UEC 代数勉強会 第 7 回

9trap/ 隕石

2021/07/01

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。

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

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

が次の条件を満たすとき、組 $(G, \circ)$ を群という。

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

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

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

が次の条件を満たすとき、組 $(A, +, \cdot)$ を環という。

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

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

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

が次の条件を満たすとき、組 $(K, +, \cdot)$ を環という。

(1)$\big(K,+\big)$は可換群を成す

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

(3)$\forall a,b,c\in A\Big[a\big(b+c\big)=ab+ac\Big]$　　(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 $\varphi:G\to H$ が以下を満たすとき、写像 φ を準同型であるという。

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

命題 5　写像 φ が群 G から H への準同型であるとき、

$$(1)\varphi\big(e_G\big)=e_H$$
$$(2)\forall x\in G\Big[\varphi\big(x^{-1}\big)=\varphi(x)^{-1}\Big]$$

証明　G の任意の元 x について、

$$\begin{aligned}\varphi\big(e_Gx\big)&=\varphi\big(e_G\big)\varphi(x)\\ \varphi(x)&=\varphi\big(e_G\big)\varphi(x)\\ e_H&=\varphi\big(e_G\big)\end{aligned}$$

また、

$$\begin{aligned}\varphi\big(x^{-1}x\big)&=\varphi\big(x^{-1}\big)\varphi(x)\\ \varphi\big(e_G\big)&=\varphi\big(x^{-1}\big)\varphi(x)\\ e_H&=\varphi\big(x^{-1}\big)\varphi(x)\\ \varphi(x)^{-1}&=\varphi\big(x^{-1}\big)\end{aligned}$$

□

定義 6 (同型写像)　準同型写像 $\varphi:G\to H$ 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 7　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。

$$\varphi\big(\varphi^{-1}(xy)\big) = xy$$
$$\varphi\big(\varphi^{-1}(xy)\big) = \varphi\big(\varphi^{-1}(x)\big)\varphi\big(\varphi^{-1}(y)\big)$$
$$\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$$

□

1.4 置換表現

命題 8 (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 9 (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 10 (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 11　群 G の有限部分集合 A について、$\big|A\big| = \big|gA\big|$

証明　命題 8 より。 □

補題 12 (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、$\exists x\big[x \in gH \wedge x \in H\big]$。

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

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 13　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 $aH = aH \wedge \big(aH = bH \Leftrightarrow bH = aH\big)$ 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。 □

系 14　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 15 (左剰余類)　ここでの同値類 gH を左剰余類という。

定理 16 (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 11 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 17 (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 18 (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

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

を以下のように定める

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

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、 □

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

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。

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

例 19 (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。

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

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 $x_{i(1)}x_{i(2)}...x_{i(k)}$ 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 20 (差積)　交代式の代表的な例に、差積がある。

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

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

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

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

定義 21 (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。

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

定義 22 (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 $\forall \boldsymbol{a},\boldsymbol{b}\left[\boldsymbol{a} \geq \boldsymbol{b} \Leftrightarrow \left(\boldsymbol{a} > \boldsymbol{b} \vee \boldsymbol{a} = \boldsymbol{b}\right)\right]$ 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 23 (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 19 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 24 (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 23 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 $\boldsymbol{a} = \left(a_1, a_2, \cdots, a_l\right)$ 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。

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

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。

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

より、

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

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。

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

より

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

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。

$$s_2^2 = \left(\sum_{1\le i_1<i_2\le n} x_{i_1} x_{i_2}\right)^2$$
$$= \sum_{1\le i_1<i_2\le n} x_{i_1}^2 x_{i_2}^2 + \sum_{1\le i_1<i_2<i_3\le n} \left(2x_{i_1}^2 x_{i_2} x_{i_3} + 2x_{i_1} x_{i_2}^2 x_{i_3} + 2x_{i_1} x_{i_2} x_{i_3}^2\right) + \sum_{1\le i_1<i_2<i_3<i_4\le n} 6 x_{i_1} x_{i_2} x_{i_3} x_{i_4}$$

