


第9回 代数系

1/7 群 def, 作用, 20-9 定理

位数の小さい群

$$15 = 3 \times 5$$

1 2 3 4 5 6 7 8 9 10
11 12 13 14 15 16 17 18 19 20

$$5 \not\equiv 1 \pmod{3}$$

準直 直積群

直積集合 $21 = 7 \times 3$

積位相 $\uparrow$

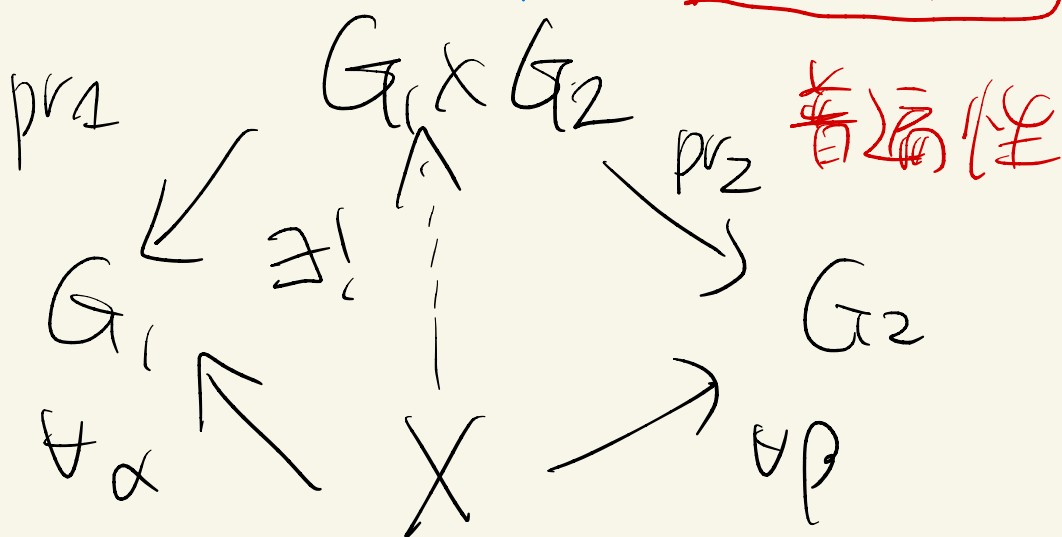
G_1, G_2 群

?

$\hookrightarrow$

右

10Pにすぎ



~~prop~~ G : 群 $\supset G_1, G_2$

直積群
の表現論

$$G_1 \cap G_2 = \{e\}$$

$$G = G_1 G_2 = \{g_1 g_2 \mid \begin{matrix} g_1 \in G_1 \\ g_2 \in G_2 \end{matrix}\}$$

$$\Rightarrow \boxed{G_1 \times G_2} \overset{\varphi}{\simeq} G$$

$$(g_1, g_2) \mapsto g_1 g_2$$

R $I, J = \{ij \mid \begin{matrix} i \in I \\ j \in J \end{matrix}\}$

$I, J \subseteq R$: ideal

外部直積

$$G = \text{int} \quad G_1 \times G_2 \\ \text{pair} \langle \text{int}, \text{int} \rangle$$



φ 是单射

$$\Rightarrow g_1 = g_2^{-1} \in G_1 \cap G_2$$

11
e

φ は 群同型 を 言うには

$$\varphi(g_1 g_1', g_2 g_2') = \varphi(g_1, g_2) \varphi(g_1', g_2')$$

$$g_1 g_1' \quad g_2 g_2' \quad \parallel \quad g_1 g_2 \quad g_1' g_2'$$

5) $g_1 g_2 = g_2 g_1$ を示す

$$g_1 g_2 g_1^{-1} g_2^{-1} = e \text{ である}$$

$$\begin{array}{ccc}
 \underbrace{(g_1' g_2 g_1'^{-1}) g_2^{-1}}_{\substack{\uparrow \\ G_2}} & = & g_1' \underbrace{(g_2 g_1'^{-1} g_2^{-1})}_{\substack{\uparrow \\ G_1}} \\
 \uparrow & & \uparrow \\
 G_2 & & G_1
 \end{array}$$

$$e \in G_1 \cap G_2 = \{e\} //$$

Rk $V \supseteq V_1, V_2$ is sub

$$V_1 \oplus V_2 = V \text{ a def}$$

$$\Leftrightarrow V = V_1 + V_2 \text{ and } V_1 \cap V_2 = \{0\}$$

半直積 (semi-direct product)

