SOME SOLUTIONS TO HOMEWORK #2

MATH 435 – SPRING 2012

Certainly there are many correct ways to do each problem.

#4 on page 54. *Verify that $Z(G)$, the center of G, is a subgroup of G.*

Proof. First note that $ea = a = ae$ for all $a \in G$ which proves that $e \in Z(G)$. Now suppose that $f, g \in Z(G)$. Then for any $a \in G$, observe that

$$(fg)a = f(ga) = f(ag) = (fa)g = (af)g = a(fg)$$

which proves that $fg \in Z(G)$ and so $Z(G)$ is closed under multiplication. Finally, suppose that $f \in Z(G)$. Then for any $a \in G$,

$$f^{-1}a = (a^{-1}f)^{-1} = (fa^{-1})^{-1} = af^{-1}$$

which proves that $f \in Z(G)$ as desired. □

#5 on page 55. *If $C(a)$ is the Centralizer of a in G, prove that $Z(G) = \bigcap_{a \in G} C(a)$.*

Proof. Let me give two proofs. The first is just words. $Z(G)$ is the set of elements that commute with everything in G. $C(a)$ is the set of elements that commute with each a. Thus $\bigcap_{a \in G} C(a)$ is the set of elements that commute with each $a \in G$. But that's exactly $Z(G)$.

Here is the second proof. Suppose that $x \in Z(G)$. Thus $xa = ax$ for each $a \in G$ and so $x \in C(a)$ for each $a \in G$. Thus $x \in \bigcap_{a \in G}$ proving that $Z(G) \subseteq \bigcap_{a \in G} C(a)$. Conversely, suppose that $x \in \bigcap_{a \in G} C(a)$. Fix $a \in G$, then since $x \in C(a)$, $xa = ax$. But this holds for all a proving that $x \in Z(G)$. This proves that $\bigcap_{a \in G} C(a) \subseteq Z(G)$. Combined, these two containments imply that $\bigcap_{a \in G} C(a) = Z(G)$. □

#13 on page 55. *If G is cyclic, prove that every subgroup of G is cyclic.*

Proof. Suppose that $H \subseteq G$ is a subgroup. If $H = \{e\}$ then we are done so we may suppose that H has non-identity elements. Now suppose that $G = \langle a \rangle$. Consider the set of integers:

$$S = \{i > 0 | a^i \in H\}$$

Now H contains an element $a^i \neq e$ since $H \neq \{e\}$. If $i < 0$, then $(a^i)^{-1} = a^{-i} \in H$ and so $-i \in S$. If $i > 0$, then $i \in S$. Either way, S is non-empty.

Set $m = \min(S)$. We will show that $H = \langle a^m \rangle$, certainly the containment $\supseteq$ is obvious. For the other containment, choose $b \in H \subseteq G$, so we can write $b = \langle a^n \rangle$. Now write $n = qm + r$ for some $q \in \mathbb{Z}$ and $0 \leq r \leq m - 1$. We will prove that $r = 0$. Note $b(a^m)^{-q} = a^{n-mq} = a^r \in H$. Thus either $r = 0$, or $r > 0$ and so $r \in S$ but the latter is impossible since $r < m$ and m is the smallest element of S. But now that $r = 0$, we have that $n = qm$ and $b = (a^m)^q$ and so $b \in \langle a^m \rangle$ proving that $\langle a^m \rangle = H$ as desired. □

 # 3 on page 63. *Let $\sim$ be a relation on a set S that satisfies (1), $a \sim b$ implies $b \sim a$ and (2), $a \sim b$ and $b \sim c$ implies $a \sim c$. These seem to imply that $a \sim a$ for all $a \in S$. For if $a \sim b$ then by (1), $b \sim a$ and so $a \sim b$ and $b \sim a$ together imply that $a \sim a$. What is wrong with the argument we have given?*

Proof. It could be that a is not related/comparable to any element. In particular, we do not know that there exists any b such that $a \sim b$. □

#9 on page 64. *In $\mathbb{Z}_{\mod 16}$ write down all cosets of the group $H = \{[0], [4], [8], [12]\}$.* Note its fine to write the elements of $\mathbb{Z}_{\mod 16}$ as the numbers $\{0, 1, \ldots, 15\}$ instead of as equivalence classes.

