Solutions to HW1

1. (a) Denote the support of $g \in \mathsf{Sym}\, X$ by $\mathsf{supp}(g) = \{x \in X : g(x) \neq x\}$. The identity element $1 \in G$ has $|\mathsf{supp}(1)| = 0$, so $1 \in \mathsf{FinSym}\, X$. For $g, h \in G$ we have $\mathsf{supp}(gh) \subseteq \mathsf{supp}(g) \cup \mathsf{supp}(h)$ and $\mathsf{supp}(g^{-1}) = \mathsf{supp}(g)$, which are finite sets. So $\mathsf{FinSym}\, X$ is a subgroup of $\mathsf{Sym}\, X$. Clearly X is proper: choose any infinite sequence $x_n \in X$ for $n \in \mathbb{Z}$ and consider the cycle which maps $x_n \mapsto x_{n+1}$ for all $n \in \mathbb{Z}$, while fixing any remaining elements of X; this cycle lies in $\mathsf{Sym}\, X$ but not in $\mathsf{FinSym}\, X$.

   (b) Given $g \in \mathsf{FinSym}\, X$, we may define g to be an even or an odd permutation of X according as g is an even or an odd permutation of its support, and we write $\mathsf{sgn}(g) = +1$ or -1 respectively. So $\mathsf{sgn} : \mathsf{FinSym}\, X \to \{\pm 1\}$ is well-defined. Clearly $\mathsf{sgn}(gh) = \mathsf{sgn}(g)\,\mathsf{sgn}(h)$ by considering the restriction of g, h, gh to $\mathsf{supp}(g) \cup \mathsf{supp}(h)$. So sgn is a homomorphism. It is surjective since the transpositions lie in $\mathsf{FinSym}\, X$. We define $\mathsf{Alt}\, X$ to be the kernel of this homomorphsim. (Remark: $\mathsf{FinSym}\, X$ is the direct limit of the family of subgroups $\mathsf{Sym}\, K \leqslant \mathsf{Sym}\, X$ over all finite subsets $K \subset X$, and $\mathsf{Alt}\, X$ is the direct limit of the alternating subgroups $\mathsf{Alt}\, K$. See the textbook for a discussion of direct limits.)

   (c) The quotient group $\mathsf{Sym}\, X / \mathsf{FinSym}\, X$ is not simple whenever X is uncountable, for the same reasons as those underlying (a): we have $\mathsf{FinSym}\, X \lhd N \lhd \mathsf{Sym}\, X$ where N consists of all permutations having countable support.

   However, the quotient group is simple whenever X is countably infinite. I think I mentioned this in class; and in Appendix I, I have supplied a proof which is elementary but somewhat technical. (Possibly you can find a shorter proof than mine? I haven't tried to look up the answer. But the strategy is similar to the proof that A_n is simple for $n \geqslant 5$; see pp.71-72 of the textbook.)

2. Let $G = GL_2(F)$ where F is an arbitrary field.

   (a) Let $Z = \{aI : 0 \neq a \in F\}$. Clearly $Z \subseteq Z(G)$ since $(aI)g = ag = g(aI)$ for all $g \in G$. Conversely, suppose $g = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in Z(G)$. Since $g\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] g$, we obtain $b = c = 0$. Also $g\left[\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right] g$ which gives $a = d$, so $g = \left[\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right] \in Z$. Thus $Z = Z(G)$ as required.

