rightarrow U$ be the projection of W onto U with kernel V_0 . Define

$$P_G(w) = \frac{1}{|G|} \sum_{g \in G} P(wg)g^{-1}$$

This is the "averaging" mentioned above. This is a $\mathbb{C}$ -linear map, but it also commutes with the action of G :

$$P_G(wh) = \frac{1}{|G|} \sum_{g \in G} P(whg)g^{-1} = \frac{1}{|G|} \sum_{g \in G} P(whg)(hg)^{-1}h = P_G(w)h$$

Thus the kernel $V = \ker(P_G)$ is a G -invariant subspace of W . Let's show P_G is still a projection. Since U is G -invariant, $P_G(u) = u$ for any $u \in U$, and thus $U \cap V = \{0\}$. This also means that for any $w \in W$, we can write $w = P_G(w) + (w - P_G(w))$, the first in U and the second in $\ker(P_G)$. We have thus shown $W = U \oplus V$. $\square$

COROLLARY 1.2: *Every representation is a direct sum of irreducibles.*

Proof. We use induction on $\dim_{\mathbb{C}}(W)$, the case $\dim_{\mathbb{C}}(W) = 1$ being obvious (invariant subspaces are *subspaces* after all!). If W has no proper invariant subspaces, then it is itself irreducible and we're done. Otherwise, choose an invariant subspace $U \leq W$ of minimal dimension. U must be irreducible. By Maschke's theorem, $W = U \oplus V$ for some invariant proper subspace V . Since $\dim_{\mathbb{C}}(V) < \dim_{\mathbb{C}}(W)$, induction shows V is a direct sum of irreducibles, and thus so is $U \oplus V$. $\square$

COROLLARY 1.3: *An irreducible representation has no proper G -invariant subspaces.*

Proof. If W is a representation, and it has a G -invariant subspace U , then by Maschke's theorem we can write $W = U \oplus V$, so that W is reducible. $\square$

Note the converse of this corollary is trivially true. So we can give an equivalent definition for irreducible representations: those with no proper G -invariant subspaces.

1.2. Classifying characters

We now turn to the uniqueness question of writing an arbitrary character or representation as a sum of irreducibles. We're going to expand our set of complex-valued functions on G : we'll be talking about **class functions** on G , which are functions $\alpha : G \rightarrow \mathbb{C}$ that are constant on conjugacy classes: $\alpha(h^{-1}gh) = \alpha(g)$ for all $g, h \in G$. Equation (2) shows this set contains all characters of G . We'll denote this set as $\mathcal{C}(G)$.

Since an element $\alpha \in \mathcal{C}(G)$ is determined precisely by its (arbitrary) values on each conjugacy class, we see $\mathcal{C}(G)$ is a $\mathbb{C}$ -vector space whose dimension is the number of conjugacy classes of G ; we'll write $\text{Cl}(G)$ for the set of conjugacy classes, so $\dim_{\mathbb{C}} \mathcal{C}(G) = |\text{Cl}(G)|$. We will now put a particularly well-chosen inner product on $\mathcal{C}(G)$:

THEOREM 1.4: *There is an inner product on $\mathcal{C}(G)$ such that the irreducible characters form an orthonormal basis.*

This innocent-looking theorem has some amazing corollaries! [Don't be fooled about its importance though; it's also often called the main theorem of character theory.]

COROLLARY 1.5: *The number of irreducible characters is $|\text{Cl}(G)|$.*

COROLLARY 1.6: *A class function α is a character if and only if it is a positive integral combination of irreducible characters.*

Proof. We basically have seen this already: a character is a finite positive sum of irreducibles, and any such finite sum is a character using the addition construction above. Now that we know any class function has a unique expression as a linear combination of irreducibles, we see this property can be used to characterize characters. $\square$

COROLLARY 1.7: *A character χ is irreducible if and only if $\|\chi\|^2 = \langle \chi, \chi \rangle = 1$.*

Proof. Since an irreducible character is orthonormal, that establishes one direction. For general χ , let

$$\chi = a_1\tau_1 + \cdots + a_m\tau_m$$

where the τ_i are irreducible, and the a_i are positive integers (this is possible by the previous corollary). Then the orthonormality and linearity of the inner product show

$$\langle \chi, \chi \rangle = \sum a_i^2$$

So if $\|\chi\|^2 = 1$, the only possibility is $a_i = 1$ and $m = 1$, so that $\chi = \tau_i$ is irreducible. $\square$

1. S_1 : Introduction

This last corollary does **not** say that any class function is irreducible if its norm-squared is 1! The corollary's prerequisite is we already know χ is a character. For example, if a and b are two complex numbers with $a^2 + b^2 = 1$, then $a\tau_1 + b\tau_2$ has norm 1 for any two irreducible characters τ_1 and τ_2 ; but this expression is only a character when a and b are positive integers by [Corollary 1.6](#).

Let $\mathcal{I}(G)$ denote the set of irreducible characters of G . The above sum expression for $\|\chi\|^2$ is important enough to capture here for all class functions:

$$\|\alpha\|^2 = \sum_{\tau \in \mathcal{I}(G)} \|\langle \alpha, \tau \rangle\|^2 \quad (6)$$

where the right-hand side $\|\cdot\|$ is the complex number norm.

Let's now define this inner product, and then prove [Theorem 1.4](#). If we think of $\alpha \in \mathcal{C}(G)$ as just a sequence of $|\text{Cl}(G)|$ complex numbers, a natural inner product would then be

$$\langle \alpha, \beta \rangle = \sum_{g \in \text{Cl}(G)} \alpha(g) \bar{\beta}(g)$$

This almost works, but we want to actually weight things by the size of the conjugacy classes as well, so we arrive at:

$$\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha(g) \bar{\beta}(g) \quad (7)$$

The scaling factor of $|G|^{-1}$ is so that the irreducibles are not merely orthogonal, but orthonormal.

In order to prove the theorem, we need to explore the irreducible representations of G a bit more. Note that a representation of G is nothing more than a module over $\mathbb{C}[G]$. Recall that from Maschke's theorem ([1.1](#)) that every representation is completely reducible, including the regular representation R_G coming from the regular module of $\mathbb{C}[G]$. Also, since G is finite, we know the group ring $\mathbb{C}[G]$ is Artinian. We can thus apply Artin-Wedderburn theory to write

$$\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_m}(\mathbb{C}) \quad (8)$$

where the n_i are positive integers and $M_n(\mathbb{C})$ means the ring of $n \times n$ matrices over $\mathbb{C}$. The group ring $\mathbb{C}[G]$ has one isomorphism type of minimal right ideal for each n_i : the set J_{n_i} of matrices in $M_{n_i}(\mathbb{C})$ with all but the first row zero. These are all the isomorphism types. These are irreducible representations, since they have no proper submodules (see [Corollary 1.3](#)). Conversely (also by [Corollary 1.3](#)), every irreducible representation is a quotient of $\mathbb{C}[G]$, and complete reducibility then implies it's isomorphic to a submodule of the group ring. We have thus shown that the J_{n_i} represent a complete set of isomorphism types for irreducible representations of G .

1. S_1 : Introduction

Proof of Theorem 1.4. Let τ_i be the irreducible character afforded by J_{n_i} from above. For any character of G , we can extend it linearly to get a map from $\mathbb{C}[G] \rightarrow \mathbb{C}$.

We can write $1 = \sum e_i$ based on the decomposition in equation (8), where $e_i \in M_{n_i}(\mathbb{C})$ is idempotent (it's the identity matrix). Then we have e_i acting trivially on J_{n_i} , but $J_{n_j}e_i = 0$ for $i \neq j$. Thus

$$\tau_i(e_j) = \delta_{ij}n_i = \begin{cases} n_i & i = j \\ 0 & i \neq j \end{cases}$$

This shows the irreducible characters afforded by the J_{n_i} (at least when extended to $\mathbb{C}[G]$) are distinct. Of course, if $\tau_i = \tau_j$ on G , then the same holds (by linearity) on $\mathbb{C}[G]$.

We have $\mathcal{I}(G) = \{\tau_1, \dots, \tau_m\}$. Now we show $\mathcal{I}(G)$ is a basis for $\mathcal{C}(G)$. To see they are linearly independent, suppose

$$\sum c_i \tau_i \equiv 0$$

Then by applying the above sum to e_i , we see that $c_i n_i = 0$, implying $c_i = 0$. This is true for all i , so the sum is identically zero, and the τ_i are linearly independent. To see they form a basis, we need to show that $|\mathcal{I}(G)| = m$ is equal to $\dim \mathcal{C}(G) = k = |\text{Cl}(G)|$. To do that, we compute $\dim Z(\mathbb{C}[G])$ in two ways. If $z \in Z(\mathbb{C}[G])$, then from $h^{-1}zh = z$ we see that the coefficient of $h^{-1}gh$ in z is equal to the coefficient for g . These coefficients are arbitrary, as long as they agree on conjugacy classes, so $\dim Z(\mathbb{C}[G]) = k$. From the Artin-Wedderburn decomposition in (8) above, the center of $\mathbb{C}[G]$ is the direct product of the center of each $M_{n_i}(\mathbb{C})$, which is always the set of scalar matrices. Each of these centers contributes 1 dimension (being isomorphic to $\mathbb{C}$), so $\dim Z(\mathbb{C}[G]) = m$.

Finally we will show the $\mathcal{I}(G)$ are orthonormal. For that we need to express the e_i as linear combinations of the elements of G . To that end, we consider R_G , the regular representation, with associated character we'll call ρ . The basis for R_G is G itself, and G the group acts on this basis via right multiplication. It follows then that

$$\rho(g) = \begin{cases} |G| & g = e \\ 0 & g \neq e \end{cases} \quad (9)$$

We use this to determine the coefficient of g in the expression for e_i . Write $e_i = \sum a_g g$ for complex numbers a_g . Then from the above we have $\rho(e_i g^{-1}) = a_g |G|$. But $e_j e_i = 0$ for $j \neq i$, and $e_i^2 = e_i$ is the identity in $M_{n_i}(\mathbb{C})$, so $e_i g^{-1}$ acts as 0 on J_{n_j} and as g^{-1} on J_{n_i} . Since $M_{n_i}(\mathbb{C}) \cong (J_{n_i})^{n_i}$ (one for each row that can be non-zero), we thus have $\rho(e_i g^{-1}) = n_i \tau_i(g^{-1})$ and

$$e_i = \frac{n_i}{|G|} \sum_{g \in G} \tau_i(g^{-1}) g = \frac{\tau_i(e)}{|G|} \sum_{g \in G} \bar{\tau}_i(g) g \quad (10)$$

Now orthogonality and orthonormality follow from

$$\delta_{ij} n_j = \tau_j(e_i) = \frac{\tau_i(e)}{|G|} \sum_{g \in G} \bar{\tau}_i(g) \tau_j(g) = \tau_i(e) \langle \tau_j, \tau_i \rangle \quad \square$$

1.3. Consequences

We already know that $|\mathcal{I}(G)| = \dim \mathcal{C}(G) = |\text{Cl}(G)|$. We can recover $|G|$ itself from the irreducible character degrees:

LEMMA 1.8: We have $\sum_{\tau \in \mathcal{I}(G)} \tau(e)^2 = |G|$.

Proof. If we write $\mathcal{I}(G) = \{\tau_1, \dots, \tau_m\}$, then we saw above that $\tau_i(e) = \dim J_{n_i} = n_i$. The Artin-Wedderburn decomposition in eq. (8) then says

$$|G| = \dim \mathbb{C}[G] = \sum n_i^2 = \sum \tau_i(e)^2 \quad \square$$

Of course orthonormality implies that every character (and indeed every class function) has a unique expression as a linear sum of irreducible characters. The following shows this uniqueness extends to decompositions of representations.

LEMMA 1.9: If V is a representation of G , then we can write $V = \bigoplus J_{n_i}^{a_i}$, where $a_i = \langle \chi_V, \tau_i \rangle$.

Proof. We know such an expression is possible by Corollary 1.2; we just don't know how to determine the a_i . The coefficient of τ_i in the decomposition of χ_V is indeed $\langle \chi_V, \tau_i \rangle$. But it is also a_i since the block diagonal formula (5) shows

$$\chi_V = \sum a_i \tau_i \quad \square$$

We close this introductory section with the stated goal, of establishing the characters of the trivial group S_1 , and checking some of the above results in this case. Of course, the only representations of S_1 are trivial, so to be irreducible, they have to be irreducible as $\mathbb{C}[S_1] \cong \mathbb{C}$ modules; that is, as vector spaces! So the only possibility is the vector space $\mathbb{C}$ itself, which affords a trivial character: $\chi_1(g) = 1$ for all $g \in G$. Every group has such a trivial homomorphism, and hence has this trivial representation with trivial character.

S_1 has one conjugacy class, and we've established one irreducible character, so Corollary 1.5 holds. S_1 also has order 1, and $\chi_1(e)^2 = 1$, so Lemma 1.8 also holds. We also have for a general group G

$$\langle \chi_1, \chi_1 \rangle = \frac{1}{|G|} \sum_{g \in G} \bar{\chi}_1(g) \chi_1(g) = \frac{1}{|G|} \sum_{g \in G} 1 = 1$$

so Corollary 1.7 correctly identifies that χ_1 is irreducible for all groups G , and in particular S_1 .

A. Exceptional isomorphisms

In this appendix we show that A_5 is the rotational symmetry group I of the icosahedron in $\mathbb{R}^3$, and use that to help establish some of the Lie type exceptional isomorphisms:

$$\begin{array}{lll} PSL(2,3) \cong A_4 & PSL(2,5) \cong A_5 & PGL(2,5) \cong S_5 \\ PGL(2,3) \cong S_4 & PSL(2,4) \cong A_5 & PSL(2,9) \cong A_6 \end{array}$$

Where possible, we will provide alternative proofs of these isomorphisms, but the common thread will be the A_5 action on the icosahedron, and the associated representation in its symmetry group. In fact, we will establish isomorphisms in almost every possible pairing for A_5 :

$$\begin{array}{ccc} SL(2,4) & & PSL(2,5) \\ & \nwarrow \cong & \nearrow \cong \\ & I & \\ & \downarrow \cong & \\ & A_5 & \end{array}$$

(Note: Curved arrows also connect $SL(2,4)$ to A_5 and $PSL(2,5)$ to A_5 , both labeled $\cong$.)