Proof. I'll just write the answer.

$$\begin{array}{rcccccccl} 0+H & = & 4+H & = & 8+H & = & 12+H & = & \{[0],[4],[8],[12]\} \\ 1+H & = & 5+H & = & 9+H & = & 13+H & = & \{[1],[5],[9],[13]\} \\ 2+H & = & 6+H & = & 10+H & = & 14+H & = & \{[2],[6],[10],[14]\} \\ 3+H & = & 7+H & = & 11+H & = & 15+H & = & \{[3],[7],[11],[15]\} \end{array}$$

□

#15 on page 64. *If p is a prime, show that the only solutions to $x^2 \equiv_{\mod p} 1$ are $x \equiv_{\mod p} 1$ and $x \equiv_{\mod p} p-1 \equiv_{\mod p} -1$.*

Proof. Suppose that x is one of $0, \ldots, p-1$ and that $x^2 \equiv_{\mod p} = 1$. Thus $x^2 = qp + 1$ for some $q \in \mathbb{Z}$. Thus $(x^2 - 1) = qp$ so $(x-1)(x+1) = qp$. This implies that p divides $x-1$ or p divides $x+1$. If p divides $x-1$ and x is between 0 and $p-1$, we must therefore have $x - 1 = 0$ and so $x = 1$. On the other hand, if p divides $x+1$ then again because x is between 0 and $p-1$, we must have $x + 1 = p$ and so $x = p - 1$. So either $x = 1$ or $x = p - 1$ as desired. □

#26 on page 65. *Let G be a group, H a subgroup of G, and let S be the set of all distinct right costs of H in G, T the set of all left cosets of H in G. Prove that there is a 1-1 mapping of S onto T.*

Proof. If G is finite, the number of left or right cosets is just $|G|/|H|$ by the proof of Lagrange's theorem. However, we need to do the general case. Let me tell you what the map is and I'll let you fill in the details.

Send the coset Ha to $a^{-1}H$.

You have to show that this is *well defined*, injective and surjective (proving it is surjective is trivial – why?) □

(3) – not from the book. *Show that every Abelian group of order 6 is cyclic.*

Proof. Suppose first that G is an Abelian group of order 6 and suppose it is not cyclic.

We will first show that G contains an element of order 2. Indeed, suppose not to this other question as well. This means that every non-identity element of G must be order 3 by Lagrange's theorem. In particular, fix $a \in G$ to be an element of order 3, then $a^2 \neq e$ and $a^3 = e$. There are three elements of G not in $\langle a \rangle = \{e, a, a^2\}$. Fix $b \in G$ where $b \notin \langle a \rangle$. Thus $b^2 = b^{-1} \notin \langle a \rangle$ either because $\langle a \rangle$ is itself a (sub)group. Thus there is exactly 1 element $c \in G$ where $c \notin \langle a \rangle$ and $c \notin \langle b \rangle$. But then $c^2 = c^{-1} \neq e$ (because c has order 3) and $c^2 \notin \langle a \rangle \cup \langle b \rangle$. Finally, $c^2 \neq c$ since $c \neq e$. But this is impossible as then we have 7 distinct elements of G, $e, a, a^2, b, b^2, c, c^2$.

We now show that G contains an element of order 3. Indeed suppose not. Thus every non-identity element of G must be order 2. (We could argue as above, but we give a different argument). Suppose that $a, b \in G$ are distinct elements of order 2. Then consider the set $H = \{e, a, b, ab\}$. It is easy to see that this set is closed under multiplication (for example, $b(ab) = ab^2 = ae = a$ and $(ab)a = a^2b = b$). It follows that this set is a subgroup of G since it is finite, also note that $ab \neq a$ and $ab \neq b$ because in the first case, then $b = e$ and in the second case $a = e$ (but a and b are order 2). So H is a subgroup of G of order 4. Therefore by Lagrange's theorem, 4 divides the order of G, which is 6, which is a contradiction.

Ok, we've now proven that G contains an element f of order 2 and an element g of order 3. Consider now order of fg, note that $fg \neq e$ since f and g already have inverses, f and g^2

respectively, thus the order of fg is bigger than 1. Using that G is Abelian we have:

$$\begin{array}{lllllllll} (fg)^2 & = & (fg)(fg) & = & f^2g^2 & = & eg^2 & = & g^2 \neq e \\ (fg)^3 & = & (fg)(fg)(fg) & = & ff^2g^3 & = & fee & = & f \neq e \end{array}$$

Thus the order of fg divides 6 by Lagrange's theorem, and is not 1, 2 or 3. In other words, the order of fg is 6 which proves that $|\langle fg\rangle| = 6$ and so $\langle fg\rangle = G$. This last statement proves that G is cyclic as desired. □