GroupAction5

2023年3月4日 星期六 上午11:59

Bezout's Lemma.

Chinese Remainder Theorem

Equivalence Relation

Equivalence Class

Theorem: Let G be a cyclic group.

(a) If $|G| = n$ is finite, then G is isomorphic to C_n.

(b) If $|G|$ is infinite, then G is isomorphic to $\mathbb{Z}$.

proof: (a) Let g be a generator of G.

$$G = \langle g \rangle = \{e, g, g^2, \cdots g^{n-1}\}$$

By proposition, G is isomorphic to C_n.

(b). If g is a generator of G with infinite order:

$$\phi: G \to \mathbb{Z}$$

$$\phi(g^r) \to r \quad \text{isomorphism.}$$

$$\phi(g^{r_1}) + \phi(g^{r_2}) = \phi(g^{r_1} g^{r_2}) = \phi(g^{r_1+r_2})$$

$$r_1 + r_2 \qquad = r_1 + r_2 \ \checkmark \qquad \square$$

Theorem: Let G be a cyclic group and $H \leq G$, Then H is cyclic.

proof: Let $G = \langle g \rangle$, If $H = \{e\}$ $H = \langle e \rangle$ ✓

Otherwise, we define $n = \min\{\overbrace{k>0}: g^k \in H\}$.

$g^k \in H \neq \{e\}$. for some $k \neq 0$ well-defined.

H is a subgroup. $g^{-k} = (g^k)^{-1} \in H$ $\pm k$ one of them is positive

We want to show that. $H = \langle g^n \rangle$.

We want to show that. $H = \langle g^n \rangle$.

$g^n \in H \quad \langle g^n \rangle \subseteq H$

$g^a \in H$. division algorithm. $\exists q, r \in \mathbb{Z}$, $a = qn + r$. $0 \le r < n$.

$g^r = g^{a-qn} = g^a \cdot (g^n)^{-q} \in H$.

By minimality of n. $r = 0$. $\quad e = g^a \cdot (g^n)^{-q} \Rightarrow g^a = (g^n)^q \in \langle g^n \rangle$.

$H \subseteq \langle g^n \rangle$ □

Subgroup of $\mathbb{Z} = m\mathbb{Z}$. $m \in \mathbb{Z}$.

Proposition: Let m, n be non-zero integers.

$\langle m, n \rangle = \langle h \rangle$ highest common factor hcf. gcd $\quad \langle m \rangle \cap \langle n \rangle = \langle l \rangle$ lcm

for some $h, l > 0$. h. has the following properties.

(a) $h \mid m$ and $h \mid n$.

(b) if $x \mid m$ and $x \mid n$ then $x \mid h$.

(c). $\exists u, v \in \mathbb{Z}$ such that $um + vn = h$. Bézout's Lemma

l has the following properties

(d) $m \mid l$ and $n \mid l$.

(e). if $m \mid x$ and $n \mid x$, then $l \mid x$.

proof: (a). $m = 1m + 0n \in \langle m, n \rangle = \langle h \rangle$. $\underbrace{h_1 + h_1 \cdots}_{i}$ $\quad i \cdot h_1 = m \quad h \mid m$. $h \mid n$.

(c). $\langle m, n \rangle = \{\underbrace{um + vn}_{m^u n^v}. \ u, v \in \mathbb{Z}\} = \langle h \rangle$ $\quad um + vn = h$.

(b) $x \mid \underbrace{um + vn}_{h}$ $\quad x \mid h$.

(d). $l \in \underbrace{\langle m \rangle}_{j \cdot m_1}$ $\quad m \mid l$. $\quad n \mid l$.

(e). $m \mid \underbrace{x}_{jm_1}$. $\quad x \in \langle m \rangle$. $\quad x \in \langle n \rangle$. $\quad x \in \langle m \rangle \cap \langle n \rangle = \langle l \rangle$ $\quad l \mid x$. □

Chinese Remainder Theorem. CRT.