より、

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

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。

$$s_1 s_3 = \left(\sum_{i}^{n} x_i\right)\left(\sum_{1\le i_1<i_2<i_3\le n} x_{i_1} x_{i_2} x_{i_3}\right)$$
$$= \sum_{1\le i_1<i_2<i_3\le n} \left(x_{i_1}^2 x_{i_2} x_{i_3} + x_{i_1} x_{i_2}^2 x_{i_3} + x_{i_1} x_{i_2} x_{i_3}^2\right) + \sum_{1\le i_1<i_2<i_3<i_4\le n} 4 x_{i_1} x_{i_2} x_{i_3} x_{i_4}$$

より、

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

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 25 (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

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

は差積で見たように交代式である。

例 26 (判別式) $\alpha_1, \cdots, \alpha_n$ を根にもつ多項式 $f = (x-\alpha)\cdots\left(x-\alpha_n\right)$ の判別式 D を

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

で定義する。

判別式が 0 になるとき、またそのときのみ $\exists i, j\Big[\alpha_i = \alpha_j\Big]$、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、$\exists i, j\Big[\big(\alpha_i - \alpha_j\big)\Big] \in \mathbb{C}$ 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 27 (共役) 群 G の元 g と部分群 H について、

$$g^{-1}Hg := \Big\{g^{-1}hg \;\Big|\; h \in H\Big\}$$

を H の x による共役という。

記法 28 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 29 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 $\forall g \in G\Big[g^{-1}Hg = H\Big]$ であるとき、

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

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

$$\begin{aligned}
\big(a_1 a_2\big)H &= \big(g_1 h_1 g_2 h_2\big)H \\
&= \big(g_1 h_1 g_2\big)H && H\text{は群であるから、}\ h_2 H = H \\
&= \big(g_1 h_1 g_2 g_2^{-1} h_2 g_2\big)H && g_2^{-1}Hg_2 = H\text{より} g_2^{-1}h_2 g_2 H = H \\
&= \big(g_1 h_1 h_2 g_2\big)H \\
&= \big(g_1 h_1 h_2 g_2 g_2^{-1}\big)Hg_2 && g_2^{-1}Hg_2 = H \\
&= \big(g_1 h_1 h_2\big)Hg_2 \\
&= \big(g_1\big)Hg_2 \\
&= \big(g_1 g_2\big)H && g_2^{-1}Hg_2 = H
\end{aligned}$$

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。

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

命題 29 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 30　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。

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

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

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

証明　(1) ⇒ (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、$\exists h' \in H\Big[h' = g^{-1}hg\Big]$。

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

すべての元は逆元をもつため、以上より

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

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

(1) ⇐ (2) を示す。雑な導出木を示しておきます。　□

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(2)}{\forall g\Big[g^{-1}Hg \supset H\Big]}}{g^{-1}Hg \supset H}}{\forall h\Big[h \in H \Rightarrow h \in g^{-1}Hg\Big]}}{h \in H \Rightarrow h \in g^{-1}Hg}\ \text{<h>}}{h \in g^{-1}Hg}\quad h \in H}{\exists h' \in H\Big[g^{-1}hg = h'\Big]}}{g^{-1}hg = h'}}{ghg^{-1} = h'^{-1}}}{h = g^{-1}h'^{-1}g}}{\exists a \in H\Big[h = g^{-1}ag\Big]}}{h \in g^{-1}Hg}\ \text{仮定の除去}}{h \in H \Rightarrow h \in g^{-1}Hg}\ \text{<h>}}{\forall h\Big[h \in H \Rightarrow h \in g^{-1}Hg\Big]}\ \text{⊃の定義}}{g^{-1}Hg \supset H}\ \text{仮定の除去}}{g \in G \Rightarrow g^{-1}Hg \supset H}\ \text{<g>}}{\forall g\Big[g \in G \Rightarrow g^{-1}Hg \supset H\Big]}}{\forall g \in G\Big[g^{-1}Hg \supset H\Big]}\ \text{(2) の定義}}{(2)}\ \text{仮定 (1) の除去}}{(1) \Leftarrow (2)}$$

