数学入門公開講座

平成6年8月8日（月）から8月12日（金）まで

京都大学数理解析研究所

講師及び内容

1．代数曲線の幾何（6時間15分）

京都大学数理解析研究所・教授　森　　重　文

代数幾何は代数的に定義された図形（代数多様体）を研究する学問である。19世紀に始まり、現在までに目覚ましい発展を遂げている。図形には次元という概念があり、現在は1次元（曲線）、2次元（曲面）そして3次元までが大まかに分類されてきている。

ここでは、曲線について、その形そして分類などを中心に入門的な話をする。

2．プログラミング言語の数理モデル（6時間15分）

京都大学数理解析研究所・助教授　大　堀　　淳

プログラミング言語は、単なる計算の手順を記述する手段であるばかりでなく、複雑なプログラムを構築する上で必要な抽象化の概念と構造化の機構を提供するものです。ここでは、プログラミング言語の持つべき種々の望ましい性質の分析や新しいプログラミング言語の設計などを行なう基礎となる数学的モデルの概略を解説した後、プログラミング言語研究における最近の話題を幾つか紹介します。

3．楕円曲線と整数論（6時間15分）

京都大学数理解析研究所・助手　玉　川　安騎男

楕円曲線は、代数幾何学的には、（有理点を1つ与えられた）種数1の代数曲線として特徴づけられる比較的易しい代数多様体であるが、整数論的には、多くの重要な問題（しかもその多くは現在もなお未解決）と関連した、たいへん豊かな対象である。この講義では、予備知識の解説を含む楕円曲線についての入門的な話と並行して、いくつかのより進んだ「夢のある」話も折り込んでいく予定である。

時　間　割

日 / 時間	8月8日(月)	9日(火)	10日(水)	11日(木)	12日(金)
10：30～11：45	森	森	森	森	森
11：45～13：00	休　憩				
13：00～14：15	大堀	大堀	大堀	大堀	大堀
14：15～14：45	休　憩				
14：45～16：00	玉川	玉川	玉川	玉川	玉川

平成6年度(第16回)数学入門公開講座テキスト(京都大学数理解析研究所, 平成6年8月8日～8月12日開催)

楕円曲線と整数論

京都大学数理解析研究所・助　手　玉川安騎男

1994, AUGUST 8, 9, 10, 11, 12,　　14:45 ~ 16:00

楕円曲線と整数論

玉川安騎男

毎回、最初の１時間は（５日連続の）講義形式の話、最後の１５分間は日替わりの「夢のある」話をする予定です。以下のテキストは最初の１時間（× ５）の分です。

§1. はじめに（Diophantus 方程式について）

記法：

$$\begin{aligned}
&\mathbb{Z} = \{\text{整数全体}\} = \{0, \pm 1, \pm 2, \dots\},\\
&\mathbb{Q} = \{\text{有理数全体}\} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\},\\
&\mathbb{R} = \{\text{実数全体}\},\\
&\mathbb{C} = \{\text{複素数全体}\} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\}.
\end{aligned}$$

Diophantus 方程式（＝不定方程式）とは、$\mathbb{Z}$ に係数を持つ有限個の（多変数）方程式で、変数も $\mathbb{Z}$（あるいは $\mathbb{Q}$）に制限して考えたものをいいます。より具体的には、$f_1, \dots, f_m$ を m 個の $\mathbb{Z}$ - 係数 n 変数多項式とした時、連立方程式

$$\begin{aligned}
&f_1(x_1, \dots, x_n) = 0\\
&\cdots\\
&f_m(x_1, \dots, x_n) = 0
\end{aligned}$$

の $\mathbb{Z}$（あるいは $\mathbb{Q}$）における解を求めよ、という問題です。

以下では、主に $m = 1, n = 2$ の場合を考えます。

例１：（Fermat の問題。） $x^n + y^n = 1$ の $\mathbb{Q}$ における解は、$n \geqq 3$ の時、

$$(x, y) = \begin{cases} (1,0), (0,1), & n：\text{奇数} \\ (\pm 1, 0), (0, \pm 1), & n：\text{偶数} \end{cases}$$

