1　アフィン曲線

1.1　アフィン空間

定義 1.1 (アフィン空間 (大雑把な定義))**.** 体 k について、

$$\mathbb{A}^n = \mathbb{A}^n_k = k^n$$

を k 上の n 次元アフィン空間 (Affine space) と呼ぶ。

1.2　アフィン曲線

定義 1.2. $f \in k[x, y] - 0$ に対して、その零点集合

$$C = \mathcal{Z}(f) = \{p \in \mathbb{A}^2 | f(p) = 0\}$$

をアフィン曲線と呼ぶ。この曲線 C を他には

$$C : f = 0 \text{ in } \mathbb{A}^2$$

と書く。

他に次の用語を導入する。

C の定義多項式:　f
C の定義方程式:　f=0

f の $k[x, y]$ に於ける既約分解を以下のようにする。

$$f = cf_1^{e_1} \cdots f_i^{e_i} \cdots f_n^{e_n}$$
$$(c \in k,\ f_i : k[x, y] \text{ の既約元},\ e_i \geq 1)$$

このとき、$C = \cup_{i=1}^n \mathcal{Z}(f_i)$ となる。

(証明).

$$\begin{aligned} & p \in C \\ \iff & f(p) = 0 \\ \iff & c \prod f_i(p) = 0 \end{aligned}$$

k は整域なので、

$$\begin{aligned} \iff & \exists i, f_i(p) = 0 \\ \iff & \exists i, p \in \mathcal{Z}(f_i) \\ \iff & p \in \cup_{i=1}^n \mathcal{Z}(f_i) \end{aligned}$$

■

このようにして得られた $C_i = \mathcal{Z}(f_i)$ 達を C の既約成分、$C = \cup C_i$ を C の既約分解と呼ぶ。また、f が既約多項式の時は C を既約曲線と呼ぶ。$\deg C = \deg f$ とし、$d = \deg f$ の時には C を d 次曲線と呼ぶ。

1.2.1 重複度

以下、$C : f = 0 \text{ in } \mathbb{A}^2$ とする。今、

$$f = \sum_{i,j} a_{ij} x^i y^j \ (a_{ij} \in k)$$

とする。$p_0 = (a, b) \in \mathbb{A}^2$ について、

$$x = (x - a) + a, y = (y - b) + b$$

を代入して $(x - a), (y - b)$ についてまとめると、f は次のように変形できる。

$$f_k = \sum_{i+j=k} c_{ij} (x - a)^i (y - b)^j$$
$$f = \sum_k f_k$$

この表示を f の p_0 におけるテイラー展開と呼ぶ。

1.2.2 偏微分

一般の体 k について偏微分を定義できる。ここでは $\mathbb{A}^n$ を考える。

定義 1.3 (偏微分)**.**

$$f = \sum_{i_1,\ldots,i_n} a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \in k[x_1, \ldots, x_n]$$

に対して、f の偏微分を、

$$\frac{\partial f}{\partial x_j} = \sum i_j \cdot a_{i_1 \ldots i_n} (x_1^{i_1} \cdots x^{i_j - 1} \cdots x_n^{i_n})$$

と定義する。

標数 0 の体については、次が成り立つ。

$$c_{i_1 \ldots i_n} = \frac{1}{i_1! \ldots i_n!} f_{x_{i_1}^{i_1} \ldots x_{i_n}^{i_n}}(p_0) = \frac{1}{i_1! \ldots i_n!} \frac{\partial^{i_1 + \cdots + i_n} f}{\partial x_{i_1}^{i_1} \ldots \partial x_{i_n}^{i_n}}(p_0)$$

ただし $c_{i_1 \ldots i_n}$ は f を $(x_1 - p_0^{(1)}), (x_2 - p_0^{(2)}), \ldots$ の多項式として表した時の係数であることに注意。特に $n = 2$ の時は次のよう。

$$c_{i_1 \ldots i_n} = \frac{1}{i!j!} f_{x^i y^j}(p_0) = \frac{1}{i!j!} \frac{\partial^{i+j} f}{\partial x^i \partial y^j}(p_0)$$

1.3 接線と特異点

点 $p_0 := (a, b)$ とおく。他の点は p で表す。

定義 1.4 (C の p に於ける重複度)**.** $m_p(C) = \min\{k : f_k(p) \neq 0\}$

$m = m_p(C)$ のとき、p を C の m 重点と呼ぶ。

再び 2 次元アフィン空間を考える。$f_0 = c_{00} = f(p)$ から、

$$m_p(C) > 0 \iff f(p) = 0 \iff p \in C$$

が成り立つ。

$p = (x, y) \in C$ とする。

$$f_1(p) = f_x(p_0)(x-a) + f_y(p_0)(y-b) = c_{01}(x-a) + c_{10}(y-b)$$

よって、

$$m_p(C) = 1 \iff f_1(p) \neq 0 \iff f_x(p) \neq 0 \text{ or } f_y(p) \neq 0$$

。

定義 1.5 (単純点と特異点)**.** $m_p(C) = 1$ の時 p を C の単純点、$m_p(C) > 1$ の時 p を C の特異点と呼ぶ。

単純点 p における C の接線は定義方程式 $f_1 = 0$ で定められる。これを

$$T_p(C) = \mathcal{Z}(f_1) \subset \mathbb{A}^2$$

と書く。

p が特異点の時はどうだろうか。以下では $m = m_p(C) \geq 2$ とする。このとき、

$$f = \underbrace{f_0 + \cdots + f_{m-1}}_{=0} + f_m + f_{m+1} + \ldots$$

となっている。実は k が代数閉体ならば、f_m は次のように x, y の一次式の積に分解される（後に示す）。つまり、

$$f_m(x) = \prod_{i=1}^{e} (\alpha_i(x-a) + \beta_i(y-b))^{m_i}$$

$$\alpha_i, \beta_i \in k,\ m_i \geq 1,\ \sum_{i=1}^{e} m_i = m$$

と表すことが出来る。α_i, β_i は単数倍で等しいものをまとめられるので、

$$\begin{vmatrix} \alpha_i & \beta_i \\ \alpha_j & \beta_j \end{vmatrix} \neq 0 \ (i \neq j)$$

として良い（？）。

この時、e 本の直線 $\alpha_i(x-a) + \beta_i(y-b) = 0$ を p における C の接線とする。また、m_i をその重複度と呼ぶ。

定義 1.6. $m = e$ (i.e. $\forall i, m_i = 1$) の時、p を C の通常特異点 (ordinary singular point) と呼ぶ。通常 2 重点を結節点と呼ぶ。

1.4　斉次多項式

k を体とする。$f \in k[X_1, \ldots, X_n] = k[\mathbb{X}]$ は、

$$f = \sum c_{i_0 \ldots i_n} X_0^{i_0} \ldots X_n^{i_n} = \sum c_{\mathbb{I}} \mathbb{X}^{\mathbb{I}} \ (\mathbb{I} = (i_0, \ldots, i_n))$$

と表される。$\mathbb{X}^{\mathbb{I}}$ を単項式、$|\mathbb{I}| = i_0 + \cdots + i_n$ をその次数と呼ぶ。$f(\neq 0)$ のに現れる次数が全て等しい時、f を斉次多項式と呼ぶ。

$$f = \sum_{d \geq 0} \left(\sum_{|\mathbb{I}|=d} c_{\mathbb{I}} \mathbb{X}^{\mathbb{I}} \right)$$

() 内を f_d と置けば $f = \sum_{d \geq 0} f_d$ となる。f_d はそれぞれ d 次の斉次多項式。そこで、この表示を f の斉次分解と呼ぶ。

次の補題は 2 次斉次多項式と 1 変数多項式が同型であることを言っている。

補題 1.7. $F(x, y) \in k[x, y]$ を d 次の斉次多項式とする。$f(t) = F(1, t) \in k[t]$ とおくと、以下が成り立つ。

$$F(x, y) = x^d f(\frac{y}{x})$$

(証明).