Def H, N : 群

$f: H \rightarrow \text{Aut}(N)$: group hom

$\{ \varphi: N \rightarrow N \mid \text{group ^{isom} ~~hom~~ } \}$

合成 $\circ$ 群

$N \rtimes_f H$: 半直積 単位元 (e_N, e_H)

$= N \times H$: 直積集合に積を

$$(n, h)(n', h') = (n \cdot f(h)(n'), hh') \quad \begin{matrix} n, n' \in N \\ h, h' \in H \end{matrix}$$

$f(h) \in \text{Aut}(N)$ γ def (f, γ) の

とすると $N \rtimes_f H$ は群になる

(注) $f: H \rightarrow \text{Aut}(N)$

$$h \mapsto f(h) = \text{id}_N \quad a \notin$$

$$N \rtimes_f H = N \rtimes H$$

prop $G \supseteq N$: 正規 sit. $H \cap N = \{e\}$

$\cup$

H

部分群

$$G = HN (= NH) \text{ 部分群}$$

$$\text{従って } N \rtimes_f H \xrightarrow{\varphi} G$$

$\cong \cong$

$$f: H \rightarrow \text{Aut}(V)$$

$$h \mapsto f(h): V \xrightarrow{\sim} V$$

$$n \mapsto hnh^{-1} \quad \text{内部自己}$$

$\uparrow$

check if f is a group hom

$$f(h_1)f(h_2) = f(h_1h_2) \text{ in } \text{Aut}(V)$$

② φ is an isomorphism (or not)

φ is a group hom & check

$$\varphi(n, h) \varphi(n', h') = \varphi(n f(h) n', h h')$$

$$n h n' h' = n \underline{h n' h^{-1}} h h' = n f(h)(n') h h'$$

Ex $A\vec{x} + \vec{b}$ 形の $\mathbb{R}^n \rightarrow \mathbb{R}^n$: $b \neq 0$
の合成

記法 $n \geq 1$

$\mathbb{Z}/n\mathbb{Z}$ の 加法群 $\cong C_n$

$(\mathbb{Z}/n\mathbb{Z}, +, [0])$

prop $|G| = n \Rightarrow \exists g \in G, \text{ord}_G(g) = n$

$\Rightarrow G \cong C_n$

① $\mathbb{Z} \rightarrow G$ に ~~同型~~ 型 $m \mapsto g^m$ 適用

$\ker = n\mathbb{Z}$. but ord a def by $\leq d \mid 3$

$$\therefore \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} G$$

Ex $|G| = p$: 素数 $\Rightarrow G \cong C_p$

④ $g \in G \setminus \{e\}$ の order は $1 \leq \leq p$

Lemma G : fin group $\supseteq A, B$: sub group

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}$$

Pr 以下の正規部分群 N のとき

$$H \subset HN \twoheadrightarrow HN/N$$

$$\Rightarrow H/H \cap N \twoheadrightarrow HN/N$$

$$\text{Def } V_1 \hookrightarrow V_1 + V_2 \rightarrow \frac{V_1 + V_2}{V_2}$$

$$\therefore \frac{V_1}{V_1 \cap V_2} \xrightarrow{\sim} \frac{V_1 + V_2}{V_2}$$

$$\textcircled{1} A \times B \curvearrowright G$$

$$((a, b), g) \mapsto agb^{-1}$$

$$AB = e \text{ a orbit}$$

$$\therefore |AB| = \frac{|A \times B|}{|\text{Stab}_{A \times B}(e)|}$$

$$\text{Stab}_{A \times B}(e) = \{(a, b) \in A \times B \mid aeb^t = e\}$$

$$\Downarrow$$

$$a=b$$

$$\therefore \text{Stab}_{A \times B}(e) = \{(x, x) \mid x \in A \cap B\}$$

~~proof~~ p : 素数

$$|G| = p^2 \Rightarrow G \cong C_{p^2} \text{ or } C_p \times C_p$$

実は G : 可換群 だった (後)

