Homework 9

Due Monday, April 20th

Recall the following important Lemma from the April 8th lecture.

Lemma 1. *Let G be a finite group, and $H \trianglelefteq G$ a normal subgroup. Let $P \leq H$ be a Sylow p subgroup of H. If $P \trianglelefteq H$ then $P \trianglelefteq G$.*

We noted in class that this feels like a normal Sylow subgroup is somehow *strongly* normal, in such a way that we get transitivity of normal subgroups. The following definition makes this precise.

Definition 1 (Characteristic Subgroups)**.** *A subgroup $H \leq G$ is called characteristic in G if for every automorphism $\varphi \in \operatorname{Aut} G$, we have $\varphi(H) = H$. This is denoted by $H \operatorname{char} G$.*

1. Let's prove some basic facts about characteristic subgroups and use them to prove Lemma 1.

   (a) Show that characteristic subgroups are normal. That is, if $H \operatorname{char} G$ then $H \trianglelefteq G$.

   Proof. Fix $g \in G$. Then $x \mapsto gxg^{-1}$ is an automorphism of G. In particular, it fixes H. Thus $gHg^{-1} = H$ and H is normal. □

   (b) Let $H \leq G$ be the unique subgroup of G of a given order. Then $H \operatorname{char} G$.

   Proof. Let $\varphi \in \operatorname{Aut}(G)$. Then $\varphi(H) \leq G$ is a subgroup of G isomorphic to H. In particular $|\varphi(H)| = |H|$. Since H is the unique subgroup of G with that order, we have that $\varphi(H) = H$. But φ was arbitrary, so $H \operatorname{char} G$. □

   (c) Let $K \operatorname{char} H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$. (This is the transitivity statement alluded to, and justifies the feeling that a characteristic subgroup is somehow *strongly normal*).

   Proof. Fix $g \in G$. The normality of H implies that $gHg^{-1} = H$, so that conjugation by g induces an automorphism of H. Since K is fixed by automorphisms of H, this means $gKg^{-1} = K$. But $g \in G$ was arbitrary, so K is normal in G. □

   (d) Let G be a finite group and P a Sylow p-subgroup of G. Show that $P \trianglelefteq G$ if and only if $P \operatorname{char} G$.

   Proof. If $P \operatorname{char} G$ then P is normal by part (a). Conversely, if P is a normal p-Sylow subgroup of G, it is the unique p-Sylow subgroup of G, so that it is the unique subgroup of G with order $|P|$. By part (b) then $P \operatorname{char} G$. □

   (e) Put all this together to deduce Lemma 1.

   Proof. Let $P \leq H \trianglelefteq G$ as in the statement of the Lemma. If $P \trianglelefteq H$ then by part (d) we have $P \operatorname{char} H$. Therefore by part (c) $P \trianglelefteq G$, completing the proof. □

2. Recall from HW7 exercise 5 the definition of the subgroup $SL_n(F) \leq GL_n(F)$, which consists of matrices whose determinant is 1. Let's use the tools we've developed to study $SL_2(\mathbb{F}_3)$.

   (a) Compute the order of $SL_2(\mathbb{F}_3)$ (*cf.* HW7 problem 5e).

Proof. By HW7 5e the order is $3^3 - 3 - 1 = 24$. □

(b) Show that the matrices:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

generate a subgroup $H \leq SL_2(\mathbb{F}_3)$ which is isomorphic to Q_8.