$$F(x, y) = \sum a_{ij} x^i y^j$$
$$f(t) = \sum a_{ij} t^j$$
$$f\left(\frac{y}{x}\right) = \sum a_{ij} x^{-j} y^j$$

$F(x, y)$ は d 次の斉次多項式だから $i + j = d$。よって、

$$x^d f\left(\frac{y}{x}\right) = \sum a_{ij} x^i y^j$$

∎

命題 1.8. $F(x, y) \in k[x, y]$ を d 次の斉次多項式とする。k が代数的閉包の時、$F(x, y)$ は次の形に分解される。

$$F(x, y) = \prod_{i=1}^{e} (\alpha_i (x - a) + \beta_i (y - b))^{d_i}$$
$$(\alpha_i, \beta_i \in k, \ d_i \geq 1, \ \sum_{i=1}^{e} d_i = d)$$

(証明). $f(t) = F(1, t)$ とおく。$\bar{k} = k$ だから、$f(t)$ は一次式に分解される。

$$f(t) = c \prod_{i=1}^{l} (t - \gamma_i)$$
$$(\gamma_i \in k, c \in k^{\times})$$

ただし $l=\deg f$。先ほどの補題より、以下の様にして命題が成り立つ。

$$\begin{aligned}
&F(x,y)\\
&\quad = x^d f\left(\frac{y}{x}\right)\\
&\quad = cx^d \prod_{i=1}^{l}\left(\frac{y}{x}-\gamma_i\right)\\
&\quad = cx^{d-l}\prod_{i=1}^{l}(y-\gamma_i x)\\
&\quad = (1\cdot x+0\cdot y)^{d-l}\prod_{i=1}^{l}\left(c^{\frac{1}{l}}y-c^{\frac{1}{l}}\gamma_i x\right)
\end{aligned}$$

∎

命題 1.9. $F(x,y)\in k[x,y]$ を d 次の斉次多項式とする。$(\lambda,\mu)\in k^2,(\lambda,\mu)\neq(0,0)$ に対して、

$$F(\lambda,\mu)=0 \iff (\lambda y-\mu x)|F(x,y)$$

(証明). ($\Longleftarrow$) は自明なので ($\Longrightarrow$) を示す。

λ,μ の両方が同時に 0 になることは無いので、$\lambda\neq 0$ とする。$\mu\neq 0$ としても以降の文字をただ置き換えれば証明が出来る。

$$\begin{aligned}
& F(\lambda,\mu)=0\\
\iff\ & \lambda^d F\left(1,\frac{\mu}{\lambda}\right)=0\\
\iff\ & f\left(\frac{\mu}{\lambda}\right)=0\\
\iff\ & \exists g\in k[t]\ s.t.\ f\left(\frac{\mu}{\lambda}\right)=\left(t-\frac{\mu}{\lambda}\right)g\left(\frac{\mu}{\lambda}\right)\\
& \text{以下、行頭には } \exists g \text{ があると思え。補題から次が成り立つ。}\\
\iff\ & F(x,y)=x^d f(t)=x^d\left(\frac{y}{x}-\frac{\mu}{\lambda}\right)g\left(\frac{y}{x}\right)\\
\iff\ & F(x,y)=\frac{1}{\lambda}(\lambda y-\mu x)\cdot x^{d-1}g\left(\frac{y}{x}\right)
\end{aligned}$$

ここで、$\deg g=\deg f-1\leq \deg F-1=d-1$。よって $x^{d-1}g\left(\frac{y}{x}\right)\in k[x,y]$ (x の指数は全て 0 以上)。

∎

1.5 直線との交点数

$C=\mathcal{Z}(f), f\in k[x,y]\setminus\{0\}, p=(a,b)\in C$ とする。p を通る直線 L に対して、C と L との p における交点数 $i(C,L;p)$ を以下のとおり定める。

定義 1.10. 直線 L のパラメータ表示を以下のようにおく。

$$L:(x,y)=(a+\lambda t,b+\mu t)$$
$$(\lambda,\mu\in k,(\lambda,\mu)\neq(0,0))$$

このとき、交点数 $i(C,L;p)$ は、次のよう。

$$i(C,L;p) := \mathrm{ord}_t\, f(a+\lambda t, b+\mu t) := \max\{d : t^d | f(a+\lambda t, b+\mu t)\}$$

$p \in L$ なので $i(C,L;p) \geq 1$。さらに、この定義は L のパラメータ表示によらないことが示せる。

命題 1.11. C を曲線、L を点 $p \in C$ を通る直線とする。

$$i(C,L;p) \geq m_p(C)$$

特に、次が成り立つ。

$$i(C,L;p) > m_p(C) \iff \text{L は p に於ける C の接線の一つ}$$

(証明). 座標全体を平行移動して $p=(0,0)$ とする。このとき L のパラメータ表示は、

$$\begin{gathered} L : (x,y) = (\lambda t, \mu t) \\ (\lambda, \mu \in k, (\lambda,\mu) \neq (0,0)) \end{gathered}$$

となる。$m := m_p(C)$ とおくと、p における f のテイラー展開は以下の様。

$$f = \sum_{k \geq m} \left(\sum_{i+j=k} c_{ij} x^i y^j \right)$$

L 上の点では、

$$\begin{aligned} f &= \sum_{k \geq m} x^k \left(\sum_{i+j=k} c_{ij} \lambda^i \mu^j \right) \\ &= \sum_{k \geq m} x^k f_k(\lambda, \mu) \end{aligned}$$

$k \geq m$ から、$i(C,L;p) \geq m$。さらに、$i(C,L;p) > m \iff f_m(\lambda,\mu) = 0$ だから、斉次因数定理より次が成り立つ。

$$\begin{aligned} & f_m(\lambda,\mu) = 0 \\ \iff & (\lambda y - \mu x) | f_m(\lambda,\mu) \\ \iff & \mathcal{Z}(\lambda y - \mu x) \text{ は } f \text{ の接線の一つ（接線の定義を見よ）} \\ \iff & L \text{ は } f \text{ の接線の一つ} \end{aligned}$$

∎

2 射影曲線

2.1 射影空間

$\mathbb{A}^{n+1} \setminus \{0\}$ において、$\mathbf{a} = (a_0, \ldots, a_n)$, $\mathbf{b} = (b_0, \ldots, b_n)$ に対し、以下のように同値関係を入れる (同値関係であることは自明)。

$$\mathbf{a} \sim \mathbf{b} \iff \exists \lambda \in k^{\times}\ s.t.\ \lambda \mathbf{a} = \mathbf{b}$$

そこで、n 次元射影空間を以下で定める。

$$\mathbb{P}^n := (\mathbb{A}^{n+1} \setminus \{0\})/\sim$$

点 $A \in \mathbb{P}^n$ に対し、その代表元として $\mathbf{a} = (a_0, \ldots, a_n)$ をとる。このとき、$A = (a_0 : \cdots : a_n)$ と表し、a_i 達を A の斉次座標と呼ぶ。全ての a_i が 0 になる点は無い。

各 $i = 0, 1, \ldots, n$ に対し、

$$\sqcup_i := \{(a_0 : a_1 : \cdots : a_n) | a_i \neq 0\} \subset \mathbb{P}^n$$

このとき、$\mathbb{P}^n = \bigcup_{i=0}^n \sqcup_i$ となる。この $\{\sqcup_i\}_{i=0}^n$ をアフィン開被覆と呼ぶ。

補題 2.1. 各 i に対し、ϕ_i を

$$\begin{aligned} \phi_i : \sqcup_i &\to \mathbb{A}^n \\ (a_0 : \cdots : a_i : \cdots : a_n) &\mapsto (a_0/a_i, \ldots, a_n/a_i) \end{aligned}$$

とおく。これは全単射で、

$$\begin{aligned} \psi_i : \mathbb{A}^n &\to \sqcup_i \\ (a_0, \ldots, a_n) &\mapsto (a_0 : \cdots : \underset{i\text{ 番目の要素}}{1} : \cdots : a_n) \end{aligned}$$

