Math 417 Problem Set 11 Solutions

Starred (*) problems were due Friday, November 30.

(*) 75. Show that if $H, K \subseteq G$ are subgroups of G, and HK is also a subgroup, then $|H| \cdot |K| = |HK| \cdot |H \cap K|$.

[Hint: show that if you pick coset representatives $A = \{a_1(H\cap K), \ldots, a_n(H\cap K)\}$ of the subgroup $H\cap K$ in H, then the map $A \times K \to HK$ given by $(a(H\cap K), k) \mapsto ak$ is a <u>bijection</u>.]

Let's do what the hint says. $H \cap K$ is a subgroup of G, and $H\cap K \subseteq H$, so we can treat $H\cap K$ as a subgroup of H, and so it has left cosets. If we call them $a_1(H\cap K), \ldots, a_n(H\cap K)$, then we can use them to build the function described in the hint: $(a_i(H\cap K), k) \mapsto a_i k$. We will show that this function is both injective and surjective.

For injective, since $A \times K$ is <u>not</u> a group (and we <u>don't</u> expect this function to be a homomorphism), we really need to show that (*) $a_{i_1}k_1 = a_{i_2}k_2$ implies $a_{i_1} = a_{i_2}$ and $k_1 = k_2$. But means that $x = a_{i_2}^{-1}a_{i_1} = k_2k_1^{-1}$, and so x is in H (because the a_i's are) and in K (since the k_i's are), so $a_{i_2}^{-1}a_{i_1} \in H\cap K$, so $a_{i_1}(H\cap K) = a_{i_2}(H\cap K)$. So $a_{i_1} = a_{i_2}$ since the a_i come from distinct (and therefore disjoint) cosets. Then $x = k_2k_1^{-1} = a_{i_2}^{-1}a_{i_1} = e_G$, so $k_1 = k_2$. So $(a_{i_1}, k_1) = (a_{i_2}, k_2)$, and so the function φ is injective.

For surjective, we start with $x \in HK$, so $x = hk$ with $h \in H$ and $k \in K$. Then $h(H\cap K)$ is a coset of $H\cap K$ in H and so $h(H\cap K) = a_i(H\cap K)$ for some i. But this means that $a_i^{-1}h \in H\cap K$, so $a_i^{-1}h = w$ for some $w \in H\cap K$, and so $h = a_i w$. Then $x = hk = (a_i w)k = a_i(wk)$ with $w \in H\cap K \subseteq K$ and $k \in K$¡ so $wk = k' \in K$. So $x = a_i k' = \varphi(a_i, k^prime)$, so w is in theimage of φ. So φ is surjective.

Consequently, φ is a bijection, so $|HK| = |A \times K| = |A| \cdot |K|$. But $|A| = [H : H\cap K] = |H|/|H\cap K|$ is the index of $H\cap K$ in H; rearrranging terms, we get $|HK| \cdot |H\cap K| = |H| \cdot |K|$, as desired.

(*) 77. If $|G| = p^n$ with p prime, show that for every k, $1 \le k \le n$, there is a <u>normal</u> subgroup $N \le G$ with $|N| = p^k$.

[Hint: take the quotient by some element of the center of G, and use induction!]

We will argue by induction. The base case is $n = 0$, i.e., $|G| = p^0 = 1$; then for every factor of $|G|$ (i.e., 1), we have a normal subgroup $H = G$ wwith $|H| =$ the factor. We now assume that the result is true for every group with order p^k for $k < n$.

We have seen in class that every group G with $|G| = p^n$ has non-trivial center, $Z(G) \neq \{e_G\}$. Picking $g \in Z(G)$, $g \neq e_G$, then $|g|$ divides $|G| = p^k$, so $|g| = p^\ell$ for some $\ell > 0$. Then we know that, setting $x = g^{p^{\ell-1}}$, we have $|x| = |g^{p^{\ell-1}}| = p$, and $x \in Z(G)$, so $N = \langle x \rangle$ is a normal subgroup of G.