Proof. Denote the first matrix by A and the second by B. We show that the map $\varphi : Q_8 \to \langle A, B\rangle$ given by the rule $\varphi(i) = A$ and $\varphi(j) = B$ is an isomorphism. Since the generators are in the image of φ, it suffices to show it is an injective homomorphism and surjectivity will follow. To show it is a homomorphism it suffices to show that A and B satisfy the relations from Takehome 2 problem 1(b). We will use the relations $i^2 = j^2 = -1$ and $ij = -ji$ noting that -1 corresponds to $-I$ where I is the identity matrix in $SL_2(\mathbb{F}_3)$. One readily checks that $A^2 = -I$. For B^2 we use that $2 \equiv -1 \mod 3$, that is:

$$B^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \equiv -I \mod 3.$$

Then we compute:

$$AB = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \quad , \quad BA = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}.$$

Injectivity follows because we just observed i, j, ij don't map to I, and neither do their negatives. Since -1 maps to $-I$, the kernel is strictly $1 \in Q_8$. □

(c) Conclude (*cf.* takehome 2 problem 3) that $SL_2(\mathbb{F}_3)$ and S_4 are 2 nonisomorphic groups of the same order. (We point out that this is in contrast to $GL_2(\mathbb{F}_2)$ being isomorphic to S_3.)

Proof. By Takehome 2 problem 3, S_4 doesn't contain any subgroups isomorphic to Q_8. Since $SL_2(\mathbb{F}_3)$ does, they cannot be isomorphic. Therefore S_4 and $SL_2(\mathbb{F}_3)$ are two isomorphic groups of order 24. □

(d) Compute the number of Sylow 3-subgroups of $SL_2(\mathbb{F}_3)$.

Proof. $24 = 2^3 * 3$. So $n_3 = \{1, 4, 7, \cdots\}$ must divide 8, so either $n_3 = 1$ or $n_3 = 4$. We will show that $n_3 = 4$, noting that all we have to do is exhibit 2 different subgroups of order 3, as the Sylow 3-subgroups have order 3 so this will show $n_3 > 1$. To exhibit a group of order 3 it suffices to produce an element of order 3. For example:

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then we compute:

$$M^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad , \quad M^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \equiv I \mod 3.$$

So $\langle M \rangle$ is a Sylow 3-subgroup. But symmetrically, we see that:

$$N = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

also has order 3, and we observe that $N \notin \langle M \rangle$. Thus $\langle N \rangle$ is a distinct Sylow 3-subgroup from M. Thererefore $n_3 \geq 2$, so that $n_3 = 4$.

We remark that it would have also sufficed to check explicitly that M is not normal, so that it cannot be the unique Sylow 3-subgroup. □

(e) Show that the subgroup defined in part (b) is the unique Sylow 2-subgroup of $SL_2(\mathbb{F}_3)$. (Hint, use a counting argument together with part (d)).

Proof. First let's point out that by part (d), we know that $SL_2(\mathbb{F}_3)$ has 8 distinct elements of order 3 (2 for each Sylow 3-subgroup).

The subgroup $\langle A, B \rangle$ defined in part (b) has order 8, so it is a Sylow 2-subgroup of $SL_2(\mathbb{F}_3)$. Therefore it is normal if and only if $n_2 = 1$ By Sylow's theorem we know n_2 is odd, and also that it divides 3. So there are either 1 or 3 Sylow 2-subgroups. I claim that if there are 3 this gives us at least 16 elements of $SL_2(\mathbb{F}_3)$ of 2 power order. We first remark that together with the 8 elements of order 3, this gives us 24 elements of $SL_2(\mathbb{F}_3)$ that have order either a power of 2 or precisely 3 (this includes the identity matrix of order 2^0). But arguing as in part (d), the matrix:

$$\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$$

has order 6, which is neither a power of 2 or 3. This is a contradiction since the group only has 24 elements one of which must be the identity. We have therefore reduced to proving the following lemma.

