Chapter 4

<u>Thm 4.1</u>: Let G be a group and $a \in G$

① If a has infinite order then
$\forall i,j \in \mathbb{Z} \quad a^i = a^j \iff i = j$

② If a has order n then
$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$
and $\forall i,j \in \mathbb{Z} \quad a^i = a^j \iff n \mid (i-j)$

<u>Pf</u>: ① Assume a has infinite order. Clearly $i=j \Rightarrow a^i = a^j$. Conversely, suppose $a^i = a^j$. By symmetry, we can assume $i \geq j$. Then multiplying by a^{-j} gives $a^{i-j} = e$. If $i-j > 0$ the a has order at most $i-j < \infty$, a contradiction. So $i-j = 0$ and $i=j$

② Assume a has order n. For every $k \in \mathbb{Z}$ there are $q, r \in \mathbb{Z}$ with $k = nq + r$ and $0 \leq r < n$. So
$$a^k = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r \in \{e, a, \dots, a^{n-1}\}.$$
Thus $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$

Next let $i,j \in \mathbb{Z}$ and assume $n \mid (i-j)$. Say $i-j = nq$. Then $a^{i-j} = a^{nq} = (a^n)^q = e^q = e$ and therefore $a^i = a^j$. Conversely suppose $i,j \in \mathbb{Z}$ and $a^i = a^j$. Then $a^{i-j} = e$. Pick $q, r \in \mathbb{Z}$ with $i-j = nq + r$ and $0 \leq r < n$. We have
$$e = a^{i-j} = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$$

Since a has order n, $a^r = e$, and $0 \le r < n$, we must have $r = 0$. Therefore $i - j = nq + r = nq$ and $n \mid (i-j)$. $\square$

Cor 1: For any group G and any $a \in G$, the order of a is equal to $|\langle a \rangle|$.

Cor 2: Let G be a group and $a \in G$. If a has order n and $a^k = e$ then $n \mid k$

Pf: $a^k = e = a^0$ so $n \mid (k - 0)$ (by Thm 4.1) and hence $n \mid k$. $\square$

Cor 3: Let G be a group and let $a, b \in G$. If a and b commute and have finite order then the order of ab divides (order of a)$\cdot$(order of b)

Pf: Let n be the order of a, m be the order of b. Then

$$(ab)^{nm} = \underbrace{(ab)(ab)\cdots(ab)}_{nm \text{ factors}} \underset{a,b \text{ commute}}{=} \underbrace{(aa\cdots a)}_{nm}\underbrace{(bb\cdots b)}_{\text{factors}}$$

$$= a^{nm} b^{nm} = (a^n)^m (b^m)^n = e^m e^n = e.$$

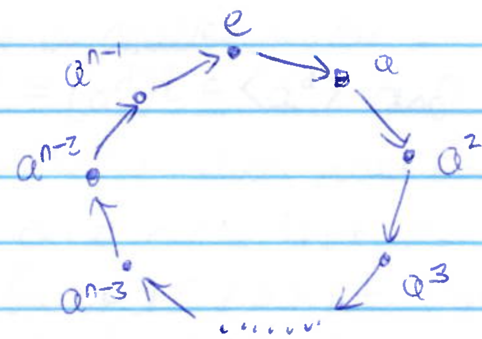
Now apply Cor. 2. $\square$

Note: By Thm 4.1, multiplication by a on $\langle a \rangle$ looks like

$$\cdots \to a^{-3} \to a^{-2} \to a^{-1} \to e \to a \to a^2 \to a^3 \to \cdots$$

when a has infinite order

OR



when a has order n

Moreover, multiplication in $\langle a \rangle$ behaves like addition in $\mathbb{Z}$ when a has infinite order and behaves like addition in $\mathbb{Z}_n$ when a has order n.

Specifically:

- when a has infinite order
  $$a^i a^j = a^k \iff i+j=k$$
- when a has order n (equals k if $k \in \mathbb{Z}_n$)
  $$a^i a^j = a^k \iff (i+j) \bmod n = k \bmod n$$

For this reason, the cyclic groups $\mathbb{Z}$ and $\mathbb{Z}_n$ serve as prototypes for <u>all</u> cyclic groups.