   (b) Consider a point of the projective line $\langle u \rangle \in \mathbb{P}^1 F$ where $0 \neq u \in F^2$. Note that by definition, $\langle u \rangle$ is a one-dimensional subspace of F^2; and this subspace is fixed

by $g \in G$ iff u is an eigenvector of g. If $\langle u\rangle$, $\langle v\rangle$ and $\langle w\rangle$ are three distinct points of $\mathbb{P}^1F$ fixed by g, then $gu = \lambda u$, $gv = \mu v$ and $gw = \nu w$ for some nonzero scalars $\lambda, \mu, \nu \in F$. Since we started with three distinct one-dimensional subspaces, any two of the vectors u, v, w form a basis for F^2. So $w = au + bv$ for some nonzero $a, b \in F$ and $\nu(au + bv) = \nu w = gw = agu + bgv = a\lambda v + b\mu v$. Comparing coefficients yields $a\nu = a\lambda$ and $b\nu = b\mu$. Since a and b are nonzero, we obtain $\lambda = \mu = \nu$. Since both basis vectors u, v are eigenvectors for g with the same eigenvalue λ, we have $g = \left[\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right] \in Z$. Conversely, given $g = \left[\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right] \in Z$, every vector is a λ-eigenvector for g, so g fixes every one-dimensional subspace.

Yes, $\mathsf{Alt}\, X$ is simple. Let $K \trianglelefteq \mathsf{Alt}\, X$ be any nontrivial normal subgroup, and let $g \in K$ be a nontrivial element. Then $g \in A_n$ for some positive integer n. We may suppose $n \geqslant 5$. Since A_m is simple for all $m \geqslant 5$, we have $K \supseteq A_m$ for all $m \geqslant n$. So $K = \mathsf{Alt}\, K$. This proves that $\mathsf{Alt}\, X$ is simple.

(c) The kernel of the homomorphism $G \to \mathsf{Sym}\, \mathbb{P}^1F$ is by definition the set of all $g \in G$ fixing every point. The number of fixed points for every such g is $|\mathbb{P}^1F| = |F|+1 \geqslant 3$; so by (b), every such g is in Z. Conversely, every $g \in Z$ fixes every point of $\mathbb{P}^1F$.

3. Since B is real symmetric, $B = U^TD'U$ for some $U \in O_n(\mathbb{R})$ and real $n \times n$ diagonal matrix D'. We may write $D' = D^2$ for some *diagonal* complex $n \times n$ matrix D. So $B = M^TM$ where $M = DU$. Since B is invertible, so is M. Now $A \in O(B, \mathbb{C})$ iff $A^TBA = B$ iff $(A^TM^T)(MA) = M^TM$ iff $(M^{-T}A^TM^T)(MAM^{-1}) = I$ iff $MAM^{-1} \in O(I, \mathbb{C})$. The map $O(B, \mathbb{C}) \to O(I, \mathbb{C})$, $A \mapsto MAM^{-1}$ is clearly an isomorphism (conjugation by M is an inner automorphism of $GL(\mathbb{C}^n)$, and we are restricting this isomorphism to the subgroup $O(B, \mathbb{C})$).

Remarks. An n-dimensional vector space F^n over F has subspaces of dimension $1, 2, 3, \ldots, n-1$ which are called projective points, lines, planes, ..., hyperplanes of the projective $(n-1)$-space $\mathbb{P}^{n-1}F$ over F. The group $GL_n(F)$ acts on the projective space, transitively permuting the subspaces of each fixed dimension. Since the center $Z = Z(GL_n(F)) = \{aI : 0 \neq a \in F\}$ acts trivially on $\mathbb{P}^{n-1}F$, the permutation group induced by $GL_n(F)$ is the *projective general linear group* $PGL_n(F) = GL_n(F)/Z$.

The isometry group $O(Q, F)$ of a quadratic form $Q : F^n \to F$ does not act transitively on points. Over $\mathbb{C}$, there are two point orbits: the points $\langle u\rangle$ satisfying $Q(u) = 0$ (the point set known as the corresponding *quadric*) and the points for which $Q(u) \neq 0$. It is useful to keep this perspective in mind for #4. Actually in #4, the quadric is simply a curve in the projective plane $\mathbb{P}^2\mathbb{C}$: it is the set of points $\langle (a, b, c)^T\rangle$ satisfying $b^2 - 4ac = 0$. These points all clearly have the form

- the points $\langle (1, 2\lambda, \lambda^2)^T \rangle$ for $\lambda \in \mathbb{C}$; and
- the point $\langle (0, 0, 1)^T \rangle$.