We will also look at the other Platonic solids through the course of our work, to help give some (easier) examples of the coordinate ring reduction technique discussed later. These other solids will establish the smaller group isomorphisms mentioned above. The ideas and isomorphisms here are a beautiful combination of high-level concepts and getting your hands dirty (as far as you want to!), spanning several areas (group theory, (permutation) representations, geometric algebra, finite linear groups, etc.). The final section of the appendix will show how to prove most of these isomorphisms directly from projective actions.

A.1. Rotational symmetries

A rotational symmetry σ of an object $P \subset \mathbb{R}^3$ is determined by an **axis of rotation** and an **angle**, and is required to preserve P setwise: $\sigma(P) = P$. Here the axis of rotation $L = \{t\mathbf{u} \mid t \in \mathbb{R}\}$ is a line through the origin determined by a unit vector $\mathbf{u}$, and the angle of rotation θ is considered modulo 2π . Note that we need an orientation to talk about

A. Exceptional isomorphisms

clockwise vs. counterclockwise rotations. So we insist that rotations are always clockwise when facing along the *positive* direction of L (where t is increasing). Of course, the rotation determined by θ and $\theta + 2\pi$ are the same, as are all the rotations with $\theta = 0$ (independent of what $\mathbf{u}$ we might choose). Slightly more subtle is that $(\mathbf{u}, \theta)$ determines the same rotation as $(-\mathbf{u}, -\theta)$, since their positive directions are different ($-\theta$ is just the counterclockwise rotation by θ).

A key fact is that a rotation is nothing more than an element of the special orthogonal group $SO(3, \mathbb{R})$. To see that, we need to establish that an arbitrary rotation σ is linear, and its matrix representation A_σ is such that both $\det(A_\sigma) = 1$ and $A_\sigma^T A_\sigma = I$, the identity matrix. In fact, defining a rotation without referencing a linear transformation or isometry is quite subtle, but we'll ignore most of that and be a bit handwavy. What we need to know is that a rotation preserves angles and lengths in $\mathbb{R}^3$. From there, if $\mathbf{v}$ and $\mathbf{w}$ are two vectors based at the origin, then they form a parallelogram with $\mathbf{v} + \mathbf{w}$ one of the other sides. Rotating gives a new parallelogram, with sides $\sigma(\mathbf{v}), \sigma(\mathbf{w}), \sigma(\mathbf{v} + \mathbf{w})$, and we have thus shown $\sigma(\mathbf{v} + \mathbf{w}) = \sigma(\mathbf{v}) + \sigma(\mathbf{w})$. Preserving lengths clearly means that $\sigma(r\mathbf{v}) = r\sigma(\mathbf{v})$ as well, so that σ is indeed a linear transformation. Now let $\mathbf{u}$ be the unit vector defining the axis of rotation for σ . Then σ fixes its axis pointwise, so that $\sigma(\mathbf{u}) = \mathbf{u}$. Expand this to an orthogonal basis $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ for $\mathbb{R}^3$. Then σ is acting as a rotation on the plane spanned by $\{\mathbf{v}, \mathbf{w}\}$, and so in this basis we have

$$A_\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{pmatrix} \quad (11)$$

It's an easy calculation that $\det(A_\sigma) = 1$ and $A_\sigma^T A_\sigma$ is the identity, and thus $A_\sigma \in SO(3, \mathbb{R})$. What's nice is that the converse is true too: every element $A \in SO(3, \mathbb{R})$ is a rotation, and this is usually considered a modern version of a theorem of Euler. To prove the converse, note that the characteristic polynomial $\chi_A(t)$ of A has degree 3, and hence by the intermediate value theorem has a real root. This real root λ is an eigenvalue of A , with corresponding unit eigenvector: $A\mathbf{u} = \lambda\mathbf{u}$. Since A is orthogonal, it preserves lengths, so that $\|\mathbf{u}\| = \|A\mathbf{u}\| = |\lambda|\|\mathbf{u}\|$, implying $|\lambda| = 1$ and $\lambda = \pm 1$. First we show that we can always take $\lambda = 1$. Otherwise, if $\lambda = -1$, then consider the other roots of $\chi_A(t)$. If they are all real, then they are all ± 1 , but their product is $\det(A) = 1$, so at least one must be $+1$. If $\chi_A(t)$ has two complex conjugate roots, say $a \pm bi$, then we have

$$1 = \det(A) = \lambda(a + bi)(a - bi) = -(a^2 + b^2) \leq 0$$

and this contradiction shows this case doesn't happen. So in all cases we can assume $\lambda = 1$. But then if we expand to an orthogonal basis $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$, A will fix the plane spanned by $\{\mathbf{v}, \mathbf{w}\}$ by orthogonality, and having determinant 1 on that plane implies it looks like the right-hand side of Equation (11). This is clearly a rotation with axis determined by $\mathbf{u}$ and angle θ , so we've successfully shown $SO(3, \mathbb{R})$ is exactly the set of rotational symmetries of $\mathbb{R}^3$.

This has some nice consequences. For example, a product of rotations is another rotation, something that isn't immediately obvious from a geometric description. Also, the rotational symmetries of an object $P \subset \mathbb{R}^3$ form a subgroup of $SO(3, \mathbb{R})$. For example, when $P = \{0\}$, then this group is all of $SO(3, \mathbb{R})$. When P is a line through the origin, then the rotational symmetry group is trivial: $\{I\}$. And when P is a regular n -sided polygon in the $(\mathbf{x}, \mathbf{y})$ -plane centered at the origin, then the rotational symmetry group is cyclic of order n , generated by an element like in Equation (11) with $\theta = \frac{2\pi}{n}$.

We will next look at other highly symmetric objects in $\mathbb{R}^3$, and their corresponding (finite!) rotational symmetry groups. These shapes are the five Platonic solids. Their potential existence can be proven using Euler's formula relating number of points, edges, and faces of a convex polyhedron. Their *actual* existence usually starts with the cube as a given, and constructs the rest from the cube. We will also start with the cube in our studies.

A.2. Rotations of the cube

Define the cube $\mathcal{C}$ as the usual shape, with 8 vertices at $(\pm 1, \pm 1, \pm 1)$. We will write C for its rotational symmetry group, which we consider living in $SO(3, \mathbb{R})$. Before beginning, we note that the octahedron (another of the five Platonic solids) is **dual** to $\mathcal{C}$, meaning it is constructed from swapping faces and vertices, and drawing edges based on incidence. What's important for us is that C is also the rotational symmetry group of the regular octahedron, so we don't lose anything by focusing on the cube. This same situation will happen with the icosahedron and dodecahedron (the tetrahedron is self-dual, so is the odd one out).

Our strategy will be the same for all the Platonic solids we encounter. First, we establish the order and conjugacy classes of the rotational symmetry group. We then digress a bit to show the isomorphism type of the symmetry group based on pure finite group theory. Then we build the **coordinate ring** of the group (which will be defined later in this section). Quotienting out by a maximal ideal of this coordinate ring lands our symmetry group in a finite linear group (that is, a linear group over a finite field: $SL(3, q)$ for some prime power q). From there, we either look for an invariant plane, or "projectivize", to lower the dimension and get a map into some $PGL(2, q)$ group. We will show when the composition of these various homomorphisms is injective, and finally order considerations will give us some of the exceptional isomorphisms laid out at the beginning of this appendix. All the details will be made clear over the next several sections.

From just playing around with a physical cube, it should be obvious that any face can be rotated to any other face. And if a rotation fixes a face, then it is essentially rotating a square in a plane (the plane that contains the face), and so from what was discussed above, this stabilizer is cyclic of order 4. The orbit-stabilizer theorem then implies $|C| = 6 \cdot 4 = 24$, since there are 6 faces. For every rotation, its axis determines a half-ray $\{t\mathbf{u} \mid t \geq 0\}$ that

A. Exceptional isomorphisms

will intersect the cube in exactly one point. We discuss what happens when that point is a vertex, lies on an edge, or lies on a face.

When the axis goes through a face, it actually goes through two opposite faces, and must be a rotation of the squares that form these faces. In particular, the corresponding rotation is a symmetry of these squares, and so is a rotation by an angle that is a multiple of $\frac{2\pi}{4}$. Consider the ones that are an odd such multiple, so they have order 4 in C . There are $3 \cdot 2 = 6$ such rotations: 3 pairs of opposite faces, 2 angle choices (up to 2π). Now a rotation by $\frac{2\pi}{4}$ around one face is equivalent to a rotation by $\frac{6\pi}{4}$ around the opposite face (this is just saying the same thing we said above: $(\mathbf{u}, \frac{2\pi}{4})$ is equivalent to $(-\mathbf{u}, -\frac{2\pi}{4})$). Since C acts transitively on faces, we see that all 6 of these elements are conjugate. Similarly, the remaining 3 elements that are rotations by π around an axis through a face are also conjugate. If the axis for our rotation goes through an edge, then it must be a rotation by π (since it interchanges the two faces that meet at that edge). There are 12 edges to the cube, and they get paired up in opposites, since an axis of rotation will go through two of them. So we get $\frac{12}{2} = 6$ such rotations, and because C acts transitively on edges, these are all conjugate. Finally, suppose our axis goes through a vertex. Then as before, it goes through 2 of them, and the angle of rotation is a multiple of $\frac{2\pi}{3}$, since three edges meet there. There are $\frac{8}{2} \cdot 2 = 8$ such elements, and they are all conjugate (because $\frac{4\pi}{3}$ is equivalent to $-\frac{2\pi}{3}$).

We have already listed $6 + 3 + 6 + 8 = 23$ non-identity elements of C , and $|C| = 24$, so we know all its elements. Note that if $\sigma \in C$ fixes a vertex/edge/face, then any conjugate fixes the same type of thing, since C preserves setwise the vertices, edges, and faces. So the above really does describe the conjugacy classes of C . It turns out that this is already enough to give the isomorphism type of C .

PROPOSITION A.1: *Let G be a group of order 24, that does not have a normal Sylow subgroup. Then $G \cong S_4$.*

Note C cannot have a normal Sylow 2-subgroup, since it has $6 + 3 + 6 > 7$ elements of order dividing 4, and it cannot have a normal Sylow 3-subgroup because it has $8 > 2$ elements of order 3. So this proposition really does show $C \cong S_4$.

Proof. Since G has more than one Sylow 3-subgroup, and the number of them divides 8, it must have 4 such subgroups. The action via conjugation gives a map from $G \rightarrow S_4$; we will show this map is injective, so that by order considerations it gives an isomorphism $G \cong S_4$.

Let K be the kernel of the map above, so that K is a normal subgroup that normalizes every Sylow 3-subgroup of G . Since $4 = [G : N_G(P)]$ for any Sylow 3-subgroup $P \leq G$, the only possibility is $|K| = 2$. Then G/K is a group of order 12 with 4 Sylow 3-subgroups. That accounts for 8 elements of order 3, so G/K can only have one Sylow 2-subgroup, which is thus normal. The preimage of this subgroup is then a normal Sylow 2-subgroup of G . This contradicts our hypothesis, however, so K must be trivial, as claimed. $\square$

There is another way to see $C \cong S_4$: it follows because C acts on the 4 main diagonals of the cube, and this action is faithful, so gives an embedding $C \rightarrow S_4$, and again order considerations show this is an isomorphism.

Consider an arbitrary element $\sigma \in C$. Using the standard basis $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ of $\mathbb{R}^3$ (which point into the centers of three faces of $\mathfrak{C}$), we see that σ takes this basis set into the set $\{\pm\mathbf{x}, \pm\mathbf{y}, \pm\mathbf{z}\}$, the full set of centers of faces of $\mathfrak{C}$. In this basis, then, the entries of A_σ are all from the set $\{0, \pm 1\}$. This means that $C \leq SL(3, \mathbb{Z})$: every A_σ has determinant 1, and integer entries. This is the crux of reducing the coordinate ring. Before we proceed however, note that saying A_σ is orthogonal is the same as saying it preserves length, because

$$\|\mathbf{v}\|^2 = \mathbf{v}^T \mathbf{v} = \mathbf{v} (A_\sigma^T A_\sigma) \mathbf{v} = (A_\sigma \mathbf{v})^T (A_\sigma \mathbf{v}) = \|A_\sigma \mathbf{v}\|^2$$

so that being orthogonal means preserving the quadratic sum $x^2 + y^2 + z^2$ of vector coordinates. This is our replacement for talking about orthogonality in the finite linear groups we consider next.

A.3. Reducing the coordinate ring

If $J \leq \mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, then $\mathbb{Z}/J$ is a field, and if we reduce the coefficients of $A \in SL(3, \mathbb{Z})$ modulo $I = J$, we get a map into $SL(3, \mathbb{Z}/J)$. Note that $J = \langle p \rangle$ in this case, so we are getting a map into $SL(3, \mathbb{F}_p)$, sometimes written $SL(3, p)$. We will use hats to distinguish elements in these finite linear groups, so that $\hat{C}$ represents the image of C in $SL(3, \mathbb{F}_p)$. Even in this linear group over our reduced coordinate ring, we still have $\det(\hat{A}_\sigma) = 1$, and it preserves the quadratic form $x^2 + y^2 + z^2$. For example, if $p = 2$, we get a mapping from C to $\hat{C} \leq SL(3, \mathbb{F}_2)$. Now if $\hat{C}$ preserves $x^2 + y^2 + z^2 = (x + y + z)^2$, then it preserves the plane $x + y + z = 0$ in $\mathbb{F}_2^3$. Restriction of the action of $\hat{C}$ to this plane gives a homomorphism of $\hat{C}$ into $GL(2, \mathbb{F}_2)$; note we can't assert the determinant is still 1 in the general case. Composing all these homomorphisms gives a map from C to $GL(2, 2)$.

Our technique therefore, of **reducing the coordinate ring**, is to find a subring of $\mathbb{R}$ where all the coefficients of all the A_σ live. This will always be a finitely generated ring, of the form $R := \mathbb{Z}[\alpha_1, \dots, \alpha_m]$, because our rotational symmetry groups will always be finite, so there's only finitely many matrix entries to consider. We will then find a maximal ideal $M \leq R$, and by reducing entries modulo M we get a mapping from our group into the linear group $SL(3, R/M)$. The important part is that because R is a finitely generated ring, it turns out for $\mathbb{Z} \leq R$, the ideal $\mathbb{Z} \cap M$ is also a maximal ideal of $\mathbb{Z}$, and that R/M is actually a **finite** field extension over $\mathbb{Z}/(\mathbb{Z} \cap M)$; in particular, R/M is a finite field. We won't prove this general fact about finitely generated rings; it is a special case of a generalization of Hilbert's Nullstellensatz. In the cases we will consider, we will construct the R and M explicitly, and identify the quotients directly. We only mention the general theory to assure you that the technique always works.

