Cyclic groups

Recall: A group G is <u>cyclic</u> if $\exists\, g \in G$ s.t. (generator for g)

$$G = \langle g \rangle = \{ g^k : k \in \mathbb{Z} \}.$$ (or $\{k \cdot g : k \in \mathbb{Z}\}$ if G is written additively)

If $G = \langle g \rangle$, $H = \langle h \rangle$, and $|G| = |H|$, then

the map $\tau : G \to H$ defined by $\tau(g^k) = h^k$

is an isomorphism.

- If G is cyclic and $|G| = n \in \mathbb{N}$ then

$$G \cong C_n = \langle x \mid x^n = e \rangle.$$ (presentation for C_n)

Ex: $\mathbb{Z}/n\mathbb{Z} \cong C_n$

- If G is cyclic and $|G| = \infty$ then

$$G \cong C_\infty = \langle x \mid \emptyset \rangle$$ (one generator and no relations)

Ex: $\mathbb{Z} \cong C_\infty$

Orders of elements in cyclic groups

Recall from Subgroups video:

If $g \in G$ then the order of g, denoted $|g|$ or $o(g)$, is defined to be the smallest $k \in \mathbb{N}$ satisfying $g^k = e$, or ∞ if there is no such k.

Theorem 0: $\forall g \in G$, $|g| = |\langle g \rangle|$. More precisely:

i) If $|g| = \infty$ then $g^i \neq g^j$, $\forall\, i,j \in \mathbb{Z}$ with $i \neq j$.

ii) If $|g| = n \in \mathbb{N}$ then $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$, and $g^i = g^j$ for $i,j \in \mathbb{Z}$ iff $i \equiv j \bmod n$.

- Infinite cyclic groups:

  Write $C_\infty = \langle x \rangle$. Then

  - $|\overset{=e}{x^0}| = 1$ ✓
  - $\forall k \in \mathbb{Z} \setminus \{0\}$, $|x^k| = \infty$ ✓

    Pf: Suppose $|x^k| = q$ for some $q \in \mathbb{N}$. Then

    $e = (x^k)^q = x^{kq} \Rightarrow |x| \leq |kq| \Rightarrow |C_\infty| < \infty$.

    Contradiction $\Rightarrow |x^k| = \infty$. $\boxtimes$

- Finite cyclic groups:

  * Lemma: If G is any group, $g \in G$, and $|g| = n \in \mathbb{N}$, then $\forall m \in \mathbb{Z}$,

$$g^m = e \iff m \equiv 0 \bmod n.$$

Pf: Suppose $g \in G$ and $|g| = n$. Then

- $m \equiv 0 \bmod n \Rightarrow g^m = e$: ✓

  $m = \ell n$ for some $\ell \in \mathbb{Z} \Rightarrow g^m = g^{\ell n} = (\underbrace{g^n}_{=e})^{\ell} = e$.

- $g^m = e \Rightarrow m \equiv 0 \bmod n$: ✓

  Write $m = qn + r$, $0 \le r < n$. Then

  $g^r = (g^n)^q g^r = g^m = e \Rightarrow r = 0$. (def. of order of g) ☒

Suppose $n \in \mathbb{N}$, write $C_n = \langle x \rangle$. Then

$$\forall k \in \mathbb{Z}, \quad |x^k| = \frac{n}{(k,n)}. \qquad \left(\text{Note: } \frac{n}{(k,n)} \in \mathbb{N}\right)$$

Pf: Using the lemma,

$$\{m \in \mathbb{Z} : (x^k)^m = e\} = \{m \in \mathbb{Z} : x^{km} = e\}$$

$$= \{m \in \mathbb{Z} : km \equiv 0 \bmod n\}$$

$$= \left\{m \in \mathbb{Z} : m \equiv 0 \bmod \frac{n}{(k,n)}\right\}. \quad (\text{see Integers modulo } n)$$

The order of x^k is the smallest positive integer in this set, which is $\frac{n}{(k,n)}$. ☒

Generators for C_n:

$$C_n = \langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}.$$

Since $|x^k| = \frac{n}{(k,n)}$, we have that

$$C_n = \langle x^k \rangle \iff (k,n) = 1.$$

So there are $\varphi(n)$ generators for C_n.

Exs: 1) $n = 15 = 3 \cdot 5$, $C_{15} = \langle x \rangle$ $(\varphi(15) = 2 \cdot 4 = 8)$

generators for C_{15}: $x^1, x^2, x^4, x^7, x^8, x^{11}, x^{13}, x^{14}$.

2a) If $n = p^\ell$, p an odd prime, $\ell \in \mathbb{N}$, then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, (Primitive Root Theorem) and $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n) = p^{\ell-1}(p-1)$.

- The number of primitive roots modulo n is $\varphi(\varphi(n)) = \varphi(p^{\ell-1}(p-1))$.
- If g is any primitive root mod n, then the collection of all primitive roots mod n is

$$\{g^k : 1 \leq k \leq \varphi(n), (k, \varphi(n)) = 1\}$$

(mod n)

2b) 5 is a primitive root mod 103 (from previous video)

$\varphi(103) = 102 = 2 \cdot 3 \cdot 17$

$\varphi(\varphi(103)) = \varphi(102) = 1 \cdot 2 \cdot 16 = 32$

Collection of all primitive roots mod 103:

$$\{\underbrace{5^k}_{(\text{mod } 103)} : 1 \le k \le 102,\ (k, 102) = 1\}.$$

Subgroups of cyclic groups

Theorem 1: If $G = \langle x \rangle$ and $H \leq G$ then either $H = \{e\}$ or $H = \langle x^k \rangle$, where k is the smallest positive integer with the property that $x^k \in H$.