Thm 4.2: Let G be a group and $a \in G$. If a has order n and $k \in \mathbb{Z} \setminus \{0\}$ then

① $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ $\boxed{= \langle a^d \rangle}$

② The order of a^k is $\frac{n}{\gcd(n,k)}$ $\boxed{= \frac{n}{d}}$ $\boxed{=h}$

Pf: Set $d = \gcd(n,k)$.

① We know d divides k, so $k = dq$ for some $q \in \mathbb{Z}$. Then $a^k = (a^d)^q \in \langle a^d \rangle$ and therefore $\langle a^k \rangle \subseteq \langle a^d \rangle$ (every power of a^k is a power of a^d).
On the other hand, there are $s, t \in \mathbb{Z}$ with $d = \gcd(n,k) = ns + kt$. Therefore
$a^d = a^{ns+kt} = (a^n)^s (a^k)^t = e(a^k)^t = (a^k)^t$
and thus $\langle a^d \rangle \subseteq \langle a^k \rangle$
We conclude $\langle a^k \rangle = \langle a^d \rangle$

② We know d divides n, so $\boxed{n = dh}$ for some $h \in \mathbb{Z}$, $h > 0$.
Since a has order n, $a^r \neq e$ whenever $0 < r < n$.
In particular $(a^d)^i = a^{di} \neq e$ whenever $0 < i < h$, since $0 < di < n$. Therefore a^d has order at least h. On the other hand $(a^d)^h = a^{dh} = a^n = e$, so a^d has order precisely h. So by Corollary 1 and ①

order of $a^k = |\langle a^k \rangle| \overset{①}{=} |\langle a^d \rangle| =$ order of $a^d = h$ $\square$

Ex: In $\mathbb{Z}_{35}$ find

① the order of 15 and $\langle 15 \rangle$

Sol: $\gcd(15,35)=5$ so $\langle 15\rangle = \langle 5 \rangle$ and 15 has order $\frac{35}{5}=7$

② $\langle 28 \rangle$ and the order of 28

Sol: $\gcd(28,35)=7$ so $\langle 28\rangle=\langle 7\rangle$ and 28 has order $\frac{35}{7}=5$

③ $\langle 23\rangle$ and the order of 23

Sol: $\gcd(23,35)=1$ so $\langle 23\rangle = \langle 1 \rangle = \mathbb{Z}_{35}$ and 23 has order $\frac{35}{1}=35$.

Similarly, in any group, if a has order 35 then

- a^{15} has order 7 and $\langle a^{15}\rangle = \langle a^5\rangle$
- a^{28} has order 5 and $\langle a^{28}\rangle = \langle a^7 \rangle$
- a^{23} has order 35 and $\langle a^{23}\rangle = \langle a \rangle$

Cor 1: If G is cyclic and $a\in G$ then order of a divides order of G

Cor 2: If G is any group and $a \in G$ has order n then

$$\forall i,j\in\mathbb{Z} \quad \langle a^i\rangle \overset{①}{=} \langle a^j\rangle \iff \gcd(i,n) \overset{②}{=} \gcd(j,n)$$
$$\iff (\text{order of } a^i) \overset{③}{=} (\text{order of } a^j)$$

Pf: ③ $\xrightarrow{\text{Thm 4.2}}$ ② $\xrightarrow{\text{Thm 4.2}}$ ① $\xrightarrow{\text{Cor 1 of Thm 4.1}}$ ③. $\square$

Cor 3: If G is any group and $a\in G$ has order n then
$\langle a\rangle = \langle a^j\rangle \iff \gcd(n,j)=1 \iff a^j$ has order n

Cor 4: In $\mathbb{Z}_n$, $\langle k\rangle = \mathbb{Z}_n \iff \gcd(n,k)=1$.

Thm 4.3 (Fundamental Theorem of Cyclic Groups):

Let $G = \langle a \rangle$ be a cyclic group of order $n = |G|$.

① If $H \leq G$ then H is cyclic and $|H| \mid n$.

