現代数学への流れ　第13回

Projective Geometry

$k = \mathbb{C}$

$\mathbb{P}^n_{\mathbb{C}} = (\mathbb{C}^{n+1} - \{0\}) / \sim$ 　　$v \sim w \iff \exists \lambda \in k^\times = k - \{0\}$ s.t. $\lambda v = w$

これを n-次元 射影空間 という. $(x_0, \cdots, x_n) \in \mathbb{C}^{n+1} - \{0\}$ に対して その同値類を $[x_0 : \cdots : x_n]$ と書く.

$\mathbb{P}^n(\mathbb{Q}) = (\mathbb{Q}^{n+1} - \{0\}) / \sim_{\mathbb{Q}}$ 　　$v \sim_{\mathbb{Q}} w \iff \exists \lambda \in \mathbb{Q}^\times$ s.t. $v = \lambda v$

$\cap$ 　　で 有理点 の集合

$\mathbb{P}^n_{\mathbb{C}}(\mathbb{Q})$

U_i 全 $= \{ [x_0 : \cdots : x_n] \in \mathbb{P}^n_{\mathbb{C}} \mid x_i \neq 0 \}$

このとき.

$$\begin{array}{ccc} U_i & \to & \mathbb{A}^n_{\mathbb{C}} = \mathbb{C}^n \\ \cup & & \cup \\ (x_0 : \cdots : x_i : \cdots : x_n) & \mapsto & \left(\frac{x_0}{x_i}, \cdots, \overset{\vee}{\frac{x_i}{x_i}}, \cdots, \frac{x_n}{x_i}\right) \\ \cap & & \| \\ (y_0 : \cdots : 1) : \cdots : y_n) & \leftarrow\!\shortmid & (y_0, \cdots, \overset{\vee}{y_i}, \cdots, y_n) \end{array}$$

ただし $\vee$ は除くという意味.

は全単射. このとき.

$$\mathbb{P}^n_{\mathbb{C}} = \bigcup_{i=0}^{n} U_i$$

$$H_i = \{ [x_0 : \cdots : x_n] \in \mathbb{P}^n_{\mathbb{C}} \mid x_i = 0 \} \cong \mathbb{P}^{n-1}_{\mathbb{C}}$$

なので.

$$\mathbb{P}^n_{\mathbb{C}} = U_0 \sqcup \mathbb{P}^{n-1}_{\mathbb{C}} = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \mathbb{P}^{n-2}_{\mathbb{C}}$$

$$\vdots$$

$$= \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^1 \sqcup \mathbb{A}^0 \quad \text{とできる.}$$

V_0 を 射影平面 という.

$F(x,y,z) \in k[x,y,z]$ について

$F(x,y,z)$ に表われる 全ての 単項式の 次数 がそろっているとき.

$F(x,y,z)$ は 斉次である という.

例1 $F(x,y,z) = x^4 + y^4 - z^4$

$F(x,y,z) = y^2z - x^3 + z^3$

また $F(x,y,z) \in k[x,y,z]$ が 既約 であるとは.

$F(x,y,z) = GH \quad (G,H \in k[x,y,z]) \Rightarrow G \in k^\times$ または $H \in k^\times$

が 成り立つ ことを いう.

例

$F(X,Y,Z) = X^N + Y^N - Z^N$　キヤク

$F(X,Y,Z) = Y^2 Z - X^3 + Z^3$　キヤク

$F(X,Y,Z) = X^2 + Y^2$

$= (X + \sqrt{-1}\,Y)(X - \sqrt{-1}\,Y)$　キヤクでない.

定義1　$F(X,Y,Z) \in k[X,Y,Z]$：キヤクな斉次多項式

このとき

$$C = \{ [X:Y:Z] \in \mathbb{P}^2_k \mid F(X,Y,Z) = 0 \}$$

を平面曲線という.

このとき $F(X,Y,Z)$ は一般に値をもたないが

$F(X,Y,Z) = 0$ かどうかは代表元に依らず一意に決まる.

このとき F の次数を C の次数という.

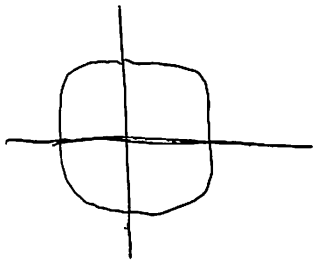
こうに $F(X,Y,Z) \in \mathbb{Q}[X,Y,Z]$ のとき.

$$C(\mathbb{Q}) = C \cap \mathbb{P}^2(\mathbb{Q})$$

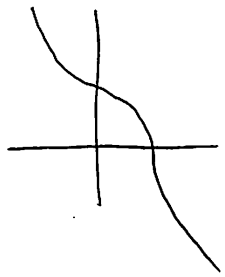
で定義し. 有理点の集合という.

