


第8回 代数系

JNF の議論

$$\text{例} \rightarrow f: V \rightarrow V : \mathbb{C}\text{-linear} \\ \text{s.t. } f^2 = \text{id}_V$$

$$\{v \in V \mid f v = \pm v\} \leftarrow \text{方程式の解}$$

陰

$$\left\{ \frac{v \pm f(v)}{2} \mid v \in V \right\} \leftarrow \text{陽}$$

線形代数

$$A \vec{x} = \vec{0}$$

陰

$$\vec{x} = c_1 \vec{x}_1 + \dots + c_d \vec{x}_d$$

陽

$$A: m \times n \quad \vec{x} \in K^n$$

群

PID上へ加群 $\rightarrow$ Jordan

可換環

$U(R)$

"

$R \mapsto R^X$: 乘法群

"

$\{a \in R \mid \exists b \in R \text{ s.t. } ab = 1_R\}$

Def $(G, \cdot, e)$: 群

結合, e : 単位元, 逆元

加群 = 群 + 可換

R 加群 = 加群 _{V} + " $R \times V \rightarrow V$ "

$X \cap \dots$: 群 $\&C$ に有限, 非可換 s.t. --

$H \subseteq G$ 部分群

群 $(G, \cdot, e)$

def $\Downarrow$
 $(H, \cdot|_{H \times H}, e)$ 群 $\left(\begin{array}{l} \text{と} \\ e \in H \end{array} \right)$

$\Updownarrow$ def $\Leftarrow$ 群を別々に (e.g. 環)

$\Downarrow$ 普通 用いられ

$\Updownarrow$ iff $H \neq \emptyset, \forall a \in H, b \in H, ab^{-1} \in H$

$\Downarrow$ 明証

剰余類

$$G \supseteq H$$

群 部分群

$$g \sim g' \stackrel{\text{def}}{=} g^{-1}g' \in H$$

これに同値関係 $\sim$ を与える

$$\text{同値類 } C_g = [g] = gH$$

$$= \{ ga \mid a \in H \}$$

商集合 G/H と書く G

15

$$G = \coprod gH$$

$$[g] \in G/H$$

$$\cup \\ gH$$

$$\sum G = \text{有限} \Rightarrow |H| \mid |G|$$

$\cup$

H : 部分群

$$(\because) \forall g \in G, |gH| = |H| \text{ となる}$$

$$\varphi_g: G \rightarrow G \quad \text{これは単射}$$

$$x \mapsto gx \quad (gx = gx' \Rightarrow x = x')$$

$$\varphi_g^{-1}(gH) = H$$

Def G : 有限群

ψ
 g

$g^0, g^1, \dots$

$$\exists n \geq 1 \quad g^n = e$$

$$\left(\because \exists a \neq \exists b \quad g^a = g^b \right) \\ \geq 1, \therefore g^{a-b} = e$$

n 的最小值 $\text{ord}_G(g)$

引 $\text{ord}_G(g) \mid |G|$

$g^0, g^1, \dots, g^{\text{ord}_G(g)-1}$

$$\textcircled{1} H = \{ g^n \mid n \in \mathbb{Z} \} \subseteq G$$

是 G 的子群, $|H| = \text{ord}_G(g)$ //

10.17 フェルマの小定理

$$n \geq 1 \quad \phi(n) = \left| (\mathbb{Z}/n\mathbb{Z})^\times \right|$$

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{ [a] \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1 \}$$

sketch $\gcd(a, n) = 1$

$$\Rightarrow \exists x, \exists y \in \mathbb{Z} \quad ax + ny = 1$$

$$[a][x] = [1] \text{ in } \mathbb{Z}/n\mathbb{Z}$$

$$\phi(n) = \left| \{ 1 \leq a \leq n \mid \gcd(a, n) = 1 \} \right|$$

ex $a: n \text{ と互いに素} \quad a^{\phi(n)} \equiv 1 \pmod{n}$

$(\mathbb{Z}/n\mathbb{Z})^\times$ にラグランジュ apply

$$p: \text{素数} \quad \phi(p) = p-1$$

$$p: \text{奇素数} \quad 2^{p-1} \equiv 1 \pmod{p}$$

(フェルマーの小定理)

