Lecture 22

Basic Properties of Groups

Theorem 22.1. Let $G$ be a group, and let $a, b, c \in G$. Then

(i) $G$ has a unique identity element.

(ii) The cancellation property holds in $G$:

$$a * b = a * c \implies b = c.$$ 

(iii) Each element of $G$ has a unique inverse.

Proof.

(i) Suppose $e$ and $e'$ satisfy

$$g * e = e * g = g, \quad \forall g \in G$$

$$g * e' = e' * g = g, \quad \forall g \in G$$

Then

$$e = e * e' = e'.$$

(ii) Suppose

$$a * b = a * c$$

Since an element $a^{-1}$ such that $a^{-1} * a = e$ exists for all $a \in G$, we have

$$b = e * b = a^{-1} * a * b = a^{-1} * a * c = c.$$ 

(iii)

Suppose

$$a * b = e = b * a \quad \text{and} \quad a * b' = e = b' * a.$$ 

Then

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'.$$

Corollary 22.2. If $G$ is a group and $a, b \in G$, then

$$i(i) \ (ab)^{-1} = a^{-1} b^{-1}. \ i(ii) \ (a^{-1})^{-1} = a.$$ 

Definition 22.3. Let $G$ be a group and let $n$ be a positive integer. Then

$$a^n \equiv a * a * \cdots * a \quad (n \text{ factors})$$

$$a^0 \equiv e$$

$$a^{-n} \equiv a^{-1} * a^{-1} * \cdots * a^{-1} \quad (n \text{ factors})$$

Theorem 22.4. Let $G$ be a group and let $a \in G$. Then for all $m, n \in \mathbb{Z}$

$$a^m * a^n = a^{m+n}$$

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

Definition 22.5. Let $G$ be a group. An element $a \in G$ is said to have finite order if $a^k = e$ for some positive integer $k$. In this case, the order of $a$ is the smallest positive integer $n$ such that $a^n = e$. If there exists no $n \geq 1$ such $a^n = e$ then $a$ is said to have infinite order.
Examples.

Recall that every ring is a abelian group under addition. In particular, the rings $\mathbb{Z}_n$ are abelian groups. In this case,

$$|a|^n = |a| + |a| + \cdots + |a| \quad (n \text{ terms})$$

$$\equiv [a] + [a] + \cdots + [a] \quad (n \text{ factors})$$

$$= n[a]$$

$$= [na]$$

$$= [0]$$

$$\equiv e$$

and so every element of the group $\mathbb{Z}_n$ (under addition) has finite order.

In the multiplicative group $\mathbb{R}^\times$ of non-zero real numbers, the element 2 has infinite order since

$$2^k \neq 1 \quad \forall k \geq 1.$$ 

Theorem 22.6. Let $G$ be a group and let $a \in G$. (i) If $a$ has infinite order, then the elements $a^k$, with $k \in \mathbb{Z}$, are all distinct.

(ii) If $a$ has finite order $n$, then

$$a^k = e \iff n \mid k$$

and

$$a^i = a^j \iff i \equiv j \pmod{n}.$$ 

(iii) If $a$ has finite order $n$ and $n = td$ with $d > 0$, then $a^t$ has order $d$.

Proof.

(i) We shall prove the contrapositive: i.e., if the $a^k$ are not all distinct, then $a$ has finite order. Suppose $a^i = a^j$ with $i < j$. Then multiplying both sides by $a^{-i} = (a^{-1})^i$ yields

$$e = a^0 = a^{j-i}.$$ 

Since $j - i > 0$, this says that $a$ has finite order.

(ii) Let $a$ be an element of finite order $n$. If $n$ divides $k$, say $k = nt$, then

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

Conversely, suppose $a^k = e$. By the Division Algorithm,

$$k = nq + r \quad 0 \leq r < n.$$ 

Consequently,

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

By the definition of order, $n$ is the smallest positive integer such that $a^n = e$. But the division algorithm requires $0 \leq r < n$. Thus, the only way to maintain both (??) and (??) without contradiction is to take $r = 0$. Thus, $n \mid k$.

Finally, note that $a^i = a^j$ if and only if $a^{i-j} = e$. But in view of the argument above, this is possible if and only if $n \mid (i - j)$. In other words, $i \equiv j \pmod{n}$.

(iii) Assume $a$ has finite order $n$ and that $n = td$. We then have

$$(a^t)^d = a^{td} = a^n = e.$$
We must show that $d$ is the smallest positive integer with this property. If $k$ is any positive integer such that $a^k = e$, then $a^{tk} = e$. Therefore $n \mid tk$ by part (ii) above.

Say $tk = nq = (td)q$.

Then $k = dq$. Since $d$ and $k$ are positive and $d \mid k$, we must have $d \leq k$. 

**Corollary 22.7.** Let $G$ be a group and let $a \in G$. If $a^i = a^j$ with $i \neq j$, then $a$ has finite order.

**Proof.**

This is an immediate consequence of statement (i) of the preceding theorem.