SOME SOLUTIONS TO HOMEWORK #3

MATH 435 – SPRING 2012

Certainly there are many correct ways to do each problem.

#28 on page 65. *If G is a cyclic group of order n, show that there are $\varphi(n)$ generators for G. Give their form explicitly.*

Proof. Suppose that $G = \langle a \rangle$. Then I claim that $\langle a^i \rangle = G$ if and only if i is relatively prime to n. This will indeed finish the problem, since there exactly $\varphi(n)$ positive integers $i < n$ with this property.

Suppose first that i is relatively prime to n and also suppose that $e = (a^i)^k = a^{ik}$. It follows immediately that n divides ik. But if i is relatively prime to n, we also have n dividing k. In particular, the order of $(a^i) \geq n$. But the order of any element of G is $\leq n$ and so the order of (a^i) is exactly n.

Now suppose conversely that a^i generates G. In particular, this means that the order of a^i is exactly n. But now suppose that $k > 0$ divides both i and n and we will obtain a contradiction. Then $(a^i)^{n/k} = (a^n)^{i/k} = e^{i/k} = e$. In particular, the order of a^i is less than $n/k < n$. This is a contradiction. $\square$

#1 on page 73. *Determine in each of the parts if the given mapping is a homomorphism. If so, identify the kernel and whether the mapping is one-to-one or onto..*

(a) *$G = \mathbb{Z}$ under $+$, $G' = \mathbb{Z}_{\mathrm{mod}\, n}$, $\phi(a) = [a]$ for $a \in \mathbb{Z}$*

Proof. This is a homomorphism since $\phi(a + b) = [a + b] = [a] + [b] = \phi(a) + \phi(b)$. The kernel is $n\mathbb{Z}$. It is onto but not one-to-one (note the kernel is not trivial). $\square$

(b) *G group, $\phi : G \to G$ defined by $\phi(a) = a^{-1}$ for $a \in G$.*

Proof. This is not a homomorphism since $\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = \phi(b)\phi(a)$ which need not equal $\phi(a)\phi(b)$ in general. $\square$

(c) *G Abelian group, $\phi : G \to G$ defined by $\phi(a) = a^{-1}$ for $a \in G$.*

Proof. If G is Abelian it is a homomorphism, then the map from (b) is a homomorphism and in fact it is both injective and surjective. $\square$

(d) *G group of non-zero real numbers under multiplication, $G' = [-1, 1]$, $\phi(r) = 1$ if r is positive and $\phi(r) = -1$ if r is negative*

Proof. This is a homomorphism. Indeed, we can also write $\phi(r) = r/|r|$. Then $\phi(rs) = (rs)/|rs| = (r/|r|)(s/|s|) = \phi(r)\phi(s)$. It is clearly not injective since $\phi(1) = \phi(2)$. It is not surjective since nothing is sent to $\frac{1}{2}$. $\square$

(e) *G an Abelian group, $n > 1$ a fixed integer and $\phi : G \to G$ defined by $\phi(a) = a^n$*

Proof. This is a homomorphism since $\phi(ab) = (ab)^n = a^n b^n = \phi(a)\phi(b)$ using the fact that G is Abelian. However, if $G = \{e, a\|\}$ is a cyclic group of order 2 and if $n = 2$, then the ϕ map is neither injective or surjective. It might be sometimes though (in the same example, if $n = 3$...) $\square$

#2 on page 73. *Prove that for all groups G_1, G_2, G_3:*

(a) $G_1 \cong G_1$

Proof. The identity map $G_1 \to G_1$ is clearly an isomorphism. □

(b) $G_1 \cong G_2$ implies that $G_2 \cong G_1$.

Proof. Given a bijective homomorphism $\phi : G_1 \to G_2$, we consider $\psi = \phi^{-1} : G_2 \to G_1$. This is clearly a bijective function and we need to prove it is also a homomorphism. Suppose that $x, y \in G_2$, then we need to show that $\psi(xy) = \psi(x)\psi(y)$. Consider then $\phi(\psi(xy)) = xy = \phi(\psi(x))\phi(\psi(y)) = \phi(\psi(x)\psi(y))$. Since ϕ is injective, we see that $\psi(xy) = \psi(x)\psi(y)$ as desired. □

(c) $G_1 \cong G_2$, $G_2 \cong G_3$ implies that $G_1 \cong G_2$.