A. Exceptional isomorphisms

Once we've reduced the coordinate ring, we've mapped our group into a finite linear group. The next step (at least in the cases treated in this appendix) is to try and reduce the dimension. The typical way to do that is to find an invariant proper linear subspace: this is what we did above with $\hat{C} \leq SL(3, \mathbb{F}_2)$ fixing a plane (dimension 2 linear subspace), so we actually can treat $\hat{C}$ as living in $GL(2, \mathbb{F}_2)$. In the rotation groups we work with here, this nice invariant linear subspace will only exist in characteristic 2 (and essentially for the same reasons outlined for $\hat{C}$ above). In odd characteristic, reducing the dimension requires projectivization.

The idea of **projectivization** is that, in our cases, our finite linear subgroups will always fix the zero set of some homogeneous quadratic ($x^2 + y^2 + z^2$ above). So if we move from the affine vector space $\mathbb{F}_q^3$ to the projective plane $\mathbb{P}_q^2$, we will have a well-defined subset (the zero set of our quadratic) on which our linear subgroup acts. For example, continuing with the cube case, if we let $J = \langle 3 \rangle$ be a maximal ideal of $\mathbb{Z}$, then we get $C \rightarrow \hat{C} \leq SL(3, \mathbb{F}_3)$. This subgroup $\hat{C}$ fixes the zero set $V := \{(x, y, z) \mid x^2 + y^2 + z^2 = 0\}$, but it does not fix any proper linear subspace of $\mathbb{F}_3^3$. If we map $\hat{C}$ down to the projective group $GL(3, \mathbb{F}_3) \rightarrow PGL(3, \mathbb{F}_3)$, then we get a subgroup $\hat{C}_{\mathbb{P}} \leq PGL(3, \mathbb{F}_3)$ that fixes the zero set of $V_{\mathbb{P}} := \{[x : y : z] \mid x^2 + y^2 + z^2 = 0\}$. In the affine space $\mathbb{F}_3^3$, V is a conic containing 9 points; in particular, it's not a linear subspace. In the projective plane $\mathbb{P}_3^2$, however, $V_{\mathbb{P}}$ is now a subspace with 4 points, and is in fact isomorphic to a projective line $\mathbb{P}_3^1$. That is to say, in the projective plane, our (projective) linear group $\hat{C}_{\mathbb{P}}$ *does* fix a (projective) linear subspace, and we get an induced inclusion $\hat{C}_{\mathbb{P}} \leq PGL(2, \mathbb{F}_3)$. In odd characteristic, this is what we will use to reduce dimension.

Let's flesh out this example a bit. The four points of $V_{\mathbb{P}}$ are $[1 : 1 : 1]$ and coordinate permutations of $[-1 : 1 : 1]$. For a non-degenerate conic like $V_{\mathbb{P}}$, there is always a linear transformation of $\mathbb{P}_q^2$ that takes the conic to the zero set $W_{\mathbb{P}} = \{[x : y : z] \mid xy + xz + yz = 0\}$. The four points of $W_{\mathbb{P}}$ in $\mathbb{P}_3^2$ are $[1 : 1 : 1]$ and coordinate permutations of $[1 : 0 : 0]$. The exact linear transformation varies depending on the original quadratic equation and the underlying field, but in our present case it can be taken to be $O + I$, where O is a matrix with every entry 1, and I is the identity matrix. The reason the equation for $W_{\mathbb{P}}$ is so nice lies in the fact it can be written as $(x + z)(y + z) = z^2$, and that has a very natural parameterization from the projective line: $[r : s] \mapsto [r^2 : s^2 : rs]$. Composing this with our linear transformation $O + I$, we get the following isomorphism from $\mathbb{P}_3^1$ to $V_{\mathbb{P}}$:

$$[r : s] \mapsto [r^2 + s^2 : (r - s)^2 + s^2 : (r + s)^2 + s^2] \quad (12)$$

To recap then, for a finite subgroup G of $SO(3, \mathbb{R})$, we can find a finitely generated subring $R \leq \mathbb{R}$ such that $G \leq SL(3, R)$ and it preserves some homogeneous quadratic form. If we pick a maximal ideal $M \leq R$, then R/M is a finite field and we get a map from G to $\hat{G} \leq SL(3, R/M)$, still preserving that quadratic form. If R/M is characteristic 2, then it's very likely $\hat{G}$ preserves a plane, so is really a subgroup of $GL(2, R/M)$. In the odd characteristic case, the zero set of the quadratic is a conic, that after projectivization becomes isomorphic

A. Exceptional isomorphisms

to a projective line; in this case, we can consider $\hat{G}$ as a subgroup of $PGL(2, R/M)$. As noted before, we will always make these steps explicit.

Going back to $\hat{C}_{\mathbb{P}} \leq PGL(2, \mathbb{F}_3)$: we want to show that the induced homomorphism $C \rightarrow \hat{C}_{\mathbb{P}}$ is injective. Consider one of the order 4 rotations σ that fixes a face of the cube $\mathfrak{C}$. We choose σ so that it fixes the face whose corners all have z -coordinate $+1$, and rotates that face by $\frac{\pi}{2}$ clockwise when viewing the face from the positive z -axis. Then we have

$$\sigma(\mathbf{x}) = -\mathbf{y} \quad \sigma(\mathbf{y}) = \mathbf{x} \quad \sigma(\mathbf{z}) = \mathbf{z}$$

In particular, σ^2 (the element we really care about) negates $\mathbf{x}$ and $\mathbf{y}$ and fixes $\mathbf{z}$. This action is still non-trivial in $SL(3, \mathbb{F}_3)$, so $\hat{\sigma}^2 \neq 1$. In the induced projective action on $V_{\mathbb{P}}$, $\hat{\sigma}_{\mathbb{P}}^2$ will send $[1:1:1]$ to $[1:1:-1]$, and so is also non-trivial there. We have thus shown that σ is not in the kernel of $C \rightarrow \hat{C}_{\mathbb{P}}$. But because we know $C \cong S_4$, it has a unique minimal normal subgroup that contains σ (and all its conjugates). This means the map $C \rightarrow \hat{C}_{\mathbb{P}} \leq PGL(2, \mathbb{F}_3)$ must be injective. But $|C| = |S_4| = 24 = |PGL(2, \mathbb{F}_3)|$ (see the last section of this appendix for the order of $PGL(2, \mathbb{F}_3)$), and we thus have an isomorphism $S_4 \cong C \cong PGL(2, 3)$.

A.4. Rotations of the tetrahedron

We will let $\mathfrak{T}$ be the regular tetrahedron on $\mathbb{R}^3$; it can be constructed using four adjacent vertices of the cube, namely $(1, 1, 1)$ and coordinate permutations of $(-1, 1, 1)$. Then just draw edges between every pair of vertices, to make a solid with 4 vertices, 6 edges, and 4 triangular faces. We write T for the rotational symmetry group of $\mathfrak{T}$.

Just as with the cube case above, we can use the orbit-stabilizer theorem to compute $|T|$. A rotation with an axis through an edge will have order 2, and that's the full stabilizer; there are 6 edges, so $|T| = 12$. A rotation whose axis goes through an edge has order 2, and the axis goes through an opposite edge as well. There are thus $\frac{6}{2} = 3$ such rotations in T . A rotation with an axis through a vertex is slightly different for $\mathfrak{T}$ than it was for the cube: on the opposite side of the vertex there isn't another vertex, but rather a face. Since the face has 3 sides, the rotation is a multiple of $\frac{2\pi}{3}$. But unlike in the cube case, we can't identify a rotation with its negative (counter-clockwise) inverse, because there's no way to rotate a vertex to a face. So there are 4 possible axes, and 2 possible non-trivial angles to rotate by, giving 8 elements. Since $1 + 3 + 8 = 12$, these are all the elements of T . Of course, since T is transitive on vertices, all the $\frac{2\pi}{3}$ rotations are conjugate (there are 4 of them, one for each vertex). But these are *not* conjugate to the other 4 rotations of angle $-\frac{2\pi}{3}$. One way to see this is to note 8 doesn't divide $12 = |T|$, and a size of a conjugacy class always divides the group order. So T has 4 conjugacy classes of rotations.

Just as before, this is enough to identify the isomorphism type of T , since it has 8 elements of order 3, and thus can't have a normal Sylow 3-subgroup.

A. Exceptional isomorphisms

PROPOSITION A.2: *If a group G has order 12 and doesn't have a normal Sylow 3-subgroup, then $G \cong A_4$.*

Proof. If G doesn't have one Sylow 3-subgroup, it must have 4. The conjugation action on these 4 gives a map $G \rightarrow S_4$, and the kernel is trivial (as a proper subgroup of a Sylow 3-subgroup). Thus G is isomorphic to an order 12 subgroup of S_4 , which must be A_4 . $\square$

We now follow the same plan as for the cube group C : we want to identify the coordinate ring of T . We will do that in a different coordinate system than the standard (x, y, z) -axes in $\mathbb{R}^3$; this will change the entries of our matrices, and will also change our invariant quadratic form. We will use three of the vertices of $\mathfrak{T}$ as basis elements: $\mathbf{a} = (-1, 1, 1)$, and similarly define $\mathbf{b}$ and $\mathbf{c}$. These are *not* orthogonal, and so they change the quadratic form that T will preserve as a subgroup of $SO(3, \mathbb{R})$. Let P be the change-of-basis matrix, which is just a matrix with columns $\mathbf{a}, \mathbf{b}, \mathbf{c}$. Since the original quadratic form is $\mathbf{v}^T \mathbf{v}$, the new one is

$$(P\mathbf{v})^T(P\mathbf{v}) = \mathbf{v}^T(P^T P)\mathbf{v} = \mathbf{v}^T(-O + 4I)\mathbf{v} = -(x + y + z)^2 + 4(x^2 + y^2 + z^2) \quad (13)$$

As before, O is the matrix with all entries 1, and I is the identity matrix. We compute $P^T P = -O + 4I$ directly; the right-hand side above is easy to calculate when we express the matrix as a linear combination of O and I .

So T fixes this quadratic form. Let $\sigma \in T$ be the $\frac{2\pi}{3}$ rotation about the vertex $(1, 1, 1)$ of $\mathfrak{T}$. This fixes that vertex and sends $\mathbf{c} \mapsto \mathbf{b} \mapsto \mathbf{a} \mapsto \mathbf{c}$. Thus $A_\sigma \in SO(3, \mathbb{R})$ has integer entries. Similarly, a rotation fixing vertex $\mathbf{a}$ will cyclically permute $\mathbf{b}, \mathbf{c}$, and $(1, 1, 1) = \mathbf{a} + \mathbf{b} + \mathbf{c}$. So all order 3 elements of T have integer entries in their matrices. Since these elements generate T , it must be that the coordinate ring for T is $\mathbb{Z} \subset \mathbb{R}$, and we can consider $T \leq SL(3, \mathbb{Z})$. Once again we can reduce the coordinate ring modulo some maximal ideals of $\mathbb{Z}$. Reducing by the ideal $J = \langle 3 \rangle$ gives a map from T to a subgroup $\hat{T} \leq SL(3, \mathbb{F}_3)$, preserving the quadratic form $x^2 + y^2 + z^2 - (x + y + z)^2$. If V is the zero set of this quadratic in $\mathbb{F}_3^3$, then when we projectivize, $V_{\mathbb{P}}$ is a set of 4 points (those where every coordinate is non-zero, just like before). Again we have an isomorphism of $V_{\mathbb{P}}$ and $\mathbb{P}_3^1$, so we get an induced homomorphism $\hat{T} \rightarrow \hat{T}_{\mathbb{P}} \leq PGL(2, \mathbb{F}_3)$. Note that $V_{\mathbb{P}}$ contains the coordinate vectors: $\{\hat{\mathbf{a}}, \hat{\mathbf{b}}, \hat{\mathbf{c}}\} \subset V_{\mathbb{P}}$. So the induced action by elements of T is non-trivial (only the identity in T can fix 3 [hence all] vertices), and $T \rightarrow \hat{T}_{\mathbb{P}}$ is an embedding.

Order considerations aren't enough here, since $|T| < |PGL(2, \mathbb{F}_3)|$. Of course, we know from the cube work above that $PGL(2, 3) \cong S_4$, so there is only possible subgroup of order 12 that T can be mapping to, and that's $PSL(2, \mathbb{F}_3)$. But let's see that directly. We continue to use σ to denote the rotation that fixes $\mathbf{a} + \mathbf{b} + \mathbf{c}$, and cyclically permutes $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$. This action restricted to $V_{\mathbb{P}}$ will thus fix the point $[1 : 1 : 1]$, and rotate $[1 : 1 : -1]$ by "moving the minus sign to the left". According to Equation (12) then, since $[1 : 0] \mapsto [1 : 1 : 1]$ and $[0 : 1] \mapsto [-1 : 1 : 1]$, $\hat{\sigma}_{\mathbb{P}}$ acts on $\mathbb{P}_3^1$ as the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, which has determinant 1. Since T

is generated by the conjugates of σ , all elements of $\hat{T}_{\mathbb{P}}$ then have determinant 1, so in fact $\hat{T}_{\mathbb{P}}$ is contained in $PSL(2, \mathbb{F}_3)$, and we now have seen directly that

$$A_4 \cong T \cong PSL(2, 3)$$

We'll finish with a word of caution: the above worked because determinant is well-defined on $PGL(2, \mathbb{F}_3)$, since every scalar matrix in $GL(2, \mathbb{F}_3)$ has determinant 1. In other fields (like $\mathbb{F}_5$ in the next section), the determinant is only well-defined up to the quadratic residues of the field.

