18 February 2021 13:38

Alg-9

$|G| = n$, $G = \langle a \rangle$

a^r is a generator of G

$\iff (n, r) = 1$

$n = p$ is prime then # of generators of G is $p-1$

# of generators of $G = \langle a \rangle$, $|G| = n$ is $\varphi(n)$ — Euler's totient function

$= \{ r \in \{1, \dots n\} \text{ s.t } (r, n) = 1 \}$

$\varphi(1) = 1$, for $n \geq 2$

$\Leftarrow (n, r) = 1 \implies a^r$ is a generator

$\langle a^r \rangle \subseteq G \subseteq \langle a^r \rangle$

$a^r \in G$, $\{e, a^r, a^{2r}, \dots\} = \langle a^r \rangle \subseteq G$

$G \subseteq \langle a^r \rangle$

$a \in \langle a^r \rangle \quad a = (a^r)^s$ for some $s \in \mathbb{Z}$.

$(n, r) = 1 \Rightarrow$

$\exists\, s, t \in \mathbb{Z}$

$nt + rs = 1.$

$a = a' = (a^n)^t (a^r)^s = (a^r)^s$

a^r is a generator of $G = \langle a \rangle$

$\langle a^r \rangle = \langle a \rangle \quad x \in \langle a^r \rangle$

$a = (a^r)^s$ for some $s \in \mathbb{Z}$

$a = a^{rs}$

$a^{1-rs} = e \Rightarrow n \mid 1-rs$

$\Rightarrow 1 - rs = nt$ for $t \in \mathbb{Z}$

$\Rightarrow 1 - rs = nt$ for some $t \in \mathbb{Z}$

$\Rightarrow 1 = rs + nt$

$\gcd(r, n) = 1$

$|\langle a \rangle| = |G| = n$

$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

$b \in \langle a \rangle \quad b = a^m$ for $m \in \{0, \ldots n-1\}$

proof or order $|b| = 0$ if $m = 0$

$|b| = |a^m|$ if $m \geq 1$

$$|b| = |a^m| = \frac{n}{\gcd(n, m)}$$

$\langle b \rangle = \langle a \rangle, \; |a| = n$

$$|b| = n = \frac{n}{\gcd(n, m)} \Rightarrow 1 = \gcd(n, m)$$

Inner automorphisms of a group

Inner automorphisms of a group G

For $a \in G$ fixed, define $c_a : G \to G$ by

$c_a(x) = axa^{-1}$, conjugation of x by a

c_a is (1) homo, (2) bijection $\Rightarrow$ c_a is auto

$$c_a(x_1 x_2) = a x_1 x_2 a^{-1}$$
$$= a x_1 a^{-1} a x_2 a^{-1}$$
$$= c_a(x_1) c_a(x_2).$$

$\Rightarrow$ c_a is homo

injective: $c_a(x_1) = c_a(x_2)$

$\Rightarrow$ $a x_1 a^{-1} = a x_2 a^{-1}$

$\Rightarrow$ $x_1 = x_2$ using left and right

' left and right cancellation laws for G

Surjective: $y \in G$ to find

$x \in G$ s.t. $C_a(x) = y$

Take $x = a^{-1} y a \in G$.

$\Rightarrow C_a(x) = axa^{-1} = a(a^{-1} y a)a^{-1}$

$= y$. ✓

✓

Define $\varphi: G \longrightarrow Aut(G)$

by $\varphi(a) = C_a \in Aut(G)$

φ is a homo

$\varphi(ab) = C_{ab}$

$C_{ab}(x) = abx(ab)^{-1}$

$= abxb^{-1}a^{-1}$

$= c(bxb^{-1})$

$$= c_a(c_b(x))$$

$$= (c_a \circ c_b)(x) \quad \forall x \in G$$

$$\Rightarrow I_G = c_{ab} = c_a \circ c_b \checkmark$$

$$\boxed{c_a^{-1} = c_{a^{-1}}} \quad \eta$$

$$c_a = I_G \iff a = e.$$

$$Inn(G) = \{c_a : a \in G\} \leq Aut(G)$$

the set of all inner automorphisms of G.

$Inn(G)$ is a subgroup of G

$\varphi(G) = Inn(G)$

$\varphi(a) = c_a$, $\varphi: G \to Aut(G)$ homo

Later we will find

$\ker \varphi = Z(G)$

the center of G

Zentrum is German for center & this term was coined by J. A. de Seguier in 1904

$Z(G) = \{a \in G : xa = ax \text{ for } \forall x \in G\}$

$Z(G)$ is a subgroup of G

see more later

$Aut(\mathbb{Z}/n\mathbb{Z}) \simeq U_n = \{[x]_n \in \mathbb{Z}/n\mathbb{Z} : \exists [y] \in \mathbb{Z}/n\mathbb{Z}$

$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ $\quad$ $\exists [y] \in \mathbb{Z}/n\mathbb{Z}$ with $[x][y] = 1$ }

U_n is a multiplicative group. $U_n \cong \mathbb{Z}/n\mathbb{Z}$

$|U_n| = \varphi(n)$

Def Let A be an abelian group $(A, +)$

$B \& C$ are subsets of A

(1) $B + C \overset{\text{def}}{=} \{b + c \in A : b \in B \,\&\, c \in C\}$

(2) $B_1 + \cdots + B_r = \{b_1 + \cdots + b_r \in A : b_i \in B_i, i = 1 \cdots r\}$

Fact Suppose $B \& C$ are subgroups of A. Then $B + C$ is a subgroup of A.

