Homework Assignment 8

Due Friday, March 19

Recall the following important Lemma from the March 11th 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. □

Sylow's theorem and some of the work you did last week makes it easy to prove Cauchy's theorem:

Theorem 1 (Cauchy's Theorem)**.** *Let G be a finite group and p a prime number dividing the order of G. Then G has an element of order p.*

2. (a) Prove the following strong version of Cauchy's theorem: Suppose G is a finite group of order n, and that p a prime number such that $p^d|n$ for some $d \geq 0$. Prove that G has a subgroup H of order p^d.

Proof. Let p^α be the maximal p-divisor of $|G|$. By Sylow's theorem (part 1) there is a p-sylow subgroup $P \leq G$, so that $|P| = p^\alpha$. Now suppose p^d divides the order of G. Then in particular $d \leq \alpha$, so that by HW7 Problem 3(b) P has a subgroup H of order p^d. But the H is also a subgroup of G of the same order, thereby giving the result. □

(b) Deduce Cauchy's theorem as a special case of part (a).

Proof. By part (a) there is a subgroup $K \leq G$ of order p. Let $x \in K$ be any element not equal to the unit. Then $|x| = p$ by Lagrange's theorem. □

3. Let G be a group of order p^2q for primes $p \neq q$. We will show that G always has a nontrivial *normal* Sylow subgroup.

(a) Suppose $p > q$. Show that G has a normal subgroup of order p^2.

Proof. Let n_p be the number of p-Sylow subgroups. By Sylow III $n_p = 1 + kp$ for some $k \geq 0$. Also by Sylow III, we know that n_p divides q, so that in particular $1 + kp \leq q$. Since $p > q$ this means $k = 0$ so that $n_p = 1$. Then letting P be the Sylow p-subgroup of G, we see that P is the unique subgroup of order p^2 and therefore must be normal by 1(b). (You may also use that we proved in class that $n_p = 1$ if and only if a Sylow p-subgroup is normal, which is a consequence of Sylow II.) □

(b) Suppose $q > p$. Show that either G has a normal subgroup of order q, or else $G \cong A_4$.

Proof. Let n_q be the number of q-Sylow subgroups. Then $n_q = 1 + kq$ for some $k \geq 0$. We also know that n_q divides p^2, so that $n_q \in \{1, p, p^2\}$. If $n_q = 1$ we are done (as the unique Sylow q-subgroup would be normal arguing as in part (a)). Else $k \geq 1$ so that $1 + kq > q > p$, so that $n_q = p^2$. In particular:

$$kq = p^2 - 1 = (p+1)(p-1).$$

Again since $q > p$ this means that q divides $p - 1$, so that in particular $q = p - 1$. The only primes that are one apart are 2 and 3. So this means $q = 3$ and $p = 2$, and our group has order 12. We now cite the March 11 lecture where we proved that a group of order 12 either has a normal subgroup of order 3, or else is isomorphic to A_4. □

(c) Explain why a group of order p^2q for primes $p \neq q$ can never be simple.

Proof. If $p > q$ we have a normal Sylow p-subgroup so G isn's simple. If $q > p$ we either have a normal Sylow q-subgroup (so G isn't simple), or else $G \cong A_4$. One can observe that A_4 has a normal subgroup of order 4 in a number of ways. We outline 2. The first is that in the February 23rd lecture we found the lattice of A_4, and saw that $H = \langle (12)(34), (13)(24) \rangle$ is the unique subgroup of order 4, so it is normal by 1(b). A second proof is to notice that H is the subgroup of 1 and all of the permutations of cycle type (2,2). Let $\sigma \in H$, and consider $\tau * \sigma = \tau\sigma\tau^{-1}$. If $\sigma = 1$ then $\tau * \sigma = \sigma \in H$. Else $\tau * \sigma$ still ahs cycle type (2,2) so it remains in H, directly showing the normality of H. □

4. In class we've alluded many times to the fact that if G is an abelian group of order pq for primes $p \neq q$, then $G \cong Z_{pq}$. Let's prove it.