に限るか？

このような問題は一般にはたいへん難しいことが多く、ある意味で一般的な解法が存在しないことさえ知られています（Hilbert の第１０問題）。

さて、与えられた Diophantus 方程式 $f(x, y) = 0$ を解くという問題を考える時、この問題をいくつかの段階に分けることができます。

問題Ａ：$f(x, y) = 0$ に解があるかないか？

問題Ｂ：$f(x, y) = 0$ の解は（たかだか）有限個か？

問題Ｃ１：解が有限個の場合は、すべて書き上げよ。

問題Ｃ２：解が無限個の場合は、なんとかして（！）記述せよ。

もちろん、これらの問題が $\mathbb{Z}$ と $\mathbb{Q}$ に対してそれぞれ考えられるわけです。

これらの問題について現在どのようなことがわかっているかを述べる前に、$\mathbb{R}$ と $\mathbb{C}$ における方程式 $f(x,y)=0$ の解について見てみましょう。

$\mathbb{R}$ における $f(x,y)=0$ の解全体 $\{(x,y)\in\mathbb{R}^2 \mid f(x,y)=0\}$ は、平面 $\mathbb{R}^2$ 上のグラフによって表すことができます。（$x^2+y^2+1=0$ のように、空集合になってしまうこともあります。）

一方、$\mathbb{C}$ における $f(x,y)=0$ の解全体 $\{(x,y)\in\mathbb{C}^2 \mid f(x,y)=0\}$ は、$\mathbb{C}^2$ が実4次元の空間なので目に見えるグラフを作ることはできませんが、解全体のなす図形だけを取り出せば、（伸ばしたり縮めたりして）3次元空間 $\mathbb{R}^3$ に埋め込むことができます。f が $\mathbb{C}$ 上の多項式として既約で、「特異点を持たない」図形を定める時には、$\mathbb{C}$ における $f(x,y)=0$ の解全体のなす図形は、n 個の点でパンクした g 人乗りの浮き袋のような形をしていることが知られています。ここで、$g\geqq 0$ と $n\geqq 1$ は f から決まるある整数です。（g を種数といいます。n は「無限遠点」の個数です。）

しかし、これらのグラフや図形をいくらながめていても、$\mathbb{Z}$ あるいは $\mathbb{Q}$ に座標をもつ点がどこにあるのかさっぱりわかりません。

ところが、たいへん不思議なことに、Diophantus 問題（＝ Diophantus 方程式を解く問題）は、その方程式の $\mathbb{C}$ における解全体の定める図形の「形」に大きく依存していることがわかってきています。　例えば、$\mathbb{Q}$ における問題Ａについては

$g=0$：判定法あり（Hasse 原理）。
$g\geqq 1$：一般には Hasse 原理は成立しない。

問題Ｂについては

$g=0$：解は0個または無限個。
$g=1$：解は有限個のことも無限個のこともある。
$g\geqq 2$：解はいつでも有限個。

となっています。最後の結果は Mordell 予想と呼ばれていたもので、１０年ほど前に Faltings によって証明されました：

定理（Faltings）：$g\geqq 2$ の時、$f(x,y)=0$ の $\mathbb{Q}$ における解は有限個。

なお、$\mathbb{Z}$ における解についても、同様の結果があります。

定理（Siegel）：$g=0, n\geqq 3$ または $g\geqq 1$ の時、$f(x,y)=0$ の $\mathbb{Z}$ における解は有限個。

問題Ｃ１は、問題Ｂの答えが Yes であっても（つまり、解の個数が有限個であることがわかっても）、簡単ではありません。順番に代入していく方法では、いつになった

ら終わってよいのかわかりません。例えば、例1の $x^n + y^n = 1$ の場合、$\mathbb{C}$ における解全体のなす図形の種数 g は $\frac{1}{2}(n-1)(n-2)$ となり、したがって、Faltings の定理によって $n \geqq 4$ ならば $\mathbb{Q}$ における解の個数が有限個であることがわかります（実は、$n = 3$ の時も有限個になることが示せます）。しかし、その有限個の解全部を書き上げることは、また別の問題です。

最後に問題C 2についてですが、無限個の解を記述する方法としては、パラメータを使って表示する方法（例2）、いくつかの基本解からある（いくつかの）操作によって帰納的に与えていく方法（例3）、などが考えられます。

例2： $x^2 = 3y^2 + 1$ の $\mathbb{Q}$ における解全体は、

$$\{(\frac{3t^2+1}{3t^2-1}, \frac{-2t}{3t^2-1}) \mid t \in \mathbb{Q}\} \cup \{(1,0)\}$$