A.5. Rotations of the icosahedron

The icosahedron case is more interesting than the previous two, because (as we'll see) the coordinate ring is not just $\mathbb{Z}$. We begin by constructing a regular icosahedron $\mathcal{I} \subset \mathbb{R}^3$. To that end, let's first figure out how many vertices, edges, and faces we should expect. Euler's formula for any convex polyhedron shows $V - E + F = 2$, where V is the number of vertices, E the number of edges, and F the number of faces. Suppose that each face is a regular n -gon, and that k faces meet at each vertex. Then plugging in $E = kV/2$ and $F = kV/n$ gives

$$2 = V - E + F = V - \frac{kV}{2} + \frac{kV}{n} = V \left(1 - \frac{k}{2} + \frac{k}{n} \right) \quad (14)$$

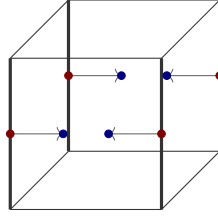
Of course $n \geq 3$ and $k \geq 3$ (since otherwise the internal angle is too large), and since the expression in parentheses above must be positive, this forces $k < 6$. We can easily solve for V and n (assuming k fixed):

$$\begin{aligned} n &= \frac{2kV}{(k-2)V + 4} \\ &< \frac{2k}{k-2} \\ V &= \frac{4n}{(2-k)n + 2k} \end{aligned}$$

Taking $k \in \{3, 4, 5\}$ and solving the above equations leads to 5 triples of integers; these correspond to the 5 Platonic solids. In particular, there's only one solution when k is maximal ($= 5$), giving $n = 3$ and $V = 12$; this will be our icosahedron, with $E = 30$ and $F = 20$.

To construct this icosahedron, we start with 12 points on the unit cube $[-1, 1]^3$, each midpoint of the cube's 12 edges. For each pair of opposite faces of the cube, we select 4 parallel edges, and then slide the corresponding 4 midpoints into the face by some distance by scaling by t , with $0 < t < 1$. The faces are chosen cyclically: for example, the four midpoints on edges parallel to the y -axis slide in the x direction, on edges parallel to the z -axis in the y direction, and on edges parallel to the x -axis in the z direction. This is what it looks like for the points that slide in the x direction:

A. Exceptional isomorphisms



We're left with 12 vertices that look like $(\pm t, 0, \pm 1)$, and cyclic permutations of these. For any fixed vertex, like $(t, 0, 1)$, we want it to have exactly 5 other vertices that are equidistant from it, since this is the number of edges that should meet at each vertex. We compute the distances (squared) from the vertex $(t, 0, 1)$ to the other 11 to get the table below.

Table A.1: Vertex distances

Distance ²	Vertices
4	$(t, 0, -1)$
$4t^2$	$(-t, 0, 1)$
$4(t^2 + 1)$	$(-t, 0, -1)$
$2(t^2 - t + 1)$	$(0, 1, \pm t); (\pm 1, -t, 0)$
$2(t^2 + t + 1)$	$(0, -1, \pm t); (\pm 1, t, 0)$

So to have 5 equidistant neighbors, one of the first 3 distances (accounting for a single vertex) must be equal to one of the last 2 distances (accounting for 4 vertices each). We can solve all 6 combinations for t , and since $0 < t < 1$ we get one possible solution: $t = \varphi - 1$, where φ is the **golden ratio**, the positive root of $s^2 = s + 1$; it will be hugely important throughout this section. We then scale everything by φ (noting $\varphi(\varphi - 1) = 1$), just to make things a bit easier to write. This leaves us with 12 vertices that are cyclic permutations of $(\pm\varphi, \pm 1, 0)$. If we connect each vertex to its 5 nearest neighbors, we get a regular icosahedron $\mathfrak{I}$ with edge length 2. We write I for the rotational symmetry group of $\mathfrak{I}$.

Consider the action of I on the 30 edges; this action is transitive (just as always), and as always the stabilizer is order 2 (the rotations with axis through the midpoint of the edge), so $|I| = 30 \cdot 2 = 60$. Now we investigate the conjugacy classes of I . Every nontrivial rotation $\sigma \in I$ must have an axis going through a vertex, an edge, or a face of $\mathfrak{I}$. If the axis of σ goes through a face, then σ is a rotation of either $\frac{2\pi}{3}$ or $\frac{4\pi}{3}$. Because every such axis will actually go through two faces, we see that σ is one of 20 elements of I (10 pairs of faces, 2 rotation angles). But a rotation of $\frac{2\pi}{3}$ around one face is (when viewed from its opposite face) a rotation about $\frac{4\pi}{3}$. Because I acts transitively on the faces of $\mathfrak{I}$, we thus see that all these 20 elements are conjugate. Similarly, if the axis of σ goes through an edge, then it is a rotation of angle π , because 2 triangles meet at an edge. And because I acts transitively on edges, all these are conjugate in I . As above, these axes go through pairs of opposite edges, so there are 15 of them. Finally, consider σ with axis through a vertex. There are 5 triangles

A. Exceptional isomorphisms

meeting at a vertex, so σ is a rotation by $k\frac{2\pi}{5}$ with $0 < k < 5$. There are $4 \cdot (12/2) = 24$ such rotations. Just as before, all such rotations with angles in $\{\frac{2\pi}{5}, \frac{8\pi}{5}\}$ are conjugate, and all those with angles in $\{\frac{4\pi}{5}, \frac{6\pi}{5}\}$ are conjugate.

But these are all the nontrivial elements of I . Indeed, we've found $20 + 15 + 24 = 59$ such elements, and I has order 60. Note that since conjugacy class size must divide the group size, the two classes of vertex rotations are not in fact the same class (since 24 doesn't divide 60). We also now know enough to show I is simple, relying on the following basic fact: a normal subgroup has order dividing the group order, is the union of conjugacy classes, and must contain the identity class. If S is any proper nonempty subset of $\{20, 15, 12, 12\}$, it can be checked easily that $1 + \sum S$ is not a divisor of 60, and thus the only possible normal subgroups of I are the one where S is empty (so the identity subgroup), and the one where S is not proper (so the whole group). Thus I is simple.

We can now establish the isomorphism with A_5 .

PROPOSITION A.3: *If G is a simple group of order 60, then $G \cong A_5$.*

Proof. Consider a Sylow 5-subgroup $P \leq G$. The number of such Sylow 5-subgroups is an element of the set $\{1, 6\}$ By Sylow's theorems. Since P is not normal in G (by simplicity), we see the number of such Sylow 5-subgroups is 6. The conjugation action of G on these Sylow subgroups gives a mapping $\rho : G \rightarrow S_6$. Because G is simple, this is an injective homomorphism, and since $[G : G \cap A_6] \leq 2$, we must have $\rho(G) \leq A_6$. Consider $\rho(G)$ acting on the 6 cosets of $\rho(G)$ in A_6 . It fixes the coset $\rho(G)$, and so acts on the remaining 5, which gives a homomorphism $\nu : \rho(G) \rightarrow S_5$. Thus $\nu\rho : G \rightarrow S_5$ is a homomorphism. As before, simplicity implies it's injective, and the image is in A_5 . Now because $|G| = 60 = |A_5|$, we see that $\nu\rho$ is actually an isomorphism. $\square$

The idea in the above proof can be used to say something nice about low-index subgroups of S_n .

PROPOSITION A.4: *Let $H \leq S_n$ be a proper non-normal subgroup with $n \geq 5$. Then $[S_n : H] \geq n$, with equality if and only if $H \cong S_{n-1}$.*

Proof. Suppose that $[S_n : H] = d < n$. Then S_n acts on the d cosets of H in S_n , and thus gives a homomorphism $\rho : S_n \rightarrow S_d$. Order considerations show the kernel must be non-trivial; because H is non-normal, the kernel must be A_n (here we use $n \geq 5$ because then A_n is the only non-trivial normal subgroup of S_n). But the kernel is contained in H , and thus $[S_n : H] \leq 2$, contradicting our hypotheses. Thus $d \geq n$.

Of course if $H \cong S_{n-1}$ then $d = n$. Conversely, assume $d = n$. Then we consider H acting on its n cosets, where it fixes the trivial coset H . We thus get a homomorphism $\nu : H \rightarrow S_{n-1}$. Note that $\ker(\nu) = \ker(\rho)$, which (arguing as above) must be trivial. So ν is an injective homomorphism, and since $|H| = |S_{n-1}|$, we see it is an isomorphism. $\square$

A.6. Characters and coordinates

We will digress a bit to use the action of I on $\mathcal{I}$ described above to compute the corresponding character of I (viewing $I \leq SO(3, \mathbb{R})$). Recall that we saw I had 5 conjugacy classes: the identity class represented by 1; the class of rotations fixing a face, represented by an element we'll call τ ; the class of rotations fixing an edge, represented by an element we'll call ϵ ; and two classes of rotations fixing a vertex, represented by elements we'll call v_1 and v_2 .

For any rotation, the fixed axis can be taken as the first element of a basis for $\mathbb{R}^3$, and the corresponding matrix (which has the same trace as the original) will look like (see Equation (11))

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix} \quad (15)$$

where θ is the angle of rotation. [There is some subtlety here regarding orientations, corresponding to how we measure the angle (clockwise or counter-clockwise); although it won't matter in the end, we'll fix to our usual rule.] So we see that the character for that rotation is just $1 + 2\cos(\theta)$. We can then construct the character for the 5 conjugacy classes of I as shown:

Table A.2: Character of rotation group I

Class	Angle	Character
1	0	3
τ	$\frac{2\pi}{3}$	0
ϵ	π	-1
v_1	$\frac{2\pi}{5}$	φ
v_2	$\frac{4\pi}{5}$	$1 - \varphi$

Here φ is again the golden ratio $\frac{1}{2}(1 + \sqrt{5})$. Since $\cos(\frac{2\pi}{5})$ is not as obvious as the other two, we'll show how to find its value next. But first notice that this representation is **irreducible**. That should be clear from the fact that I can't fix any line or plane in $\mathbb{R}^3$ (as a group of rotations without a common axis), but it can be confirmed by computing the norm of the above character. Note that if we used a different orientation, the angles would change from θ to $-\theta$, but that wouldn't change their cosines, so the character values would be exactly the same.

To quickly compute $\cos(\frac{2\pi}{5})$, note that $2\cos(\frac{2\pi}{5})$ is equal to $\zeta + \zeta^{-1}$, where $\zeta = e^{2\pi/5}$. If we square $x = \zeta + \zeta^{-1}$, we see that $x^2 = \zeta^2 + \zeta^{-2} + 2$. This shows that

$$x^2 + x = (\zeta + \zeta^2 + \zeta^{-2} + \zeta^{-1} + 1) + 1 = 1$$

A. Exceptional isomorphisms

since the sum of all 5th roots of unity is 0. Thus $2 \cos(\frac{2\pi}{5})$ is a root of $x^2 + x - 1$, and since it's positive, it must be $\varphi - 1$. The value of $2 \cos(\frac{4\pi}{5})$ follows from the same reasoning, only it's the negative root of this polynomial (namely $-\varphi$).

Before getting back to the next steps for I (reducing the coordinate ring), we might as well compute the characters for the cube group C and tetrahedron group T . As above, τ is a rotation fixing a face, ϵ a rotation fixing an edge, and ν a rotation fixing a vertex. These are also irreducible representations.

Table A.3: Character of rotation group T

Class	Angle	Character
1	0	3
τ	$\frac{2\pi}{3}$	0
τ^2	$\frac{4\pi}{3}$	0
ϵ	π	-1

Table A.4: Character of rotation group C

Class	Angle	Character
1	0	3
τ	$\frac{\pi}{2}$	1
τ^2	π	-1
ϵ	π	-1
ν	$\frac{2\pi}{3}$	0

OK, back to our plan of action: we now reduce the coordinate ring of I modulo some well-chosen maximal ideals to establish some exceptional isomorphisms. Like in the tetrahedral case, we will choose a basis of $\mathbb{R}^3$ from vertices of $\mathfrak{I}$, namely

$$\mathbf{c} = (\varphi, 1, 0) \quad \mathbf{b} = (1, 0, \varphi) \quad \mathbf{a} = (0, \varphi, 1)$$

Note that $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ span a triangle of our icosahedron since they are all distance 2 from each other. So $\{\pm\mathbf{a}, \pm\mathbf{b}, \pm\mathbf{c}\}$ are 6 of our 12 vertices, and the rest come from negation, cyclic permutation, and the identity $(\varphi, -1, 0) = -\mathbf{a} + (\varphi - 1)(\mathbf{b} + \mathbf{c})$. In this basis, an element $\sigma \in I$ will move the basis elements to other vertices of $\mathfrak{I}$, and so as just seen, the matrix entries for σ will consist of elements from the ring $\mathbb{Z}[\varphi]$. This is true for any element of I , so we see that the matrices of I actually have values in the coordinate ring $\mathbb{Z}[\varphi] \subset \mathbb{R}$. This is different than the other cases we've done, but the procedure for reducing to finite fields will be mostly the same. The key is that $\mathbb{Z}[\varphi]$ is nothing more than $\mathbb{Z}[t]/\langle t^2 - t - 1 \rangle$.

Before we begin though, an important point: the basis $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ is *not* orthogonal, so it does not preserve the usual bilinear form $x^2 + y^2 + z^2$. Instead, if we let P be the change of basis matrix from the "standard" basis $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ to $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ -coordinates, then our "orthogonal" elements are those preserving the bilinear form $v^T(P^T P)v$. Direct calculation shows P is $\varphi O + 2I$, where O is the matrix with every entry 1, and I is the identity matrix. This shows the bilinear form corresponding to our chosen basis is

$$2(x^2 + y^2 + z^2) + \varphi(x + y + z)^2 \tag{16}$$

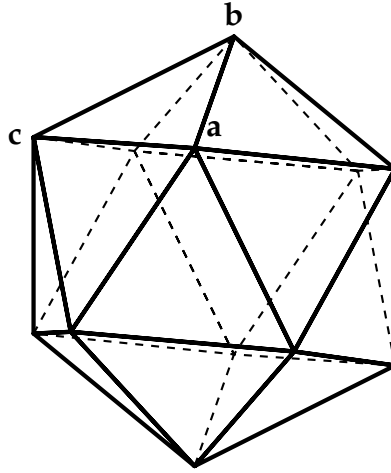
For example, let $J = \langle 2 \rangle$ be the ideal of $\mathbb{Z}[\varphi]$ generated by the element 2. We have

$$\mathbb{Z}[\varphi]/J \cong \mathbb{Z}[t]/\langle 2, t^2 - t - 1 \rangle \cong \mathbb{F}_2[t]/\langle t^2 - t - 1 \rangle \cong \mathbb{F}_4$$

A. Exceptional isomorphisms

Where the last isomorphism comes from $t^2 - t - 1$ being irreducible over $\mathbb{F}_2$ (since it has no roots). Thus if we reduce all matrix entries modulo J , we get a homomorphism from $I \leq SO(3, \mathbb{R})$ to $\hat{I} \leq SL(3, \mathbb{F}_4)$. Note that elements of $SO(3, \mathbb{R})$ are precisely those with determinant 1 and fixing the bilinear form in Equation (16), so $\hat{I}$ will fix the bilinear form $(x + y + z)^2$ since we're in characteristic 2. In particular, $\hat{I}$ fixes the 2-dimensional plane $L := \{(x, y, z) \mid x + y + z = 0\}$. It thus restricts to a subgroup of $SL(2, \mathbb{F}_4)$, and so we get a map from I to $\hat{I}$ to $SL(2, \mathbb{F}_4)$. We show below that $\hat{I}$ acts non-trivially. Since we showed I is simple, this is an injective homomorphism; since $|I| = 60 = |SL(2, \mathbb{F}_4)|$, we get an isomorphism $A_5 \cong I \cong SL(2, 4)$.