$$n = p_1^{e_1} \cdots p_s^{e_s} \quad p_1 \sim p_s: \text{互いに素}$$

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right) \quad e_i \geq 1$$

☺ CRT

$$\mathbb{Z}/n\mathbb{Z} \simeq \underbrace{(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{e_s}\mathbb{Z})}_{\text{ax は}}$$

$$(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^{\times} \times \cdots \times (\mathbb{Z}/p_s^{e_s}\mathbb{Z})^{\times}$$

$$\left| \left(\mathbb{Z}/p\mathbb{Z} \right)^{\times} \right| = p \left(1 - \frac{1}{p} \right) \text{ の場合、}$$

p : 素数

$e \geq 1$

つまり $g \sim g' \stackrel{\text{def}}{\iff} g^{-1}g' \in H \quad C_g = gH$

と $g'g^{-1} \in H$ とも同様に

議論は可能

$$(C_g = Hg := \{hg \mid h \in H\})$$

Def G : 群

$\cup$

正規部分群

H : 部分群

$(H \trianglelefteq G)$

$$\Leftrightarrow \forall g \in G \quad gH = Hg \text{ in } G$$

$$\Leftrightarrow \forall g \in G, \quad g^t H g = H$$

R 環
 I ideal

R/I : 商環

群 G 正規部分群 N G/N : 商群

G : 群 $\supset N$: 正規部分群

G/N は 10 通りの方法で群になる

def G_1, G_2 : 群 = 積, 単位, 逆元

写像 $\varphi: G_1 \rightarrow G_2$: 群準同型

$$\Rightarrow \textcircled{1} \forall g \forall g' \quad \varphi(gg') = \varphi(g)\varphi(g')$$

def $\textcircled{2} \varphi(e_1) = e_2$

$$\textcircled{3} \forall g \quad \varphi(g^{-1}) = \varphi(g)^{-1}$$

(環も同様にするのと同じ)

$$\Leftrightarrow \forall g \forall g' \quad \varphi(gg') = \varphi(g)\varphi(g')$$

iff

この講義では逆元を積の

逆元として定めている。

prop $G \xrightarrow{f} G/N$ は群準同型

Cor G の正規部分群

例 $f: G \rightarrow G'$: group hom $\circ$ $\ker f$

$$\{g \in G \mid f(g) = e_{G'}\}$$

① 一般に $\ker f \trianglelefteq G$ は易し

$$\ker(G \rightarrow G/N) = N //$$

環と ideal Z "同値"

