M621 HW 3, due Sept 15

1. Recall that if $(G, *) = G$ and $H = (H, \circ)$ are groups, then a map $\Gamma : G \to H$ is a homomorphism if Γ is compatible with the operations—more formally, Γ is a homomorphism if for all $y, z \in G$, $\Gamma(y * z) = \Gamma(y) \circ \Gamma(z)$.

   (a) True or false? If "false", provide a specific counterexample: If G is a group and $b \in G$, then $l_b : G \to G$ given by $l_b(h) = b * h$ for all $h \in H$, is a homomorphism. (You can use "bh" in place of the more cumbersome "$b * h$".)

   False. Let $G = \mathbb{Z}/2\mathbb{Z}$, the two-element group having elements $\{0, 1\}$, with operation addition mod 2. Let $b = 1$. We have $l_1(0 + 0) = l + (0 + 0) = 1 + 0 = 1$, but $l_1(0) + l_1(0) = (1 + 0) + (1 + 0) = 1 + 1 = 0$. So l_b is not a homomorphism.

   (b) True or false? If "false", provide a specific counterexample: If G is an Abelian group, and $g \in G$, then l_b (given above), is a homomorphism.

   False. Use the counterexample above—-$\mathbb{Z}/2\mathbb{Z}$ is Abelian.

   (c) Let e_G be the identity of G, and let e_H be the identity of H. Prove that if $\Gamma : G \to H$ is a homomorphism, then $\Gamma(e_G) = e_H$.

   Proof. We have $\Gamma(e_G) \circ \Gamma(e_G) = \Gamma(e_G * e_G) = \Gamma(e_G)$, the left-most equality because Γ is a homomorphism, the right-most equality because e_G is the identity of G. Now using the left-cancellativity property of groups, $\Gamma(e_G) \circ \Gamma(e_G) = \Gamma(e_G * e_G) = \Gamma(e_G)$ implies that $\Gamma(e_G) = e_H$. $\square$

   (d) The *kernel of* Γ, $ker(\Gamma)$, is the set of all $g \in G$ such that $\Gamma(g) = e_H$. So $ker(G) = \{g \in G : \Gamma(g) = e_H\}$. Prove that $ker(\Gamma)$ is a subgroup of G.

   Proof. We'll show that $ker(\Gamma)$ is closed under the operation (of G) and closed under inverses in G. Suppose y and z are both in $ker(\Gamma)$. We have $\Gamma(yz) = \Gamma(y)\Gamma(z) = e_H e_H = e_H$, the left-most equality because Γ is a homomorphism, the second-to-leftmost equality from the definition of "kernel of a homomorphism", and the rightmost equality from the definition of the identity of a group. Thus, $ker(\Gamma)$ is closed under operation. With $y \in ker(\Gamma)$, we have $\Gamma(y^{-1}) = \Gamma(y)^{-1} = e_H^{-1} = e_H$, the left-most equality a property of homomorphisms, the right-most equality a property of the identity. $\square$

   It's a bit easier to prove the above using the "1-step Subgroup Test", namely that a non-empty subset A of a group B is a subgroup of B if and only if for all u, v in B, $uv^{-1} \in B$.

2. **page 23, problem 33.**

   (a) (a) Suppose $|x| = n$ is odd, i is a positive integer, with $n > i > 0$. Suppose for contradiction that $x^i = x^{-i}$. Thus, $x^{2i} = e$. Using the Division Theorem (dividing n into $2i$), there exists q, r with $n > r \geq 0$, such that $2i = nq + r$. So $e = x^{2i} = x^{nq}x^r = x^r$. Since $|x| = n$ and $n > r \geq 0$, from the definition of order of an element, it follows that $r = 0$. So $2i = nq$. If $q = 0$, $i = 0$, contradicting that $i > 0$; thus, $q > 0$. But $n > i$ implies that $2n > 2i$, and $q > 0$ and q is an integer, implies that $2i = n$, contradicting that n is odd.

   (b) See www.scribd.com/doc/81298835/Solutions-to-Abstract-Algebra-Chapter-1-Dummit-and-Foote-3e

   (b) **Short answer.** page 28, problem 15: This is not difficult since $\mathbb{Z}/n\mathbb{Z}$ is cyclic—that is, "1-generated"—so a presentation that involves only one generator (and one relation, for that matter) can be given.