To see $\hat{I}$ must act non-trivially, note that L is spanned by the images of $\{\mathbf{a} + \mathbf{b}, \mathbf{a} + \mathbf{c}\}$. But there is an element $\sigma \in I$ that fixes $\mathbf{a}$ and rotates $\mathbf{b}$ to $\mathbf{c}$, so $\hat{\sigma} \in \hat{I}$ is not acting trivially (it sends $\mathbf{a} + \mathbf{b}$ to $\mathbf{a} + \mathbf{c}$). This shows $\hat{\sigma}$ is not in the kernel of the map to $SL(2, \mathbb{F}_4)$. The existence of the element σ can be verified directly pictorially (see picture below).



Note that $\sqrt{5} = 2\varphi - 1 \in \mathbb{Z}[\varphi]$ with $5 = \sqrt{5}^2$, and if we let $K = \langle \sqrt{5} \rangle$ be an ideal of $\mathbb{Z}[\varphi]$, we similarly get

$$\mathbb{Z}[\varphi]/K \cong \mathbb{Z}[t]/\langle 5, t^2 - t - 1, 2t - 1 \rangle \cong \mathbb{F}_5[t]/\langle t^2 - t - 1, 2t - 1 \rangle \cong \mathbb{F}_5$$

Where the last isomorphism follows because $t = 3 \in \mathbb{F}_5$ is already a root of those two polynomials. Just as before, this gives a homomorphism from I to $\hat{I} \leq SL(3, \mathbb{F}_5)$, where the image fixes the bilinear form $xy + xz + yz$ (this follows by replacing φ with 3 and reducing modulo 5 in Equation (16)). If we projectivize the entire 3-space (to get a projective plane), we get $\hat{I}_{\mathbb{P}}$ acting on the projective subspace $V_{\mathbb{P}}$ defined by $xy + xz + yz = 0$, which is isomorphic to $\mathbb{P}_5$.

Thus we similarly get an induced homomorphism from I to $\hat{I}_{\mathbb{P}} \leq PGL(2, \mathbb{F}_5)$; we don't know that I lands in $PSL(2, \mathbb{F}_5)$, because determinants are not necessarily preserved when we projectivize a conic like this. In our case, however, the determinant is preserved. To see that, first consider the element $\sigma \in I$ from above, that fixes $\mathbf{a}$ and $\sigma(\mathbf{b}) = \mathbf{c}$. In $V_{\mathbb{P}}$ then, using

the images of $\mathbf{a}$ and $\mathbf{b}$ as a basis, $\hat{\sigma}_{\mathbb{P}} \in \hat{I}_{\mathbb{P}}$ acts as the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. This has determinant 1, and since $\hat{I}_{\mathbb{P}}$ is simple, it is generated by $\hat{\sigma}_{\mathbb{P}}$ and its conjugates, so that all elements of $\hat{I}_{\mathbb{P}}$ have determinant 1 as a subgroup of $PGL(2, 5)$. Thus $\hat{I}_{\mathbb{P}}$ ends up in $PSL(2, \mathbb{F}_5)$. [There is a subtlety here that determinant is only defined up to squares in $PGL(2, \mathbb{F}_5)$, but the argument about conjugates and products having determinant 1 (modulo squares) is still valid.]

The action of $\hat{I}_{\mathbb{P}}$ is again non-trivial (shown next), I is still simple, and once again order considerations give another proof that $A_5 \cong I \cong PSL(2, 5)$. It's actually a little easier to show $\hat{I}_{\mathbb{P}}$ is acting non-trivially this time, because $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ end up in $V_{\mathbb{P}}$, as can be directly checked, and of course any non-trivial element of $\hat{I}_{\mathbb{P}}$ acts non-trivially on this basis.

A.7. Complexifying

We now want to make use of a very unique homomorphism from $SU(2, \mathbb{C})$ to $SO(3, \mathbb{R})$. In the world of Lie groups, this homomorphism comes from the two-sheeted universal covering $S^3 \rightarrow \mathbb{RP}^3$, but we'll look at it algebraically: $PSU(2, \mathbb{C}) \cong SO(3, \mathbb{R})$. To understand this isomorphism, one must know that elements of $SU(2, \mathbb{C})$ are classified by complex number pairs (z, w) with $z^2 + w^2 = 1$. And this naturally leads to a quaternionic representation $(z, w) \mapsto z + wj$, so that $SU(2, \mathbb{C})$ is nothing more than the unit quaternions; that is, the set $\{q \in \mathbb{H} \mid \|q\| = 1\}$. To get a rotation in $SO(3, \mathbb{R})$ from such a quaternion, we can look at how $q := z + wj$ acts (via conjugation!) on the 3-space spanned by $\{i, j, k\}$ in $\mathbb{H}$. We won't go through the (slightly messy) formulas here, but will present the very nice payoff: the unit quaternion $q = z + wj := a + bi + cj + dk$ gives rise to a rotation around an axis through the origin and (b, c, d) , with angle θ given by $\cos(\theta/2) = a$ (we still use the usual "clockwise" rule for orientation). Since both q and $-q$ induce the same conjugation, our map descends to $PSU(2, \mathbb{C}) \rightarrow SO(3, \mathbb{R})$, and this is an isomorphism. We haven't shown all the details (like the proof this is an actual homomorphism!), but what's missing isn't particularly hard.

Since we have $I \leq SO(3, \mathbb{R})$, there must be a group $D \leq SU(2, \mathbb{C})$ that maps to I via the above homomorphism. Since we're quotienting by the central subgroup Z in $SU(2, \mathbb{C})$, where $Z := \{\pm 1\} \triangleleft SU(2, \mathbb{C})$ is of order 2, we see that $|D| = |Z| \cdot |I| = 120$. We'll give a nice description of D a bit later. But first we need to see what the matrix entries in elements of D look like, because we're going to mimic the work of the previous sections and look at finite coordinate ring quotients. Based on the angles we rotate with elements in I , we can use the above description of quaternions over a given rotation (and cosine half-angle formulas) to see what our " a " values ($= \Re(z)$) look like in D . In particular, the angles we consider can be read from [Table A.2](#), and we thus have:

A. Exceptional isomorphisms

Table A.5: Angle cosines

θ	π	$\frac{2\pi}{3}$	$\frac{2\pi}{5}$	$\frac{4\pi}{5}$
$\cos(\theta/2)$	0	$\frac{1}{2}$	$\frac{\varphi}{2}$	$\frac{\varphi-1}{2}$

Now fix a vertex in $\mathcal{I}$, say (r, s, t) , where $r, s, t \in \{0, \pm 1, \pm \varphi\}$. We also know this vertex has norm $\sqrt{\varphi^2 + 1^2 + 0^2} = \sqrt{\varphi + 2}$. By the cosine values above, we know from $\cos^2 + \sin^2 = 1$ that

$$\sin\left(\frac{2\pi}{5}\right) = \frac{1}{2}\sqrt{\varphi + 2}$$

Thus a rotation by angle $\frac{4\pi}{5}$ around the above vertex can be expressed as a unit quaternion as $\pm \frac{1}{2}((\varphi - 1) + ri + sj + tk)$. In terms of complex pairs, we have $\pm \frac{1}{2}(\varphi - 1 + ri, s + ti)$, and both values are in the ring $\mathbb{Z}[\varphi, i, \frac{1}{2}]$.

But every element of I is a product of such rotations around vertices: these rotations form a full conjugacy class in I , so they generate a normal subgroup of I , hence by simplicity generate all of I . Since elements of $Z \leq D$ all have integer coefficients, this shows that for every complex pair (z, w) for the unit quaternions in D , both z and w live in $R := \mathbb{Z}[\varphi, i, \frac{1}{2}]$. Just as we did in the last section, we then consider $D \leq SL(2, R)$ (we won't make use of the fact elements of D are unitary, only that they have determinant 1). We'll also think of R as $\mathbb{Z}[t, u, v] / \langle t^2 - t - 1, u^2 + 1, 2v - 1 \rangle$.

Let's once again reduce by an ideal $K := \langle \sqrt{5} \rangle \leq R$. We have

$$\begin{aligned}
 R/K &\cong \mathbb{Z}[t, u, v] / \langle 5, t^2 - t - 1, 2t - 1, u^2 + 1, 2v - 1 \rangle \\
 &\cong \mathbb{F}_5[t, u, v] / \langle t^2 - t - 1, 2t - 1, u^2 + 1, 2v - 1 \rangle \\
 &\cong \mathbb{F}_5[t, u] / \langle t^2 - t - 1, 2t - 1, u^2 + 1 \rangle & (v = 3) \\
 &\cong \mathbb{F}_5[u] / \langle u^2 + 1 \rangle & (t = 3) \\
 &\cong \frac{\mathbb{F}_5[u]}{\langle u + 2 \rangle} \times \frac{\mathbb{F}_5[u]}{\langle u + 3 \rangle} \\
 &\cong \mathbb{F}_5 \times \mathbb{F}_5
 \end{aligned}$$

This isn't a field because K is not maximal (prime)! Indeed, $(i + 2)(i + 3) = 5(i + 1) \in \langle \sqrt{5} \rangle$, but neither factor is. If we redefine $K = \langle \sqrt{5}, i + 2 \rangle$, then we will in fact get $R/K \cong \mathbb{F}_5$. So we get the image $\hat{D} \leq SL(2, \mathbb{F}_5)$. Note that the center $Z \leq D \leq SU(2, \mathbb{C})$ maps onto the center of $SL(2, \mathbb{F}_5)$ under this reduction. What could the kernel $N \triangleleft D$ of this reduction be? If $Z \leq N$, then N maps to a normal subgroup of $\hat{I}$ under the map $SL(2, \mathbb{F}_5) \rightarrow PSL(2, \mathbb{F}_5)$, and $\hat{I}$ is simple, so $N = Z$ or $N = D$. The same reasoning applied to NZ shows either $N = D$ or $N \leq Z$. Since we saw that $Z \cap N = \{1\}$, it must be that $N = 1$. Since $|D| = |SL(2, \mathbb{F}_5)|$, we have then shown $D \cong \hat{D} \cong SL(2, 5)$, and given another proof that

$$A_5 \cong I \cong D/Z \cong SL(2, 5)/Z \cong PSL(2, 5)$$

A. Exceptional isomorphisms

Reducing by the ideal $\langle 2 \rangle \leq R$ won't do anything, because 2 is invertible in R , so we get the trivial ring. Instead, we look at $J = \langle 3 \rangle$. Just as before, we have

$$\begin{aligned}
 R/J &\cong \mathbb{Z}[t, u, v] / \langle 3, t^2 - t - 1, u^2 + 1, 2v - 1 \rangle \\
 &\cong \mathbb{F}_3[t, u, v] / \langle t^2 - t - 1, u^2 + 1, 2v - 1 \rangle \\
 &\cong \mathbb{F}_3[t, u] / \langle t^2 - t - 1, u^2 + 1 \rangle & (v = 2) \\
 &\cong \mathbb{F}_9[t] / \langle t^2 - t - 1 \rangle & (u = i) \\
 &\cong \frac{\mathbb{F}_9[t]}{\langle t + 1 + i \rangle} \times \frac{\mathbb{F}_9[t]}{\langle t + 1 - i \rangle} \\
 &\cong \mathbb{F}_9 \times \mathbb{F}_9
 \end{aligned}$$

Again our ideal J is not maximal, and we see the reason is $(i + i\sqrt{5})(1 - i\sqrt{5}) = 6 \in \langle 3 \rangle$. If we instead redefine $J = \langle 3, 1 + i\sqrt{5} \rangle$, then we will get $R/J \cong \mathbb{F}_9$. Once again, we get an image of D (still called $\hat{D}$) in $SL(2, \mathbb{F}_9)$. As in the previous case, Z is mapped onto the center of $SL(2, \mathbb{F}_9)$, so $D \cong \hat{D}$ and this gives an embedding of D/Z into $PSL(2, \mathbb{F}_9)$. Order considerations show this image of $D/Z \cong I$ has index 6 in $PSL(2, \mathbb{F}_9)$; let's call the image $\hat{I} \leq PSL(2, 9)$. The action of $PSL(2, 9)$ on the 6 cosets of $\hat{I}$ gives a homomorphism from $PSL(2, \mathbb{F}_9)$ to S_6 . The kernel of this action is a normal subgroup contained in the simple subgroup $\hat{I}$, and thus the kernel is either $\{1\}$ or $\hat{I}$. To see it can't be $\hat{I}$, we show below that $SL(2, \mathbb{F}_9)$ (and hence $PSL(2, \mathbb{F}_9)$) is perfect; but if $\hat{I} \triangleleft PSL(2, \mathbb{F}_9)$, we would have an order 6 quotient $PSL(2, \mathbb{F}_9)/\hat{I}$, and it's easy to see that can't be perfect. Thus our action is faithful, and the kernel is trivial. So the isomorphic image of $PSL(2, \mathbb{F}_9)$ in S_6 has order 360, and thus is index 2 (hence normal) in S_6 . This gives us our final desired isomorphism: $A_6 \cong PSL(2, 9)$.

For completeness, we prove that $SL(2, \mathbb{F}_q)$ (and more generally most $SL(2, \mathbb{F}_q)$) are perfect. Similar arguments to those given in the proof can also be used to show that $SL(n, \mathbb{F}_q)$ is perfect whenever $n > 2$. Using something known as **Iwasawa's criterion**, these same arguments will show that $PSL(n, \mathbb{F}_q)$ is simple whenever $SL(n, \mathbb{F}_q)$ is perfect (so whenever $n > 2$ or $q > 3$).

PROPOSITION A.5: *If $q > 3$ is a prime power, then $SL(2, \mathbb{F}_q)$ is perfect.*

Proof. We prove this by showing every element of $SL(2, \mathbb{F}_q)$ is a product of commutators. The name of the game is direct computation.