More generally $B_1 + \cdots + B_r$ is a subgroup of A if $B_1 \cdots B_r$ are subgroups of A.

Proof. Given $B \leq A$ & $C \leq A$

To $B+C \leq A$ need to

show
(1) $0 \in B+C$
(2) $x, y \in B+C$
$\Rightarrow x+y \in B+C$
(3) $x \in B+C$
$\Rightarrow -x \in B+C$

Def A is abelian group
B & C are two subgroups of A
A is direct sum of B & C,
denoted $A = B \oplus C$ iff
(1) $A = B+C$
(2) if $b_1+c_1 = b_2+c_2$
$\Rightarrow b_1 = b_2,\ c_1 = c_2$

$a \in A$, $\exists!$ b, c

s.t $a = b + c$

More generally $B_i \leq A$

$i = 1 \dots r$, A is abelian

$A = \bigoplus_{i=1}^{r} B_i$, A is direct sum

of $B_1, \dots B_r$ iff (1) $A = B_1 + \dots + B_r$

(2) $a = b_1 + \dots + b_r$

$= b_1' + \dots + b_r'$ for

$b_i, b_i' \in B_i$, $i = 1 \dots r$

then $b_i = b_i'$, $i = 1 \dots r$.

Thm (1) $A = B \oplus C \iff A = B + C$ and $B \cap C = \{0\}$

(2) $A = \bigoplus_{i=1}^{r} B_i \iff \prod_{i=1}^{n} B_i \longrightarrow A$

$(b_1 \dots b_r) \longmapsto b_1 + \dots + b_r$

$\dots \vee B = \prod B_i$

$B_1 \times B_2 \times \cdots \times B_r = \prod_{i=1}^{r} B_i$

is a group

Ex 15 P40. Let A be an abelian group. Assume $\exists n \in \mathbb{N}$ s.t. (n = expo of A)

$na = 0 \quad \forall a \in A$. $\left(\begin{matrix} n \\ ra \end{matrix}\right.$

Suppose $n = rs$, $r, s \in \mathbb{N}$, $(r,s) = 1$

Let $A_r = \{a \in A : ra = 0\}$

$A_s = \{a \in A : sa = 0\}$

Then (1) A_r & A_s are subgroup of A.

(2) $A_r \cap A_s = \{0\}$

(3) $a \in A \Rightarrow \exists\, b \in A_r$ & $c \in A_s$ s.t. $a = b + c$ $\quad A = A_r + A_s$

iff $A = A_r \oplus A_s$.

Proof. (1) $A_r \leq A$

$0 \in A_r$, $ra_i = 0$, $i = 1, 2$

$a_1, a_2 \in A_r$, $ra_i = 0$, ...

$a_1 + a_2 \in A_r$ $\Leftarrow$ $r(a_1+a_2)$

$= ra_1 + ra_2$

$= 0 + 0$

$= 0$

$0 \in A_r$.

$a \in A_r \Rightarrow r(-a)$

$= -(ra)$

$= -0$

$= 0$

So $A_r \leq A$.

$a \in A$. To find $b \in A_r, c \in A_s$

s.t. $a = b + c$

$\gcd(r,s) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$

s.t. $xr + ys = 1$.

$a - 1a = (xr + ys)s$

$a = 1a = (xr + ys)a$

$= (xr)a + ysa$

$xra \in A_s$ and $ysa \in A_r$

$s(xra) = x(r(sa)) = x(rsa)$

$= x(na)$

$= x(0)$

$= 0$

as $rs = n$

Similarly $ysa \in A_r$.

$b = ysa \in A_r$

$c = xra \in A_s$

$a = b + c$

Next $A_r \cap A_s = \{0\}$

Suppose let $x \in A_r \cap A_s$

$rx = 0$ and $sx = 0$

$\ldots \in \mathbb{Z}$

$r x = 0$ and $s x = 0$

$(r,s) = 1$, $\exists$ $ru + sv = 1$ $\quad u, v \in \mathbb{Z}$

$$x = rux + svx$$
$$= u(rx) + v(sx)$$
$$= 0 + 0$$
$$= 0.$$

Will see later in structure theory for finite abelian groups

---

cosets and Normal subgroups

G is a group

$(G, \cdot)$ - Product

S_1, S_2 are subsets of G

(1) $S_1 S_2 \overset{\text{def}}{=} \{ s_1 s_2 \in G : s_1 \in S_1, s_2 \in S_2 \}$

(i) $(S_1 S_2) S_3 = S_1 (S_2 S_3)$

$(G, +)$ abelian

$S_1 + S_2 \overset{\text{def}}{=} \{ s_1 + s_2 \in G : s_i \in S_i, i = 1,2 \}$

$(S_1 + S_2) + S_3$

(i) $(S_1 S_2)S_3 = S_1(S_2 S_3)$ assoc!

