Reference

Tuesday, April 23, 2024 4:08 PM

http://abstract.ups.edu/aata/aata.html chapter 4, 6, 9 and 15

Isomorphism

Thursday, April 25, 2024 4:22 PM

Def: Two groups $(G, \cdot)$ and $(H, \circ)$ are $\boxed{\text{isomorphic}}$ if $\exists$ bijective mapping

$\phi: G \to H$ s.t. $\underbrace{\phi(a \cdot b)}_{\cdot \text{ then map}} = \underbrace{\phi(a) \circ \phi(b)}_{\text{map then } \circ}$ (homomorphism + bijection)

Example: $\mathbb{Z}/4\mathbb{Z} \cong \langle i \rangle$ $\quad \phi: \mathbb{Z}/4\mathbb{Z} \to \langle i \rangle$

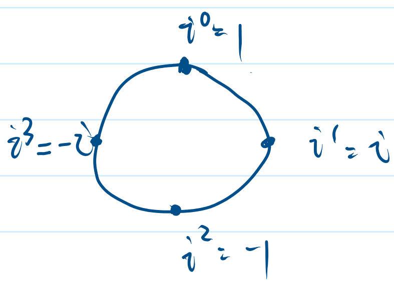
$\phi(n) \mapsto i^n$

$\phi(0) = 1 = i^0$

$\phi(1) = i = i^1$ and $\phi(m+n) = i^{m+n} = i^m i^n = \phi(m)\phi(n)$

$\phi(2) = -1 = i^2$

$\phi(3) = -i = i^3$



Theorem: $\phi: G \to H$ isomorphism, then:

1. $\phi^{-1}: H \to G$ is isomorphism
2. $|G| = |H|$
3. G abelian $\to$ H abelian
4. G cyclic $\to$ H cyclic
5. G has subgroup of order n $\to$ H has subgroup of order n

☆ **Theorem:** ① G = cyclic group of infinite order $\cong \mathbb{Z}$ $\quad \phi: \mathbb{Z} \to G$, $\phi: n \mapsto a^n$

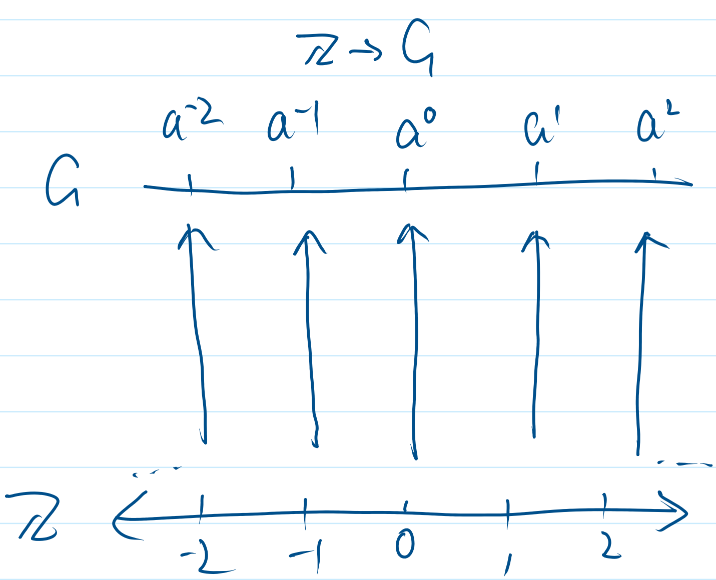
② G = cyclic group of order $n \cong \mathbb{Z}/n\mathbb{Z}$ $\quad \phi: \mathbb{Z}/n\mathbb{Z} \to G$, $\phi: k \mapsto a^k$, $0 \le k < n$

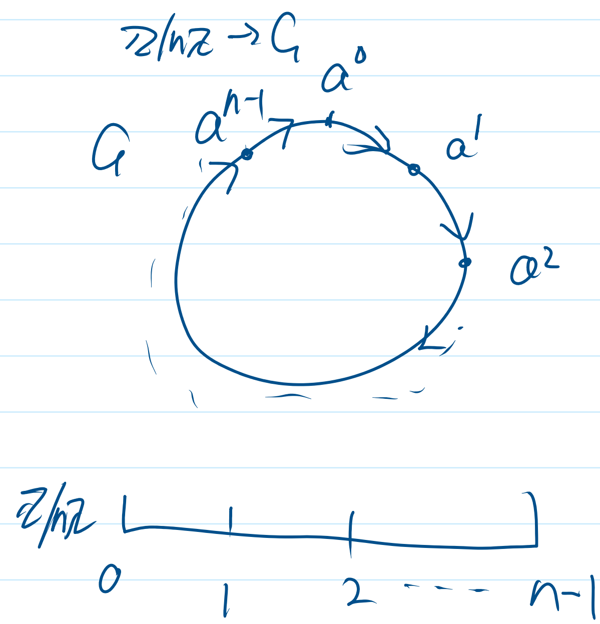
② G = cyclic group of order $n \cong \mathbb{Z}/n\mathbb{Z}$ $\quad \phi: \mathbb{Z}/n\mathbb{Z} \to G$