② If $k \mid n$ there is precisely one subgroup of order k, namely $\langle a^{\frac{n}{k}} \rangle$.

Pf: ① If $H = \{e\}$ then H is cyclic ($H = \langle e \rangle$) and $|H| = 1$ divides n.

Now assume $H \neq \{e\}$. Since $H \setminus \{e\}$ is a nonempty subset of $G = \{e, a, a^2, \dots, a^{n-1}\}$ there is a least m with $0 < m < n$ and $a^m \in H$.
We claim $H = \langle a^m \rangle$. By closure of H, $\langle a^m \rangle \subseteq H$.
Conversely, consider any $b \in H$. Say $b = a^k$.
Pick $q, r \in \mathbb{Z}$ with $k = mq + r$ and $0 \leq r < m$.
Since $a^k = b \in H$ and $a^{-mq} = (a^m)^{-q} \in H$, we have that

$$a^k a^{-mq} = a^{mq+r} a^{-mq} = a^r$$

belongs to H. Since $0 \leq r < m$ and m is the least positive integer with $a^m \in H$, we must have $r = 0$.
Therefore $k = mq + r = mq$ and $b = a^k = a^{mq} = (a^m)^q \in \langle a^m \rangle$.
This shows $H \subseteq \langle a^m \rangle$. We conclude $H = \langle a^m \rangle$.
By Thm 4.2 $|H| = \text{order of } a^m = \frac{n}{\gcd(n,m)}$ and $\frac{n}{\gcd(n,m)}$ is a divisor of n.

② Since $\gcd(n, \frac{n}{k}) = \frac{n}{k}$, $\langle a^{n/k} \rangle$ has order k by Thm 4.2.
If H is any other subgroup of order k then $H = \langle a^t \rangle$ for some t by ①. Then a^t and $a^{n/k}$ have equal order (k) and hence $H = \langle a^t \rangle = \langle a^{n/k} \rangle$ by Cor 2 to Thm 4.2. $\square$

Ex: If a has order 42, the list of subgroups of $\langle a \rangle$ is:

$\langle a \rangle$	order 42
$\langle a^2 \rangle$	order 21
$\langle a^3 \rangle$	order 14
$\langle a^6 \rangle$	order 7
$\langle a^7 \rangle$	order 6
$\langle a^{14} \rangle$	order 3
$\langle a^{21} \rangle$	order 2
$\langle a^{42} \rangle = \{e\}$	order 1

Cor: For each positive divisor k of n, $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k. These are the only subgroups of $\mathbb{Z}_n$.

Ex: Find all elements in $\mathbb{Z}_{24}$ of order 8.

Every element of order 8 must generate the unique subgroup of order 8, namely $\langle 24/8 \rangle = \langle 3 \rangle$. Since 3 has order 8, Cor 3 of Thm 4.2 tells us the generators of $\langle 3 \rangle$ are the numbers of the form $3i$ where $0 \leq i < 8$ and $\gcd(8, i) = 1$.

So they are: $3 \cdot 1,\ 3 \cdot 3,\ 3 \cdot 5,\ 3 \cdot 7$

or $3,\ 9,\ 15,\ 21$

Defn: The Euler phi function ϕ is

$$\phi(n) = |\{i \in \mathbb{Z} : 0 < i < n,\ \gcd(n, i) = 1\}| = |U(n)| \text{ when } n \in \mathbb{Z},\ n > 1$$

and $\phi(1) = 1$.

Thm 4.4 : Let G be a cyclic group of order n and let d be a positive divisor of n. Then the number of elements of G of order d is $\phi(d)$.

Pf: There is a unique subgroup of order d (Thm 4.3). By Cor 3 of Thm 4.2, the number of generators of this subgroup is $\phi(d)$. $\square$

Ex: If G is cyclic of order 24, G has $\phi(8) = 4$ elements of order 8.

Fact:
- p prime $\Rightarrow \phi(p^n) = p^n - p^{n-1}$
- n, m relatively prime $\Rightarrow \phi(nm) = \phi(n)\phi(m)$