で与えられる。（$(1,0)$ は、t に ∞ を代入したものと考えることもできる。）

例3： $x^2 = 3y^2 + 1$ の $\mathbb{Z}$ における解全体は、次のように表される。$P = (x,y)$ に対し、$\tau(P) = (2x+3y, x+2y), \iota(P) = (x,-y)$ とおく。この時、解全体は、

$$\{(\pm 1, 0)\} \cup \{\tau^n((\pm 1,0)) \mid n = 1,2,\dots\} \cup \{\iota(\tau^n((\pm 1,0))) \mid n = 1,2,\dots\}$$

で与えられる。ここで、

$$\tau^n(P) = \underbrace{\tau(\tau(\dots(\tau}_{n\text{回}}(P))\dots)).$$

なお、問題C 2は、Faltings の定理と Siegel の定理によって、$\mathbb{Q}$ における解ならば $g = 0, 1$、$\mathbb{Z}$ における解ならば $g = 0, n = 1, 2$ の場合だけが問題になります。例2、例3は、$g = 0, n = 2$ の場合です。$g = 1$ の場合に $\mathbb{Q}$ における解全体を記述する方法を考えるのが、この講義の1つの大きなテーマです。

§2. 群についての準備

この§では、群に関する知識を用語集的にまとめておきます。講義では、必要に応じて、例を出して解説を加える予定です。

群： 集合 G の上に演算 $G \times G \to G$, $(x,y) \mapsto x \circ y$ が与えられているとする。この時、次の公理1、2、3が満たされれば、G は（正確には、$(G, \circ)$ は）群であるという。

1、任意の $x, y, z \in G$ に対し、$(x \circ y) \circ z = x \circ (y \circ z)$
2、$e \in G$ があって、任意の $x \in G$ に対し、$x \circ e = e \circ x = x$
3、任意の $x \in G$ に対して、$\iota(x) \in G$ があって、$x \circ \iota(x) = \iota(x) \circ x = e$

2を満たすeはただ一つ定まる。eをGの単位元という。各xに対し、3を満たす$\iota(x)$はただ一つ定まる。$\iota(x)$をxの逆元という。

アーベル群： 群Gが、さらに

4、任意の$x, y \in G$に対し、$x \circ y = y \circ x$

を満たす時、Gをアーベル群（または、可換群）という。

（注意）普通、群の演算は積で表し、$x \circ y$をxyと書く。この時は、単位元eを1、xの逆元$\iota(x)$をx^{-1}と書く。アーベル群については、演算を和で表し$x \circ y$を$x+y$と書くこともあり、この時は、単位元eを0、xの逆元$\iota(x)$を$-x$と書く。

n乗（またはn倍）： 群の元xと整数nに対して、

$$x^n = \begin{cases} \underbrace{x \circ \cdots \circ x}_{n}, & n > 0 \\ e, & n = 0 \\ \iota(x)^{-n}, & n < 0 \end{cases}$$

をxのn乗という。演算を和で表す時には、xのn倍といい、nxで表す。すなわち、

$$nx = \begin{cases} \underbrace{x + \cdots + x}_{n}, & n > 0 \\ 0, & n = 0 \\ (-n)(-x), & n < 0 \end{cases}$$

部分群： 群Gの部分集合Hが

(i) $x, y \in H \Longrightarrow x \circ y \in H$
(ii) $e \in H$
(iii) $x \in H \Longrightarrow \iota(x) \in H$

を満たす時、HをGの部分群という。この時Hは、Gの演算$\circ$を制限することによって群となる。アーベル群の部分群はアーベル群になる。

正規部分群： 群Gの部分群Hが、

$y \in H, x \in G \Longrightarrow x \circ y \circ \iota(x) \in H$

を満たす時、HをGの正規部分群という。アーベル群のすべての部分群は正規部分群である。

商群： Gを群とし、Hをその部分群とする。この時、$x, y \in G$に対し、$\iota(x) \circ y \in H$であることを$x \sim y$で表すと、$\sim$はGの上の同値関係になる。すなわち、

(i) $x \sim x$ （反射律）
(ii) $x \sim y \Longrightarrow y \sim x$ （対称律）
(iii) $x \sim y, y \sim z \Longrightarrow x \sim z$ （推移律）。

