1　ベズーの定理

1.1　終結式

補題 1.1. UFD R 上の多項式 $f, g \in R[x] \setminus R$ に対して、以下は同値。

(i) $\exists h \in R[x] \setminus R \ s.t.\ h|f$ and $h|g$

(ii) $\exists A, B \in R[x] \ s.t.\ \deg A < \deg g,\ \deg B < \deg f$ and $Af + Bg = 0$

(証明). **(i) $\Longrightarrow$ (ii)**　仮定より $f = hB, g = -hA$ を満たす $A, B \in R[x]$ が存在する。すると明らかに $Af + Bg = 0$ となる。多項式の次数に関する部分も、$\deg h \neq 0$ から $\deg A = \deg g - \deg h < \deg g$ のようにして導かれる。

(ii) $\Longrightarrow$ (i)　仮定から、$Af = -Bg$ となる $A, B \in R[x]$ が存在する。g の全ての既約因子は Af を割り切る。このとき $\deg A < \deg g$ から、g の 1 次以上の既約因子であって f を割り切るものが有る。それを h とすれば (i) の条件を満たす。 ∎

定義 1.2. 多項式 $f, g \in k[t]$ を

$$f(t) = \sum_{0 \le i \le p} a_i t^i, g(t) = \sum_{0 \le j \le q} b_j t^j$$

とおく。これに対して以下のように $(p+q)$ 次正方行列[1]を定める。

$$M(f,g;t) = \begin{bmatrix} a_0 & a_1 & \cdots & a_q & & & \\ & a_0 & a_1 & \cdots & a_q & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_0 & a_1 & \cdots & a_q \\ b_0 & b_1 & \cdots & b_p & & & \\ & b_0 & b_1 & \cdots & b_p & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_0 & b_1 & \cdots & b_p \end{bmatrix}$$

この時、

$$\mathrm{Res}(f,g;t) = \det M(f,g;t)$$

を f, g の t に関する終結式と呼ぶ。

定理 1.3. $f, g \in R[t] \setminus R$ に対して、以下は同値。

1. $\exists h \in R[t] \ s.t.\ h|f$ and $h|g$
2. $\mathrm{Res}(f,g;t) = 0$

[1] シルベスター行列と呼ばれる。

(証明). 補題より、以下のような A, B があって $Af + Bg = 0$ を満たす。

$$A(t) = \sum_{0 \le j \le q-1} A_j t^j, B(t) = \sum_{0 \le i \le p-1} B_i t^i$$

さて、$Af + Bg = 0$ を計算してみると、以下のようになる。

$$\sum_{0 \le d \le p+q-1} \left\{ \sum_{i+j=d} (a_i A_j + b_j B_i) \right\} = 0$$

各項の係数を見ると以下が分かる。

$$\begin{aligned}
(1.) \iff \exists [A_j]_{0 \le j \le q-1}, [B_i]_{0 \le i \le p-1} \ s.t.& \\
a_0 A_0 + b_0 B_0 &= 0 \\
a_1 A_0 + b_1 B_0 + a_0 A_1 + b_0 B_1 &= 0 \\
&\vdots \\
a_{p+q-1} A_0 + \cdots + b_0 B_{p+q-1} &= 0
\end{aligned}$$

まとめて表せば次のようになる。

$$(1.) \iff$$
$$\exists [A_0, \ldots, A_{q-1}, B_0, \ldots, B_{p-1}] \in R^{p+q} \setminus \{\mathbf{0}\} \ s.t. \ [A_0, \ldots, A_{q-1}, B_0, \ldots, B_{p-1}] M(f, g; t) = \mathbf{0}$$

次元定理より $\mathrm{Res}(f, g; t) = 0$ と $\ker M(f, g; t) \neq \{\mathbf{0}\}$ は同値である [2)]。したがって (1.) $\iff$ (2.) が示された。

∎

命題 1.4.