   (a) Let $x, y \in G$ be two elements of finite order and suppose that $xy = yx$. Conclude that $|xy|$ divides the least common multiple of $|x|$ and $|y|$.

   Proof. Let l be the least common multiple of $|x|$ and $|y|$. Then $x^l = y^l = 1$, so that $(xy)^l = x^l y^l = 1$ Therefore $|xy|$ divides l (by HW2 Problem 8(c)). □

   (b) Let G be an abelian group of order pq for primes $p < q$. Use Cauchy's theorem and part (a) to conclude that G is cyclic. (This completes the argument from class about groups of order pq).

   Proof. By Cauchy's theorem, we can find $x, y \in G$ with $|x| = p$ and $|y| = q$. Since x and y commute, then applying part (a) we know that $|xy|$ divides pq, so it is one of $1, p, q, pq$. If it is 1 then $y = x^{-1}$ contradiction that their orders are not the same. If it is p then $(xy)^p = y^p = 1$ so that q divides p, which it does not. We can similarly rule out q. Thus $|xy| = pq$ so that $G = \langle xy \rangle$. □

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

   (a) Recall the order of $GL_2(\mathbb{F}_p)$ from HW5 problem 3(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 $GL_2(\mathbb{F}_p)$. 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

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

   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.

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 $\overline{T}$ has order p, is cyclic, and any nontrivial element is a generator, so $\overline{T}$ is generated by

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

The normalizer of $\overline{T}$ is therefore precisely the elements which conjugate g an element of $\overline{T}$. Let's conjugate g, by some arbitrary matrix τ.

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

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

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

In particular, τ nomralizes σ if and only if $c = 0$ if and only if τ is upper triangular, so the normalizer of $\overline{T}$ is precisely T. Then one can compute $|T| = (p-1)^2 * p$. Indeed, given an upper triangular matrix τ, we see it is invertible if and only if $ad = 0$. This means $a, d \neq 0$, giving $p-1$ choices for each, 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) Prove that T is not normal in $GL_2(\mathbb{F}_p)$. (Hint: use Lemma 1).

Proof. By part (d) we know $\overline{T} \trianglelefteq T$. Therefore if T were normal, $\overline{T}$ would have to be as well, which we saw in part (d) it is not. □

6. Prove that a group of order 200 cannot be simple.

Proof. We show that a group of order 200 has a unique Sylow 5-subgroup, which must therefore be normal. $200 = 25 * 8 = 5^2 * 8$. By Sylow's theorem, the number of Sylow 5 subgroups is one more than a multiple of 5:

$$n_5 = 1 + 5 * k \in \{1, 6, 11, 16, \cdots\}.$$

But we also by Sylow's theorem, n_5 must divide 8. The only number in that list dividing 8 is 1, so $n_5 = 1$. Thus there is a unique Sylow 5-subgroup P. Since any conjugate of P is also a Sylow 5-subgroup, we conclude that $gPg^{-1} = P$ for all $g \in G$, so that $P \trianglelefteq G$. Since $|P| = 25$, we have produced a nontrivial normal subgroup, so that G cannot be simple. □

7. Let $G_1, G_2, \cdots, G_n$ be groups. Show that:

$$Z(G_1 \times G_2 \times \cdots \times G_n) = Z(G_1) \times Z(G_2) \times \cdot \times Z(G_n).$$

Conclude that a product of groups is abelian if and only if the factors are.

Proof. If $x = (x_1, \cdots, x_n) \in Z(G_1) \times \cdots Z(G_n)$, so that each $x_i \in Z(G_i)$, then:

$$\begin{aligned} xy &= (x_1, \cdots, x_n)(y_1, \cdots, y_n) \\ &= (x_1 y_1, \cdots, x_n y_n) \\ &= (y_1 x_1, \cdots, y_n x_n) \\ &= (y_1, \cdots, y_n)(x_1, \cdots, x_n) \\ &= yx. \end{aligned}$$

