7 Broader Classes of Groups

11/28: 1. Suppose that $\mathbb{Z}/m\mathbb{Z}$ is a subgroup of S_n for some $n, m > 2$. Prove that D_{2m} is also a subgroup of S_n.

Proof. m divides $n!$. $n!/m$ is still divisible by 2? $1 \in \mathbb{Z}/m\mathbb{Z}$ functions as r; we just need to prove the existence of an order 2 element in $S_n \setminus \mathbb{Z}/m\mathbb{Z}$.

Take a 2-Sylow of S_n? Characterize that.

Since $n > 2$ and $|S_n| = n!$, $2 \big| |S_n|$. Thus, by Sylow I, there exists a 2-Sylow $P \in S_n$. Suppose $P = \langle x \rangle$. ☐

2. Let $G = \mathrm{SL}_2(\mathbb{F}_3)$. Prove that the subgroup

$$H = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \right\rangle$$

is isomorphic to the quaternion group Q (where i, j, k map to the given matrices). Deduce that $\mathrm{SL}_2(\mathbb{F}_3)$ and S_4 are not isomorphic.

Proof. Define $\phi : Q \to H$ by

$$i \mapsto \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \qquad j \mapsto \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad k \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

We need not explicitly define matrix images for entries beyond i, j, k since these three elements generate Q. Thus, ϕ is bijective; it only remains to be seen that it is a homomorphism. Fortunately, we can verify the multiplication table as follows (remember that addition everything is mod 2 here in a sense!).

$$\underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)} \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)} = -\underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)} \underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)} = \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)}$$

$$\underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)} \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)} = -\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)} \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)} = \underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)}$$

$$\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)} \underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)} = -\underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)} \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)} = \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)}$$

$$\underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}^2}_{\phi(i)^2} = \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^2}_{\phi(j)^2} = \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2}_{\phi(k)^2} = -\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{\phi(e)}$$

Suppose for the sake of contradiction that $S_4 \cong \mathrm{SL}_2(\mathbb{F}_3)$ with isomorphism $\psi : S_4 \to \mathrm{SL}_2(\mathbb{F}_3)$. $D_8 \leq S_4$ and $H \leq \mathrm{SL}_2(\mathbb{F}_3)$ are both 2-Sylows in their respective groups. Thus, by Sylow II, $\psi(D_8)$ and H are conjugate to each other. But as discussed in class, the $Q \not\approx D_8$, a contradiction. ☐

3. Let G be a group, and let $N \subset G$ be the subgroup generated by the elements $xyx^{-1}y^{-1}$ for all pairs $x, y \in G$. Prove that N is a normal subgroup, and that G/N is abelian.

Proof. To prove that N is normal, it will suffice to show that for all $z \in N$ and $g \in G$, $gzg^{-1} \in N$. Let $x^{-1}y^{-1}xy \in N$ and $g \in G$ be arbitrary. Then

$$\begin{aligned} gx^{-1}y^{-1}xyg^{-1} &= gx^{-1}(g^{-1}g)y^{-1}(g^{-1}g)x(g^{-1}g)yg^{-1} \\ &= (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) \\ &= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \\ &\in N \end{aligned}$$

as desired.

To prove that G/N is abelian, it will suffice to show that $gN * hN = hN * gN$ for all $g, h \in G$. To do so, we can show that $ghN = hgN$, or that $g^{-1}h^{-1}ghN = N$. But since an element of the form $g^{-1}h^{-1}gh \in N$ by definition, we have the desired result. □

4. Compute the order of the following groups as well as a set of generators.

   (a) The centralizer of (12345) in A_7.

   (b) The centralizer of $((12), (123))$ in $S_5 \times S_5$.