$\phi: k \mapsto a^k, \; 0 \le k < n$

③ G = group of order $p \cong \mathbb{Z}/p\mathbb{Z}$

In fact every group of order p is cyclic, and every non-identity (g!=e) element in it is generator. This is a corollary of Lagrange's Theorem.



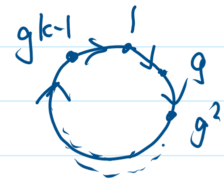


Now you see how important it is to study Z, Z/nZ and Z/pZ.

More cyclic groups

Friday, April 19, 2024 12:07 PM

Often a subgroup will depend entirely on a single element of the group



Example: $3\mathbb{Z} = \{\dots, -3, 0, 3, 6 \dots\}$ (cyclic subgroup of $\mathbb{Z}$)

generated by 3 (or -3)

Example: $H = \{2^n : n \in \mathbb{Z}\}$ under $\cdot$ (cyclic subgroup of $(\mathbb{Q}, \cdot)$)

$= \{\dots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, \dots\}$

identity

inverses

generated by 2 (or 2^{-1})

Theorem: Let G be a group and a be any element in G, then

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\} \text{ under } \cdot$$

is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G that contains a. If binary operator is $+$, then:

$$\langle a \rangle = \{na : n \in \mathbb{Z}\}$$

Def: If $G = \langle a \rangle$, then G is a cyclic group and call a generator.

Def: For $a \in G$, order of a is the smallest positive integer n s.t. $a^n = e$. $(|a| = n)$

because $a^n = e$, $a^{2n} = e$, $a^{3n} = e$, ... and so on

If no such n then $|a| = \infty$

Example: Cyclic group can have more than 1 generator:

$\mathbb{Z}/6\mathbb{Z} = \langle 1 \rangle = \langle 5 \rangle$

But not every element is generator:

$\langle 2 \rangle = \{0, 2, 4\} \neq \mathbb{Z}/6\mathbb{Z}$

Example: generators of $\mathbb{Z}$ are 1 ~~and~~ or -1

generators of $\mathbb{Z}/n\mathbb{Z}$ are 1 and some other elements

Theorem: Cyclic $\Rightarrow$ Abelian

idea: $R = \overbrace{\underbrace{a + a + \cdots + a}_{x \text{ times}}}^{P} + \overbrace{\underbrace{a + \cdots + a}_{y \text{ times}}}^{Q}$

$= \overbrace{\underbrace{a + a + \cdots + a}_{y \text{ times}}}^{Q} + \overbrace{\underbrace{a + \cdots + a}_{x \text{ times}}}^{P}$

https://www.rareskills.io/post/group-theory-and-coding

But Abelian $\not\Rightarrow$ cyclic

Theorem: Every subgroup of cyclic group is cyclic.

Corollary: Subgroups of $\mathbb{Z}$ are just $n\mathbb{Z}$ for $n \in \mathbb{Z}^+$.

Proposition: G cyclic with order n, $G = \langle a \rangle$, then $a^k = e$ iff $n \mid k$.

$a^n = e,\ a^{2n} = e,\ a^{3n} = e, \ldots$

★ element in cyclic group

☆ **Theorem:** G cyclic with order n, $G=\langle a\rangle$, then order of a^k is $\frac{n}{\gcd(k,n)}$.

element in cyclic group

Proof: Goal is to find smallest integer m s.t. $(a^k)^m = e$. By proposition above, this m is the smallest integer s.t. $n \mid km$.

order of a^k

$$n \mid km \Rightarrow \underbrace{\frac{n}{\gcd(k,n)}} \mid m \cdot \underbrace{\frac{k}{\gcd(k,n)}} \qquad \frac{n}{\gcd(k,n)} \nmid \frac{k}{\gcd(k,n)}$$

coprime

(because they are in "simplified form")

example: $\gcd(12,18)=6$

$\frac{12}{6}=2$

$\frac{18}{6}=3$

2 and 3 are coprime

$$\Rightarrow \frac{n}{\gcd(k,m)} \mid m \quad \text{must hold}$$

$$\Rightarrow \boxed{m = \frac{n}{\gcd(k,n)}} \text{ is the smallest possibility}$$

The theorem above provides a way to count # generators in a finite cyclic group.

