Alg-11

Induction
divisibility in $\mathbb{N}$, $\mathbb{Z}$,
gcd, lcm
cyclic group. period of a $\in G$,
Group, subgroup. coset of a subgroup, homo, iso, auto
quotient group

$\mathbb{Z}$ is a cyclic group

$\mathbb{Z} = \langle 1 \rangle$ | $H \leq G = \mathbb{Z}$

$H = \langle m \rangle$, $m \in \mathbb{N}$ $m = 1$

$H = \mathbb{Z}$, $m > 1$ $H \neq \mathbb{Z}$

↑ Podgr.

$\mathbb{Z}$ is abelian

$H \leq \mathbb{Z}$ is normal

left-coset of H in $\mathbb{Z}$

i.e. H is a coset of H in $\mathbb{Z}$

$H \leq G$

aH

...

$k+H$ is a coset of H in $\mathbb{Z}$

$= \{k+h : h \in H\}$

$= \{h+k : \forall h \in H\}$ as $\mathbb{Z}$ is abelian

$= H+k.$

$\mathbb{Z}/H$ = the set of all distinct cosets of H in $\mathbb{Z}$.

$H = \langle m \rangle$

$= \{nm : n \in \mathbb{Z}\}$

$k+H = l+H$

$\Rightarrow k-l \in H \Rightarrow k-l = mp$ for some $p \in \mathbb{Z}$

$k \neq l \Rightarrow m \nmid k-l$

$k \in \mathbb{Z}$, $k = qm + r$, $0 \leq r < m$

$k-r \in H.$

$k+H = r+H$, $0 \leq r \leq m-1$

$\mathbb{Z}/H = \{0+H, 1+H, 2+H, \ldots, (m-1)+H\}$

$$\mathbb{Z}/m\mathbb{Z} = \{0+H,\ 1+H,\ 2+H,\ \dots,\ (m-1)+H\}$$

$$= \{H,\ 1+H,\ \dots\ (m-1)+H\}$$

$H = [0]_m$, $1+H = [1]_m$, $\dots$ $[r]_m = r+H$

$r \in \{0, \dots m-1\}$

$n\mathbb{Z} \subseteq m\mathbb{Z} \Rightarrow n = n.1 \in n\mathbb{Z} \subseteq m\mathbb{Z}$

$n, m \in \mathbb{N} \Rightarrow n = mk$ for some $k \in \mathbb{N}$

$\Rightarrow m \mid n$

So $n\mathbb{Z} \subseteq m\mathbb{Z} \Rightarrow m \mid n$

$\Leftarrow$?

Yes

$n\mathbb{Z} \subseteq m\mathbb{Z} \Leftarrow m \mid n.$

$m\mathbb{Z} \leq \mathbb{Z}$

$n\mathbb{Z} \subseteq \mathbb{Z}$

$n\mathbb{Z} \leq m\mathbb{Z}$

subgroup

$$\left| m\mathbb{Z} / n\mathbb{Z} \right| = \frac{m}{n}$$

$m\mathbb{Z}$

is finite $\Leftrightarrow$ # of distinct cosets of $n\mathbb{Z}$ in $m\mathbb{Z}$ is finite

$S_3 = \{e, \alpha, \beta, \beta^2, \alpha\beta, \beta\alpha\}$

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

$\beta(1) = 2$
$\beta(2) = 3$ $\Leftrightarrow \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
$\beta(3) = 1$

$\alpha\beta(1) = \alpha(2) = 1$ $\Leftrightarrow \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
$\alpha\beta(2) = \alpha(3) = 3$
$\alpha\beta(3) = \alpha(1) = 2$

$\beta\alpha(1) = \beta(2) = 3$
$\beta\alpha(2) = \beta(1) = 2$ $\Leftrightarrow \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
$\beta\alpha(3) = \beta(3) = 1$

$\alpha\beta \neq \beta\alpha \Rightarrow S_3$ is not commutative
// β

$\alpha\beta \neq \beta\alpha \Rightarrow S_3$ is not

$S_3 = \{ \underbrace{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}}_{e}, \underbrace{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}}_{\alpha}, \underbrace{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}}_{\beta}$

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

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

$\beta^2(1) = \beta(\beta(1)) = \beta(2) = 3$

$\beta^2(2) = \beta(\beta(2)) = \beta(3) = 1$

$\beta^2(3) = \beta(\beta(3)) = \beta(1) = 2$

$H_1 = \{e, \alpha\} = \{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \}$

$\leq G = S_3$

S_3/H_1 = the set of distinct left cosets of H_1 in S_3

$|S_3/H_1| = (S_3 : H_1) = \frac{|S_3|}{|H_1|} = \frac{6}{2} = 3$

$S/H_1 = \{ H_1, \beta H_1, \beta^2 H_1, \alpha\beta H, \beta\alpha H \}$

" " check that = ".

