GroupAction8

2023年3月25日 星期六 下午12:00

kernel

Normal subgroup.

Centre

Quotient group.

$\phi(p^k) = p^{k-1}(p-1)$

$\phi(p) = p-1$ $\quad$ p prime

$\Rightarrow$ $\underbrace{\overbrace{1 \cdots p}^{<p-1}}_{p-1} \cdots 2p \cdots 3p \cdots p^2$ $\quad$ $p-1 \quad p-1 \quad p-1$ $\quad$ $< p(p-1)$

$p^k \cdot < p^{k-1}(p-1)$

$p^{k+1} \cdot < p^k(p-1)$

Corollary: Let G be a group and $g, h \in G$.

(i) If g and h are conjugate then $o(g) = o(h)$.

(ii) If g and h are conjugate then g^{-1} and h^{-1} are conjugate

proof: (i) $h = a^{-1}ga$. $\qquad g^{o(g)} = e$.

$g = aha^{-1}$ $\qquad \underbrace{a^{-1}g\underbrace{a \cdot a^{-1}}_{e} g \cdots g\underbrace{a \cdot a^{-1}}_{e}ga}_{o(g)} = e^{a^{-1}} {}^{a} = a^{-1}ea = a^{-1}a = e$.

$\Rightarrow g^{o(h)} = e$

$\Rightarrow o(g) = o(h)$. $\qquad \underbrace{h \cdot h \cdot h \cdots h}_{o(g)} = e \qquad h^{o(g)} = e.$

$h^{o(h) \cdot k} = e$

(ii). $h = a^{-1}g \cdot a$.

$h^{-1} \cdot a^{-1} \cdot g \cdot a = e$

$h^{-1} \cdot a^{-1} g \cdot a \cdot a^{-1} = a^{-1}$

$h^{-1} \cdot a^{-1} g = a^{-1}$

$$h^{-1}\cdot a^{-1} g\cdot \underline{a\cdot a^{-1}} = a^{-1}$$
$$h^{-1}\cdot a^{-1} g = a^{-1}$$
$$h^{-1}\cdot a^{-1}\cdot \underline{g\cdot g^{-1}} = a^{-1}\cdot g^{-1}$$
$$h^{-1}\cdot a^{-1} = a^{-1}\cdot g^{-1}$$
$$\underline{h^{-1}} = a^{-1}\underline{g^{-1}}\cdot a \qquad \square$$

$2\cdot ? = 1$. $\quad 2 + ? = 0$ $\quad -2$

proposition: Homomorphism $\phi: \underline{\mathbb{Z}} \to \mathbb{Z}$ are all of the form (group: +)

$$\phi(x) = nx \text{ for some } n \in \mathbb{Z}.$$

$x \to x^2$

$f(\underline{ab}) = f(a)f(b)$.

proof: $\phi(x) = nx$. map ✓

$\phi(x+y) = nx + ny = \phi(x) + \phi(y)$. ✓

$\phi: \mathbb{Z} \to \mathbb{Z}$.
$1 \to e$.

$\forall x$, $x>0$: $\phi(x) = \phi(\underbrace{1+1+1\cdots+1}_{x})$
$= \underbrace{\phi(1)+\phi(1)+\cdots\phi(1)}_{x} = \underline{n}x$ $\square$

$x<0$. $\phi(-x) = -\phi(x)$. Δ

If G is a cyclic group ($g_1, g_2 \cdots g_n$) with generator g. then any homomorphism from G is entirely determined by the value of $\phi(g)$. $\phi(g_1).\phi(g_2)\cdots\phi(g_n)$.

$$\phi(\underline{g^r}) = [\phi(g)]^r \text{ for any } r \in \mathbb{Z}.$$

$$\phi(g_1^m g_2^n \cdots g_n^k) = \phi(g_1)^m \phi(g_2)^n \cdots \phi(g_n)^k$$

Definition: Let $\phi: G \to H$ be a homomorphism between groups. Then.

i) the kernel of ϕ: $\ker\phi = \{g \in G : \underline{\phi(g) = e_H}\} \subseteq G$.

ii) the image of ϕ: $\operatorname{Im}\phi = \{\underline{\phi(g)} : \underline{g \in G}\} \underline{\subseteq H}$

Definition: Let G be a group and H a subgroup of G. Then H is said to be a normal subgroup of G if:

$ghg^{-1} = h_j$.

$h_1 \to h_1$, $h_2 \to h_2$

$$gH = Hg \text{ for all } g \in G.$$

$gHg^{-1} = H$

$ghg^{-1} = h_j$.

