Applied Modern Algebra Spring 2014
Homework 4
Due: Fri. Mar 7

This assignment is meant to help you become comfortable with some basics of group theory. Since we are going through this rather quickly, you may want to do a little extra reading on your own (say pickup a book on algebra from the library that looks nice, or find an online introduction to group theory) to see more examples. See also my Number Theory notes (mainly Sections 3.3 and 3.4), linked to from the course page.

Definition 1. *Let G be a set with a* binary operation $\cdot$, *i.e.,* $\cdot$ *is a function from* $G \times G \to G$, *expressed as* $(g, h) \mapsto g \cdot h$, *or simply* gh. *If* G *satisfies the following properties,*

(i) $\cdot$ *is associative:* $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ *for all* $g, h, k \in G$;

(ii) there is an identity $1 \in G$ *such that* $1 \cdot g = g \cdot 1 = g$ *for all* $g \in G$;

(iii) every $g \in G$ *has an* inverse g^{-1} *such that* $g^{-1} \cdot g = g \cdot g^{-1} = 1$;

then we say $(G, \cdot)$ *(or just* G*) is a* **group**. *If (i) through (iii) and*

(iv) $\cdot$ *is commutative:* $g \cdot h = h \cdot g$ *for all* $g, h \in G$

also hold, we say $(G, \cdot)$ *(or just* G*) is an* **abelian group**. *When the operation is understood, we typically write* gh *for* $g \cdot h$.

Exercise 1. *Prove the identity element of a group* G *must be unique.*

Exercise 2. *Let* G *be a group and* $h \in G$. *Prove that if* $h \cdot g = g$ *for* some $g \in G$, *then* h *is the identity of* G.

Exercise 3. *Prove* $(\mathbb{Z}/n\mathbb{Z})^\times$, *the set of invertible elements in* $Z/n\mathbb{Z}$, *is a finite abelian group with respect to multiplication. You may use the results in Section 3.3 of the text. (The key points are to show multiplication is a well-defined binary operation on* $(\mathbb{Z}/n\mathbb{Z})^\times$, *and to verify properties (ii) and (iii).)*

Exercise 4. *Let* S_n *be the set of permutations on* $\{1, 2, \ldots, n\}$. *Let* $g, h \in S_n$ *and* id *be the trival permutation* $id(i) = i$, $i = 1, 2, \ldots n$. *Show:*

(a) The composition $gh = g \cdot h := h \circ g$ *(do* g*, then* h*) lies in* S_n. *This means composition is a well-defined binary operation on* S_n.

(b) $id \cdot g = g \cdot id = g$.

(c) There exists $g^{-1} \in S_n$ *such that* $g^{-1}g = gg^{-1} = id$.

Since composition of functions (and in particular permutations) is associative, the above exercise shows S_n is a group with repsect to composition, and the identity is id. The group S_n is not abelian for any $n > 2$.

Exercise 5. *Let* $G = S_3$ *and* $g = (12)$, $h = (123) \in G$. *Compute* gh *and* hg. *(Remember for* S_n, gh *means do* g *first, then* h*.)*

Exercise 6. *Let* $G = (\mathbb{Z}/7\mathbb{Z})^\times$. *We represent the elements of* G *by* $1, 2, \ldots, 6$.

(i) Write down the multiplication table for G.

(ii) Let $H = \{1, 6\}$. Show H is a subgroup of G. (It suffices to check H is closed under multiplication—i.e., if $h_1, h_2 \in H$, then $h_1 h_2 \in H$—and each element of H has an inverse in H. In other words, you may use Lemma 3.9 from my number theory notes.)

(iii) Determine the cosets of H in G.

(iv) Repeat (ii) and (iii) for the set $H = \{1, 2, 4\}$.

Exercise 7. *Use the formula $a^{-1} \equiv a^{p-2}$ mod p (which we will prove in lecture) to compute the inverse of 5 mod 13. (Do this by hand.)*

Definition 2. *Let G be a* finite *group, i.e., the set G has a finite number of elements n, called the* **order** *of G. Let $g \in G$. We will see in lecture that there exists $m \in \mathbb{N}$ such that $g^m = 1$. The smallest such m is called the* **order** *of g.*

Exercise 8. *For $2 \leq k \leq 10$, do the following. Write down the elements in $(\mathbb{Z}/k\mathbb{Z})^\times$ and state the* order *of the group $(\mathbb{Z}/k\mathbb{Z})^\times$.*

Exercise 9. *Let $G = (\mathbb{Z}/11\mathbb{Z})^\times$.*

(a) What is the order of G? Write down all elements in G.

(b) For each $g \in G$, determine the order of g.