

UEC 代数勉強会 第 7 回

9trap/ 隕石

2021/06/30

目次

1 復習	1
1.1 はじめに	1
1.2 代数系	1
1.3 準同型写像	2
1.4 置換表現	3
1.5 剰余類	3
1.6 作用	4
2 対称式と交代式	4
2.1 多項式への作用	4
2.2 対称式と交代式	5
2.3 Hilbert の基底定理	8
3 正規部分群と商群	8
3.1 正規部分群と商群	8
3.2 第一同型定理 (準同型定理)	12
3.3 第二同型定理	13
3.4 指標	13
4 射影幾何について	13

1 復習

1.1 はじめに

だいぶ間が空いたので復習を入れておきます。

金子晃「応用代数講義」ISBN4-7819-1117-X を使います。

1.2 代数系

集合に演算を導入し、特定の条件を満たすようなモデルを考えると、さまざまな構造を扱えてうれしい。そう

いったモデルを代数系という。

定義 1 (群) 集合 G と G における 2 項演算

$$\circ : G \times G \rightarrow G; (a, b) \mapsto a \circ b$$

が次の条件を満たすとき、組 (G, \circ) を群という。

$$(1) \forall a, b, c \in G (a \circ b) \circ c = a \circ (b \circ c) \quad (\text{結合律})$$

$$(2) \exists e \in G [\forall a \in G [e \circ a = a \circ e = a]] \quad (\text{単位元の存在})$$

$$(3) \forall g \in G [\exists h \in G [g \circ h = h \circ g = e]] \quad (\text{逆元の存在})$$

誤解を生まないと判断された多くの場合、 G そのものを群と呼ぶ。

群 G が可換律 $\forall a, b \in G [a \circ b = b \circ a]$ を満たす場合、 G を可換群もしくは Abel 群と呼ぶ。

演算子は、可換群であれば $+$ を使ったり、そうでない場合は省略する事が多い。

定義 2 (環) 集合 A と A における積と和と呼ばれる 2 つの 2 項演算

$$\cdot : A \times A \rightarrow A; (a, b) \mapsto a \cdot b$$

$$+ : A \times A \rightarrow A; (a, b) \mapsto a + b$$

が次の条件を満たすとき、組 $(A, +, \cdot)$ を環という。

$$(1) (A, +) \text{ は可換群を成す}$$

$$(2) \forall a, b, c \in A [(ab)c = a(bc)] \quad (\text{乗法の結合律})$$

$$(3) \forall a, b, c \in A [a(b+c) = ab+ac] \quad (\text{分配律})$$

誤解を生まないと判断された多くの場合、 A そのものを環と呼ぶ。

定義 3 (体) 集合 K と K における積と和と呼ばれる 2 つの 2 項演算

$$\cdot : K \times K \rightarrow K; (x, y) \mapsto x \cdot y$$

$$+ : K \times K \rightarrow K; (x, y) \mapsto x + y$$

が次の条件を満たすとき、組 $(K, +, \cdot)$ を環という。

$$(1) (K, +) \text{ は可換群を成す}$$

$$(2) (K \setminus \{0\}, \cdot) \text{ は可換群を成す}$$

$$(3) \forall a, b, c \in A [a(b+c) = ab+ac] \quad (\text{分配律})$$

誤解を生まないと判断された多くの場合、 K そのものを体と呼ぶ。

代数系は他にも色々ある。例えば亜群 (マグマ)、半群、モノイド、Kleene 代数など。

1.3 準同型写像

定義 4 (準同型写像) 群 G, H とその間の写像 $\varphi : G \rightarrow H$ が以下を満たすとき、写像 φ を準同型であるとい

う。

$$\forall x, y \in G [\varphi(x)\varphi(y) = \varphi(xy)]$$

定義 5 (同型写像) 準同型写像 $\varphi : G \rightarrow H$ が全単射であるとき、同型写像であるといい、このように群 G と群 H のあいだに同型が存在するとき $G \cong H$ とかき、単に G と H は同型であるという。

命題 6 同型写像 φ の逆射も同型写像 (準同型写像) である。

証明 雑な証明を示す。

$$\begin{aligned}\varphi(\varphi^{-1}(xy)) &= xy \\ \varphi(\varphi^{-1}(xy)) &= \varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y)) \\ \varphi^{-1}(xy) &= \varphi^{-1}(x)\varphi^{-1}(y)\end{aligned}$$