First fix $\delta \in \mathbb{F}_q \setminus \{0, \pm 1\}$ (this is the only place we use $q > 3$). Direct computation then shows that for any $\alpha \in \mathbb{F}_q$, if we set $\gamma = \alpha(1 - \delta^2)^{-1}$, we have

$$\begin{aligned}
 \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} \delta^{-1} & 0 \\ 0 & \delta \end{pmatrix}^{-1} \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} \delta^{-1} & 0 \\ 0 & \delta \end{pmatrix} \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \\
 \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -\gamma & 1 \end{pmatrix}^{-1} \begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ -\gamma & 1 \end{pmatrix} \begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix}
 \end{aligned}$$

So these elements (commonly called **transvections**) are commutators. Now take an arbitrary element of $SL(2, \mathbb{F}_q)$ which has a 0 in the lower left corner. Direct computation then gives

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & a(1+b) - 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & d-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}$$

so that this element is a product of commutators. Note here we've used that $ad = 1$. Now for any element of $SL(2, \mathbb{F}_q)$ whose lower-left corner is not zero, we have

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 - ac^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \hat{a} & \hat{b} \\ 0 & \hat{d} \end{pmatrix}$$

where the $\hat{a}, \hat{b}, \hat{d}$ are inconsequential; all that matters is the right side is a product of commutators by the previous step. This shows all elements of $SL(2, \mathbb{F}_q)$ are products of commutators, and it's a perfect group. $\square$

A.8. Projective actions

In this last section, we establish most of the exceptional isomorphisms directly from projective group actions on projective lines. We also establish some basic facts about projective groups and spaces that are used throughout this appendix.

Let $\mathbb{P}_q^1$ be the projective line over a field $\mathbb{F}_q$ with q elements (so q is a prime power). This line has $q + 1$ points on it: all the points $[\alpha : 1]$ for $\alpha \in \mathbb{F}_q$, and the "point at infinity" $[1 : 0]$. The **projective linear group** $PGL(2, \mathbb{F}_q)$ acts on this projective line, as we now describe. First, we start with an action by the general linear group $GL(2, \mathbb{F}_q)$, where (in matrix terms) our action is just

$$[x : y] \begin{pmatrix} a & b \\ c & d \end{pmatrix} = [ax + cy : bx + dy] \quad (17)$$

Let us write M for the matrix above. By the definition of projective space, if $N = \lambda M$ is a scalar multiple of M (here $\lambda \in \mathbb{F}_q$), then we see that N acts the exact same way M does. Thus if S is the set of scalar matrices in $GL(2, \mathbb{F}_q)$, we see that our action descends to one of $GL(2, \mathbb{F}_q)/S$. We do have that S is in fact normal, since S is contained in the center (every scalar matrix is central).

In fact, S is the full center of $GL(2, \mathbb{F}_q)$. To see this, suppose the matrix M is in the center. Conjugation by well-chosen matrices shows

$$\begin{aligned} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a - c & a - c + b - d \\ c & d \end{pmatrix} \\ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} &= \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \end{aligned}$$

A. Exceptional isomorphisms

The fact both matrices on the right need to be equal to M shows that $a = d$, and $b = c = 0$, so that M is scalar. So our action on $\mathbb{P}_q^1$ is actually via $GL(2, \mathbb{F}_q)/Z(GL(2, \mathbb{F}_q)) := PGL(2, \mathbb{F}_q)$. An important point about the above conjugations is that the matrices we used are actually in $SL(2, \mathbb{F}_q)$, so $S \cap SL(2, \mathbb{F}_q) = Z(SL(2, \mathbb{F}_q))$ and we have a restricted action of $PSL(2, \mathbb{F}_q)$ on $\mathbb{P}_q^1$.

So we have an action of $PGL(2, \mathbb{F}_q)$ on $\mathbb{P}_q^1$, which has $q + 1$ points. We can say a bit more about this action. First, it is clearly transitive: we have

$$[1 : 0] \begin{pmatrix} \alpha & 1 \\ 0 & 1 \end{pmatrix} = [\alpha : 1]$$

The point stabilizer of $[1 : 0]$ is all elements of $PGL(2, \mathbb{F}_q)$ with the upper-right corner entry equal to 0. In particular,

$$[0 : 1] \begin{pmatrix} a & 0 \\ \gamma\alpha & \gamma \end{pmatrix} = [\gamma\alpha : \gamma] = [\alpha : 1]$$

for $a \neq 0$ and any $\gamma \neq 0 \in \mathbb{F}_q$, while the matrix stabilizes $[1 : 0]$. This shows $PGL(2, \mathbb{F}_q)$ is 2-transitive on $\mathbb{P}_q^1$ (and choosing $a = \gamma = 1$ shows $PSL(2, \mathbb{F}_q)$ is 2-transitive as well). By choosing $a = \gamma(\beta - \alpha)$ for $\beta \neq \alpha$, we see that the matrix takes $[1 : 1]$ to $[\beta : 1]$, and so $PGL(2, \mathbb{F}_q)$ is actually 3-transitive, but we won't need this fact.

Do any elements of $PGL(2, \mathbb{F}_q)$ act trivially? From the above, an element stabilizing $[1 : 0]$ and $[0 : 1]$ is diagonal. If the diagonal entries are a and d , then it takes $[1 : 1]$ to $[a : d]$, so to act trivially it must be $a = d$. That is, it is represented by a scalar matrix, which becomes the identity in $PGL(2, \mathbb{F}_q)$. So the action is in fact faithful (this also shows $PGL(2, \mathbb{F}_q)$ acts *sharply* 3-transitively).

The orbit-stabilizer theorem gives the order of $PGL(2, \mathbb{F}_q)$ and $PSL(2, \mathbb{F}_q)$. From the above, the stabilizer of $[1 : 0]$ is just those elements with 0 in the upper-right corner. In $PGL(2, \mathbb{F}_q)$, there are $q(q - 1)$ such elements: there are q choices for the lower-left, and $q - 1$ for each of the diagonal entries. However, the scalars (of order $q - 1$) act on these, so the actual number of such elements in the projective group is $q(q - 1)^2 / (q - 1) = q(q - 1)$. In $PSL(2, \mathbb{F}_q)$, we can only pick one diagonal entry, so there are $q(q - 1)/k$ such elements, where $k = |Z(SL(2, \mathbb{F}_q))|$. Taking determinants of scalar matrices in $SL(2, \mathbb{F}_q)$, we see that k is the number of solutions to $x^2 = 1$ in $\mathbb{F}_q$. So $k = 1$ when the characteristic of $\mathbb{F}_q$ is 2, and $k = 2$ otherwise. Since $\mathbb{P}_q^1$ has $q + 1$ elements, we see

$$\begin{aligned} |PGL(2, \mathbb{F}_q)| &= q(q - 1)(q + 1) \\ |PSL(2, \mathbb{F}_q)| &= q(q - 1)(q + 1)/k \end{aligned} \quad k = \begin{cases} 2 & q \text{ odd} \\ 1 & q \text{ even} \end{cases}$$

In particular, when q is a power of 2, we see that $PSL(2, \mathbb{F}_q)$ and $PGL(2, \mathbb{F}_q)$ have the same order, and are thus isomorphic. (Note in this case we actually have $PSL(2, \mathbb{F}_q) \cong SL(2, \mathbb{F}_q)$ since $-1 = 1 \pmod{2}$).

A. Exceptional isomorphisms

The action of $PGL(2, \mathbb{F}_3)$ on $\mathbb{P}_3^1$ is an action on $3 + 1 = 4$ points, and thus gives a homomorphism into S_4 . Since the action is faithful, we get an embedding of $PGL(2, \mathbb{F}_3)$ into S_4 . Order considerations then show $PGL(2, 3) \cong S_4$, as shown earlier. Since $PSL(2, \mathbb{F}_3) \leq PGL(2, \mathbb{F}_3)$ has order 12, we see that also $A_4 \cong PSL(2, 3)$. Similarly, the action of $PGL(2, \mathbb{F}_4)$ on $\mathbb{P}_4^1$ is an action on $4 + 1 = 5$ points, and thus gives an injective homomorphism into S_5 . By the above, $PGL(2, \mathbb{F}_4)$ has order 60, and thus the image of this embedding is A_5 . We thus see that $A_5 \cong PGL(2, 4)$ (also $PSL(2, 4)$ and $SL(2, 4)$). We also have an action of $PGL(2, \mathbb{F}_5)$ on $5 + 1 = 6$ points, and an embedding into S_6 . From the above, $|PGL(2, \mathbb{F}_5)| = 120$, and thus the image of this embedding is a subgroup of index 6 in S_6 . By [Proposition A.4](#), we see $S_5 \cong PGL(2, 5)$. Since $PSL(2, \mathbb{F}_5)$ has order 60 and is a subgroup of $PGL(2, \mathbb{F}_5)$, we get another isomorphism $A_5 \cong PSL(2, 5)$.

B. Structure of groups of Lie type

In this appendix we investigate the structure of $SL(2, \mathbb{F}_q)$, enough to be able to identify the conjugacy classes. We also do the same work for $PSL(2, \mathbb{F}_q)$. We first identify a few important subgroups of $SL(2, \mathbb{F}_q)$, and establish some important group-theoretic properties. We then discuss split and non-split tori, before focusing on the conjugacy classes of $SL(2, \mathbb{F}_q)$. We will see that the conjugacy classes of $PSL(2, \mathbb{F}_q)$ are fairly easy to find once we know those of $SL(2, \mathbb{F}_q)$. One thing of note here is that we do almost all of our investigation in a basis-free setting; this makes it clear that the subgroups/properties are intrinsic to the groups. However, it does make some things hard to see concretely, so we will discuss particularly nice bases later in the appendix.

B.1. Stabilizer subgroups

It's easy to see that $|GL(2, \mathbb{F}_q)| = (q^2 - 1)(q^2 - q)$, since that is the number of ways to choose a basis of F_q^2 : first pick a non-zero vector, then pick another one not on the same line. Since $\det : GL(2, \mathbb{F}_q) \rightarrow \mathbb{F}_q^*$ is surjective, we see that $\ker(\det) = SL(2, \mathbb{F}_q)$ must have order $q(q - 1)(q + 1)$. We will treat the vector space that $G := SL(2, \mathbb{F}_q)$ acts on as $V := \mathbb{F}_{q^2}/\mathbb{F}_q$. If $x \in V$ is non-zero, and $u \in G$ fixes x (so that $xu = x$), then of course u fixes every element on the "line" $\{ax \mid a \in \mathbb{F}_q\}$. If $y \in V$ is any other vector not on that line, then we can write $yu = ax + by$ with $a, b \in \mathbb{F}_q$. Since $\det(u) = 1$ we must have $b = 1$, so that $yu = ax + y$. Since there are q choices for $a \in \mathbb{F}_q$, and all of them are possible, we see that the stabilizer $U \leq G$ of $x \in V$ has order q . Since $V \setminus \{0\}$ has order $q^2 - 1 = [G : U]$, we also see G acts transitively on V . This implies G acts transitively on $\mathbb{P}^1(V)$ as well; in fact, G acts 2-transitively on $\mathbb{P}^1(V)$. To see that, note that from our description of U above, we see that it fixes $[x] \in \mathbb{P}^1(V)$, but only the $a = 0$ case fixes $[y]$. Since $|U| = |\mathbb{P}^1(V) \setminus \{[x]\}|$, we have U acting transitively (even regularly) on $\mathbb{P}^1(V) \setminus \{[x]\}$, and so G does act 2-transitively.

If we let $B \leq G$ be the stabilizer of $[x] \in \mathbb{P}^1(V)$, then since G is 2-transitive we know that B is a maximal subgroup of G , and that for any $g \in G \setminus B$, we can write

$$G = B \bigsqcup BgB \tag{18}$$

This double coset decomposition is called the **Bruhat decomposition**, and B is called a **Borel subgroup**. We have $U \leq B$ of course. We let $T \leq B$ be the subgroup that fixes both

B. Structure of groups of Lie type

$[x]$ and $[y]$; note $|T| = q - 1$ by the orbit-stabilizer theorem. Since V is 2-dimensional, any element $z \in G$ fixing 3 or more points in $\mathbb{P}^1(V)$ must actually fix every line in V , and hence be a scalar transformation: multiplication by an element $a \in \mathbb{F}_q$. But $\det(z) = 1$ implies $a^2 = 1$, so that $z = \pm 1$ (treating $1 \in G$ as the identity transformation). Obviously $z \in Z(G)$ since all elements of G are $\mathbb{F}_q$ -linear. Conversely, an element in $Z(G)$ must fix every line (and hence be a scalar) in order to commute with every conjugate of U . Here we see our first distinction based on the parity of q : $Z(G)$ is trivial when q is even, but $|Z(G)| = 2$ when q is odd.

Let $b \in B$ and $u \in U$, and note that

$$x(b^{-1}ub) = xa^{-1}(ub) = (xa^{-1})b = x$$

Here $xb = ax$ for $a \in \mathbb{F}_q$ since b stabilizes $[x]$, and of course u fixes x . Thus $u^b \in U$, so that $U \triangleleft B$. Because $[B : T] = q = |U|$ and $U \cap T = \{1\}$ (U acts regularly), we then have that $B = UT$, a semidirect product. Also because $U \leq B$ is a regular normal subgroup and $T \leq B$ the point stabilizer of $[y]$, we know that T acts on U (via conjugation) the same way it acts on $\mathbb{P}^1(V) \setminus \{[x]\}$, with $[y]$ corresponding to $1 \in U$. But the only elements of T stabilizing a third point of $\mathbb{P}^1(V)$ are $Z(G)$ as noted above, so that T has an orbit of size $q - 1$ on U^* when q is even, and of size $\frac{1}{2}(q - 1)$ when q is odd. Thus when q is even, U^* is one conjugacy class under T , and when q is odd, U^* is two conjugacy classes of equal sizes under T . Since $|U| = q$ we know U is a p -group. If $u \in \Phi(U)$ is non-trivial, then $u^T \subset \Phi(U)$, so that

$$|\Phi(U)| \geq \frac{q}{2} + 1 > \frac{|U|}{2}$$

This implies $\Phi(U) = U$, which is impossible, and the contradiction shows $u \in \Phi(U)$ doesn't exist. Thus $\Phi(U) = \{1\}$ and U is an elementary Abelian p -group of order q , and $U \cong \mathbb{F}_q^+$, the additive group. In fact, U is a Sylow p -subgroup of G , B is its normalizer, and T is one of the complements to U in $N_G(U)$. Thus G acts on $\mathbb{P}^1(V)$ the same way it acts on its Sylow p -subgroups.