がその逆写像である。

(証明). 全単射の定義にしたがって調べれば良い。 ∎

零点集合 $\mathcal{Z}(X_i) = \{(a_0 : a_1 : \cdots : a_n) | a_i = 0\}$ を $\sqcup_i$ の無限遠超平面と言う。これはそれぞれ $\sqcup_i$ の補集合で、$\mathbb{A}^n \simeq \sqcup_i = \mathbb{P}^n \setminus \mathcal{Z}(X_i)$ が成り立つ。零点集合はぞれぞれ $\sqcup_i$ と無限遠で交わる。

2.2 射影曲線

定義 2.2 (射影曲線)**.** 体 k 上の斉次多項式 $F \in k[X, Y, Z]$ について、以下で定まる集合を射影曲線と呼ぶ。

$$C := \mathcal{Z}(F) = \{p \in \mathbb{P}^2 : F(p) = 0\}$$

$\deg C := \deg F = d$ を C の次数と呼び、また、C を d 次曲線と呼ぶ。

これは well-defined である。なぜなら任意の点 $p \in \mathbb{P}^2$ と、任意の $\lambda \in k^\times$ について、$F(\lambda p) = (\lambda^{\deg F})F(p)$ だからである。したがって $F(p) = 0$ の解集合は点 p の斉次座標のとり方によらない。これは F が斉次多項式であることから成り立つ。逆に、このように射影曲線 C が well-defined であるためには F は斉次多項式でなくてはならない。

命題 2.3. 2 点 $\mathbf{a}, \mathbf{b} \in \mathbb{P}^2$（ただし $\mathbf{a} \neq \mathbf{b}$）を通る直線はただ一つであり、[1]その定義多項式 $\bar{F}$ は以下で与えられる。

$$\bar{F} = \begin{vmatrix} X & Y & Z \\ a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{vmatrix}$$

ここで $\mathbf{a} = (a_0 : a_1 : a_2), \mathbf{b} = (b_0 : b_1 : b_2)$ とした。

[1] $\lambda\mathbf{a}, \mu\mathbf{b}$ も同じ 2 点を表すということを考えれば、これは自明ではない。

(証明). 主張に有る $\bar{F}$ は $\mathbf{a}$ か $\mathbf{b}$ を代入すると同じ行を 2 つもつ行列式になるから、0 になる。また、$\bar{F}$ は一次斉次多項式である。したがって $\bar{F}$ は $\mathbf{a}, \mathbf{b}$ を通る直線の定義多項式の一つである。以下、このような直線がただ一つであることを示す。

直線の定義多項式 F は 1 次斉次多項式だから、$F(X,Y,Z) = \alpha X + \beta Y + \gamma Z$ のように表される。写像 ε を以下で定義する。

$$\begin{aligned} \varepsilon : \{\text{k 上の 1 次斉次多項式全体}\} &\to k^2 \\ F &\mapsto \begin{bmatrix} F(\mathbf{a}) \\ F(\mathbf{b}) \end{bmatrix} \end{aligned}$$

ε で F を送った先が $\mathbf{0}$ であれば F は 2 点 $\mathbf{a}, \mathbf{b}$ を通る。すなわち、定義多項式は $\ker \varepsilon$ の元である。すでに述べたように、$\bar{F} \in \ker \varepsilon$ となっている。

ε で F を送った先をもう少し考えると、次のようになる。

$$F \mapsto \begin{bmatrix} F(\mathbf{a}) \\ F(\mathbf{b}) \end{bmatrix} = \begin{bmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$$

$\mathbf{a} \neq \mathbf{b}$ から、$\operatorname{rank} \begin{bmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{bmatrix} = 2$ である。したがって $\dim \ker \varepsilon = 3 - 2 = 1$ となる。つまり、$\ker \varepsilon$ は $\bar{F}$ を有る一つのパラメータで変化させたもの全体。実際、$\bar{F}$ を $k^\times$ 倍したものも $\ker \varepsilon$ の元である[2)]。以上の議論から、$\ker \varepsilon$ の元は $k^\times$ 倍を除いて一意。したがって、2 点 $\mathbf{a}, \mathbf{b}$ を結ぶ直線 $\mathcal{Z}(F)$ は一意。

∎

定義 2.4. $\mathbb{P}^2$ 内の直線全体のなす集合を $\check{\mathbb{P}}^2$ と書く。

$$\check{\mathbb{P}}^2 := \{\mathcal{Z}(\alpha X + \beta Y + \gamma Z) : (\alpha, \beta, \gamma) \in k^3 \setminus \{0\}\}$$

これを双対射影空間と呼ぶ。

実際、$\check{\mathbb{P}}^2 \ni \mathcal{Z}(\alpha X + \beta Y + \gamma Z) \mapsto (\alpha : \beta : \gamma) \in \mathbb{P}^2$ は全単射。

問。素数 p について $\mathbb{P}^2_{\mathbb{F}_p}$ に含まれる直線は何本か。

2.3 多項式の斉次化・非斉次化

以下では k を体、$\mathbb{X} = (X_0, \ldots, X_n)$[3)], $\mathbb{Y} = (Y_1, \ldots, Y_n)$[4)] とおく。

定義 2.5 (非斉次化)**.**

$$\begin{aligned} \alpha : k[\mathbb{X}] &\to k[\mathbb{Y}] \\ F(\mathbb{X}) &\mapsto F(1, Y_1, \ldots, Y_n) \end{aligned}$$

これを X_0 に関する非斉次化と呼ぶ。

これは代入なので環の準同型写像である。

---

2) $\bar{F}$ の X の係数だけ変化させても $\ker \varepsilon$ の元になる、といった可能性を排除するための議論だった。

3) $(n+1)$ 個の不定元。

4) n 個の不定元。

定義 2.6 (斉次化)**.**

$$
\begin{aligned}
\beta : k[\mathbb{Y}] &\to k[\mathbb{X}] \\
f(\mathbb{Y}) &\mapsto X_0^{\deg f} f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right)
\end{aligned}
$$

これを X_0 に関する斉次化と呼ぶ。

これは次に示すように準同型写像でない。

命題 2.7. $f \in k[\mathbb{Y}]$ に対して $\beta(f)$ は斉次多項式。さらに、f の斉次分解を $f = \sum_{k=0}^{d} f_k(\mathbb{X})$ とした時

$$
\beta(f)(\mathbb{X}) = \sum_{k=0}^{d} X_0^{d-k} f_k(\mathbb{X}')
$$

となる。ただし $d := \deg f$, $\mathbb{X}' = (X_1, \ldots, X_n)$[5] とした。

(証明). 「さらに、」以降の主張から前半の主張は明らか。$f(\mathbb{Y}) = \sum_{0 \le k \le d} \sum_{|\mathbb{I}|=k} c_{\mathbb{I}} \mathbb{Y}^{\mathbb{I}}$ とする。$\beta(f)$ は次のようになる。

$$
\begin{aligned}
\beta(f)(\mathbb{X}) &= X_0^d \sum_{k=0}^{d} \left(\sum_{|\mathbb{I}|=k} c_{\mathbb{I}} \left(\frac{X_1}{X_0}\right)^{i_1} \cdots \left(\frac{X_n}{X_0}\right)^{i_n} \right) \\
&= \sum_{k=0}^{d} \left(\sum_{|\mathbb{I}|=k} X_0^{d-|\mathbb{I}|} \cdot c_{\mathbb{I}} \mathbb{X}'^{\mathbb{I}} \right) \\
&= \sum_{k=0}^{d} X_0^{d-k} f_k(\mathbb{X}')
\end{aligned}
$$

∎

2.3.1 α, β の関係

証明は略すが、$\alpha(\beta(f)) = f$ が成り立つ。しかし $\beta(\alpha(F)) = F$ は一般に成立しない。

補題 2.8. 斉次多項式 $F \in k[\mathbb{X}]$ に対し、ある $e \ge 0$ が存在して次式が成り立つ。

$$
F(\mathbb{X}) = X_0^e \cdot \beta(\alpha(F(\mathbb{X})))
$$

(証明). $d := \deg F$ として、

$$
F(\mathbb{X}) = \sum_{|\mathbb{I}|=d} c_{\mathbb{I}} X_0^{i_0} \cdots X_n^{i_n}
$$

