Math 417 Problem Set 6

Starred (*) problems are due Friday, October 5.

(*) 36. Show that every element of S_n can be written as a product of transpositions of the form $(1,k)$ for $2 \leq k \leq n$. (Assume that $n > 1$ so that you don't have to worry about the philosophical challenges of $S_1 = \{()\}$...)

[Hint: why is it enough to show that this is true for transpositions?]

We have shown in class that every permutation $\alpha \in S_n$ can be written as a product of transpositions $\alpha(a_1, b_1) \cdots (a_k, b_k)$. If we show that every transposition can be written as a product of transpositions $(1,k)$, then by writing each (a_i, b_i) this way, and then multiplying these representations together, we will write α as a product of (products of transpositions of the form $(1,k)$), and so it will be a product of such transpositions.

And to show that any transposition (a,b) can be written this way, we can start by asking: Is either of a or b equal to 1? If yes, then $(a,b) = (1,b)$, or $(a,b) = (a,1) = (1,a)$, and so if <u>is</u> a transposition of the form $(1,k)$. If no, then both $(1,a)$ and $(1,b)$ are 'real' transpositions, and then we can start taking products of these:

$(1,a)(1,b) = (1,b,a)$, and so

$$(1,b)(1,a)(1,b) = (1,b)(1,b,a) = (1)(b,a) = (b,a) = (a,b),$$

and so (a,b) can be written as a sum of transpositions $(1,k)$, as desired.

(*) 38. Show that the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = e^x$, thought of as a function frm the group $(\mathbb{R}, +, 0)$ of real numbers under addition to the group $(\mathbb{R}^+, *, 1)$ of positive real numbers under multiplication, is an isomorphism of groups.

First, we show that f is a homomorphism. What this means, since $f : G \to H$ has G written additively and H written multiplicitively, that we want $f(a+b) = f(a)f(b)$. But this means that we want $e^{a+b} = a^a e^b$, which is true! This is the "law of exponents". So f is a homomorphism.

Then to show that f is in fact an isomorphism, we need to show that f is both 1-to-1 and onto. Here, again, we basically delve into some results from calculus: if $f(a) = f(b)$ then $e^a = e^b$, so $a = \ln(e^a) = \ln(e^b) = b$, so f is one-to-one. And if $a \in \mathbb{R}^+$ then $a \in \mathbb{R}$ and $a > 0$, so $= b\ln(a)$ makes sense, and $f(b) = e^b = e^{\ln a} = a$, since $\ln x$ is the inverse of e^x. So f is onto. Together, this shows that $f(x) = e^x$ is an isomorphism.

This last part can be summed up more compactly by asserting that $f(x) = e^x$ is 1-to-1 and onto because $g(x) = \ln x$ is (from calculus) the inverse of the function f. So since f has an inverse function, f is a bijection.

(*) 42. (Gallian, p.133, # 32) Suppose that $\varphi : (\mathbb{Z}_{50}, +, 0) \to (\mathbb{Z}_{50}, +, 0)$ is an isomorphism and $\varphi(7) = 13$. Show that, for all x, $\varphi(x) = kx$ for a certain k, and find k !

Because φ is a homomorphism and $\mathbb{Z}_{50}$ is cyclic (generated, when written additively, by 1), we know that $\varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = xk = kx$, where $k = \varphi(1)$. Note that this calculation is making some conceptual shifts: $\varphi(x \cdot 1) = x\varphi(1)$ is interpreting x (in $\mathbb{Z}_{50}$) as an integer, and $x \cdot 1$ means an x-fold sum of 1's, and employs induction (or really, our result that $\varphi(a^n) = (\varphi(a))^n$ in an additive setting) to show that $\varphi(x \cdot 1) = x\varphi(1)$. Also, $xk = kx$ reinterprets x as first in $\mathbb{Z}$ and then in $\mathbb{Z}_{50}$, while k shifts from $\mathbb{Z}_{50}$ to $\mathbb{Z}$. This really uses the fact that multiplication is well-defined in the ring $\mathbb{Z}_{50}$! The result of these computations is that φ is multiplication by (some) integer k, modulo 50. [Note, also, that this didn't really use the hypothesis that φ is an isomorphism; but the fact that $\varphi(7) = 13$, will imply this, once we figure out what k needs to be.]