Thus a nondegenerate conic in the projective plane $\mathbb{P}^2\mathbb{C}$ is indexed by $\mathbb{C} \cup \{\infty\}$, just like the points of the projective line $\mathbb{P}^1\mathbb{C}$. The goal of #4 is to show more: the conic and the projective line have isomorphic groups $PSL_2(\mathbb{C})$ and $PSO_3(\mathbb{C})$ acting on them. Moreover, these two permutation actions are equivalent.

---

4. (a) If $g \in GL_2(\mathbb{C})$ then $g = h\left[\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right]$ where $d = \det g$ and $h \in SL_2(\mathbb{C})$. Now

$$\left[\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right] f(x, y) = ad^2x^2 + bdxy + cy^2 \quad \text{and} \quad Q\left(\left[\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right] f\right) = (bd)^2 - 4ad^2c = d^2Q(f),$$

so it remains only to show that $Q(hf) = Q(f)$ for all $h \in SL_2(\mathbb{C})$. The matrix $h = \left[\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right]$ satisfies

$$\begin{aligned} (hf)(x, y) &= ax^2 + bx(\lambda x + y) + c(\lambda x + y)^2 = (a + \lambda b + \lambda^2 c)x^2 + (b + 2\lambda c)xy + cy^2, \\ Q(hf) &= (b + 2\lambda c)^2 - 4(a + \lambda b + \lambda^2 c)c = b^2 - 4ac = Q(f). \end{aligned}$$

The same computation holds for h^T; and since such matrices are known to generate $SL_2(\mathbb{C})$ (see Appendix II), we have $Q(hf) = Q(f)$ for all $h \in SL_2(\mathbb{C})$ as required.

(b) This was part of our proof in (a).

(c) For the matrix $h = \left[\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right]$, the computation in (a) shows that the matrix of h with resect to the basis $\{x^2, xy, y^2\}$ of V is

$$R_h = \begin{bmatrix} 1 & \lambda & \lambda^2 \\ 0 & 1 & 2\lambda \\ 0 & 0 & 1 \end{bmatrix} \in SL_3(\mathbb{C})$$

and a similar computation holds for h^T. Once again since these matrices generate $SL_2(\mathbb{C})$ and the map $h \mapsto R_h$ is a homomorphism, $R_h \in SL_3(\mathbb{C})$ for all $h \in SL_2(\mathbb{C})$. (Alternatively, the map $SL_2(\mathbb{C}) \to \mathbb{C}^\times$, $h \mapsto \det R_h$ is a homomorphism, so its kernel is a normal subgroup of $SL_2(\mathbb{C})$. The kernel contains all commutators $[h, k] = hkh^{-1}k^{-1}$. Since $PSL_2(\mathbb{C})$ is nonabelian simple, the kernel must be all of $SL_2(\mathbb{C})$.)

So $R_h \in O_3(\mathbb{C}) \cap SL_3(\mathbb{C}) = SO_3(\mathbb{C})$ for all $h \in SL_2(\mathbb{C})$. The fact that $R_hR_k = R_{hk}$ follows directly from the fact that $SL_2(\mathbb{C})$ is acting on V by linear changes of variable; and by definition, composition of such changes of variable is associative:

$$R_{hk}f = (hk)f = h(kf) = R_hR_kf.$$

Before proceeding further, we point out that the upper triangular matrices found in (c) fix the point $\langle u \rangle$ of the conic, where $u = (1,0,0)^T$. These matrices constitute almost the full stabilizer of the point $\langle u \rangle$ in $S \cong SO_3(\mathbb{C})$, the subgroup of $SL(V)$ preserving the quadratic form Q. The column vectors u and $v = (0,0,1)^T$ represent the basis vectors $x^2, y^2 \in V$ respectively. Here we compute their respective stabilizers in S.