と表せる。この時、

$$
\alpha(F)(\mathbb{X}) = \sum_{|\mathbb{I}|=d} c_{\mathbb{I}} 1^{i_0} X_1^{i_1} \cdots X_n^{i_n}
$$

5) X_0 を $\mathbb{X}$ から消した。

明らかに $\deg\alpha(F) \le d$ なので、この差を e と置く。つまり $\deg\alpha(F) = d - e$ とする。すると $d - \sum_{1\le j\le n} i_j = i_0$ より、以下のようになる。

$$
\begin{aligned}
X_0^e \cdot \beta(\alpha(F(\mathbb{X})))& \\
&= X_0^e \left(X_0^{d-e} \sum_{|\mathbb{I}|=d} c_{\mathbb{I}} \left(\frac{X_1}{X_0}\right)^{i_1} \cdots \left(\frac{X_n}{X_0}\right)^{i_n} \right) \\
&= \left(\sum_{|\mathbb{I}|=d} c_{\mathbb{I}} X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n} \right) \\
&= F(\mathbb{X})
\end{aligned}
$$

等号が成立するのは $i_0 = 0 \implies c_{\mathbb{I}} = 0$ の時。

∎

2.4 アフィン曲線の射影化

定義 2.9. 多項式 $f \in k[x,y]$ によって定まるアフィン曲線 $C := \mathcal{Z}_a(f) \subset \mathbb{A}^2$ に対し、$\mathcal{Z}_p(\beta(f)) \subset \mathbb{P}^2$ を C の射影化と呼ぶ。ただし、β は Z に関する斉次化、すなわち $\beta : f(x,y) \mapsto Z^{\deg f} f\left(\frac{X}{Z}, \frac{Y}{Z}\right)$ である。

定義 2.10. 斉次多項式 $F \in k[X,Y,Z]$ により定まる射影曲線 $C := zerosp(F)$ に対し、$zerosa(\alpha(F)) \subset \mathbb{A}^2$ をその $Z \neq 0$ のアフィン部分と呼ぶ。ただし α は Z に関する非斉次化、すなわち $\alpha : F(X,Y,Z) \mapsto F(x,y,1)$ である。

アフィン部分には他に X に関するもの、Y に関するものがある。

命題 2.11. 斉次多項式 $F \in k[X,Y,Z]$ に対して、

$$zerosp(F) \cap \sqcup_c = \psi_c(zerosa(\alpha(F)))$$

ただし $\sqcup_c$ と ψ_c は補題 1 で定義したものである。

(証明). $\sqcup_c \ni p = (a : b : 1)$ をとる。

$$
\begin{aligned}
& p \in zerosp(F) \\
\iff & F(a,b,1) = 0 \\
\iff & \alpha(F)(a,b) = 0 \\
\iff & \phi_c(p) \in zerosa(\alpha(F)) \\
\iff & p \in \psi_c(zerosa(\alpha(F)))
\end{aligned}
$$

∎

補題 2.12. $f \in k[x,y]$ に対して、

$$\overline{\psi(zerosa(f))} = zerosp(\beta(f))$$

ただし、左辺は Zariski 位相での閉包である。

この補題は利用しないので証明もしない。

2.5 特異点

定義 2.13 (射影曲線の特異点)**.** 斉次多項式 F により定まる射影曲線 $C := zerosp(F)$ において、$p \in C$ が C の特異点であるとは、p を含むアフィン開被覆における C のアフィン部分が p に於いて特異点を持つことと定める。

したがって、$p \in C$ が C の特異点であるとは、$p \in \sqcup_i$ のとき、アフィン部分 $zerosa(\alpha(F))$ が $\phi_i(p)$ に於いて特異点を持つことである。

補題 2.14. p が $zerosp(F)$ の特異点である。$\iff F_X(p) = F_Y(p) = F_Z(p) = 0$ [6)]

(証明). $\sqcup_c \ni p = (a : b : 1)$ をとり、$f := \alpha(F) = F(x, y, 1)$ とおく。$C := zerosa(f)$ が特異点 p を持つとは、f の斉次分解 $\{f_k\}$ について $m_p(C) = \min\{k : f_k(p) = 0\} > 1$ ということ。したがって、

$$f_x(a, b) = f_y(a, b) = 0$$

ここで $F_X(x, y, 1) = f_x(x, y)$, $F_Y(x, y, 1) = f_y(x, y)$ だったから、

$$F_X(a, b, 1) = F_Y(a, b, 1) = 0$$

が成り立つ。これは特異点の定義と同値。

さらにここでオイラーの公式

$$XF_X + YF_Y + ZF_Z = (\deg F)F$$

を用いると、

$$a \cdot F_X(p) + b \cdot F_Y(p) + 1 \cdot F_Z(p) = (\deg F)F(p) = 0$$

だから、$F_Z(a, b, 1) = 0$ も出る。逆に、$F_X(p) = F_Y(p) = F_Z(p) = 0$ は明らかに $F_X(p) = F_Y(p) = 0$ を含む。

∎

2.6 接線

定義 2.15 (射影曲線の接線)**.** 射影曲線 C の点 $p \in C$ における接線を、p を含むアフィン開被覆の $\phi(p)$ における接線の射影化として定める。

補題 2.16. 斉次多項式 F について、$p \in C := zerosp(F)$ が C の非特異点（単純点）であるとき、p における C の接線は次式で定まる。

$$F_X(p)X + F_Y(p)Y + F_Z(p)Z = 0$$

(証明). $\sqcup_c \ni p = (a : b : 1)$ をとり、$f := \alpha(F)$ とする。C の $\sqcup_c$ におけるアフィン部分 $zerosa(f)$ への $\phi_c(p)$ に於ける接線は次で定まる。

$$f_x(a, b)(x - a) + f_y(a, b)(y - b) = 0$$

f の定義より、

$$F_X(a, b, 1)(x - a) + F_Y(a, b, 1)(y - b) = 0$$

---

6) F_X は斉次多項式 F を X について偏微分したものである。F_Y なども同様。

これを斉次化すれば

$$F_X(a,b,1)(X-aZ)+F_Y(a,b,1)(Y-bZ)=0$$

オイラーの公式を用いれば、結論が得られる。 ∎

例として $F=XZ-Y^2$ を取ると、これの点 $p=(a:b:c)$ における接線は $cX-2bY+aZ=0$ となる。標数 2 の体に於いては、$cX+aZ=0$ となり、これは点 $(0:1:0)$ を常に通る。接線が定点を通る曲線を strange 曲線と呼ぶが、これは以下の定理の通り、かなり限られた状況のものしか無い。

定理 2.17 (Samuel)**.** 非特異射影曲線で strange のものは、直線（自明な場合）か標数 2 の 2 次曲線に限る。

証明は Hartshorn, IV, Theorem 3.9 にある。

2.7 直線との交点数

$A=(a_0:a_1:a_2), B=(b_0:b_1:b_2)\in\mathbb{P}^2$ とおく。A,B を通る直線 L のパラメータ表示として、

$$L:(X:Y:Z)=sA+tB=(sa_0+tb_0:sa_1+tb_1:sa_2+tb_2)$$

をとる。斉次多項式 F に L のパラメータ表示を代入して得られる多項式を

$$\Phi(s,t)=F(sa_0+tb_0,sa_1+tb_1,sa_2+tb_2)$$

と置く。

L 上の点 P は $(s_0,t_0)\neq(0,0)$ によって $P=s_0A+t_0B$ と表される。このとき、$C\cap L$ に於ける C と L の交点数を

$$I(C,L;P)=\max\{m:(s_0t-t_0s)^m|\Phi(s,t)\}$$

で定義する。これは well-defined である。

■問 射影曲線 $C=\mathcal{Z}(F)$ と直線 L に対して、$L\not\subset C$ とする。体 k が代数的閉包ならば、

$$\sum_{P\in C\cap L}I(C,L;P)=\deg F$$

となる。これを示せ。ヒントはテイラー展開。

命題 2.18. $P\in\mathbb{P}^2$ を含むアフィン開被覆での、C と L のアフィン部分を C_0,L_0 とすれば

$$I(C,L;P)=i(C_0,L_0;\phi(P))$$

が成立する。

(証明). **定義の確認** 適当に座標変換して $L=zerosp(Y),P=(0:0:1)$ とする。$f(x,y)=\alpha(F)=F(x,y,1)$ と置けば、$C:=zerosp(F)$ と L のアフィン部分は

$$C_0:=zerosa(f),L_0:=zerosa(y)$$

である。L_0 のパラメータ表示は $(x,y)=(t,0)$ とすれば、$P=(0:0:1)$ に対応する点は $t=0$ で与えられる。アフィン曲線の交点数の定義より、$i(C_0,L_0;\phi(P))=\max\{k:t^k|f(t,0)\}$