□

1.4 置換表現

命題 7 (群の積の単射性) 有限群 G の演算について、片方の引数を $g \in G$ に固定した写像 $\varphi : G \rightarrow G; a \mapsto ga$ は単射である。

証明 任意の $a, b \in G$ について、

$$a = b \Leftrightarrow g^{-1}a = g^{-1}b$$

□

つまり、この写像は群の要素の置換とみなすことができる。各元に番号をつける写像を f とすると、 $f \circ \varphi \circ f^{-1}$ は S_n の元である。

定義 8 (左移動による置換表現) この写像 φ を左移動といい、 $f \circ \varphi \circ f^{-1}$ は左移動による置換表現という。

1.5 剰余類

記法 9 (左移動の像) 群 G の部分集合 A について、 g による左移動の A の像を gA とかく。すなわち、

$$gA := \{ga \mid a \in A\}$$

命題 10 群 G の有限部分集合 A について、 $|A| = |gA|$

証明 命題 7 より。

□

補題 11 (部分群の左移動) 群 G の部分群 H について、 $g \in H$ ならば $gH = H$ 、 $g \notin H$ ならば $gH \cap H = \emptyset$

証明 前者は群の演算が閉じていることから自明。

$g \notin H$ の場合、 $gH \cap H \neq \emptyset$ とすると、 $\exists x[x \in gH \wedge x \in H]$ 。

その x について、 $x \in gH$ だから $\exists y[x = gy \wedge y \in H]$ 。

その y について、 $xy^{-1} = g$ 。 $x \in H, y \in H$ より $g \in H$ が導かれるがこれは仮定に矛盾する。よって、帰謬法から $gH \cap H = \emptyset$ 。 \square

命題 12 群 G とその部分群 H について、 $a \sim b \Leftrightarrow aH = bH$ として関係を定義すると、この関係 \sim は同値関係となる。

証明 自明に $aH = aH \wedge (aH = bH \Leftrightarrow bH = aH)$ であるから、反射律と対称律が成り立つ。

$aH = bH \wedge bH = cH$ と仮定すると、 $=$ の推移律から $aH = cH$ 。よって、推移律も満たす。 \square

系 13 上で定めた関係は同値関係であるから、同値類 gH により、群 G が分割される。

定義 14 (左剰余類) ここでの同値類 gH を左剰余類という。

定理 15 (Lagrange の定理) 部分群の位数は元の群の位数の約数である。

証明 命題 10 から、部分群から導かれる左剰余類はすべて要素数が同じである。よって、分轄数 $[G : H]$ について、 $|G| = [G : H] \cdot |H|$ 。 \square

1.6 作用

定義 16 (作用) 群 G から集合 X について、演算 $\bullet : G \times X \rightarrow X$ が以下を満たすとき、これを作用という。

- (1) $\forall x \in X [e \bullet x = x]$
- (2) $\forall g, h \in G [\forall x \in X [(hg) \bullet x = h \bullet (g \bullet x)]]$

2 対称式と交代式

2.1 多項式への作用

命題 17 (置換群の多項式への作用) 置換群から n 変数多項式環 / 有理関数体の変換への対応

$$\sigma \in S_n \mapsto (\sigma f)(x_1, x_2, \dots, x_n)$$

を以下のように定める

$$(\sigma f)(x_1, x_2, \dots, x_n) := f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

このとき、この対応は作用である。

証明 置換群の単位元は恒等射であるから、条件 (1) がみたされる。

また、 \square

$$\begin{aligned}
(\sigma(\tau f))(x_1, x_2, \dots, x_n) &= (\tau f)(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) \\
&= f(x_{\tau(\sigma(1))}, x_{\tau(\sigma(2))}, \dots, x_{\tau(\sigma(n))}) \\
&= f(x_{(\sigma\tau)(1)}, x_{(\sigma\tau)(2)}, \dots, x_{(\sigma\tau)(n)}) \\
&= (\sigma\tau)f(x_1, x_2, \dots, x_n)
\end{aligned}$$