Every matrix $A \in S_{\langle u \rangle}$ must have the form

$$A = \begin{bmatrix} \varepsilon & \alpha & \beta \\ 0 & \gamma & \delta \\ 0 & \mu & \nu \end{bmatrix}$$

for some $\alpha, \beta, \gamma, \delta, \varepsilon, \mu, \nu \in \mathbb{C}$. The conditions $ABA^T = B$ and $\det A = 1$ give equations in $\alpha, \beta, \ldots, \nu$ which are easy to solve, leading to

$$A = \begin{bmatrix} \varepsilon & \varepsilon\lambda & \varepsilon\lambda^2 \\ 0 & 1 & 2\lambda \\ 0 & 0 & \varepsilon \end{bmatrix}, \quad \varepsilon = \pm 1.$$

Extending the computation in (a,c), we see that these matrices all have the form R_h where $h = \left[\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} i & 0 \\ i\lambda & -i \end{smallmatrix}\right]$. Similarly, the stabilizer $S_{\langle v \rangle}$ consists of all R_h where $h = \left[\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} i & -i\lambda \\ 0 & -i \end{smallmatrix}\right]$.

Our proof of Part (d) below uses the Frattini Argument (Appendix III). As preparation for this, you might consider reading the two proofs we have given in Appendix II, with and without the Frattini Argument.

(d) Let $S = SO_3(\mathbb{C})$, and denote the image of our homomorphism by $H = \{R_h : h \in SL_2(\mathbb{C})\} \leqslant S$. By the computations above, $\langle S_{\langle u \rangle}, S_{\langle v \rangle} \rangle \leqslant H$. The subgroup $S_{\langle v \rangle}$ fixes a single point $\langle v \rangle$ of the conic, while transitively permuting the remaining points of the conic (these points have the form $\langle (1, 2\lambda, \lambda^2)^T \rangle = R_h u$ where $h = \left[\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right]$, $R_h \in S_{\langle v \rangle}$). Similarly, $S_{\langle u \rangle}$ has two orbits on the points of the conic: $\{\langle u \rangle\}$ and all the remaining points of the conic. From this it follows that $\langle S_{\langle u \rangle}, S_{\langle v \rangle} \rangle$ is transitive on the conic. By the Frattini argument (Appendix III),

$$S = \langle S_{\langle u \rangle}, S_{\langle v \rangle} \rangle S_{\langle v \rangle} = \langle S_{\langle u \rangle}, S_{\langle v \rangle} \rangle \leqslant H \leqslant S.$$

This gives $H = S$ as required.

(e) All that is left is to show that the map $h \mapsto R_h$ has kernel $\pm I$, for then $PSL_2(\mathbb{C}) = SL_2(\mathbb{C})/\{\pm I\} \cong SO_3(\mathbb{C})$ by the First Isomorphism Theorem. We already know that the kernel contains $\pm I$; and since our homomorphism is onto $SO_3(\mathbb{C})$, the kernel must be a proper normal subgroup of $SL_2(\mathbb{C})$ containing $\pm I$. Given that $PSL_2(\mathbb{C})$ is simple, the kernel equals $\{\pm I\}$ and we are done. Put another way, the only proper normal subgroups $K \lhd SL_2(C)$ are $\{I\}$ and $Z = \{\pm I\}$. See Appendix IV for a proof of this standard fact.

Appendix I

Theorem. *If X is countably infinite, then the quotient group $\mathsf{Sym}\, X/\,\mathsf{FinSym}\, X$ is simple.*

Before proceeding with the proof, note that every permutation of X is a product of disjoint cycles, just as in the finite case. Moreover every cycle is either finite or infinite in length. For example, the permutation $\pi \in \mathsf{Sym}\,\mathbb{Z}$ defined by

$$\pi(n) = \begin{cases} n+5, & \text{if } n \not\equiv 0 \mod 5; \\ -n, & \text{if } n \in \{\pm 5, \pm 10, \pm 15\}; \\ n, & \text{otherwise} \end{cases}$$

has infinitely many fixed points, three cycles of length 2, and four infinite cycles. This we express symbolically as $\pi \vdash (1)^\infty(2)^3(\infty)^4$. Similarly, we write $\pi \vdash \prod_i (n_i)^{m_i}$ to indicate that $\pi \in \mathsf{Sym}\, X$ has $m_i \in \{0, 1, 2, 3, \ldots\} \cup \{\infty\}$ cycles of length $n_i \in \{1, 2, 3, \ldots\} \cup \{\infty\}$. Here '$\infty$' means countably infinite, assuming X is countably infinite; so actually ∞ means $\aleph_0$ here.