Proof: Suppose $H \neq \{e\}$ and let $S = \{\ell \in \mathbb{N} : x^\ell \in H\}$.

Note that $\exists \ell \in \mathbb{Z} \setminus \{0\}$ s.t. $x^\ell \in H$, and also $x^{-\ell} \in H$, so $S \neq \phi$. Therefore, by the Well Ordering Principle, S has a smallest element, which we call k.

Now we have that:

- $\langle x^k \rangle \subseteq H$: ✓ $\quad x^k \in H \Rightarrow \langle x^k \rangle \subseteq H$.
- $H \subseteq \langle x^k \rangle$: ✓

(Division Algorithm)

$\forall h \in H$, $h = x^\ell$, for some $\ell \in \mathbb{Z}$. Write $\ell = qk + r$, $0 \leq r < k$.

Then $x^{-qk} \in H \Rightarrow x^r = x^{-qk} x^\ell \in H \Rightarrow r = 0$. (k is the smallest element of S)

Therefore, $h = (x^k)^q \in \langle x^k \rangle$.

We conclude that $H = \langle x^k \rangle$. ∎

- Infinite cyclic groups:

The distinct subgroups of $C_\infty = \langle x \rangle$ are

$$\{\langle x^k \rangle : k = 0, 1, 2, \ldots\}.$$

Proof: By Thm. 1, every subgroup of $C_\infty = \langle x \rangle$ is of the form $\langle x^k \rangle$, for some $k \in \{0, 1, 2, \ldots\}$. Suppose $k, \ell \in \{0, 1, 2, \ldots\}$ and $k < \ell$.

- If $k = 0$ then $\langle x^k \rangle = \{e\}$ but $|\langle x^\ell \rangle| = |x^\ell| = \infty$, so $\langle x^k \rangle \neq \langle x^\ell \rangle$.

- If $k > 0$ then $k \neq q\ell$, for any $q \in \mathbb{Z}$ so, by Theorem 0, $x^k \neq x^{q\ell}$, $\forall\, q \in \mathbb{Z}$. Therefore $x^k \notin \langle x^\ell \rangle$, so $\langle x^k \rangle \neq \langle x^\ell \rangle$. $\blacksquare$

Note: It follows from this that the only generators for $C_\infty = \langle x \rangle$ are x and x^{-1}.

To see this: Suppose $C_\infty = \langle x^\ell \rangle$ for some $\ell \in \mathbb{Z}$. Then $C_\infty = \langle x^{|\ell|} \rangle = \langle x^1 \rangle$ and, since the subgroups listed above are distinct, $|\ell| = 1 \Rightarrow \ell = \pm 1$.

- Finite cyclic groups:

Suppose $n \in \mathbb{N}$, write $C_n = \langle x \rangle$. Then there is exactly one subgroup of C_n of order d, for every $d \in \mathbb{N}$ with $d \mid n$. More precisely:

i) If $H \leq C_n$ then $|H| \mid n$.

ii) If $d \in \mathbb{N}$, $d \mid n$, then $|\langle x^{n/d} \rangle| = d$.

iii) If $H \leq C_n$ with $|H| = d$, for some $d \mid n$, then $H = \langle x^{n/d} \rangle$.

Pf. of i): Follows from Lagrange's Theorem. $\blacksquare$

Pf. of ii): $|\langle x^{n/d} \rangle| = |x^{n/d}|$ (Thm 0)

$$= \frac{n}{(n/d, n)} = \frac{n}{(n/d)} = d. \quad \blacksquare$$

$n = d(n/d) \Rightarrow \frac{n}{d} \mid n$

Pf of iii): Let k be the smallest positive integer with the property that $x^k \in H$, so that $H = \langle x^k \rangle$. Then

$$d = |H| = |x^k| = \frac{n}{(k,n)} \Rightarrow (k,n) = \frac{n}{d}$$

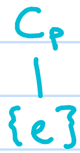
$$\Rightarrow \frac{n}{d} \mid k \Rightarrow x^k \in \langle x^{n/d} \rangle$$

$$\Rightarrow H \leq \langle x^{n/d} \rangle.$$

But $|H| = d = |\langle x^{n/d} \rangle| \Rightarrow H = \langle x^{n/d} \rangle$. $\blacksquare$

Exs: Lattices of subgroups of cyclic groups

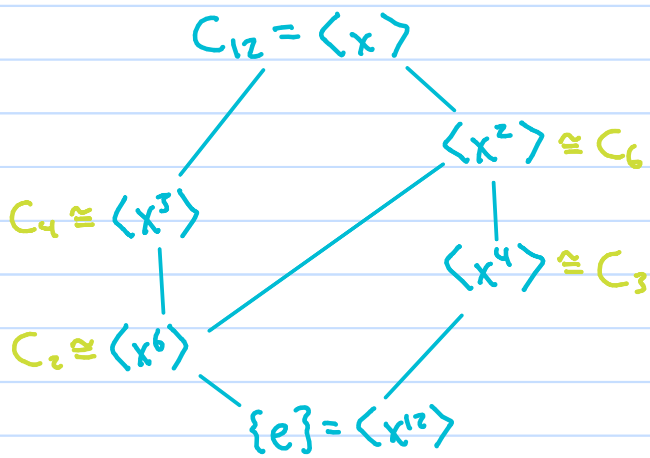
1) p prime:



2) $C_{12} = \langle x \rangle$: $12 = 2^2 \cdot 3^1$

(6 total)

divisors of 12: $2^a 3^b$, $0 \le a \le 2$, $0 \le b \le 1$: 1, 2, 3, 4, 6, 12



3) $C_\infty = \langle x \rangle$: $\langle x^k \rangle \le \langle x^\ell \rangle \iff \ell \mid k$