2.2 対称式と交代式

多項式のうち変数置換で不変であるものを対称式といい、符号が変わるものを交代式という。

交代式の符号は置換の符号と一致することを導けるが、ここでは示さない。

$$(\sigma f)(x_1, x_2, \dots, x_n) = (\operatorname{sgn} \sigma) f(x_1, x_2, \dots, x_n)$$

例 18 (基本対称式) 対称式の代表的な例に、以下のような基本対称式がある。

$$s_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}$$

いま、 x_k と x_l を入れ替えたとする。すなわち、 (k, l) を作用させたとする。ただし、 $(k, l) = (l, k)$ であるから、 $k < l$ とする。 $l < k$ の場合はメタ的に k と l を入れ替えた文言を用意すればいい。 $k = l$ ならば、恒等置換であるので s_k が不変であるのは言うまでもない。

s_k は、全ての長さ k の狭義単調増加自然数列 $i : (1, \dots, k) \rightarrow (1, \dots, n); a \mapsto i(a)$ についての項 $x_{i(1)} x_{i(2)} \dots x_{i(k)}$ の和である。

x_k と x_l 両方が含まれる項と両方とも含まれない項は k, l の置換によって不変である。任意の x_k が含まれていて x_l が含まれていない項 t について、 tx_l/x_k は項であり s_k に含まれる。これらの和は x_k と x_l の置換で不変であり、任意の x_l が含まれていて x_k が含まれていない項はこれらで尽くされるため s_k は互換で不変。

任意の置換は互換の積で表せるから s_k は任意の置換で不変である。

例 19 (差積) 交代式の代表的な例に、差積がある。

$$\Delta(x_1, x_2, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

x_k, x_l を入れ替えることを考える。差積が $(x_p - x_k)$ で割り切れるとする。このとき、 $(x_p - x_l)$ でも割り切れる。 $(x_p - x_k)(x_p - x_l)$ は k, l の置換で不変である。

差積が $(x_k - x_p)$ で割り切れるとする。 $p < l$ のとき、差積は $(x_p - x_l)$ で割り切れる。それらの積 $(x_k - x_p)(x_p - x_l)$ は k, l の置換で不変。 $p > l$ のとき、差積は $(x_l - x_p)$ で割り切れる。それらの積 $(x_k - x_p)(x_l - x_p)$ は k, l の置換で不変。

以上より、 $(x_k - x_l)$ 以外の積は k, l の置換で不変であるが、 $(x_k - x_l)$ だけは符号が変わってしまう。よって、差積は交代式。

定義 20 (単項式の型) n 変数の単項式の型とは、 x_i の次数による n つ組 \mathbf{a} のことをいう。

$$x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} \text{ の型は } \mathbf{a} = (a_1, a_2, \dots, a_n)$$

定義 21 (単項式の順序) 型 \mathbf{a}, \mathbf{b} の半順序 $>$ を辞書式順序とする。すなわち、 $a_i \neq b_i$ である最小の i について、 $a_i > b_i$ であるとき、またそのときのみ $\mathbf{a} > \mathbf{b}$ とする。

また、順序 \geq を $\forall \mathbf{a}, \mathbf{b} [\mathbf{a} \geq \mathbf{b} \Leftrightarrow (\mathbf{a} > \mathbf{b} \vee \mathbf{a} = \mathbf{b})]$ で定める。

順序 \geq は自然数の順序によるから全順序である。 n 次の単項式全体の集合は有限であるから、この順序において単項式の集合の最大元が存在する。

命題 22 (基本対称式の積による単項式) 基本対称式の積 $s_1^{d_1} s_2^{d_2} \cdots s_n^{d_n}$ の単項式のうち上で定めた順序で最大の項は $\sum_{k=1}^n d_k \sum_{k=2}^n d_k \cdots x^{d_n}$ である。

証明 辞書式順序では小さい添字の次数のほうが優先されるから、 $s_1^{d_1} s_2^{d_2} \cdots s_n^{d_n}$ のうち、 x_1 の次数が一番高いものが候補である。

例 18 の定義からどの s_k の単項式も x_l の次数はたかだか 1 である。よって、すべての s_k について x_1 を含む項の積によってなる単項式の字数である $d_1 + d_2 + \cdots + d_n$ が x_1 の次数の最大である。 s_k の各項の次数は k であるから x_1 を含む項は $n - 1$ 個のうちから $k - 1$ 個を選ぶ組み合わせの数と同じであって、 x_1 がこの次数である項はいくつかあることがある。 s_1 の各項の次数は 1 であって x_1 を含むと x_2 を含むことができないから、これらの単項式のうち x_2 の次数が最大であるものは $d_2 + \cdots + d_n$ である。続きは帰納的に示される。

