Math 417 Problem Set 7 Solutions

Starred (*) problems were due Friday, October 12.

(*) 44. (Gallian, p.134, #44) Suppose that G is a finite *abelian* group, and that no element of G has order 2. Show that the function $\varphi : G \to G$ given by $\varphi(g) = g^2$ is an isomorphism. Show that if G is infinite then φ is a homomorphism, but need not be an isomorphism. (How many infinite abelian groups do we know at this point?)

[Hint: show that the hypothesis about orders implies that φ is injective.]

In general, when G is abelian,

$$\varphi(gg') = (gg')^2 = gg'gg' = ggg'g' = g^2(g')^2 = \varphi(g)\varphi(g'),$$

so φ will always be a homomorphism. If, in addition, G is finite, and has no element of order 2, then for $g \neq e$ we will always have $g^2 \neq e$. Then if we have $g, h \in G$ with $\varphi(g) = g^2 = h^2 = \varphi(h)$, then $e = g^2(h^2)^{-1} = g^2(h^{-1})^2 = (gh^{-1})^2$ [where this last equality is because G is abelian], and so by our hypothesis we have $gh^{-1} = e$, i.e., $g = h$. So $\varphi(g) = \varphi(h)$ implies that $g = h$, and so φ is an injective function. But since φ maps from G to G, it is an injective map from a set of n elements to a set of n elements, and so the Pigeonhole Principle tells us that φ is also surjective. So φ is a bijective homomorphism; that is, φ is an isomorphism.

When G is infinite, most of what we did goes through; if G has no elements of order 2 then $\varphi(g) = g^2$ is an injective homomorphism. But since G is infinite we have no Pigeonhole Principle to tell us that φ is surjective, and, in fact, it doesn't need to be. For example, in $G = (\mathbb{Q}^*, \cdot, 1)$ (the group of non-zero rational numbers under multiplication), $\varphi(x) = x^2$ is not surjective since, e.g., there is no rational x with $x^2 = 2$. A more down-to-earth example is $G = (\mathbb{Z}, +, 0)$, with $\varphi(x) = 2x$ [since the group is written additively]. Since there is no integer x with $2x = 1$, the map is not surjective.

(*) 48. Let $(\mathbb{Z}[x], +, 0)$ be the group of polynomials with integer coefficients, under addition, and let $k \in \mathbb{Z}$. Show that the function $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ given by $\varphi(p(x)) = p(k)$ [the 'evaluation function'] is a homomomorphism.

What we need to show is that if $p, q \in \mathbb{Z}[x]$ then $\varphi(p+q) = \varphi(p) + \varphi(q)$. [Note that we are treating $\mathbb{Z}$ as a group under addition.] But $\varphi(p + q) = (p + q)(k) = p(k) + q(k) = (\varphi(p)) + (\varphi(q))$, since that is how addition of functions is applied to an element of the domain. Therefore, φ sends sums to sums, so φ is a homomorphism.

(*) 49. A subgroup $H \leq G$ is called characteristic if $\varphi(H) = H$ for every $\varphi \in \mathrm{Aut}(G)$. Show that if K is a characteristic subgroup of H and H is a characteristic subgroup of G, then K is a characteristic subgroup of G.

We want to show that if $\varphi : G \to G$ is an automorphism of G, then $\varphi(K) = K$. What we know, since H is characteristic, is that $\varphi(H) = H$. But then if we define $\psi : H \to H$

by $\psi(h) = \varphi(h)$, then ψ is a homomorphism (since φ is) which is injective (since φ is!) and surjective, since $\psi(H) = \varphi(H) = H$. So ψ is an automorphism of H. Then since K is characteristic, we have $\psi(K) = K$ (thought of as a subgroup of H). But since $\psi = \varphi$ on elements of H, we then have $\varphi(K) = \psi(K) = K$. So K is carried to itself by any automorphism of G consequently, K is a characteristic subgroup of G.

A selection of further solutions.

43. Show that if $n \geq 3$, then $Z(S_n) = \{e\}$ is the 'trivial' subgroup of S_n.

[Hint: Show that if $\alpha(a) \neq a$ for some a, then $\tau\alpha \neq \alpha\tau$ for some transposition τ; note that you can assume there are three distinct integers a, b, c you can build things out of (that's important! $S_2 \cong \mathbb{Z}_2$ ...).]

We need to show that if $n \geq 3$ and $g \in S_n$, $g \neq e$, then there is an $h \in S_n$ so that $gh \neq hg$. But since $g \neq e$ there is an $a \in \{1, \ldots n\}$ so that $g(a) \neq a$, let's say $g(a) = b \neq a$. But since $n \geq 3$ there is a $c \in \{1, \ldots, n\}$ with $c \neq a$ and $c \neq b$. But then $(bc)g$ sends a (to b) to c, while $g(bc)$ sends a (to a) to b, since we apply the permutations from right to left when we determine where a product sends a number. So we have found that $(bc)g$ and $g(bc)$ send a to different places, so we functions they are not equal. Therefore, as elements of S_n we have $(bc)g \neq g(bc)$, so g does not commute with (bc), so $g \notin Z(S_n)$. Therefore, $g \neq e$ implies that $g \notin Z(S_n)$, so for $n \geq 3$ we have $Z(S_n) = \{e\}$.

45. (Gallian, p.135, #47) For G a group and $g \in G$ we write $\phi_g : G \to G$ to be the automorphism $\phi_g(x) = gxg^{-1}$. Show that if $\phi_g = \phi_h$ then $g^{-1}h \in Z(G)$.

Suppose that $\phi_g = \phi_h$. Then for every $x \in G$ we have $gxg^{-1} = \phi_g(x) = \phi_h(x) = hxh^{-1}$ So we have $gxg^{-1} = hxh^{-1}$, so $xg^{-1} = g^{-1}hxh^{-1}$, so $xg^{-1}h = g^{-1}hx$, for every $x \in G$. This means that if we set $u = g^{-1}h$, then $xu = ux$ for all $x \in G$, so $ux = xu$ for all $x \in G$, so $u \in Z(G)$. Therefore, if $\phi_g = \phi_h$, then $g^{-1}h \in Z(G)$.