The quotient group $H = G/N$ has order $|G|/|N| = p^n/p = p^{n-1}$, and so, by the inductive hypothesis, for every k with $1 \le k \le n$, we have $k-1 \le n-1$ and so there is a normal subgroup N_1 in H with order p^{k-1}. The quotient map $\varphi : G \to H = G/N$ is surjective, and so by a previous problem set, we know that the inverse image $N_2 = \varphi^{-1}(N_1)$ is a normal subgroup of G, and $[G : N_2] = [H : N_1] = |H|/|N_1| = p^{n-1}/p^{k-1} = p^{n-k}$, and so $|N_2| = |G|/[G : N_2] = p^n/p^{n-k} = p^k$. So N_2 is a normal subgroup of G of order p^k. So for every group G with $|G| = p^n$ and every $1 \le k \le n$ we have found a normal subgroup of G of order p^k. This establishes the inductive step.

So, we have shown by induction that for every group G with $|G| = p^n$ and every $1 \le k \le n$ there is a normal subgroup of G of order p^k .

(*) 79. In class we showed that for p a prime, $|GL(2, \mathbb{Z}_p)| = p(p-1)(p^2-1)$. So, for example, $|GL(2, \mathbb{Z}_5)| = 5 \cdot 4 \cdot 24 = 480$, and so (by Sylow) $GL(2, \mathbb{Z}_5)$ must have elements of order 3 and of order 5. Find some! Are the subgroups that they generate normal?

There are many ways to do this; $480 = 3 \cdot 160 = 3 \cdot 2^5 \cdot 5$ and $480 = 5 \cdot 96 = 5 \cdot 2^5 \cdot 3$, and so Sylow theory tells us that the 3-Sylow subgroup(s) have order 3, and the 5-Sylow subgroup(s) have order 5. Sylow theory tells us that all 3-Sylow and 5-Sylow subgroups are conjugate, and so one such subgroup is normal $\Leftrightarrow$ this is one such subgroup. A 3-Sylow subgroup contains 2 elements of order 3, and a 5-Sylow subgroup contains 4 elements of order 5, so finding more than that many elements of each order in $GL(2, \mathbb{Z}_5)$ will imply that the Sylow subgroups cannot be normal....

Actually finding such elements can be accomplished by some experimentation. For example, we could start with a matrix at random, like

$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$,

and take powers of it, hoping to find that its order is a multiple of 3 or 5; then an appropriate power of A has order 3 (or 5). In this case,

$A^2 = \begin{pmatrix} 0 & 3 \\ 3 & 2 \end{pmatrix}$, $A^3 = \begin{pmatrix} 3 & 3 \\ 3 & 0 \end{pmatrix}$, $A^4 = \begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix}$, $A^5 = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = -I$, and so

$A^{10} = (-I)^2 = I$, and so $B = A^2 = \begin{pmatrix} 0 & 3 \\ 3 & 2 \end{pmatrix}$ has order 5.

This matrix has determinant 1, and so any power of it has determinant 1, and any matrix conjugate to it has determinant 1. On the other hand,

$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has $A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $A^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$, $A^4 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$, and $A^5 = I$. So $|A| = 5$ and no power of A is B, so $\langle A \rangle \neq \langle B \rangle$, so neither subgroup can be normal!

Finding elements of order 3 took me somewhat longer! But (you can check!) the matrix $A = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$ has $A^6 = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$, and so $A^{12} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$ and $A^{24} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$. So $C = A^8 = \begin{pmatrix} 4 & 3 \\ 3 & 0 \end{pmatrix}$ has order dividing 3; since C isn't the identity, it has order 3 (!).

$\langle C \rangle$ is normal $\Leftrightarrow$ every conjugate of C is either C or C^2. But $C^2 = \begin{pmatrix} 0 & 2 \\ 2 & 4 \end{pmatrix}$ while (picking a conjugating element at random) taking $X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ we have $XCX^{-1} = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$, and so $\langle C \rangle$ is not normal.

So, Sylow theory tells us that <u>no</u> subgroup of order 3 or 5 in $GL(2, \mathbb{Z}_5)$ will be a normal subgroup!

A selection of further solutions.