□

定理 23 (対称式の表現) すべての対称式は基本対称式の多項式で表される。

証明 命題 22 から、順に基本対称式の積で表せる最大の単項式を引いていくと 0 になる。

具体的には、対称式 f の最大次数 l の最大の単項式の型 $\mathbf{a} = (a_1, a_2, \dots, a_l)$ とすると、 $s_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_n^{a_n}$ の最大の項の型は \mathbf{a} だから、 $f - s_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_n^{a_n}$ の最大の項の型 \mathbf{b} について、 $\mathbf{a} > \mathbf{b}$ 。帰納的に項の数が減っていく (もとの項の数を p とすると j ステップ目の項の数は $p - j$ であることを帰納的に示すことができる)。よって、定理を示すことができる。

問 1 $x_1^4 + \cdots + x_n^4$ を基本対称式の多項式で表せ (参考書問 3.9)。

x_1^4 を最大の単項式として含む基本対称式による単項式は s_1^4 。

$$\begin{aligned} s_1^4 &= \left(\sum_{i=1}^n x_i \right)^4 \\ &= \sum_{i=1}^n x_i^4 + \sum_{1 \leq i_1 < i_2 \leq n} (4x_{i_1}^3 x_{i_2} + 6x_{i_1}^2 x_{i_2}^2 + 4x_{i_1} x_{i_2}^3) + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} (12x_{i_1}^2 x_{i_2} x_{i_3} + 12x_{i_1} x_{i_2}^2 x_{i_3} + 12x_{i_1}^2 x_{i_2} x_{i_3}^2) \\ &\quad + \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq n} 24x_{i_1} x_{i_2} x_{i_3} x_{i_4} \end{aligned}$$

より、

$$\begin{aligned} \sum_{i=1}^n x_i^4 - s_1^4 &= - \sum_{1 \leq i_1 < i_2 \leq n} (4x_{i_1}^3 x_{i_2} + 6x_{i_1}^2 x_{i_2}^2 + 4x_{i_1} x_{i_2}^3) - \sum_{1 \leq i_1 < i_2 < i_3 \leq n} (12x_{i_1}^2 x_{i_2} x_{i_3} + 12x_{i_1} x_{i_2}^2 x_{i_3} + 12x_{i_1} x_{i_2} x_{i_3}^2) \\ &\quad - \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq n} 24x_{i_1} x_{i_2} x_{i_3} x_{i_4} \end{aligned}$$

次に最大の単項は $-4x_1^3 x_2$ であるから、 $-4s_1^2 s_2$ を引けば良い。

$$\begin{aligned} s_1^2 s_2 &= \left(\sum_{i=1}^n x_i \right)^2 \left(\sum_{1 \leq i_1 < i_2 \leq n} x_{i_1} x_{i_2} \right) \\ &= \left(\sum_{i=1}^n x_i^2 + \sum_{1 \leq i_1 < i_2 \leq n} 2x_{i_1} x_{i_2} \right) \left(\sum_{1 \leq i_1 < i_2 \leq n} x_{i_1} x_{i_2} \right) \\ &= \sum_{1 \leq i_1 < i_2 \leq n} (x_{i_1}^3 x_{i_2} + 2x_{i_1}^2 x_{i_2}^2 + x_{i_1} x_{i_2}^3) + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} (5x_{i_1}^2 x_{i_2} x_{i_3} + 5x_{i_1} x_{i_2}^2 x_{i_3} + 5x_{i_1} x_{i_2} x_{i_3}^2) \\ &\quad + \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq n} 12x_{i_1} x_{i_2} x_{i_3} x_{i_4} \end{aligned}$$

より

$$\begin{aligned} \left(\sum_{i=1}^n x_i^4 \right) - s_1^4 + 4s_1^2 s_2 &= \sum_{1 \leq i_1 < i_2 \leq n} 2x_{i_1}^2 x_{i_2}^2 + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} (8x_{i_1}^2 x_{i_2} x_{i_3} + 8x_{i_1} x_{i_2}^2 x_{i_3} + 8x_{i_1} x_{i_2} x_{i_3}^2) \\ &\quad + \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq n} 24x_{i_1} x_{i_2} x_{i_3} x_{i_4} \end{aligned}$$