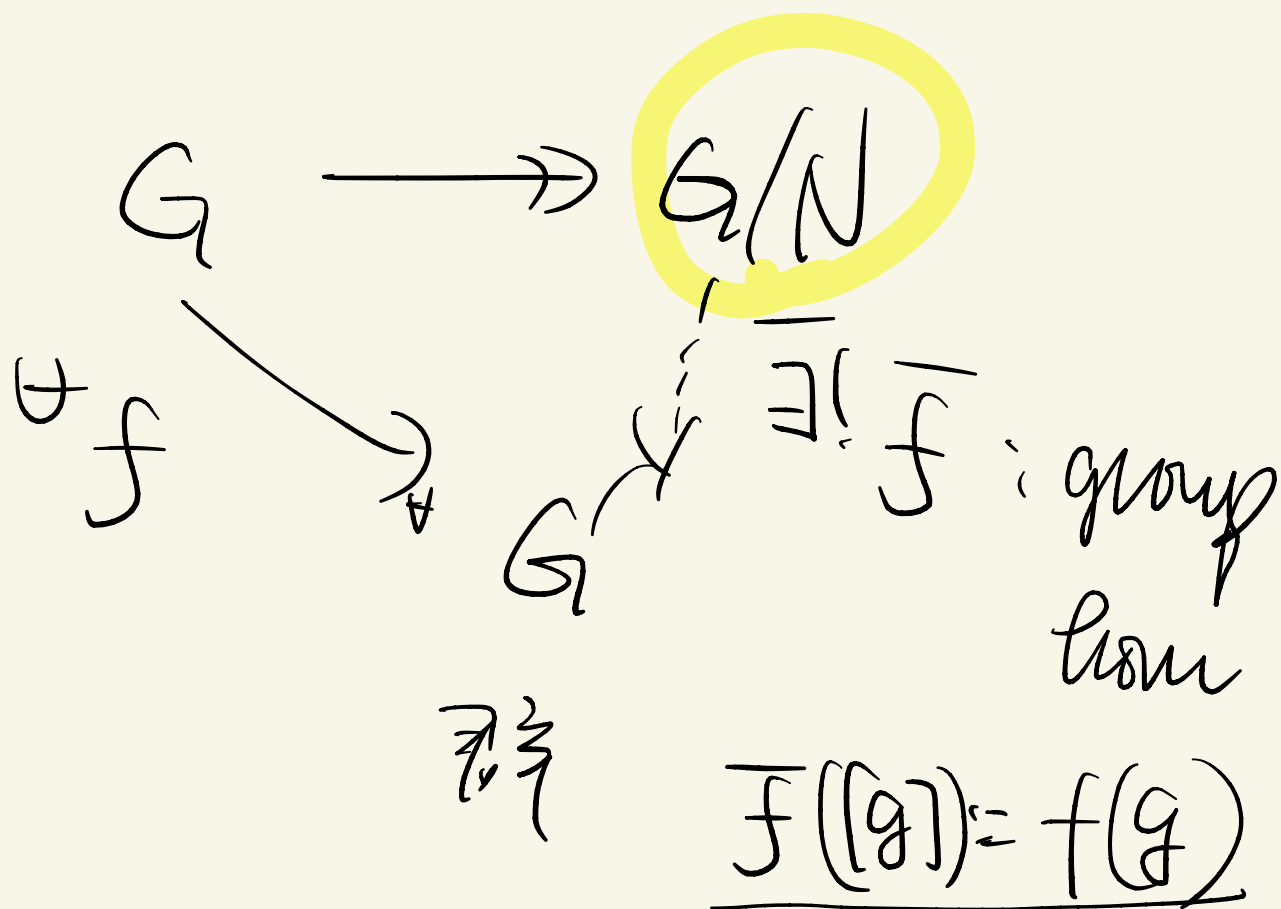
//

環準同型 $\circ$ $\ker$

I

$$\ker(R \rightarrow R/I)$$

~~prop~~ $G: \text{群}$ $N: \text{正规}$



f : group hom

$$g_1 \sim g_2 \Rightarrow f(g_1) = f(g_2)$$



$$g_1 N = g_2 N$$



$$Ng_1 = Ng_2$$

Thm (群の同型定理)

$$\begin{array}{ccc} G & \xrightarrow{f} & G' : \text{group hom} \\ \downarrow & \nearrow \exists! \bar{f} & \\ & G/\ker f & \end{array}$$

f は単射 $G/\ker f \cong \text{Im } f$
 同型

$\uparrow$

$$g_1 \sim g_2 \Leftrightarrow f(g_1) = f(g_2)$$

を check する.

$\Rightarrow$ と言うと $\dots \rightarrow \exists!$ だけを示す

群的作用 $\triangleq$ R 为群 $R \times V \rightarrow V$

def $G \curvearrowright X$: 作用为

群 集合

映射 $G \times X \rightarrow X$

$$(g, x) \mapsto gx$$

s.t. $\forall g_1, g_2 \in G, \forall x \in X$

①

$$g_1(g_2 x) = (g_1 g_2) x$$

② $\forall x \in X, ex = x$

Ex

$$X: \text{集合} \quad \mathcal{S}_X = \text{Bij}(X) \quad \text{双射群}$$

$$\mathcal{S}_X \times X \rightarrow X \quad \text{作用}$$

$$(f, x) \mapsto f(x)$$

$$g(f(x)) = (g \circ f)(x)$$

$$\cong M_n(\mathbb{C}) \times \mathbb{C}^n \rightarrow \mathbb{C}^n$$

$$(A, \vec{v}) \mapsto A\vec{v}$$

$$\text{End}(V) \times V \rightarrow V$$

$$\{f: V \rightarrow V: \text{线性}\} \quad (f, v) \mapsto f(v)$$

$$\text{Ex } GL_n(\mathbb{C}) \times M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$$