Also, two permutations $\beta, \gamma \in \mathsf{Sym}\, X$ are conjugate iff they have the same cycle structure, meaning that they have the same number of cycles of each length (i.e. the same number of cycles of length n for each positive integer n, and the same number of cycles of infinite length).

Our proof of the theorem above is in three steps:

(1) We first show that there exists $\pi \in N$ such that $\pi \vdash (1)^\infty(\infty)^2$.
(2) Next we show that for every $m \in \{0, 1, 2, 3, \ldots\} \cup \{\infty\}$, there exists $\pi \in N$ such that $\pi \vdash (1)^m(2)^\infty$.
(3) Finally, we show that $N = \mathsf{Sym}\, X$.

Since $\alpha \in N$ has infinite support, it is easy to partition X into three disjoint infinite subsets as $X = A \sqcup B \sqcup C$ where $A = \{a_n : n \in \mathbb{Z}\}$, $B = \{b_n : n \in \mathbb{Z}\}$ and $C = \{c_n : n \in \mathbb{Z}\}$ such that $\alpha(a_n) = b_n$ for all n. Let $\rho \in \mathsf{Sym}\, X$ be the infinite cycle mapping $a_n \mapsto a_{n+1}$ for each $n \in \mathbb{Z}$, and fixing all other points of X, i.e. $\rho(b_n) = b_n$ and $\rho(c_n) = c_n$. Since N is a normal subgroup containing α, it also contains $\beta = \alpha(\rho\alpha^{-1}\rho^{-1})$. But β maps $a_n \mapsto a_{n-1}$, $b_n \mapsto b_{n+1}$, $c_n \mapsto c_n$ so $\beta \vdash (1)^\infty(\infty)^2$. This proves (1).

Once again let $X = A \sqcup B \sqcup C$ be a partition into three infinite subsets with $A = \{a_n : n \in \mathbb{Z}\}$, $B = \{b_n : n \in \mathbb{Z}\}$ and $C = \{c_n : n \in \mathbb{Z}\}$. By (1) and the fact that N is normal, N contains every permutation of type $(1)^\infty(\infty)^2$. So $\gamma, \delta \in N$ where γ maps $a_n \mapsto a_{n+1}$, $b_n \mapsto b_{n+1}$ and $c_n \mapsto c_n$; and δ maps $a_n \mapsto b_{n-1}$, $b_n \mapsto a_{n-1}$ and $c_n \mapsto c_n$. Then $\gamma\delta \in N$ which interchanges $a_n \leftrightarrow b_n$ and maps $c_n \mapsto c_n$, so $\gamma\delta \vdash (1)^\infty(2)^\infty$.

Now it only remains to verify (2) in the case that m is a positive integer. In this case we partition $X = A \sqcup B \sqcup C$ where $|A| = |B| = \infty$ and $|C| = m$. By the previous paragraph, there exist permutations $\alpha, \beta \in N$ such that α fixes every point of $B \sqcup C$,

and is a product of disjoint 2-cycles on A; also β fixes every point of $A \sqcup C$, and is a product of disjoint 2-cycles on B. Then $\alpha\beta \in N$ with $\alpha\beta \vdash (1)^m(2)^\infty$. So (2) holds for all $m \in \{0, 1, 2, 3, \ldots\} \cup \{\infty\}$.

