SOME SOLUTIONS TO HOMEWORK #1

MATH 435 – SPRING 2012

Certainly there are many correct ways to do each problem.

#2 from page 50. Suppose G is a finite set with a associative binary operation satisfying the rule $ab = ac$ implies that $b = c$ and also that $ba = ca$ implies that $b = c$. We want to prove that G is a group. Closure and associativity were both given and so first we prove the identity (note we cannot even hope to show that inverses exist until after we show that there is an identity). Consider first the set $\{a^1, a^2, \dots, a^n, \dots\} \subseteq G$. Since G is finite, $a^n = a^m$ for some $m > n \geq 1$. Set $e = a^{m-n}$, we need to prove that e is the identity which will show that G in fact possesses an identity. So fix $b \in G$ and write $eb = c \in G$ where of course we want to prove that $c = b$. Multiplying both sides by a^n we obtain:

$$a^n c = a^n eb = a^n a^{m-n} b = a^m b = a^n b.$$

Using cancelation implies that $c = b$ as desired. Likewise if $be = d$, then multiplying both sides on the right by a^{m-n}, simplifying and canceling as before proves again that $b = d$ which proves that e is in fact the identity.

Now, we need to show that inverses exist. Fix $a \in G$ and choose $m > n$ as before such that $a^n = a^m$, we can certainly also assume that $m - n > 1$. Thus by cancelation $a^1 = a^{m-n+1}$ and so $ea = a^{m-n+1}$. Cancelation again implies that $e = aa^{m-n-1} = a^{m-n-1}a$ and so since $m - n - 1 > 0$, we see that a^{m-n-1} makes sense and is an inverse to a.

#5 from page 50. Suppose G is a group for which $(ab)^3 = a^3b^3$ and $(ab)^5 = a^5b^5$ for all $a, b \in G$. We want to prove that G is Abelian.

Proof. Fix $a, b \in G$. Then $(ab)(ab)(ab)(ab)(ab) = (ab)^5 = a^5b^5$ and cancelation of the end-terms, or multiplication by inverses, implies that $(ba)^4 = b(ab)(ab)(ab)a = a^4b^4$. Likewise, $(ab)(ab)(ab) = (ab)^3 = a^3b^3$ which implies that

$$(ba)^2 = a^2b^2 \tag{1}$$

again by cancelation. But $(ba)^4 = (ba)^2(ba)^2 = a^2b^2a^2b^2$ so that $a^4b^4 = a^2b^2a^2b^2$. Cancelation again implies $a^2b^2 = b^2a^2$ which is certainly getting us closer. Now, using Equation 1, but switching the roles of a and b, we have $(ab)^2 = b^2a^2$, so that $a^2b^2 = b^2a^2 = (ab)^2 = (ab)(ab)$. Cancelation of the end-terms one last time yields $ab = ba$ which proves that G is Abelian. □

#8 from page 55. In this problem, G is an Abelian group and $H = \{a \in G | a^2 = e\}$ and we want to show that H is a subgroup. Certainly $e \in H$, since $e^2 = e$. Now we prove closure, suppose that $a, b \in H$, then to show $ab \in H$ we need to show that $(ab)^2 = e$. But $(ab)^2 = (ab)(ab) = a^2b^2 = ee = e$ (using the fact that G is Abelian). Finally, we have $a \in H$ and we need to prove $a^{-1} \in H$. But if $a \in H$, then $a^2 = aa = e$ so that $a^{-1} = a$, thus $a^{-1} \in H$ as well. Thus H is a subgroup as desired.

#18 from page 55. In this problem, $A(S)$ is the set of bijection functions from S back to S with group operation composition. Consider $T(X)$ as defined. Certainly if $f, g \in T(X)$, then to show $f \circ g \in T(X)$, we consider $(f \circ g)(X) = f(g(X)) \subseteq f(X) \subseteq X$ by hypothesis. This proves that $T(X)$ is closed under composition. It is easy to see that the identity function is in $T(X)$

since $\mathrm{id}(X) = X$ by definition. Finally, we need to prove that if $f \in T(X)$, that $f^{-1} \in T(X)$ also. To do that, we need to show that $f^{-1}(X) \subseteq X$. Now, consider $f|_X$ (f restricted to X). This is a function from X to X which is injective, since f is injective. It is therefore surjective onto X since X is finite. Thus for every element $x \in X$, the element $y \in S$ such that $f(y) = x$ actually satisfies $y \in X$. In other words, we have just shown that $f^{-1}(X) \subseteq X$ as desired.

#22 from page 55. This is very easy with Lagrange's theorem. Set $k = |AB|$. Note k is at most mn (since $AB = \{ab | a \in A, b \in B\}$). On the other hand AB is itself a group by #19 and A and B are clearly subgroups of AB (since $e \in B$ and $e \in A$ respectively). Therefore $m|k$ and $n|k$, this clearly implies that $mn|k$ since m and n are coprime. Thus $mn|k$ and $k \leq mn$, which certainly implies that $k = mn$ as desired.

#26 from page 56. This follows from the material in the text on equivalence relations and Lagrange's theorem. Note that Ha is the equivalence class of a under the relation we (and the book) discusses in the next chapter.

#29 from page 56. We assume that $y^{-1}My \subseteq M$ for *ALL* $y \in G$ and we want to prove equality for all $y \in G$. Thus fix $x \in G$. We know $x^{-1}Mx \subseteq M$ and we need to prove $\supseteq$. So fix $m \in M$ and consider $m' = xmx^{-1}$. If we set $y = x^{-1}$ then $m' = y^{-1}my \in y^{-1}My \subseteq M$ because that containment holds for any y, and so $m' \in M$. But then $x^{-1}Mx$ contains $x^{-1}m'x = x^{-1}xmx^{-1}x = eme = m$ which proves the other containment and completes the proof.