$\forall f, g \in R[t] \backslash R, \ \exists A, B \in R[t] \ s.t. \ \deg A < \deg g, \deg B < \deg f$ and $Af + Bg = \mathrm{Res}(f, g; t)$

(証明). 各 $i = 2, 3, \ldots, p+q$ に対して、$M(f, g; t)$ の各 i 列目の t^i 倍を 1 列目に加える。すると次のようになる。

$$M' = \begin{bmatrix}
f & a_1 & \cdots & a_q & & & \\
tf & a_0 & a_1 & \cdots & a_q & & \\
 & & \ddots & \ddots & & \ddots & \\
t^{q-1} f & & & a_0 & a_1 & \cdots & a_q \\
g & b_1 & \cdots & b_p & & & \\
tg & b_0 & b_1 & \cdots & b_p & & \\
 & & \ddots & \ddots & & \ddots & \\
t^{p-1} g & & & b_0 & b_1 & \cdots & b_p
\end{bmatrix}$$

2) 次元定理より、$M(f, g; t)$ が正則ならば ker の次元は 0 であるから、ker の元は自明な物に限る

この操作は基本操作であるから、行列式を変えない。M' を第 1 列で余因子展開する。

$$
\begin{aligned}
\mathrm{Res}(f,g;t) &= \det M' \\
&= (fA_0 + tfA_1 + \cdots + t^{q-1}fA_{q-1}) + (gB_0 + tgB_1 + \cdots + t^{p-1}gB_{p-1}) \quad (A_i, B_j \in R) \\
&= (A_0 + tA_1 + \cdots + t^{q-1}A_{q-1})f + (B_0 + tB_1 + \cdots + t^{p-1}B_{p-1})g \\
&= Af + Bg
\end{aligned}
$$

∎

注意　$f, g \in k[x_1, \ldots, x_n, t]$ に対して、$\mathrm{Res}(f,g;t)$ は f, g が成すイデアルに属す。

1.1.1　例

$F = X^3 - YZ^2, G = X^2 - YZ \in k[X,Y,Z]$ を考える。$C := \mathcal{Z}_p(F), D := \mathcal{Z}_p(G) \in \mathbb{P}^2$ とおき、C と D の交点を求める。

$$
R(X,Z) := \mathrm{Res}(F,G;Y)^{3)} = \begin{bmatrix} -Z^3 & X^3 \\ -Z & Z^2 \end{bmatrix} = X^2 Z(X-Z)
$$

したがって C, D の交点は $X = 0, Z = 0, X - Z = 0$ の上に有る。

例えば $\mathcal{Z}(X) \cap C \cap D$ の属す交点を $P = (a:b:c)$ とする。$0 = F(a,b,c) = -bc^2, 0 = G(a,b,c) = -bc$ なので $bc = 0$ となるが、$(a:b:c) \neq (0:0:0)$ なので、$P = (0:0:1)$ または $P = (0:1:0)$ となる。同様に $Z = 0, X - Z = 0$ についても計算して、$C \cap D = \{(0:0:1), (0:1:0), (0:1:0)\}$ となる。

1.2　弱ベズーの定理

補題 1.5. k を無限体、斉次多項式 $F, G \in k[X,Y,Z]$ とし、$m := \deg F, n := \deg G$ と置く。この時、$R(X,Y) := \mathrm{Res}(F,G;Z)$ は mn 次斉次多項式

(証明). 主張は $R(tX,tY) = t^{mn} \cdot R(X,Y)$ と同値なので、これを考える。計算のため、

$$
\begin{aligned}
F &= \sum_{0 \le i \le m} a_i Z^{m-i} \\
G &= \sum_{0 \le j \le n} b_j Z^{n-j}
\end{aligned}
$$

とおく。この時、a_i, b_j はそれぞれ $k[X,Y]$ に属す i 次斉次多項式と j 次斉次多項式である。したがって、

$$
\begin{aligned}
a_i(tX,tY) &= t^i \cdot a_i(X,Y) \\
b_j(tX,tY) &= t^j \cdot b_j(X,Y)
\end{aligned}
$$

が成り立つ。

[3] Y についての射影化と解釈できる？

このことを使うと、$R(tX, tY)$ は次のようになっている。

$$R(tX,tY) = \begin{vmatrix} a_0 & ta_1 & \cdots & t^m a_m & & & \\ & a_0 & ta_1 & \cdots & t^m a_m & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_0 & ta_1 & \cdots & t^m a_m \\ b_0 & tb_1 & \cdots & t^n b_n & & & \\ & b_0 & tb_1 & \cdots & t^n b_n & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_0 & tb_1 & \cdots & t^n b_n \end{vmatrix}$$

