GroupAction6

2023年3月11日 星期六 下午12:06

partition

Modular Arithmetic

Order

Langrange's Theorem.

Theorem: Let S be a set.

(a) given an equivalence relation $\sim$ on S then the equivalence classes of $\sim$ form a partition $P(\sim)$ of S (where $P(\sim)a = \bar{a}$ for each $a \in S$)

(b) given a partition P of S then the relation $\sim_P$ on S defined by

$$a \sim_P b \text{ if.f. } b \in P_a$$

is an equivalence relation on S.

(c) (a) and (b) are inverse of one another.

$P(\sim_P) = P$ ✓ and $\sim_{P(\sim)} = \sim$.

$P \to \sim$

$\sim \to P'$

Proof: (a) ✓

(b) P is a partition of S.

i) Let $a \in S$ Then $a \in P_a$ by definition $a \sim_P a$

ii) If $a \sim_P b$ then $b \in P_a$ and $b \in P_b$ by definition.

$b \in P_a \cap P_b \neq \emptyset$ $P_a = P_b$. $a \in P_b$. $b \sim_P a$.

iii) $a \sim_P b$. $b \sim_P c$ then $b \in P_a$, $c \in P_b$.

$b \in P_a \cap P_b \neq \emptyset$ $P_a = P_b$ $c \in P_a$ $a \sim_P c$.

(c) Let P be a partition of S.

$b \in P_a \cap P_b \neq \emptyset \quad P_a = P_b \quad c \in P_a \quad a \sim_P c.$

(c) Let P be a partition of S.

$A \in P(\sim_P) \Leftrightarrow \exists\, a \in A$ s.t. A is the $\sim_P$ equivalence classes of a.

$\Leftrightarrow \exists\, a \in A.\ A = P_a.$

$\Leftrightarrow A \in P.$

$a \sim_{P(\sim)} b \Leftrightarrow b \in (P(\sim))_a \Leftrightarrow a \in \bar{b} \Leftrightarrow a \sim b.$ □

52 ? equivalence relations.

5 elements

$X = \{1, 2, 3, 4, 5\}$

Partition.	$P(X)$
5.	1
4+1	5
3+2	10
3+1+1	10
2+2+1	$\frac{1}{2!}C_5^2 \cdot C_3^2 = 15$
2+1+1+1	10
1+1+1+1+1	1.

How many partitions are there of a set with 22 elements into 4 subsets of size 3 and 2 subsets of size 5?

$$\frac{C_{22}^3 C_{19}^3 C_{16}^3 C_{13}^3 C_{10}^5 C_5^5}{4!2!} = \frac{22!}{(3!)^4 (5!)^2 \, 4!2!}$$

shuffling within subsets; shuffling same-size subsets.

Modular Arithmetic.

odd — Even × odd = Even.

even — Odd + Odd = Even

+	E	O
E	E	O
O	O	E

×	E	O
E	E	E
O	E	O

$\{E, O\}$ abelian group.

E. identity.

modulo 2. remainders

mod 2.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

mod 2.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

$1+1=0$. (clockwork arithmetic)

$5+9=2$

$1-7=6$.

$2+7\times 3=11$

Definition: If we are doing arithmetic mod n $(n\geq 2)$

n possible remainders: $0, 1, \cdots n-1$.

$a+b$ = remainder when $a+b$ is divided by n.

$a-b$ = remainder when $a-b$ is divided by n

ab = ... ab. ..

$\mathbb{Z}_n$. $\{0,1,2,\cdots n-1\}$.

mod 7 $3+6=2 \mod 7$. $a\sim b$ if.f. $a=b \mod n$.

$3-5=5 \mod 7$

$3\times 5=1 \mod 7$.

Definition: Let $\mathbb{Z}_n$ denote the equivalence classes $\bar{0}, \bar{1}, \bar{2}, \cdots \overline{n-1}$ of $\mathbb{Z}$.

$+, \times$ on $\mathbb{Z}_n$. $\bar{a}+\bar{b}=\overline{a+b}$ well-defined. $\bar{0}=\bar{7}$ in $\mathbb{Z}_6$.

