数学入門公開講座

平成１１年８月２日（月）から８月６日（金）まで

京都大学数理解析研究所

講師及び内容

1．多項式の解の近似がとりもつ数論と幾何の関係（6時間15分）

京都大学数理解析研究所・助教授　望月　新一

多項式の有理数解の研究は、歴史が長いだけに、様々なアプローチを産み出しているが、二十世紀の後半に開発され、現在では数々の輝かしい成果を挙げているアプローチとして、現代数論幾何がある。本講義の目標は、その現代数論幾何の世界を紹介することにある。現代数論幾何の基本は、標語的にいえば、多項式の解の近似にあるといってもよい。つまり、有理数というものは、整数論の対象としては構造が複雑すぎるため、数論的にはより単純な構造をした実数や複素数のような数で近似することによって多項式の有理数解を調べるのである。このような近似解のなす集合は、有理数解のなす集合と違い、「滑らかな物質」で出来た幾何的な対象をなしていて、その対象の幾何的性質が、有理数解の性質に大きく影響することが知られている。

2．計算幾何学入門（6時間15分）

京都大学数理解析研究所・助教授　田村　明久

平面上に与えられた有限個の点の集合に対して、これを含む最小の凸多角形を求める問題を（2次元）凸包問題とよびます。計算幾何学とは、このような幾何的な問題を解くアルゴリズム（解法）を研究する計算機科学の一分野です。

本講座では凸包問題のほかに勢力圏のモデルとして利用されるボロノイ図など、計算幾何学において基礎的な問題とそれらに対するアルゴリズムを紹介します。また、アルゴリズムの効率性の評価についてもふれます。

3．微積分をつうじて多様体が見える（6時間15分）

京都大学数理解析研究所・教授　宮岡　洋一

「多様体」は現代数学を理解する上で鍵となる概念です。

数学のなかでも最も古い伝統をもつ幾何学は、三次元空間という入れ物にはいっている図形という素朴な直感から出発したわけですが、百五十年ほど前のこと、リーマンは、必ずしも入れ物を必要とせず、いくらでも高い次元をもてる、多様体の概念に到達しました。この概念は解析学を複雑な図形のなかで自由に展開することを可能とし、その結果として宇宙全体の幾何構造といったものまで考察することまでできるようになったのです。

この講義では、多様体の豊かな世界への入門として、積分を通じて解析（微分形式）と幾何（コホモロジー）とがかかわりあう、その様子に焦点をしぼって解説したいと思います。

時　間　割

日 / 時　間	8月2日（月）	3日（火）	4日（水）	5日（木）	6日（金）
10：30～11：45	望月	望月	望月	望月	望月
11：45～13：00	休　憩				
13：00～14：15	田村	田村	田村	田村	田村
14：15～14：45	休　憩				
14：45～16：00	宮岡	宮岡	宮岡	宮岡	宮岡

平成11年度(第21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11年8月2日～8月6日開催)

多項式の解の近似がとりもつ数論と幾何の関係

京都大学数理解析研究所・助教授　望月新一

1999, AUGUST 2,3,4,5,6, 10:30～11:45

多項式の解の近似がとりもつ
数論と幾何の関係

望月 新一 （京大数理研）

目次

I. 数論幾何の起源と主な（数学的）登場人物

(A.) 多項式の有理数解の研究

純粋数学のルーツを辿っていくと、そもそも

「数」とは一体何なのか？

という問いに必然的にぶち当たる。最も簡単な答えは、普通に数える時に用いる数字、

$$1, 2, 3, 4, 5, \ldots$$

つまり、数学では「自然数」と呼ばれる数たちである。ところで、自然数しか扱わない世界でしばらく暮らしてみると、小さい数から大きい数を引いたり、また小さい数を大きい数で割ったりしようとすると、何となくその結果として出てくるものが「数」だという感覚があっても、「一、二、三、四、...」という自然数の言葉だけでは直接語れないものになってしまう。この問題は、ギリシャやインドをはじめ、「数」について真剣に考えたことのある古代文明でも、現代の小中学生でも、馴染み深いもの（のはず）である。そこで、0 や $-1, -2, -3, \ldots$ など、正でない数が生まれ、「整数」という概念が作られ、更に分数も入れて「有理数」というものが定義されたことによって、「数」の概念が補充されてきた。現代数学では、整数全体を**整数環**と呼んで