この右辺の各行にそれぞれ $t^0 = 1, t^1 = t, \ldots, t^{n-1}, t^0, t^1, \ldots, t^{m-1}$ を掛け、左辺にもこれらをまとめて掛ける。

$$R(tX,tY) \cdot t^{0+1+\cdots+(m-1)+0+1+\cdots+(n-1)} = \begin{vmatrix} a_0 & ta_1 & \cdots & t^m a_m & & & \\ & ta_0 & t^2 a_1 & \cdots & t^{m+1} a_m & & \\ & & \ddots & \ddots & & \ddots & \\ & & & t^m a_0 & t^{m+1} a_1 & \cdots & t^{m+n-1} a_m \\ b_0 & tb_1 & \cdots & t^n b_n & & & \\ & tb_0 & t^2 b_1 & \cdots & t^{n+1} b_n & & \\ & & \ddots & \ddots & & \ddots & \\ & & & t^{m-1} b_0 & t^m b_1 & \cdots & t^{m+n-1} b_n \end{vmatrix}$$

右辺の各列はそれぞれ $t^0 = 1, t^1 = t, \ldots, t^{m+n-1}$ でくくり出し、$t^{\cdots} \cdot R(X,Y)$ の形にすることが出来る。

$$R(tX,tY) \cdot t^{\frac{m(m-1)}{2} + \frac{n(n-1)}{2}} = R(X,Y) \cdot t^{\frac{(m+n)(m+n-1)}{2}}$$

そして、

$$\frac{(m+n)(m+n-1)}{2} - \left(\frac{m(m-1)}{2} + \frac{n(n-1)}{2} \right) = mn$$

より、$R(tX,tY) = t^{mn} \cdot R(X,Y)$ が成り立つ。

$\blacksquare$

補題 1.6. k が無限体であるとき、斉次多項式 $F \in k[X,Y,Z] \setminus \{0\}$ に対して $\mathbb{P}^2_k \setminus \mathcal{Z}(F)$ は空でない。

(証明). 対偶を示す。

$$\forall P \in \mathbb{P}^2,\ F(P) = 0 \implies F = 0$$

$F \in (k[X,Y])[Z]$ と見て、

$$F = \sum_{i=0}^{d} G_i Z^{d-i}$$

と書く。ただし $d := \deg F$ で、G_i は $k[X, Y]$ に属す i 次斉次多項式である。

任意の $P = (a : b : c) \in \mathbb{P}_k^2$ に対して、$F(a, b, c) = 0$ であるとする。任意の $a, b \in k$ に対し、

$$f(Z) := F(a, b, Z) = \sum_{i=0}^{d} G_i(a, b) Z^{d-i}$$

は $k[Z]$ の関する多項式である。

任意の $c \in k \setminus \{0\}$ に対して $f(c) = 0$ となるから、

$$\#(\mathcal{Z}(f(Z))) = \#(k \setminus \{0\}) = \infty$$

となる。ここで $f(Z) \neq 0$ と仮定すると、

$$\#(\mathcal{Z}(f(Z))) \leq \deg f(Z) < \infty$$

となってしまうので $f(Z) = 0$ が分かる。

$$\forall i,\ \forall a, b \in k,\ G_i(a, b) = 0$$

さて、$G_i(X, Y)$ の $\mathbb{P}_k^1$ における零点集合 $\mathcal{Z}(G_i)$ を考える。G_i は任意の $a, b \in k$ に対して $G_i(a, b) = 0$ となるから、

$$\#(\mathcal{Z}_p(G_i)) = \#\mathbb{P}^1 = \infty$$

ここで $G_i \neq 0$ と仮定すると、斉次因数定理より

$$\#\mathcal{Z}_p(G_i) \leq \deg G_i = i < \infty$$

となってしまうので $G_i = 0$

合わせて、$F = 0$ が示された。

$\blacksquare$

なお、k が無限体でない時はこれは成り立たない。例えば $k = \mathbb{F}_2$ の時、$F(X, Y, Z) = (X - Y)(Y - Z)(Z - X)$ とおくと $F \neq 0$ にも関わらず $\mathcal{Z}(F) = \mathbb{P}_{\mathbb{F}_2}^2$ となる。

