Cyclic Groups

Recall G is cyclic if $G = \langle a \rangle$ for some $a \in G$.

$$\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$$

$$a^0 = e, \quad a^k = \underbrace{a * a * \cdots * a}_{k \text{ times}}$$
$$a^{-k} = a^{-1} * a^{-1} * \cdots * a^{-1}$$

As we go on, we may write ab to mean $a * b$

Theorem: If G is cyclic, then G is abelian.

Proof:

Know $G = \langle a \rangle$ for some $a \in G$.

$x = a^k$, $y = a^l$

$$x * y = (\underbrace{a * a * \cdots * a}_{k\text{-times}}) * (\underbrace{a * a * \cdots * a}_{l\text{-times}}) = a^{k+l}$$

$y * x = a^{l+k}$ Since $l+k = k+l$, $x * y = y * x$.

Big idea $a^k * a^l = a^{k+l}$, so its commutative! $\square$

Theorem: Let G be a cyclic group. Then either $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}_n$ for $n = |G|$.

Proof: $G = \langle a \rangle$ for $a \in G$.

Case I ($|G|$ is infinite)

Define a function

$$f : \mathbb{Z} \longrightarrow G$$
$$m \longmapsto a^m$$

If $x \in G$, then $x = a^m$ for some m

Therefore $x = f(m)$. Thus f is surjective!

Now suppose f is <u>not</u> injective. Then there exists $m, n \in \mathbb{Z}$ with $m \neq n$ but $f(m) = f(n)$.

Then $a^m = a^n \Rightarrow a^{n-m} = e$

$$G = \langle a \rangle = \{a, a^2, a^3, \ldots, a^{n-m-1}, e, a, a^2, \ldots, a^{n-m-1}, e, \ldots\}$$
$$= \{e, a, a^2, \ldots, a^{n-m-1}\}.$$

Assumed $|G|$ infinite! $\Rightarrow\Leftarrow$.

Thus f injective!

$\boxed{\text{Thus } f \text{ is bijective!}}$

Last thing ~ NTS $f(m+n) = f(m) * f(n)$ $\forall\, m, n \in \mathbb{Z}$

$f(m+n) = a^{m+n}$

$f(m) * f(n) = \underbrace{(a * a * \ldots * a)}_{m} \underbrace{(a * a * \ldots * a)}_{n} = a^{m+n}$

$=$

Case 2 ($|G| = n < \infty$)

$$f : \mathbb{Z}_n \longrightarrow G, \quad f(k) = a^k$$

TRY THIS AT HOME: Show f is an isomorphism!

$\square$

Moral of the story: cyclic groups are really just $\mathbb{Z}$ or $\mathbb{Z}_n$.

<u>Theorem</u>: Suppose $G = \mathbb{Z}_n$. Then $f : G \to G$ is an isomorphism if and only if

$f(k) = mk$ for some m relatively prime to n.

<u>Proof</u>:

$f : G \to G$ be an isomorphism

Then $\boxed{f(1) = m}$ for some $m \in \mathbb{Z}_n$.

But f is a bijection! So also $\exists\ k \in \mathbb{Z}_n$ so that $\boxed{f(k) = 1.}$

$$\boxed{f(k) = f(1+1+1+1+\ldots+1)} = f(1)+f(1)+f(1)+\ldots+f(1)$$
$$= m + m + m + \ldots + m = mk$$

$mk = 1$ in $\mathbb{Z}_n$ $\Rightarrow \exists\ \ell \in \mathbb{Z}$ with $mk = 1 + \ell n$

$mk - \ell n = 1$ $\therefore$ m, n are relatively prime!

For any j, $f(j) = mj$

In summary,

$f(j) = mj\ \forall\ j \in \mathbb{Z}_n$ and m, n are relatively prime.

Conversely, if we start with $m \in \mathbb{Z}_n$ with m, n relatively prime, then

$f(j) = mj$ is an isomorphism.

