GroupAction7

2023年3月18日 星期六 下午12:07

Fermat's Little Theorem.

Euler's Theorem

Wilson's Theorem.

Homomorphism

Corollary. Let G be a finite group and $g \in G$, then $o(g)$ divides $|G|$.

proof: $\langle g \rangle = \{e, g, g^2 \cdots g^{o(g)-1}\}$ $\quad g^{o(g)} = e$

is a subgroup of G with order $o(g)$ $\square$

Corollary: Let G be a finite group with $|G| = p$, a prime. Then G is cyclic.

$|G| = 3$. $|G| = 13$. $\{e, g, g^2 \cdots g^{p-1}\}$

proof: let $g \in G$, $g \neq e$. $\Rightarrow o(g) \neq 1$, $o(g)$ divides $|G| = p \Rightarrow o(g) = p$ $\quad |\langle g \rangle| = p$.

$\langle g \rangle = G$ and G is cyclic. $\square$

Corollary: Let G be a finite group and $g \in G$. Then $g^{|G|} = e$. $\triangleleft$

proof: $|G|$ is multiple of $o(g)$ $\quad |G| = k \cdot o(g)$.

$g^{|G|} = g^{k \cdot o(g)} = (g^{o(g)})^k = e^k = e$. $\square$

Fermat's little theorem: Let p be a prime and $a \in \mathbb{Z}$. such that p does not divides a.

$a^{p-1} = 1 \mod p$. $\quad \mathbb{Z}_p^* = \{1, 2, \cdots p-1\}$.

proof: $|\mathbb{Z}_p^*| = p-1$ $\quad o(g) \mid |G|$ $\quad \cdots \quad p-1$

$\mathbb{Z}_p^* = \{1, 2, \cdots p-1\}$.

proof: $|\mathbb{Z}_p^*| = p-1$. $g^{|G|} = e \Rightarrow a^{p-1} = 1 \mod p$. □

Euler's theorem: Let $n \geq 2$ and let $a \in \mathbb{Z}$ be coprime with n. Then.

$$a^{\phi(n)} = 1 \mod n.$$

$\phi(n) = |\{k : 0 < k \leq n, \ hcf(k, n) = 1\}|$. phi function.

$\phi(5)$ 1, 2, 3, 4. $\phi(5) = 4$. $\phi(2) = 1$.

$\phi(10)$. 1 2 3 4 5 6 7 8 9 $\phi(10) = 4 = \phi(5) \cdot \phi(2) = 4 \cdot 1$.

i). $\phi(p) = p-1$ for a prime p.

ii) $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ for a prime p.

iii) $\phi(mn) = \phi(m) \cdot \phi(n)$ if m and n are coprime.

proof: $G = \mathbb{Z}_n^*$ $|G| = |\mathbb{Z}_n^*|$ $\phi(n) = |\mathbb{Z}_n^*|$.

$a^{\phi(n)} = 1 \mod n$. $a^{|\mathbb{Z}_n^*|} = 1 \mod n$.

$a^{\phi(n)} = 1 \mod n$.

$\mathbb{Z}_n$.

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$.

$2 * 2 = 4$

$4 * 2 = 8$

$8 * 2 = 6 \mod 10$

$6 * 2 = 2 \mod 10$ □

a, $\exists a^{-1} \cdot a = e$. a^{-1} is the inverse of a.

Lemma: Let G be a group. Then the relation $\sim$ on G defined by.

$$x \sim y \Leftrightarrow x = y \text{ or } x = y^{-1}. \quad \Leftarrow$$

is an equivalence relation. The equivalence relation are generally of the form $\bar{x} = \{x, x^{-1}\}$ unless x is self inverse in which $\bar{x} = \{x\}$.

proof: (1). $x \sim x$. $x \sim x \Leftrightarrow x = x$.

(2) $x \sim y \Rightarrow y \sim x$ $x = y. \Rightarrow y \sim x \Leftrightarrow y = x$ $x = y^{-1} \Rightarrow y = x^{-1} \Rightarrow y \sim x$.

(3) $x \sim y$. $y \sim z \Rightarrow x \sim z$

$x = y$ $y = z$. $x \sim z$.

$x = y$ $y = z^{-1}$ $z = y^{-1} = x^{-1} \Rightarrow x \sim z$. □.

Wilson's theorem: If p is a prime, then

$$(p-1)! = -1 \mod p.$$

$\bar{3} = -1$.