命題 1.7. (弱ベズーの定理) k を無限体、斉次多項式 $F, G \in k[X, Y, Z]$ により定まる曲線を $C := \mathcal{Z}(F), D := \mathcal{Z}(G) \in \mathbb{P}^2$ とし、$m := \deg F, n := \deg G$ とする。もし F, G に共通因子がないならば、

$$|C \cap D| \leq mn$$

が成り立つ。

(証明). $|C \cap D| > mn$ であると仮定し、矛盾を導く。$C \cap D \supset \{P_1, P_2, \ldots, P_{mn+1}\} (i \neq j \implies P_i \neq P_j)$ とおく。さらに、P_i と P_j を通る直線を L_{ij} とする。

k は無限体であるから、点 O として

$$O \notin C \cup D \cup \bigsqcup_{i \neq j} L_i j$$

となるものが取れる。この点 O が $(0:0:1)$ になるように $\mathbb{P}^2$ 全体を射影変換し、各 P_i も射影変換したものにラベルを貼り直しておく。

$F,G \in (k[X,Y])[Z]$ とみて、

$$F = \sum_{0\le i\le m} a_i Z^{m-i}, G = \sum_{0\le j\le n} b_j Z^{n-j}$$

とおく。ただし $a_i, b_j \in k[X,Y]$ であって、$\deg a_i = i, \deg b_j = j$ である。すると、$C,D \not\ni 0$ より $0 \neq F(O) = a_0, 0 \neq G(O) = b_0$ が成り立つ。したがって $R(X,Y) := \mathrm{Res}(F,G;Z)$ とおくと、$R(X,Y) \neq 0$ となる。

準備をする。$(a,b) \in k^2 \setminus \{(0,0)\}$ を取る。この時、以下が成り立つ。

$$\begin{aligned}
& \exists c \in k,\ (a:b:c) \in C \cap D \\
\iff & \exists c \in k,\ F(a,b,c) = G(a,b,c) = 0 \\
\implies & F(a,b,Z), G(a,b,Z) \text{ は共通因子をもつ。} \\
\iff & R(a,b) = \mathrm{Res}(F(a,b,Z), G(a,b,Z); Z) = 0 \\
\iff & (aY - bX) | R(X,Y)
\end{aligned}$$

ただし、3 行目の $\implies$ は k が代数的閉包の時には逆も成り立つ。また、4 行目は前の定理を、そして 5 行目は斉次因数定理を用いている。

$P_i = (a_i : b_i : c_i)$ とおくと、$P_i \in C \cap D$ だから、すでに示したとおり、

$$(a_i Y - b_i X) | R(X,Y)$$

ここで、L_{ij} の定義式は

$$\begin{vmatrix} a_i & b_i & c_i \\ a_j & b_j & c_j \\ X & Y & Z \end{vmatrix} = 0$$

$O \notin L_{ij}$ なので、

$$0 \neq \begin{vmatrix} a_i & b_i & c_i \\ a_j & b_j & c_j \\ 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix}$$

したがって $\{(a_i Y - b_i X)\}$ の各元は単数倍で一致しない。つまり $\{(a_i Y - b_i X)\}$ のそれぞれが異なる $R(X,Y)$ の 1 次因子である。ゆえに

$$\deg R(X,Y) \geq |\{(a_i Y - b_i X)\}| = mn + 1$$

となり、補題に反する。

∎

1.2.1 注意

体の拡大を考える。$\mathcal{Z}_k(F) := (a:b:c) \in k^3 : F(a,b,c) = 0$ とおくと、一般に斉次多項式 $F \in k[X,Y,Z]$ について

$$K/k :: \text{体の拡大} \implies \mathcal{Z}_K(F) \supset \mathcal{Z}_k(F)$$

例として $F = X^2 + Y^2 + Z^2$ と $\bar{\mathbb{Q}}/\mathbb{Q}$ を考えよ。

1.3 ベズーの定理

定理 1.8. (ベズーの定理) F, G, C, D, m, n の定義は今までと同じようにする。$C \cap D = \{P_1, P_2, \ldots, P_r\}$ とする。基礎体 k が代数的閉包であるとき、各 P_i について交点数 $I_R(C, D; P_i)$ が定義され、以下が成立する。