$$\mathbf{Z} = \{\ldots, -3, -2-1, 0, 1, 2, 3, \ldots\}$$

という記号で表し、有理数全体を**有理数体**と呼んで

$$\mathbf{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbf{Z},\ n \neq 0 \right\}$$

で表す。なお、$X^2 - 2 = 0$ のような一変数の多項式の解が必要な時は、有理数係数の多項式の解全体、つまり、いわゆる「代数的数」（すう）

$$\overline{\mathbf{Q}} = \{x \mid x^n + c_1 \cdot x^{n-1} + \ldots + c_n = 0,\ c_1, \ldots, c_n \in \mathbf{Q}\}$$

を考えたくなることもある。

これで、任意の一変数の多項式が解けるほどの数が、少なくとも**概念上**はできたことになるが、本当は $\overline{\mathbf{Q}}$ は大き過ぎて、具体的に何なのかは（有理数体 $\mathbf{Q}$ と較べて）極めて把握し難い。つまり、（例えば、有理数係数の一変数）

多項式はいつ有理数解を持つか？

という問題に関心が向く。一変数の多項式だと、その有理数解がどんな様子をしているか具体的に知らなくても、多項式の次数が n なら、有理数解は多くても n **個しかない**という「定性的な」ことは、多項式の素因子分解を考えることによって直ちに分かる。

ところが、変数の数が2以上になると、そのような定性的なことすら全く分からなくなってしまう。実際に具体的な多項式、例えば

$$x^n + y^n = 1 \quad (n \geq 3 \text{ は自然数})$$

（＝有名なフェルマの問題に出てくる多項式）の有理数解を計算しようとすると、有理数解が極めて少なく珍しい（有難い？）ものだという印象は直ちに受ける。しかし、それがどの位少ないか、例えば、有理数解全体の集合が有限なのか、無限なのかといったようなことは、初等的な見地から式をいじってみただけではなかなか分からない。実際、人類はちょうどこのような初等的な見地から式をいじることによって多項式の有理数解の様子を解明しようとして（勘定の仕方によっては）二千年以上の歳月を費やしてきているが、

初等的な式変形という手法には限界がある

というのが、歴史上の主な当時者のおよそ共通した認識といえよう。

(B.) スキーム論の意味：「数は関数」

そこで問題の本質を見抜いたより概念的なアプローチを開発したくなるわけだが、そのようなアプローチの説明に入る前に、まず、**「多項式の有理数解の様子を理解せよ」**という命題の主な「登場人物」を確認しておこう。もちろん、視点によってこの「登場人物」の名簿は変わってくるが、ここでは次のような名簿を採用させて頂く：

問題の主要な登場人物＝「数」、「多項式」

「数の理論」、つまり「整数論」は、独自の長い歴史を持っていて、その顕著な成果の一つとして、日本とも縁が深い「類体論」を生むなど、ここ数百年の数学の中で重要な位置を占めている分野である。一方、多項式の研究、特にその多項式が‘定める’（＝高校で勉強する二次式が放物線や楕円などを定めるように）幾何的な対象「代数多様体」の研究は、代数幾何と呼ばれ、これもこ

こ数百年の数学の中で中心的な分野の一つといえよう。ただ、この「数の研究」と「多項式の研究」の歴史が長い割には、二者が明確な形で結び付いた分野 — 本稿ではこの分野のことを**(現代)数論幾何**と呼ぶことにする — は１９６０年代まで誕生しなかった。現代数論幾何の最も基本的な概念は**「スキーム」**と呼ばれるものだが、スキーム論を支えている発想は一言でいうと、

