Algebra. Lec 5.

Cyclic groups

$(\mathbb{Z},+)$ infinite group

$\{0\} \neq H \leq \mathbb{Z}$. let $a \in H$ be the smallest positive integer.

$\Rightarrow H = \{na \mid n \in \mathbb{Z}\}$

Pf. $y \in H$. $y = na + r$, $0 \leq r < a$.

$r = y - na \in H \Rightarrow r = 0$ $\square$

Def. G is cyclic if $\exists\, a \in G$, s.t. every element of G can be written in the form a^n, for some n. a: generator of G

i.e. $G = \langle a \rangle$ for some $a \in G$

$f: \mathbb{Z} \twoheadrightarrow G$ surjective, hom

$\# \longrightarrow a^{\#}$

Rmk. G: group. $a \in G$

$\{a^n \mid n \in \mathbb{Z}\} \leq G$

Cyclic subgroup of G

· $f : \mathbb{Z} \to G$ group hom
$\# \mapsto a^{\#}$

$H = \ker(f)$

① H is trivial $\Rightarrow$ $\mathbb{Z}/\ker(f) \simeq \operatorname{im}(f) = \langle a \rangle \hookrightarrow G$

$$\mathbb{Z}/\ker(f) = \mathbb{Z}$$

② H is not trivial. $\Rightarrow \ker f \leq \mathbb{Z}$

$H \leq \mathbb{Z}$

$\ker f = \{nd \mid n \in \mathbb{Z}\}$ for some d.

$\Rightarrow \mathbb{Z}/d\mathbb{Z} \simeq \operatorname{im}(f) = \langle a \rangle = \{1, a, a^2, \dots, a^{d-1}\}$.

order of a is d.

order of $\langle a \rangle$ is d.

period.

Rmk. G. finite group $|G| = n$.

$e \neq a \in G \Rightarrow \langle a \rangle \leq G$

$|a| \mid |G|$

Rmk. $|G| = p$. prime.

$\forall.\ e \neq a \in G \Rightarrow |a| = p$.

$\Rightarrow G$ is cyclic

Prop. G. cyclic. $\Rightarrow$ ① any subgroup of G is cyclic

② $f: G \to G'$ hom

$\mathrm{im}(f)$ is cyclic

Pf. ① • G is infinite cyclic

$G \simeq \mathbb{Z}$. (every subgroup of $\mathbb{Z}$ is cyclic) we already have this

• G is finite. cyclic.

$H \leq G$. (want to show H is cyclic).

$$\begin{array}{ccc} & & \langle a \rangle \\ & & \shortparallel \\ f: \mathbb{Z} & \twoheadrightarrow & G \quad \text{hom} \\ \# & \longmapsto & a^{\#} \\ \rotatebox{90}{$\leq$} & & \rotatebox{90}{$\leq$} \\ f^{-1}(H) & \twoheadrightarrow & H. \end{array}$$

use subgroup criterion.

$f^{-1}(H) = \{ n \cdot m \mid n \in \mathbb{Z} \}$. for some m.

$$\begin{array}{c} f: f^{-1}(H) \twoheadrightarrow H \quad \text{hom} \\ \shortparallel \\ \langle m \rangle \end{array}$$

$\Rightarrow f(m)$ generates H.

Rmk.

① 2 cyclic groups of same order m are iso.

$G=\langle a\rangle$. $|G|=m$.

$$f: \mathbb{Z} \twoheadrightarrow G$$
$$n \mapsto a^n$$

if $\ker(f) = k\mathbb{Z}$. $\mathbb{Z}/k\mathbb{Z} \simeq G \Rightarrow k=m$.

$$G' \simeq \mathbb{Z}/m\mathbb{Z} \simeq G.$$

② any infinite cyclic group has exactly 2 generators $(-1 / 1)$

③ G finite cyclic group of order n

$$\underset{\langle x\rangle}{G} \simeq \mathbb{Z}/n\mathbb{Z}$$

$\{\text{generators of } G\} = \{y\in G \mid \langle y\rangle = G\}$

$$= \underbrace{\{x^{\nu} \mid (\nu, n)=1\}} \qquad |\{x^{\nu} \mid (\nu,n)=1\}| = \varphi(n)$$

Euler φ-function

if $(\nu,n)=1 \Rightarrow \exists a, b.$ s.t. $a\nu+bn=1$.

$$(x^{\nu})^a = x^{1-bn} = x. \quad x\in\langle x^{\nu}\rangle \Rightarrow \langle x\rangle \leq \langle x^{\nu}\rangle \leq G$$