If $\mathbb{F}_q^* = \langle a \rangle$, then there is a linear transformation that sends $x \mapsto ax$ and $y \mapsto a^{-1}y$. This is an element of G of order $|\mathbb{F}_q^*| = q - 1$, and it fixes both $[x]$ and $[y]$, so it lives in T . Since $|T| = q - 1$, this shows T is cyclic, and $T \cong \mathbb{F}_q^*$. So $B \cong \mathbb{F}_q^+ \rtimes \mathbb{F}_q^*$ is the affine linear group over $\mathbb{F}_q$ (this is especially clear, as will be seen later, when we choose x and y to give a particularly nice basis). Now let $k \in G$ be an element that swaps $[x]$ and $[y]$, which exists because G is 2-transitive on $\mathbb{P}^1(V)$. Then $T^k = T$ of course, and $k^2 \in T$. Note that if $g \in G$ normalized T , then we would have

$$\{[x], [y]\}g = \{[x], [y]\}$$

so that either $g \in T$ or $k^{-1}g \in T$, and hence $N_G(T) = T \cup kT = \langle T, k \rangle$. How does k act on T ? Suppose $yk = cx$, as well as $xt = ax$ and $yt = by$ for $a, b, c \in \mathbb{F}_q$. Then

$$xt^k t = x(k^{-1}tkt) = c^{-1}y(tkt) = bc^{-1}y(kt) = bx(t) = abx$$

B. Structure of groups of Lie type

From $\det(t) = ab = 1$, we then see that $t^k t \in U$. But also $t^k t \in T$, and hence $t^k t = 1$, implying $t^k = t^{-1}$. Note that $k^2 \in T$ is centralized by k , so is its own inverse, implying $k^2 \in Z(G)$. We will see later that when q is odd, we have that k is contained in a torus, so that $k^2 = -1$ in this case (since $k^2 = 1$ would imply incorrectly that $k = -1$ is already central).

Because k doesn't stabilize $[x]$, we have $k \notin B$, and hence by the Bruhat decomposition (eq. (18)) we know $G = B \sqcup BkB$. In fact, we will write this as $B \sqcup Bk^{-1}B$ for notational convenience later on. If $u \in U^*$, then u^k fixes y , so $u^k \notin B$. Given that $B = UT = TU$ this means we can write

$$u^k = (v^{-1}s)k^{-1}(tw^{-1}) \quad (19)$$

where again we've used the Bruhat decomposition, and also used inverses for later notational convenience. Here $v, w \in U$ and $s, t \in T$. This representation isn't unique; it is only unique up to splicing in an element from $B \cap kBk^{-1}$, but this is T (since kBk^{-1} is the stabilizer of $[x]k^{-1} = [y]$). For any $r \in T$, we can rewrite eq. (19) as $u^k = (v^{-1}[sr^k])k^{-1}([r^{-1}t]w^{-1})$, and all $|T|$ choices for r give the $|T|$ distinct ways of writing u^k as an element of this double coset. In particular, choosing $r = t$ and re-arranging gives

$$vu^k w = sk^{-1} \quad (20)$$

and in this case, v , w , and s are uniquely determined by u^k . This means that the map from U^* to T , given by sending u to $vu^k w k$, is injective. Since $|U^*| = q - 1 = |T|$, this means every element of T can be written this way, implying $T \leq \langle U, k \rangle$. Then $B = TU < \langle U, k \rangle$, so by the maximality of B we see that $G = \langle U, k \rangle$. If we pick a $u \in U^*$ such that the corresponding $s = k^2$, then we have

$$\begin{aligned} vu^k w k &= k^2 \\ vu^k w &= k \end{aligned}$$

showing that $k \in \langle U, U^k \rangle$, and hence we have another expression for $G = \langle U, U^k \rangle$. This is equivalent to saying the normal closure U^G is equal to G . Since $UG' \triangleleft G$ is a normal subgroup containing U , we thus also have $G = UG'$.

Now fix a $u \in U^*$, and note that $S := \{[u, t] \mid t \in T\}$ has $|T/Z(G)|$ elements in it, since having $u^t = u^s$ implies ts^{-1} fixes a non-trivial point of U , hence of $\mathbb{P}^1(V) \setminus \{[x], [y]\}$, and thus $ts^{-1} \in Z(G)$. If q is even, then $|S| = q - 1$, and if q is odd then $S = \frac{1}{2}(q - 1)$. But $S \leq U \cap G'$. If q is even, then $|S| > q/2$ when $q > 2$, and when q is odd $|S| > q/3$ when $q > 3$. Since $q/2$ (respectively $q/3$) are the maximal sizes of a proper subgroup of U , we see that $q > 3$ implies $U \cap G'$ is not proper, and $U \leq G'$. Since $G = UG'$ then, we see that $q > 3$ implies $G = G'$ is a perfect group. The case $q \in \{2, 3\}$ does not actually yield a perfect group, and in fact in those cases $U \cap G' = \{1\}$. Also note that this result was also proved in a more mechanical manner in Proposition A.5.

We finish this section by describing the normal subgroups of G in the case $q > 3$, or equivalently in the case when G is perfect. Suppose $N \triangleleft G$ is a normal subgroup. If $N \leq B$,

B. Structure of groups of Lie type

then $N \leq \cap B^g$, so that N fixes all points of $\mathbb{P}^1(V)$, implying $N \leq Z(G)$. If $N \not\leq B$, then maximality implies $G = BN$. But then

$$G/N \cong BN/N \cong B/(B \cap N)$$

shows that G/N is isomorphic to a perfect quotient of B . Since $U \triangleleft B$ is Abelian and so is $B/U \cong T$, B is a solvable group, so its only perfect quotient is the trivial group. This shows G/N is trivial and $G = N$. Thus, when $q > 3$, the only non-trivial normal subgroup of G is $Z(G)$ when q is odd; in the q even case G is a simple group. In both even and odd cases $G/Z(G) = PSL(2, \mathbb{F}_q)$ is simple.

B.2. Tori and coordinates

The subgroup T constructed in the previous section is called a **split torus** of G . In this section we explain that terminology, and also discuss the non-split tori of G . We also spend some time on choosing clever bases for V to get a more intuitive feel of what elements in G look like.

We typically hear the word "torus" to denote a product of circles in topology. Here a circle in $\mathbb{C}$ is the set of all elements of norm 1. To work in (discrete) finite fields, we will instead focus on the dense subset of points in the circle that are roots of unity. So in our finite field case, we replace circle with roots of unity, and call a torus a product of "circles". In particular, since every element of $\mathbb{F}_q$ is a root of unity, we're talking about finite products $\mathbb{F}_q^* \times \cdots \times \mathbb{F}_q^*$. This is a **split torus**. Of course, unlike $\mathbb{C}$, $\mathbb{F}_q$ is not algebraically closed, so we're not really getting the "dense" set of circle points we'd want. So if L is a linear group over some finite-dimensional $\mathbb{F}_q$ -vector space, and $H \leq L$ is a subgroup isomorphic to a subgroup of $\mathbb{F}_1^* \times \cdots \times \mathbb{F}_n^*$ with each $\mathbb{F}_i$ a finite extension of $\mathbb{F}_q$, then we call H a **torus**. We call H **non-split** if it is not simply a direct product of $\mathbb{F}_q^*$, but includes some elements (at least in one coordinate) coming from an extension field. Still H is not dense, of course, but this does allow us to talk of *maximal* tori, and in the limit (viewed over $\overline{\mathbb{F}_q}$) we do get something similar to the topological torus. But we won't talk any more about that.

Another point of view is more algebraic in nature, and comes from looking at finite-dimensional commutative algebras over $\mathbb{F}_q$, and their groups of units (these are the tori). In the two-dimensional case, there are two such algebras: $\mathbb{F}_q \times \mathbb{F}_q$ and $\mathbb{F}_{q^2}$, with corresponding groups of units $\mathbb{F}_q^* \times \mathbb{F}_q^*$ and $\mathbb{F}_{q^2}^*$. The first is the split case (since the algebra is decomposable), and the latter the non-split case. Both of these tori live in $GL(2, \mathbb{F}_q)$, and their intersection with G gives the tori we discuss below.

Now it makes sense to say that our $T \leq B \leq G$ is a split torus: we showed above that $T \cong \mathbb{F}_q^*$. As we'll see in the next section, every split torus in G is actually a conjugate of T . So now we seek to find a representative non-split torus in G . For that, we will heavily leverage the

B. Structure of groups of Lie type

identification of V with the elements of the extension field $\mathbb{F}_{q^2}/\mathbb{F}_q$. For example, let $\alpha \in \mathbb{F}_{q^2}$, and note that the map $V \rightarrow V$ (really a map $\mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$) given by $x \mapsto \alpha x$ is $\mathbb{F}_q$ -linear, since multiplication is distributive. We write $m_\alpha \in GL(2, \mathbb{F}_q)$ for this linear transformation. Obviously the map $m : \mathbb{F}_{q^2}^* \rightarrow GL(2, \mathbb{F}_q)$ is an injective homomorphism. To see when the image of m lands in $G := SL(2, \mathbb{F}_q)$, we need to review a bit about the Galois extension $\mathbb{F}_{q^2}/\mathbb{F}_q$.

Recall that the Galois group of $\mathbb{F}_{q^2}/\mathbb{F}_q$ is of order 2, and the non-trivial element is the **Frobenius automorphism**, given by $F(x) = x^q$. Also for any Galois extension (including this one), we have well-defined homomorphisms

$$\mathfrak{N} : \mathbb{F}_{q^2}^* \rightarrow \mathbb{F}_q^* \quad \mathfrak{T} : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_q$$

called the **norm** and the **trace**, respectively. In our simple case, $\mathfrak{N}(\alpha) = \alpha F(\alpha) = \alpha^{q+1}$ and $\mathfrak{T}(\alpha) = \alpha + F(\alpha) = \alpha + \alpha^q$. As is well-known, we have that $\mathfrak{N}(\alpha) = \det(m_\alpha)$ and $\mathfrak{T}(\alpha) = \text{Tr}(m_\alpha)$. So, for m_α to be in G , it is necessary and sufficient that $\det(m_\alpha) = \alpha^{q+1} = 1$. If $C \leq \mathbb{F}_{q^2}^*$ is the cyclic subgroup of order $q+1$, then we see that

$$m(\mathbb{F}_{q^2}^*) \cap G = m(C)$$

and we write $\hat{T} := m(C) \leq G$ for the cyclic subgroup of order $q+1$ in G ; this is our non-split torus, since $\hat{T} \cong C \leq \mathbb{F}_{q^2}^*$, and since $|C| > |\mathbb{F}_q^*|$, we are certainly not in the split case. We also note that if $\alpha \in C \cap \mathbb{F}_q^*$, then

$$1 = \alpha^{q+1} = \alpha^{q-1}\alpha^2 = \alpha^2$$

so that $\alpha = \pm 1$. This shows that $\hat{T} \cap m(\mathbb{F}_q^*) = Z(G)$.

We'd also like to think of F as an element of G , since it is certainly $\mathbb{F}_q$ -linear. However, this isn't always possible. If x is a generator of $\mathbb{F}_{q^2}^*$, then $\{x, x^q\}$ is a basis for V , because otherwise we reach the contradiction (with $a, b \in \mathbb{F}_q$)

$$\begin{aligned} ax^q + bx &= 0 \\ x^{q-1} &\in \mathbb{F}_q \\ x^{(q-1)^2} &= 1 \\ (q-1)^2 &\geq q^2 - 1 \\ q &\leq 1 \end{aligned}$$

In the basis $\{x, x^q\}$, we see that F simply swaps basis elements, and hence has determinant -1 . So when q is even, we indeed have F belonging to G , but that's not the case when q is odd. Nevertheless, we can remedy this. When q is odd, $|\mathbb{F}_{q^2}^*| = (q-1)(q+1)$ is divisible by $2(q+1)$, and since $-1 \in \mathbb{F}_{q^2}^*$ is the unique element of order 2, there exists $z \in \mathbb{F}_{q^2}^*$ such that $z^{q+1} = -1$. But then

$$\det(m_z) = \mathfrak{N}(z) = z^{q+1} = -1$$

B. Structure of groups of Lie type

and thus $\det(Fm_z) = 1$ and we can consider Fm_z as an element of G . We write $\hat{k}$ for this element, in parallel to the element k we constructed when studying the split torus T . (Of course, we choose $z = 1$ when q is even, so this element $\hat{k}$ exists for all q). Note that $\hat{k}^{-1}$ is nothing more than $-Fm_z$, showing that $\hat{k}^2 = -1$.

For $x \in V = \mathbb{F}_{q^2}$ and $m_\alpha \in \hat{T}$, we see that

$$x(\hat{k}m_\alpha\hat{k}^{-1}) = x^q z(m_\alpha\hat{k}^{-1}) = \alpha x^q z(\hat{k}^{-1}) = -\alpha^q x z^{q+1} = \alpha^{-1}x$$

showing that $m_\alpha^{\hat{k}} = m(\alpha^{-1}) = m_\alpha^{-1}$. Thus $\hat{T}^{\hat{k}} = \hat{T}$, with $\hat{k}$ acting via inversion, similar to how T and k interact.

We now take a look at our various distinguished subgroups and elements of G from the previous two sections, and pick clever bases for V to get a better concrete understanding of how they look. First, we choose $[x] = [1 : 0] \in \mathbb{P}^1(V)$, the "point at infinity", and let $[y] = [0 : 1]$ be the "zero" point. In this basis, the Borel subgroup $B \leq G$ is nothing more than the upper-triangular matrices. Meanwhile, U fixing x means U is the group of unipotent matrices, while T fixing both $[1 : 0]$ and $[0 : 1]$ makes T diagonal. Also, $k \in G$ swapping $[x]$ and $[y]$ allows us to write it in a particularly nice form:

$$\begin{aligned} B &= \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a, b \in \mathbb{F}_q \right\} \\ U &= \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_q \right\} \\ T &= \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_q^* \right\} \\ k &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

Note this is possibly the clearest way to see that $k^2 = -1$. Thinking of elements of G as fractional linear transformations of $\mathbb{P}^1(V)$, elements of B (fixing "infinity") are traditional linear maps, with elements of U being translations $x \mapsto x + b$ and elements of T being dilations $x \mapsto a^2x$. This also shows that for such a $u \in U$ and $t \in T$, we must have u^t being the map $x \mapsto x + a^2b$. When q is even, and every element is a square, this shows that T acts transitively on U^* . Meanwhile, when q is odd, this makes it clear what the two T -conjugacy classes of U^* are: translations by squares and translations by non-squares. To round out the fractional linear transformations, k is acting via inversion: $x \mapsto -x^{-1}$.