$(S_1+S_2)+S_3$
$= S_1+(S_2+S_3)$

(ii) $S_1(S_2 \cup S_3) = S_1S_2 \cup S_1S_3$

$S_1+(S_2 \cup S_3)$
$= (S_1+S_2) \cup (S_1+S_3)$

(iii) $H \leq G$
$HH = H$

$H+H = H$.

Proof (i) $S_1(S_2S_3) \subseteq (S_1S_2)S_3 \subseteq S_1(S_2S_3)$

$x \in S_1(S_2S_3) \Rightarrow x = s_1(s_2s_3)$ $s_i \in S_i$

$= (s_1s_2)s_3$ using assoc. law

$\in (S_1S_2)S_3$

(ii) To show $S_1(S_2 \cup S_3) \subseteq S_1S_2 \cup S_1S_3$

$\subseteq S(S \cup S_2)$

$\subseteq S_1(S_2 \cup S_3)$

$x \in S_1(S_2 \cup S_3)$

$x = st$, $s \in S_1$, $t \in S_2 \cup S_3$

$\Rightarrow t \in S_2$ or $t \in S_3$

$x = st \in S_1 S_2$ if $t \in S_2$

or $\in S_1 S_3$ if $t \in S_3$

i.e. $x \in S_1 S_2 \cup S_1 S_3$

(iii) $HH \subseteq H \subseteq HH$ if $H \leq G$

$x \in HH$, $x = hk$ for $h, k \in H$

$\in H$ as $H \leq G$

$\Rightarrow HH \subseteq H \subseteq HH$

$= HH$

$h \in H$, $h = he \in HH$

G is a group, $H \leq G$, $a, b \in G$

(i) $aH = \{ah : h \in H\}$ is called a left coset of H in G

(ii) $Hb = \{hb : h \in H\}$ is called a right of H in G

Any element of (aH) is called a coset representative of the coset aH.

$ah \in aH$ is a coset rep of aH

$a = ae \in aH$ is also a coset rep of aH.

... of H in G

Proof. Any two left cosets of H in G are either disjoint or identical.

aH, bH are two left cosets then $aH \cap bH = \phi$ or else $aH = bH$

Proof. If $aH \cap bH = \phi$, done

If not $aH \cap bH \neq \phi$.

let $x \in aH \cap bH$.

$x = ah_1 = bh_2$ for $h_1, h_2 \in H$.

Now $h_1 H = h_2 H = H$ as

H is a subgroup

$h_1 H = H = h_2 H$ (check it)

$aH = a(h_1 H) = (ah_1)H = (bh_2)H$

$= b(h_2 H)$

$= bH$.

Let G be a group, $H \leq G$

$$G = \bigcup_{i \in I} b_i H$$

where $\{b_i : i \in I\}$ is a collection of distinct elements of G

Notation $H \leq G$

$G/H = \{aH : a \in G\}$, the set of all left cosets of H in G

$H \backslash G = \{Hb : b \in G\}$ the set of right cosets of H in G

$(G : H) = [G : H] = |G/H|$

$=$ # of elements in G/H

2 is called the index of H in G

Thm. G is a finite group $H \leq G$. Then

(1) $(G:H)|H| = |G|$

(2) $|H| \mid |G|$ (Lagrange's Thm proved in 1770)

↑ divides & $|H| = \#H$

(3) $a \in G$, $|a| \mid |G|$

(4) $K \subseteq H \subseteq G$, K & H are subgroups of G

then $(G:K) = (G:H)(H:K)$

To this theorem need a

Lemma $H \leq G$. Then H and aH have the same number of elements

number of elements.

Proof. Define $f: H \to aH$

by $f(h) = ah$.

Then f is (1) injective

(2) surjective.

$f(h_1) = f(h_2) \Rightarrow ah_1 = ah_2$

$\Rightarrow h_1 = h_2$

using left cancellation law

showing ψ is injective

check that f is surjective

$|G| < \infty$, $G = \bigcup_{i=1}^{r} q_i H$

where $q_1, \ldots q_r$ are distinct elements of G so that the left cosets $q_1H, \ldots q_rH$ are all distinct

$|qH| = |H|$

$\vdots$

$= n$

$$|G| = |\bigcup_{i=1}^{n} a_i H|$$

$$= |a_1 H| + \cdots + |a_r H|$$

$$= r|H|$$

$$r = |G/H| = (G : H)$$

$$|G| = (G : H)|H|$$

$$\Rightarrow |H| \mid |G|$$

(3) $\langle a \rangle = H$, $|H| = |a|$ &
$|a| = |H| \mid |G|$.