「数」も「多項式」も実は同じ「関数」なのである

というものである。この発想は特に、先ほど挙げた基本的な問い掛け「数とは何か？」に対して、「それは、関数なのである」、しかも「多項式も関数であるから、数と多項式は実は何と、‘**同類**’つまり‘**対等**’な対象なのである」という考え方を訴えているわけである。

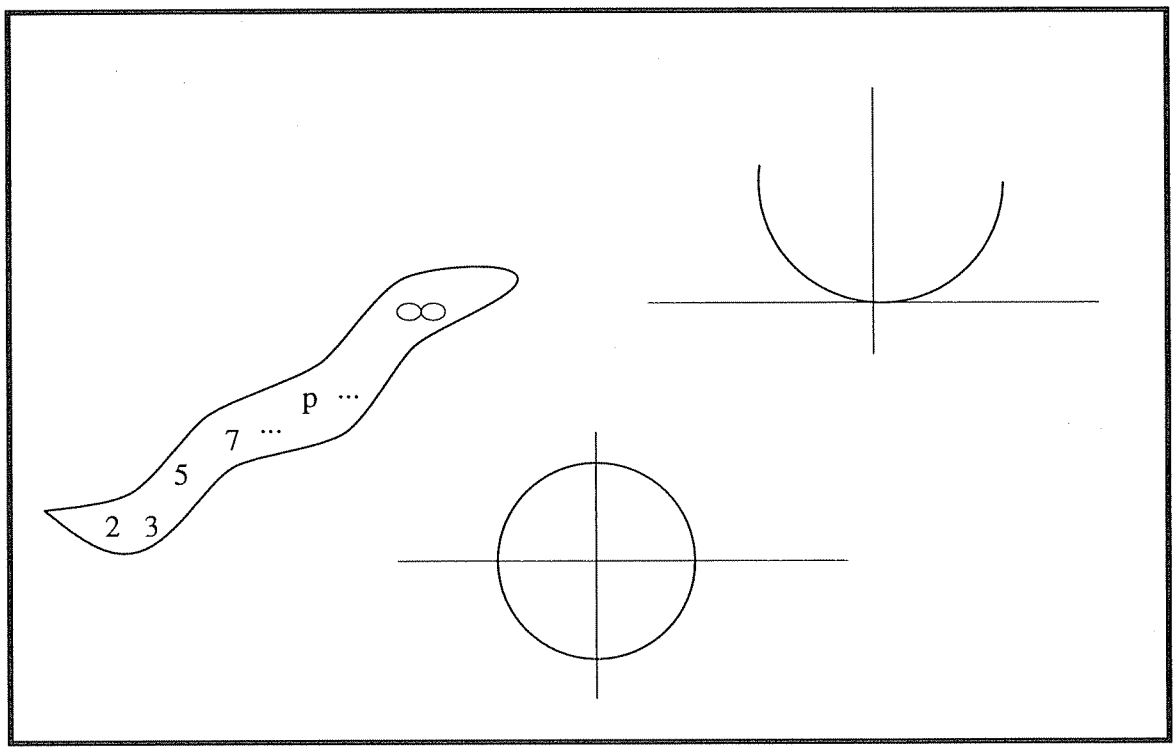

図１：多項式が定めるスキーム(「放物線」、「単位円」など)と整数環が定めるスキーム $\mathrm{Spec}(\mathbf{Z})$ は対等である。

ただ、「数は関数だ」と言われてもピンと来ない読者は少なからずいるだろう。そもそも「関数」というと、どのような**領域**の上で定義され、どのような**値**をとるものを念頭に置いているか、指定しないと話の趣旨が釈然としない