$\bar{a}\times\bar{b}=\overline{a\times b}$.

1 $\bar{a}=\bar{\alpha}$, $\overline{a+b} \neq \overline{\alpha+\beta}$.

2 $\bar{b}=\bar{\beta}$. $\bar{1}+\bar{2} \neq \overline{7+8}$.

Proposition: $+, \times$ is well-defined on $\mathbb{Z}_n$.

Proof: Suppose $\bar{a}=\bar{\alpha}$, $\bar{b}=\bar{\beta}$ $\quad a-\alpha=kn$, $b-\beta=ln$. $k, l\in\mathbb{Z}$.

$$(a+b)-(\alpha+\beta)=(a-\alpha)+(b-\beta)=(k+l)\cdot n$$

$$ab-\alpha\beta=(\alpha+kn)(\beta+ln)-\alpha\beta=(k\beta+l\alpha+kln)n. \quad \square$$

$ab \sim \alpha\beta$.

Proposition: (a) $(\mathbb{Z}_n, +)$ is an abelian group isomorphic to C_n. $\{e, g, g^2, \cdots g^{n-1}\}$. $\bar{a}\ \bar{1}$.

(b) $\times$ is associative, commutative and distributes over $+$.

$a\times(b+c)=a\times b+a\times c$.

proof: $\bar{a}, \bar{b}, \bar{c}\in\mathbb{Z}_n$.

$a \times (b+c) = a \times b + a \times c$.

proof: $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$.

$\bar{a}(\bar{b}+\bar{c}) = \bar{a}(\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} = \bar{ab} + \bar{ac} = \bar{a}\cdot\bar{b} + \bar{b}\cdot\bar{c}$.

□.

$\bar{0}$. $\bar{e}$.

proposition: Let $\bar{x} \in \mathbb{Z}_n$ with $x \neq 0$.

(a) $\bar{x}$ has a multiplicative inverse. iff. $hcf(x, n) = 1$

n is a prime. $\mathbb{Z}_n$ is a field.

(b). $\bar{x}$ / those. with a multiplicative inverse. form a group $\mathbb{Z}_n^*$ under multiplication.

units.

proof: ...

$\mathbb{Z}_{12}$. 1, 5, 7, 11.

$12 = 2^2 \times 3$.

$\{1, 2, 3, \cdots 11\}$.

$2 \times 2 = 4$

$2 \times 2^2 = 8$

$2 \times 2 \times 2 \times 2 = 16. = 4$.

$\mathbb{Z}_{12}^*$. 6.

*	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

isomorphic to $C_2 \times C_2$.

Order.

o(g).

Definition: Let G be a group. and $g \in G$. If there is a positive integer k. s.t. $g^k = e$ then the order $o(g)$ of $g \in G$ is defined as.

$$o(g) = \min\{m > 0 : g^m = e\}.$$

Otherwise we say that the order of g is infinite.

proposition: If G is finite, then $o(g)$ is finite for every $g \in G$.

proof: $g, g^2, g^3, g^4 \cdots$ □. G is finite

repeat.

repeat.

$i>j$. $\exists\, g^i=g^j$. $g^{i-j}=e$ $\{m>0,\ g^m=e\}$. is non-empty and has a minimal element. □

proposition: If $g\in G$ and $o(g)$ is finite, then $g^n=e$ iff. $o(g)\mid n$.

proof: $\Leftarrow$ $n=k\cdot o(g)$. $g^n=g^{k(o(g))}=(g^{o(g)})^k=e^k=e$.

$\Rightarrow$ $g^n=e$. $g^n=g^{q(o(g))+r}$. q,r. integers $0\le r<o(g)$.

$g^r=g^{n-q(o(g))}=\underline{g^n}\cdot\underline{(g^{o(g)})^{-q}}=e$.