(c) $\nexists g \in G, \text{ord}_G(g) = p^2$ と仮定

$$\exists a \in G \quad \text{ord}_G(a) = p$$

$$\exists b \in G \setminus \langle a \rangle$$

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \cong C_p$$

同様(2)

$$\langle b \rangle \cong C_p$$

5. G : 可換 $\mathbb{F}_p$ 上の 2 次元ベクトル空間

$$G \supset \langle a \rangle = G_1$$

$$G \supset G_1 \times G_2$$

$$\langle b \rangle = G_1$$



$$G_1 \cap G_2 = \{e\} \quad \text{よって} \quad G_1 G_2 = G$$

$$(\because) \quad G_1 \cap G_2 \subseteq G_1, G_2 \quad \text{位数} \neq |G|$$

Lemma $|G| = p^2 \Rightarrow G$ is abelian

(1) $G \neq Z(G)$ する

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

類群

$$|G| = |Z(G)| + \sum_{\text{共役類 } C_i} |C_i|$$

$$\text{s.t. } |C_i| > 1$$

$$|C_i| = \frac{|G|}{|C_G(g_i)|}$$

$$C_i = \text{conj}_G(g_i) = \{ h g_i h^{-1} \mid h \in G \}$$

よ) $|C_i|$ is prime divisor

$$\therefore |Z(G)| \nmid p \neq 1$$

$$\therefore |Z(G)| = p$$

$$\text{よ} \quad Z(G) = \{a^0, a^1, \dots, a^{p-1}\}$$

同様に $b \in G \setminus Z(G)$ をとる.

$$\text{ord}_G(b) = p \text{ となる.}$$

$$H = \langle b \rangle \text{ とする}$$

$$Z(G) \cap H = \{e\} \text{ となる}$$

$$G = Z(G)H \text{ となる.}$$

Ex 2

$$G = \{ a^i b^j \mid 0 \leq i, j < p \}$$

$$a^i b^j a^k b^l$$

$$= a^i a^k b^j b^l$$

$$= a^k a^i b^l b^j$$

$$= a^k b^l a^i b^j$$

Ex 2 $\chi(G) = G$ (2 $\overline{\chi}$ 有)

位数 pq の場合 ($p > q$: 素数)

Lemma $|G| = pq$ $p > q$

$$|\text{Syl}_p(G)| = 1$$

① $k_p = |\text{Syl}_p(G)| \nmid q$

$$k_p \equiv 1 \pmod{p}$$

$$k_p \mid |G| \Leftarrow \text{①} \text{ となる } p\text{-Sylow 群}$$

1, q , p , pq

$$\therefore k_p = 1$$

$$G \cong \text{Syl}_p(G) \ltimes \text{Syl}_q(G)$$
$$(g, p) \mapsto (gPg^{-1})$$
$$|\text{Syl}_p(G)| = |G| / |\text{Syl}_q(G)|$$

Ex 5.1: $p \not\equiv 1 \pmod{q} \nmid \exists \mathbb{Z}$

$$G \simeq C_{pq} \simeq C_p \times C_q$$

⊖ $p_q = |Syl_q(G)| \equiv 1 \pmod{q}$

$p_q = 1$ ~~$p < q$~~ ~~$p \nmid q$~~ $\mathbb{Q}/p\mathbb{Q} \simeq \mathbb{Q}/p\mathbb{Q} \times \mathbb{Q}/q\mathbb{Q}$