ものである。スキーム論では、その関数が定義されている領域という幾何的な対象のことを「スキーム」という。例えば、数論幾何では、ある意味では最も重要かつ基本的なスキームは、整数環 $\mathbf{Z}$ に対応するスキーム

$$\mathrm{Spec}(\mathbf{Z})$$

である。有理数体 $\mathbf{Q}$ や代数的数全体がなす「体」 $\overline{\mathbf{Q}}$ もそれぞれ、$\mathrm{Spec}(\mathbf{Q})$、$\mathrm{Spec}(\overline{\mathbf{Q}})$ というスキームに対応しているが、これらのスキームは、より基本的な $\mathrm{Spec}(\mathbf{Z})$ からある単純かつ自然な操作を施すことによって直ちに導かれるものなので、本稿では、$\mathrm{Spec}(\mathbf{Z})$ に集中することにする。一方、$x^n + y^n = 1$ のような方程式もスキームを定義している。そのスキームのことを、通常

$$V(x^n + y^n = 1)$$

と書く。このように多項式で定義されるスキームは名実ともに幾何学的な図形＝「代数多様体」なのである。例えば、$V(x^2 + y^2 = 1)$ の場合、高校数学からも想像が付くように、「単位円」のような代数多様体になる。

ところで、今まで気にしなかったことだが、代数多様体 $V(x^n + y^n = 1)$ は、2つの変数に対して、1つの制約を課すことによって定義されるものなので、その**次元**は、[自由度の数]−[制約の数]$= 2 - 1 = 1$ である。一次元の代数多様体のことを**代数曲線**という。一方、$\mathrm{Spec}(\mathbf{Z})$ は、スキームであっても、代数多様体（つまり幾何学的な図形）ではないので、その次元はそう簡単には定義できないが、数論幾何では、代数多様体の場合の（比較的透明な）次元の定義を適当に加工し抽象化することによって、$\mathrm{Spec}(\mathbf{Z})$ の次元を定義することもできる。その次元は、実は1なのである。そのことが縁で、$\mathrm{Spec}(\mathbf{Z})$ は「数論的な曲線」と呼ばれたり、代数曲線に類似的な性質をたくさん持っているのである。実際、このような視点は、上で紹介したスキーム論の精神にぴったりと符合するものである。ただし、$V(x^2 + y^2 = 1)$ が大体「単位円」のような形をしている＝「その点は大体単位円の点と思っていい」という状況と違って、$\mathrm{Spec}(\mathbf{Z})$ の点の正体はこれまでの話だけからは決して明らかではない。「付値」という名前で呼ばれ、集合としては、素数と、後「∞（＝無限大）」という記号からなる**数論的曲線 $\mathrm{Spec}(\mathbf{Z})$ の「点」**

$$2, 3, 5, 7, 11, 13, \ldots, p, \ldots, \infty$$

については、次節で詳しく説明する。

II. 有理数体の付値： 数と数の間の距離の色々な測り方

(A.) 距離と局所化

現代数論幾何の大きなテーマの一つは、「多項式の有理数解の様子を理解せよ」という非常に難しい命題に対して、

「多項式の有理数解は、その近似から攻めよ」

という考え方で対応することである。「近似」とはつまり、ぴったりと問題の多項式の解になっていなくてもその解に**近い**、すなわち問題の多項式を満たすのに近いもののことを言う。次節の「完備化」の話では、そのような近似の成す空間について考える予定だが、その前に、近似という概念を確立させるためには、まず、キーワードの「近い」という単語の意味について考察してみる必要がある。

そこで、二つの数、例えば整数 x, y が「近い」とは一体どういうことなのだろう。まず、一般論としてすぐ思い付くことは、x と y が「近い」ということは、要するにその差の $x-y$ が「小さい」ということと同じである。従って、「近さ」の概念を確立させるためには、「大きさ／小ささ」の概念を作れば十分である。それでは、

ある整数が「大きい / 小さい」とはどういうことなのだろう？

スキーム論の大義名分は即ち、「整数＝一種の関数」という主義の下で作業せよというものだから、それに従って考えるなら、まず「関数が小さい」とはどういうことなのか、検討しなければならない。図２には、典型的な関数の様子が描かれているが、それを見ると、関数が比較的大きくなっている「箇所」、「区域」もあれば、比較的小さくなっている「箇所」、「区域」もある。そこで、そのことからは、どのような結論を導けばいいかということが問題になる。もちろん、哲学的なレベルで考えると色々な結論は有り得るが、スキーム論が採用している視点は次のものである：