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 31 (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

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

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 $\pi : G \to G/H$ は全射かつ準同型である。

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

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

雑導出木なので断りなく使っていたが、 存在量化子からの演繹で現れる記号は存在量化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。

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{g \in G \wedge A = gH}{g \in G}}{\pi(g) = gH} \qquad \dfrac{g \in G \wedge A = gH}{gH = A}}{\pi(g) = A}}{\exists g\big[\pi(g) = A\big]}}{A \in G/H \Rightarrow \exists g\big[\pi(g) = A\big]}\ \text{<A>}$$
$$\forall A \in G/H\Big[\exists g\big[\pi(g) = A\big]\Big]$$

定義 32 (正規部分群) 群 G の部分群 H が、$\forall g \in G \forall h \in H\Big[g^{-1}hg \in H\Big]$ を満たすとき、H を正規部分群といい、$G \rhd H$ とかく。

正規部分群の条件が $\forall g \in G\big[gH = Hg\big]$ 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 33 (内部自己同型) 群 G から G への写像 $\varphi_g : G \to G; h \mapsto g^{-1}hg$ 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 34 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 $ghg^{-1} = \left(g^{-1}\right)^{-1}hg^{-1}$ 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 35　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 $\forall g \in G_1\left[g^{-1}xg \in H\right]$。

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

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

これによって参考書問 4.1 は解かれた。

問 2 (参考書問 4.2)　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、$G_xx = \{x\}$ 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、$a^{-1}G_xa = G_y$ かつ $a^{-1}G_ya = G_x$ 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 36 (第一同系定理 (準同型定理))　群 G から群 H への写像 $\varphi : G \to H$ 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、

$$G \rhd \mathrm{Ker}\,\varphi$$

また、

$$G/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi$$

さらに、G が有限群であるならば

$$\left|G\right|/\left|\mathrm{Ker}\,\varphi\right| = \left|\mathrm{Im}\,\varphi\right|$$

証明　$\mathrm{Ker}\,\varphi$ の元 x について、

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

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

ここで、$\mathrm{Ker}\,\varphi$ 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、

$$\forall A \in G/\mathrm{Ker}\,\varphi\Big[\forall x, y \in A\big[\varphi(x) = \varphi(y)\big]\Big]$$

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

つまり、$\mathrm{Ker}\,\varphi$ 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、$G/\mathrm{Ker}\,\varphi$ 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 $\psi : G/\mathrm{Ker}\,\varphi \to \mathrm{Im}\,\varphi$ 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、$\psi\big(A\big) = \psi(B)$ であるとする。$A = g_1\mathrm{Ker}\,\varphi, B = g_2\mathrm{Ker}\,\varphi$ である g_1, g_2 が存在するから、$\varphi\big(g_1\big) = \varphi\big(g_2\big)$。

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

より $g_2^{-1}g_1 \in \mathrm{Ker}\,\varphi$ であるから、$g_1 = g_2h$ となる $h \in \mathrm{Ker}\,\varphi$ が存在する。$h\,\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\varphi$ より、$g_1\mathrm{Ker}\,\varphi = g_2\mathrm{Ker}\,\varphi$ つまり、$A = B$。よって、ψ は単射である。

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

$$G/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi$$

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

Lagrange の定理 (定理 16) より、$\big|G/\mathrm{Ker}\,\varphi\big| = \big|G\big|/\big|\mathrm{Ker}\,\varphi\big|$ であるから

$$\big|G\big|/\big|\mathrm{Ker}\,\varphi\big| = \big|\mathrm{Im}\,\varphi\big|$$

□

この準同型定理は群論に限らず普遍的に代数系でなりたつものである。

例えば線形代数でいえば次元定理は $\big|G\big|/\big|\mathrm{Ker}\,\varphi\big| = \big|\mathrm{Im}\,\varphi\big|$ にあたる。普遍性を俯瞰したい場合は圏論をすることになる。

例 37　交代群は対称群の正規部分群である。

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、対応づけされている second 要素が一意であることで、これを一意対応という。

