Math 417 Problem Set 6 Solutions

Starred (*) problems were due Friday, March 4.

(*) 45. (Gallian, p.220, # 10) Suppose that G is a *dihedral group* (i.e., a group of symmetries of some regular n-gon), and define the function $\varphi : G \to H = (\{-1, 1\}, *, 1)$ to the group H (isomorphic to $\mathbb{Z}_2$) by $\varphi(\text{rotation}) = 1$ and $\varphi(\text{reflection}) = -1$. Show that φ is a homomorphism.

We need to show that for $g, g' \in G$, we have $\varphi(gg') = \varphi(g)\varphi(g')$. This amounts to showing that:

If $\varphi(g), \varphi(g') = 1$, then $\varphi(gg') = 1$, and

if $\varphi(g) = 1, \varphi(g') - 1$, then $\varphi(gg') = -1$, and

if $\varphi(g) = -1, \varphi(g') = 1$, then $\varphi(gg') = -1$, and

if $\varphi(g), \varphi(g') = -1$, then $\varphi(gg') = 1$.

This translates to:

If g and g' are rotations, then gg' is a rotation, and

if g is a rotation and g' is a reflection, then gg' is a reflection, and

if g is a reflection and g' is a rotation, then gg' is a reflection, and

If g and g' are reflections, then gg' is a rotation.

But this is precisely (except for the first case?) exactly what one of our previous problems, problem # 1, showed! And a routine calculation with their matrix representations will show that the composition of two rotations is a rotation (by the sum of the angles that the two elements rotate by). So every case behaves the way it should, and so φ is a homomorphism.

(*) 47. (Gallian, p.140, # 30) Suppose that $\varphi : (\mathbb{Z}_{50}, +, 0) \to (\mathbb{Z}_{50}, +, 0)$ is an isomorphism and $\varphi(11) = 13$. 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 $\varphi(11) = 13$, 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 $\varphi(11) = 13 = k \cdot 11$ to determine k, by solving $13 = 11k$ in (the ring) $\mathbb{Z}_50$. We can do this by using the Euclidean algorithm to find the inverse of 11 modulo 50, $11n \equiv_{50} 1$ and then $k \equiv k(11n) \equiv (11k)n \equiv 13n$.

Since $50 = 4 \cdot 11 + 6$ and $11 = 1 \cdot 6 + 5$ and $6 = 1 \cdot 5 + 1$, we can reverse engineer this to get $1 = 6 - 1 \cdot 5 = 6 - 1 \cdot (11 - 1 \cdot 6) = 2 \cdot 6 - 1 \cdot 11 = 2 \cdot (50 - 4 \cdot 11) - 1 \cdot 11 = 2 \cdot 50 - 9 \cdot 11$, and so $11^{-1} = -9 \equiv 41$. So $k = 13n \equiv 13 \cdot 41 = 533 \equiv 33$. So our homomorphism φ is $\varphi(x) = 33x \pmod{50}$.

As a check of this, we have $\varphi(11) = 11 \cdot 33 \equiv 363 = 7 \cdot 50 + 13 \equiv 13$, as desired.

(*) 48. (Gallian, p.141, #42) 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.

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.

A selection of further solutions.

44. 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.

To show that H_2 is a subgroup we need to show three things: closure under multiplication, e_{G_2} lives in H_2, and closure under inversion. But:

If $a, b \in H_2$ then $a = \varphi(c)$ and $b = \varphi(d)$ for some $c, d \in H_1$. Then $cd \in H_1$ since H_1 is a subgroup, and $\varphi(cd) = \varphi(c)\varphi(d) = ab$, so $ab \in \varphi(H_1) = H_2$. Also, since $e_{G_1} \in H_1$ since H_1 is a subgroup, and $\varphi(e_{G_1}) = e_{G_2}$, we have $e_{G_2} \in H_2$. Finally, if $a \in H_2$ then $a = \varphi(b)$ for some $b \in H_1$. Then since H_1 is a subgroup, $b^{-1} \in H_1$, and then $a^{-1} = (\varphi(b))^{-1} = \varphi(b^{-1}) \in H_2$, so H_2 is closed under inversion, as well.

So since H_2 is closed under multiplication, inversion, and contains he identity element of G_2, H_2 is a subgroup of G_2.

46. (Gallian, p.139, # 26) Show that the function $\varphi : \mathbb{Z}_{16}^* \to \mathbb{Z}_{16}^*$ given by $\varphi(a) = a^3$ is an isomorphism. What about $a \mapsto a^5$? Or $a \mapsto a^7$?

First, φ is a homomorphism, since it is well-defined [if $a \equiv_{16} b$ then $16|b-a$, so $b-a = 16k$, and then $\varphi(b)-\varphi(a) = b^3-a^3 = (b-a)(b^2+ab+a^2) = 16(k(b^2+ab+a^2)$ is also divisible by 16; also, if $\gcd(a, 16) = 1$ then $\gcd(a^3, 16) = 1$ (why?).], and we have $\varphi(ab) = (ab)^3 = a^3b^3 = \varphi(a)\varphi(b)$. To show that φ is an isomorphism, we need to show that it is a bijection; since $\mathbb{Z}_{16}^*$ is finite, it is enough to show that φ is <u>either</u> an injection <u>or</u> a surjection.

We could show either if these by brute force: $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$, and we could cube them to get our answer. A more roundabout way is to show that $16|a^3 - b^3$ implies $16|a - b$, <u>provided</u> $a, b \in \mathbb{Z}_{16}^*$. This is because, as we saw above, $a^3 - b^3 = (a-b)(a^2+ab+b^2)$; but since a and b are both odd, a^2+ab+b^2 is <u>odd</u>, and therefore $\gcd(16, a^2 + ab + b^2) = 1$. Consequently, $16|(a - b)(a^2 + ab + b^2)$ does imply that $16|a - b$, as desired!.

The maps $a \mapsto a^5$ and $a \mapsto a^7$ are, for the same reasons, homomorphisms from $\mathbb{Z}_{16}^*$ to $\mathbb{Z}_{16}^*$, and are, for the same reasons, injections and therefore bijections. We need $a^4+a^3b+a^2b^2+ab^3+b^4$ and $a^6+a^5b+a^4b^2+a^3b^3+a^2b^4+ab^5+b^6$ both odd whenver a and b are odd, but they both are the sum of an odd number of odd numbers!.