   Proof. Order: We have that $|\{(12)\}| = 10$ in S_5 and $|\{(123)\}| = 20$ in S_5. Thus, $|\{(12), (123)\}| = 10 \cdot 20 = 200$ in S_5^2. It follows that

$$\begin{aligned} |S_5^2| &= |\{(12), (123)\}| \cdot |C_G(((12), (123)))| \\ 5!^2 &= 200|C_G(((12), (123)))| \\ \boxed{|C_G(((12), (123)))| = 72} \end{aligned}$$

□

   (c) The normalizer of $H = \langle (12), (34), (56), (78) \rangle$ in S_8.

   Proof. We observe: Image of (12) under conjugation by an element of $N_{S_8}(H)$ must be (12), (34), (56), or (78). Conjugation preserves cycle structure. These are the only 2-cycles in H, so conjugation on H needs to take them to each other. Main point: The set of generators needs to go to the set of generators. Think about what sorts of relabelings will do these kinds of things and which will be possible in the normalizer. □

5. **Projective Linear Groups Over Finite Fields.** Let p be prime, and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Note that one can add and multiply elements of $\mathbb{F}_p$. Let $\mathrm{GL}_2(\mathbb{F}_p)$ be the group of 2×2 invertible matrices over $\mathbb{F}_p$, and let $\mathrm{SL}_2(\mathbb{F}_p) \subset \mathrm{GL}_2(\mathbb{F}_p)$ denote the subgroup of matrices of determinant one.

   (a) There are $p^2 - 1$ non-zero vectors $v \in \mathbb{F}_p^2$. Let a "line" $\ell = [v] \subset \mathbb{F}_p^2$ denote the scalar multiples λv of a non-zero vector v. Prove that the set X of lines has cardinality $|X| = p + 1$.

   Proof. Let $\mathbb{F}_p \circlearrowright \mathbb{F}_p^2$. □

   (b) Prove that $\mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{GL}_2(\mathbb{F}_p)$ act naturally on X by $g \cdot [v] = [g \cdot v]$.

   Proof. Let $G = \mathrm{GL}_2(\mathbb{F}_p)$. Define $G \circlearrowright X$ by left multiplication. To confirm that this is a group action, it will suffice to show that for all $g, h \in G$ and $[v] \in X$, $g \cdot (h \cdot [v]) = gh \cdot [v]$ and for all $[v] \in X$, $e \cdot [v] = [v]$. With respect to the first statement, we have since g, h are linear that

$$g \cdot (h \cdot [v]) = g \cdot [hv] = [ghv] = gh \cdot [v]$$

   With respect to the latter statement,

$$e \cdot [v] = [ev] = [v]$$

   as desired.

   An analogous argument can treat the $\mathrm{SL}_2(\mathbb{F}_p)$ case. □

   (c) Prove that this action is transitive for both $\mathrm{GL}_2(\mathbb{F}_p)$ and $\mathrm{SL}_2(\mathbb{F}_p)$.

   Proof. Suppose $gu = v$, then $g = vu^{-1}$. □

   (d) Prove that the kernel of the action consists precisely of the scalar matrices λI in either $\mathrm{SL}_2(\mathbb{F}_p)$ or $\mathrm{GL}_2(\mathbb{F}_p)$.

Proof. Let λI be a scalar matrix. Then

$$\lambda I \cdot [v] = [\lambda v] = [v]$$

Similarly, if $g \cdot [v] = [v]$ and $g \cdot [u] = [u]$ for $u \neq v \in \mathbb{F}_p$, then $gv = \lambda v$ for some λ and $gu = \lambda u$ as well, i.e., $g = \lambda I$. ☐

(e) Let $\mathrm{PGL}_2(\mathbb{F}_p)$ and $\mathrm{PSL}_2(\mathbb{F}_p)$ denote the quotient of G and H by the subgroup of scalar matrices. Prove that $|\mathrm{PGL}_2(\mathbb{F}_p)| = (p^2-1)p$ and $|\mathrm{PSL}_2(\mathbb{F}_p)| = 6$ if $p = 2$ and $\frac{1}{2}(p^2-1)p$ otherwise.