例 $C = \{X^N + Y^N = Z^N\} \subset \mathbb{P}^2_{\mathbb{Q}}$

N: even



N: odd



$$C_0 = C \cap U_{Z\neq 0} = \{(x,y) \in \mathbb{A}^2 \mid x^N + y^N = 1\}$$

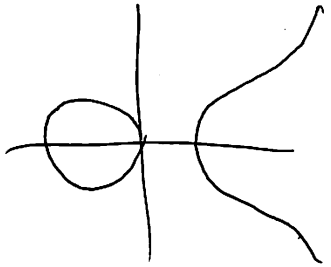
$$C \cap \{Z=0\} = \{(1 : \zeta_N^i : 0) \mid i = 0, \cdots, N-1\}$$

$$\zeta_N = e^{\frac{2\pi i}{N}}$$

例1

$$C = \{ Y^2 Z = X^3 \pm XZ^2 \}$$

$$C \cap U_2 = C_2 = \{ y^2 = x^3 - x \} \subset \mathbb{A}^2$$



$$C \cap \{Z=0\} = \{ (0:1:0) \}$$

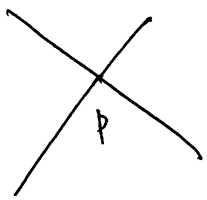
Bezout の定理

C_1, C_2 : 相異なる平面曲線

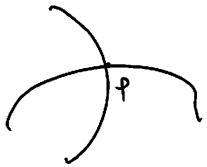
このとき $C_1 \cap C_2$ は有限集合

$p \in C_1 \cap C_2$ において local intersection multiplicity $I(C_1, C_2, p)$ が定まる.

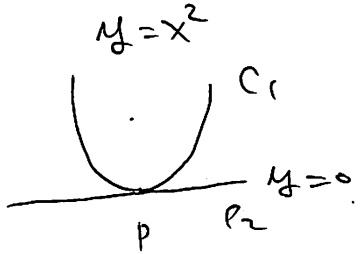
例1



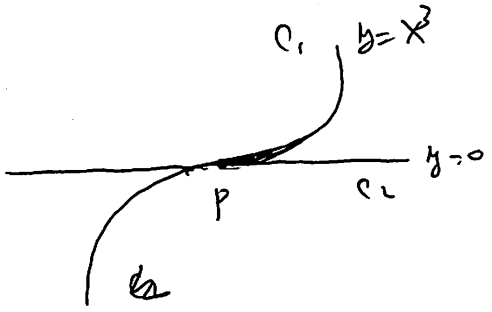
$I(C_1, C_2, p) = 1$



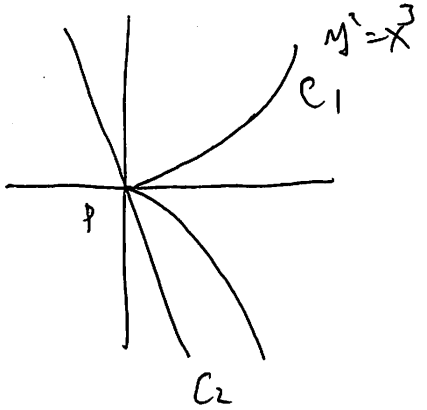
$I(C_1, C_2, p)$



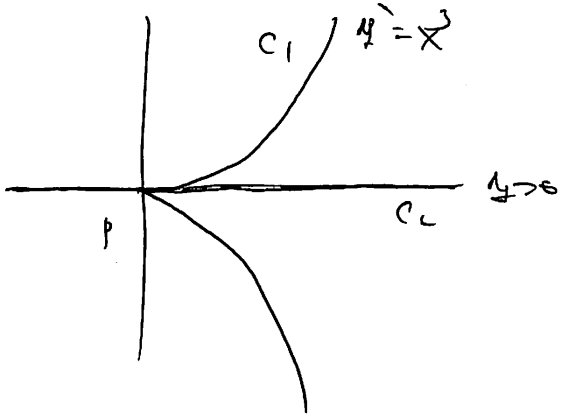
$I(C_1, C_2, p) = 2$



$I(C_1, C_2, p) = 3$



$I(C_1, C_2, p) = 2$



$I(C_1, C_2, p) = 3$

定義2　C_1, C_2: 相異なる平面曲線

このとき C_1とC_2の交点数を $C_1 : C_2 = \sum_{p \in C_1 \cap C_2} I(C_1, C_2, p)$

で def する.