置換の符号 sgn の核がちょうど交代群となることから自明。

例 38　特殊線形群 $SL\big(n,\mathbb{R}\big)$ は一般線形群 $GL\big(n,\mathbb{R}\big)$ の正規部分群である。

行列式の核が特殊線形群となっている。

命題 39　指数が 2 の部分群は正規部分群である。

証明　群を G、部分群を H とする。$g\notin H$ とすると、G は H と gH に分割されるから、$gH = Hg$ となる。よって、H は G の正規部分群。 □

問 3 (参考書問 4.3(1),(3))　群 G と H とその間の写像 $\varphi : G \to H$ について、H_1 が H の正規部分群であるとき、逆像 $\varphi^{-1}\big\{H_1\big\}$ は G の部分群であるか、正規部分群であるか。もしそうであれば証明を、そうでなければ反例を与えよ。

G の任意の元 g について、

$$\begin{aligned}\varphi\Big\{g^{-1}\varphi^{-1}\big\{H_1\big\}g\Big\} &= \varphi(g)^{-1}\varphi\Big\{\varphi^{-1}\big\{H_1\big\}\Big\}\varphi(g) && \varphi\text{は準同型写像}\\ &= \varphi(g)^{-1}H_1\varphi(g)\\ &= H_1 && H_1\text{は正規部分群}\end{aligned}$$

より、$g^{-1}\varphi^{-1}\big\{H_1\big\}g = \varphi^{-1}\big\{H_1\big\}$ が成り立つ。

よって、$\varphi^{-1}\big\{H_1\big\}$ は G の正規部分群であり、当然部分群でもある。

問 4 (参考書問 4.3(2),(4))　群 G と H とその間の写像 $\varphi : G \to H$ について、G_1 が G の正規部分群であるとき、像 $\varphi\big\{G_1\big\}$ は H の部分群であるか、正規部分群であるか。もしそうであれば証明を、そうでなければ反例を与えよ。

G_1 は群であり、φ は準同型であるから、$\varphi\big\{G_1\big\}$ は単位元を持ち、演算について閉じていて、すべての元が逆元を持つ。よって、部分群である。

しかし、φ が全射ではないとき、$\forall x \in G\big[h \neq \varphi(x)\big]$ となる h がある。この h について、準同型からの G_1 の性質を引き継ぐことができないため $h^{-1}\varphi\big\{G_1\big\}h$ が $\varphi\big\{G_1\big\}$ にならないことがありうる。

実際、$G = S_3$、$H = S_4$、$G_1 = A_3$ とし、φ を包含写像 (要素自体はそのまんま) とすると、φ は準同型であるが、A_3 は S_4 の正規部分群ではない。

問 5 (参考書問 4.4)　群 G の正規部分群 H_1, H_2 について、$H_1 \cap H_2 = \{e\}$ であるとき、H_1 の元と H_2 の元は可換となることを示せ。

H_1 の元 x と H_2 の元 y について、$x^{-1} \in H_1$ であるから $yx^{-1}y^{-1} \in H_1$ が成り立つ。よって、$xyx^{-1}y^{-1} \in H_1$。

また、$y^{-1} \in H_2$ かつ $x^{-1}yx \in H_2$ より、$xyx^{-1}y^{-1} \in H_2$。

以上より、$xyx^{-1}y^{-1} \in H_1 \cap H_2$ だが、$H_1 \cap H_2 = \{e\}$ より、$xyx^{-1}y^{-1} = e$ だから、

$$\begin{aligned}e &= xyx^{-1}y^{-1}\\ eyx &= xyx^{-1}y^{-1}yx\\ yx &= xy\end{aligned}$$

よって、H_1 の元と H_2 の元は可換。

3.3 第二同型定理

定理 40 (第二同型定理) 群 G の部分群 S と正規部分群 N について、

$$(1)SN\text{は }G\text{の部分群である}$$
$$(2)S \rhd S \cap N$$
$$(3)\big(SN\big)/N \cong S/\big(S \cap N\big)$$