$\alpha H_1 = H_1$, check that $\alpha\beta H = \beta^2 H$.

$S/H_1 = \{H_1, \beta H_1, \beta^2 H_1\}$

is not a group

Last time: if $H \triangleleft G$ △

then $G/H = \{bH : b \in G\}$

is a group: $(aH)(bH) = abH$

◁ — normal.

H is normal $\iff$ either

$N_G(H)\, aHx^{-1} = H \quad \forall x \in G$

$\Updownarrow$

$H = \ker f$ for some hom $f: G \to G'$ for some gp G'

If $H = \ker f$, $f: G \to G'$ is homo

then $xHx^{-1} = H$

Proof. We show $xHx^{-1} \subseteq H$, $\forall x \in G$.

then $x^{-1}H(x^{-1})^{-1} \subseteq H$ by taking $x^{-1} \in G$

$\|$

Assume $x^{-1}Hx \subseteq H$

$\Rightarrow$ prove $H \subseteq xHx^{-1}$

$h \in H$, $x^{-1}hx \in H$

$h_1 = x^{-1}hx \in H$

$\Rightarrow xh_1x^{-1} \in xHx^{-1}$

$H = \ker f$. $xHx^{-1} \subseteq H$

$y \in xHx^{-1}$, $y = xhx^{-1}$, $h \in H = \ker f$

$f(h) = e'$

Recall that

$\ker f = \{a \in G : f(a) = e'\}$

$f(y) = f(xhx^{-1}) = f(x)f(h)f(x)^{-1}$

$= f(x)e'f(x)^{-1}$

$= f(x)f(x)^{-1} = e'$

$\Rightarrow xhx^{-1} \in H$

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

So $xHx^{-1} = H$

$\Leftrightarrow xH = Hx$

$aH = bH \Leftrightarrow b^{-1}a \in H$

$\Leftrightarrow a^{-1}b \in H$

G. H. Hardy

(1) Prove Riemann Hypothesis.

$$\zeta(z) = \sum_{n \in \mathbb{N}} \frac{1}{n^z}$$

(2) Prove non-existence of God

(3) Be a great cricket player

(4) To kill Mussolini.

David Hilbert, Hilbert Space

David Trilfaro

Thm $H \trianglelefteq G$.

Then G/H = the set of all left cosets of H in G is a group under coset product:

$(aH)(bH) = abH$.

Proof $(aH)(bH) = a(Hb)H = a(bH)H$

as $Hb = bH$

$= (ab)HH$

$= abH$

as $HH = H$ since H is a subgroup.

Is this product well defined?

$aH = a'H \iff a'^{-1}a \in H$

$bH = b'H \iff b'^{-1}b \in H$

$(aH)(bH) = (a'H)(b'H)$?

$abH = a'b'H$?

$(a'b')^{-1}(ab) \in^{?} H$

$(a'b')(ab) \in H$

$b'^{-1}(a'^{-1}a)b \overset{?}{\in} H$ finish it.

- $(aH)(bH) = abH \in G/H$.

associative $(aH)[(bH)(cH)]$

$= [(aH)(bH)](cH)$

$(aH)[(bH)(cH)] = (aH)(bcH)$

$= a(bc)H$

$= (ab)cH$

$= (abH)(cH)$

$= [(aH)(bH)](cH)$

$e_{G/H} = H$, $(aH)H \overset{?}{=} aH$

$= H(aH)$

$(aH)(H) = a(HH) = aH$,

$H(aH) = H(Ha) = (HH)a = Ha$

$H = H(Ha)$

$$(aH)H = aH = H(Ha)$$

For each $aH \in G/H$

$$(aH)^{-1} \stackrel{?}{=} a^{-1}H$$

$$(aH)(a^{-1}H) = aa^{-1}H = eH = H$$

$$(a^{-1}H)(aH) = a^{-1}aH = eH = H$$

$$\Rightarrow (aH)^{-1} = a^{-1}H .$$

$$\mathbb{Z}/m\mathbb{Z} = \{ r + m\mathbb{Z} : 0 \le r \le m-1 \}$$

group

$$(r+m\mathbb{Z}) + (s+m\mathbb{Z}) = r+s+m\mathbb{Z}$$

$$\mathbb{Z}/10\mathbb{Z} = \{ r+10\mathbb{Z} : 0 \le r \le 9 \}$$

$$(8+10\mathbb{Z}) + (7+10\mathbb{Z}) = 15 + 10\mathbb{Z}$$

$(8+10\mathbb{Z})+(7+10\mathbb{Z})=\cdots$

$=5+10+10\mathbb{Z}$

$=5+10\mathbb{Z}$.

$-(8+10\mathbb{Z})=2+10\mathbb{Z}$.