$(p-1)! \equiv -1 \bmod p$.

proof: $p=2$. $1! \equiv -1 \bmod 2$ ✓.

$p \geq 3$. consider self-inverse element in $\mathbb{Z}_p^*$.

$\bar{x} = \bar{x}^{-1} \Leftrightarrow \bar{x}^2 = \bar{1} \Leftrightarrow (\bar{x}-\bar{1})(\bar{x}+\bar{1}) = \bar{0} \Leftrightarrow \bar{x} = \bar{1}$ or $-\bar{1}$.

$\{\bar{1}\}$. $\{-\bar{1}\}$. are the only singleton equivalence classes of $\sim$ (lemma).

$\{\bar{x}, \bar{x}^{-1}\}$. all others. ⇐. $\bar{x}\cdot\bar{x}^{-1} = \bar{1}$.

equivalence classes partition $\mathbb{Z}_p^*$. then.

$$(p-1)! = \prod_{k \in \mathbb{Z}_p^*} \bar{k} = \bar{1} \times -\bar{1} \times \underbrace{\left[\prod \bar{k}\right]}_{\text{all others}} = -1 \bmod p. \quad \square$$

Corollary: Let G be a group with even order, then G has an element of order 2.

$\exists x,\ x^2 = e$.

proof: consider the equivalence relation $\sim$ (Lemma)

equivalence classes: singleton n, doubleton m

$$2m + n = |G|$$

n: even, $|G|$: even

$e \cdot e = e$.

e is self-inverse $n \geq 1 \Rightarrow n \geq 2$ (n even). there is a non-identity element. x.

$x = x^{-1} \Rightarrow x^2 = e \Rightarrow \exists x.\ x^2 = e$. $\square$

Theorem: Let G be a finite group with $|G| = 2p$ where $p \geq 3$ is prime. Then G is isomorphic to C_{2p} or D_{2p}. $\langle x, y : x^2 = y^p = e,\ yx = xy^{p-1} \rangle$. ✱

i.e. $\{g, \cdots g^{2p-1}\}$.

proof: Assume that G is not cyclic. ($x^2 = e$)

$2p = 1 \cdot 2p = 2 \cdot p$. $g \in G$. ① $g^1 = e$ ② $g^2 = e$ (must exist) ③ $g^p = e$.

i). $g^2 = e$ for all $g \in G$. $G \cong (\mathbb{Z}_2)^n$ for some n. (is not possible $p \geq 3$). ?

i). $g^2=e$ for all $g\in G$. $G\cong(\mathbb{Z}_2)^n$ for some n. (is not possible $p\geq 3$). ?

ii) there exists an element $y\in G$ of order p $\{y, y^2, \cdots y^{p-1}\}$ has order p.

$x\notin\langle y\rangle$.

$G=\{e, \underbrace{y, y^2, \cdots y^{p-1}}_{p}, \underbrace{x, xy, xy^2 \cdots xy^{p-1}}_{p}\}$ yx. y^2x.

if $yx=y^i \Rightarrow x=y^{i-1}$ contradiction.

if $yx=xy^j$ $1\leq j<p$.

$yx=xy^{p-1}$.

$(yx)^2=yx\cdot yx=y\cdot x\cdot(xy^j)=y\cdot e\cdot y^j=y^{j+1}$.

$(yx)^3=xy^j\cdot(yx)^2=x\cdot y^{2j+1}$.

$\vdots$

$(yx)^{2k}=y^{k(j+1)}$

$(yx)^{2k+1}=xy^{kj+k+j}$.

$(yx)^{2k}$ can be e.

yx has an even order.

$o(yx)=2$.

$y^{j+1}=e$

$j=p-1$

$G=\langle x, y; x^2=y^p=e, yx=xy^{p-1}\rangle$. □

Homomorphisms and Isomorphisms.

Definition: Let G and H be groups. an isomorphism $\phi: G\to H$ is a bijection. such that:

homomorphism

map.

bijection

$f(a,b)=f(a)f(b)$.

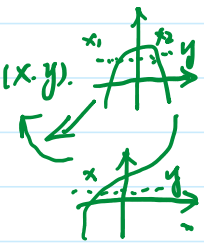
$$\phi(g_1 *_G g_2)=\phi(g_1)*_H\phi(g_2) \quad \forall g_1, g_2\in G.$$

G and H are isomorphic.

bijection. $f(x)=y$. unique. (x,y).

map. $f(x_1)=y$ (x_1,y)

$f(x_2)=y$. (x_2,y).