Ex 2 $Syl_p(G) = \{P\}$

$Syl_q(G) = \{Q\}$

φ
 $\mathbb{Z}/p\mathbb{Z}$

$G \supseteq P$
 $\leq Q$

$P \cap Q = \{e\}$

$PQ = G$

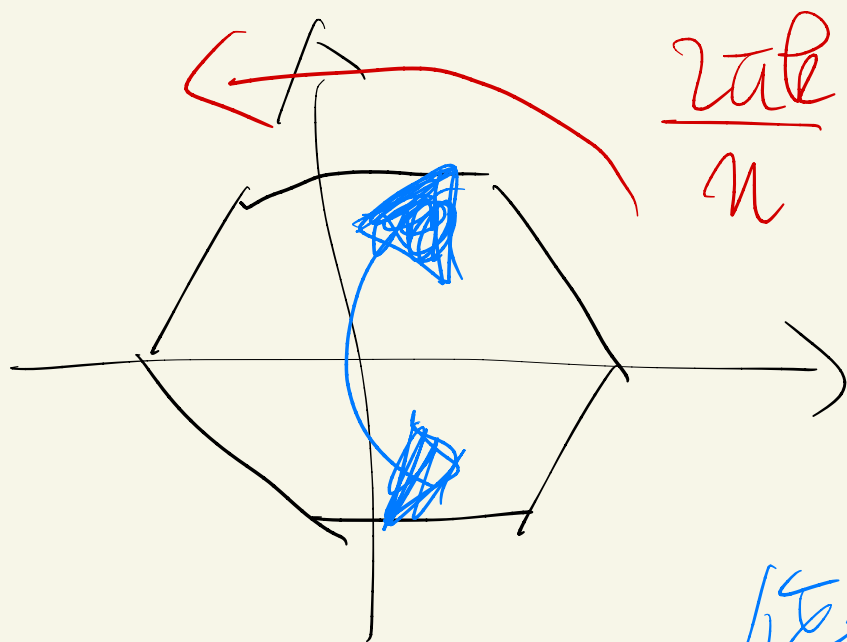
$\therefore G \simeq P \times Q$

Def 2面体群

$$D_n = \left\{ \begin{pmatrix} \cos k\theta_n & -\sin k\theta_n \\ \sin k\theta_n & \cos k\theta_n \end{pmatrix}, \dots \right\}$$

R_k

S_k



$\frac{2\pi k}{n}$ 回転

位数 $2n$ 群

$n=6$

$$D_n \supseteq C_n \supseteq \{e\}$$

prop $p \geq 3$: ~~奇数~~ ^{素数}

$$|G| = 2p$$

$$\Rightarrow G \cong C_{2p} \text{ or } D_p$$

~~定理~~ を使う

$$\textcircled{!} \text{ Syl}_p(G) = \{p\}$$

$$C \in \text{Syl}_2(G)$$

$$C \cap P = \{e\}, \quad PC = G$$

$$\therefore G \cong P \rtimes_f C$$

$$\{e, g\}$$

where $f: C \rightarrow \text{Aut}(P)$

$$P = \{e, h, \dots, h^{p-1}\}$$

$$f(e) = f(g) = \text{id}_P \text{ and } \neq$$

$$G \simeq C \rtimes P \cong C_2 \rtimes C_p \leq C_{2p}$$

$$\underline{f(g) \neq \text{id}_P \text{ and } \neq}$$

$$f(g)(h) = h^{-1} \text{ and } \neq \text{ and } \neq$$

$$\rightarrow G \simeq D_p \text{ and } \neq \text{ and } \neq$$

$p \xrightarrow{\varphi} p : \text{group hom}$

h の 1 行 1 列 要素

$$\left(\varphi(h^a) = \varphi(h)^a \right)$$

$$f(g) f(g) = \text{id}_p$$

$$\text{これより } f(g)(h) = h^{\pm 1}$$

2 通りしか 高々 あり得る //

一般の pg の場合も少し
かんがえる必要がある

有限 Abel 群⁴ $G \rightarrow$ 後に示す

$$\exists! d_1 \mid \exists! d_2 \mid \cdots \mid \exists! d_s$$

$2 \leq$

$$\text{s.t. } G \cong C_{d_1} \times \cdots \times C_{d_s}$$

Ex $|G|=8$, 可換

$$(8) \quad (2,4) \quad (2,2,2)$$

$$\updownarrow$$

$$\updownarrow$$

$$\updownarrow$$

$$C_8$$

$$C_2 \times C_4$$

$$C_2 \times C_2 \times C_2$$

$$6 \hookrightarrow (6) \quad \cancel{(2,3)}$$

位数 29 の有限群 は $\mathbb{Z}/29\mathbb{Z}$ である

位数 2000 以下の群のうち

位数 1024 の群 は 99.9% である

応用 $p \geq 2$: 素数 (原始根)

