UEC 代数勉強会 第 4 回

9trap

uec19 情報理工学域 II 類 P1

今日の構成

- 置換表現
- 剰余類
- 巡回群の位数
- ゲームの置換群
- 作用
- 対称性の例

左移動

Definition 4.1.1 (左移動[*1]). 群 G とその元 g について、$\lambda_g : G \to G, a \mapsto ga$ で定義される写像 λ_g を G の g による左移動という．

1 番号振りは、勉強会番号．章．順番 としている

勿論右移動も存在して、左移動の g^{-1} を右からかける写像を指す .

左移動と右移動は双対の関係にあり、以下の左移動に関する議論は、すべて左を右に、g^{-1} を右からかけることで右移動にも適用できる (双対原理).

右移動の定義は、作用の定義にもよる . これは後述する .

Lemma 4.1.2 群 G と、その元 g による左移動 λ_g は、全単射である．

Proof. G の任意の元 a, b について、g の逆元の存在から

$ga = gb \Rightarrow a = b$. よって、$\lambda_g$ は単射．

G の任意の元 a について、g の逆元の存在から

$\exists x \in G\left[x = g^{-1}a\right]$. そのような x について、$gx = a$.

よって、λ_g は全射．

以上より λ_g は単射であり全射であるから、全単射である． ■

表現

Definition 4.1.3 (表現). 群 G について、

G の元 g を線型空間 V 上の線型変換 $T(g)$ に対応させる写像 T であって、$\forall g, h \in G\left[T(gh) = T(g)T(h)\right]$ であるものを G の表現という．

Remark 4.1.4 (線型空間と線型写像). 思い出してください .

置換表現

Definition 4.1.5 (置換表現). 群 G が有限群であるとき、G は $\mathbb{Z}_n (n \in \mathbb{N})$ と対等であり[*2]、その対応 $\varphi : G \to \mathbb{Z}_n$ と左移動 λ_g について、$G \to S_n, g \mapsto \varphi \circ \left(\lambda_g \circ \varphi^{-1}\right)$[*3]で定義される写像 λ を群 G の左移動による置換表現という．

2 実はこれ自体が集合が有限であることの定義となりうる．そうでない場合 (無限でないとする) も定理として導くことができる．

3 置換を $\mathbb{Z}_n \to \mathbb{Z}_n$ とした

Theorem 4.1.6 群 G の左移動による置換表現 λ は準同型である．

Proof. G の元 g, h について、$\lambda(g), \lambda(h) \in S_n$ の合成は、

$\varphi \circ \lambda_h \circ \varphi^{-1} \circ \varphi \circ \lambda_g \circ \varphi^{-1}$. 写像の合成では結合則が成り立つので、これは $\varphi \circ \left(\lambda_h \circ \lambda_g\right) \circ \varphi^{-1}$ である．

ここで、$\forall a \in G\left[\left(\lambda_h \circ \lambda_g\right)(a) = gha = \lambda_{gh}(a)\right]$ より、$\lambda(gh) = \lambda(g)\lambda(h)$. よって λ は準同型． ■

忠実

Definition 4.1.7 (忠実). 群 G の表現 τ が単射であるとき、表現 τ は忠実であるという．

Theorem 4.1.8 群 G の左移動による置換表現 λ は忠実である．

Proof. G の単位元 e は $g, h \in G$ によって g, h へ移されるため、$g \neq h$ のとき少なくともこの部分で誘導される置換が異なる．

よって、左移動による置換表現 λ は単射である． ■

もちろん置換表現も表現であり、たとえば $(1,2) \in S_3$ に対応するのは $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in GL(3,\mathbb{R})$ である．

Problem 4.1.9 (参考書 問 2.2). S_3 の左移動による置換表現を求めよ .

