Alg-14

11 March 2021 13:13

Alg-14

1- Let G be a group, $H \leq Z(G)$. Then (Center)

Then H is normal in G and if G/H is cyclic then G is abelian

(# 8 in P57 Lang with $H = Z(G)$)

Proof. $xHx^{-1} \subseteq H$ for each $x \in G$

But $H \subseteq Z(G) \Rightarrow xh = hx \ \forall h \in H$

$\Rightarrow xHx^{-1} = H$ & hence normal

Suppose G/H is cyclic. $G/H = \langle xH \rangle = \langle \bar{x} \rangle$

for some $x \in G$

$a, b \in G. \Rightarrow aH \in G/H = \langle xH \rangle$

$\boxed{\langle u \rangle = G.\ v \in G \Rightarrow v = u^r \text{ for some } r \in \mathbb{Z}}$ & $bH \in G/H = \langle xH \rangle$

$aH = (xH)^r$ for some $r \in \mathbb{Z}$

$bH = (xH)^s$ for some $s \in \mathbb{Z}$

$aH = x^r H, \ bH = x^s H$

$a = ae \in aH = x^r H$

$a = x^r h_1$ for $h_1, h_2 \in H \subseteq Z(G)$

$b = x^s h_2$

$ab = (x^r)(x^s) = (x^r h_1)(h_2 x^s)$ ...

$b = x^s h_2$

$$ab = (x^r h_1)(x^s h_2) = (x^r h_1)(h_2 x^s) \quad \text{as } h_2 \in Z(G)$$

$$= x^r (h_1 h_2)(x^s) \quad x h_2 = h_2 x$$

$$= x^r (h_2 h_1)(x^s) \quad x^s h_2 = h_2 x^s \text{ by induction}$$

$$= (h_2 x^r)(x^s h_1)$$

$$= h_2 (x^s \cdot x^r) h_1$$

$$= (x^s h_2)(x^r h_1)$$

$$= ba.$$

$\Rightarrow$ G is abelian

Cor $H = Z(G)$. Then $G/Z(G) = \{Z(G)\}$

Proof From above G is abelian

$H = Z(G) = G \Rightarrow G/H = G/Z(G) = \{Z(G)\}$

#9 Lang P57 $|G| < \infty$, $H \leq G$
s.t. $H \subseteq Z(G)$. Assume $(G:H) = p$,
a prime. Then G is abelian

Proof Since $H \leq G$ and $H \subseteq Z(G)$
$H \trianglelefteq G$. $\Rightarrow$ G/H is a group

$$\left| G/H \right| = \frac{|G|}{|H|} = (G:H) = p \text{ prime}$$

G/H is cyclic (Fact: $|G| = p$, a
prime. $\Rightarrow$ G is cyclic. $a \in G$, $a \neq e$

G/H is cyclic (...

prime, $\Rightarrow$ G is cyclic. $a \in G, a \neq e$

$H = \langle a \rangle \leq G$, $|H| \,\big|\, |G| = p$

$|H| = 1, p$, $|H| = p$, $H = G$

Then apply the previous proofs

$\Rightarrow$ G is abelian

G is nonabelian $\Rightarrow$ $G/Z(G)$ is not cyclic.

Thm - G is nonabelian,
$|G| = pq$, p, q are prime. Then $Z(G) = \{e\}$

Proof Suppose $|Z(G)| > 1$, $Z(G) \trianglelefteq G$

$|Z(G)| \,\big|\, |G| \Rightarrow |Z(G)| = p$ or q

Suppose $|Z(G)| = p$

Now $|G/Z(G)| = q \Rightarrow$

$G/Z(G)$ is cyclic

$\Rightarrow G = Z(G) \Rightarrow$ a contradiction. that is

$Z(G) = \{e\}$

Permutations

$\ldots$ $P_{\ldots}(S) = \{f : S \to S$ bijection$\}$

Permutations

$\phi \neq S$. $Perm(S) = \{f : S \to S \text{ bijection}\}$

$f \in Perm(S)$ is called a permutation

& $(Perm(S), \circ)$ is a group &

Perm S is noncommutative group

$S = J_n = \{1, 2, \dots n\}$, $n > 1$,

Write $Perm(S) = Perm(J_n) = S_n$

symmetric group.

$|S_n| = n!$, $n = 1$, $S_1 = \{\varepsilon\}$

$\varepsilon(1) = 1$

$n > 1$. $\varepsilon(j) = j$, $\forall j \in S_n$ for

the identity element of S_n

$\alpha\varepsilon = \varepsilon\alpha = \alpha$ $\forall \alpha \in S_n$

Permutations were first introduced by Cauchy in 1815

Notation $\alpha \in S_n$

$\alpha(i) \in J_n$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & - & - & n \\ \alpha(1) & \alpha(2) & \alpha(3) & - & & \alpha(n) \end{pmatrix}$$

due to Cauchy.

