9-9-1993

More about groups.

I'll prove a few simple properties of groups, and then I'll give some additional examples.

Proposition. Let G be a group.

1. The identity element of G is unique.

2. The inverse of an element is unique.

Proof. To show a thing is unique, you assume that you have two things of that kind, then show that the two things must in fact be the same.

Suppose 1, $1'$ are identity elements for G. Then $1 \cdot 1' = 1'$ because 1 is an identity, but $1 \cdot 1' = 1$ because $1'$ is an identity. Therefore, $1 = 1 \cdot 1' = 1'$. The identity element of G is unique.

Suppose $g \in G$ and that I have elements $a, b \in G$ which behave like the inverse of g. This means that

$$ag = 1 = ga \text{ and } bg = 1 = gb.$$

Now

$$ag = 1 \text{ so } (ag)b = 1 \cdot b = b.$$

By associativity, $a(gb) = b$, but $gb = 1$. So $a \cdot 1 = b$, and $a = b$. The inverse of an element is unique. □

Computational stuff. I'll use the following algebraic rules a lot. In what follows, G is group and $a, b, c \in G$.

1. If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.

$$ab = ac, \quad a^{-1}(ab) = a^{-1}(ac), \quad (a^{-1}a)b = (a^{-1}a)c, \quad 1 \cdot b = 1 \cdot c, \quad b = c.$$

   You can prove the second result in similar fashion. □

2. $(ab)^{-1} = b^{-1}a^{-1}$.
   I am going to be a little cavalier about associativity.

$$b^{-1}a^{-1} \cdot ab = b^{-1} \cdot 1 \cdot b = b^{-1} \cdot b = 1,$$

   and likewise $ab \cdot b^{-1}a^{-1} = 1$. So $b^{-1}a^{-1}$ must be the inverse of ab, i.e. $(ab)^{-1}$.

3. $(a^{-1})^{-1} = a$.

$$a^{-1} \cdot a = 1 = a \cdot a^{-1}$$

   shows that a is the inverse of a^{-1} — that is, $a = (a^{-1})^{-1}$.

Notation. If a is an element of a group G with identity 1, then $a^0 = 1$. If n is a positive integer,

$$a^n \text{ means } \overbrace{a \cdot \cdots \cdot a}^{n \text{times}}.$$

If n is a negative integer, a^n means $(a^{-n})^{-1}$. It's easy to show that this is the same as

$$\overbrace{a^{-1} \cdot \cdots \cdot a^{-1}}^{n \text{times}}.$$

It's also easy to show (induction!) that $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$. □

Remark. A common convention is to use $\cdot$ ("multiplication") for the group operation symbol in an arbitrary group, but $+$ ("addition") for the group operation symbol in an *abelian* group. The first is referred to as **multiplicative notation** while the second is referred to as **additive notation**. Here is a translation table:

Arbitrary group	**Abelian group**
$a \cdot b$ or ab	$a + b$
a^n	$n \cdot a$ or na
1	0
a^{-1}	$-a$

In other words, if you *know* or *are assuming* that a group is abelian, you *normally* use additive notation (but it is not wrong to use multiplicative notation). In a group which is not known to be abelian, you *almost always* use multiplicative notation. $\square$

Example. The **order** of a group G is denoted $|G|$. It is the number of elements in G (if G is finite).

Suppose $|G| = 2$. Then $G = \{1, a\}$, where 1 is the identity and $a \neq 1$ is another element. a must have an inverse; since $a \cdot 1 = a$, the inverse of a is not 1. Therefore, the inverse of a is a, and $a \cdot a = 1$. The multiplication table for G looks like this:

	1	a
1	1	a
a	a	1

Up to renaming the elements or rearranging the row and columns of the table, this is the only group of order 2. It is the same as $\mathbb{Z}_2$, the cyclic group of order 2. $\square$

Example. Suppose that G is a group and $|G| = 3$. Let $G = \{1, a, b\}$, where $a, b \neq 1$ and $a \neq b$.

If $aa = a$, then $aaa^{-1} = aa^{-1} = 1$, or $a = 1$ $\times$. If $aa = 1$, then $ab = b$ (because $ab = a$ gives $aab = aa = 1$, or $b = 1$ $\times$). But then $abb^{-1} = bb^{-1} = 1$, so $a = 1$ $\times$. Hence, $aa = b$. Using the principle that each row or column of a multiplication table contains each element exactly once, I can fill in the rest of the table:

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

This is the same as $\mathbb{Z}_3$, and is the only group of order 3. $\square$

There are two groups of order 4, one group of order 5, two groups of order 6, and one group of order 7. As I mentioned earlier, no one knows a formula for determining how many groups of order n there are. And the method of the preceding examples — essentially, trial and error — is untenable once n gets large.