This shows the right side is a subset of the left one. On the other hand, if $x = (x_1, \cdots, x_n) \in Z(G_1 \times \cdots \times G_n)$. Notice that the projection maps $\pi : G_1 \times \cdots \times G_n \to G_i$ is surjective for each i. In particular, each element of $y_i \in G_i$ is $\pi(y)$ for some y in the product group. Notice that:

$$\pi(x)y_i = \pi(x)\pi(y) = \pi(xy) = \pi(yx) = \pi(y)\pi(x) = y_i\pi(x).$$

Thus $\pi(x) = x_i \in Z(G_i)$. Since each coordinate of x is in the center of its respective group, we have $x \in Z(G_1) \times \cdots \times Z(G_n)$, proving the left side includes in the right one, completing the proof.

Now notice that if every G_i is abelian, then:

$$Z(G_1 \times \cdots \times G_n) = Z(G_1) \times \cdots \times Z(G_n) = G_1 \times \cdots \times G_n,$$

so that the product group is abelian. Conversely, if the product group is abelian, fix some $g_i \in G_i$, then $(1, \cdots, g_i, \cdots, 1)$ is in the center of the product group (everything is!), so g_i is in the center of G_i. Since g_i was arbitrary, G_i is abelian. □

Let's finish with an important cancellation lemma for direct products.

Lemma 2. *Let M, M', N, N' groups, and suppose $M \times N \cong M' \times N'$. If M and M' are finite and $M \cong M'$ then $N \cong N'$.*

8. Let's explore and prove Lemma 2. It is actually more subtle then you might think.

(a) You will need to make use of the following fact, so we prove it first. If G_1, G_2 are groups and $H_i \trianglelefteq G_i$ for $i = 1, 2$. Then under the usual identifications, $H_1 \times H_2 \trianglelefteq G_1 \times G_2$ and:

$$(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2).$$

Proof. Define a map

$$\Psi : G_1 \times G_2 \to (G_1/H_1) \times (G_2/H_2).$$

It is plainly surjective and the kernel is elements (g_1, g_2) with each $g_i \in H_i$. But this is precisely $H_1 \times H_2$ and the result follows by the first isomorphism theorem. □

(b) Give an example to show that Lemma 2 is not true without the finiteness assumption. (Hint: Let G a nontrivial group and $M = G \times G \times G \times \cdots$ an infinite product of copies of G).

Proof. Let $M = G \times G \times \cdots$ as suggested, and notice that $M \times G$ is also an infinite product of copies of G. Therefore:

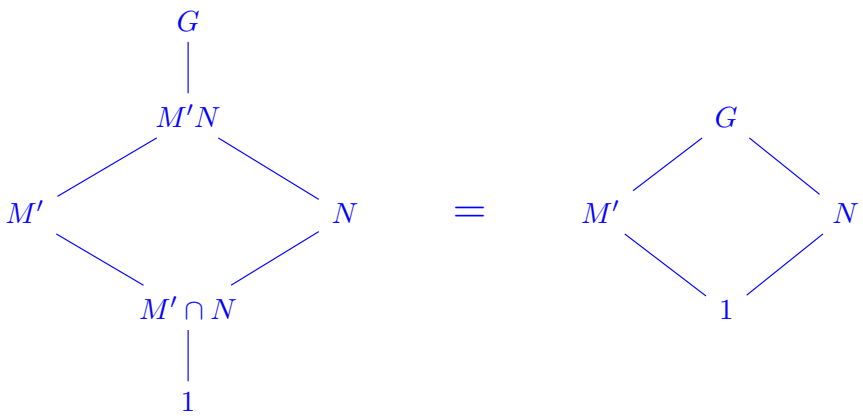
$$M \times G \cong M \cong M \times \{1\},$$

where $\{1\}$ is the trivial group. Since $G \ncong \{1\}$ (because by assumption G is nontrivial), we cannot cancel the M's on the left and right side of the equation. □

(c) Identify $M \times N$ and $M' \times N'$ as the same group G. Show that if either $M' \cap N = 1$, or if $M \cap N' = 1$ then Lemma 2 holds. (Hint: 2nd isomorphism theorem).