■F の分解　ここで、F を Y の多項式として整理する。つまり、F を多項式環 $k[X,Z][Y]$ の元として見る。$d := \deg F$ とおき、$F_i \in k[X,Z]$ を i 次斉次多項式とする。

$$F = F_d(X,Z) + F_{d-1}(X,Z)Y + \cdots + F_0(X,Z)Y^d$$

すると、

$$f(t,0) = F(t,0,1) = F_d(t,1)$$

となるから、

$$i(C_0, L_0; \phi(P)) = \max\{k : t^k | F_d(t,1)\}$$

となる。

■Φ の表示を見る　一方 L のパラメータ表示として $(X,Y,Z) = (t:0:s)$ をとれば、$P(=(0:0:1))$ に対応するのは $(s_0,t_0) = (1,0)$ が与える点。したがって $\Phi(s,t) = F(t,0,s) = F_d(t,s)$ となり、あとは単なる計算で結論が得られる。

$$\begin{aligned}
&I(C,L;P)\\
&= \max\{m : (s_0t - t_0s)^m | \Phi(s,t)\}\\
&= \max\{k : t^k | F_d(t,s)\}\\
&= \max\{k : t^k | F_d(t,1)\}\\
&= i(C_0, L_0; \phi(P))
\end{aligned}$$

■

2.8　射影変換

　正則行列 $A \in GL(3,k)$ による線形写像

$$\begin{aligned}
A : \mathbb{A}^3 &\to \mathbb{A}^3\\
\begin{bmatrix} x\\ y\\ z \end{bmatrix} &\mapsto A \begin{bmatrix} x\\ y\\ z \end{bmatrix}
\end{aligned}$$

が定まる。任意の $\lambda \in k$ に対し、

$$\lambda \begin{bmatrix} x\\ y\\ z \end{bmatrix} \mapsto A \begin{bmatrix} \lambda x\\ \lambda y\\ \lambda z \end{bmatrix}$$

となるので、正則行列 A によって

$$\begin{aligned}
\phi_A : \mathbb{P}^2 &\to \mathbb{P}^2\\
(a:b:c) &\mapsto \psi_Z(A \cdot {}^t[a\ b\ c])
\end{aligned}$$

が定まる。これは well-defined である。

　明らかに以下が成り立つ。

$$\begin{aligned}
\phi_E &= id_{\mathbb{P}^2}\\
\phi_{AB} &= \phi_A \circ \phi_B \ (\forall A, B \in GL(3,k))
\end{aligned}$$

下の式から正則行列 A について ϕ_A は全単射となり、

$$(\phi_A)^{-1} = \phi_{A^{-1}}$$

となる。特に射影変換全体

$$PGL(2,k) := \{\phi_A : A \in GL(3,k)\}$$

は群を成す。これを射影変換群と呼ぶ。

補題 2.19. 正則行列 A が定める射影変換 ϕ_A を考える。3 点 $P_1, P_2, P_3 \in \mathbb{P}^2$ に対して、P_1, P_2, P_3 が同一直線上に有ることと $\phi_A(P_1), \phi_A(P_2), \phi_A(P_2)$ が同一直線上に有ることは同値。

(証明). $P_i = (p_{i0} : p_{i1} : p_{i2}) \in \mathbb{P}^2$ に対して $\mathbf{p}_i = {}^t[p_{i0}, p_{i1}, p_{i2}]$ とおく。この時、アフィン空間に於いて 2 点を通る直線は行列式で書ける、という命題から、以下のように証明が出来る。

$$\begin{aligned}
& P_1, P_2, P_3 \text{ が同一直線上に有る} \\
\iff & \det[\mathbf{p}_1\ \mathbf{p}_2\ \mathbf{p}_3] = 0 \\
\iff & (\det A)(\det[\mathbf{p}_1\ \mathbf{p}_2\ \mathbf{p}_3]) = 0 \\
\iff & \det[A\mathbf{p}_1\ A\mathbf{p}_2\ A\mathbf{p}_3] = 0 \\
\iff & \phi_A(P_1), \phi_A(P_2), \phi_A(P_2) \text{ が同一直線上に有る}
\end{aligned}$$

∎

命題 2.20 (Four Points Lemma)**.** 4 点 $P_1, P_2, P_3, P_4 \in \mathbb{P}^2$ はどの 3 点も同一直線上にないとする。$O_1 = (1:0:0), O_2 = (0:1:0), O_3 = (0:0:1), O_4 = (1:1:1)$ とするとき、

$$\phi(P_i) = O_i \ (i = 1, 2, 3, 4)$$

となる射影変換はただ一つ存在する。

(証明). P_i と $\mathbf{p}_i$ と前のように定める。$B' = [\mathbf{p}_1\ \mathbf{p}_2\ \mathbf{p}_3]$ と置けば、P_i はどの 3 つも同一直線上にないので B' は正則。$B = (B')^{-1}$ と置くと、

$$B[\mathbf{p}_1\ \mathbf{p}_2\ \mathbf{p}_3] = BB' = E$$

なので、$i = 1, 2, 3$ について $\phi_B(P_i) = O_i$ となる。

$\phi(P_4)$ を考える。そのために

$$B\mathbf{p}_4 = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix} = \sum_{i=1}^{4} (\lambda_i \cdot B\mathbf{p}_i) \tag{1}$$

とする。この時、$\lambda_i \neq 0$ である。実際、例えば λ_1 とすると

$$\phi_B(P_2) = O_2,\ \phi_B(P_3) = O_3,\ \phi_B(P_4) = (0 : \lambda_2 : \lambda_3)$$

となり、これらは直線 $X = 0$ 上にある。補題よりこれは 3 点 P_2, P_3, P_4 が同一直線上に有ることと同値であり、したがって仮定に反する。そこで正則行列 A を

$$A = \begin{bmatrix} 1/\lambda_1 & & \\ & 1/\lambda_2 & \\ & & 1/\lambda_3 \end{bmatrix} B$$

と置けば、ϕ_A が求める射影変換。実際に計算してみると、

$$\begin{aligned}\phi_A(P_1) &= \psi_c(A\mathbf{p}_1) = (\lambda_1 : 0 : 0) = O_1\\ \phi_A(P_2) &= \psi_c(A\mathbf{p}_2) = (0 : \lambda_2 : 0) = O_2\\ \phi_A(P_3) &= \psi_c(A\mathbf{p}_3) = (0 : 0 : \lambda_3) = O_3\\ \phi_A(P_4) &= \psi_c(A\mathbf{p}_4) = (1 : 1 : 1) = O_4\end{aligned}$$

もしも $A' \in GL(3,k)$ によって $\phi_{A'}(P_i) = O_i$ が成立したとする。この時ある定数 $\alpha \in k^\times$ によって $A = \alpha A'$ となることを示す。この時、0 でない定数 μ_i によって、

$$A'[\mathbf{p}_1\ \mathbf{p}_2\ \mathbf{p}_3\ \mathbf{p}_4] = \begin{bmatrix}\mu_1 & 0 & 0 & \mu_4\\ 0 & \mu_2 & 0 & \mu_4\\ 0 & 0 & \mu_3 & \mu_4\end{bmatrix}$$