さらに、H が G の正規部分群の時、

(iv) $x \sim y, z \sim w \Longrightarrow x \circ z \sim y \circ w$

も満たされ、この時、同値関係 $\sim$ による G の商集合は、G の演算から誘導される演算によって群となる。この群を G/H で表し、G の H による商群と呼ぶ。

直積： $(G, \circ), (G', \circ')$ を 2 つの群とする。この時、G と G' の直積集合 $G \times G'$ の上に

$$(x, x') \cdot (y, y') = (x \circ y, x' \circ y')$$

によって演算 $\cdot$ を定義すると、$(G \times G', \cdot)$ は群となる。これを G と G' の直積（群）という。3 つ以上の群の直積も同様に定義される。

準同型と同型： $(G, \circ), (G', \circ')$ を 2 つの群とする。G から G' への写像 f が、任意の $x, y \in G$ に対して

$$f(x \circ y) = f(x) \circ' f(y)$$

を満たす時、f を G から G' への準同型（写像）という。この時、

$$f(e) = e', \ f(\iota(x)) = \iota'(f(x))$$

となる。（e' は G' の単位元、$\iota'(x')$ は $x' \in G'$ の逆元を表す。）

さらに f が全単射の時、f を G から G' への同型（写像）という。この時、f の逆写像 f^{-1} は G' から G への同型写像となる。

2 つの群 G, G' の間に同型写像が（一つでも）ある時、G と G' は（互いに）同型であるといい、$G \simeq G'$ と表す。

像と核： f を群 G から群 G' への準同型写像とする。この時、f の像

$$\mathrm{Im}(f) = \{f(x) \mid x \in G\}$$

は G' の部分群となる。また、f の核

$$\mathrm{Ker}(f) = \{x \in G \mid f(x) = e'\}$$

は G の正規部分群となる。

準同型定理： f を G から G' への準同型写像とする時、

$$G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)。$$

有限生成アーベル群の基本定理： $(G, +)$ をアーベル群とする。もし、有限個の G の元 $x_1, \ldots, x_N$ があって、すべての G の元 x が

$$x = n_1 x_1 + \cdots + n_N x_N, \ n_1, \ldots, n_N \in \mathbb{Z}$$

という形に表されるならば、G は有限生成であるという。

定理： G を有限生成なアーベル群とする。この時、整数 $r \geqq 0$ と自然数 $e_1, \ldots, e_s$ があって、

$$G \simeq \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r} \times (\mathbb{Z}/e_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/e_s\mathbb{Z})$$

となる。r は G によって一意的に定まる。また、$e_1, \ldots, e_s$ は、$1 < e_1 | e_2 | \ldots | e_s$ を満たすように選べ、この条件の下では一意的に定まる。

§3. 射影空間と平面曲線

この§では、複素数体 $\mathbb{C}$ 上の射影空間について考えます。射影空間は最も基本的な代数多様体（＝多項式で定義された図形）の一つで、さまざまな代数多様体の「入れ物」になります。

[射影空間]

$\mathbb{C}^{n+1} - \{(0, \ldots, 0)\}$ の上の同値関係 $\sim$ を次のように定義します。

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Longleftrightarrow \lambda \in \mathbb{C} - \{0\} \text{ があって} y_0 = \lambda x_0, \ldots, y_n = \lambda x_n$$

この同値関係 $\sim$ による同値類全体の集合を $\mathbb{P}^n$ $(= \mathbb{P}^n(\mathbb{C}))$ で表し、n 次元射影空間と呼びます。$\mathbb{P}^0$ は 1 点集合で、また、$\mathbb{P}^1$、$\mathbb{P}^2$ は、それぞれ射影直線、射影平面と呼ばれます。$(x_0, \ldots, x_n) \in \mathbb{C}^{n+1} - \{(0, \ldots, 0)\}$ の定める $\mathbb{P}^n$ の元を $(x_0 : \cdots : x_n)$ と書くことにします。

同様の構成は $\mathbb{Q}$ や $\mathbb{R}$ についても可能で、自然に

$$\mathbb{P}^n(\mathbb{Q}) \subset \mathbb{P}^n(\mathbb{R}) \subset \mathbb{P}^n(\mathbb{C}) = \mathbb{P}^n$$

となっています。

[斉次多項式とその零点]