Finally, let $\pi \in \mathsf{Sym}\, X$, and let $X = \bigsqcup_n X_n$ be the partition into orbits of $\langle\pi\rangle$. (Here the orbits do not necessarily have distinct lengths; if m_i is the number of orbits X_n having length $|X_n| = i$, then $\pi \vdash (i)^{m_i}$.) Expressing π as a product of disjoint cycles, we have $\pi = \prod_i \pi_i$ where π_i cycles just the points of X_i. We may write $\pi_i = \alpha_i\beta_i$ where $\alpha_i, \beta_i, \pi_i \in \mathsf{Sym}\, X_i$ with $\alpha_i^2 = \beta_i^2 = \pi_i^{|X_i|} = 1$.

Here you should first consider the case $i \in \{3, 4, 5, \ldots\}$ and view X_i as the vertex set of a regular $|X_i|$-gon. Here $\langle\alpha_i, \beta_i\rangle$ is the dihedral symmetry group of the regular polygon, generated by two reflections α_i and β_i, and having $\alpha_i\beta_i = \pi_i$ as a rotational syummetry. If $|X_i| = 2$ then instead $\mathsf{Sym}\, X_i = \{\alpha_i, \beta_i\}$ where $\alpha_i = 1$ and $\beta_i = \pi_i$ transposes the two points in X_i. If $|X_i| = 1$ then $\alpha_i = \beta_i = \pi_i$ is the identity permutation of the singleton set X_i. If $|X_i| = \infty$ then once again the infinite cycle π_i has the required form $\pi_i = \alpha_i\beta_i$ in the infinite dihedral group $\langle\alpha_i, \beta_i\rangle$. (Up to equivalence here, we may take $X_i = \mathbb{Z}$, $\pi_i(x) = x+1$, $\alpha_i(x) = 1-x$, $\beta_i(x) = -x$.)

Note that $\pi = \prod_i \pi_i = \alpha\beta$ where $\alpha = \prod_i \alpha_i$ and $\beta = \prod_i \beta_i$. Note that α_i commutes with β_j whenever $i \neq j$, since their supports are disjoint. Also note that $\alpha, \beta \in N$ since they have cycle structure as in (2). So $\pi = \alpha\beta \in N$ as required. □

Appendix II

Theorem. *Let F be a field. The group $SL_2(F)$ is generated by $S := \{h_\lambda, h_\lambda^T : \lambda \in F\}$ where $h_\lambda = \left[\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right]$.*

First Proof. Let $g = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in SL_2(F)$. We show that $g \in \langle S\rangle$, in three cases.

Case (i). If $a = 0$, then $bc = -1$ and $g = h_b h_c^T h_{1-bd} \in \langle S\rangle$.

Case (ii). If $c = 0$, then $g = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & -d \\ a & b \end{smallmatrix}\right] \in \langle S\rangle$ by case (i).

Case (iii). Otherwise $ac \neq 0$ and $h_{-a/c}g$ has first entry zero so $h_{-a/c}g \in \langle S\rangle$ by case (i). This gives $g \in \langle S\rangle$ as required. □

Second Proof. The group $G := SL_2(F)$ permutes the nonzero vectors of F^2. The vectors $u = (1, 0)^T$ and $v = (0, 1)^T$ have stabilizers $G_u = \{h_\lambda : \lambda \in F\}$ and $G_v = \{h_\lambda^T : \lambda \in F\}$ respectively. Let $H = \langle G_u, G_v\rangle$; we must show that $H = G$. The crux of this argument is to show that H permutes the nonzero vectors in F^2 transitively. The orbit $Hv = \{hv : h \in H\}$ contains all vectors of the form $h_\lambda v = (\lambda, 1)^T$, $\lambda \in F$. Now if $\lambda \neq 0$ and $\nu \in F$, then $h^T_{(\nu-1)/\lambda}(\lambda, 1)^T = (\lambda, \nu)^T \in Hv$. Finally, if $0 \neq \nu \in F$, then $(0, \nu)^T = h_1(-\nu, \nu)^T \in Hv$. So Hv is the set of all nonzero vectors in F^2, i.e H permutes the nonzero vectors in

F^2 transitively. By the Frattini Argument (Appendix III), $G = G_u H = G_u\langle G_u, G_v\rangle \leqslant \langle G_u, G_v\rangle = H \leqslant G$. The desired conclusion $H = G$ follows. □

Appendix III

The following argument, shown in class, is 'enormously useful' as Robinson says; and not just in the limited context of Sylow theory where the textbook refers to it.