証明　S も N も単位元を含むため、$ee = e$ より $e \in SN$。また、$s_1, s_2 \in S$ と $n_1, n_2 \in N$ について

$$\begin{aligned} s_1n_1s_2n_2 &= s_1n_1s_2s_2^{-1}n_2's_2 && N\text{は正規部分群であるからこのような } n_2' \in N\text{が存在する} \\ \big(s_1n_1\big)\big(s_2n_2\big) &= s_1n_1n_2's_2 \\ \big(s_1n_1\big)\big(s_2n_2\big) &= s_1s_2n's_2^{-1}s_2 && N\text{は正規部分群であるからこのような } n' \in N\text{が存在する} \\ \big(s_1n_1\big)\big(s_2n_2\big) &= s_1s_2n' \end{aligned}$$

より SN において積は閉じている。また、$s \in S$ と $n \in N$ について、

$$\begin{aligned} (sn)^{-1} &= n^{-1}s^{-1} \\ (sn)^{-1} &= s^{-1}n'ss^{-1} \\ (sn)^{-1} &= s^{-1}n' \end{aligned}$$

よって、SN は逆元を含む。

以上より、SN は G の部分群である。

(2) は正規部分群の章の初めの部分で述べた。

写像 $\varphi : S \to \big(SN\big)/N$ を $\varphi(e) = N$ と $\varphi(s) = sN$ を満たすように定める。$\big(SN\big)/N$ は sN で尽くされるから分出公理からこのような写像は一般的な集合論の公理系のもとで存在する。

定義から明らかに φ は準同型である。また、$\mathrm{Ker}\varphi = S \cap N$ であるから第一同型定理より $\big(SN\big)/N \cong S/\big(S \cap N\big)$ が成り立つ。 □

一般射影線形群と特殊射影線形群が同型であることがすぐ示せる (英語 wikipedia から引いてきた情報で、確認してません)。

$$PGL\big(2,\mathbb{C}\big) := GL\big(2,\mathbb{C}\big)/\big(\mathbb{C}^{\times}I\big) \cong SL\big(2,\mathbb{C}\big)/\{\pm I\} =: PSL\big(2,\mathbb{C}\big)$$

3.4 第三同型定理

群 G と正規部分群 N について、

(1) 任意の G/N の部分群 S について、$S = K/N$ を満たし、$N \subset K \subset G$ を満たすような G の部分群 K が存在する。

(2) 任意の G/N の正規部分群 S について、$S = K/N$ を満たし、$N \subset K \subset G$ を満たすような G の正規部分群 K が存在する。

(3) $N \subset K \subset G$ を満たすような G の正規部分群 K について、$\big(G/N\big)/\big(K/N\big) \cong G/K$ が成り立つ。

証明　雑証明をする。

(1),(2) $K = G - \bigcup\big(G/N - S\big)$ とすればよい。

(3) 写像 $\varphi : G/N \to G/K$ を考えれば第一同型定理から示すことができる。 □

3.5 第四同型定理

対応定理 (correspondence theorem) とか束定理 (lattice theorem) とか言うらしい。重いので今回はパス。

3.6 指標

定義 41 (指標)　有限群 G から非零複素数の成す乗法群 $\mathbb{C}^\times$ への準同型 χ を群 G の指標という。

問 6 (参考書問 4.5(1))　χ の像は絶対値が 1 の複素数となることを示せ。

有限群の任意の元は位数が有限値であるから、$\forall x \in G\Big[\exists n\big[\chi(x)^n = 1\big]\Big]$ となる。

1 の n 乗根の絶対値は 1 であるから χ の像は絶対値が 1 の複素数となる。

定義 42 (単位指標)　像が $\{1\}$ である指標を単位指標といい、1 とかく。

問 7 (参考書問 4.5(2))　$\displaystyle\sum_{g\in G}\chi(g)$ が $\chi = 1$ のとき $\big|G\big|$、そうでなければ 0 となることを示せ。

G の任意の元 h について、$hG = G$。よって、$\chi\{G\} = \chi\{hG\}$ であるから、

$$\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(hg)$$
$$\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(h)\chi(g)$$
$$\sum_{g\in G}\chi(g) = \chi(h)\left(\sum_{g\in G}\chi(g)\right)$$