問題の関数が定義されている領域の、小さな区域ごと＝

突き詰めていくと点ごとに、個別の「大きさ / 小ささ」の概念が定まる。

つまり、二つの数が近い、またはある数が「小さい」ということには、一通りの自然な定義があるわけではなく、整数という名の関数の「仮想的定義領域」

である $\mathrm{Spec}(\mathbf{Z})$ の「点」ごとにその点に付随する「距離」の概念があり、かつ別々の点に対応する別々の距離はすべて対等である。また、現代数論幾何では、関数がやや小さくなったりやや大きくなったりする定義領域の中の小さな**区域**というものには、**「近傍」**または**「局所化」**という名前が付けられている。標語的にまとめると、

スキームの点 $\Longleftrightarrow$ スキームの局所化 $\Longleftrightarrow$ スキームの関数の距離の概念

という三種類の対象が同値で、自然に 1 対 1 で対応している。

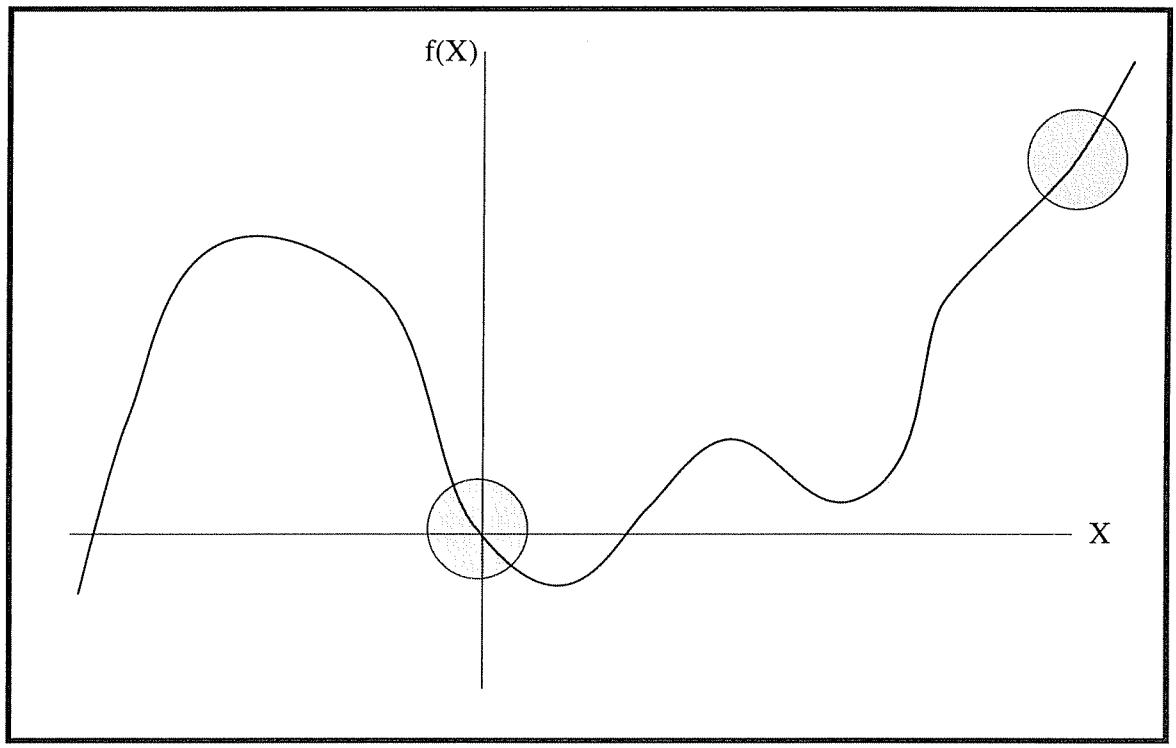

図２： 典型的な関数＋大きくなっている区域、小さくなっている区域。

さて、$\mathrm{Spec}(\mathbf{Z})$ という特定の数論的スキームにはどのような点があるのだろう。上の話によると、点を計算するには、整数環 $\mathbf{Z}$ に入る「距離」を全部調べればいいわけだが、「距離」というものには、実は自然な公理が有って、その公理を満たすもの — **付値**または**素点**と呼ぶのだが — が、実は、ある限られたものしかないことは分かっている。以下では、この $\mathrm{Spec}(\mathbf{Z})$ の付値を紹介したい。まず、一番簡単な付値は、「∞ （無限大）」という記号に対応するもので、この付値の定義は、整数 x に対して

$$|x|_\infty \stackrel{\text{def}}{=} x\text{の絶対値}$$

つまり、x の符号を忘れた数を対応させよというものである。（例：$|-3|_\infty = |3|_\infty = 3$。）この付値／素点のことを、**無限素点**ともいう。残りの付値は、**有限素点**と呼ばれ、各素数 p に対して定義されるのである。素数 p に対応する付値／素点は、**「p 進付値／素点」**といい、整数 $x = p^e \cdot y$（ただし、e, y は整数、y は p では割り切れないとする）に対して

$$|x|_p \stackrel{\text{def}}{=} p^{-e}$$