$$\sum_{i=1}^{r} I_R(C, D; P_i) = mn$$

(証明). まず、$P_i = (a_i : b_i : c_i) \in \mathbb{P}^2_k$ とおく。基礎体 k が代数的閉包であるから、$R(X, Y) = \mathrm{Res}(F, G; Z)$ は次のように一次式の積に分解される。

$$\begin{aligned} R(X, Y) &= \lambda \prod_{i=1}^{r} (a_i Y - b_i X)^{m_i} \\ mn &= \sum_{i=1}^{r} m_i \end{aligned}$$

ただし $\lambda \in k^\times, m_i \geq 1$ としている。点 P_i における交点数は $I_R(C, D; P_i) = m_i$ と定義される。定理の成立は明らか。

∎

1.3.1 例

$F = X^3 - YZ^2, G = X^2 - YZ$ をとり、交点数を求めてみる。$R(X, Y) = X^3 Y (Y - X)$ となるので、計算すると

$$L_{12} = \mathcal{Z}(X - Z), L_{23} = \mathcal{Z}(X - Y), L_{31} = \mathcal{Z}(X)$$

となる。取りうる点 $O \notin C \cap D \cap \bigcup L_{ij}$ として $O = (1 : 0 : 1)$ がある。これを $(0 : 0 : 1)$ に写す射影変換は、例えば

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

で定まる ϕ_A である。この射影変換で各交点と曲線を変換する。

$$\begin{aligned} F' &= F \circ A^{-1} = Z^3 - YX^2 \\ G' &= G \circ A^{-1} = Z^2 - YX \\ C' &= \mathcal{Z}(F') \\ D' &= \mathcal{Z}(G') \\ P_1' &= (0 : 1 : 0) \\ P_2' &= (1 : 1 : 1) \\ P_3' &= (1 : 0 : 0) \end{aligned}$$

改めて $R(X,Y)$ を計算すると、$R(X,Y) = \underbrace{X^3}_{P'_1}\underbrace{(X-Y)}_{P'_2}\underbrace{Y^2}_{P'_3}$ となる。よって、

$$\begin{aligned} I_R(C',D';P'_1) &= 3 \\ I_R(C',D';P'_2) &= 1 \\ I_R(C',D';P'_3) &= 2 \end{aligned}$$

と計算できる。

別のやり方としては $\mathrm{Res}(F,G;X)$ を計算しても良い。

$\mathrm{Res}(F,G;Z)$ なら、$\mathrm{Res}(F,G;Z)=0$ は $C\cap D$ を Z 軸上に射影した時の $C\cap D$ の各元が満たす方程式。これは終結式を計算する際に選ぶ変数の幾何学的意味。

1.3.2 (弱) ベズーの定理の応用

命題 1.9. $F,G \in k[X,Y,Z]$ を斉次多項式とし、$C := \mathcal{Z}_p(F), D := \mathcal{Z}_p(G), m := \deg F, n := \deg G$ とおく。G が既約多項式とすると、

$$\#(C\cap D) > mn$$

ならば $C \subset D$ である。さらに $m=n$ ならば $C=D$ で、$m>n$ ならば $C = C' \cup D$ を満たす $(m-n)$ 次曲線 C' が存在する。

(証明). 弱ベズーの定理から、F,G は共通因子を持つ。しかも G が既約なので、ある $F' \in k[X,Y,Z]$ が存在して $F = F'G$ が成立する。したがって $m \geq n$ となる。さらに詳しく、$m=n$ ならば $F' \in k^\times$ なので $C=D$ が成り立つ。$m>n$ なら $C' = \mathcal{Z}(F')$ とおけば $C = C'\cup D$ となる。

∎

1.4 線形系

自然数 d に対して、

$$\Lambda_d = \{F \in k[X,Y,Z] : F \text{ は斉次多項式であり } \deg F = d\} \cup \{0\}$$

これは k 上の線形空間となる。この Λ_d（または、付随する射影空間 $(\Lambda_d\setminus\{0\})/k^\times$）を次数 d の完備線形系と呼ぶ。また、これの部分空間は、単に線形系と呼ぶ。この時、$\dim \Lambda_d = \frac{1}{2}(d+1)(d+2)$ である。