Proof. Inder the identification of $M \times N$ and $M' \times N'$ of G, we identify the factors M, N, M', N' with their images, so that $M, N, M', N' \leq G$ are subgroups of G. Since isomorphisms preserve normality, they are all normal, and we still have $G/M \cong N$, $G/N \cong M$, $G/M' \cong N'$ and $G/M' \cong N'$. We prove the first for completeness. Indeed, the kernel of $M \times N \to G \to G/M$ is precisely M.

We will focus on the case where $M' \cap N = 1$ and remark that the other case is completely symmetric. We consider the following diamond:



Let's say a few words about why these two diamonds are equal. $M' \cap N = 1$ by assumption, so the bottom being 1 is clear. On the other hand, since $N \leq M'N \leq G$, we know by the third isomorphism theorem that

$$[G : N] = [G : M'N][M'N : N].$$

Notice that $G/N \cong (M \times N)/N \cong M$ (by definition), and $M'N/N \cong M'$ (by the second isomorphism theorem), so that the equation becomes:

$$|M| = [G : M'N]|M'|.$$

By assumption $M \cong M'$ so that $|M| = |M'|$. Therefore we have showed that $[G : M'N] = 1$, and in particular $G = M'N$. But now we apply the second isomorphism theorem again:

$$N \cong M'N/M' = G/M' \cong (M' \times N')/M' \cong N',$$

and we are done. □

(d) Prove Lemma 2 by induction on $|M|$. (Hint: The base case is easy (why?). For the general case, notice that if $H = M \cap N'$ or $K = M' \cap N$ are trivial, we are done by part (b). Otherwise, try manipulating $G/(H \times K)$ to apply induction).

Proof. Under the identifications $H \leq M \leq M \times N \cong G$ and $K \leq N \leq M \times N \cong G$, we can also view $H \times K \leq M \times N \cong G$ as well. Then applying part (a), we have:

$$G/(H \times K) = (M \times N)/(H \times K) \cong (M/H) \times (N/K).$$

On the other hand, again symmetric reasoning we also have:

$$G/(K \times H) = (M' \times N')/(K \times H) \cong (M'/K) \times (N'/H).$$

In summary:

$$(M/H) \times (N/K) \cong (M'/K) \cong (N'/H). \tag{1}$$

We'd like to use induction, because either H or K are trivial (in which case we are done by part (c)), or both M/H and M'/K are smaller then M, so we can apply induction. But they are not the isomorphic, so we cannot cancel yet. We have to do something clever to put this in the correct form. We use the assumption here that $M \cong M'$, and "multiply both sides" by M' on the right and M on the left.

$$M \times \Big((M/H) \times N/K)\Big) \cong M' \times \Big((M'/K) \times (N'/H)\Big). \tag{2}$$

We first make the following observations, using part (a) yet again.

$$\begin{aligned} M \times (N/K) &= (M/1) \times (N/K) \\ &\cong (M \times N)/(1 \times K) \\ &= G/K \\ &= (M' \times N')/(K \times 1) \\ &\cong (M'/K) \times N' \end{aligned}$$

And similarly:

$$\begin{aligned} M' \times (N'/H) &\cong (M' \times N')/H \\ &= (M \times N)/H \\ &\cong (M/H) \times N. \end{aligned}$$

Therefore we can adjust the left hand side of Equation 2 to:

$$M \times \Big((M/H) \times (N/K)\Big) = \Big(M \times (N/K)\Big) \times M/H \cong \Big((M'/K) \times N)\Big) \times M/H.$$

And the right hand side to:

$$M' \times \Big((M'/K) \times (N'/H)\Big) = \Big(M' \times (N'/H)\Big) \times M'/K \cong \Big((M/H) \times N')\Big) \times M'/K.$$

Reordering the terms, Equation 2 becomes:

$$M'/K \times M/H \times N \cong M'/K \times M/H \times N'.$$

Since $|M'/K| < |M|$, by induction we can cancel:

$$M/H \times N \cong M/H \times N'.$$

Since $|M/H| < |M|$, by induction we can cancel again:

$$N \cong N',$$

completing the argument. □