Once we know that $\varphi(x) = kx$ for some k, we can use $\varphi(7) = 13 = k \cdot 7$ to determine k, by solving $13 = 7k$ in (the ring) $\mathbb{Z}_5 0$. We can do this by using the Euclidean algorithm to find the inverse n of 7 modulo 50, since then $7n \equiv_{50} 1$ and then $k \equiv k(7n) \equiv (7k)n \equiv 13n$ (all modulo 50). Since $50 = 7 \cdot 7 + 1$, this actually tells us that $1 = 50 - 7 \cdot 7 = 50 + (-7) \cdot 7$, so the inverse of 7 is $-7 \equiv 43 = n$. So $k = 13n \equiv 13 \cdot 43 = 559 \equiv 9$. So our homomorphism φ is $\varphi(x) = 9x \pmod{50}$.

As a check of this, we have $\varphi(7) = 9 \cdot 7 \equiv 62 = 1 \cdot 50 + 13 \equiv 13$, as desired.

A selection of further solutions.

37. (Gallian, p.115, #46) Show that in the symmetric group S_7, there is no element $x \in S_7$ so that $x^2 = (1, 2, 3, 4)$. On the other hand, find two distinct elements $y \in S_7$ so that $y^3 = (1, 2, 3, 4)$.

$(1, 2, 3, 4)$ is a 4-cycle, so it is an odd permutation. But for any $x \in S_7$, x^2 is always an even permutation, This is because when x is written as a product of transpositions, $x = \tau_1 \cdots \tau_k$, we have $x^2 = \tau_1 \cdots \tau_k \tau_1 \cdots \tau_k$ is a product of $2k$ transpositions, and therefore an even permutation! Since a permutation can't be both even and odd, x^2 can never be the same as $(1, 2, 3, 4)$.

On the other hand, x^3 does not have this same problem! And in fact, since $a = (1, 2, 3, 4)$ has $a^4 = e$, then $a = a^{-3} = (a^{-1})^3$, so $x = a^{-1} = (4, 3, 2, 1) = (1, 4, 3, 2)$ has $x^3 = (1, 2, 3, 4)$. Coming up with a second example can be arranged by noticing that we are supposed to be living in S_7 (!), so $y = (5, 6, 7) \in S_7$ and has $y^3 = e$. Since x and y are disjoint cycles, $z = xy$ satisfies $z^3 = (xy)^3 = x^3y^3 = (1, 2, 3, 4)e = (1, 2, 3, 4)$. So $x = (1, 4, 3, 2)(5, 6, 7)$ is a second example.

40. Show that if G_1, G_2 are groups, $H_1 \leq G_1$ is a subgroup of G_1, and $\varphi : G_1 \to G_2$ is a homomorphism, then $H_2 = \{\varphi(h) \ : \ h \in H_1\}$ (the *image* of H_1) is a subgroup of G_2.

We need to show that H_2 is closed under both multiplication (in G_2) and inversion. So if $g_1, g_2 \in H_2$, then by definition $g_1 = \varphi(h_1)$ and $g_2 = \varphi(h_2)$ for some $h_1, h_2 \in H_1$. Then $g_1g_2 = \varphi(h_1)\varphi(h_2) = \varphi(h_1h_2)$, since φ is a homomorphism. But since $h_1, h_2 \in H_1$ and H_1 is a subgroup, we have $h_1h_2 = h \in H_1$. So $g_1g_2 = \varphi(h_1h_2) = \varphi(h)$ with $h \in H_1$, so $g_1g_2 \in H_2$. So H_2 is closed under multiplication.

Second, if $g \in H_2$, then $g = \varphi(h)$ for some $h \in H_1$. But then $h^{-1} \in H_1$ since H_1 is a subgroup, and $\varphi(h^{-1}) = (\varphi(h))^{-1} = g^{-1}$, since φ is a homomorphism. So $g^{-1} = \varphi(h^{-1})$, and so $g^{-1} \in H_2$. This means that H_2 is closed under inversion.

So, since H_2 is closed under multiplication and inversion, H_2 is a subgroup.