と定義される。従って例えば、p^{1000} のような数は、無限素点では非常に大きいけれども、p 進素点では小さいという寸法になっている。これらの付値はすべて $|x \cdot y^{-1}|_v = |x|_v \cdot |y|_v^{-1}$（ただし、$v$ は素数 p または ∞）という条件を満たすように任意の有理数 x と $y \neq 0$ に対して定義することができる。

最後に、「整数＝一種の関数」という描像を完結させるためには、整数 x が、例えば、$\mathrm{Spec}(\mathbf{Z})$ の素点 p（$= |\sim|_p$）でとる値が何なのかを説明しなければならない。（無限素点でとる値の話はもうちょっと難しいので、ここでは、有限素点の場合を中心に話を進める。）まず、二つの関数がある点で同じ値をとるということは、言い換えれば、その二つの関数の差がその点ではゼロ＝その点の近傍では差が小さいということである。例えば、x と y という整数が素点 p で同じ値をとるということは、$|x-y|_p < 1$ という条件で定義されている。つまり、$|\sim|_p$ の定義を思い出してこの条件を書き下してみると、それは要するに、「$x-y$ は p で割り切れる」＝「x と y は p を法として合同である」ということである。記号で書けば、

$$x \equiv y \bmod p$$

（ただし、mod は「modulo」（モジュロ）の略）と表される。つまり、スキーム論では、x という整数＝$\mathrm{Spec}(\mathbf{Z})$ 上の一種の関数が、**素点 p でとる値は、**「p を法として合同である」という同値関係に関する**「同値類」**なのである。従って、素点 p の場合は、$0, 1, 2, \ldots, p-1$ という p 個の数で（簡単に確認できるように）その同値類は尽きるわけだから、素点 p で整数がとり得る値は、ちょうどこの p 個の値

$$\{0 \bmod p,\ 1 \bmod p,\ 2 \bmod p,\ \ldots,\ p-1 \bmod p\}$$

の内の一つだということになる。

(B.) 積公式と大域化

上の話では、$\mathrm{Spec}(\mathbf{Z})$ の諸々の素点の多様性を強調してきたが、この素点たちが、完全にばらばらで独立かというと、そうでもなく、実は以下で紹介する法則に従って**連動**しているのである。その法則は**積公式**と呼ばれ、スキーム論の整数論の問題への応用では、極めて重要な役割を果たす。