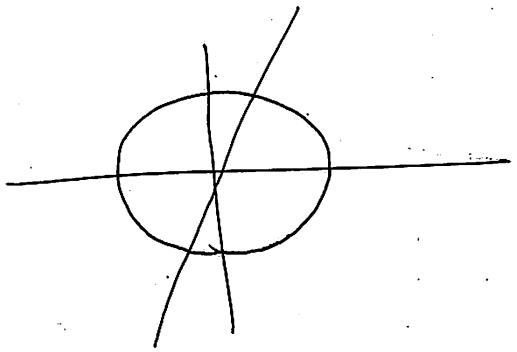
定理 (Bezout の定理) C_1, C_2: 相異なる 平面曲線

このとき $C_1 \cdot C_2 = \deg C_1 \cdot \deg C_2$

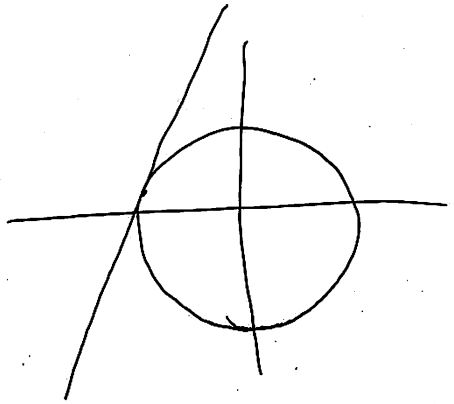
例 $C_1 = \{ x^2 + y^2 = z^2 \}$

$C_1 = \{ ax + by + cz = 0 \}$

$\mathbb{A}^2$



$1 + 1 = 2 = 1 \cdot 2$



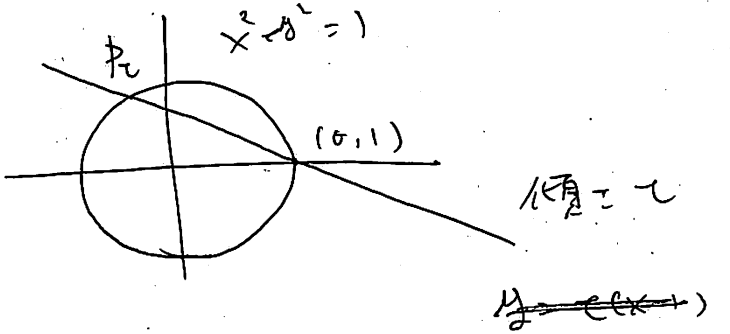
$2 = 2 = 1 \cdot 2$

有理点

例 $C = \{x^2 + y^2 = z^2\}$

$C(\mathbb{R})$ は どんなもの？

$C_0 = \{(x, y) \in \mathbb{A}^2 \mid x^2 + y^2 = 1\}$



こんなこと. $C_0(\mathbb{Q}) \supset \{(0, 1)\}$

~~$y = t(x+1)$~~

$y = tx + 1$

~~$y = t(x+1)$~~

$y = t(x+1)$

$t \in \mathbb{R}$ とこと. $p_t \in C(\mathbb{R})$ が 対応する.

$x^2 + y^2 = 1$

$y = tx + 1$

$\Rightarrow \quad x^2 + (tx+1)^2 = 1$

$\Rightarrow (1+t^2)x^2 + 2tx = 0$

$\Rightarrow (1+t^2)x\left(x + \frac{2t}{1+t^2}\right) = 0 \qquad y = 1 - \frac{-2t^2}{1+t^2} = \frac{1-t^2}{1+t^2}$

$\therefore \quad P_t = \left(-\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$

$C(\mathbb{Q}) = \left\{ (-2t : 1-t^2 : 1+t^2) \mid t \in \mathbb{Q} \right\} \cup \{(0:1:1)\}$

$= \left\{ (-2rs : s^2 - r^2 : s^2 + r^2) \mid (s:r) \in \mathbb{P}^1(\mathbb{Q}) \right\}_{t = \frac{r}{s}}$

例 $C = \{x^2 + y^2 = 3z^2\}$

このとき $C(\mathbb{Q}) = \phi$

☺ $p \in C(\mathbb{Q})$ が存在するとする.