$$(P, M) \mapsto PMP^{-1}$$

(作用)

の M 軌道の ϕ に
JNF(M) の軌道

(これは
代表でもある)

$P^{-1}MP$ による作用 (軌道) (軌道)

$$(P, M) \mapsto P^{-1}MP$$

$$(QP, M) \mapsto (QP)^{-1}M(QP)$$

$\times ?$

$$Q^{-1}(P^{-1}MP)Q$$

$$(PQ)^{-1}MPQ$$

Ex $M_{mn}(\mathbb{C})$

(1)

$$M \mapsto PMQ$$

$$(GL_m(\mathbb{C}) \times GL_n(\mathbb{C})) \times M_{m,n}(\mathbb{C})$$

$$((P, Q), M)$$

$\downarrow$

$$PMQ^T$$

$$\downarrow$$

$$M_{m,n}(\mathbb{C})$$

軌道の

代表として

$$\begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix} \text{ 等}$$

とある。

(τ_0)

$$X \times Y$$

$$\uparrow \exists !$$

$$P_X$$

$$P_Y$$

$$P_X$$

$$X$$

$$\alpha$$

$$\uparrow$$

$$Z$$

$$Z$$

$$\rightarrow \beta$$

$$Y$$

Ex G 群 $\supset H$ 部分群

$$G \times G/H \rightarrow G/H$$

$$(g, [g']) \mapsto [gg']$$

記法 $G \times X \rightarrow X : \text{作用}$

$$x \in X \quad G \cdot x = \{gx \mid g \in G\}$$

① 軌道 $\bigcup_x$

$$\textcircled{2} \text{Stab}_G(x) = \{g \in G \mid gx = x\}$$

Q は G の部分群

~~prop~~ $G \times X \rightarrow X : \text{pr}_2$

$$\textcircled{1} x \sim x' \stackrel{\text{def}}{\iff} Gx = Gx'$$

~~iff~~ ~~def~~ $\Downarrow$ $\{x \in X \mid \dots\}$ は X 上の同値関係

$$(Gx \cap Gx' \neq \emptyset)$$

$$\textcircled{2} G/\text{Stab}_G(x) \xrightarrow[\text{bij.}]{\sim} G \cdot x$$

$\textcircled{1} \textcircled{2}$ 易しい

$$\textcircled{2} G \twoheadrightarrow Gx$$

$$g \mapsto gx$$

$\downarrow$ $G/\text{Stab}_G(x)$

$$x = g^{-1}g'x$$

$\uparrow$

$$gx = g'x$$

$$\Downarrow$$

$$g^{-1}g' \in \text{Stab}_G(x)$$

ポリマの数え上げ理論

~~X~~

G
 G

作用

系 G : 有限群 $\curvearrowright X$ 集合

$$\Rightarrow \forall x \in X, \quad |Gx| \neq |G| \quad \text{約数}$$

$(\text{Stab}_G(x))$

共役類

G : 群

$$G \times G \longrightarrow G$$
$$(g, x) \mapsto gxg^{-1} \quad (\text{共役})$$

軌道 $Gx = \text{Conj}_G(x)$

①

$$= \{gxg^{-1} \mid g \in G\}$$

x の共役類

② $\text{Stab}_G(x) = \{g \in G \mid gx = xg\}$

$$= C_G(x) : \text{centralizer}$$

$$(3) \bigcap_{x \in G} C_G(x) = Z(G) \quad \Phi(G)$$

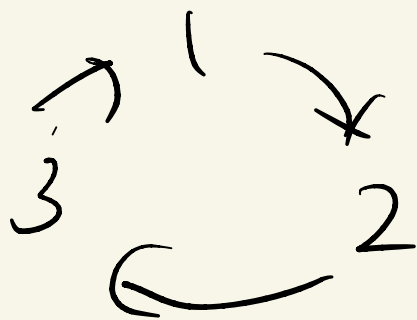
$$\{g \in G \mid \forall h \in G \ gh = hg\}$$