74. If $H, K \subseteq G$ are subgroups of G, then we can define the <u>product</u> (sets)

$$HK = \{hk \ : \ h \in H, \ k \in K\} \qquad \text{and} \qquad KH = \{kh \ : \ k \in K, \ h \in H\}\ .$$

Show that HK is a subgroup of $G \Leftrightarrow HK = KH$.

We need to show two things: if HK is a subgroup then $HK - KH$, and if $HK = KH$ then HK is a subgroup.

For the first, we want to show that $HK = KH$, that is, $HK \subseteq KH$ and $KH \subseteq HK$. But if HK is a subgroup then it is closed under multiplcation. Then given $h \in H$ and $k \in K$, we have (since H and K are subgroups) $e \in H$ and $e \in K$, so $k = ek \in HK$ and $h = he \in HK$, so $kh \in HK$ and so $KH = \{kh \ : \ k \in K \text{ and } h \in H\} \subseteq HK$.

On the other hand, if $x \in HK$ then $x^{-1} \in HK$ since HK is a subgroup, and so $x^{-1} = hk$ for some $h \in H$ and $k \in K$. Then $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1}$, with $k^{-1} \in K$ and $h^{-1} \in H$ (since they are subgroups), so $x \in KH$. So $KH \subseteq HK$, and so $HK = KH$

If, conversely, we start with $HK = KH$, then we wish to show hat HK is a subgroup, that is, $e \in HK$, HK is closed under multiplication, and HK is closed under inversion. (we could combine these, using the 'one-step' subgroup test; we will not do that here). But $e \in H$ and $e \in K$, since both are subgroups, so $e = ee \in HK$. And if $x, y \in HK$, then $x = g_1h_1$ and $y = g_2h_2$ for some $g_1, g_2 \in H$ and $h_1, h_2 \in K$. Then

$$xy = (g_1h_1)(g_2h_2) = g_1(h_1g_2)h_2 = g_1(gh)h_2 = (g_1g)(hh_2) \in HK$$

since, because $KH = HK$, $h_1g_2 \in KH$ can be expressed as gh for some $g \in H$ and $h \in K$. So HK is closed under multiplication.

Finally, if $x \in HK$ then $x = hk$ for some $h \in H$ and $k \in K$, and then $x^{-1} = (hk)^{-1} = k^{-1}h^{-1}$ with $k^{-1} \in K$ and $h^{-1} \in H$ (since H and K are subgroups), so $x^-1 \in KH = HK$ (by hypothesis), so HK is closed under inversion. So all of the properties of a subgroup hold an d so HK is a subgroup of G, so long as $HK = KH$.

80. Show that every group of order 175 is abelian.

$175 = 5 \cdot 35 = 5 \cdot 5 \cdot 7 = 5^2 \cdot 7$. So Sylow theory tells us that G has subgroups H_5 and H_7 with $|H_5| = 25$ and $|H_7| = 7$. If $\mathcal{H}_5$ and $\mathcal{H}_7$ are the sets of 5-Sylow and 7-Sylow subgroups, then $n = |\mathscr{H}_5|$ divides 175 (so is one of $1, 5, 7, 25, 35, 175$) and is $\equiv 1 \bmod 5$, so is <u>not</u> a multiple of 5, and so is 1 or 7, and therfore is 1. So H_5 has no other conjugates, and so H_5 is a normal subgroup of G. In adddition, $m = |\mathscr{H}_7|$ divides 175 and is $\equiv 1 \bmod 7$ (so is not a multiple of 7, so is one of $1, 5, 25$), so $|\mathscr{H}_7| = 1$, and so H_7 is a normal subgroup.

Then we have the quotient groups G/H_5 and G/H_7, and $|G/H_5| = 175/25 = 7$ and $|G/H_7| = 175/7 = 25$, so we know that both of these groups are abelian. And we can build the homomorphism $\varphi : G \to G/H_5 \oplus G/H_7$ which sends $g \in G$ to (gH_5, gH_7), and this homomorphism is 1-to-1 (since its kernel is $H_5 \cap H_7$, whose order divides both 25 and 7, so $|H_5 \cap H_7| = 1$ and φ has trivial kernel). Therefore, under φ we have that G is isomorphic to its image, which is a subgroup of an abelian group, and so is abelian.