Lemma 2. *If a group G is a group of order 24 with 3 distinct Sylow 2 subgroups H_1, H_2, H_3, $|H_1 \cup H_2 \cup H_3| \geq 16$.*

Proof. We first notice that by the inclusion exclusion principle

$$|H_1 \cup H_2 \cup H_3| = |H_1| + |H_2| + |H_3| - |H_1 \cap H_2| - |H_2 \cap H_3| - |H_1 \cap H_3| + |H_1 \cap H_2 \cap H_3|.$$

We remark that this is not a group theoretic fact, but a set theoretic one, and is easily seen by considering, for example, a venn diagram. By Lagrange's theorem, we see that for $i \neq j$, we have $|H_i \cap H_j| \leq 4$. Substituting this into the above equation give the inequality:

$$|H_1 \cap H_2 \cap H_3| \geq 8 + 8 + 8 - 4 - 4 - 4 + |H_1 \cap H_2 \cap H_3| = 12 + |H_1 \cap H_2 \cap H_3|.$$

Thus it suffices to show that $|H_1 \cap H_2 \cap H_3| \geq 4$. Notice that G acts on the set of Sylow 2-subgroups $\{H_1, H_2, H_3\}$ by conjugation. The kernel of this action is are elements which fix each H_i when conjugating, thus are precisely the intersection of the normalizers of the H_i. Now observe that:

$$H_i \leq N_G(H_i) \leq G.$$

By Lagrange's theorem then $|N_G(H_i)|$ is divisible by 8 and divides 24, so it is 8 or 24. If it is 24 then H_i is normal, contradicting that $n_2 = 3$ Thus $N_G(H_i) = H_i$. In particular, we see the kernel of the action is:

$$N_G(H_1) \cap N_G(H_2) \cap N_G(H_3) = H_1 \cap H_2 \cap H_3.$$

Translating this to the permutation representation, and applying the first isomorphism theorem gives the following diagram:

$$\begin{tikzcd} G \arrow[r] \arrow[d] & S_3 \\ \frac{G}{H_1 \cap H_2 \cap H_3} \arrow[ur, hook] & \end{tikzcd}$$

In particular, applying Lagranges theorem, $|G|/|H_1 \cap H_2 \cap H_3|$ must divide the order of S_3. So $24/|H_1 \cap H_2 \cap H_3|$ divides 6. Thus $|H_1 \cap H_2 \cap H_3|$ must be greater than or equal to 4, and we are done. □

□

(f) Show that $Z(SL_2(\mathbb{F}_3)) = \{\pm I\}$ where I is the identity matrix. (You will need to use what you learned in parts (d) and (e) together with the computation of $Z(Q_8)$ from the takehome).

Proof. It's clear that $\{\pm I\} \leq Z(SL_2(\mathbb{F}_3)$. Conversely, fix $X \in SL_2(\mathbb{F}_3)$. Notice that X has order dividing 24, so its order is $2^\alpha * 3^\beta$. If $\beta \neq 2$, then X^{2^α} has order 3. If X were in the center, so is X^{2^α}, and so the Sylow 3-subgroup it generates must be normal, contradicting part (d). So for X to be in the center, it must have order a power of 2. Then by Sylow's theorem, we have $X \in \langle A, B \rangle$ the unique Sylow 2-subgroup, and if it in the center of $SL_2(\mathbb{F}_3)$., it must be in the center of $\langle A, B \rangle$ as well. In Takehome 2 part 1g we computed this to be ± 1, so that $X = \pm I$, completing the proof. □

(g) Prove that $SL_2(\mathbb{F}_3)/Z(SL_2(\mathbb{F}_3)) \cong A_4$. (Hint: Use what we know about groups of order 12).

Proof. Denote the quotient group by $\overline{G}$. By part (f) we know it has order 12. We've shown that a group of order 12 either has a normal subgroup of order 3, or it is isomorphic to A_4. So assume for the sake of contradiction that $|\overline{G}|$ has a normal subgroup of order 3, say $\overline{H}$. Then by the fourth isomorphism theorem, there is a subgroup $H \trianglelefteq SL_2(\mathbb{F}_3)$ containing $\{\pm I\}$, whose quotient by $\{\pm I\}$ is $\overline{H}$. In particular, H is a subgroup of order $6 = 2 * 3$. Using our classification of groups of order pq, we know that H has a normal Sylow 3-subgroup P. By problem 1, $P \operatorname{char} H \trianglelefteq SL_2(\mathbb{F}_3)$, so that $P \trianglelefteq SL_2(\mathbb{F}_3)$. This contradicts part (d). □

3. Next lets poke and prod $GL_2(\mathbb{F}_p)$.

(a) Recall the order of $GL_2(\mathbb{F}_p)$ from HW7 problem 4(d). What is the maximal p divisor of $|GL_2(\mathbb{F}_p)|$?

