UEC 代数勉強会 第 7 回

9trap/ 隕石

2021/06/22

目次

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。

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

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

が次の条件を満たすとき、組 $\left(G, \circ\right)$ を群という。

$$
\begin{aligned}
&(1)\forall a,b,c \in G(a \circ b) \circ c = a \circ (b \circ c) && \text{(結合律)}\\
&(2)\exists e \in G\big[\forall a \in G[e \circ a = a \circ e = a]\big] && \text{(単位元の存在)}\\
&(3)\forall g \in G\big[\exists h \in G[g \circ h = h \circ g = e]\big] && \text{(逆元の存在)}
\end{aligned}
$$

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

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

が次の条件を満たすとき、組 $\left(A, +, \cdot\right)$ を環という。

$$
\begin{aligned}
&(1)\big(A, +\big)\text{は可換群を成す}\\
&(2)\forall a,b,c \in A\big[(ab)c = a(bc)\big] && \text{(乗法の結合律)}\\
&(3)\forall a,b,c \in A\big[a(b+c) = ab + ac\big] && \text{(分配律)}
\end{aligned}
$$

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

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

が次の条件を満たすとき、組 $\left(K, +, \cdot\right)$ を環という。

$$
\begin{aligned}
&(1)\big(K, +\big)\text{は可換群を成す}\\
&(2)\big(K \backslash \{0\}, \cdot\big)\text{は可換群を成す}\\
&(3)\forall a,b,c \in A\big[a(b+c) = ab + ac\big] && \text{(分配律)}
\end{aligned}
$$

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 $\varphi : G \to H$ が以下を満たすとき、写像 φ を準同型であるという。

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

1.4　置換表現

命題 5 (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 $\varphi : G \to G; a \mapsto ga$ 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 6 (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 7 (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 8　群 G の有限部分集合 A について、$\lvert A \rvert = \lvert gA \rvert$

証明　命題 5 より。 □

補題 9 (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、$\exists x[x \in gH \land x \in H]$。

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

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 $gH \cap H = \emptyset$。 □

命題 10　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 $aH = aH \land (aH = bH \Leftrightarrow bH = aH)$ であるから、反射律と対称律が成り立つ。

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

系 11　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 12 (左剰余類)　ここでの同値類 gH を左剰余類という。

定理 13 (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 8 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、$\left|G\right| = [G:H]\cdot\left|H\right|$。 □

1.6　作用

定義 14 (作用)　群 G から集合 X について、演算 $\bullet : G \times X \to X$ が以下を満たすとき、これを作用という。

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

2　対称式と交代式

2.1　多項式への作用

命題 15 (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

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

を以下のように定める

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

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、 □

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

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。

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

例 16 (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。

$$s_k = \sum_{1\le i_1<i_2<\cdots<i_k\le n} x_{i_1}x_{i_2}\ldots x_{i_k}$$

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 $i : (1, \cdots, k) \to (1, \cdots, n); a \mapsto i(a)$ についての項 $x_{i(1)}x_{i(2)}\ldots x_{i(k)}$ 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 17 (差積)　対称式の代表的な例に、差積がある。

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

定義 18 (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 $\boldsymbol{a}$ のことをいう。

$x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ の型は $\boldsymbol{a} = (a_1, a_2, \cdots, a_n)$

定義 19 (単項式の順序)　型 $\boldsymbol{a}, \boldsymbol{b}$ 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 $\boldsymbol{a} > \boldsymbol{b}$ とする。

また、順序 $\geq$ を $\forall \boldsymbol{a}, \boldsymbol{b}\left[\boldsymbol{a} \geq \boldsymbol{b} \Leftrightarrow (\boldsymbol{a} > \boldsymbol{b} \vee \boldsymbol{a} = \boldsymbol{b})\right]$ 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 20 (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 $x^{\sum_{k=1}^{n} d_k} x^{\sum_{k=2}^{n} d_k} \cdots x^{d_n}$ 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 16 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 21 (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 20 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 $\boldsymbol{a} = (a_1, a_2, \cdots, a_l)$ 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 $\boldsymbol{a}$ 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 $\boldsymbol{b}$ について、$\boldsymbol{a} > \boldsymbol{b}$。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。

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

3.2 準同型定理

3.3 次元定理

3.4 指標

4 射影幾何について