次に最大の単項は $2x_1^2 x_2^2$ であるから、 $2s_2^2$ を引けば良い。

$$\begin{aligned} s_2^2 &= \left(\sum_{1 \leq i_1 < i_2 \leq n} x_{i_1} x_{i_2} \right)^2 \\ &= \sum_{1 \leq i_1 < i_2 \leq n} x_{i_1}^2 x_{i_2}^2 + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} (2x_{i_1}^2 x_{i_2} x_{i_3} + 2x_{i_1} x_{i_2}^2 x_{i_3} + 2x_{i_1} x_{i_2} x_{i_3}^2) + \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq n} 6x_{i_1} x_{i_2} x_{i_3} x_{i_4} \end{aligned}$$

より、

$$\begin{aligned} \left(\sum_{i=1}^n x_i^4 \right) - s_1^4 + 4s_1^2 s_2 - 2s_2^2 &= \sum_{1 \leq i_1 < i_2 < i_3 \leq n} (4x_{i_1}^2 x_{i_2} x_{i_3} + 4x_{i_1} x_{i_2}^2 x_{i_3} + 4x_{i_1} x_{i_2} x_{i_3}^2) \\ &\quad + \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq n} 12x_{i_1} x_{i_2} x_{i_3} x_{i_4} \end{aligned}$$

次に最大の単項は $4x_1^2 x_2 x_3$ であるから、 $4s_1 s_3$ を引けば良い。

$$\begin{aligned}
s_1 s_3 &= \left(\sum_i^n x_i \right) \left(\sum_{1 \leq i_1 < i_2 < i_3 \leq n} x_{i_1} x_{i_2} x_{i_3} \right) \\
&= \sum_{1 \leq i_1 < i_2 < i_3 \leq n} \left(x_{i_1}^2 x_{i_2} x_{i_3} + x_{i_1} x_{i_2}^2 x_{i_3} + x_{i_1} x_{i_2} x_{i_3}^2 \right) + \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq n} 4x_{i_1} x_{i_2} x_{i_3} x_{i_4}
\end{aligned}$$

より、

$$\begin{aligned}
\left(\sum_{i=1}^n x_i^4 \right) - s_1^4 + 4s_1^2 s_2 - 2s_2^2 - 4s_1 s_3 &= - \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq n} 4x_{i_1} x_{i_2} x_{i_3} x_{i_4} \\
&= -4s_4
\end{aligned}$$

よって、 $\sum_{i=1}^n x_i^4 = s_1^4 - 4s_1^2 s_2 + 2s_2^2 + 4s_1 s_3 - 4s_4$ 。

例 24 (Vandermonde の行列式) 等比級数になっているベクトルを並べた行列の行列式

$$V_n = \left| \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{pmatrix} \right| = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

は差積で見たように交代式である。

例 25 (判別式) $\alpha_1, \dots, \alpha_n$ を根にもつ多項式 $f = (x - \alpha) \cdots (x - \alpha_n)$ の判別式 D を

$$D = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = \Delta(\alpha_1, \dots, \alpha_n)$$

で定義する。

判別式が 0 になるとき、またそのときのみ $\exists i, j [\alpha_i = \alpha_j]$ 、すなわち重根をもつことは自明である。

判別式が負であるとき、 $\exists i, j [(\alpha_i - \alpha_j)] \in \mathbb{C}$ であるから、複素数解をもつ。

2.3 Hilbert の基底定理

ここがわかりやすい。

3 正規部分群と商群

3.1 正規部分群と商群

定義 26 (共役) 群 G の元 g と部分群 H について、

$$g^{-1}Hg := \{g^{-1}hg \mid h \in H\}$$

を H の x による共役という。

記法 27 群 G の部分集合 H, K について

$$HK := \{hk \mid h \in H \wedge k \in K\}$$

命題 28 群 G と部分群 H について、 H の任意の共役が H に等しい、すなわち $\forall g \in G [g^{-1}Hg = H]$ であるとき、

$$\forall g_1, g_2 \in G \left[\forall a_1 \in g_1 H \forall a_2 \in g_2 H \left[(a_1 a_2) H = (g_1 g_2) H \right] \right]$$

