Chapter 4 Cyclic groups

Theorem 4.1 Let G be a group and $a \in G$.

(1) Suppose a has infinite order. Then $a^i = a^j$ if and only if $i = j$.

(2) Suppose a has finite order n. Then $a^i = a^j$ if and only if n divides $i - j$.

Let $\langle a \rangle = \{ a^n : n \in \mathbb{Z} \}$ is a subgroup.

$$a^n = \underbrace{a * \cdots * a}_{n} \quad \text{if } n \in \mathbb{N}$$

$$a^0 = e$$

$$a^{-n} = \underbrace{(a^{-1}) * \cdots * (a^{-1})}_{n} = (a^n)^{-1}.$$

(1) Assume a has infinite order, To prove $a^i = a^j$ if and only if $i = j$ in $\mathbb{Z}$.

($\Leftarrow$) If $i = j$, then $a^i = a^j$.

($\Rightarrow$) If $a^i = a^j$ and yet $i \neq j$.
then we may assume $j > i$.
So that $e = a^i a^{-i} = a^j a^{-i} = a^{j-i}$.
So there is $j - i \in \mathbb{N}$ s.t. $a^{j-i} = e$.
Hence a has finite order!

---

(2) Assume a has order n, i.e., $|a| = n$.

($\Rightarrow$) Assume $j - i = nk$. Then $a^j = a^{i+nk} = a^i a^{nk} = a^i (a^n)^k = a^i e^k = a^i e = a^i$.
for $k \in \mathbb{Z}$.

($\Leftarrow$) Assume $a^i = a^j$, we may WLOG assume $j \geq i$

Case1 If $j = i$, then $j - i = 0 \cdot n$.

Case2 If $j > i$, then $j - i = s > 0$. → so that $a^s = a^j a^{-i} = e$

Consider $s = nq + r$ with $r = 0, 1, \cdots, n-1$.

If $r > 0$, then $a^r = a^{s-nq} = a^{(s-nq)} = e^{q} = e$

This contradicts then $|a| = n$

Corollary Let G be a group, and $a \in G$. Then $H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\} \leq G$ is Abelian.

(1) $|a| = |\langle a \rangle|$.

(2) If $|a| = n$, then H is isomorphic to $\mathbb{Z}_n$.

(3) If $|a|$ is infinite, then H is isomorphic to $\mathbb{Z}$.

Remarks

- The group $H = \langle a \rangle$ is called the cyclic subgroup of G generated by a.
- If $H = G$, then G is a cyclic group generated by a.
- Every cyclic group is either isomorphic to $\mathbb{Z}_n$ or isomorphic to $\mathbb{Z}$.
- If $G = \langle a \rangle$ is isomorphic to $\mathbb{Z}$, then every subgroup has the form $\langle a^k \rangle = \langle a^{-k} \rangle$, which is isomorphic to $\mathbb{Z}$ is $k \neq 0$.

Proof: Let $H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\} \leq G$.

To prove (G4), let $x, y \in H$.

$x = a^m$, $y = a^k$, $m, k \in \mathbb{Z}$.

$\therefore \quad xy = a^{m+k} = a^{k+m} = yx$.

(1) & (2) Two cases:

$|a| = |\langle a \rangle|$

If $|a| = n$, then

$\langle a \rangle = \{a, a^2, \cdots, a^n = e\}$.

For $a^i \in H$, write $i = nq + r$, $r = 0, \cdots, n-1$.

Then $a^i = a^r$.

Moreover, $a^i \neq a^j$ if $1 \leq i < j \leq n$

Define $\Phi : H \to \mathbb{Z}_n$ by $\Phi(a^i) = [i] \in \mathbb{Z}_n$. $i = 0, \cdots, n-1$.

Then Φ is a bijection.

Moreover. For any $x, y \in H$,

we have $x = a^m$, $y = a^k$.

$\Phi(xy) = \Phi(a^{m+k}) = [m+k]$

$\Phi(x) + \Phi(y) = [m] + [k] = [m+k]$

(1) & (3) Let $|a| = \infty$.

