LECTURE 22

Basic Properties of Groups

THEOREM 22.1. *Let G be a group, and let $a, b, c \in G$. Then ı(i) G has a unique identity element. ı(ii) The cancellation property holds in G:*

$$a * b = a * c \quad \Rightarrow \quad b = c \quad .$$

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

Proof.

(i) Suppose e and e' satisfy

$$\begin{aligned} g * e &= e * g = g \quad , \quad \forall\, g \in G \\ g * e' &= e' * g = g \quad , \quad \forall\, g \in G \end{aligned}$$

Then

$$e = e * e' = e' \quad .$$

(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

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

(iii)

Suppose

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

Then

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

∎

COROLLARY 22.2. *If G is a group and $a, b \in G$, then ı(i) $(ab)^{-1} = a^{-1}b^{-1}$. ı(ii) $\left(a^{-1}\right)^{-1} = a$.*

DEFINITION 22.3. *Let G be a group and let n be a positive integer. Then*

$$\begin{aligned} a^n &\equiv a * a * \cdots * a \qquad (n \text{ factors}) \\ a^0 &\equiv e \\ a^{-n} &\equiv a^{-1} * a^{-1} * \cdots * a^{-1} \qquad (n \text{ factors}) \quad . \end{aligned}$$

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

$$\begin{aligned} a^m * a^n &= a^{m+n} \\ (a^n)^m &= a^{nm} \quad . \end{aligned}$$

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,

$$
\begin{aligned}
[a]^n &= [a] * [a] * \cdots * [a] \qquad (n \text{ factors}) \\
&\equiv [a] + [a] + \cdots + [a] \qquad (n \text{ terms}) \\
&= n[a] \\
&= [na] \\
&= [0] \\
&\equiv e
\end{aligned}
$$

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

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

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

ı(ii) If a has finite order n, then

$$a^k = e \qquad \Leftrightarrow \qquad n \mid k$$

and

$$a^i = a^j \qquad \Leftrightarrow \qquad i \equiv j \pmod n \quad .$$

ı(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

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

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

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

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

$$k = nq + r \quad , \quad 0 \leq r < n \quad . \tag{22.1}$$

Consequently,

$$e = a^k = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = a^r \quad . \tag{22.2}$$

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, $i \equiv j$ (mod n).

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

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

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

$$tk = nq = (td)q \quad .$$

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.