GROUP THEORY: THE BASICS

MATH CIRCLE (HS1) 5/4/2014

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

A group is called an abelian if $\ast$ is commutative $(a \ast b = b \ast a)$. If $k$ is a positive integer, $x^k$ denotes $x \ast x \ast \cdots \ast x$, $k$ times. Similarly, $x^0 = e$, and $x^{-k} = (x^{-1})^k$.

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

For example, the following are all groups:

- $\mathbb{Z}^+: \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, with operation $+$ and identity element $0$,
- $\mathbb{R}_+: \mathbb{R}^{>0}$ the positive real numbers, with operation $\times$ and identity element $1$,
- $\mathbb{Z}_k^+: \{0, 1, 2, \ldots, k-1\}$, for $k$ a positive integer, with operation $+$(mod $k$) and identity element $0$,
- $\mathbb{Z}_p^\times: \{1, 2, 3, \ldots p-1\}$, for $p$ a positive prime number, with operation $\times$(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 $\mathbb{Z}_7^+$.  
   a) Find the inverse of every element of $G$. 
   b) Find the order of every element of $G$. 
2) a) Repeat 2) for $\mathbb{Z}_8^+$. 
   b) Repeat 2) for $\mathbb{Z}_7^\times$. 
3) Why is $\mathbb{Z}_8^\times$ 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 $|a| \leq |G|$).
**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 $n, m$, \((a^n)^m = a^{nm}\).

**Example (proof of 2.):**

First suppose $n, m \geq 0$. Then \(a^n a^m = (a \cdot \ldots \cdot a) \cdot (a \cdot \ldots \cdot a)\) 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 \(a^n a^m = (a \cdot \ldots \cdot a) \cdot (a^{-1} \cdot \ldots \cdot a^{-1})\) 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 \(a^n a^m = (a^{-1})^{-n-m} = a^{n+m}\) as needed.

Finally suppose $n, m < 0$. Then \(a^n a^m = (a^{-1} \cdot \ldots \cdot a^{-1}) \cdot (a^{-1} \cdot \ldots \cdot a^{-1})\) 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.