④. G : group $a \in G$

$$a^m = 1 = a^n \Rightarrow a^{(m,n)} = 1$$

Pf. $lm + kn = (m,n)$

$$a^{lm+kn} = 1 = a^{(m,n)}$$

⑤ $G = \langle a \rangle$. $|a| = n$.

$$\Rightarrow |a^k| = \frac{n}{(n,k)}$$

Pf. let $(n,k) = c$

$$\begin{pmatrix} n = lc \\ k = mc \\ (l,m) = 1 \end{pmatrix} \quad \frac{n}{(n,k)} = \frac{n}{c} = l$$

$$(a^k)^l = a^{mcl} = (a^n)^m = 1$$

$\Rightarrow |a^k| \,\big|\, l.$ ← there. $|a^k|$ is min.

$a^n = 1 = (a^k)^{|a^k|} \Rightarrow n \,\big|\, k|a^k|$ ← there. n is min

$$\Rightarrow lc \,\big|\, mc|a^k| \Rightarrow l \,\big|\, |a^k| \Rightarrow l = |a^k|$$

⑥. $G=\langle a\rangle=\langle b\rangle$.

$$f: G \to G \qquad \text{i.e. } f\in \mathrm{Aut}(G).$$
$$a \mapsto b.$$

⑦. G is cyclic of order n, $d \mid n$

$\Rightarrow \exists!$ subgroup of G of order d. $(\mathbb{Z}/10\mathbb{Z})$.

Pf: $G=\langle a\rangle=\{1, a, a^2, \dots, a^{n-1}\}$

we have $H=\langle a^{\frac{n}{d}}\rangle=\{1, a^{\frac{n}{d}}, a^{\frac{2n}{d}}, \dots, a^{\frac{(d-1)n}{d}}\}$

Suppose $K\leq G$. $|K|=d$

K: cyclic $\Rightarrow K=\langle a^k\rangle$ for some k

$d=|K|=|a^k|=\frac{n}{(n,k)}$ $\quad (n,k)=\frac{n}{d} \Rightarrow k=\frac{n}{d}$.

⑧. G_1, G_2 . cyclic groups of order m, n respectively

$(m,n)=1$

$\Rightarrow G_1\times G_2$ is cyclic of order mn. e.g. $(\mathbb{Z}/3\mathbb{Z})\times(\mathbb{Z}/5\mathbb{Z})\times(\mathbb{Z}/7\mathbb{Z})\cong(\mathbb{Z}/105\mathbb{Z})$

Pf. $G_1=\langle a\rangle$. $G_2=\langle b\rangle$. $|a|=m$, $|b|=n$.

$$f : \mathbb{Z} \to G_1 \times G_2 \qquad \text{hom.}$$
$$\# \mapsto (a^{\#}, b^{\#})$$

$(m,n)=1 \Rightarrow \exists\, l, k$ s.t. $lm+kn=1$

$$lm \longmapsto (a^{lm}, b^{1-kn}) = (1, b)$$
$$kn \longmapsto (a^{1-lm}, b^{kn}) = (a, 1)$$

$$f(h_2(lm)+h_1(kn))$$
$$= (a,1)^{h_1}(1,b)^{h_2}$$
$$= (a^{h_1}, 1)(1, b^{h_2})$$
$$= (a^{h_1}, b^{h_2})$$

$\Rightarrow$ surjective

$$\ker(f) = \{h \in \mathbb{Z} \mid m \mid h,\ n \mid h.\} = mn\mathbb{Z}$$

$$\Rightarrow \mathbb{Z}/mn\mathbb{Z} \simeq G_1 \times G_2.$$

Chinese Remainder

For example.
$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$
$$x \longmapsto (x \pmod 3,\ x \pmod 5,\ x \pmod 7).$$

$\Rightarrow \ker(f) = 105\mathbb{Z}$. & surjective.

Exercise

[DF] Sec 2.3. ex 21 . ex 23 . ex 26.

hint. $(\mathbb{Z}/2^n\mathbb{Z})^\times$ not cyclic

find 2 distinct order 2 elements.

2^n-1. $2^{n-1}-1$

[Reading]. [L] Butterfly proof

Conrad's note

$$(\mathbb{Z}/p\mathbb{Z})^\times \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +).$$

as set. $\{\bar{k} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{k}$ has a multiplicative inverse $\}$

i.e. $\exists\, \bar{k}'$ s.t $\bar{k}\bar{k}' = \bar{1}$

if. $(k, n) = 1$. $\exists\, ak + bn = 1$

$\Rightarrow \bar{a}\bar{k} = \bar{1}$

$(k, n) = 1$

$((\mathbb{Z}/n\mathbb{Z})^\times, \cdot) \Rightarrow$ group.