Proof. Fix $\phi : G_1 \to G_2$ a bijective homomorphism and $\psi : G_2 \to G_3$ another bijective homomorphism. We consider $(\psi \circ \phi) : G_1 \to G_3$. This is certainly bijective since a composition of bijective functions is bijective (see the first chapter of the book). Then for $a, b \in G_1$, we have

$$(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi)(a)(\psi \circ \phi)(b).$$

This completes the proof. □

#12 on page 74. *Prove that $Z(G)$ is a normal subgroup of G.*

Proof. Suppose that $x \in G$. Then $xZ(G) = \{xz | z \in Z(G)\} = \{zx | z \in Z(G)\} = Z(G)x$ where the middle equality comes from the fact that $z \in Z(G)$ commute with everything in G. □

#14 on page 74. *Suppose that $\phi : G \to G'$ is a surjective homomorphism with G Abelian. Prove that G' is also Abelian.*

Proof. Suppose that $a', b' \in G'$. Since ϕ is surjective, there exist $a, b \in G$ such that $\phi(a) = a'$ and $\phi(b) = b'$. Thus

$$a'b' = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = b'a'.$$

Since a' and b' are arbitrary, this proves that G' is Abelian. □

#23 on page 75. *Let G be a group such that all subgroups are normal. If $a, b \in G$ show that $ba = ab^j$ for some $j \in \mathbb{Z}$.*

Proof. Consider the cyclic subgroup $H = \langle a \rangle$. Since H is normal, we know that $bH = Hb$. Now, $ba \in bH = Hb = \{a^j b | j \in \mathbb{Z}\}$. Thus $ba = a^j b$ for some $j \in \mathbb{Z}$ which completes the proof. □

#43 on page 75. *Prove that a group of order 9 must be Abelian.*

Proof. First suppose that G is a group of order 9 that is not Abelian. Since every cyclic group is Abelian, it follows that G is also not cyclic. Thus the order of every non-identity element of G is necessarily equal to 3.

I'll give a proof that is different from the brute-force ad-hoc proofs which are certainly also possible (in fact, what I do below proves that statement for any group of order p^2 for a prime p).

Define an equivalence relation as follows. $x \sim y$ if there exists $a \in G$ such that $axa^{-1} = y$. It is easy to verify that this is indeed an equivalence relation and so I will leave it to you.

Let us consider the various equivalence classes. Notice that e is in its own equivalence class, $[e] = \{e\}$. Now, fix $x \in G$ and consider the set $S_x \subseteq G$ made up of the elements a such that $axa^{-1} = x$. It is easy to see that S_x is a subgroup of G.

Claim 1. *I claim that $|[x]| = |G|/|S_x|$ which is equal to the number of cosets of S_x.*

Proof of claim. Consider the function $\psi : G \to \{bxb^{-1} | b \in G\}$ which sends a to axa^{-1}. Note that this map is surjective by construction. Suppose that $aS_x = bS_x$, then I claim that $\psi(a) = \psi(b)$. To see this, simply write $b = as$ for some $s \in S_x$, then observe that $\psi(b) = \psi(as) = (as)x(as)^{-1} = a(sxs^{-1})a^{-1} = axa^{-1} = \psi(a)$. Conversely, if $\psi(a) = \psi(b)$, then a similar argument implies that $aS_x = bS_x$.

But what does this do for us. Well, $\psi(a) = \psi(b)$ if and only if the cosets aS_x and bS_x are equal. But this means that the elements of $\{bxb^{-1} | b \in G\} = [x]$ are in bijective correspondence with the distinct cosets aS_x of S_x. This is all that we claimed. □

We have now proved the claim. The reason we wanted this claim was because it proved that

The number of elements of each $[x]$ *divides the order of* G.

Moving onto the rest of the problem, we notice that

$$G = \bigcup [x]$$

where the union runs over distinct equivalence classes of x. One of these equivalence classes is size 1, the equivalence class of e. Note that G is Abelian if and only if every equivalence class has size 1, so let's suppose that this is not the case. But since the size of each $[x]$ divides the order of the group, we see that we can have two equivalence classes of size 3 and 3 equivalence classes of size 1, or 1 equivalence class of size 3 and 6 equivalence classes of size 1.

The set of equivalence classes of size 1 exactly makes up the center $Z(G)$ inside G. Thus the second possibility is ruled out. Thus there must exist 2 equivalence classes of size 3 and $Z := Z(G)$ is the union of the remaining equivalence classes, each of which are of size 1. We need to derive a contradiction in this case as well. Now, $Z = Z(G)$ is a normal subgroup and so since $|Z| = 3$, we have that G/Z is a group of size 3 as well. In particular, G/Z is cyclic since 3 is prime. Choose cZ such that $\langle cZ \rangle = G/Z$. Then for any $a, b \in G$, we know that $aZ = c^i Z$ and $bZ = c^j Z$ for some integers i, j. Thus $a = c^i z$ and $b = c^j z'$ for some $z, z' \in Z$. Then using the fact that elements of Z commute with everything, we have

$$ab = (c^i z)(c^j z') = (c^i c^j z z') = (z' c^{i+j} z) = (z' c^j)(c^i z) = ba.$$

But this proves that G is Abelian, a contradiction. □