GROUP THEORY: THE BASICS

MATH CIRCLE (HS1) 5/4/2014

A **group** is a set/universe with a binary function $*$ that is associative ($a*(b*c) = (a*b)*c$), a unique identity element e ($a*e = e*a = a$ for all a), and every element has an inverse (for each a, there is a (unique) a^{-1} such that $a*a^{-1} = a^{-1}*a = e$).

A group is called call it an **abelian** if $*$ is commutative ($a*b = b*a$).

If k is a positive integer, x^k denotes $x*x*\cdots*x$, k times. Similarly, $x^0 = e$, and $x^{-k} = (x^{-1})^k$.

We'll often omit the operation $*$ when the context is clear, i.e. xy denotes $x*y$.

For example, the following are all groups:

- $\mathcal{Z}^+$: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, with operation $+$ and identity element 0,
- $\mathcal{R}^\times$: $\mathbb{R}^{>0}$ the positive real numbers, with operation $\times$ and identity element 1,
- $\mathcal{Z}_k^+$: $\{0, 1, 2, \ldots, k-1\}$, for k a positive integer, with operation $+(\text{mod } k)$ and identity element 0,
- $\mathcal{Z}_p^\times$: $\{1, 2, 3, \ldots p-1\}$, for p a positive prime number, with operation $\times(\text{mod } k)$ and identity element 1,
- S_n, the symmetric group on n elements, from last week.

Order of an Element

Suppose a is in G. The **order** of a, denoted $|a|$, is the smallest n such that $a^n = e$, if such an n exists. Otherwise, we say a has infinite order (denoted $|a| = \infty$).

1) Suppose G is $\mathcal{Z}_7^+$.

a) Find the inverse of every element of G.

b) Find the order of every element of G.

2) a) Repeat 2) for Z_8^+.

b) Repeat 2) for $Z_7^\times$.

3) Why is $Z_8^\times$ not a group?

4) Let G be a finite group and $|G|$ denote the size of G.

a) Suppose a is in G, and $|a| = n$. Prove that $e, a, a^2, a^3, \ldots, a^{n-1}$ are all distinct.

b) Prove that if $|a| = n$ then $n \leq |G|$.

c)* In fact, prove that for any a in G, $|a| \leq |G|$ (i.e. $|a|$ is finite and $|a| \leq |G|$).

Copyright ©2008-2014 Olga Radko/Los Angeles Math Circle/UCLA Department of Mathematics.

This handout was constructed using the first few chapters of Abstract Algebra by Dummit and Foote as a guide.

Proposition: Let G be a group and a an element of G.

(1) For any positive integer k, $(a^{-1})^k = a^{-k} = (a^k)^{-1}$.
(2) For any integers n, m, $a^n a^m = a^{n+m}$.
(3) For any integers n, m, $(a^n)^m = a^{n \cdot m}$.

Example (proof of 2.):

First suppose $n, m \geq 0$. Then $a^n a^m = (a * \cdots * a) * (a * \cdots a)$ where a appears n times in the first product and m times in the second. Hence a appears $n + m$ times in total, so $a^n a^m = a^{n+m}$ as needed.

Now suppose $n \geq 0, m < 0$ (the case $n < 0, m \geq 0$ is similar). Then $a^n a^m = (a * \cdots * a) * (a^{-1} * \cdots a^{-1})$ where a appears n times in the first product and a^{-1} appears $-m$ times in the second. By associativity, the a's and a^{-1}'s will cancel. If $n \geq -m$, then we are left with $n - (-m) = n + m$ a's, so $a^n a^m = a^{n+m}$ as needed. If $n < -m$, then we are left with $-m - n$ a^{-1}'s. Hence, we have $a^n a^m = (a^{-1})^{-m-n} = a^{n+m}$ as needed.

Finally suppose $n, m < 0$. Then $a^n a^m = (a^{-1} * \cdots * a^{-1}) * (a^{-1} * \cdots a^{-1})$ where a^{-1} appears $-n$ times in the first product and $-m$ times in the second. Hence a appears $-n - m$ times in total, so $a^n a^m = (a^{-1})^{-n-m} = a^{n+m}$ as needed.

5) Prove parts 1. and 3. of the proposition.

6) Suppose a is in G with $|a| = n$. Show that $a^{-1} = a^{n-1}$.

7) Suppose a is in G. Show that a and a^{-1} have the same order. Hint: Break into cases based on whether a,a^{-1} have finite/infinite order.

Extra Questions

8) a) For x, g in G, show that $|x| = |g^{-1}xg|$.

b) Show that $|ab| = |ba|$ for any a, b in G.

9 Prove that if $x^2 = e$ for any x in G, then G is abelian.

10) Prove that any finite group of even size has an element of order 2.

Hint: Let T denote the elements g of G such that $g \neq g^{-1}$. Prove that T has even size. Then look at the elements of G not in T.

11) a) Show that there is only one possible group of size 1 and and only one possible group of size 2.

b) Show that there is only one possible group of size 3. Hint: Suppose $G = \{e, a, b\}$ for distinct e, a, b. Show that $ab = e$.

c) Show that there are two possible groups of size 4. Hint: Break into cases based on whether or not G has an element with order 4.