線型表現

対称群の線型表現は $\sigma \in S_n$ から

$$T_\sigma : \left(\boldsymbol{e}_1 \dots \boldsymbol{e}_n\right) \mapsto \left(\boldsymbol{e}_{\sigma(1)} \dots \boldsymbol{e}_{\sigma(n)}\right)$$

で定義される $T_\sigma \in GL(n, \mathbb{R})$ への対応によって定まる．

明らかに $\boldsymbol{u} \cdot \boldsymbol{v} = T_\sigma(\boldsymbol{u}) \cdot T_\sigma(\boldsymbol{v})$ である (計量、つまり内積が保存される) から、T_σ は直交行列である．

剰余類への準備

Definition 4.2.1 群 G の元 g と部分群 A について、

$\{ga \mid a \in A\}$ を gA とかく．

同様に、$\{ag \mid a \in A\}$ を Ag とかく．

単なる記法 (notation) のはなし．

左移動の性質

Lemma 4.2.2 (参考書 補題 2.5). 群 G の部分群 A について、

$$\forall g_1, g_2 \in G\left[g_1\left(g_2 A\right) = \left(g_1 g_2\right)A\right]$$

また、G の部分群 A, B について、

$\forall g \in G[A = B \Leftrightarrow gA = gB \Leftrightarrow Ag = Bg]$. さらに、$G$ の部分群 A が有限群のとき、

$$\forall g \in G\left[\left|A\right| = \left|gA\right| = \left|Ag\right|\right].$$

Proof. 補題4.1.2と定理4.1.6からわかる . ■

Lemma 4.2.3 (参考書 補題 2.6). 群 G の元 g と部分群 H について、

$$g \in H \Leftrightarrow gH = H,$$

$$g \notin H \Leftrightarrow gH \cap H = \emptyset,$$

$$\forall g_1, g_2 \in G\left[g_1 H = g_2 H \vee g_1 H \cap g_2 H = \emptyset\right]$$

Proof. 参考書参照 . ■

Lemma 4.2.4 群 G とその部分群 H について、

$$\forall g, h \in G\left[gH = hH \Leftrightarrow g^{-1}h \in H\right]$$

Proof. $gH = hH \Leftrightarrow g^{-1}hH = H$ だから補題4.2.3より直ちに従う． ■

左移動による同値関係

Theorem 4.2.5 (左移動による同値関係). 群 G とその部分群 H について、$\forall g, h \in G\left[g \sim h \Leftrightarrow g^{-1}h \in H\right]$.

で定められる関係は同値関係である .

Proof. $\forall g \in G\left[g^{-1}g = e\right]$ であり、単位元 e はどの部分群にも含まれるため、$g \sim g$ となりこの関係は反射律を満たす .

また、部分群は逆元も含むため、$g \sim h$ すなわち $g^{-1}h \in H$ ならば、$\left(g^{-1}h\right)^{-1} = h^{-1}g \in H$ すなわち $h \sim g$. よって、対称律が満たされる .

さらに、$f, g, h \in H$ について、$f \sim g$ かつ $g \sim h$ ならば、$f^{-1}g \in H$ かつ $g^{-1}h \in H$. 部分群は演算について閉じているため、$f^{-1}h = f^{-1}gg^{-1}h \in H$ すなわち $f \sim h$. よって、推移律が満たされた . ■

同値類

Definition 4.2.6 (同値類). 関係 $\sim$ が集合 S の同値関係であり $a \in S$ とき、$\{x \in S \mid x \sim a\}$ を a の $\sim$ の同値類といい、誤解を招かない限り (a) とかく．

補題4.2.4からわかるように、群 G の任意の元 g について、gH は同値類を与える．

Lemma 4.2.7 $\forall a \in S\bigl[a \in (a)\bigr]$

Proof. 同値関係の反射律から $a \sim a$. よって、$a \in (a)$. ■

Lemma 4.2.8 $\forall a, b \in S\bigl[(a) \cap (b) \neq \emptyset \Rightarrow (a) = (b)\bigr]$

Proof. $(a) \cap (b) \neq \emptyset$ を仮定すると、$\exists c \in S\bigl[c \in (a) \wedge c \in (b)\bigr]$. そのような c について、$c \sim a \wedge c \sim b$. よって、$x \in (a)$ ならば、$x \sim a$ でありかつ $c \sim a \wedge c \sim b$ だから同値関係の推移律から $x \sim b$、つまり $x \in (b)$.