Proof. We know from HW3 Q6 that $|G| = (p^2-1)(p^2-p)$. Additionally, since there are $p-1$ scalar matrices (λI for $\lambda = 1, \dots, p-1$), we have by the corollary from Lecture 3.3 that

$$|\mathrm{PGL}_2(\mathbb{F}_p)| = \frac{|G|}{|\lambda I|} = \frac{(p^2-1)p(p-1)}{p-1} = (p^2-1)p$$

☐

(f) Prove that $\mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) = S_3$.

(g) Prove that $\mathrm{PGL}_2(\mathbb{F}_3) = S_4$ and $\mathrm{PSL}_2(\mathbb{F}_3) = A_4$. (Compare with Question 2.)

(h) Prove that $\mathrm{PSL}_2(\mathbb{F}_5) = A_5$ and $\mathrm{PGL}_2(\mathbb{F}_5) = S_5$. (Hint: Using that A_6 is simple, prove that any index 6 subgroup of A_6 or S_6 is A_5 or S_5, respectively.)

Proof. Any index 6 subgroup of A_6 or S_6 is A_5 or S_5, respectively. Let $H \subset A_6$ be such that $[A_6 : H] = 6$. Then A_6/H has 6 elements. Let $H \circlearrowright A_6/H$ by left multiplication. This is transitive because we can always sent the identity coset H to any other coset. Recall that any group action on n elements induces a homomorphism from the group to S_n. Thus, we have a homomorphism from A_6 to S_6 (since A_6/H has 6 elements). This is not necessarily the usual injection; it could be very different. Let's call this map $\varphi : A_6 \to S_6$. A priori, φ need not be injective. Injectivity iff $A_6 \circlearrowright A_6/H$ is faithful. But in this case, φ is injective! Since A_6 is simple, $\ker\varphi = A_6$ or $\ker\varphi = \{e\}$. But it's not A_6 (stuff is being moved around??), so it's e. Therefore, $A_6 \circlearrowright A_6/H$ is faithful and φ gives an injection of A_6 in S_6. Restrict attention to $h \subset A_6$. $\varphi|_H : H \to S_6$ is injective. $H \circlearrowright A_6/H$, H fixes the identity coset. Therefore, H permutes the other five (nonidentity) cosets. But this gives an action of H on *five* elements. Indeed, the image $\varphi|_H(H) = S_5$. $\varphi|_H : H \to S_5$ is injective. Recap: H acts on 6 elements, but since every element of H fixes one of the six elements, then its really permuting five elements. The action $H \circlearrowright A_6/H \setminus \{H\}$ is faithful (fixes non-identity cosets implies fixes all cosets). When did we argue that $H \circlearrowright A_6/H$ faithfully? Recall that $A_6 \circlearrowright A_6/H$ faithfully because of simplicity. Now we look at the restriction $H \circlearrowright A_6/H$ to the subgroup $H \leq A_6$. This will also naturally be faithful. Lastly, $H \circlearrowright A_6/H \setminus \{H\}$ is faithful since if $h \in H$ fixes all five nonidentity cosets, then we already know h fixes H (identity coset), so h fixes all six cosets A_6/H since $H \circlearrowright A_6/H$ is faithful. So since $\psi : H \to S_5$ is injective, we have

$$|H| = \frac{|A_6|}{6} = \frac{6!/2}{6} = \frac{360}{6} = 60$$

Then $[S_5 : \psi(H)] = 2$, so $\psi(H) = A_5$ and $H \cong A_5$. What about $S_5 \subset S_6$? Idea: Can do a similar strategy, except "kernel is e or A_6" should be replaced with "kernel is e, A_6, or S_6." What Abhijit means by similar strategy: Suppose $[S_6 : H] = 6$. Then $S_6 \circlearrowright S_6/H$. Use the simplicity of A_6 even in the S_6 case.

Look at the action on the lines faithfully. Something with a group action and counting can help. Prove something is always a normal subgroup. Circumvents the hint. ☐