   An answer. $< x|x^n = e >$. In fact, up to isomorphism, $\mathbb{Z}/n\mathbb{Z}$ is the largest group that satisfies the generators, relations provided.

   (c) page 28, problem 17. Be sure to read the discussion on page 26-27.

   See: www.scribd.com/doc/81298835/Solutions-to-Abstract-Algebra-Chapter-1-Dummit-and-Foote-3e

   (d) page 45, problem 18.

   G acts on a set A. Define a binary relation on A as follows: $a\ b$ if there exists $g \in G$ such that $ga = b$. It will be shown that is an equivalence relation—that is, is reflexive, symmetric, and transitive: For reflexivity, $ea = a$ for all $a \in A$ (a group action axiom). For transitivity, suppose for a, b, c in A, we have $a\ b$ and $b\ c$. In that case, there exist $g, h \in G$ such that $ga = b$ and $hb = c$. But then $(gh)a = g(ha) = gb = c$, the left-most equality from a group action axiom, and by definition of the relation, $a\ c$. Lastly, suppose $a\ b$. That means there exists $g \in G$ such that $ga = b$. Using group action axioms, $g^{-1}(ga) = (g^{-1}g)a = ea = a$. Since $ga = b$, we have shown that $g^{-1}(b) = a$, so $b\ a$, showing that the relation is symmetric, completing this important exercise.

   Comment. As you know, equivalence relations and partitions are essentially the same things: The sets of the form $A_u = \{v \in A : u\ v\}$ partition A. So a group action G on a set A partitions A. For $a \in A$, the **orbit** of a is its equivalence class under .

   Under this partitioning of A, if there is just is one equivalence class (so it would be A itself), then G is said to act **transitively** on A. For example, S_n acts transitively on $\{1, \ldots, n\} = A$.

Here's a very interesting class of group actions that are **not** transitive:

Examples. Let H be a proper subgroup of a group G, and let H act on G as follows: For all $h \in H$ and $g \in G$, let $h \cdot g = hg$. So H acts on G by left multiplication. It is not difficult to verify that this does define an action. Of course $e \in G$, the orbit of e is H, a proper subset of G. So under this action, H does not act transitively on G.

3. Let G be a group, and let A be a set. Suppose that G acts on A. You can use "ga" in place of "$g \cdot a$" for the action of $g \in G$ on an element $a \in A$.

   (a) Let $a \in A$. The *stabilizer of* a, $St(a)$, is the set $\{g \in G : ga = a\}$. Provide a short proof that $St(a)$ is a subgroup of G.

   Proof. G acts on A, meaning that for all $g, h \in G$, and all $a \in A$, we have $(gh)a = g(ha)$, and $ea = a$. I'll assume these defining properties of group action in the proof that follows: We show $St(a)$ is a subgroup. Suppose $g, h \in St(a)$. We have $(gh)(a) = g(ha) = ga = a$. We also have $(g^{-1}g)a = ea = a$. But $g^{-1}(a) = g^{-1}(ga) = g^{-1}ga = ea = a$. $\square$

   (b) As discussed in class, this one needs some modification: "$gB \subseteq B$" doesn't always imply that $St(B)$ is closed under inverse. In the statement of the corrected problem, "$gB \subseteq B$" is replaced by "$gB = B$".

   Let B be a non-empty subset of A. The *stabilizer of* B, $St(B)$, is the set $\{g \in G : gB = B\}$. Provide a short proof that $St(B)$ is a subgroup of G.

   Proof. It must be shown that if $g, h \in St(B)$, then $gh \in St(B)$, and $g^{-1} \in St(B)$. Let $b \in B$. We have $(gh)b = g(hb)$. Since $h \in St(B)$, $c = hb \in B$, and since $g \in St(B)$, $gc \in B$. Thus, $(gh)b \in B$. Consider $g^{-1}(b)$. Since $gB = B$, there exists $c \in B$ such that $gc = b$; thus, $g^{-1}(b) = g^{-1}(gc) = (g^{-1}g)c = c \in B$. It has been shown that $St(B)$ is closed under inverses, completing the exercise.