$gHg^{-1} = H$ $\Leftrightarrow$ $gH = Hg$ for all $g \in G$.

$g^{-1} \cdot h \cdot g \in H$ for all $g \in G$, $h \in H$.

$H \triangleleft G$ $\quad \theta = a^{-1}ga$

i) $gh \neq hg$ $\quad$ G is abelian. $gh = hg$. $H \leq G \Rightarrow H \triangleleft G$.

$\Rightarrow$ ii) $\{e\} \triangleleft G$ ✓

$G \triangleleft G$. ✓ $gG = Gg$. $\quad \bar{g}\bar{g} = \bar{g}g \quad \bar{g} = g^{-1} \cdot \bar{g} g$.

proposition: $\ker \phi \triangleleft G$.

$\phi(\ker \phi) = e$.

$G \to H$

proof: i) $k_1, k_2 \in \ker \phi$. $g \in G$. $\quad \phi(e_G) = e_H$.

$k_1 k_2 \in \ker \phi \quad \phi(k_1 k_2) = \phi(k_1)\phi(k_2) = e_H \cdot e_H = e_H$.

$k_1^{-1} \in \ker \phi$. $\quad \phi(k_1^{-1}) = [\phi(k_1)]^{-1} = e_H^{-1} = e_H$

ii) $\phi(g^{-1} \cdot k_1 g) = \phi(g^{-1}) \cdot \underbrace{\phi(k_1)}_{e_H} \cdot \phi(g) = \phi(g)^{-1} \cdot e_H \cdot \phi(g) = e_H$.

$g^{-1} k_1 g \in \ker \phi$

$\ker \phi \triangleleft G$. $\square$.

proposition: $\mathrm{Im}\, \phi \leq H$.

proof: $\phi(e_G) = e_H \in \mathrm{Im}\phi$. $\quad h_1, h_2 \in \mathrm{Im}\phi$. $\quad \phi(g_i) = h_i$. $\quad g_i \in G$

$h_1 \cdot h_2 = \phi(g_1) \cdot \phi(g_2) = \phi(g_1 g_2) \in \mathrm{Im}\phi$

$h_1^{-1} = [\phi(g_1)]^{-1} = \phi(g_1^{-1}) \in \mathrm{Im}\phi$ $\quad (g_1^{-1} \in G)$ $\square$.

$\phi: \mathbb{Z} \to \mathbb{Z}_n$. $\quad \phi(n) = \bar{n}$. $\quad$ kernel: $n\mathbb{Z}$. $\quad n*1, n*2, \cdots$

$\{1, 2, 3, 4 \cdots n\}$. $\quad$ image: $\mathbb{Z}_n$.

$S_n \to \{\pm 1\}$. $\quad A_n \to +1$. $\quad$ kernel: A_n

e_{S_n} $\quad$ image: $\{\pm 1\}$.

S_3. $3 \times 2 \times 1 = 6$.

123 $\quad$ 123 $\cdots$

123 $\quad$ 213

(12).

proposition: A homomorphism is constant on a coset of $\ker \phi$ and takes different values on different cosets.

$\phi(g_1) \quad \phi(g_1) = \phi(g_2) \Rightarrow g_1 \ker \phi = g_2 \ker \phi$.

different values on different cosets.

$\phi(g_1)$ $\phi(g_2)$ $\phi(g_1)=\phi(g_2) \Rightarrow g_1 \ker\phi = g_2 \ker\phi$.

proof: $\phi(g_2)^{-1}\cdot\phi(g_2) = e_H \Rightarrow \phi(g_2^{-1})\phi(g_1) = \phi(g_2^{-1}g_1) = e_H$

$g_2^{-1} g_1 \in \ker\phi$. $\{h_1, \cdots h_n\}$.

$g_2^{-1}, g_1 \in \ker\phi$. $g_1 \ker\phi = g_2 \ker\phi$. $\square$

$g_1 h_1$ $g_2 h_1$
$g_1 h_2$ $g_2 h_2$

Remark: subgroup $H \leq G$ is normal in G if and only if H is a union of conjugacy classes. $\triangle$

proposition: Let $H \leq G$ If $|G/H| = 2$, then $H \triangleleft G$.

g_1H, g_2H.

proof. $eH = He = H$.
left cosets right cosets.

H^c the complement of H.

If $g \in H$. $gH = H = Hg$.

H H^c $H \oplus H^c = G$. $g \notin H$ $gH = H^c = Hg$.

$H \triangleleft G$. $\square$.