と書ける。

$$\frac{1}{\mu_4}A'\mathbf{p}_4 = \frac{1}{\mu_1}A'\mathbf{p}_1 + \frac{1}{\mu_2}A'\mathbf{p}_2 + \frac{1}{\mu_3}A'\mathbf{p}_3$$

また、式 (1) の左に $\frac{1}{\mu_4}A'B'$ を掛けると、

$$\frac{1}{\mu_4}A'\mathbf{p}_4 = \frac{\lambda_1}{\mu_4}A'\mathbf{p}_1 + \frac{\lambda_2}{\mu_4}A'\mathbf{p}_2 + \frac{\lambda_3}{\mu_4}A'\mathbf{p}_3$$

仮定より、$A'\mathbf{p}_i$ は基底になっているから、係数が一致して

$$\frac{\lambda_i}{\mu_4} = \frac{1}{\mu_i} \quad (i = 1, 2, 3, 4)$$

が成立する。したがって、

$$\mu_4 A[\mathbf{p}_1\ \mathbf{p}_2\ \mathbf{p}_3] = A'[\mathbf{p}_1\ \mathbf{p}_2\ \mathbf{p}_3]$$

と、$B' = [\mathbf{p}_1\ \mathbf{p}_2\ \mathbf{p}_3]$ が正則であることから、

$$\mu_4 A = A'$$

が成立する。よって $\phi_A = \phi_{A'}$ である。これで一意性が言えた。

∎

補題 2.21. 斉次多項式 $F \in k[X,Y,Z]$ により定まる射影曲線 $C := zerosp(F)$ を ϕ_A で写した像は

$$\phi_A(C) = \mathcal{Z}(F \circ A^{-1})$$

さらに $\deg(\phi_A(C)) = \deg C$ である。

(証明). 任意の $P \in \mathbb{P}^2$ に対して、以下のようになる。

$$P \in \phi_A(C) \iff \phi_A^{-1}(P) \in C \iff F(A^{-1}P) = 0 \iff P \in \mathcal{Z}(F \circ A^{-1})$$

さらに、一般に行列 M について $\deg F \geq \deg(F \circ M)$ であることを用いて後半を証明する。

$$\underbrace{\deg(F \circ A^{-1}) \leq \deg F}_{M=A^{-1}} = \underbrace{\deg(F \circ A^{-1} \circ A) \leq \deg(F \circ A^{-1})}_{M=A}$$

∎

定義 2.22. F, G を斉次多項式とし、$C := \mathcal{Z}(F), D := \mathcal{Z}(G)$ とおく。C, D が射影同値であるとは、ある $A \in GL(3,k), \lambda \in k^\times$ によって

$$G = \lambda F \circ A^{-1}$$

となることである。

■**注意**　k が代数的閉包であるときは $\lambda' = \lambda^{1/\deg F} \in k$ となるので、$F \circ (\lambda' A)^{-1} = \lambda F \circ A^{-1}$ が成り立つ。つまり、定数 λ を行列 A に纏めることが出来る。

■**例: 平行移動**　アフィン空間における平行移動 $(x, y) \mapsto (x-a, y-b)$ を、射影化 ψ_Z によって射影変換にする。

$$\phi_A : (X : Y : Z) \mapsto (X - aZ : Y - bZ : Z)$$

このような射影変換 ϕ_A を与える正則行列 A を求めよう。

Four Points Lemma より、射影変換は 4 点の写った先が決まれば一意に定まる。4 点として $(0,0), (0,1), (1,0), (1,1)$ をとり、これを射影化してから ϕ_A で写す。するとその値から、

$$A = \begin{bmatrix} 1 & & -a \\ & 1 & -b \\ & & 1 \end{bmatrix}$$

と定まる。

3　ベズーの定理

3.1　終結式

補題 3.1. 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) $\implies$ (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) $\implies$ (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 3.2. 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[7]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 3.3. $f,g \in R[t] \setminus R$ に対して、以下は同値。

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

(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[8]。したがって $(1.) \iff (2.)$ が示された。

∎

[7] シルベスター行列と呼ばれる。

[8] 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

命題 3.4.

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

(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。

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

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。

3.1.1　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。

$$R(X, Z) := \mathrm{Res}(F, G; Y)^{9)} = \begin{bmatrix} -Z^3 & X^3 \\ -Z & Z^2 \end{bmatrix} = X^2 Z(X - Z)$$

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。

3.2　弱ベズーの定理

補題 3.5. 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

9) Y についての射影化と解釈できる？

(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、

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

とおく。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、

$$a_i(tX,tY)=t^i\cdot a_i(X,Y)$$
$$b_j(tX,tY)=t^j\cdot b_j(X,Y)$$

が成り立つ。

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 $t^0=1, t^1=t,\dots,t^{n-1}, t^0, t^1,\dots,t^{m-1}$ を掛け、左辺にもこれらをまとめて掛ける。

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

右辺の各列はそれぞれ $t^0=1, t^1=t,\dots,t^{m+n-1}$ 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。

∎

補題 3.6. 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 $P = (a:b:c) \in \mathbb{P}^2_k$ 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 $\mathbb{P}^1_k$ 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。

∎

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 $\mathcal{Z}(F) = \mathbb{P}^2_{\mathbb{F}_2}$ となる。

命題 3.7. (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。$C\cap D\supset\{P_1,P_2,\dots,P_{mn+1}\}(i\neq j\implies P_i\neq P_j)$ 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

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

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、

$$F=\sum_{0\leq i\leq m}a_iZ^{m-i},G=\sum_{0\leq j\leq n}b_jZ^{n-j}$$

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、

$$(a_iY-b_iX)|R(X,Y)$$

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

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

となり、補題に反する。

∎

3.2.1　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。

3.3　ベズーの定理

定理 3.8. (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、$P_i = (a_i : b_i : c_i) \in \mathbb{P}_k^2$ 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。

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

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。

∎

3.3.1　例

$F = X^3 - YZ^2, G = X^2 - YZ$ をとり、交点数を求めてみる。$R(X,Y) = X^3Y(Y - X)$ 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。

3.3.2 (弱) ベズーの定理の応用

命題 3.9. $F, G \in k[X,Y,Z]$ 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。

∎

3.4 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 3.10. $\Lambda(S)$ 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。

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

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。

$$\begin{aligned} & \dim \Lambda(S) = \dim \Lambda - s \\ \iff & \phi_S :: \text{全射} \\ \implies & \phi_{S'} :: \text{全射} \\ \iff & \dim \Lambda(S') = \dim \Lambda - s' \end{aligned}$$

∎

命題 3.11. 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[10]。

∎

10) $\dim \Lambda_d = 0$ 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。

命題 3.12. 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。

(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 $S = \{P_1, \ldots, P_5\}$ 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。

∎

4 平面 3 次曲線

4.1 結合律のための準備

平面 3 次曲線の点にアーベル群の構造が入ることを示す中で、特に結合律が成り立つことは自明でない。その証明のために準備する。

補題 4.1. 相異なる 5 点 $P_1, \ldots, P_5 \in \mathbb{P}^2$ が、どの 4 点も一直線上にないならば、その 5 点を通る 2 次曲線は高々 1 つ。

(証明). 相異なる 2 次曲線 C, C' で $P_1, \ldots, P_5$ を通るものがあると仮定する。このとき $F, F' \in \Lambda_2(\{P_1, \ldots, P_5\})$ によって $C = \mathcal{Z}(F), C' = \mathcal{Z}(F')$ と表せる。$C \cap C' \supset \{P_1, \ldots, P_5\}$ が成り立つから弱ベズーの定理より、F, F' は共通因子を持つ。$C \neq C'$ から、共通因子は 1 次式。