$\alpha(1)\ \alpha(2)\ \alpha(3)$ ... Cauchy.

(1815)

Defn $\tau \in S_n$ is called a transposition iff $\exists\, i, j \in J_n$ s.t. $\tau(i) = j$, $\tau(j) = i$, and τ fixes the rest i.e. $\tau(k) = k$ for $k \in J_n - \{i, j\}$

i.e. $k \neq i$ or $k \neq j$

Note τ is a transposition

$\Rightarrow |\tau| = 2$, $\tau^{-1} = 2$

$\tau(i) = j$, $\tau(\tau(i)) = \tau(j) = i$

$\tau^2(i) = i$, $\tau^2(j) = \tau(\tau(j))$

$= \tau(i) = j$

$\tau^2(k) = \tau(\tau(k)) = \tau(k) = k$

$\Rightarrow \tau \neq \varepsilon$, $\tau^2 = \varepsilon$.

$\tau^{-1} = \tau$.

Thm Every $\sigma \in S_n$, $\exists\, \tau_1 \ldots \tau_r$ transpositions s.t. $\sigma = \tau_1 \cdots \tau_r$.

Proof Induction on n. $n = 1$ Nothing to prove. ε. suppose $n > 1$, assume every permutation in S_{n-1} is product of transpositions.

Let $\sigma \in S_n$. $\sigma(n) = k$, for some $k \in J_n$

$\tau(n) = k$, $\tau(k) = n$. i.e. τ is a trans

$\tau(n)=k,\ \tau(k)=n$. i.e. τ is a trans

position. $\tau\sigma$ fixes n. i.e. $(\tau\sigma)(n)$

$=\tau(\sigma(n))=\tau(k)=n$. So

$\tau\sigma\in S_{n-1}$. $\exists\ \tau_2\cdots\tau_r$

transpositions s.t. $\tau\sigma=\tau_2\cdots\tau_r$

by induction

$\Rightarrow \sigma=\underbrace{\tau_1^{-1}\tau_2\cdots\tau_r}_{\text{transpositions.}}$

Fact $\sigma\in S_n$

$\sigma=\tau_1\cdots\tau_r$ $\quad\tau_1\cdots\tau_r$

$=\alpha_1\cdots\alpha_s$, $\alpha_1\cdots\alpha_s$ are transpositions

then both r, s are even or both are odd.

2 $\varepsilon=$ product of even # of transpositions

Thm $A_n=\{\sigma\in S_n : \sigma$ is product of even transpositions$\}$

then A_n is a subgroup of S_n.

$\alpha,\beta\in A_n \Rightarrow \alpha\beta$ is product of even # of transpositions.

$\alpha = \tau_1 \cdots \tau_r$

$\alpha^{-1} = \tau_r^{-1} \cdots \tau_1^{-1} = \underbrace{\tau_r \cdots \tau_1}_{\text{even}}$

$\alpha \in A_n \Rightarrow \alpha^{-1} \in A_n.$

$|A_n| = \frac{|S_n|}{2}.$

$A_n \trianglelefteq G = S_n$

Def $\alpha \in S_n$ is an r-cycle $1 \le r \le n$ iff $\exists \{i_1 \ldots i_r\} \subseteq J_n$ s.t.

$\alpha(i_1) = i_2,\ \alpha(i_2) = i_3, \ldots \alpha(i_{r-1}) = i_r$

and $\alpha(i_r) = i_1,\ \alpha(k) = k,\ k \in J_n - \{i_1 \ldots i_r\}$

1-cycle is ε

α is r-cycle, $\alpha = \begin{pmatrix} i_1 & i_2 & & i_{r-1} & i_r \\ i_2 & i_3 & & i_r & i_1 \end{pmatrix}$

$(i_1\, i_2 \cdots i_r) = [i_1 \cdots i_r]$

r-cycle

Note $(i_1\, i_2\, i_3 \cdots i_r) = (i_2\, i_3 \cdots i_r\, i_1)$

$= (i_3\, i_4 \cdots i_r\, i_1\, i_2)$

$= (i_r\, i_1 \cdots i_{r-1})$

How ~~r~~-cycles in S_n?

$(i_1 i_2 \cdot\cdot i_r)$ $\qquad \dfrac{n.n-1 \ldots (n-r+1)}{r} = \left(\dfrac{n!}{(n-r)!}\right)\dfrac{1}{r}$

A 2-cycle is a transposition.