逆もしかり . よって、$(a) = (b)$. ■

分割

Definition 4.2.9 (分割). 集合 P が集合 S の分割であるとは、$\bigcup P = S \wedge \forall u, v \in S[u \cap v \neq \emptyset \to u = v]$ を満たすことをいう．

分割

Theorem 4.2.10 (同値関係が導く分割). 関係 $\sim$ が集合 S の同値関係であるとき、$\{(a) \mid a \in S\}$ は S の分割を与える .

Proof. $a \in S$ について、補題4.2.7より $a \in (a)$.

よって、$\exists x \in \{(a) \mid a \in S\}[a \in x]$.

よって、$\bigcup\{(a) \mid a \in S\} = S$.

また、補題4.2.8より、そのまま 2 個目の要請が満たされる . ■

剰余類

Definition 4.2.11 (剰余類). 群 G とその元 g、部分群 H について、gH を g を代表元とする左剰余類という．

定義4.2.9と定理4.2.10をみると、$\{gH \mid g \in G\}$ が G の分割となっていることがわかる．

Definition 4.2.12 $\left|\{gH \mid g \in G\}\right|$ を $[G : H]$ とかく．

Lagrange の定理

Theorem 4.2.13 (Lagrange の定理). 有限群 G の部分群 H の位数は G の位数の約数である.

Proof. 補題4.1.2から、すべての剰余類の要素の個数は同じ. よって、$|G| = |H|[G : H]$ となる. ■

Problem 4.2.14 (参考書 問 2.3). $g \sim h \Leftrightarrow h^{-1}g \in H$ で定められた関係が同値関係であることを示せ．

元の位数

Definition 4.3.1 (元の位数). 群 G の元 g について、$g^m = e$ となる最小正の整数 m が存在するとき、m を元 g の位数という．そのような正の整数が存在しないとき、元 g の位数は無限大であるという．

Corollary 4.3.2 有限群の元の位数は群の位数の約数である．

Proof. 定理4.2.13(lagrange) から明らか． ■

Problem 4.3.3 (参考書 問 2.4). S_3 の各元の位数を求めよ .

Problem 4.3.4 (参考書 問 2.5). 群 G の元 x の位数が 12 のとき、$x^k (1 \leq k \leq 12)$ の位数を求めよ .

Problem 4.3.5 (参考書 問 2.6). S_4 において、

$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ とする．

1. a の位数を求めよ．

2. $x^m = a$ となるような x と m は $x = a$ と $m = 1$ 以外に存在するか？

Problem 4.3.6 (参考書 問 2.7). S_3 の元 $a = (1,2,3)$ と $b = (1,2)$ を生成元として取ったときの基本関係式を示せ．また、S_4, A_4 の生成元と基本関係式をそれぞれ 1 組あたえよ．

Proposition 4.3.7 (巡回群の判定). 有限群 G の位数と等しい位数を持つ元が G に存在すれば、G はその元を生成元とする巡回群となる．

Proof. 参考書参照．■

Corollary 4.3.8 (参考書 系 2.10). 位数が素数 p の群 G は巡回群であり、単位元以外の元が生成元である．

Proof. 参考書参照．■

Corollary 4.3.9 (参考書　系 2.11).　位数が素数 p の群 G は巡回群であり、単位元以外の元が生成元である．

Proof.　参考書参照．■

Problem 4.3.10 (参考書 問 2.8). 位数 15 の巡回群の生成元となりうる元はいくつあるか？

Problem 4.3.11 (参考書 問 2.9). 位数 24 の巡回群の部分群をすべてあげよ．

Problem 4.3.12 (参考書 問 2.10).

1. 群 G の 2 つの部分巡回群の共通部分は巡回群となることを示せ .

2. 位数が互いに素な 2 つの巡回部分群の共通部分は単位元だけであることを示せ .

15 並べ

こういうやつ https://www.afsgames.com/15puzzle.htm

デフォルトの 1-15 までの並びをそのまま $\mathbb{Z}_{15}$ としてみると、15 並べの操作一つ一つは置換とみなせる．このとき、実は 15 ならべで許される全操作は偶置換となっている．左右のずらしはそもそも数字のならびが変わらず、上下の移動は 4 つの連続した場所が循環シフトしていて、これは偶置換である．

よって、15 ならべの操作の全体は A_{15} となる．

15 並べ

Problem 4.4.13 (参考書 問 2.11). 参考書参照 .