Theorem (Frattini Argument). *Suppose G permutes a set X, with a transitive subgroup $H \leqslant G$. Then for every point $x \in X$, we have $G = G_x H = HG_x$.*

Proof. Of course $G_x H \subseteq G$; our job is to prove the reverse inclusion. Let $g \in G$, and denote $y = g(x) \in X$. Since H permutes X transitively, there exists $h \in H$ such that $h(y) = x$. Now $(hg)(x) = h(y) = x$, so $hg \in G_x$ and $g = h^{-1}\cdot hg \in HG_x$. This gives $G = HG_x$; and taking inverses on both sides gives $G_x H = G$. □

Appendix IV

The group $PSL_2(F)$ is simple whenever $|F| \geqslant 4$. Here is a proof when $F = \mathbb{C}$, and the general case is almost as easy.

Theorem. *Let $Z \lhd K \leqslant SL_2(\mathbb{C})$ where $Z = \{\pm I\}$ (note: K is a normal subgroup which properly contains Z). Then $K = SL_2(\mathbb{C})$. In other words, the group $PSL_2(\mathbb{C})$ is simple.*

Proof. Let $g \in K$, $g \notin Z$. The characteristic polynomial of g is $t^2 - 2at + 1$ for some $a \in \mathbb{C}$. There are three cases to consider:

(i) $a^2 \neq 1$ and g is similar to $D := \left[\begin{smallmatrix} d^{-1} & 0 \\ 0 & d \end{smallmatrix}\right]$, $d + d^{-1} = 2a$, $d \notin \{0, \pm 1\}$. Since g has two distinct eigenvalues, there exists $A \in GL_2(\mathbb{C})$ whose columns form a basis of $\mathbb{C}^2$ consisting of corresponding eigenvectors for g. After scaling these eigenvectors if necessary, we may further assume $A \in SL_2(\mathbb{C})$. Now $g = ADA^{-1}$. Since $K \leqslant SL_2(\mathbb{C})$, we obtain $D \in K$. Also given $\lambda \in \mathbb{C}$, the matrix $B = \left[\begin{smallmatrix} d^{-1} & d\lambda \\ 0 & d \end{smallmatrix}\right]$ has characteristic polynomial $t^2 - 2at + 1$; it is similar to D and the same argument gives $B \in K$. So $DB = \left[\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right] \in K$. A similar argument gives $\left[\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right] \in K$, So $K = SL_2(\mathbb{C})$ by Appendix II. In this case we are done.

(ii) $a = 1$ and g is similar to $B = \left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right]$, $b \neq 0$. Using similarity as in the previous case, we get $B \in K$. Let $0 \neq \lambda \in \mathbb{C}$. Conjugating by $D = \left[\begin{smallmatrix} d^{-1} & 0 \\ 0 & d \end{smallmatrix}\right]$ where $d = \pm\sqrt{\lambda/b}$, we obtain $DBD^{-1} = \left[\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right] \in K$ since K is normal. Also, $\left[\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right] \in K$. As before, $K = SL_2(\mathbb{C})$ and we are done.

(iii) $a = -1$ and g is similar to $B = \left[\begin{smallmatrix} -1 & b \\ 0 & -1 \end{smallmatrix}\right]$, $b \neq 0$. Using similarity as before, $B \in K$. So $B^2 = \left[\begin{smallmatrix} 1 & -2b \\ 0 & 1 \end{smallmatrix}\right] \in K$. The result follows from case (ii). □