Proof. $p^4 - p^3 - p^2 + p = p(p^3 - p^2 - p + 1)$ and since the second term is one more than a multiple of p, p cannot divide it. So the maximal p divisor of $|GL_2(\mathbb{F}_p)|$ is p itself. □

(b) The subset of *upper triangular matrices* of $GL_2(\mathbb{F}_p)$ is:

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{F}_p) \right\}.$$

The subset of *strictly upper triangular matrices* is:

$$\overline{T} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_p) \right\}.$$

Show that T and $\overline{T}$ are subgroups of $GL_w(\mathbb{F}_p)$. We will see that they are not normal.

Proof. To show T is a subgroup notice:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & dz \end{pmatrix} \in T,$$

and applying HW 7 problem 3c

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \frac{1}{ad} \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \in T.$$

Similarly, to show that $\overline{T}$ is a subgroup notice:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} \in \overline{T},$$

and

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -b & 0 & 1 \end{pmatrix} \in \overline{T}.$$

□

(c) Show that $\overline{T}$ is a Sylow p-subgroup of $GL_2(\mathbb{F}_p)$ and of T.

Proof. It's straightforward to see that $|\overline{T}| = p$, which shows the first statement applying part (a). By Lagrange's theorem, p divides the order of T, which divides the order of $GL_2(\mathbb{F}_p)$, so that p is a maximal p divisor of $GL_2(\mathbb{F}_p)$, proving the second statement. □

(d) Show that $GL_2(\mathbb{F}_p)$ has $p+1$ Sylow p-subgroups (Hint: you only need to exhibit one more than you already have). Conclude that $\overline{T}$ is not normal in $GL_2(\mathbb{F}_p)$.

Proof. Sylow's theorem says that $n_p = |GL_2(\mathbb{F}_p) : N(\overline{T})|$, so we begin by computing the normalizer of $\overline{T}$. Since $\overline{T}$ is cyclic generated by

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

the normalizer of $\overline{T}$ is precisely the elements which conjugate g an element of $\overline{T}$. Let's conjugate g.

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \frac{1}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \frac{1}{ad-bc} \begin{pmatrix} ad-bc-ad & a^2 \\ c^2 & ad-bc-ac \end{pmatrix} \end{aligned}$$

If this is in $\overline{T}$ then $c = 0$, and conversely, if $c = 0$ then this is:

$$\frac{1}{ad}\begin{pmatrix} ad & a^2 \\ 0 & ad \end{pmatrix} = \begin{pmatrix} 1 & a^2 \\ 0 & 1 \end{pmatrix} \in \overline{T}.$$

So the normalizer of $\overline{T}$ is precisely T. Then one can compute $|T| = (p-1)^2 * p$, noticing that the matrix having a, d can be any nonzero element of $\mathbb{F}_p$, and b can be any element of $\mathbb{F}_p$. Thus:

$$n_p = |GL_2(\mathbb{F}_p) : T| = \frac{p(p-1)^2(p+1)}{p(p-1)^2} = p + 1.$$

□

(e) Show that $\overline{T} \trianglelefteq T$.

Proof. We proved this in the previous section when computing the normalizer of $\overline{T}$. □

(f) Conclude that T is not normal in $GL_2(\mathbb{F}_p)$. (Hint: use Lemma 1).

