Lecture 10

Proposition 3: Let $(G, *)$ be a group. For any $a_1, a_2, \dots, a_n \in G$ the value of $a_1 * a_2 * \cdots * a_n$ is independent of how the expression is bracketed. (generalized associative law)

Proof: Exercise.

Def: (1) A group G is finite (infinite) if the set G is finite (infinite).

(2) If G is finite, the number of elements of G is denoted by $|G|$ and called the order of G.

Ex:
- $(\mathbb{Z}, +)$ is of finite order, $|\mathbb{Z}| = \infty$
- $(\mathbb{Z}/n, +)$ has order n, $|\mathbb{Z}/n| = n$

Powers of $a \in G$ are important!

Let $(G, *)$ be a group and let $a \in G$. Now $a^2 = a * a \in G$ and by induction, we can show that $a^m \in G$ for all $m \geqslant 1$. Thus, $\{a, a^2, \dots, a^m, \dots\} \subseteq G$.

If G is finite, all elements of the set $\{a, a^2, \dots, a^m, \dots\}$ cannot be distinct. Hence, $\exists k, l \in \mathbb{Z}^+$, $k > l$ s.t. $a^k = a^l$. This(*) implies $a^{k-l} = 1$, i.e.

$$\exists n \in \mathbb{Z}^+ \text{ s.t. } a^n = 1.$$

If G is infinite, then it may still be possible that $a^n = 1$ for some $n \in \mathbb{Z}^+$.

(*) See Q5 (a), PS5.

This leads us to the following definition.

Def: For a group $(G,*)$ and $a \in G$, we define the order of a to be the smallest positive integer n such that $\underbrace{a * a * \cdots * a}_{n\text{-times}} = e$, and denote this integer by $|a|$. If there is no such integer, the order of a is said to be infinite.

Remark:

- In multiplicative notation $a * \cdots * a = a \cdots a = a^n$ and $e = 1$. Then $|a| = n$ means $a^n = 1$ and n is the smallest.
- In additive notation $a * \cdots * a = a + \cdots + a = na$ and $e = 0$. Then $|a| = n$ means $na = 0$ and n is the smallest.

Ex:

- $\forall a \in G$, $|a| = 1$ iff $a = 1$.

- In $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under addition:

  $|0| = 1$ and $\forall a \neq 0$, $|a| = \infty$, because $\forall n \in \mathbb{Z}^+$ $\forall a \neq 0$ $na \neq 0$.

- In $\mathbb{R} \setminus \{0\}$ or $\mathbb{Q} \setminus \{0\}$ under multiplication:

  $|1| = 1$, $|-1| = 2$, and $\forall a \notin \{-1, 0, 1\}$ $|a| = \infty$.

- In $(\mathbb{Z}/9, +)$ the element $[6]$ has order 3 because

$$1[6] = [6] \neq [0]$$
$$2[6] = [6] + [6] = [12] = [3] \neq [0]$$
$$3[6] = [6] + [6] + [6] = [18] = [0] \quad \Longrightarrow \quad |[6]| = 3$$

- In $((\mathbb{Z}/7)^{\times}, \cdot)$ the element 3 has order 6 because

$$[3] \neq [1] \qquad [3]^3 \neq [1] \qquad [3]^5 \neq [1]$$

$$[3]^2 = [9] = [2] \neq [1] \qquad [3]^4 \neq [1] \qquad [3]^6 = [1] \qquad \Rightarrow \quad |[3]| = 6$$

- In $L = \{\pm 1, \pm i\}$ we have $|i| = 4$ because $i \neq 1$, $i^2 = -1 \neq 1$, $i^3 = -i \neq 1$, $i^4 = 1$

- Exercise: Consider $GL(2, \mathbb{R})$. Show that

i. $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ has order 2

ii. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has infinite order.

Convention: From now on, if I write "G is a group", I mean G is a group under multiplicative notation, $(G, \cdot)$.

Theorem 4: Let G be a group and let $a \in G$.

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

(2) If $a^i = a^j$ with $i \neq j$, then a has finite order.

Proof: (1) See Q7(a), PS5.

(2) Observe that this statement is the contrapositive of (1):

$$\left(|a| = \infty \Rightarrow \forall\, i \neq j,\ a^i \neq a^j \right) \Longleftrightarrow \left(\exists\, i \neq j,\ a^i = a^j \Rightarrow |a| < \infty \right)$$

It is enough to prove either (1) or (2). ■

Theorem 5: Let G be a group and $a \in G$ an element of finite order n. Then:

(1) $\exists\, m \in \mathbb{Z}$ such that $a^m = 1$ iff $n \mid m$.

(2) $a^i = a^j$ iff $i \equiv j \pmod{n}$

(3) For every $m \in \mathbb{Z}^+$, $|a^m| = \dfrac{n}{\gcd(m,n)}$

Proof:

(1) ($\Longrightarrow$) Since $|a| = n$, then $n \leq m$. By the Division Algorithm, $m = nq + r$ with $0 \leq r < n$. WTS that $r = 0$.

Suppose $r \neq 0$. Observe that, $1 = a^m = a^{nq} a^r = (a^n)^q a^r = 1^q a^r = a^r$, which implies $n \leq r$. Contradiction!!! because $0 < r < n$.

Thus, $m = nq$.

($\Leftarrow$) If $n \mid m$, then $m = nl$ for some $l \in \mathbb{Z}$ and $a^m = a^{nl} = (a^n)^l = 1$.

(2) $a^i = a^j \iff a^{i-j} = a^{j-j} = a^0 = 1 \iff n \mid (i-j) \iff i \equiv j \pmod{n}$

(3) Let $k := |a^m|$, then $a^{mk} = 1$. By (1), $n \mid mk$, i.e. $mk \overset{\circledast}{=} nr$ for some $r \in \mathbb{Z}$.

Let $d := \gcd(m,n)$, then $m \overset{\dagger}{=} du$ and $n \overset{\blacktriangle}{=} dv$ with $\gcd(u,v) = 1$

for some $u, v \in \mathbb{Z}^+$. (if $\gcd(u,v) \neq 1$, then $d\gcd(u,v)$ is a common divisor of m and

n s.t. $d < d\gcd(u,v)$. Contradiction!!!)

$\boxed{\text{WTS: } k = v}$ How? $v \mid k$ and $k \mid v \Rightarrow k = v$

Let's see that $v \mid k$.

Substitute $\dagger$ and $\blacktriangle$ into $\circledast$, then $duk = dvr$, i.e. $uk = vr$.

That means, $v \mid uk$. Since $\gcd(u,v)=1$, then $v \mid k$ by Prop 7, Module 1.

- Let's see that $k \mid v$.

  Observe that $(a^m)^v = a^{mv} = a^{duv} = a^{nv} = (a^n)^v = 1$. Then by (1),

  $k \mid v$. ∎