$$(\mathbb{Z}/p\mathbb{Z})^\times \simeq C_{p-1}$$

① S

$$C_{d_1} \times \cdots \times C_{d_s}$$

$s \geq 1$ とおき $\chi^{d_i} = 1$ かつ $d_i \nmid d_j$ である

これは $(\mathbb{Q}/p\mathbb{Q})[x]$ の $\mathbb{Q}$ 上

$x^{d_i} - 1$ の解は $d_i \leq$ 以下に与えらる

RK $\mathbb{Q}/6\mathbb{Q}$ 上 $(x-1)(x-2) = 0$
 $x^2 - 3x + 2$

$\neq x = 1, 2, 4, 5$

Cor ウィルソンの定理

$p \geq 2$ は素数 $(p-1)! \equiv -1 \pmod{p}$

$$\textcircled{1} (\mathbb{Z}/p\mathbb{Z})^\times = \{g^0, g^1, \dots, g^{p-1}\}$$

$$\exists g$$

$$\text{Ex } (\mathbb{Z}/5\mathbb{Z})^\times = \{2^0, 2^1, 2^2, 2^3\} \cong C_4$$

$\parallel$
1

$\parallel$
2

$\parallel$
4

$\parallel$
3

$$(p-1)! \equiv g^0 \times \dots \times g^{p-1} \pmod{p}$$

$$= g^{\frac{p(p-1)}{2}} = (g^p)^{\frac{p-1}{2}}$$

$$x^{2-1} = g^{\frac{p-1}{2}}$$

$$\left(g^{\frac{p-1}{2}}\right)^2 = g^{p-1} = 1 \quad \therefore g^{\frac{p-1}{2}} = \pm 1$$

一般化 $n \geq 2$

$$\prod_{1 \leq m < n} m \equiv \pm 1 \pmod{n}$$

$$(m, n) = 1$$

$$-1 \Leftrightarrow n = p^e, 2 \cdot p^e, 2 \cdot 4$$

p : 素数

有限体の性質 (可換環)

対称群

Def $S_n = \text{Sym}(\{1, \dots, n\})$

Thm $\forall G$: 有限群は $S_{|G|}$ の
部分群と同型

記法 $(\bar{v}_i)$ 区間

$\begin{matrix} & \bar{v}_1 & \searrow & & \\ \nearrow & & & \bar{v}_2 & \\ \bar{v}_k & & & & \end{matrix} \quad (\bar{v}_1, \dots, \bar{v}_k)$
 $\begin{matrix} & & & & \\ & & & \bar{v}_j & \swarrow \end{matrix}$
区間区間区間

Ex

next-permutation

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

" " "
id (2,3) (1,2) = s_i

$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

" " "
(1,2,3) (1,3,2) (1,3)

" "
(1,2) (2,3) (2,3)(1,2)

Ex $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id} = s_i^2$

Rk $\det A = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}$

Def $A_n = \ker(\text{sgn} : S_n \rightarrow \{\pm 1\})$
偶置換

$$|A_n| = \frac{n!}{2}$$

記法 cycle type (g)

$$g = \begin{pmatrix} \textcircled{1} \textcircled{2} \textcircled{3} \textcircled{4} \textcircled{5} & 6 & \textcircled{7} \textcircled{8} \\ \textcircled{3} \textcircled{4} \textcircled{5} \textcircled{2} \textcircled{1} & 6 & \textcircled{8} \textcircled{7} \end{pmatrix} \in S_8$$