証明 $\exists h_1 \in H [a_1 = g_1 h_1]$ 、 a_2 も同様であるから、

□

$$\begin{aligned} (a_1 a_2) H &= (g_1 h_1 g_2 h_2) H \\ &= (g_1 h_1 g_2) H && H \text{ は群であるから、 } h_2 H = H \\ &= (g_1 h_1 g_2 g_2^{-1} h_2 g_2) H && g_2^{-1} H g_2 = H \text{ より } g_2^{-1} h_2 g_2 H = H \\ &= (g_1 h_1 h_2 g_2) H \\ &= (g_1 h_1 h_2 g_2 g_2^{-1}) H g_2 && g_2^{-1} H g_2 = H \\ &= (g_1 h_1 h_2) H g_2 \\ &= (g_1) H g_2 \\ &= (g_1 g_2) H && g_2^{-1} H g_2 = H \end{aligned}$$

群 G の元 g_1, g_2 と部分群 H について、以下のような剰余群の 2 項演算が定まる。

$$g_1 H g_2 H := (g_1 g_2) H$$

命題 28 から代表元に関してこの積は一意であるから、剰余類同士の演算として定められる。

命題 29 群 G とその部分群 H について、以下の命題はすべて互いに同値である。

$$(1) \forall g \in G [g^{-1}Hg \subset H]$$

$$(2) \forall g \in G [g^{-1}Hg \supset H]$$

$$(3) \forall g \in G [g^{-1}Hg = H]$$

証明 (1) \Rightarrow (2) を示す。

(1) を仮定する。任意の $g \in G$ と $h \in H$ について、(1) から $g^{-1}hg \in H$ 。すなわち、 $\exists h' \in H [h' = g^{-1}hg]$ 。

そのような h' について、 $h = gh'g^{-1} = (g^{-1})^{-1}h'g^{-1}$

すべての元は逆元をもつため、以上より

$$\forall g \in G \forall h \in H [\exists h' \in H [h = g^{-1}h'g]]$$

すなわち、 $\forall g \in G [g^{-1}Hg \supset H]$ を得る。

(1) \Leftarrow (2) を示す。雑な導出木を示しておきます。

□

$$\begin{array}{c}
(2) \\
\hline
\forall g[g^{-1}Hg \supset H] \\
\hline
g^{-1}Hg \supset H \\
<h> \frac{\forall h[h \in H \Rightarrow h \in g^{-1}Hg]}{h \in H \Rightarrow h \in g^{-1}Hg} \\
\hline
h \in H \\
\hline
h \in g^{-1}Hg \\
\hline
\exists h' \in H[g^{-1}hg = h'] \\
\hline
g^{-1}hg = h' \\
\hline
ghg^{-1} = h'^{-1} \\
\hline
h = g^{-1}h'^{-1}g \\
\hline
\exists a \in H[h = g^{-1}ag] \\
\hline
h \in g^{-1}Hg \\
\text{仮定の除去} \frac{h \in g^{-1}Hg}{h \in H \Rightarrow h \in g^{-1}Hg} \\
<h> \frac{\forall h[h \in H \Rightarrow h \in g^{-1}Hg]}{g^{-1}Hg \supset H} \\
\text{の定義} \frac{g^{-1}Hg \supset H}{g \in G \Rightarrow g^{-1}Hg \supset H} \\
\text{仮定の除去} \frac{g \in G \Rightarrow g^{-1}Hg \supset H}{\forall g[g \in G \Rightarrow g^{-1}Hg \supset H]} \\
<g> \frac{\forall g[g \in G \Rightarrow g^{-1}Hg \supset H]}{\forall g \in G[g^{-1}Hg \supset H]} \\
(2) \text{ の定義} \frac{\forall g \in G[g^{-1}Hg \supset H]}{(2)} \\
\text{仮定 (1) の除去} \frac{(2)}{(1) \Leftarrow (2)}
\end{array}$$