$H \triangleleft G \Rightarrow G/H$ is a group called a factor group or a quotient group, read G/H as G mod H.

There are two meanings of G/H — the set of left cosets.

If $H \triangleleft G$, then it is a group

Or $H \leq G$, $aH = Ha$ i.e. $H \triangleleft G$

Define $\pi = f : G \to G/H$ by

$\pi(a) = f(a) = aH$.

then $\pi = f$ is a homo , H.

then $\pi = f$ is a ...

and $\ker \pi = \ker f = H$.

Proof G/H is a group as

$H \trianglelefteq G$.

$$f(ab) = (ab)H = (aH)(bH)$$
$$= f(a)f(b)$$

$\Rightarrow \pi = f$ is a hom

$$a \in \ker \pi = \ker f \iff f(a) = e_{G/H}$$

$$aH = f(a) = e_{G/H} = H$$

$$H = aH \Rightarrow a \in H$$

$$\ker \pi = \ker f = H$$

$\pi : G \to G/H$ is called the canonical or natural map

(Jordan curve thm) C.

Cor. 1st Isomorphism Thm (Jordan 1870)

$f : G \to G'$ is a hom & $H = \ker f$

$\Rightarrow$ $\exists$ a map $\bar{f} : G/H \to G'$.

then there a map $\bar{f}: G/H \to G'$

defined by $\bar{f}(aH) = f(aH)$

s.t. (1) $\bar{f}$ is a homo

(2) $\bar{f}$ is iso onto $f(G) = \operatorname{im} f$

$$G/H \xrightarrow{\bar{f}} f(G)$$

$\bar{f}$: isomorphism

Proof. Note that $h \in H = \ker f$ and $a \in G$ then

$f(ah) = f(a)f(h) = f(a)e' = f(a)$

Thus $f(aH) = f(a) \in G'$

$f(aH) \in f(G) = \operatorname{im}(f) = \{f(x) \in G' : x \in G\}$

$\bar{f}(aH \cdot bH) = f(abH) = f(ab)$

$= f(a)f(b)$

$= f(aH)f(bH)$

$\Rightarrow \bar{f}$ is homo

$aH \in \ker \bar{f} \Rightarrow \bar{f}(aH) = e'$

//

$aH \subseteq H$ ker f

$f(a) \Rightarrow a \in H = \ker f$

$aH \subseteq H \Rightarrow$. Thus $\ker \bar{f} = \{H\}$

$\bar{f}$ is injective

Hence $\bar{f}(G/H) = f(G)$

i.e. $G/H \cong f(G)$.

Ex $f : (\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, \cdot)$ defined by $f(t) = e^{it}$. Then f is a homo

$f(s+t) = e^{i(s+t)} = e^{is} \cdot e^{it} = f(s) f(t)$

$\Rightarrow f$ is homo.

$f(\mathbb{R}) = S^1 = \{z \in \mathbb{C}^* : |z| = 1\}$

$\subseteq \mathbb{C}^*$.

$z \in S^1 \Leftrightarrow z = e^{it}$ for some $t \in \mathbb{R}$.

$t \in \ker f \iff f(t) = e^{it} = 1$

$\| \quad e^{it} = e^{i0}$

for some $t = 2\pi n$, $n \in \mathbb{Z}$

$\ker f = 2\pi\mathbb{Z} \leq \mathbb{R}$.

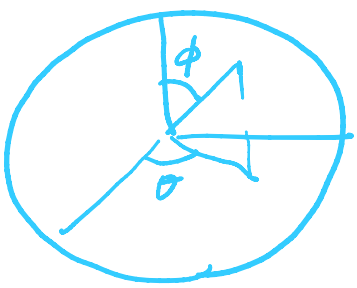
$\mathbb{R}/2\pi\mathbb{Z} \simeq f(\mathbb{R}) = S^1$

$\mathbb{R}/2\pi\mathbb{Z} = S^1$

$= \mathbb{T}$

$S^n = \{x \in \mathbb{R}^{n+1} : \|x\|_2 = 1\}$

$S^2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 = 1\}$



$\mathbb{T}^2 = T \times T$

$\mathbb{T}^n =$

Homotopy Theory

$\pi_1(\mathbb{T}^1) = \mathbb{Z}$

$\pi_1(\mathbb{T}^2) = \mathbb{Z} \times \mathbb{Z}$.

π_1 : 1st fundamental group

Cor: $|G| < \infty$. $f: G \to G'$ is homo

then $|f(G)| \mid |G|$.

Proof $|f(G)| = |G/\ker f| = \frac{|G|}{|\ker f|}$

$|G| = |\ker f|\,|f(G)|$

$\Rightarrow |f(G)| \mid |G|$.

$G \xrightarrow{f} f(G)$

$\pi \searrow \quad \nearrow \bar{f}$

G/H

$f = \bar{f} \circ \pi$