By the minimality of $o(g)$ then $r=0$ and $n=qo(g)$. □.

proposition: If $\phi: G\to H$ is an isomorphism, and $g\in G$ then $o(\phi(g))=o(g)$. ($f(ab)=f(a)\cdot f(b)$)

proof: $(\underline{\phi(g)})^k=e_H \Leftrightarrow \underline{\phi(g^k)}=\underline{e_H} \Leftrightarrow \underline{g^k}=e_G$. □.

Dg. $o(e)=1$

$o(r^2)=o(s)=o(rs)=o(r^2s)=o(r^3s)=2$.

$o(r)=o(r^3)=4$

Proposition: Let x,n be integers and $n\ge 2$. $\bar{x}\in\mathbb{Z}_n$.

$$o(\bar{x})=\frac{n}{hcf(x,n)}$$

$\bar{x}\in\mathbb{Z}_n$ is a generator iff. $hcf(x,n)=1$.

proof: ....

Definition: Let H be a subgroup of G.

left cosets of H. are the sets $gH=\{gh: h\in H\}$. G/H.

cardinality ⇒

left cosets of H. are the sets $gH = \{hg : h \in H\}$. $|G/H|$ cardinality $\Rightarrow$ index of H in G.

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

$g_1, g_2 \in G$. may represents the same coset: we can have $g_1H = g_2H$. $g_1 \neq g_2$

In general $gH \neq Hg$. If G is abelian. $gH = Hg$. $gh = hg$.

$G = S_3$. $H = \{e, (12)\}$

$eH = (12)H = \{e, (12)\}$. $He = H(12) = \{e, (12)\}$.

$(13)H = \{(13), (132)\} = (132)H$. $H(13) = \{(13), (123)\} = H(123)$.

$(123)H = \{(23), (123)\} = (123)H$. $H(23) = H(132) = \{(23), (132)\}$

$Hg \neq gH$.

$G = \mathbb{Z}$, $H = n\mathbb{Z}$. $r \in \mathbb{R}$ $r + n\mathbb{Z}$. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

$0 + n\mathbb{Z}$. $1 + n\mathbb{Z}$ $\cdots$ $(n-1) + n\mathbb{Z} = -1 + n\mathbb{Z}$.

Coset Equality lemma. Let $H \leq G$ $g, k \in G$. Then.

$gH = kH \Leftrightarrow k^{-1}g \in H$. ✓

$* \; Hg = Hk \Leftrightarrow kg^{-1} \in H$.

proof: $\Rightarrow$ $gH = kH$. $g = ge \in kH$. $\exists h \in H$, $g = kh$. $k^{-1}g = h \in H$.

$\Leftarrow$ $k^{-1}g \in H$. $k^{-1}g = h$, $gH = khH \subseteq kH$. $gH = kH$.

$kH = g \cdot g^{-1} \cdot k \cdot H = g \cdot (g^{-1}k)H = gh^{-1} \cdot H \subseteq gH$. □

$g \sim k \Leftrightarrow k^{-1}g \in H$. $\Leftarrow$ equivalence classes $\Leftarrow$ partition.

Lagrange's Theorem: Let G be a finite group and H a subgroup of G.
1771 Then $|H|$ divides $|G|$.

proof: Let G be a group and H be a group.

Partition: $g \in G$. $g = ge \in gH$. so the union is G. / of cosets

$k \in g_1H \cap g_2H$ $h_1, h_2 \in H$. $k = g_1h_1 = g_2h_2$.

/of cosets

$k \in g_1H \cap g_2H$. $h_1, h_2 \in H$. $k = g_1h_1 = g_2h_2$.

$g_2^{-1}g_1 = h_2 \cdot h_1^{-1} \in H$. by lemma, $g_1H = g_2H$.

equinumerous. $g \in G$, $h \to gh$ is a bijection between H and gH.

$|gH| = |H|$.

$h_1 \to gh_1$ $\quad gh_1 = gh_2$

$h_2 \to gh_2$. $\quad g^{-1}g h_1 = g^{-1}gh_2 \Rightarrow h_1 = h_2$.

G is finite. $|G| = |G/H| \times |H|$. hence $|H|$ divides $|G|$. □

28. Sat. 2015

4pm (+8)