To show this, need to check bijectivity + respects binary operations.

$$f(j+k) = m(j+k) = mj + mk = f(j) + f(k) \quad \checkmark$$

m, n relatively prime $\Rightarrow \exists\ a, b \in \mathbb{Z}$ w/ $am + bn = 1$

$\Rightarrow$ $am = 1$ in $\mathbb{Z}_n$. $\Rightarrow$ $f(a) = 1$

$$\Rightarrow f(aj) = f(a + a + \ldots + a)$$
$$= f(a) + f(a) + \ldots + f(a)$$
$$= 1 + 1 + \ldots + 1 = j$$

This proves surjectivity, hence bijectivity. $\square$

Subgroups of cyclic groups

Theorem: If G is cyclic and $H \leq G$ then H is cyclic!

Proof: $G = \langle a \rangle$ for some $a \in G$.

$G = \{a, a^2, a^3, \ldots\}$

$H = \{a^{k_1}, a^{k_2}, \ldots, a^{k_m}, \ldots \mid$ for some integers $k_1, k_2, \ldots\}$

Choose $r \in \mathbb{Z}$, $r > 0$ such that r is the smallest positive integer with $a^r \in H$.

Claim: $H = \langle a^r \rangle$.

$\langle a^r \rangle = \{a^r, a^{2r}, a^{3r}, \ldots\}$

Key point: H has inverses too!

S'pose $H \neq \langle a^r \rangle$. Then $\exists\, m > 0$ w/ $a^m \in H$ but $a^m \notin \langle a^r \rangle$.

I know $m > r$ $\quad m = jr + s$ where $0 \leq s < r$

Then

$a^s = a^{m-rj} = a^m * (a^{-r})^j \in H$ $\quad$ Thus $a^s \in H$ $\Rightarrow\Leftarrow$ because r is smallest.

Thus $H = \langle a^r \rangle$

$\square$

Example: Subgroups of $\mathbb{Z}_6$.

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0, 1, 2, \ldots 5\} = \mathbb{Z}_6$

$\langle 2 \rangle = \{0, 2, 4\}$

$\langle 3 \rangle = \{0, 3\}$

~~$\langle 4 \rangle = \{4, 2, 0\}$~~

~~$\langle 5 \rangle = \{5, 4, 3, 2, 1, 0\}$~~

Generators:

G group. $\quad a, b \in G$

$a^2, \ b^2, \ ab, \ ba, \ aba, \ ab^2ab^3a^7, \ldots$

$a^{-2}bab^{-3}a^2, \ldots$

All these guys together form a group $\langle a, b \rangle$ called the subgroup generated by a and b.

Proposition: S'pose $\Lambda \subseteq \mathcal{P}(G)$ is a collection of subgroups of G.

Then

$$\bigcap_{H \in \Lambda} H = \{ x \in G \mid x \in H \ \forall \ H \in \Lambda \}$$

is a subgroup of G.

Proof:

NTS $a, b \in \bigcap_{H \in \Lambda} H$, $ab^{-1} \in \bigcap_{H \in \Lambda} H$

I know $a, b \in H \ \forall \ H \in \Lambda \Rightarrow ab^{-1} \in H \ \forall \ H \in \Lambda$

$\Rightarrow ab^{-1} \in \bigcap_{H \in \Lambda} H$

$\square$

Particular case: $S \subseteq G$

$\Lambda = \{ H \leq G \mid S \subseteq H \}$

$\bigcap_{H \in \Lambda} H$ is a subgroup

It's the smallest subgroup containing S

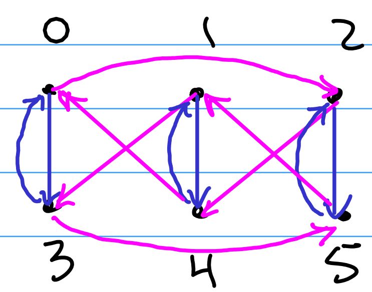
This is the subgroup $\langle S \rangle$ generated by S.

Ex: $\mathbb{Z}_6$ is generated by 2, 3

$\underline{2+2} = 4$, $\underline{2+3} = 5$, $\underline{2+2+3} = 1$

$\underline{3+3} = 0$

Visualize how things generate a group with a <u>Cayley digraph</u>.



<u>Group</u>: $\mathbb{Z}/6$

<u>Generators</u>: 2, 3