## Sections 6 & 8

Last time: $G$ a group, $a \in G$, then

$$\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \} \subseteq G$$

is the cyclic subgroup generated by $a$. If $G = \langle a \rangle$, say $G$ is cyclic, generated by $a$.

Today: If $G$ is cyclic, what can it look like?

Answer: Up to isomorphism, $G$ is either

I $(\mathbb{Z}, +)$ or

II $(\mathbb{Z}_n, +)$ for some $n$.

If $H \leq G$, what can $H$ be?

Answer: In case I, $H = m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$ for some $m \in \mathbb{Z}$.

In case II $H = \{0, d, 2d, \ldots, n-d\} \subseteq \mathbb{Z}_n$ for some $d$ dividing $n$.

---

**Thm** Let $G$ be a cyclic group. Then $G$ is abelian.

**Proof** Let $a \in G$ be a generator, so $G = \langle a \rangle$, and all elements in $G$ are of the form $a^m$, $m \in \mathbb{Z}$. Given $a^m, a^n \in G$, have

$$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m. \qquad \square$$

**Division with remainder**: Let $n \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then there is a unique pair of integers $q, r$ with $r \in \{0, 1, \ldots, m-1\}$ such that

$$n = qm + r$$

Note: r = rest

Call $q$ "quotient" of $n$ by $m$ $\left(q = \left\lfloor \frac{n}{m} \right\rfloor\right)$

$r$ "remainder" when dividing $n$ by $m$

Example

$n = 23, \quad m = 7$

$23 : 7 = 3$

$\frac{21}{2}$ ($3 \uparrow q$, $2 \uparrow r$)

$n \quad q \quad m \quad r$

$23 = 3 \cdot 7 + 2$

**Thm** Let $G$ be a cyclic group, $H \leq G$. Then $H$ is cyclic.

**Proof** Let $a$ be generator of $G$, so all elements of $G$ & $H$ of the form $a^n$. (e.g. $G = \{a^n \mid n \in \mathbb{Z}\}$, $H = \{a^0, a^2, a^3, a^{-4}, \ldots\}$)

Case I $H = \{e\} = \{a^0\} \Longrightarrow H = \langle e \rangle$, cyclic

Case II $H \neq \{e\}$, so contains $a^n$ for some $n \neq 0$. Since $a^n \in H \overset{H \text{ group}}{\Longrightarrow} a^{-n} \in H$, must have some $a^n \in H$ with $n > 0$.

Let $m$ = smallest positive integer such that $a^m \in H$. Let $c = a^m$

Claim $H = \langle c \rangle$.

Let $a^n \in H$, & write $n = qm + r$, $r \in \{0, \ldots, m-1\}$.

Then $r = n - qm$, so

$$a^r = a^{n-qm} = a^n \{a^{-qm} = a^n (a^m)^{-q}$$

$a^n \in H$, $a^m \in H \Longrightarrow a^r = a^n (a^m)^{-q} \in H$.

Since $m$ was minimal positive s.t. $a^m \in H$, & $0 \leq r < m$, must have $r = 0$. Thus

$$a^n = a^{mq} = (a^m)^q \in \langle a^m \rangle.$$

□

Example $(\mathbb{Z}, +)$ is cyclic, so its subgroups are all of the form $\langle n \rangle = n\mathbb{Z}$ for $n \in \mathbb{Z}$.

Thm Let $G$ be cyclic group. If $|G| = \infty$, then $G \cong (\mathbb{Z}, +)$. If $|G| = n$, then $G \cong (\mathbb{Z}_n, +)$.

Proof Let $a$ be generator of $G$.

Case I: $a^m \neq e$ for all $m > 0$. (*)

Claim: Then all $a^n$, $n \in \mathbb{Z}$ are distinct. Assume for contradiction that $k < h$ with $a^k = a^h$.

$$a^{h-k} = a^h a^{-k} = a^h (a^k)^{-1} = e,$$ contradicting (*).

Function $\phi : \mathbb{Z} \to G$ given by $\phi(n) = a^n$ is one-to-one, onto, & $\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$, hence an isomorphism.

Case II $a^m = e$ for some $m > 0$, let $n$ be minimal positive integer s.t. $a^n = e$.

Claim: $a^0, a^1, \ldots, a^{n-1}$ are distinct.

Proof: If $0 \leq k < h \leq n-1$ s.t. $a^k = a^h$, then $a^{h-k} = e$. $0 < h-k < n$, contradicts $n$ minimal.

For all $s \in \mathbb{Z}$, have $s = nq + r$, $0 \leq r < n$, so

$$a^s = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r.$$

Hence $G = \{a^0, a^1, \ldots, a^{n-1}\}$. $\phi : \mathbb{Z}_n \to G$ $\phi(i) = a^i$ gives isomorphism $\mathbb{Z}_n \cong G$.

---

Starte felles divisor

Let $m, n \in \mathbb{Z}^+$. The greatest common divisor of $m$ & $n$, denoted $\gcd(m, n)$ is the biggest $d$ such that $d$ divides $m$ & $n$.

Notation: Write $d \mid m$ for "$d$ divides $m$".

E.g. $m=4$, $n=6$, divisors of 4: $\{1, 2, 4\}$
— " — 6: $\{1, 2, 3\}$
$\gcd(4,6)=2$.

