Math 417 Midterm Exam Solutions

Note: Many problems had several approaches to their solution; these illustrate some of them.

A.1. Show that the group $\mathbb{Z}_{14}^*$ of units modulo 14 is a cyclic group.

The numbers between 1 and 14 that are relatively prime to 14 are the odd numbers that are not (multiples of) 7, that is, $1, 3, 5, 9, 11, 13$. So $|\mathbb{Z}_{14}^*| = 6$, and so to show that $\mathbb{Z}_{14}^*$ is cyclic we need to find an element in $\mathbb{Z}_{14}^*$ of order 6. Since the order of any element $a \in \mathbb{Z}_{14}^*$ must divide 6, it will equal 6 so long as a, a^2, and a^3 are $\neq 1$. Having no better place to start, we compute:

$3 \not\equiv_{14} 1$, $3^2 = 9 \not\equiv_{14} 1$, and $3^3 = 27 \equiv_{14} 13 \not\equiv_{14} 1$, and so 3 has order 6, and so $\mathbb{Z}_{14}^* = \langle 3 \rangle$.

[N.B. We know then that the (only) other generator of $\mathbb{Z}_{14}^*$, since 1 ad 5 are the only numbers relatively prime to $6 = |\mathbb{Z}_{14}^*|$, is $3^5 = 243 = 14 * 17 + 5 \equiv_{14} 5$.]

A.2. Show, on the other hand, that $\mathbb{Z}_{15}^*$ is <u>not</u> a cyclic group. What is the largest order of any element of $\mathbb{Z}_{15}^*$?

The numbers relatively prime to 15 are numbers not a multiple of 3 or 5, which are 1,2,4,7,8,11,13,14, and so $|\mathbb{Z}_{15}^*| = 8$. Therefore every element of $\mathbb{Z}_{15}^*$ has order dividing 8, and we wish to show that no element has order 8, and so every element should instead have order dividing 4. We can show that by showing that for every $a \in \mathbb{Z}_{15}^*$ we have $a^4 \equiv_{15} 1$, that is, $15 | a^4 - 1$.

This can be done directly, or we can come at it sideways: since $15 = 3 \cdot 5$ and $\gcd(3, 5) = 1$, $15|a^4 - 1$ precisely when $3|a^4 - 1$ and $5|a^4 - 1$. But because 3 and 5 are prime, $3|a^2 - 1$ for any a not a multiple of 3, and $5|a^4 - 1$ for any 1 not a multiple of 5, by Fermat's Little Theorem. And since $a^4 - 1 = (a^2 - 1)(a^2 + 1)$, this means that 3 also divides $a^4 - 1$. Therefore, for every a relatively prime to 15 (so a is not a multiple of 3 or 5) we have $3|a^4 - 1$ and $5|a^4 - 1$, so $15|a^4 - 1$, as desired.

So no element of $\mathbb{Z}_{15}^*$ has order 8, so $\mathbb{Z}_{15}^*$ is not cyclic. On the other hand, $2^2 = 4 \not\equiv_{15} 1$, and so 2 has order greater than 2, and so must have order 4. This makes 4 the largst order of any element of $\mathbb{Z}_{15}^*$.

B.1. Show that the product of two 2-cycles, $\alpha = (a_1, a_2)(b_1, b_2) \in S_n$, can be written as a product of 3-cycles. [The interesting case is $\{a_1, a_2\} \cap \{b_1, b_2\} = \emptyset$; effectively, succeeding for $\alpha = (1, 2)(3, 4)$ should show you how to do them all.] Conclude that every element of the alternating group $A_n \subseteq S_n$ is equal to a product of 3-cycles.

There are, like with our method for writing a permutation as a product of 2-cycles, different cases that it is convenient to consider.

If $\{a_1, a_2\} = \{b_1, b_2\}$, then $(a_1, a_2) = (b_1, b_2) = (b_2, b_1) = (b_1, b_2)^{-1}$, and so $(a_1, a_2)(b_1, b_2) = e$, which we can either treat as a product of 0 3-cycles [that's my choice] or as $(a_1, a_2, x)^3$ (since 3-cycles have order 3) for some choice of third letter x.

If we are not in the first case, but $\{a_1, a_2\} \cap \{b_1, b_2\} \neq \emptyset$, then (exactly) one of the a_i equals one of the b_i. After relabeling we can assume (since $(a_1, a_2) = (a_2, a_1)$ so relabeling doesn't change the group elements) that $a_1 = b_1$, and so $\alpha = (a_1, a_2)(a_1, b_2) = (a_1, b_2, a_2)$ [by carrying out the composition], which ia a product of 1 3-cycle, as desired.

Finally, if $\{a_1, a_2\} \cap \{b_1, b_2\} = \emptyset$, then after a little experimentation [I know of no 'better' way to find out] we can find that

$(1,2)(3,4) = (1,2,3)(2,3,4)$, or $= (1,2,4)(2,4,3)$, or $= (1,3,4)(2,4,1)$, or a bunch of others, and so

$(a_1, a_2)(b_1, b_2) = (a_1, a_2, b_1)(a_2, b_1, b_2)$ is a product of 3-cycles.

Then since every element α of A_n is a product $\tau_1 \cdot \tau_2 \cdot \cdots \cdot \tau_{2k}$ of an <u>even</u> number of 2-cycles, by grouping them in pairs $\tau_{2i-1}\tau_{2i}$ we can convert each pair of 2-cycles into a product of 3-cycles; multiplying these products together expresses α as a product of 3-cycles.