$P = (x_0 : \cdots : x_n)$ を $\mathbb{P}^n$ の点とします。一般の $(n+1)$- 変数多項式 F に対しては、$F(P) = 0$ かどうかを論ずることはできませんが、F が斉次多項式の場合には、

$$F(P) = 0 \Longleftrightarrow F(x_1, \ldots, x_n) = 0$$

と定義することによって、代表 $(x_0, \ldots, x_n)$ のとり方によらずに F の零点を定義することができます。（但し、$F(P)$ の値そのものを考えることはできません。意味があるのは、$F(P) = 0$ かどうかだけです。）

[射影曲線]

以下では、$n = 2$ の場合を考えます。ある 3 変数 d 次斉次多項式 $F(X_0, X_1, X_2)$ によって定義される $\mathbb{P}^2$ の部分集合

$$V(F) = \{P \in \mathbb{P}^2 \mid F(P) = 0\}$$

を d 次射影平面曲線といいます。（曲線は、しばしば curve の頭文字をとって C で表します。）射影平面曲線 $C = V(F)$ は、F が $\mathbb{Q}$ - 係数多項式の時、$\mathbb{Q}$ 上定義されている、といいます。この時、$C \cap \mathbb{P}^2(\mathbb{Q})$ を $C(\mathbb{Q})$ で表します。

[アフィン曲線との関係]
次にアフィン平面曲線との関係を見てみましょう。$\mathbb{P}^2$ の部分集合

$$U_0 = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 \mid x_0 \neq 0\}$$

を考えます。($U_0 = \mathbb{P}^2 - V(X_0)$ とみることができます。) この時、対応

$$(x, y) \leftrightarrow (1 : x : y)$$

によって $\mathbb{C}^2$ と U_0 を同一視することができます。
この同一視の下で、(3 変数) 斉次多項式 F に対して $f(X, Y) = F(1, X, Y)$ とおくと、

$$V(F) \cap U_0 = \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\}$$

となっています。$V(X_0)$ ($= \mathbb{P}^2 - U_0$) と $V(F)$ の交わりは、(F が X_0 で割り切れない時は) 有限個の点からなります。これが、曲線 $V(F)$ の無限遠点です。
なお、$C = V(F)$ が $\mathbb{Q}$ 上定義されている時は、

$$C(\mathbb{Q}) \cap U_0 = \{(x, y) \in \mathbb{Q}^2 \mid f(x, y) = 0\}$$

となります。

[平面曲線の特異点]
次に、平面曲線の特異点の定義を述べます。(つぎの§で出てくる「楕円曲線」は、特異点を持ちません。) 射影平面曲線 $C = V(F)$ の特異点集合 $\mathrm{Sing}(C)$ は、

$$\mathrm{Sing}(C) = \{P \in C \mid \frac{\partial F}{\partial X_0}(P) = \frac{\partial F}{\partial X_1}(P) = \frac{\partial F}{\partial X_2}(P) = 0\}$$

で定まる C の部分集合です。(F が平方因子を含まなければ) $\mathrm{Sing}(C)$ は有限集合で、C の「なめらかでない」点 (=特異点) 全体の集合になっています。なお、

$$\mathrm{Sing}(C) \cap U_0 = \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0, \frac{\partial f}{\partial X}(x, y) = \frac{\partial f}{\partial Y}(x, y) = 0\}$$

となっています。

[Bezout の定理]
次の Bezout の定理は重要です。

定理 (Bezout) : $C = V(F)$、$C' = V(F')$ を $\mathbb{P}^2$ 内の、それぞれ d 次、d' 次の曲線とし、C と C' は共通の既約成分を持たない ($\Longleftrightarrow$ F と F' は共通因子を持たない) と仮定する。この時、C と C' の交わりの点の個数はたかだか dd' 個で、「重複度も込めて」数えると、ちょうど dd' 個ある。

特に、d 次曲線は任意の直線 (= 1 次曲線) と、重複度を込めてちょうど d 個の点で交わります。(この事実が、楕円曲線に群の構造が入ることの基礎になります。)

§4. 楕円曲線

ようやくこの講義のタイトルにある楕円曲線が登場します。楕円曲線は、（「原点」を一つ与えられた）種数1の完備非特異代数曲線として抽象的に定義できますが、ここでは、より具体的な平面曲線としての表示から出発しましょう。楕円曲線の最も重要な性質は、群構造を持つことです。

[Weierstrass 方程式]

