CCS Discrete Math I	Professor: Padraic Bartlett
Homework 9: Groups	
Due Friday, Week 5	*UCSB 2014*

Do **three** of the **six** problems below!

1. When we defined a group in class, we used the following definition:

   Definition. A **group** $\langle G, \cdot \rangle$ is any set G along with a binary operation $\cdot : G \times G \to G$ that satisfies the following three properties:

   i. **Left identity**: there is some identity element $e \in G$ such that for any other $g \in G$, we have $e \cdot g = g$.
   ii. **Right inverses**: for any $g \in G$, there is some g^{-1} such that $g \cdot g^{-1} = e$, where e is some identity element.
   iii. **Associativity**: for any three $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

   However, there are additional properties people usually ask for, like the following:

   iv. **Uniqueness of the identity**: if e_1, e_2 are two elements that satisfy the identity property, then $e_1 = e_2$.
   v. **Left and right identity**: if e is an identity, then for any $g \in G$, $g \cdot e = e \cdot g = g$.
   vi. **Left and right inverses**: For any $g \in G$, there is a inverse element $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$, where e is the unique inverse element.

   On its face, our first definition of a group doesn't look like it necessarily satisfies these three properties!

   In this problem, you are challenged to do exactly one of the following:

   (a) Prove that anything satisfying properties i-iii satisfies properties iv-vi. In other words, using just properties i-iii and logic, show that iv-vi must hold.
   (b) Prove that properties i-iii **do not** satisfy properties iv-vi. Any such proof here would almost surely need to consist of a concrete counterexample, that would satisfy the first 3 properties but fail the other three.

2. Suppose that p is a prime number. Prove that $(p-1)! \equiv -1 \mod p$.

3. **Definition.** A **latin square** of order n is a $n \times n$ array filled with n distinct symbols (usually $\{1, \ldots n\}$, but they could be any set of N distinct symbols), such that no symbol is repeated twice in any row or column.

   Here are all of the latin squares of order 2:

1	2
2	1

2	1
1	2

Here is a Latin square of order 4:

2	1	4	3
1	2	3	4
3	4	1	2
4	3	2	1

(a) Take any finite group $\langle G, \cdot \rangle$ of order n. Make a **group table** for G (as defined in class/the notes.) Show that this table is a Latin square of order n.

(b) Does the converse hold? That is: is it true that every Latin square corresponds to some group table of some group G? Or is there some Latin square that cannot correspond to any group table of any group?

4. Suppose that G is a set with a binary operation $\cdot$ that has the following properties:

- **Associativity.**
- **Left cancellation**: For any $a, b, c \in G$, if $a \cdot b = a \cdot c$, then $b = c$.
- **Suspicious**[1]: There exists some element $a \in G$ such that for any $x \in G$, we have $x^3 = axa$.

Show that G is an abelian group. (Abelian means **commutative**, which means "For all $x, y \in G, x \cdot y = y \cdot x$.")

5. The **free group** on n generators $a_1, \ldots a_n$, denoted

$$\langle a_1, \ldots a_n \rangle,$$

is the following group:

- The elements of the group are all of the finite-length strings of the form

$$a_{i_1}^{\pm 1} a_{i_2}^{\pm 1} a_{i_3}^{\pm 1} a_{i_4}^{\pm 1} \ldots a_{i_l}^{\pm 1}$$

  where the indices $i_1, \ldots i_l$ are all between 1 and n, with possible repetitions.
- We denote the "string of length zero, the "empty string," with the symbol e.
- Given two strings s_1, s_2, we **concatenate** these two strings into the word $s_1 s_2$ by writing the string that consists of the string s_1 followed by the string s_2.
- Finally, if we ever have an $a^{+1}a^{-1}$ or an $a^{-1}a^{+1}$ occurring next to each other in a string, we simply remove those two elements from our string.

(a) Prove that this is a group!

(b) Consider the free group on one generator, $\langle a \rangle$. Prove that this group is isomorphic to the integers under addition.

[1] As always, I made up any particularly strange words.

6. In our above discussion, we have primarily defined groups by giving a set and an operation on that set. There are other ways of defining a group, though!

Definition. A **group presentation** is a collection of n generators $a_1, \dots a_n$ and m words $R_1, \dots R_m$ from the free group $\langle a_1, \dots a_n \rangle$, which we write as

$$\langle a_1, \dots a_n \mid R_1 = e, \dots R_m = e \rangle.$$

We associate this presentation with the group defined as follows:

- Start off with the free group $\langle a_1, \dots a_n \rangle$.
- Now, declare that within this free group, the words $R_1, \dots R_m$ are all equal to the empty string e: i.e. if we have any words that contain some R_i as a substring, we can simply "delete" this R_i from the word.

Example. Consider the group with presentation

$$\langle a \mid a^n = e \rangle,$$

where we let a^n denote the string consisting of n a's in a row. Notice that this is the collection of all words written with one symbol a, where we regard $a^n = e$: i.e. it's just

$$e, a, a^2, a^3, \dots a^{n-1}.$$

This is because given any string $a^k \in \langle a \rangle$, we have $a^k = a^l$ for any $k \equiv l \mod n$. This is because we can simply concatenate copies of the strings a^n, a^{-n} as many times as we want without changing a string, as $a^n = e$!

(a) Show that $\langle a \mid a^n = e \rangle$ is isomorphic to the group given by $\mathbb{Z}/n\mathbb{Z}$ with respect to addition.

(b) Describe D_8, the collection of symmetries of a square, via a group presentation. (In other words, create a group with presentation that is isomorphic to D_8.)