Corollary: $G=\langle a\rangle$ order n cyclic group, then a^k is a generator iff $\gcd(k,n)=1$. # generators $=\phi(n)$

element in cyclic group

Euler's phi function

Example: $\mathbb{Z}/16\mathbb{Z}$ coprime elements: $\underbrace{1,3,5,7,9,11,13,15}$

They are all generators

For example, $\langle 9\rangle$:

$1\cdot 9=9$	$2\cdot 9=2$	$3\cdot 9=11$
$4\cdot 9=4$	$5\cdot 9=13$	$6\cdot 9=6$
$7\cdot 9=15$	$8\cdot 9=8$	$9\cdot 9=1$
$10\cdot 9=10$	$11\cdot 9=3$	$12\cdot 9=12$
$13\cdot 9=5$	$14\cdot 9=14$	$15\cdot 9=7$

$13 \cdot 9 = 5 \quad 14 \cdot 9 = 14 \quad 15 \cdot 9 = 7$

$(\bmod 16)$

Coset

Tuesday, April 23, 2024 4:16 PM

Cosets were defined to help proving Lagrange's Theorem.

<u>Def:</u> $H < G$ (subgroup), left coset of H with representative $g \in G$ is:

$$gH = \{gh : h \in H\}$$

Right coset:

$$Hg = \{hg : h \in H\}$$

<u>Example:</u> $H < \mathbb{Z}/6\mathbb{Z} = \{0,3\}$. Cosets:

$$\underbrace{0+H}_{\{0,3\}} = \underbrace{3+H}_{\{3,6=0\}} = \{0,3\}$$

$$\underbrace{1+H}_{\{1,4\}} = \underbrace{4+H}_{\{4,7=1\}} = \{1,4\}$$

$$\underbrace{2+H}_{\{2,5\}} = \underbrace{5+H}_{\{5,8=2\}} = \{2,5\}$$

$(\mathbb{Z}/6\mathbb{Z}, +)$ is commutative, so left cosets = right cosets

<u>Lemma:</u> $H < G$, $g_1, g_2 \in G$. The followings are equivalent:

1. $\boxed{g_1 H = g_2 H}$
2. $H g_1^{-1} = H g_2^{-1}$
3. $g_1 H \subset g_2 H$
4. $g_2 \in g_1 H$
5. $g_1^{-1} g_2 \in H$

g_1/g_2

just tools for proofs

☆ <u>Theorem:</u> $H < G$. Left cosets of H in G partition G. That is, G is disjoint union of left cosets of H.

$G = \{g_1, \dots, g_6\}$

g_1H	g_4H
g_2H	g_5H
g_3H	g_6H

$\boxed{|gH| = |H|}$

Not going to prove this

Proof: Let g_1H and g_2H be 2 cosets. We show $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$. Suppose $g_1H \cap g_2H \neq \emptyset$, pick $a \in g_1H \cap g_2H$, then:

$$\begin{cases} a = g_1h_1 & \text{for } h_1 \in H \\ a = g_2h_2 & \text{for } h_2 \in H \end{cases}$$

$g_1H = \{g_1h : h \in H\}$

$g_2H = \{g_2h : h \in H\}$

$\Rightarrow g_1h_1 = g_2h_2$

$g_1 = g_2(h_2h_1^{-1}) \rightarrow h_2h_1^{-1} \in H$ by closure

$g_2(h_2h_1^{-1}) = \boxed{g_1 \in g_2H} \rightarrow$ because $g_2(h_2h_1^{-1}) \in H$

By Lemma above, $g_1H = g_2H$.

Def: Index = # left cosets of H in G.

$\uparrow$

$[G:H]$

Example: $\mathbb{Z}/6\mathbb{Z}$, $H = \{0,3\} < G \rightarrow [G:H] = 3$

Because:

$0+H = 3+H = \{0,3\}$

$1+H = 4+H = \{1,4\}$

$2+H = 5+H = \{2,5\}$

Lagrange's Theorem

Tuesday, April 23, 2024 4:13 PM

Lagrange's Theorem: G finite group, $H < G$, then $|H| \mid |G|$.

$$\frac{|G|}{|H|} = [G:H]$$

Corollary: G finite, $g \in G$, then order of g divides # elements in G.

Order of an element is just the size of the cyclic subgroup it generates. $\langle g \rangle$ g^k

☆ Corollary: $|G| = p$, then G is cyclic and any $g \neq e$ is generator.

https://www.ret2basic.me/2024/04/12/elliptic-curve-attacks-small-subgroup.html

First half of this article