A_4 does not have size 6 normal subgroup.

conjugacy classes: size: 1, 3, 4, 4. no selections of 1,3,4,4 adds up to 6.

S_3. normal subgroup. $\{e\}$. $\boxed{A_3}$ S_3 e. 2-cycles. 3-cycles. S_3.

1 2 3   1 3 3
2 1 3   3 2 1.

3-cycles.

$(12) * (13). = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

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

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

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

$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = e$.

Definition: Let G be a group. The centre of G denoted $Z(G)$ is the

Definition: Let G be a group. The centre of G denoted $Z(G)$ is the set
$$Z(G)=\{g\in G : gh=hg \text{ for all } h\in G\}$$

Proposition: Let G be a group. Then $Z(G)\lhd G$.

proof: $e\cdot h=h=he \quad e\in Z(G)$.

$g_1,g_2\in Z(G) \quad h\in G. \quad (g_1g_2)h=g_1hg_2=h(g_1g_2) \quad g_1g_2\in Z(G)$.

$\underbrace{g_2}_{Z(G)}$

$g\in Z(G), \quad gh=hg. \quad ghg^{-1}=h\cdot g\cdot g^{-1}=g^{-1}\cdot g\cdot hg^{-1}=g^{-1}\cdot h$.

$g^{-1}h=hg^{-1} \quad g^{-1}\in Z(G)$

$g\in Z(G) \quad h\in G. \quad h^{-1}gh=gh^{-1}\cdot h=g\in Z(G)$.

$Z(G)\lhd G$. $\square$

$Z(S_n)=\{e\}$. $n\geq 3$. $\quad \sigma\in Z(S_n)$

$(12)\sigma=\sigma(12)$

$(23)\sigma=\sigma(23)$

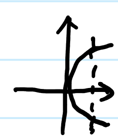
$\vdots$

$\sigma=e$.

proposition: $H\leq G$.

(a). The binary operation $*$ on G/H given by
$$(g_1H)*(g_2H)=(g_1g_2)H. \lhd$$
is well defined if and only if $H\lhd G$.

(b) If $H\lhd G$. $(G/H,*)$ is a group. quotient group.



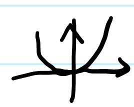
proof. (a). if $H\lhd G$. $\quad g_1H=k_1H. \quad g_2H=k_2H$. $\quad f(x)=y$.

$k_1^{-1}\cdot g_1\in H. \quad k_2^{-1}g_2\in H$. $\quad f(x_1)=y_1 \quad x_1=x_2$

well-defined. $(g_1g_2)H=(k_1k_2)H. \Leftrightarrow (k_1k_2)^{-1}\cdot g_1g_2\in H$. $\quad f(x_2)=y_2 \Rightarrow y_1=y_2$

$\Rightarrow$.

$\Leftrightarrow k_2^{-1}k_1^{-1}g_1g_2\in H$



$\Leftrightarrow k_2^{-1}(k_1^{-1}g_1)k_2(k_2^{-1}g_2)\in H$

$\in H \quad \in H.$

$\in H.$

if $*$ is well-defined. $h\in H. \; g\in G$

$\in H.$

if $*$ is well-defined. $h \in H$, $g \in G$. $\in H$.

$(g^{-1}hg)H = g^{-1}H * hH * gH$

$= g^{-1}H * eH * gH$ $\quad g^{-1}hg \in H.$

$= g^{-1}eg\, H = eH = H.$ $\quad H \triangleleft G.$

(b). $H \triangleleft G$ $\quad *$ is well-defined. associative as G is a group.

$eH * gH = (eg)H = gH = gH * eH.$ identity.

$g^{-1}H * gH = (g \cdot g^{-1})H = eH = gH * g^{-1}H.$ inverse

$(gH)^{-1} = g^{-1}H.$

$(G/H, *)$ is a group. $\square$.

$x^2+y^2 = 1000003$. $\times$ integer solution for x, y?

$x^2+y^2 = 15$? $\times$.

$x^2+y^2 = n.$ $\quad n \bmod 4 = 3 \quad \times.$

i) $x=2a.$ $y=2b$ $\quad 4a^2+4b^2 \bmod 4 = 0.$ ✓

ii) $x=2a+1$ $y=2b$ or $x=2a.$ $y=2b+1.$

$4a^2+4a+1+4b^2 \bmod 4 = 1.$ ✓

iii). $x=2a+1$ $\quad y=2b+1$

$4a^2+4a+1+4b^2+4b+1 \bmod 4 = 2$ ✓

8. April. 2023.

4pm (+8)