$a, b, c \in \mathbb{C}$ を与えられた定数とします。この時、（3変数）方程式

$$x_0x_2^2 = x_1^3 + ax_0x_1^2 + bx_0^2x_1 + cx_0^3$$

を斉次 Weierstrass 方程式といいます。この方程式により、$\mathbb{P}^2$ 内の3次曲線 E が定義されます。すなわち、

$$F(X_0, X_1, X_2) = X_0X_2^2 - (X_1^3 + aX_0X_1^2 + bX_0^2X_1 + cX_0^3)$$

とおく時、$E = V(F)$ です。

E と U_0 の交わりは、方程式

$$y^2 = x^3 + ax^2 + bx + c$$

によって与えられるアフィン曲線です。この方程式を（非斉次）Weierstrass 方程式といいます。E の無限遠点（$= E \cap V(X_0)$ の点）は $(0:0:1)$ 1点だけです。したがって

$$E = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3 + ax^2 + bx + c\} \cup \{(0:0:1)\}$$

となります。

Weierstrass 方程式によって与えられる3次曲線 E の特異点は、3次方程式 $x^3 + ax^2 + bx + c = 0$ が重根（3重根も含む）を持つ時に存在し、その重根（たかだか一つ）を e とする時、特異点集合 Sing(E) は1点 $(1 : e : 0)$（アフィンの言葉では $(e, 0)$）からなります。それ以外の時、つまり方程式 $x^3 + ax^2 + bx + c = 0$ が相異なる3根を持つ時は、E は特異点を持ちません。

[楕円曲線]

特異点を持たない3次曲線 E で、原点 $O \in E$ が与えられたものを楕円曲線といいます。（正確には、(E, O) が楕円曲線であるということになります。）楕円曲線 (E, O) は、E が $\mathbb{Q}$ 上定義された曲線で、$O \in E(\mathbb{Q})$ となる時、$\mathbb{Q}$ 上定義されている、といいます。

Weierstrass 方程式 $y^2 = x^3 + ax^2 + bx + c$ によって与えられる3次曲線 E が特異点を持たない時、$O = (0:0:1)$ と定めれば、(E, O) は楕円曲線となります。方程式の係数 a, b, c が有理数の時、(E, O) は $\mathbb{Q}$ 上定義されています。

なお、任意の 楕円曲線は、（原点 O を $(0:0:1)$ に写す）適当な「変数変換」によって Weierstrass 方程式で与えられる3次曲線にできることが知られています。したがって、楕円曲線を、Weierstrass 方程式によって与えられる3次曲線で特異点を持たないものと定義してもかまいません。

[楕円曲線の群構造]

E を特異点を持たない 3 次曲線とします。$P,Q \in E$ に対し、$L_{P,Q}$ を P,Q を通る（ただ一つの）$\mathbb{P}^2$ 内の直線とします。但し $P = Q$ の時は、$L_{P,P}$ は P における E の接線とします。（E が特異点を持たないことに注意して下さい。） Bezout の定理により、E と $L_{P,Q}$ は重複度を込めてちょうど 3 点で交わりますが、既に P,Q で交わっていますから、残る交点はあと 1 点です。この点を $P*Q$ と定義します。（重複度の解釈は次のようにします。$P \neq Q$ で $L_{P,Q}$ が P における E の接線の時は $P*Q = P$、$L_{P,Q}$ が Q における E の接線の時は $P*Q = Q$。$P = Q$ で $L_{P,P}$ が P 以外の点で E と交わる時は $P*P$ はその点、交わらない時は $P*P = P$。これ以外の場合は E と $L_{P,Q}$ は普通の意味で 3 点で交わるので、問題なし。）定義から直ちに

$$P*Q = Q*P$$

$$P*(P*Q) = Q$$

となっています。

さて、E 上に原点 O が与えられているとします。この時、

$$P \circ Q = O*(P*Q)$$

によって、E 上の演算 $\circ$ を定義します。すると、次の定理が成り立ちます。

定理： $(E,\circ)$ はアーベル群である。単位元は O、また $P \in E$ の逆元 $\iota(P)$ は

$$\iota(P) = P*(O*O)$$

によって与えられる。

アーベル群の公理 1 - 4 のうち、$(E,\circ)$ が 2、3、4 を満たすことは先に述べた $*$ の性質から容易に示せますが、結合法則 1 については、いくつか証明が知られているものの、いずれもそう易しくありません。

以下では、楕円曲線の群演算 $P \circ Q$, $\iota(P)$ を $P+Q$, $-P$ で表します。

[群演算の公式]