$|G|=p$ a prime $G\cong C_p$ $\{e, g, \cdots g^{p-1}\}$

$|G|=2p$. $p\geq 3$ a prime. $G\cong C_{2p}$ or $G\cong D_{2p}$.

$|G|\leq 7$.

Order	group.
2	C_2
3	C_3
4	C_4, $C_2\times C_2\cong V_4$; D_4.
5	C_5
6	C_6. $D_6\cong S_3$
7	C_7.
8	C_8, $C_2\times C_4$, $C_2\times C_2\times C_2$

$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

$a+bi$ $i^2=-1$.

D_8. Q_8 quaternion $a+b\underline{i}+c\underline{j}+d\underline{k}$. $i^2=j^2=k^2=$

± 1 $\pm i$ $\pm j$ $\pm k$

D_8. Q_8 quaternion $a+bi+cj+dk$. $i^2=j^2=k^2=ijk=-1$.
$\{\pm 1, \pm i, \pm j, \pm k\}$.

Automorphism: isomorphism from G to G. $Aut(G)$ form a group.

endomorphism: homomorphism from G to G.

monomorphism. epimorphism. homomorphism.
injective surjective.

Proposition: Let $\phi: G \to H$ be a homomorphism between groups and let $g \in G$, $n \in \mathbb{Z}$. Then
(i) $\phi(e_G) = e_H$.
(ii) $\phi(g^{-1}) = (\phi(g))^{-1}$
(iii) $\phi(g^n) = (\phi(g))^n$.

Proof: (i). $\phi(e_G) = \phi(e_G * e_G) \overset{def.}{=} \phi(e_G) * \phi(e_G)$. $[\phi(e_G)]^{-1}$.
$\phi(e_G) = e_H$.

(ii). $\phi(g^{-1}) \cdot \phi(g) \overset{def}{=} \phi(g^{-1} * g) = \phi(e_G) \underset{(i)}{=} e_H$. $(\phi(g))^{-1}$.
$\phi(g^{-1}) = (\phi(g))^{-1}$.

(iii): $n > 0$ induction. $n=2$. ✓
$n=k$ ✓
$n=k+1$. ✓. ⇓

$n<0$. $n=-k<0$ $\phi(g^n) = \phi((g^{-1})^k) = (\phi(g^{-1}))^k \underset{(ii)}{=} (\phi(g)^{-1})^k$
$= (\phi(g))^{-k} = (\phi(g))^n$. □

Corollary: Let $\phi: G \to H$ be a homomorphism between groups and let $g \in G$. Then $o(\phi(g))$ divides $o(g)$.

proof: $(\phi(g))^{o(g)} = \phi(g^{o(g)}) = \phi(e_G) = e_H$.
$o(\phi(g))$ divides $o(g)$.

$g^{o(g)} = e_G$
$(\phi(g))^{o(\phi(g))} = e_H$.

□

H is a subgroup of G. $\tau: H \to G$ is a homomorphism inclusion.

H is a subgroup of G. $\tau: H \to G$ is a homomorphism inclusion.

$\tau(h) = h$.

H, G groups $\phi: G \to H$. $\phi(g) = e_H$ homomorphism

$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$.

$\pi_1: (g_1, h_1) \to g_1$ are homomorphism.

$\pi_2: (g_1, h_1) \to h_1$.

$\phi: \mathbb{R}^* \to \mathbb{R}^*$, $x \to x^2$. homomorphism. $\phi(x) = x^2$, $\phi(y) = y^2$. $\phi(xy) = (xy)^2 = x^2y^2 = \phi(x) \cdot \phi(y)$

Proposition: Let $a \in G$. a group, conjugation by a.

$\theta_a: G \to G$ is an isomorphism.

$\theta_a(g) = a^{-1}ga$.

proof: $\theta_a(gh) = a^{-1}gh \cdot a = a^{-1} \cdot g \cdot \underbrace{a \cdot a^{-1}}_{e} \cdot h \cdot a = (a^{-1}ga)(a^{-1}ha) = \theta_a(g)\theta_a(h)$.

$(\theta_a)^{-1} = aga^{-1} = \theta_{a^{-1}}$. inverse. $g \to a^{-1}ga$

$a(a^{-1}ga)a^{-1}$

$= e \cdot g \cdot e = g$

θ_a is a bijection. □.

1. Apr. 2023.

4pm (+8).