上でみたように、これらの条件によって、剰余類の間に演算を定義できる。剰余類の集合 (すなわち分割) とこの演算は自明に群を成す。

定義 30 (商群、剰余群) 群 G の部分群 H による剰余類の集合 G/H と、2 項演算

$$\circ : G/H \times G/H \rightarrow G/H; g_1H \circ g_2H \mapsto (g_1g_2)H$$

の成す群を商群、または剰余群という。

商群の積の定義から、群 G の元 g を g を含む剰余類に写す自然な写像 $\pi : G \rightarrow G/H$ は全射かつ準同型である。

$$\begin{aligned}
\pi(g_1g_2) &= (g_1g_2)H \\
&= g_1Hg_2H \\
&= \pi(g_1)\pi(g_2)
\end{aligned}$$

$$\frac{A \in G/H}{\frac{\exists g \in G[A = gH]}{g \in G \wedge A = gH}}$$

雑導出木なので断りなく使っていたが、存在量子子からの演繹で現れる記号は存在量子子のかかる論理式を満たすような対象を指している。ここでは g を $g \in G \wedge A = gH$ を満たす対象を指す記号として使っている。

$$\begin{array}{c}
\frac{g \in G \wedge A = gH}{\frac{g \in G}{\pi(g) = gH} \quad \frac{g \in G \wedge A = gH}{gH = A}} \\
\frac{\pi(g) = A}{\frac{\exists g[\pi(g) = A]}{A \in G/H \Rightarrow \exists g[\pi(g) = A]}} \\
\langle A \rangle \frac{A \in G/H \Rightarrow \exists g[\pi(g) = A]}{\forall A \in G/H [\exists g[\pi(g) = A]]}
\end{array}$$

定義 31 (正規部分群) 群 G の部分群 H が、 $\forall g \in G \forall h \in H [g^{-1}hg \in H]$ を満たすとき、 H を正規部分群といい、 $G \triangleright H$ とかく。

正規部分群の条件が $\forall g \in G [gH = Hg]$ と同値であることは自明だが、このことから正規部分群とは、左右の剰余類が一致する部分群と言い換えることができる。

定義 32 (内部自己同型) 群 G から G への写像 $\varphi_g : G \rightarrow G; h \mapsto g^{-1}hg$ は自明に同型であるが、これを G の内部自己同型という。

実は共役 $g^{-1}Hg$ は部分群 H の内部自己同型による像であったことがわかる。

命題 33 群 G の元 g による部分群 H の共役 $g^{-1}Hg$ は G の部分群である。

証明 群の定義から $g^{-1}Hg$ が G の部分集合であることは自明。

H は単位元を含むため、 $g^{-1}Hg$ も単位元を含む。

H は部分群であるから h^{-1} は H の元であり、同様に g^{-1} も G の元であるから、 $g^{-1}hg$ の逆元 $ghg^{-1} = (g^{-1})^{-1}hg^{-1}$ も $g^{-1}Hg$ の元である。

$g^{-1}Hg$ の任意の元 g_1, g_2 について、それぞれ $g_1 = g^{-1}h_1g$ 、 $g_2 = g^{-1}h_2g$ となる H の元 h_1, h_2 が存在する。このとき、

$$g_1g_2 = g^{-1}h_1gg^{-1}h_2g = g^{-1}h_1h_2g \in g^{-1}Hg$$

よって、演算について閉じているため $g^{-1}Hg$ は G の部分群。 □

補題 34 群 G の正規部分群 H と部分群 G_1 の共通部分 $H \cap G_1$ は G_1 の正規部分群である。

証明 $H \cap G_1$ の元 x について、 $x \in H$ であるから、 $G_1 \subset G$ より $\forall g \in G_1 [g^{-1}xg \in H]$ 。

$x \in G_1$ でもあるから、 $\forall g \in G_1 [g^{-1}xg \in G_1]$ 。

よって、 $\forall x \in H \cap G_1 [\forall g \in G_1 [g^{-1}xg \in H \cap G_1]]$ 。 □

これによって参考書問 4.1 は解かれた。

問 2 群 G が集合 X に推移的に作用しているとき、 X の任意の点 x, y の固定群 G_x, G_y は互いに共役となることを示せ (参考書問 4.2)。

推移的に作用している、とは作用の対象となる集合 X の任意の元 x の軌道 $Gx = \{gx \mid g \in G\}$ が X に一致することを指す。

G_x が x の固定群であるというのは、 $G_x x = \{x\}$ のことである。

x, y を入れ替えるような X の変換に対応する G の要素を a とする。すなわち、

$$\forall p \in X \left[(p \neq x \wedge p \neq y \Rightarrow ap = p) \wedge (p = x \Rightarrow ap = y) \wedge (p = y \Rightarrow ap = x) \right]$$