Then $H = \{a^n : n \in \mathbb{Z}\}$.. & $a^i = a^j$ if $i \neq j$.

~~has distinct~~ So

So we all the elements a^i's are distinct for different $i \in \mathbb{Z}$.

We can define

$$\Phi : H \longrightarrow \mathbb{Z}$$

$\Phi(a^m) = m$. is a bijections

Then ~~Φ is~~ for $x, y \in H$, $x = a^m$, $y = a^k$ $m, k \in \mathbb{Z}$.

$\Phi(xy) = \Phi(a^{m+k}) = m+k$

$\Phi(x) + \Phi(y) = \Phi(a^m) + \Phi(a^k) = m+k$ } the same

Theorem 4.2 Suppose $a \in G$ has order n, and $H = \langle a \rangle$, which is isomorphic to $\mathbb{Z}_n$.

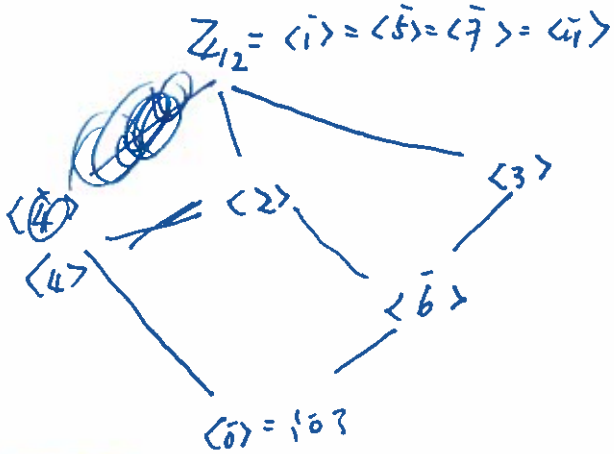
- Every subgroup of H is generated by a^k for some $k \in \{0, 1, \ldots, n-1\}$.
- For any $k \in \{0, 1, \ldots, n-1\}$, $\langle a^k \rangle = \langle a^d \rangle$ with $d = \gcd(n, k)$ so that $|a^k| = n/d$, which is a factor of n.
- For every factor m of n, there is a unique subgroup of H of order m.

Note In general, if $K \leq G$, $K \neq \langle h \rangle$ for $h \in G$. & for $R \leq K$, then $R \neq \langle k \rangle$ for some $k \in K$

Example $\mathbb{Z}_{12} = \{\bar{0}, \cdots, \bar{11}\}$

$\langle \bar{0} \rangle = \{\bar{0}\}$
$\langle \bar{1} \rangle = \mathbb{Z}_{12} = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$
$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{0}\} = \langle \bar{10} \rangle$
$\langle \bar{3} \rangle = \{\bar{3}, \bar{6}, \bar{9}, \bar{0}\} = \langle \bar{9} \rangle$
$\langle \bar{4} \rangle = \{\bar{4}, \bar{8}, \bar{0}\} = \langle \bar{8} \rangle$
$\langle \bar{6} \rangle = \{\bar{6}, \bar{0}\}$

$qk = nl$.



Proof: Let $K \leq H = \{a, a^2, \cdots, a^n = e\}$

Let $a^k \in K$ such that k is the smallest positive integer from $\{1, 2, \cdots, n\}$.

Case 1° If $k = n$, then $K = \{e\} = \langle e \rangle$

Case 2° If $k < n$, we claim that every $x = a^l$ in K satisfies $l = kq$. If not $\exists\, a^l$ in K with $l = kq + r$ $r \in \{1, \cdots, k-1\}$. Then $a^r = a^l \cdot ((a^k)^{-1})^q \in K$!!

From the proof, we see that for any subgroup $K \leq H$.

$K = \langle a^k \rangle$ and k can be chosen to be
$= \langle a^d \rangle$
if $\gcd(n, k) = d$ ~~if $k \geq d$.~~

because $d = \gcd(n, k)$ is the smallest positive integer such that $a^k \in K$ if $K \neq \{e\}$.

∎