Math 371 Lecture #26
§7.2: Basic Properties of Groups

Using just the axioms of a group and simple consequences of them, we develop the basic theory of groups.

The standard notation for the binary operation on a group $G$ is the multiplicative $ab$.

Theorem 7.5. For a group $G$ and elements $a, b, c \in G$ we have

1. $G$ has a unique identity element $e$,
2. the cancelation $ab = ac$ or $ba = ca \Rightarrow b = c$ holds in $G$, and
3. each element of $G$ has a unique inverse.

Proof. (1) Suppose $G$ has two identity elements $e$ and $e'$. Then $ee' = e$ and $ee' = e$ so that $e = ee' = e'$.

(2) You proved that $ab = ac$ implies $b = c$ in a homework problem. A similar argument works for $ba = ca$ implies $b = c$.

(3) For $a \in G$ suppose that $d$ and $d'$ are inverses of $a$.

Then $ad = e = da$ and $ad' = e = d' a$.

It follows that $d = de = d(ad') = (da)d' = ed' = d$.

Notation. We write $a^{-1}$ for the inverse of $a \in G$.

Corollary 7.6. If $G$ is a group and $a, b \in G$, then

1. $(ab)^{-1} = b^{-1}a^{-1}$, and
2. $(a^{-1})^{-1} = a$.

Proof. (1) Using associativity of the operation in $G$, we have

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e,$

and similarly $(b^{-1}a^{-1})(ab) = e$.

(2) Since $aa^{-1} = e$ and $(a^{-1})(a^{-1})^{-1} = e$ we have $a^{-1}a = a^{-1}(a^{-1})^{-1}$.

By cancelation of the $a^{-1}$ term we get $a = (a^{-1})^{-1}$.

Notation. For $a$ in a group $G$ and $n \in \mathbb{N}$, we write

$a^n = \underbrace{aaa \cdots a}_n$,

we set $a^0 = e$, and we write

$a^{-n} = \underbrace{a^{-1}a^{-1}a^{-1} \cdots a^{-1}}_n$.

Some of the exponents rules apply to groups (but not all, like $(ab)^n = a^n b^n$).
Theorem 7.7. For a group $G$, $a \in G$, and $m, n \in \mathbb{Z}$, we have

$$a^m a^n = a^{m+n}, \ (a^m)^n = a^{mn}.$$  

This is shown to be true by several cases.

When the binary operation in a group is written additively $a + b$ (as would be the case with $\mathbb{Z}_n$), these exponential type results become

$$(ma) + (na) = (m + n)a \text{ and } n(ma) = (nm)a,$$

where

$$na = a + a + a + \cdots + a, \quad \text{with } 0a = 0 = e \text{ and } a^{-1} = -a,$$

and

$$(-n)a = -a - a - a - \cdots - a.$$ 

We return to the multiplicative notation for the binary operation of a group.

Definition. An element $a$ of a group $G$ is said to have finite order if there exist $k \in \mathbb{N}$ such that $a^k = e$, in which case, the order of $a$, written $|a|$ is the smallest $n \in \mathbb{N}$ for which $a^n = e$.

An element $a \in G$ has infinite order if $a^k \neq e$ for all $k \in \mathbb{N}$.

Examples. (a) What are the orders of the elements in $U_{10} = \{1, 3, 7, 9\}$ (the group of units in $\mathbb{Z}_{10}$)? Can an element of $U_{10}$ have order 3?

We have $1^1 = 1$ so $|1| = 1$.

We have $3^2 = 9$, $3^3 = 3 \cdot 9 = 7$, and $3^4 = 3 \cdot 7 = 1$, so $|3| = 4$.

We have $7^2 = 9$, $7^3 = 7 \cdot 9 = 3$, and $7^4 = 7 \cdot 3 = 1$, so $|7| = 4$.

We have $9^2 = 1$, so $|9| = 2$.

So no element of $U_{10}$ has order 3.

(b) Are there any elements of $\mathbb{Z}$ with finite order?

For a nonzero $a \in \mathbb{Z}$ we have $ka \neq 0$ for all $k \in \mathbb{N}$.

Hence every nonzero $a \in \mathbb{Z}$ has infinite order.

Only the zero element has finite order with $|0| = 1$.

Theorem 7.8. Let $G$ be a group and $a \in G$.

(1) If $a$ has infinite order, then the elements $a^k$, $k \in \mathbb{Z}$, are all distinct.

(2) For $i, j \in \mathbb{Z}$, if $a^i = a^j$ for $i \neq j$, then $a$ has finite order.
Proof. Notice that (1) is the contrapositive of (2), so it suffices to prove (2).

WLOG, suppose $a^i = a^j$ for $i > j$.

Then multiplying both sides by $a^{-j}$ gives $a^{i-j} = a^0 = e$.

Since $i - j > 0$, then $a$ has finite order. \hfill \Box

**Theorem 7.9.** Let $G$ be a group and $a \in G$ an element of finite order $n$.

1. $a^k = e$ if and only if $n | k$.
2. $a^i = a^j$ if and only if $i \equiv j \pmod{n}$.
3. If $n = td$ with $d \geq 1$, then $a^t$ has order $d$.

Proof. (1) Suppose $n | k$. Then $k = nt$ for some $t \in \mathbb{Z}$, and so

$$a^k = a^{nt} = (a^n)^t = e^t = e.$$  

Now suppose $a^k = e$.

By the Division Algorithm, we have $k = nq + r$ with $0 \leq r < n$, and so

$$e = a^k = a^{nq+r} = a^{nq}a^r = (a^n)^qa^r = e^qa^r = a^r.$$  

Since $n = |a|$ is the smallest positive integer for which $a^n = e$, and $a^r = e$ for $0 \leq r < n$, it must be that $r = 0$.

Thus $k = nq$, and so $n | k$.

(2) Observe that $a^i = a^j$ if and only if $a^{i-j} = e$.

With $k = i - j$, we have by (1) that $a^k = a^{i-j} = e$ if and only if $n | k$, i.e., $n | (i-j)$.

Here $n | (i-j)$ if and only if $i \equiv j \pmod{n}$.

(3) With $n = td$ and $n = |a|$, we have

$$(a^t)^d = a^{td} = a^n = e.$$  

To show that $|a^t| = d$, we let $k$ be any positive integer for which $(a^t)^k = e$.

Since $(a^t)^k = a^{tk}$, we have by (1) that $n | tk$, and so $tk = nr$ for some $r \in \mathbb{Z}$.

Since $n = td$, we have $tk = tdr$, which by cancelation gives $k = dr$ (as $t \neq 0$).

Since $k$ and $d$ are positive and $d | k$, we obtain $d \leq k$. \hfill \Box

**Corollary 7.10.** Let $G$ be an abelian group in which every element has finite order. If $c \in G$ is an element of largest order in $G$ (that is $|a| \leq |c|$ for all $a \in G$), then the order of every element of $G$ divides $|c|$.

Note: we will see a better theorem later for finite groups (nonabelian as well as abelian).

**Example (Continued).** Recall for the group of units $U_{10} = \{1, 3, 7, 9\}$ in $\mathbb{Z}_{10}$ that $|1| = 1$, $|3| = 4$, $|7| = 4$, and $|9| = 2$.

So the largest order of the elements is 4, and the order of each element of $U_{10}$ divides 4.