If $m = p_1^{e_1} \cdots p_k^{e_k}$, $n = p_1^{f_1} \cdots p_k^{f_k}$ with $p_i$ distinct primes, then

$$\gcd(m,n) = p_1^{g_1} \cdots p_k^{g_k}, \qquad g_i = \min(e_i, f_i)$$

$12 = 2^2 3^1 5^0$, $10 = 2^1 3^0 5^1 \Rightarrow \gcd(12,10) = 2^1 3^0 5^0 = 2$.

**Thm** Let $G$ be cyclic group, $|G|=n$, let $b=a^s \in G$.
Then ① $\langle b \rangle$ has $\frac{n}{d}$ elements, $d=\gcd(n,s)$.
② $\langle b \rangle = \langle a^d \rangle = \{a^0, a^d, \ldots, a^{n-d}\} \simeq \mathbb{Z}_{\frac{n}{d}}$.

**Proof** Let $m$ be minimal positive such that $b^m = e$.
$|\langle b \rangle| = m$.
$b=a^s \Rightarrow m$ is minimal positive integer s.t. $a^{ms} = e$
$m$ — " — $ms = nk$ for some $k \in \mathbb{Z}$
**Fact**: minimal such is $m = \frac{n}{d}$, hence $|\langle b \rangle| = \frac{n}{d}$, proving ①.

For ②: Know $d \mid s$, since $d = \gcd(n,s)$.

$\Longrightarrow b = a^s \in \langle a^d \rangle \Rightarrow \langle b \rangle \subseteq \langle a^d \rangle$. But by ①, have $|\langle a^d \rangle| = \frac{n}{\gcd(d,n)} = \frac{n}{d}$, since $d \mid n$.
Hence $|\langle b \rangle| = |\langle a^d \rangle|$, so $\langle b \rangle = \langle a^d \rangle$.

□

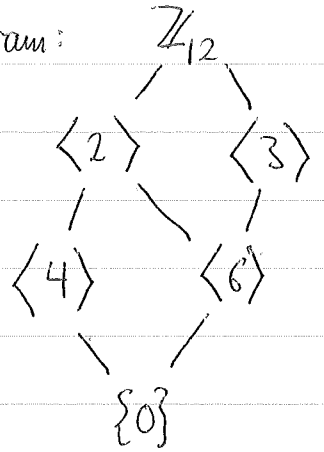
Corollary: Let $G$ be cyclic group, $|G| = n$.
Every subgroup $H \leq G$ is of the form

$$H = \langle a^d \rangle = \{a^0, a^d, \ldots, a^{n-d}\}$$

for some $d$ such that $d \mid n$.

Example: The divisors of 12 are 1, 2, 3, 4, 6, 12.
The subgroups of $(\mathbb{Z}_{12}, +_{12})$ are $\langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 6 \rangle, \langle 0 \rangle$.

Subgroup diagram:




## Permutation groups

Def Let $A$ be a set. A permutation of $A$ is a function $\phi : A \to A$ which is one-to-one & onto.
We write $S_A$ for the set of permutations of $A$.

Note If $\sigma, \tau$ are permutations of $A$, so is $\sigma \circ \tau$. Function composition $\circ$ defines a binary operation on $S_A$.

Notation: Let $\sigma \in S_A$. If $A$ is finite, can describe $\sigma$ by list of elements $x \in A$ above each value $\sigma(x)$. $\begin{pmatrix} \cdots & x & \cdots & y & \cdots \\ \cdots & \sigma(x) & \cdots & \sigma(y) & \cdots \end{pmatrix}$

Example: Let $A = \{a, b, c\}$, $\sigma \in S_A$ defined by

$$\sigma(a) = b \quad \sigma(b) = a \quad \sigma(c) = c.$$

Can write $\sigma = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$.

One more: $\sigma = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$ means $\sigma(a) = b$, $\sigma(b) = c$ $\sigma(c) = a$.

Thm Let $A$ be a set. Then $(S_A, \circ)$ is a group.

Proof: $G_1$, associative, if $\sigma, \tau, \psi \in S_A$, then

$$(\sigma \circ \tau) \circ \psi = \sigma \circ (\tau \circ \psi) \qquad \text{(Thm 2.13)}$$

• $G_2$, identity element. Let $\iota : A \to A$ be given by

$$\iota(x) = x \qquad \forall x \in A.$$

Then

$$(\sigma \circ \iota)(x) = \sigma(\iota(x)) = \sigma(x)$$
$$(\iota \circ \sigma)(x) = \iota(\sigma(x)) = \sigma(x) \qquad \forall x \in A,$$

so

$$\sigma \circ \iota = \iota \circ \sigma \iff \iota \text{ is identity element.}$$

- $G_3$, inverse. Let $\sigma \in S_A$, let $\sigma^{-1}$ be the inverse function, i.e. the one defined by

$$\sigma^{-1}(y) = x \iff y = \sigma(x).$$

$\sigma^{-1}$ exists because $\sigma$ is one-to-one & onto. Then

$$\sigma^{-1} \circ \sigma(x) = \sigma^{-1}(\sigma(x)) = x$$
$$\sigma \circ \sigma^{-1}(x) = \sigma(\sigma^{-1}(x)) = x \qquad \forall\, x \in A,$$

so $\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = \iota$.

□