$(135)(24)(6)(78)$: 2個 2置換
9置換

$$\text{cycle type}(g) = (3, 2, 2, 1)$$

8の分割 $(3^1, 2^2, 1^1)$

~~prop~~ $g, g' \in S_n$ 同値

$$\Leftrightarrow \text{cycdetype}(g) = \text{cycdetype}(g')$$

~~prop~~ cycle type 同値

$(1^{m_1} 2^{m_2} \dots n^{m_n})$ の S_n の

元の数

$$n!$$

$$1^{m_1} m_1! 2^{m_2} m_2! \dots n^{m_n} m_n!$$

コある

Ex S_5

$120 \supset A_5 \supseteq A_5$

cycle type

位数 60

共役類の数

$$(5) = (5')$$

$$\frac{120}{5!} = 24$$

24通り

A_5 共役類

$$(41) = (4'1')$$

$$\frac{120}{4!1!} = 30$$

2つは2つに
わかれる

$$(32) = (3'2')$$

$$\frac{120}{3!2!} = 20$$

$$(311) = (3'1^2)$$

$$\frac{120}{3!1^2 \cdot 2!} = 20$$

$$(221) = (2^2, 1')$$

$$\frac{120}{2^2 \cdot 2! \cdot 1!} = 15$$

$$(2111) = (2', 1^3)$$

$$\frac{120}{2! \cdot 3!} = 10$$

$$(11111) = (1^5)$$

$$\frac{120}{5!} = 1$$

$\begin{pmatrix} 12345 \\ 12345 \end{pmatrix}$

A59 共役数は 5 個あり、

$120, 120, 200, 150, 100$

と対応する

$\text{vector}(\text{vector}(\text{cnt}))$

$\text{mt} \text{ trans_num}(\text{const vector}(\text{cnt}) \&v)$

for i

for $j > i$

$v(i) > v(j) \propto$ ~~数~~

⑤ A_5 に自明 2 ' 因子
正規部分群はない

iel. $A_5 \triangleleft N \Rightarrow N = A_5$, fey

⑥ 題等式

$$\begin{array}{ccc} 60 = 1 + 15 + 12 + 12 + 20 \\ \uparrow \quad \uparrow & & \\ |A_5| & |Z(A_5)| & 4 + \binom{4}{2} + \binom{4}{3} + \binom{4}{4} \end{array}$$

18, 20, 12, 12, 20 の約数は
60 以外でないので //

Def G : 有限群が単純

$$\Leftrightarrow G \neq \{e\}$$

def

$$G \triangleright N \Rightarrow N = \{e\}, G$$

Cor A_5 は単純

Pk $G \not\triangleright N \neq \{e\}$

$G \nmid N$ と G/N が正則群

Fact $n \geq 5$ A_n は単純

Pk $p \geq 2$: 素数 C_p は単純

位数 2000 数 $\sim$ 500 億

☆ 1-型 有限単純群

~~" $GL_n(F)$ "~~

(2)

☆ 26 例 例外型

位数が 一番 大きい $=$ エニスター

☆ A_n $n \geq 5$

M

N

☆ C_p $p \geq 2$: 素数

$GL_n(\mathbb{C})$

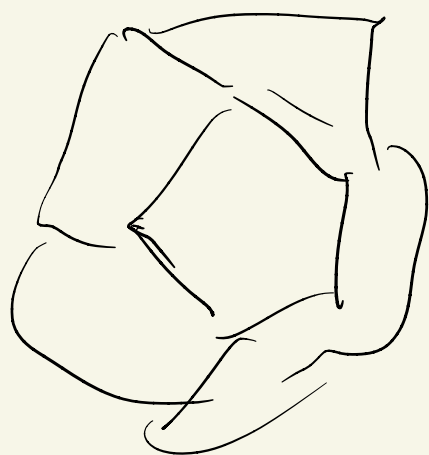
Feit-Thompson

$$1TB = 10^6$$

群 公理

3) 結集

$A_5 = \text{正20面体を保つ}$



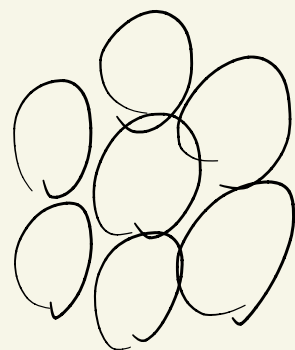
$G = \text{"Aut}(X) \text{" と 理解 (f.c.h.)}$

表現論

11-4 格子

$\rightarrow R$ 加群

8-2
24次元



$M = \text{Aut}(\text{場の理論})$

ラマヌジャン $\rightarrow$ 頂点作用素