Rubik Cube

ルービックキューブはしってるはずです．

ここがのぞくのにいいきがする

http://www.ivis.co.jp/text/20100901.pdf

あみだくじ

あみだくじが互換の積で表せることは明らか．

組紐

くみひもむず．

群の作用

Definition 4.5.14 (群の作用). 集合 X への群 G の作用とは、G の各元に X からそれ自身への写像が対応しており、それが次の公理を満たすものを言う．

1. 単位元 $e \in G$ が恒等写像に対応する．

2.$\forall f, g \in G, \forall x \in X, g\bigl(f(x)\bigr) = (g \circ f)(x)$

思い出してみると、実は左移動は作用であったことがわかる．

右移動を参考書を無視して g^{-1} を右からかけると書いたのは、作用としてみたときそうしないと 2 の条件が満たされないからである．

対称性

「群論といえば対称性！みたいな話を聞いていたけどどこが？」みたいになってたかもしれないが、作用を考えるとわかるかもしれない．

乗法群 $\{\pm 1\}$ の平面 $\mathbb{R}^2$ への作用に $(x, y) \mapsto (x,\text{-}y)$ や $(x, y) \mapsto (-x, y)$ がある．

これらは x, y 軸対称の反転で、この作用で不変の図形は線対称である．

二面体群

Definition 4.6.15 (二面体群 D_n).

$\tau = (x, y) \mapsto (x,\text{-}y)$

$$\sigma = (x, y) \mapsto \left(x\cos\left(\frac{2\pi}{n}\right) - y\sin\left(\frac{2\pi}{n}\right), y\cos\left(\frac{2\pi}{n}\right) + y\sin\left(\frac{2\pi}{n}\right)\right)$$

とすると、$D_n = \langle \sigma, \tau \rangle$ で二面体群 D_n を定義する .

σ はなんだか難しそうだが、反時計周りに $\dfrac{2\pi}{n}$ ラジアン回転させる操作である．

以下の式が基本関係式となる．

$$\tau\sigma = \sigma^{-1}\tau$$

$$\tau^2 = e$$

$$\sigma^n = e$$

n が偶数であるとき、σ^2 で $\sigma^m (0 \leq m \leq n-1)$ が尽くされないので、D_n は $H = \left\{e, \sigma, \sigma^2, \ldots, \sigma^{n-2}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-2}\right\}$ と σH に分けられる .σ^2 を別の二面体群の σ に対応させると、$H \simeq D_{n/2}$ あることがわかる .

$n/2$ が奇数のときは、$H, \sigma^{n/2} H$ にわけられるといえる $(\sigma^{n/2} \notin H)$ ので、$\sigma^{n/2}$ の巡回群 C_2 と次に示す群の直積を用いて、

$D_n \simeq D_{n/2} \times C_2$ と表せる .

Definition 4.6.16 (群の自然な直積). 群 G と群 H について、$G \times H$ に演算 $(a_1, b_1) \circ (a_2, b_2) = (a_1 a_2, b_1 b_2)$ を入れた群を 2 つの群の直積という．

Problem 4.6.17 (参考書 問 3.1). 二面体群 D_3, D_4, D_5, D_6 の置換群による表現を求めよ．

正 n 面体群

正 n 面体が $n = 4, 6, 8, 12, 20$ ですべてであることは知ってるかもしれない . 正 n 面体を不変にする $\mathbb{R}^3 \to \mathbb{R}^3$ の変換群を正 n 面体群 P_n という . 正多面体の双対 (面の中心を頂点とする正多面体との関係) を用いると、正 6 面体と正 8 面体、正 12 面体と正 20 面体はどちらか一方の変換群と双対の変換があればいいので、通常は正 4 面体群、正 8 面体群、正 20 面体群を考える .

群の無限次元空間への作用

$\mathbb{R} \to \mathbb{R}$ の関数 $f(x)$ への $\{\pm 1\}$ の作用

$$1 \mapsto \big(f(x) \mapsto f(x)\big)$$
$$-1 \mapsto \big(f(x) \mapsto f(-x)\big)$$