Let m, n be coprime natural numbers. Then C_{mn} is isomorphic to $C_m \times C_n$.

$\langle g, h \rangle$ $\quad \langle g \rangle \ \langle h \rangle$

$g^m \quad h^n$.

proof: $(g,h)^{mn} = (g^{mn}, h^{mn}) = (e^n, e^m) = (e, e)$

order of (g,h) divides mn $\quad k \mid mn$

$g^k = e$ if.f. $m \mid k$. $\quad h^k = e$ if.f. $n \mid k$

$(g,h)^k = (g^k, h^k) = (e, e)$ if.f. $m \mid k$. $n \mid k$

m, n coprime By Bézout's theorem. $um + vn = 1$ $\quad \exists\ u, v$.

$n \mid k \Rightarrow mn \mid mk$.

$m \mid k \Rightarrow mn \mid nk$

$mn \mid (umk + vnk) = (um + vn) \cdot k = k$ $\quad mn \mid k$

The order of (g,h) is mn. which equals $|C_m \times C_n|$. □

Equivalence relation.

$S = \{a, b, c\}$ $\quad (a,a) \to a \sim a$, $(a,b) \to a \sim b$, $(a,c) \to a \sim c$

Definition: A (binary) relation $\sim$ on a set S is a subset of $S \times S$.

Then for $a, b \in S$, we write $a \sim b$ if.f. $(a,b) \in \sim$.

function: $S \times S \to \{T, F\}$. $\quad$ "$\sim$" $\quad \sim^{-1}(T)$.

$S = \mathbb{Z}$. $\quad \leq (3,4) = T$. $\quad (3,4) \in \leq \quad 3 \leq 4$ ✓

$\leq$

$S = \{1,2,3\}$. $<$ is the set $\{(1,2), (1,3), (2,3)\}$

Definition: We say that a relation $\sim$ on a set S is an equivalence relation if. it is

(i) reflexive $\quad a \sim a$.

(ii) symmetric. $\quad a \sim b \Rightarrow b \sim a$.

(iii) transitive $\quad a \sim b$. $b \sim c \Rightarrow a \sim c$.

$S = \mathbb{C}$. $z \sim w$ iff $|z| = |w|$.

$S = GL(n, \mathbb{R})$ $A \sim B$ iff. $\exists\ P \in GL(n, \mathbb{R})$ s.t. $B = P^{-1}AP$.

(i) $A = I^{-1}AI$

(ii) $B = P^{-1}AP \Rightarrow A = (P^{-1})^{-1} \cdot B \cdot P^{-1}$. $\quad Q^{-1}BQ \quad \exists Q \in GL(n, \mathbb{R})$.

(iii). $B = P^{-1}AP$

$C = Q^{-1}BQ = Q^{-1}P^{-1}APQ = (PQ)^{-1}APQ \quad PQ \in GL(n, \mathbb{R})$

$S = \{$polygons in $\mathbb{R}^2\}$. $\sim$ is congruence.

S is a group. $\sim$. $x = y$ or $x = y^{-1}$.

NOT:

$S = \mathbb{Z}$. $m \sim n$ iff $m < n$.

$S = \mathbb{R}[x]$ $\quad p(x) \sim q(x)$ iff. $p(a) = q(a)$ for some $a \in \mathbb{R}$.

$a_1 + a_2x + a_3x^2 + \cdots$

$p(a) \sim q(a)$ $\quad a \in \mathbb{R}$ $\quad p(c) \sim r(c)$ ✗ $\quad c \in \mathbb{R}$

$q(b) \sim r(b)$ $\quad b \in \mathbb{R}$.

Proposition. Let $S = \mathbb{Z}$ and $n \geq 2$ be an integer. we set $a \sim b$ if $a - b$ is a multiple of n. then $\sim$ is an equivalence relation

Proof: (a) $\forall a \in \mathbb{Z}$. $a \sim a$ $\quad a - a = 0 = 0 \cdot n$.

(b) $a \sim b$ $\quad a - b = kn$. for some k.