上式が恒等的に成り立つため、$\chi \neq 1$ ならば $\displaystyle\sum_{g\in G}\chi(g) = 0$ である。

一方、$\chi = 1$ の場合は自明。

指標は表現論でたくさんでてくるっぽいので物理やるひとはこれから (もしくはすでに) 出会うことになると思う。この自主ゼミでもあとで扱ってもいいかもしれない。

4 射影幾何について

4.1 ことわり

持ってる本に射影幾何のことが少し書いてあったので載せときます。J.H. シルヴァーマン /J. テイト 著、 足

立恒雄 / 木田雅成 / 小松啓一 / 田谷久雄　訳「楕円曲線論入門」ISBN978-4-621-06453-5

自分なりに噛み砕いたりしましたが、ほとんどの内容が被り、写しに近い状態です。

4.2 Fermat 方程式との関連

Fermat 方程式 1

$$x^N + y^N = 1$$

の有理数解を求める問題がある。

試しに有理数解を $\big(a/c, b/d\big)$ とする。ただし、どちらも既約分数で、分母が正であるとする。すると、

$$a^N d^N + b^N c^N = c^N d^N$$

より、$a^N d^N$ は c で割り切れることがわかる。しかし、a/c は既約分数であることから、d^N が c で割り切れる。

同様にして c^N が d で割り切れることがわかるので、分母が正であることから $c = d$。よって以下を得る。

$$a^N + b^N = c^N$$

これにより a, b, c が Fermat 方程式 2

$$X^N + Y^N = Z^N$$

の整数解を与えることがわかる。しかし、逆については、異なる整数解が同じ Fermat 方程式 1 の有理数解を与えることもあれば、そもそもある Fermat 方程式 2 の整数解は Fermat 方程式 1 の有理数解を導かない。

前者については、異なる 2 つの整数解が (a,b,c) と (ta,tb,tc) である場合に起きることであり、後者は N が奇数のときの整数解 $(-1,1,0)$ が (∞,∞) を導くことからわかる。

これらは同次座標と無限遠点に関連している。

4.3 同次座標と射影平面

さて、上記のような要請から代数的に射影平面を定義することができる。

定義 43 (代数的射影平面) 射影平面 $\mathbb{P}^2$ を、数の集合 Z と同値関係 $(a,b,c) \sim (a',b',c') \Leftrightarrow \exists t \neq 0\big[a = ta' \wedge b = tb' \wedge c = tc'\big]$ を用いて次のように定義する。

$$\mathbb{P}^2 := \Big\{(a,b,c) \in Z^3 \;\Big|\; (a,b,c) \neq \mathbf{0}\Big\} / \sim$$

t 倍して一致する点を同じとみなすわけである。このとき、点 (a,b,c) について a,b,c を同次座標という。

平面に限らず、射影空間を定義できる。

定義 44 (代数的射影空間) 射影空間 $\mathbb{P}^n$ を、数の集合 Z と同値関係 $\boldsymbol{p} \sim \boldsymbol{p}' \Leftrightarrow \exists t \neq 0\big[\boldsymbol{p} = t\boldsymbol{p}'\big]$ を用いて次のように定義する。

$$\mathbb{P}^n := \big\{\boldsymbol{a} \in Z^n \;\big|\; \boldsymbol{a} \neq \mathbf{0}\big\} / \sim$$

このとき、$\mathbb{P}^2$ における直線とは、定数 α, β, γ に対して $\alpha a + \beta b + \gamma c = 0$ を満たす点の集合をいう。

幾何学的には、平面上の 2 点が与えられれば直線がただ 1 つに決まる。同じように、平行しない 2 直線はただ 1 つの点を共有する。しかし、平行でないという条件ははずしたほうが便利である。こういった動機から、すべての直線が通る特別な点をつけたすことにする。

