Math 417 Problem Set 9 Solutions

Starred (*) problems were due Friday, April 15.

(*) 69. Show that in the symmetric group S_n, every commutator $\alpha\beta\alpha^{-1}\beta^{-1}$ is an element of the subgroup A_n = the alternating group. Show, in addition, that every 3-cycle (a, b, c) can be written as a commutator $\alpha\beta\alpha^{-1}\beta^{-1}$. Conclude that every element of A_n can be written as a product of commutators.

Whatever they are, α can be expressed as a product of some number r of transpositions $\alpha = \tau_1 \cdots \tau_r$, and then $\alpha^{-1} = \tau_r \cdots \tau_1$ (since $\tau_i^{-1} = \tau_i$ is also a product of r transpositions. Similarly, $\beta = \sigma_1 \cdots \sigma_m$ is a product of m transpositions, and $\beta^{-1} = \sigma_m \cdots \sigma_1$. Then

$$\alpha\beta\alpha^{-1}\beta^{-1} = \tau_1 \cdots \tau_r \sigma_1 \cdots \sigma_m \tau_r \cdots \tau_1 \sigma_m \cdots \sigma_1$$

is a product of $2r + 2m$ transpositions. In particular, it is a product of an even number of transpositions, and so is an even permutation, and so $\alpha\beta\alpha^{-1}\beta^{-1} \in A_n$.

A 3-cycle can be expressed as a commutator of two 2-cycles, in fact; a little experimenting shows that $(a, b, c) = (a, b)(a, c)(a, b)(a, c) = (a, b)(a, c)(a, b)^{-1}(a, c)^{-1}$.

Finally, we have seen (in a previous problem set) that every element of A_n can be written as a product of 3-cycles. Since every 3-cycle can be expressed as a commutator, every element of A_n can then be expressed as a product of commutators.

(*) 72. (Gallian, p.416, # 33) If $|G| = p^n$ with p prime, show that for every k, $1 \le k \le n$, there is a normal 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 .

(*) 74. In class we (essentially) 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 $GL(2,\mathbb{Z}_5)$ 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 <u>one</u> such subgroup is normal $\Leftrightarrow$ this <u>is</u> 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 <u>multiple</u> 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:

68. Show that if $\varphi : G \to H$ is a homomorphism, and $N \leq H$ is a <u>normal</u> subgroup of H, then $\varphi^{-1}(N) = \{x \in G \ : \ \varphi(x) \in N\}$ is a normal subgroup of G, and $G/\varphi^{-1}(N) \cong \varphi(G)/[\varphi(G) \cap N]$.

    If $h \in \varphi^{-1}(N)$ and $g \in G$, we need to show that $ghg^{-1} \in \varphi^{-1}(N)$. But then $\varphi(h) = n \in N$ and $\varphi(g) = x \in H$, and so $xnx^{-1} \in N$, since N is normal. That is, $xnx^{-1} = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(ghg^{-1}) \in N$. But then ghg^{-1} has image lying in N, so $ghg^{-1} \in \varphi^{-1}(N)$, as desired.

    To show that $G/\varphi^{-1}(N) \cong \varphi(G)/[\varphi(G) \cap N]$, we start with the (surjective) homomorphism $\varphi : G \to \varphi(G)$. The subgroup (of G) $\varphi(G) \cap N$ is actually a normal subgroup of $\varphi(G)$; this is because if $x \in \varphi(G)$ and $n \in \varphi(G) \cap N$ then $n \in N$ and $x \in G$ so $xnx^{-1} \in N$, and $x, n \in \varphi(G)$ so $x^{-1} \in \varphi(G)$, so $xnx^{-1} \in \varphi(G)$, so $xnx^{-1} \in \varphi(G) \cap N$. Then the composition $\psi : G \to \varphi(G) \to \varphi(G)/[\varphi(G) \cap N]$ is a surjective homomorphism, and so by the first isomorphism theorem, $G/\mathrm{k}er(\psi) \cong \varphi(G)/[\varphi(G) \cap N]$. It only remains to find out what $\mathrm{k}er(\psi)$ is!

    The composition sends $g \in G$ to $\varphi(g)(\varphi(G) \cap N)$, and so $g \in \mathrm{k}er(\psi) \Leftrightarrow \varphi(g) \in \varphi(G) \cap N$ $\Leftrightarrow \varphi(g) \in N$ (since $\varphi(g)$ is automatically in $\varphi(G)$) $\Leftrightarrow g \in \varphi^{-1}(N)$. So $\mathrm{k}er(\psi) = \varphi^{-1}(N)$, as desired.

71. (Gallian, p.415, # 5 (sort of)) If $|G| = 36 = 2^2 \cdot 3^2$ and G has a 2-Sylow subgroup H and a 3-Sylow subgroup K that are both normal, show that the "natural" homomorphism $G \to G/H \oplus G/K$ given by $x \mapsto (xH, xK)$ is an isomorphism, and conclude (from earlier results) that G must be <u>abelian</u>.

    A 2-Sylow subgroup H_2 has order 4 and index 9 (and, by Sylow theory, has either 1, 3, or 9 conjugates) and a 3-Sylow subgroup H_3 has order 9 and index 4 (and has 1 or 4 conjugates). Under the <u>assumption</u> that H_2 and H_3 are both normal, then G/H_2 and G/H_3 are (quotient) groups, of orders $9 = 3^2$ and $4 = 2^2$, respectively. But we know from work in class that both G/H_2 and G/H_3 are then both abelian. The (natural) quotient homomorphisms combine to give a homomorphism $\psi : G \to G/H_2 \oplus G/H_3$ given by $\psi(g) = (gH_2, gH_3)$. This homomorphism is injective: $\psi(g) = (e_{G/H_2}, e_{G/H_3}) = (H_2, H_3) \Leftrightarrow g \in H_2$ and $g \in H_3$. But then $|g|$ divides both $|H_2| = 4$ and $|H_3| = 9$, and so $|g| = 1$, i.e., $g = e_G$. So ψ is injective.

    Therefore, G is isomorphic to $\psi(G)$, which is a subgroup of the direct sum of two abelian groups, which is abelian. So $\psi(G)$ is a subgroup of an abelian group, and so is abelian. So G is isomorphic to an abelian group, and so is abelian!