$b - a = -kn$. $\quad b \sim a$

(c). $a \sim b$ $\quad a - b = kn$

$b \sim c$ $\quad b - c = ln$

$a - c = (a - b) + (b - c) = kn + ln = (k + l)n$

$a \sim c$. □

Definition. Let G be a group. $g, h \in G$. g, h are said to be conjugate in G. if there exists. $k \in G$ s.t. $g = k^{-1}hk$.

Proposition: Conjugacy is an equivalence relation.

Proof: $g \sim h$. if there exists $g = k^{-1}hk$.

(a) $g \sim g$ $\quad g = e^{-1} \cdot g \cdot e$. $\forall g$.

(b) $g \sim h$

(c) $g \sim h$. $h \sim k \Rightarrow g \sim k$. $\square$.

Definition: Given an equivalence relation $\sim$ on a set S with $a \in S$. then the equivalence class of a. $\bar{a}$ or $[a]$ is the set.

$$\bar{a} = \{x \in S : x \sim a\}$$

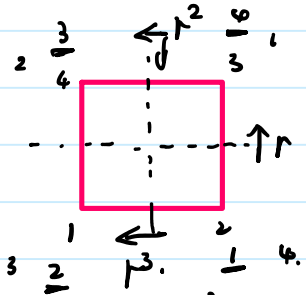
$a \sim b$ if $a - b = kn$. $\quad a, b \in \mathbb{Z}$.

$\bar{0}, \bar{1}, \bar{2}, \overline{n-1}$,

$n\mathbb{Z}$. $1+n\mathbb{Z}$. $\quad n-1+n\mathbb{Z} = -1+n\mathbb{Z}$.

$s^{-1} \cdot r \cdot s$

$s \cdot r$. $\quad s \cdot r \cdot s = r$.



D_8 $\quad e, r, r^2, r^3, s, rs, r^2s, r^3s$.

conjugacy classes

$\{e\}$. $\{r, r^3\}$. $\{r^2\}$. $\{s, r^2s\}$ $\{rs, r^3s\}$.

$s = r^2s$.

D_{10} $\{e\}$. $\{r, r^4\}$. $\{r^2, r^3\}$. $\{s, rs, r^2s, r^3s, r^4s\}$

Definition: Let S be a set and Λ be an indexing set. We say that a collection of subsets A_λ of S $(\lambda \in \Lambda)$ is a partition of S if:

(i) $A_\lambda \neq \emptyset$ for each $\lambda \in A$

(ii) $\bigcup_{\lambda \in \Lambda} A_\lambda = S$

(iii). If $\lambda \neq \mu$ then $A_\lambda \cap A_\mu = \emptyset$ $\quad$ If $A_\lambda \cap A_\mu \neq \emptyset$ then $\lambda = \mu$.

partition P of S $\quad a \in S$. unique P_a s.t. $a \in P_a$.

Theorem: Let $\sim$ be an equivalence relation on a set S. then $\sim$-equivalence classes partition S.

proof: $a \in \bar{a}$. reflexivity. non-empty $\quad \forall a \in S$. $a \in \bar{a}$.

$c \in \bar{a} \cap \bar{b}$. $a, b, c \in S$. $\bar{a} = \bar{b}$ ✓ $\quad \bigcup_{\lambda \in \Lambda} A_\lambda = S$.

$c \in \bar{a}$ $c \sim a$. symmetry. $\frac{a \sim c}{b \sim c}$. transitivity. $a \sim b$ △

$c \in \bar{b}$ $c \sim b$ $b \sim a$. △

$\forall x \in \bar{a}$. $\frac{x \sim a \sim b}{\text{def. } \triangle}$ $\frac{x \sim b.}{\text{transitivity.}}$ $\bar{a} \subseteq \bar{b}$. $\bar{a} = \bar{b}$

$\forall x \in \bar{b}$ $x \sim b \sim a$ $x \sim b$ $\bar{b} \subseteq \bar{a}$ □.

18. Mar. 2023.
4pm (+8).