この特別な点はただ 1 つでいいだろうか？ためしに平行する 2 直線 L_1, L_2 が点 P を通るとしよう。また、平行する 2 直線 L_1', L_2' が点 P' を通ることにして、さらに L_1 とは平行でないとする。

このとき、L_1 と L_1' は交点 $Q = L_1 \cap L_1'$ を共有する。しかし、2 つの直線はただ 1 つの交点をもつはずだから $P \in L_1$ と $P' \in L_1'$ は異なる。

よって、特別な点は 1 つではすまないどころか、直線の方向の分だけ追加しなければならない。

こういった幾何学的動機から射影平面を定義すると、以下のようになる。

定義 45 (Euclid 平面) 通常の Euclid 平面を次のように定義する。

$$\mathbb{A}^2 = \big\{(x,y) \;\big|\; x,y\text{は数}\big\}$$

定義 46 (幾何的射影平面) 射影平面を次のように定義する。

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \Big\{\mathbb{A}^2\text{における方向の集合}\Big\}$$

方向とは、直線がもつもので、2 つの直線が平行なとき同じ方向をもつという。つまり、これは平行線の同値類ともいえる。このとき、$\mathbb{P}^2 - \mathbb{A}^2$ が無限遠点の集合となる。

こうしてついに、任意の 2 点を通る直線はただ 1 つに定まり、任意の 2 直線はただ 1 つの交点をもつことになり、平行線とそうでない 2 直線を特に区別する必要がなくなる。というより、$\mathbb{P}^2$ には平行線は存在しない。任意の 2 点を通る直線はただ 1 つに定まり、任意の 2 直線はただ 1 つの交点をもつことになるということを考えると、実は無限遠点の集合 L_∞ も直線であることがわかる。

さて、幾何的な射影平面と代数的な射影平面は同じと言っていいものなのだろうか？　それを検証するためには方向の集合とはなにか？ということを解析的に考える必要がある。

方向を考えるとき、これを原点を通る直線として考えることができる。なぜなら、任意の直線は原点を通る唯一の直線と平行 (同じ方向をもつ) からである。原点を通る直線は、ともに 0 になることがない数 A, B を用いて

$$Ay = Bx$$

と表せる。この式を用いて方向を数の対で表すと、(A, B) と (A', B') が同じ方向を表す必要十分条件は $\exists t \neq 0\Big[(A', B') = (tA, tB)\Big]$ で与えられる。

同じ方向を表すものは同じとみなすから、この条件を同値関係とした同値類が方向の集合となる。つまり、この方向の集合は射影直線上の点の集合 $\mathbb{P}$ である。

となると、射影平面 $\mathbb{P}^2$ は

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}$$

で表されることになるが、これは代数的定義とどう対応するのだろうか。

写像 $p : \mathbb{P}^2 \to \mathbb{A}^2 \cup \mathbb{P}$ を以下のように定める

$$\begin{aligned}
\big[a,b,c\big] &\longmapsto \left(\frac{a}{c}, \frac{b}{c}\right) \in \mathbb{A}(c \neq 0) \\
\big[a,b,0\big] &\longmapsto \big[a,b\big] \in \mathbb{P} \\
\big[x,y,1\big] &\longleftarrow\!\shortmid (x,y) \in \mathbb{A}^2 \\
\big[A,B,0\big] &\longleftarrow\!\shortmid \big[A,B\big] \in \mathbb{P}
\end{aligned}$$

このとき、写像 p は自明に全単射である。

たとえば、$c \neq 0$ ならば

$$[a,b,c] \;\longmapsto\; \left(\frac{a}{c},\frac{b}{c}\right) \;\longmapsto\; \left[\frac{a}{c},\frac{b}{c},1\right] = [a,b,c]$$