Finding a basis for V to similarly gain insight into $\hat{T}$ and $\hat{k}$ is harder. When q is odd, we can choose a basis $\{1, z^q\}$ for V , and using $z^{q+1} = -1$ and $\mathfrak{T}(z) = z + z^q$ shows

B. Structure of groups of Lie type

$$\begin{aligned} F &= \begin{pmatrix} 1 & \mathfrak{I}(z) \\ 0 & -1 \end{pmatrix} \\ m_z &= \begin{pmatrix} \mathfrak{I}(z) & -1 \\ -1 & 0 \end{pmatrix} \\ \hat{k} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

When q is even $\hat{k} = F$, so as seen before, still has the form above. Note this implies (with the description of k above) that k and $\hat{k}$ are conjugate (for all q). In $SL(2, \mathbb{F}_{q^2})$ every element of $\hat{T}$ is (simultaneously) diagonalizable, and so with a well-chosen conjugation matrix we can get an explicit description of $\hat{T} \leq G$. One way to do this is to look at irreducible quadratics over $\mathbb{F}_q$. For q odd we can choose $x^2 - \epsilon = 0$ for a non-square $\epsilon \in \mathbb{F}_q$. Let δ be a root of this polynomial, so $\mathbb{F}_{q^2} = \mathbb{F}_q(\delta)$. The Frobenius automorphism is then such that $F(\delta) = -\delta$, implying $\mathfrak{N}(a + b\delta) = a^2 - b^2\epsilon$. So we have

$$m(C) = \{a + b\delta \mid a^2 - b^2\epsilon = 1\}$$

And in the basis $\{1, \delta\}$ we see that

$$\hat{T} = \left\{ \begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix} \mid a^2 - b^2\epsilon = 1 \right\}$$

It's worth pointing out the similarity here with the case over base field $\mathbb{R}$, where our quadratic extension is $\mathbb{C}$, and we can choose our irreducible quadratic to be $x^2 + 1 = 0$. Then the above is just the construction of $SO(2) \leq SL(2, \mathbb{R})$, realizing the unit circle (a torus!).

When q is even, we need a slightly different quadratic, and we can choose $x^2 + x + \epsilon = 0$, chosen such that it has no roots in $\mathbb{F}_q$. Again let δ be a root with $\mathbb{F}_{q^2} = \mathbb{F}_q(\delta)$. The Frobenius automorphism is then $F(\delta) = \delta + 1$ (the other root), implying in the basis $\{1, \delta\}$ we have (as before)

$$\begin{aligned} \mathfrak{N}(a + b\delta) &= a^2 + ab + b^2\epsilon \\ m(C) &= \{a + b\delta \mid a^2 + ab + b^2\epsilon = 1\} \\ \hat{T} &= \left\{ \begin{pmatrix} a & b\epsilon \\ b & a + b \end{pmatrix} \mid a^2 + ab + b^2\epsilon = 1 \right\} \end{aligned}$$

B.3. Conjugacy classes

We start our investigation with q odd, but we'll see that very few changes are required when q is even. Of course every element of $Z(G) = \{\pm 1\}$ is in its own conjugacy class of

B. Structure of groups of Lie type

size 1. For the rest of $G \setminus Z(G)$, we will investigate their centralizers to find the sizes of their conjugacy classes. Throughout this section, we write g^G to denote the conjugacy class of $g \in G$.

First let $u \in U^*$. We know u^G contains $\frac{1}{2}(q-1)$ elements of U , just from the action of T . Suppose that $g \in G$ centralizes u , so that $u^g = u$. Then u^g fixes both $x \in V$ and $xg \in V$, and since u is not a scalar transformation, it must be that $xg = x$, so that $g \in B$. Thus $C_G(u) = C_B(u)$. But we know that $C_B(u) \cap T = Z(G)$, since T acts on U^* the same way it acts on $\mathbb{P}^1(V) \setminus \{[x], [y]\}$. In other words, $C_B(u) = U \times Z(G)$, and $|u^G| = \frac{1}{2}(q^2 - 1)$. If $\hat{u} \in U^*$ is an element not conjugate to u , then the same reasoning shows $|\hat{u}^G| = \frac{1}{2}(q^2 - 1)$ as well. Now $-u \notin U$ since it has even order, but $C_G(-u) = C_G(u)$, so $(-u)^G$ and $(-\hat{u})^G$ are two more conjugacy classes of size $\frac{1}{2}(q^2 - 1)$. As we'll see, these are all the unipotent elements (fixing a non-zero vector in V) contained in G .

Now let $t \in T \setminus Z(G)$. Obviously t is never conjugated into U , since t doesn't have order p . If $g \in G$ is such that $t^g = t$, then g must permute $\{[x], [y]\}$, meaning that $g \in T \cup kT = N_G(T)$. Now T is Abelian, but $t^k = t^{-1} \neq t$ since T has a unique element of order 2 ($-1 \in Z(G)$). So $C_G(T) = T$, and $|t^G| = q(q+1)$. Note that if we assume $t^g \in T$, the same conclusion follows: g permutes $\{[x], [y]\}$, so $g \in N_G(T)$. So $t^G \cap T = \{t, t^{-1}\}$, and by pairing elements with their inverses we have

$$\frac{|T| - |Z(G)|}{2} = \frac{q-3}{2}$$

conjugacy classes of this type. Again, as we'll see, these are all the elements in split tori in G .

Finally, let $m_\alpha \in \hat{T} \setminus Z(G)$; note this means that $\alpha \notin \mathbb{F}_q$, and that m_α lives in no conjugate of B (hence isn't covered by the classes above). Suppose $g \in G$ is such that $m_\alpha^g = m_\alpha$. Now every element of $\mathbb{F}_{q^2}$ can be written as $a\alpha + b$ with $a, b \in \mathbb{F}_q$, because $\{1, \alpha\}$ forms an $\mathbb{F}_q$ -basis of V . But then

$$(a\alpha + b)g = (a\alpha)g + (b)g = a(1\alpha)g + b(1)g = a\alpha(1)g + b(1)g = (a\alpha + b)(1)g$$

where the third equality follows from $m_\alpha g = g m_\alpha$. This shows that g is actually $\mathbb{F}_{q^2}$ -linear on V , so it is scalar multiplication: $g \equiv m_\beta$ for some $\beta \in \mathbb{F}_{q^2}^*$. In other words, $g \in \hat{T}$. Just as before then, $C_G(m_\alpha) = \hat{T}$ and $|m_\alpha^G| = q(q-1)$. Suppose instead that $m_\alpha^g = m_\beta \in \hat{T}$. Then $\mathfrak{T}(\alpha) = \mathfrak{T}(\beta)$, and so if $\alpha \neq \beta$, we would have

$$0 = \mathfrak{T}(\alpha) - \mathfrak{T}(\beta) = (\alpha^q - \beta^q) + (\alpha - \beta) = (\alpha - \beta)^q + (\alpha - \beta)$$

This implies that $\beta = a\gamma + \alpha$ for some $\gamma \in \mathbb{F}_{q^2}$ with $\gamma^{q-1} = -1$ (here we fix γ but let $a \in \mathbb{F}_q^*$ vary). Since $\beta^{q+1} = 1$, this allows us to solve for a to show at most one such β exists, so that $m_\alpha^G \cap \hat{T}$ has size at most 2. This of course implies $m_\alpha^G \cap \hat{T} = \{m_\alpha, m_\alpha^{-1}\}$ (remembering that $m_\alpha^k = m_\alpha^{-1}$), so that by pairing elements with their inverses we get $\frac{1}{2}(q-1)$ such classes. Note that this implies $N_G(\hat{T}) = \hat{T} \cup \hat{k}\hat{T} = \langle \hat{T}, \hat{k} \rangle$, similar to the case of T .

B. Structure of groups of Lie type

But this must be all the conjugacy classes of G :

$$2 \cdot 1 + 4 \cdot \frac{q^2 - 1}{2} + \frac{q - 3}{2} \cdot q(q + 1) + \frac{q - 1}{2} \cdot q(q - 1) = q(q - 1)(q + 1) = |G|$$

Putting it into table format:

Table B.1: Conjugacy classes of $SL(2, \mathbb{F}_q)$ when q is odd

Type	Class Size	# Classes
± 1	1	2
$\{\pm u, \pm \hat{u}\}$	$\frac{1}{2}(q^2 - 1)$	4
t	$q(q + 1)$	$\frac{1}{2}(q - 3)$
m_α	$q(q - 1)$	$\frac{1}{2}(q - 1)$
4	$q(q - 1)(q + 1)$	$q + 4$

When q is even, we have to make a few adjustments. First, $Z(G)$ is trivial. Also T acts transitively on U , so $u^G = \hat{u}^G$, and of course also $u = -u$. In this case $C_G(u) = U$ so the class is twice the size, but there's only one of these type, not 4. Finally, from $|Z(G)| = 1$ we have to adjust the number of classes similar to $t \in T$ or $m_\alpha \in \hat{T}$. Other than that, though, we have our table:

Table B.2: Conjugacy classes of $SL(2, \mathbb{F}_q)$ when q is even

Type	Class Size	# Classes
1	1	1
u	$q^2 - 1$	1
t	$q(q + 1)$	$\frac{1}{2}(q - 2)$
m_α	$q(q - 1)$	$\frac{q}{2}$
4	$q(q - 1)(q + 1)$	$q + 1$

Before moving on to the $PSL(2, \mathbb{F}_q)$ case, it's worth saying a few words about these conjugacy classes. We see that in the case q is odd, there are 4 unipotent classes, corresponding to fractional linear transformations $x + b$ for b square and non-square, and the reciprocals of those. We see that all non-central elements of a split torus are in their own conjugacy classes, up to inversion; similarly this also holds for the non-split torus. Amusingly, the only classes outside B (or one of its conjugates) are the classes coming from $\hat{T}$. That is, an element that doesn't fix any point of $\mathbb{P}^1(V)$ lives in a non-split torus.

What about k and $\hat{k}$? As mentioned in the previous section, k and $\hat{k}$ are actually conjugate. When q is even they both live in conjugates of U . When q is odd, they always live in a torus:

B. Structure of groups of Lie type

sometimes a split torus, sometimes a non-split torus, depending on q . The deciding factor is whether k (and hence its conjugate $\hat{k}$) fixes any line in $\mathbb{P}^1(V)$, which depends on whether $-1 \in \mathbb{F}_q$ is a square or not, and that ultimately comes down to $q \pmod{4}$. We've already seen the parity of q affecting the conjugacy classes of G above; in $PSL(2, \mathbb{F}_q)$ we'll see that $q \pmod{4}$ also influences the class structure.

For the rest of this section, we let $H = PSL(2, \mathbb{F}_q)$, and we only consider q odd (since in the even case $H = G$ is already covered above). Of course since $H = G/Z(G)$ the two classes of $Z(G)$ get fused into 1 in H . We'll investigate how the other classes of G fuse in H in order to get the full conjugacy class structure. We'll write elements of H using the same symbols used in G , which should introduce no confusion. We'll use $g_1 \equiv g_2$ to mean that $g_1, g_2 \in G$ represent the same element in H .

Now in H , $u \equiv -u$ since $-1 \in Z(G)$; similarly $\hat{u} \equiv -\hat{u}$. Since the conjugacy classes of both u and $\hat{u}$ are contained in U , and so are disjoint from $Z(G)$, we see that the classes map injectively into H . That is, u and $\hat{u}$ both give classes of size $\frac{1}{2}(q^2 - 1)$ in H .

For the other classes, we need to distinguish $q \pmod{4}$. We first treat the case $q \equiv 1 \pmod{4}$. Then $T/Z(G)$ has a single element of order 2, which is centralized (in H) by the image of k . We call this unique involution $t_{\mathbb{P}}$, and note that its conjugacy class size gets cut in half, since its centralizer doubles in size in H . Otherwise, the elements of T give the same classes (and size) that they do in G , but there are fewer of these classes; indeed, removing $\{1, t_{\mathbb{P}}\}$ we now have only

$$\frac{|T/Z(G)| - 2}{2} = \frac{q - 5}{4}$$

classes. The case for $\hat{T}$ is much simpler, since $\hat{T}/Z(G)$ has odd order, so no elements equal to their own inverses. Indeed, the classes stay the same (and their sizes), except there are half as many. Again, adding up class sizes shows we are done, and we have

Table B.3: Conjugacy classes of $PSL(2, \mathbb{F}_q)$ when $q \equiv 1 \pmod{4}$

Type	Class Size	# Classes
1	1	1
$\{u, \hat{u}\}$	$\frac{1}{2}(q^2 - 1)$	2
$t_{\mathbb{P}}$	$\frac{1}{2}q(q + 1)$	1
t	$q(q + 1)$	$\frac{1}{4}(q - 5)$
m_{α}	$q(q - 1)$	$\frac{1}{4}(q - 1)$
5	$\frac{1}{2}q(q - 1)(q + 1)$	$\frac{1}{2}(q + 5)$

When $q \equiv 3 \pmod{4}$, the same analysis as above holds, except we swap the roles of T and $\hat{T}$, since now $T/Z(G)$ has odd order, and $\hat{T}/Z(G)$ has a unique involution, which we call $\hat{t}_{\mathbb{P}}$.

B. Structure of groups of Lie type

Just as above $\hat{k}$ centralizes $\hat{t}_{\mathbb{P}}$ in H . This also means the number of conjugacy classes coming from T gets cut in half, but we lose one coming from $\hat{T}$. We have

Table B.4: Conjugacy classes of $PSL(2, \mathbb{F}_q)$ when $q \equiv 3 \pmod{4}$

Type	Class Size	# Classes
1	1	1
$\{u, \hat{u}\}$	$\frac{1}{2}(q^2 - 1)$	2
$\hat{t}_{\mathbb{P}}$	$\frac{1}{2}q(q - 1)$	1
t	$q(q + 1)$	$\frac{1}{4}(q - 3)$
m_{α}	$q(q - 1)$	$\frac{1}{4}(q - 3)$
5	$\frac{1}{2}q(q - 1)(q + 1)$	$\frac{1}{2}(q + 5)$