このとき、 $a^{-1}G_x a = G_y$ かつ $a^{-1}G_y a = G_x$ となるから、 G_x と G_y は a によって互いに共役。

3.2 第一同型定理 (準同型定理)

定理 35 (第一同系定理 (準同型定理)) 群 G から群 H への写像 $\varphi : G \rightarrow H$ が準同型であるとき、 φ の核は G の正規部分群である。つまり、

$$G \triangleright \text{Ker } \varphi$$

また、

$$G/\text{Ker } \varphi \cong \text{Im } \varphi$$

さらに、 G が有限群であるならば

$$|G|/|\text{Ker } \varphi| = |\text{Im } \varphi|$$

証明 $\text{Ker } \varphi$ の元 x について、

$$\begin{aligned} \varphi(g^{-1}xg) &= \varphi(g)^{-1}\varphi(x)\varphi(g) && \varphi \text{ は準同型} \\ &= \varphi(g)^{-1}e_H\varphi(g) && x \text{ は } \varphi \text{ によって単位元に写る} \\ &= \varphi(g)^{-1}\varphi(g) \\ &= e_H \end{aligned}$$

よって、 $g^{-1}\text{Ker } \varphi g = \text{Ker } \varphi$ 。

ここで、 $\text{Ker } \varphi$ による任意の剰余類について、その任意の元の φ の写す先は一致する。すなわち、

$$\forall A \in G/\text{Ker } \varphi \left[\forall x, y \in A [\varphi(x) = \varphi(y)] \right]$$

これは、 $A \in G/\text{Ker } \varphi$ は $g\text{Ker } \varphi$ より像は $\varphi\{g\text{Ker } \varphi\} = \{\varphi(g)\}$ となることから示すことができる。

つまり、 $\text{Ker } \varphi$ による剰余類においては φ の写す先は一意である。よって、 $G/\text{Ker } \varphi$ の元からその代表元 (なんでもよい) の φ による行き先を対応付けると、これは写像 (一意対応) となる。¹⁾

そのような写像 $\psi : G/\text{Ker } \varphi \rightarrow \text{Im } \varphi$ は明らかに全射であり、 φ が準同型であることから、これも準同型である。

任意の剰余類 A, B について、 $\psi(A) = \psi(B)$ であるとする。 $A = g_1\text{Ker } \varphi, B = g_2\text{Ker } \varphi$ である g_1, g_2 が存在するから、 $\varphi(g_1) = \varphi(g_2)$ 。

1) 写像よりも緩いものに対応がある。これは多対多の結びつけを許すもので、集合論で言えば冪集合そのものである。グラフの辺もこれで表される。対応が写像である条件は、任意の first 要素について、対応づけられている second 要素が一意であることで、これを一意対応という。

$$\begin{aligned}\varphi(g_1) &= \varphi(g_2) \\ \varphi(g_2)^{-1} \varphi(g_1) &= e_H \\ \varphi(g_2^{-1} g_1) &= e_H\end{aligned}$$

より $g_2^{-1} g_1 \in \text{Ker } \varphi$ であるから、 $g_1 = g_2 h$ となる $h \in \text{Ker } \varphi$ が存在する。 $h \text{Ker } \varphi = \text{Ker } \varphi$ より、 $g_1 \text{Ker } \varphi = g_2 \text{Ker } \varphi$ つまり、 $A = B$ 。よって、 ψ は単射である。

以上より、 $\psi : G/\text{Ker } \varphi \rightarrow \text{Im } \varphi$ は全単射で準同型であるから、同型である。よって

$$G/\text{Ker } \varphi \cong \text{Im } \varphi$$

G が有限群であるとき、全単射の存在から $|G/\text{Ker } \varphi| = |\text{Im } \varphi|$ 。

Lagrange の定理 (定理 15) より、 $|G/\text{Ker } \varphi| = |G|/|\text{Ker } \varphi|$ であるから

$$|G|/|\text{Ker } \varphi| = |\text{Im } \varphi|$$

□

3.3 第二同型定理

3.4 指標

4 射影幾何について