$c = 0$ ならば

$$[a,b,0] \;\longmapsto\; [a,b] \;\longmapsto\; [a,b,0]$$

要素が一対一に対応することはわかったが、幾何的な構造を保持するのだろうか。2 つの射影平面での直線は同じものを指すのだろうか。

例として、式

$$\alpha X + \beta Y + \gamma Z = 0$$

を満たす点の集合である直線 L を考える。

α, β はともに 0 であるとはないとする。L 内の点 $[a,b,c]$ は $c \neq 0$ のとき p によって直線 $\alpha x + \beta y + \gamma = 0$ 上の点 $\left(\frac{a}{c},\frac{b}{c}\right) \in \mathbb{A}^2$ に送られる。$c = 0$ のときは $[a,b] \in \mathbb{P}$ に送られるが、これは $\alpha a + \beta b = 0$ を満たし、直線 $\alpha x + \beta y + \gamma = 0$ と平行 (同じ方向をもつ) となっている。

α, β がともに 0 である場合、直線上の点 $[a,b,c]$ は $c = 0$ となるからすべて $[a,b] \in \mathbb{P}$ に送られ、像が $\mathbb{P}$ となるから送られた先では無限遠点からなる直線 L_∞ となる。

このように、代数的な定義も幾何的な定義も矛盾なく同一視できる。

4.4 射影平面上の曲線

定義 47 (代数曲線) アフィン平面 $\mathbb{A}^2$ 内において、方程式

$$f(x,y) = 0$$

で表される曲線を代数曲線という。

しかし、射影平面 $\mathbb{P}^2$ で曲線を定義しようとすると、同時座標は変数が 3 つあるから 3 変数の式を立てなくていけなくなる。さらに、同次座標は同じとみなさなければならない。そこで、

$$\forall t\big[F(a,b,c) = 0 \Rightarrow F(ta,tb,tc) = 0\big]$$

となる $F(a,b,c)$ に注目すると、これは同次多項式となる。つまり、

$$F(ta,tb,tc) = t^d F(a,b,c)$$

もしくは、F は次数が d の項の一次結合で表される (これらは同値)。

このような方程式で表される解の集合を $\mathbb{P}^2$ における曲線 C と定義する。

$$C : F(X,Y,Z) = 0$$

この曲線を幾何的に見てみよう。

$F(a,b,c)$ は同次式だから

$$\frac{1}{c^d} F\left(\frac{a}{c},\frac{b}{c},1\right) = F(a,b,c) = 0$$

ここで、$f(x,y) := F\left(\frac{a}{c},\frac{b}{c},1\right)$ と定義すると以下のように曲線 $C : F(a,b,c)$ 上の点を $\mathbb{A}^2 \cup \mathbb{P}$ に対応させ

ることを考える。$c \neq 0$ とすると、

$$\begin{array}{ccc} \Big\{[a,b,c] \in C \;\Big|\; c \neq 0\Big\} & \longrightarrow & \Big\{(x,y) \in \mathbb{A}^2 \;\Big|\; f\big(x,y\big) = 0\Big\} \\ [a,b,c] & \longmapsto & \left(\dfrac{a}{c},\dfrac{b}{c}\right) \end{array}$$

この写像が全単射であることはすぐに確かめられる。この $\mathbb{A}^2$ の曲線 $f\big(x,y\big) = 0$ を射影曲線 C のアフィン部分という。

$c = 0$ の点は無限遠点、つまり方向に写される。実際、この方向は曲線上で無限遠に極限をとったときの接戦の傾きに一致する。

射影幾何の勉強化ではないのでこのくらいにしておきます。

4.5 射影幾何の資料

時間がなくて紹介したり読み切ったりできなかったんですが、面白そうです。ということでリンクだけ丸投げします。

学問入門講座 射影の幾何学 西山享

代数幾何の源流を求めて 向井茂

射影幾何学とカント空間 田山令史

フィボナッチと射影幾何 吉永正彦

2 体問題の解析的解法を 264 年ぶりに発見してレファレンスのない論文を書いた！佐藤勲

2013 年度数学科リレー講座 4 日目 ～非ユークリッド幾何学の例 2 ～ ～射影幾何学～ 原 崇泰・平山 裕之

修士論文 射影平面における円錐曲線の性質について 高校数学における古典的教材の視点から 金濱千明

幾何学の精神 青空学園数学科

高校生のための現代数学講座「いろいろな幾何学」講義 (3) 坂井 秀隆　「作図と演算」