$F = GH, F' = GH'$ が成り立つように $G, H, H' \in \Lambda_1$ を取る。$L := \mathcal{Z}(G), M := \mathcal{Z}(H), M' := \mathcal{Z}(H')$ とおくと、$C \neq C'$ より $M \neq M'$。

$$C = L \cup M, C' = L \cup M'$$

となるから、

$$\begin{aligned} C \cap C' &= (L \cup M) \cap (L \cup M') \\ &= L \cup (M \cap M') \\ &\in \{P_1, \ldots, P_5\} \end{aligned}$$

M, M' は直線で $M \neq M'$ だから $M \cap M'$ は高々 1 点。よって直線 L 上に 4 点があり、仮定に矛盾する。∎

さらに、定理の証明には以下が必要である。証明はこの二つの補題の証明は演習問題。

補題 4.2. k を代数的閉体だとする。$F \in k[X, Y, Z] \setminus \{0\}$ によって $C := \mathcal{Z}(F)$ とおくと、

$$|C| = \infty$$

補題 4.3. k を無限体とする。$L \subset \mathbb{P}^2$ が直線なら、

$$|L| = \infty$$

こちらは証明が難しい。

命題 4.4. k を無限体とする。$F \in \Lambda_2[X, Y, Z], C := \mathcal{Z}(F)$ とおく。このとき、

$$|C| \neq 0 \implies |C| = \infty$$

定理 4.5. k を無限体とする。相異なる 8 点 $P_1, \ldots, P_8 \in \mathbb{P}_k^2$ はどの 4 点も一直線上に無く、どの 7 点も既約 2 次曲線上に無いとする。この時、

$$\dim \Lambda_3(\{P_1, \ldots, P_8\}) = 2$$

となる。

(証明). 前章の補題から

$$\dim \Lambda_3(\{P_1, \ldots, P_8\}) \geq 10 - 8 = 2$$

が分かる。以下では $\leq$ も成り立つことを示す。そのために与えられた 8 点の分布の仕方によって場合分けをする。

場合 I

8 点 $P_1, \ldots, P_8$ が以下を満たす場合。

1. どの 3 点も 1 つの直線上にない
2. どの 6 点も 1 つの 2 次曲線上にない

もしある 6 点が可約な 1 つの 2 次曲線上にあるとすると、それらの点は 2 本の直線に載っている。したがって条件 2. と条件 1. とを満たす 8 点は「どの 6 点も 1 つの既約 2 次曲線上にない」も満たす。

$\dim \Lambda_3(\{P_1, \ldots, P_8\}) \geq 3$ として矛盾を導く。直線 L を 2 点 P_1, P_2 を結ぶものとする（L の定義式も L と表す）。このとき条件 1. より $P_1, \ldots, P_8 \notin L$ となる。互いに異なる 2 点 P_9, P_{10} を $L \setminus \{P_1, P_2\}$ から取る。前章の補題より、

$$\dim \Lambda_3(\{P_1, \ldots, P_8\} \cup \{P_9, P_{10}\}) \geq 3 - 2 = 1$$

となるので、$F \in \Lambda_3(\{P_1, \ldots, P_{10}\}) \setminus \{0\}$ が取れる。

曲線 $C := \mathcal{Z}(F)$ を考える。$C \cap L \subset \{P_1, P_2, P_9, P_{10}\}$ となるから、

$$|C \cap L| \geq 4 > \deg C \cdot \deg L = 3$$

したがって弱ベズーの定理より、F と L は共通因子を持つ。L は既約なので、ある $G \in \Lambda_2$ が存在して $F = L \cdot G$ となる。さらに $P_3, \ldots, P_8 \notin L$ から $P_3, \ldots, P_8 \notin \mathcal{Z}(G)$ が分かる。これは条件 2. に反する。

条件 1., 2. と $\dim \Lambda_3(\{P_1, \ldots, P_8\}) \geq 3$ を仮定して条件 2. と矛盾したが、条件 1., 2. を満たす点の分布は存在する。よって $\dim \Lambda_3(\{P_1, \ldots, P_8\}) \geq 3$ は否定され、

$$\text{条件 1., 2.} \implies \dim \Lambda_3(\{P_1, \ldots, P_8\}) = 2$$

が成立する。

場合 II

3 点 $P_1, \ldots, P_3$ が直線 L 上にある場合。

$P_9 \in L \setminus \{P_1, P_2, P_3\}$ を取る。前章の補題より、

$$\dim \Lambda_3(\{P_1, \ldots, P_8, P_9\}) \geq 10 - 9 = 1$$

となるので、$F \in \Lambda_3(\{P_1, \ldots, P_9\}) \setminus \{0\}$ が取れる。そして場合 I と同様に $G \in \Lambda_2$ が存在して $F = L \cdot G$ となる。ここで定義の前提より $P_4, \ldots, P_8 \notin L$ であった。したがって $P_4, \ldots, P_8 \in \mathcal{Z}(G)$。つまり

$$G \in \Lambda_3(\{P_4, \ldots, P_8\})$$

F は $\Lambda_3(\{P_1, \ldots, P_9\}) \setminus \{0\}$ から任意に取り、また $\{P_1, P_2, P_3, P_9\} \subset L$ だから

$$\Lambda_3(\{P_1, \ldots, P_9\}) = L \cdot \Lambda_3(\{P_4, \ldots, P_8\}) \subset \Lambda_3$$

補題 4.1 より $\dim \Lambda_3(\{P_4, \ldots, P_8\}) = 1$。ゆえに

$$\Lambda_3(\{P_1, \ldots, P_9\}) = 1$$

よって

$$\dim \Lambda_3(\{P_1, \ldots, P_8\}) \leq 2$$

場合 III

6 点 $P_1, \ldots, P_6$ が既約 2 次曲線 $D := \mathcal{Z}(G)$ 上にある場合。

$P_9 \in D \setminus \{P_1, \ldots, P_6\}$ を取る。前章の補題より、

$$\dim \Lambda_3(\{P_1, \ldots, P_8, P_9\}) \geq 10 - 9 = 1$$

となるので、$F \in \Lambda_3(\{P_1, \ldots, P_9\}) \setminus \{0\}$ が取れる。そして場合 I と同様に $L \in \Lambda_1$ が存在して $F = L \cdot G$ となる。ここで定義の前提より $P_7, P_8 \notin D$ であった。したがって $P_7, P_8 \in L$。つまり

$$L \in \Lambda_1(\{P_7, P_8\})$$

F は $\Lambda_3(\{P_1, \ldots, P_9\}) \setminus \{0\}$ から任意に取り、また $\{P_1, P_2, P_3, P_9\} \subset L$ だから

$$\Lambda_3(\{P_1, \ldots, P_9\}) = G \cdot \Lambda_3(\{P_7, P_8\}) \subset \Lambda_3$$

$\dim \Lambda_1(\{P_7, P_8\}) = 1$ であるから、

$$\Lambda_3(\{P_1, \ldots, P_9\}) = 1$$

よって

$$\dim \Lambda_3(\{P_1, \ldots, P_8\}) \leq 2$$

∎

系 4.6. k を無限体とする。$C_1, C_2 \subset \mathbb{P}^2$ を共通成分を持たない 3 次曲線とし、

$$C_1 \cap C_2 = \{P_1, \ldots, P_9\}$$

とおく。この時、任意の 3 次曲線 $C \subset \mathbb{P}^2$ について

$$P_1, \ldots, P_8 \in C \implies P_9 \in C$$

が成り立つ。

(証明). $\{P_1,\dots,P_8\}$ はどの 4 点も一直線上に無い。実際、ある 4 点は直線 L 上に会ったとすると、$|C_i \cap L| \geq 4 > 3\cdot 1 = 3 (i=1,2)$ となり、弱ベズーの定理から $L \subset C_i$。よって $L \subset (C_1 \cap C_2)$ となり、C_1 と C_2 が共通因子を持たないことに反する。同様にして、どの 7 点も 1 つの既約 2 次曲線上に無い。ゆえに $\{P_1,\dots,P_8\}$ は定理の仮定を満たす。したがって $\dim \Lambda_3(\{P_1,\dots,P_8\}) = 2$。