E が具体的に Weierstrass 方程式

$$y^2 = x^3 + ax^2 + bx + c$$

で与えられ、O として無限遠点 $(0:0:1)$ をとる場合には、以下のように群演算を具体的な公式によって表すことができます。

まず、O における E の接線は無限遠直線 $L_0 = V(X_0)$ となり、E と L_0 の交点は O だけですから、$O*O = O$ となります。したがって、$P \in E$ に対して、$-P = P*O$ となります。$P = (\xi,\eta) = (1:\xi:\eta)$ と $O = (0:0:1)$ を通る直線 $L_{P,O}$ は $x_1 = \xi x_0$（アフィンで見れば、$x = \xi$）で与えられますから、$L_{P,O}$ と E の 3 番目の交点は、$(\xi,-\eta)$ となります。（$\eta = 0$ の時は、$L_{P,O}$ は P における E の接線になります。）以上により、

$$-P = \begin{cases} (\xi,-\eta), & P = (\xi,\eta) \\ O, & P = O \end{cases}$$

和の公式はもっと複雑です。$P+O=P$, $O+Q=Q$, $P+(-P)=O$ はわかっていますから、$P\neq O$, $Q\neq O, \pm P$ の場合と $P=Q\neq O$ の場合を考えればよいことになります。前者の場合、$P=(\xi,\eta), Q=(\xi',\eta')$ とすると $\xi\neq\xi'$ で、$L_{P,Q}$ は（アフィンの言葉で）

$$y=\lambda x+\nu$$

但し、

$$\lambda=\frac{\eta'-\eta}{\xi'-\xi},\ \nu=\frac{\eta\xi'-\eta'\xi}{\xi'-\xi}$$

となります。後者の場合、$P=Q=(\xi,\eta)=(\xi',\eta')$ とすると、その点における E の接線 $L_{P,P}$ は、

$$y=\lambda x+\nu$$

但し、今度は

$$\lambda=\frac{3\xi^2+2a\xi+b}{2\eta},\ \nu=\frac{-\xi^3+b\xi+2c}{2\eta}$$

となります。いずれの場合も $P+Q=(\xi'',\eta'')$ は、

$$\xi''=\lambda^2-a-\xi-\xi',\ \eta''=-(\lambda\xi''+\nu)$$

によって計算できます。$P=Q$ の時は、さらに計算すると

$$\xi''=\frac{\xi^4-2b\xi^2-8c\xi+b^2-4ac}{4(\xi^3+a\xi^2+b\xi+c)}$$

と表すこともできます（2倍公式）。

なお、これらの公式からわかるように、E が $\mathbb{Q}$ 上定義されている時は、$E(\mathbb{Q})$ は $E=E(\mathbb{C})$ の部分群になっています。（a,b,c が整数の場合でも、Weierstrass 方程式の $\mathbb{Z}$ における解全体 $\{(x,y)\in\mathbb{Z}^2 \mid y^2=x^3+ax^2+bx+c\}$ は、無限遠点を付け加えても一般には E の部分群にはなりません。）

§5. Mordell の定理

次の定理を Mordell の定理（または Mordell-Weil の定理）といいます。

定理（Mordell）： E を $\mathbb{Q}$ 上定義された楕円曲線とする。この時、$E(\mathbb{Q})$ は有限生成アーベル群である。

系： $E(\mathbb{Q})\simeq \underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{r}\times$(有限アーベル群).

Mordell の定理は、$E(\mathbb{Q})$ の元（あるいは、より具体的にいえば、Diophantus 方程式 $y^2=x^3+ax^2+bx+c$ の $\mathbb{Q}$ における解）が、有限個の基本解から出発して群演算を繰り返し施すことによってすべて得られることを保証しています。なお、アーベル群 $E(\mathbb{Q})$ を E の Mordell-Weil 群といい、r をその階数といいます。

Mordell の定理の証明には、ガロア・コホモロジー、代数体と局所体の整数論、高さ（height）の理論など、現代の整数論において基本的なかずかずの道具立てが用いられます。講義では、Mordell の定理の特別な場合（E が Weierstrass 方程式 $y^2=x^3+ax^2+bx+c$ で与えられ、しかも $x^3+ax^2+bx+c=0$ の根がすべて $\mathbb{Q}$ に入る場合）の証明の紹介を試みようと思っています。