$p = [x_0 : y_0 : z_0]$. このとき $x_0, y_0, z_0 \in \mathbb{Z}$ で $\gcd(x_0, y_0, z_0) = 1$

となる. x_0

$$x_0^2 + y_0^2 \equiv 3z_0^2 \pmod 4$$

ここで

$$x^2 \equiv 0, 1 \pmod 4$$

$(x_0, y_0, z_0) \equiv (0, 0, 0) \pmod 4$ は不適.

x_0	y_0	z_0
0	1	0
0	0	1

1	1	×
1	0	0

1	0	1
1	1	1

矛盾.

C を Φ 上 定義された次曲線とする.

$C(\Phi) \neq \emptyset$ なれば $P \in C(\Phi)$ を fixして

P を通る 任意の Φ 上の直線 l_t について $C \cap l_t = \{P, P_t\}$

$$C(\Phi) = \{ P_t \mid t \in \Phi \cup \{\infty\} \}$$

ここで.

$C(\Phi) \neq \emptyset \iff |C(\Phi)| = \infty$ がいえる.

例 (Fermat の最終定理)

$$C = \{ X^d + Y^d = Z^d \} \qquad d \geq 3$$

$$C(\mathbb{Q}) = \begin{cases} \{(0:\zeta_d^i:1), (\zeta_d^i:0:1) \mid i = 0, \dots, d-1\} & d = \text{even} \\ \{(0:\pm 1:1), (\pm 1:0:1)\} & \\ \{(0:\zeta_d^i:1), (\zeta_d^i:0:1) \mid i = 0, \dots, d-1\} & \\ \{(0:1:1), (1:1:0), (1:-1:0)\} & d = \text{odd} \end{cases}$$

楕円曲線

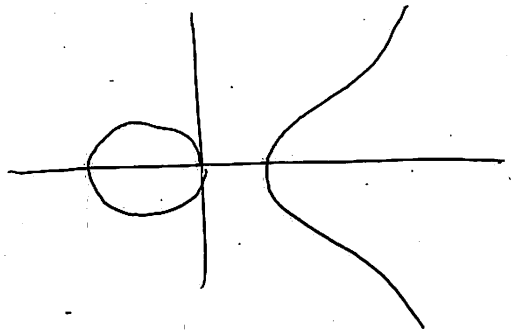
定義 $A, B \in k$ $4A^3 + 27B^2 \neq 0$ を仮定する.

$$E = \{ Y^2Z = X^3 + AXZ^2 + BZ^3 \} \subset \mathbb{P}^2_k$$

を 楕円曲線 という.

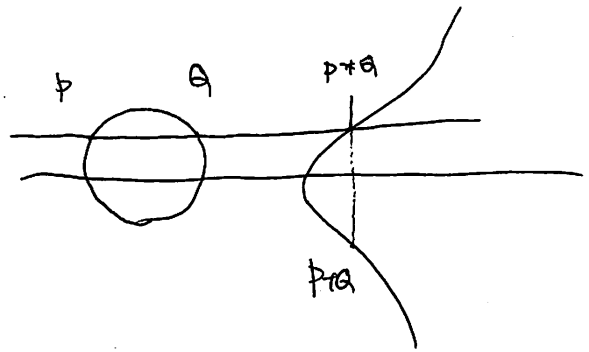
$$E = E_0 \amalg \{O\} \quad (O = {}^{t}(0:1:0))$$

$$\| \quad \{ (x, y) \in \mathbb{A}^2 \mid y^2 = x^3 + Ax + B \}$$



E: 楕円曲線　　P, Q ∈ E に対し

P+Q を図のように定義する



すると、(E, +) はアーベル群になる。

このとき、O が単位元

P = (x, y) に対し　-P = (x, -y)

が成立。

2P は接線を使って def できる。

$A, B \in \mathbb{Q}$ をとったとき.

$P, Q \in E(\mathbb{Q})$ に対して $P+Q \in E(\mathbb{Q})$ が従う.

$\therefore$ $E(\mathbb{Q})$ は 群の部分群.

(Mordell-Weil の定理)

定理5 $A, B \in \mathbb{Q}$ $4A^3+27B^2 \neq 0$ で

$$E = \{ Y^2 Z = X^3 + AXZ^2 + BZ^3 \}$$

このとき, $E(\mathbb{Q})$ は 有限生成アーベル群

すなわち $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \left(\mathbb{Z}/n_1\mathbb{Z}\right) \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$

となっている.

定理6 (Wiles) $E/\mathbb{Q}$: 楕円曲線 $\rightsquigarrow$ Fermat の最終定理

の一般化.

$\Rightarrow$ これは modular