$\alpha \in S_3$, $\quad \alpha(1)=2, \alpha(2)=1, \alpha(3)=3$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \alpha=(1\,2)$$

$$\beta \in S_3 \Rightarrow \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$$

α is an r-cycle

$$\alpha = (i_1 \cdot\cdot\, i_r)$$

$$\alpha^{-1} = (i_r\, i_{r-1} \cdot\cdot\cdot\, i_1)$$

$\beta = (1 2 3)$

$\beta^{-1} = (3 2 1)$

$$\beta\beta^{-1} = (123)(321)$$

$$= (1)(2)(3) = \varepsilon$$

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

$$= \varepsilon$$

$(1 2 3)(3 4)$ in S_4

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$(123)(34) = (1234)$$

$$(34)(123) = (1243)$$

Defn. α & β ~~ε~~ S_n are disjoint permutations iff what is fixed by one is moved by the other i.e. $\alpha(k)=k$, then $\beta(k) \neq k$ & $\beta(j)=j$ Then $\alpha(j) \neq j$

Ex $\alpha = (i_1 \ldots i_r)$, $\beta = (j_1 \ldots j_s)$ be two cycles in S_n

α & β are disjoint iff $\{i_1 \ldots i_r\} \cap \{j_1 \ldots j_s\} = \phi$

$\alpha = (123)$, $\beta = (34)$ Are α & β disjoint cycles? No

$$\{1,2,3\} \cap \{3,4\} = \{3\}$$

Proof α & β are two disjoint permutations then $\alpha\beta = \beta\alpha$

Problem $\alpha \in S_n$, $|\alpha| = ?$

$k \in \mathbb{N}$ is smallest s.t.

$\alpha^k = e$, $k = |\alpha|$ - period

Thm 1- Any $\alpha \in S_n$ is either a cycle or product of disjoint cycles (product decomposition.

(Ruffini, 1799)

2. $|\alpha| = lcm$ (order of cycles in product decomposition

$\alpha = \beta_1 \cdots \beta_k$ $\quad$ β_i is r_i cycle

β_i & β_j are disjoint for $i \neq j$

$|\alpha| = lcm(r_1, r_2 \ldots r_k)$.

Ex $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}$

$= (1\,6)(2\,4)(3\,7\,8\,9)$ are disjoint.

$$|\alpha| = \mathrm{lcm}\{2,2,4\} = 4$$

Want to find $|\alpha|$ for each $\alpha \in S_7$, $|S_7| = 7! = 5040$

Notation $(\underline{r})$ denotes an r-cycle $|(\underline{r})| = r$

$i_1 \ldots i_7$

$(\underline{7})$ — has order 7 & there are 6!

$(\underline{6})(\underline{1})$ — 6 - - -

$(\underline{5})(\underline{2})$ — 10

$(\underline{5})(\underline{1})(\underline{1})$ — 5

$(\underline{4})(\underline{3})$ — 12

$(\underline{4})(\underline{2})(\underline{1})$ — 4

$(\underline{4})(\underline{1})(\underline{1})(\underline{1})$ — 4

✓ $(\underline{3})(\underline{3})(\underline{1})$ — 3

$(\underline{3})(\underline{2})(\underline{1})(\underline{1})$ — 6

$\boxed{✓\ (\underline{3})(\underline{1})(\underline{1})(\underline{1})(\underline{1}) — 3}$

$(\underline{2})(\underline{2})(\underline{2})(\underline{1})$ — 2

$\frac{7.6.5}{3} = 70$

$(\underline{2})(\underline{2})(\underline{1})(\underline{1})(\underline{1})$ — 2

$(\underline{2})(\underline{1})(\underline{1})(\underline{1},\underline{1})(\underline{1})$ — 2

$(\underline{1})(\underline{1})$ - - $(\underline{1}) = 1.$

$(1)\ (1) -\quad - \qquad (1) = 1.$

How many $\alpha \in S_3$ s.t.
$|\alpha| = 3$

$(i_1\ i_2\ i_3)(j_1\ j_2\ j_3)\ (k)$

$\{i_1, i_2, i_3\} \cap \{j_1, j_2, j_3\} = \phi$

$\left(\frac{7.6.5}{3}\right)\left(\frac{4.3.2}{3}\right)$
$= 70 \cdot 8 = 560$

$560 + 70 = 630$ permutations in S_7
have order 3

Rotman – A first course on abstract Algebra (Permutation (2.2)) (3rd Ed)

Gallian – Contemporary Modern Algebra (9th Ed)