Proof. By part (c) and (e) we see that $\overline{T}$ is the unique Sylow p-subgroup of T, so that $\overline{T}\operatorname{char}T$. If $T \trianglelefteq GL_2(\mathbb{F}_p)$, then by Lemma 1 $\overline{T} \trianglelefteq GL_2(\mathbb{F}_p)$, contradicting part (d). □

4. Let's study $SL_2(\mathbb{F}_4)$. SKIP THIS PROBLEM

   (a) Compute the order of $SL_2(\mathbb{F}_4)$.

   (b) Give 2 subgroups of order 5 in $SL_2(\mathbb{F}_4)$

   (c) Conclude that $SL_2(\mathbb{F}_4)$ is simple and isomorphic to A_5.

5. Next let's study the dihedral group.

   (a) Let P be a Sylow 2-subgroup of D_{2n}. Show that $N_{D_{2n}}(P) = P$.

Proof. We prove (a) and (b) simultaneously. We begin with the following lemma.

Lemma 3. *Let G be a finite group and $N \trianglelefteq G$ a normal subgroup. If $P \leq G$ is Sylow p-subgroup of G, then $P \cap N \leq N$ is a Sylow p-subgroup of N.*

Proof. Note that PN is a group and $P \leq PN$. Notice that P is a p-Sylow subgroup of PN. Indeed, if $|G| = p^\alpha m$ with p not dividing m, and $|P| = p^\alpha$, then Lagrange's theorem p^α divides $|PN|$. But since $|PN|$ divides $p^\alpha m$ we must have that $|PN| = p^\alpha k$ for k dividing m, and so p^α is a maximal p divisor of $|PN|$ as well.
Now applying the second isomorphism theorem we see that $k = |PN : P| = |N : P \cap N|$. Since $P \cap N \leq P$, it must a p group, say of order p^β. Then $|N| = p^\beta k$ for p not dividing k and so we are done. □

Now we fix notation as in part (b), where $2n = 2^a k$ for some odd k. Let P be a Sylow 2-subgroup (so that it has order 2^k), and $N = \langle r \rangle \trianglelefteq D_{2n}$ be the subgroup of rotations. Notice that $|N| = n = 2^{a-1}k$. By the lemma, $P \cap N \leq N$ is a Sylow 2-subgroup of N, and therefore has order 2^{a-1}. Putting all this together, we see that every Sylow 2-subgroup has 2^{a-1} rotation elements (of the form r^t), and 2^{a-1} reflection elements (of the form sr^t).

Notice that in total, there are $n = 2^{a-1}k$ reflections in D_{2n}. Each one has order 2 (HW2 problem 8), and so by Sylow's theorem is contained in some Sylow 2-subgroup. Each Sylow 2-subgroup has 2^{a-1} reflections by the previous paragraph, so we need at least k Sylow 2-subgroups to accomodate each reflection. But n_2 must also divide k by Sylow's theorem, so $n_2 = k$. This proves part (b).

Part (a) follows immediately. Suppose P is a Sylow 2-subgroup. Then by Sylow's theorem $|D_{2n} : N_{D_{2n}}(P)| = n_2 = k$. But $P \leq N_{D_{2n}}(P)$ already has index k, so that $P = N_{D_{2n}}(P)$. □

(b) Suppose that $2n = 2^a k$ for some odd k. Show that the number of Sylow 2-subgroups is k.

Proof. This was proved in part (a). □

(c) List all the Sylow 2-subgroups of D_{2n} if n is odd.

Proof. If n is odd, then 2 is the maximal 2-divisor of $2n$. In particular, Sylow 2-subgroups are of order 2. Since reflections are order 2, they generate 2 sylow subgroups. Considering the groups $\langle sr^i \rangle$ as i ranges from 0 to $n-1$ lists all the Syow 2-subggroups. □

(d) Give an example of a Sylow 2-subgroup of D_{12}.

Proof. Since $12 = 2^2 * 3$, this is a subgroup of order 4. There should be 3 of them. We list them all:

$$\langle r^3, s \rangle, \langle r^3, sr \rangle, \langle r^3, sr^2 \rangle.$$

□