Ex $S_3 = S_{\{1,2,3\}} = \text{Bij}(\{1,2,3\})$

ψ
 $f \quad \delta$

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$$

$$1 \rightarrow 2 \rightarrow 3$$



類等式

$$G \times X \rightarrow X \quad \text{作用}$$

$\hookrightarrow$

$$X = \bigsqcup G \cdot x$$

$$[x] \in X/\sim$$

同値関係

これを今の設定に apply すると

$$G = \bigsqcup_{x \in S} \text{Conj}_G(x) \quad \exists \quad S \subseteq X$$

$$= Z(G) \sqcup \bigsqcup_{x \in S \setminus Z(G)} \text{Conj}_G(x)$$

全 S_3 に位数 2 の正規部分群
は存在しない

① 類方程式

$$6 = 1 + 3 + 2 \quad \hookrightarrow \text{conj}(\mathbb{C})$$

$$\quad \quad \quad \uparrow \quad \quad \quad \uparrow$$

$$Z(S_3) \quad \text{conj}(\mathbb{C})$$

$N \ntriangleleft S_3$

$N \neq \text{conj}(a)$ の union

1 と他を使つて 2 は作れない //

三D-9 定理

位数129群?

Def p : 素数

① P : fin grp or p -群 $\Leftrightarrow |P| = p^n$

② G : fin grp

$\cup$

P : p -群 or p -Sylow 部分群

$$\Leftrightarrow \frac{|G|}{|P|} \in \mathbb{N}$$

def

例 $|G| = p^n \cdot m$ $p \nmid m$ and

$$|P| = p^n \text{ and } 3 = 3$$

$$|S_3| = 6 = 2 \cdot 3$$

Thm p : 素数 G : 有限群

$$\text{Syl}_p(G) \neq \emptyset$$

一般に $\forall n \mid |G|$ について

$$\exists H \subseteq G : \text{部分群} \quad (H \mid = n)$$

($\neq$ 不成立) -

Thm ① $H \subseteq G$: p -部分群

$$\exists P \in \text{Syl}_p(G) \text{ s.t. } H \subseteq P$$

$$(H = \{e\} \text{ と } \text{Syl}_p(G) \neq \emptyset)$$

② $P_1, P_2 \in \text{Syl}_p(G)$ は互いに共役

$$\text{③ } |\text{Syl}_p(G)| \equiv 1 \pmod{p}$$

Ex S_3

$$\{e, g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, g^2\} \quad 3 \equiv 0 -$$

$$\begin{array}{c} | \\ \langle e \rangle \end{array} \quad \begin{array}{c} | \sqsupset \\ | \sqsubset \\ | \sqsubset \\ 1 \pmod 3 \end{array}$$

S_3

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

$$\begin{array}{c} | \\ \langle e \rangle \end{array}$$

$$2 \equiv 0 -$$

$$3 \equiv 1 \pmod 2$$

$$\textcircled{1} \quad |G| = p^n \cdot m \quad n \geq 1 \\ m \notin p\mathbb{Z}$$

$$X := \{ S \subseteq G \mid |S| = p^n \}$$

$$\binom{G}{p^n} \supset \text{ある} = \frac{p^n \cdot m (p^n m - 1) \cdots (p^n m - p^n + 1)}{p^n!}$$

claim $p \mid |X|$

$\textcircled{2}$ 初等整数論

$$\text{作用} \quad G \times X \rightarrow X \\ (g, S) \mapsto gS$$

claim #1) $\exists S' \in X$ s.t.