[N.B. Note that every 3-cycle lies in A_n, and so this gives a characterization of A_n which doesn't (explicitly) use the word 'even': A_n consists of all of the products of 3-cycles.]

B.2. Express the (even) permutations $\alpha = (1,2,3,4,5,6,7)$ and $\beta = (1,2,3,4)(5,6,7,8)$ as products of 3-cycles.

Probably the most straightforward approach is to explicitly follow the plan given above.

$(1,2,3,4,5,6,7) = (1,2)(2,3)(3,4)(4,5)(5,6)(6,7) = (1,2,3)(3,4,5)(5,6,7)$ [OK, that was nicer than I had expected...]

$(1,2,3,4)(5,6,7,8) = (1,2)(2,3)(3,4)(5,6)(6,7)(7,8) = [(1,2)(2,3)][(3,4)(5,6)][(6,7)(7,8)] = (1,2,3)[(3,4,5)(4,5,6)](6,7,8) = (1,2,3)(3,4,5)(4,5,6)(6,7,8)$

C.1. Show that if $\varphi : G \to G$ is an automorphism of G, then $\varphi(Z(G)) = Z(G)$, where $Z(G) =$ the center of G.

[N.B.: Subgroups that are invariant under every automorphism of G are called 'characteristic subgroups'.]

$\varphi(Z(G)) = Z(G)$ <u>means</u> that $\varphi(Z(G)) \subseteq Z(G)$ and $Z(G) \subseteq \varphi(Z(G))$. This in turn means that the image if something in $Z(G)$ is in $Z(G)$, .i.e., if $g \in Z(G)$, then $\varphi(g) \in Z(G)$, <u>and</u> everything in $Z(G)$ is the image of something in $Z(G)$, i.e, if $g \in Z(G)$, then there is an $h \in Z(G)$ so that $g = \varphi(h)$.

To show the first inclusion, suppose that $g \in Z(G)$, so $gx = xg$ for every $x \in G$. We want to show that $\varphi(g) \in Z(G)$, i.e., $\varphi(g)y = y\varphi(g)$ for every $y \in G$. But since φ is an automorphism, it is a surjective homomorphism, so $y = \varphi(x)$ for some $x \in G$, Then

$$\varphi(g)y\varphi(g)\varphi(x) = \varphi(gx) = \varphi(xg) = \varphi(x)\varphi(g) = y\varphi(g)$$

as desired, where the middle equality uses that $g \in Z(G)$ and the two equalities flanking it use that φ is a homomorphism.

For the opposite inclusion, given $g \in Z(G)$, since φ is a bijection, there is, in fact, a <u>unique</u> $h \in G$ with $\varphi(h) = g$. What we wish to show is that $h \in Z(G)$ (!) So suppose it isn't. Then there is an $x \in G$ so that $hx \neq xh$. But then since φ is (an automorphism andn so) injective, this means that $\varphi(hx) \neq \varphi(xh)$. But then since φ is also a homomorphism, we find that

$$g\varphi(x) = \varphi(h)\varphi(x) = \varphi(hx) \neq \varphi(xh) = \varphi(x)\varphi(h) = \varphi(x)g$$

and so, setting $y = \varphi(x) \in G$, we have $gy \neq yg$, so $g \neq Z(G)$. This is a contradiction, and so we must have $h \in Z(G)$ [with $\varphi(h) = g$], as desired.

C.2. Show that if $g, h \in G$, then $gh \in Z(G) \Leftrightarrow hg \in Z(G)$.

We can do this directly (see below), or we can, in fact, use part (1), since there is an automorphism φ of G which sends gh to hg, and so by part (1), $gh \in Z(G)$ implies $\varphi(gh) = hg \in Z(G)$. That automorphism φ must 'erase' the h on the right and make it appear on the left of g; the function $\varphi(x) = hxh^{-1}$ will do precisely that, and conjugation by $h \in G$ is an automorphism of G. That is, if $gh \in Z(G)$, then $\varphi(gh) = h(gh)h^{-1} = hg(hh^{-1}) = hg \in Z(G)$.

The more direct approach is to show that if $gh \in Z(G)$, so $(gh)x = x(gh)$ for every $x \in G$, then we must have $hg \in Z(G)$, that is, $(hg)y = y(hg)$ for every $y \in G$. And there are a few ways to go about doing this (which all, ultimately, involve conjugation); here is one.

$(hg)y = (hg)(hh^{-1})y = h(gh)(h^{-1}y) = h(h^{-1}y)(gh) = y(gh) = (gh)y$

where the third and fifth equalities use that $gh \in Z(g)$. But then we have $(hg)y = (gh)y$, and so cancellation implies that $hg = gh$ (!). So since $gh \in Z(G)$, $hg = gh \in Z(G)$

OK, that was unexpected! And here is a more direct proof of it:

$hg = (hg)(hh^{-1}) = h(gh)h^{-1} = hh^{-1}(gh) = (hh^{-1})(gh) = e(gh) = gh$. So the question probably should have really read "If $gh \in Z(G)$ then $gh = hg$", since that's true (and a stronger statement)!

D. If $H, K \subseteq G$ are subgroups of G, then we can define the product (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 that 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 $HK = KH$.