$C_i = \mathcal{Z}(F_i)$ とすると、$C_1 \neq C_2$ より、F_1, F_2 は一次独立である。さらに

$$F_1, F_2 \in \Lambda_3(\{P_1,\dots,P_8\}), \dim \Lambda_3(\{P_1,\dots,P_8\}) = 2$$

であるから、F_1, F_2 は $\Lambda_3(\{P_1,\dots,P_8\})$ の基底となっている。よってある斉次多項式 $F \in \Lambda_3(\{P_1,\dots,P_8\})$ によって 3 次曲線 $C = \mathcal{Z}(F)$ と置くと、

$$F = aF_1 + bF_2 (a, b \in k)$$

の様になる。このことから直ちに

$$C \supset C_1 \cap C_2$$

が分かる。 ∎

4.2 平面 3 次曲線にはアーベル群の構造が入る

定義 4.7. 3 次斉次多項式 $F \in k[X,Y,Z] \setminus \{0\}$ によって $C := \mathcal{Z}(F)$ とおく。この C に対し、以下のように二項演算 $* : C \times C \to C$ を定める。2 点 $P, Q \in C$ を取る。

- $P \neq Q$ の時
  - $\#(\overline{PQ} \cap C) = 3$ の時、$P * Q = (\overline{PQ} \cap C) \setminus \{P, Q\}$
  - $\#(\overline{PQ} \cap C) = 2$ の時、
    - $\overline{PQ}$ が P に於いて C に接する時、$P * Q = P$
    - $\overline{PQ}$ が Q に於いて C に接する時、$P * Q = Q$
- $P = Q$ の時、L を P に於ける C の接線として、
  - $\#(L \cap C) = 2$ の時、$P * Q = (L \cap C) \setminus \{P\}$
  - $\#(L \cap C) = 1$ の時、$P * Q = P$

場合分けが上の定義で尽くされることと $P * Q$ が存在することはベズーの定理による。

注意 4.8. 定義から明らかに $P * Q = Q * P$。更に $R = P * Q$ の時、$P * R = R * Q = Q$ が成立する。$Q * R$ でも同様。

さて、点 $O \in C$ を 1 つ取って固定する。その上で二項演算 $+$ を以下のように定める。

$$\begin{aligned} + : C \times C &\to C \\ (P, Q) &\mapsto (P * Q) * O \end{aligned}$$

これがアーベル群を作る。

定理 4.9. $(C, +)$ はアーベル群を成す。

(証明). 以下を順に示す。ただし $P, Q, R \in C$ とする。

1. $P+Q=Q+P$(可換律の成立)
2. O が単位元 (単位元の存在)
3. P の逆元は $P*(O*O)$(逆元の存在)
4. $(P+Q)+R=P+(Q+R)$(結合律の成立)

(1.) 注意 4.8 より、

$$P+Q=(P*Q)*O=(Q*P)*O=Q+P$$

(2.) $R:=P*O$ と置くと、注意 4.8 より $R*O=P$。よって

$$P+O=(P*O)*O=R*O=P$$

(3.) $O:=O*O$ とおく。さらに $Q:=P*O'=P*(O*O)$ とすれば、

$$P*Q=O',O'*O=O$$

ゆえに

$$P+Q=(P*Q)*O=O'*O=O$$

すなわち $-P=Q=P*(O*O)$。

(4.) まず $P\neq Q$ として証明する。

$$(P+Q)+R=(((P*Q)*O)*R)*O$$
$$P+(Q+R)=(P*((Q*R)*O))*O$$

なので示したいことは $(P+Q)*R=P*(Q+R)$ と同値。

直線 L_1,L_2,L_3 と M_1,M_2,M_3 を以下のように定義する。

$$L_1=\overline{P,Q},\ L_2=\overline{Q+R,O},\ L_3=\overline{P+Q,R}$$
$$M_1=\overline{Q,R},\ M_2=\overline{O,P+Q},\ M_3=\overline{P,Q+R}$$

そしてこれらを用いて 3 次曲線 L,M を

$$L:=L_1\cup L_2\cup L_3, M:=M_1\cup M_2\cup M_3$$

定義し、これらの交点を考える。

$$\mathcal{J}:=\{P,Q,R,O,P*Q,Q*R,P+Q,Q+R\}$$
$$T:=L_3\cap M_3$$

と定義すると明らかに $L\cap M=\mathcal{J}\cup\{T\}$ である。この時、$J\subset C$ なので、系 4.6 より $T\in C$ が成り立つ。ここで $C\cap L=\{(P+Q)*R\}\cup\mathcal{J}$ であるから、$T=(P+Q)*R$。同様に $C\cap M$ を考えて、$T=P*(Q+R)$。

次に $P=Q$ として証明する。これは二項演算子 $+$ の連続性を用い、$P\to Q$ の極限として結合律を証明する。まず写像 $\phi_1,\phi_2:C^3\to C$ を以下で定義する。

$$\phi_1(P,Q,R)=(P+Q)+R \tag{2}$$
$$\phi_2(P,Q,R)=P+(Q+R) \tag{3}$$

さらに

$$E=\{(P,Q,R)\in C^3:\phi_1(P,Q,R)=\phi_2(P,Q,R)\}$$

これは Zariski 位相で閉。示したいことは $E = C^3$ と表現できる。一方、

$$\sqcup = \{(P, Q, R) \in C^3 : \#(\mathcal{J} \cup \{T\}) = 9\}$$

（ただし $\mathcal{J}$ は上で定めたもの）とおくと、$\sqcup$ は C^3 の空ではない開集合となる。C^3(既約) の中で $\sqcup$ が稠密であることは前半の証明から分かる。

$$\sqcup \subset E \subset C^3$$

なので、閉包 $\bar{\sqcup}$ が $\sqcup$ を含む最小の閉集合であることより、

$$C^3 = \bar{\sqcup} \subset E \subset C^3$$

すなわち $C^3 = E$。 ∎

例 4.10. $y^2 + y = x^3 - x \in \mathbb{A}^2$ を考え、

$$F(X, Y, Z) = Y^2Z + YZ^2 - X^3 + XZ^2$$

として $C := \mathcal{Z}(F)$ を調べる。

補題 4.11. 体 k に於いて $C \subset \mathbb{P}^2$ が特異点を持つ $\iff p := \mathrm{char}(k) = 37$

(証明). $P \in C$ が特異点である必要十分条件は $F_X(P) = F_Y(P) = F_Z(P) = 0$ である。

$$\begin{aligned} F_X &= -3X^2 + Z^2 \\ F_Y &= 2YZ + Z^2 \\ F_Z &= Y^2 + 2YZ + 2XZ \end{aligned}$$

$P = (a : b : c) \in C$ が特異点だとする。$p = 37$ である時に $P = (5 : 18 : 1), (32 : 18 : 1)$ が特異点であることを示す。 ∎

$O = (0 : 1 : 0) \in C$ として群構造を調べる。

補題 4.12. $O * O = O$ が成り立つ。特に任意の $Q \in C$ に対し $-Q = Q * O, Q = (-Q) * O$ が成立し、さらに $P * Q = -(P + Q)$。

(証明). 点 O における C の接線は $Z = 0$ であり、これを満たす C 上の点は O しかない。したがって $O * O = O$ が成り立つ。任意の楕円曲線と $Z = 0$ と $O = (0 : 1 : 0)$ の交点は O だけであり、しかも O における接線は必ず $Z = 0$ となるから、これは任意の楕円曲線で成り立つ。

また、$R := Q * O$ とおくと

$$\begin{aligned} & R = Q * O \\ \iff & Q * R = O \\ \iff & (Q * R) * O = O * O \\ \iff & Q + R = O \\ \iff & R = -Q = Q * O \end{aligned}$$

となる。このことから更に $(P * Q) * O = P + Q = -(P * Q)$ が分かる。 ∎

補題 4.13. $Q = (a : b : 1)$ に対して $-Q = Q * O = (a : -b - 1 : 1)$