$$|G \cdot S'| \notin p\mathbb{Q}$$

$$\begin{aligned} \frac{|G|}{|\text{Stab}_G(S')|} &= \frac{|G|}{|P_0|} \notin p\mathbb{Q} \\ \Rightarrow |P_0| &\geq p^n \end{aligned}$$

$$\text{Stab}_G(S') =: P_0 \in \text{Syl}_p(G) \nsubseteq \pi \mathcal{G}.$$

$$P_0 \cdot S' = S' \quad \forall s \in S' : \text{fix}$$

$$P_0 \cdot S' \subseteq S' \quad \#1 \quad |P_0| \leq |S'| = p^n$$

$$\text{f.z. } |P_0| = p^n \quad \therefore \text{Syl}_p(G) \neq \emptyset.$$

$$Y := \{ g p_0 g^{-1} \mid g \in G \}$$

作用 $H \times Y \rightarrow Y$

$$(h, Q) \mapsto h Q h^{-1}$$

$$G \times \text{Syl}_p(G) \rightarrow \text{Syl}_p(G)$$

$$(g, P) \mapsto g P g^{-1}$$

$$Y = G \cdot p_0$$

$$|Y| = \frac{|G|}{|\text{Stab}_G(p_0)|} \quad \Bigg| \quad \frac{|G|}{|P_0|}$$

p_0 は既約元

$$p^0 \equiv |H| \text{ 約数}$$

$$\text{Stab}_G(p_0) \supseteq P_0$$



ゆえに $P \nmid |Y|$ となる $\forall P$ は H の素数

$$\text{よって } p^0 = 1 \text{ となる } p \text{ は素数}$$

それを $\mathbb{Q}$ とする

$$1) a \text{ 可逆ならば } (\Rightarrow) \forall h \in H \quad aQ = Qh$$

$$2) a \text{ 不可逆ならば } HQ = \{ah \mid h \in H, a \in \mathbb{Q}\}$$

は $\mathbb{Q}$ の部分群である。

$$(ah(a'h')^{-1}) \in HQ$$

$$\underbrace{ah(a'h')^{-1}}_{\substack{|| \\ ah}} \in \mathbb{Q}(ah(a'h')^{-1}) \dots$$

$$\text{さらに } HQ \not\subseteq \mathbb{Q}$$

$$\text{今 } H \hookrightarrow HQ \twoheadrightarrow HQ/\mathbb{Q}$$

$$\text{に準同型定理より } H/H \cap \mathbb{Q} \cong HQ/\mathbb{Q}$$

$$\therefore \frac{|H| \cdot |Q|}{p \neq \emptyset} = \frac{|H \cap Q|}{|H \cap Q|}$$

$$\text{So } |H \cap Q| \neq p \neq \emptyset$$

$$Q \subseteq H \cap Q \subseteq G \text{ as } H \cap Q = Q$$

$$H \subseteq Q \quad \text{as } H \subseteq Q \quad \text{as } H \subseteq Q$$

$$\textcircled{2} \text{ Syl}_p(G) \ni H_1 = Q_1 = g_1 p_0 g_1^{-1}$$

$$\text{Syl}_p(G) \ni H_2 = Q_2 = g_2 p_0 g_2^{-1}$$

$$g_2^{-1} H_2 g_2 = g_1^{-1} H_1 g_1 = p_0$$

$$H_2 = g_2 g_1^{-1} H_1 g_1 g_2^{-1}$$

$$(3) \quad |\text{Syl}_p(G)| \equiv 1 \pmod{p}$$

$$Y = \{ g p_0 g^{-1} \mid g \in G \}$$

$$= \text{Syl}_p(G) \quad (2 \neq p)$$

$$H \in \text{Syl}_p(G) : \text{fix}$$

YQH東道 179元 Q

$$\Rightarrow Q = -1$$

12 24

とくに、アフリカの交通の発展が、重要。

(17) (11) 約數 (11 個數)