次数 d の線形系 $\Lambda(\subset \Lambda_d)$ と $S \subset \mathbb{P}^2$ に対して、

$$\Lambda(S) := \{F \in \Lambda : \forall P,\ F(P) = 0\}$$

と定義する。

補題 1.10. $\Lambda(S)$ は線形空間で、

$$\dim \Lambda(S) \geq \dim \Lambda - \#S$$

さらに “=”の時、

$$S' \subset S \implies \dim \Lambda(S) = \dim \Lambda - \#S$$

(証明). もし $s := \#S = \infty$ なら $\Lambda(S) = \{0\}$ となるので $\#S < \infty$ とする。この時、選択公理を仮定せずとも S の元を整列できるので、$S = \{P_1, \ldots, P_s\}, P_i = (p_{i0} : p_{i1} : p_{i2})$ とおく。この設定の上で、次のように線形写像 ϕ_S を定義する。

$$
\begin{array}{rcl}
\phi_S : \Lambda & \to & k^{\oplus s} \\
F & \mapsto & (F(p_{i0}, p_{i1}, p_{i2}))_{1 \leq i \leq s}
\end{array}
$$

すると、この時 $\ker \phi_S = \Lambda(S)$ である。よって $\Lambda(S)$ は S の部分空間で、しかも

$$\dim \Lambda(S) \geq \dim \Lambda - s$$

が成り立つ。

さらに、$S' \subset S, s' := \#S'$ とするとき、以下の図式が可換となる。

$$
\begin{tikzcd}
\Lambda \arrow[r, "\phi_S"] \arrow[dr, "\phi_{S'}"'] & k^{\oplus s} \arrow[d, "\pi"] \\
& k^{\oplus s'}
\end{tikzcd}
$$

そして、以下の様になる。

$$
\begin{array}{rl}
& \dim \Lambda(S) = \dim \Lambda - s \\
\Longleftrightarrow & \phi_S :: \text{全射} \\
\Longrightarrow & \phi_{S'} :: \text{全射} \\
\Longleftrightarrow & \dim \Lambda(S') = \dim \Lambda - s'
\end{array}
$$

∎

命題 1.11. 与えられた $\frac{1}{2}d(d+3)$ 個の点を通る d 次の射影曲線が存在する。

(証明). 与えられた点の集合を S とする。仮定より $\#S = \frac{1}{2}d(d+3)$ である。補題より

$$\dim \Lambda_d(S) \geq \dim \Lambda_d - \#S = \frac{1}{2}(d+1)(d+2) - \frac{1}{2}d(d+3) = 1$$

よって $F\Lambda_d(S), F \neq 0$ となるものが存在する [4]。

∎

命題 1.12. 相異なる 5 点に対し、どの 3 点も一直線上に無いとする。この時、この 5 点を通る既約 2 次曲線がただ一つ存在する。

---

[4] $\dim \Lambda_d = 0$ ならば Λ_d が 1 点、すなわち 0 のみからなることを意味する。

(証明). すでに示した命題より、そのような二次曲線 $C := \mathcal{Z}(F)$ が存在する。この F が既約であることと、ただ一つであることを示す。

F が既約でないとすると、F は 1 次式の積に分解される。すると C は 2 直線の和集合ということになる。しかしこれは与えられた 5 点の内どの 3 点も一直線上に無いという仮定に反する。よって F は既約。

与えられた 5 点を $S = \{P_1, \dots, P_5\}$ とおく。$\dim \Lambda_d(S) \geq 2$ とすると、F と一次独立な $F' \in \Lambda_d(S)$ が取れる。F,F' は既約で一次独立だから、共通因子を持たない。したがって弱ベズーの定理が適用できて、

$$\#(\mathcal{Z}(F) \cap \mathcal{Z}(F')) \leq 2 \cdot 2 = 4$$

となる。しかし $\mathcal{Z}(F) \cap \mathcal{Z}(F') \supset S$ なので、矛盾する。よってこのような F' は存在せず、$\dim \Lambda_d(S) = 1$ である。

∎