積公式： 任意の零でない有理数 x は次の式を満たす：

$$\prod_{v=p,\infty} |x|_v = 1$$

ただし、この積で v は $\mathrm{Spec}(\mathbf{Z})$ のすべての付値を走るとする。

この性質の証明は、性質自身の重要性や応用範囲の割にはいたって簡単である。零でない有理数 x は、必ず

$$x = \pm p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$

（ただし、r は自然数、$p_1, p_2, \ldots, p_r$ は相異なる素数、$e_1, e_2, \ldots, e_r$ は整数とする）という形に書け、v が $p_1, p_2, \ldots, p_r$ の内のどれか一つ $= p_i$ の時、

$$|x|_v = p_i^{-e_i}$$

となり、v が $p_1, p_2, \ldots, p_r$ 以外の有限素点の時は、

$$|x|_v = 1$$

となる。なお、$v = \infty$ の時は、

$$|x|_\infty = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$

となるので、全部掛け合わせると、1 になる。（証明終）

次に、積公式の典型的な応用方法を紹介しよう：

例： $|a|_\infty \leq 8$ を満たす整数 a に対して、次の多項式を考えよう：

$$X^2 - a = 0$$

この多項式の解の候補として、例えば次の条件を満たす整数 n があがっているとする：

(1.) $|n|_\infty \leq 5$
(2.) $|n^2 - a|_5 < 1$
(3.) $|n^2 - a|_7 < 1$

つまり、n は無限素点ではさほど大きくない数で、しかも 5 と 7 という素点では、多項式 $X^2 - a = 0$ を満たすのに近い。こうしたとき、整数 $N \stackrel{\text{def}}{=} n^2 - a$ を見てみると、N は、$|N|_5 < 1$, $|N|_7 < 1$、従って（p 進付値の定義より）$|N|_5 \leq 5^{-1}$, $|N|_7 \leq 7^{-1}$ を満たしている上に、すべての有限素点 v では、$|N|_v \leq 1$ を満たし、かつ無限素点では、$|N| \leq 5^2 + |a| \leq 25 + 8 = 33$ を満たす。この情報を積公式に入力すると、$N \neq 0$ なら

$$1 \leq 5^{-1} \cdot 7^{-1} \cdot 33$$

となり矛盾が出る。従って、多項式 $X^2 - a = 0$ の解の候補としてあがっていた数 n は、表向き（つまり、仮定した条件を見た限り）ではただの近似でも、本当は、**完全に解になってしまわざるを得ない**（つまり、$n^2 - a = 0$）ことは、**積公式のおかげで**分かったわけである。

上の例は、積公式の応用の、簡単かつ初等的ながら非常に代表的なものである。抽象化すると、近似を、ある**局所的な条件**（$= |\sim|_v$ たちに関する条件）を満たすように用意し、それから積公式、つまり $|\sim|_v$ たちが連動しているという**大域的な**性質を利用することによって結論を導く。言い換えれば、局所化（＝各々の $|\sim|_v$ での状況を考えること）は、難しい大域的な問題（＝多項式の有理数解の決定のように、個々の $|\sim|_v$ たちで何かが小さいかどうかだけでは分からない問題）を、**よりやさしい局所的な問題に分解、解体する**役割を果たし、積公式はそうして入手した**諸々の局所的な情報を「張り合わせる」**（＝再大域化する、組立て直す）役割を果たすのである。

III. 完備化： 数列の極限が織り成す数論と幾何

(A.) 完備体にすむ数たち

前節では、近似というものの重要性を議論してきたが、多くの場合、一個の近似ではなく、精度が次第に良くなっていくたくさん（無限個）の近似を組織的に扱った方が、物事の様子が分かりやすくなる。このように「たくさんの

近似を組織的に扱うこと」、即ち**近似の列**やその**極限**を導入し、多項式の解の研究に応用することは、専門用語でいうと、**「完備化」**を考えるということに当たる。

ただ、完備化を定義する前に、まず「体」という概念を導入しなければならない。**体**とは、足し算、引き算、掛け算、（零でない元による）割り算という四つの操作ができる「数」の集合である。例えば、有理数体は体であり、証明はもうちょっと難しくなるが、I., (A.), に出てきた代数的数全体のなす集合 $\overline{\mathbf{Q}}$ も体になる。なお、高校数学にも登場する実数体 $\mathbf{R}$ や複素数体 $\mathbf{C} = \{a + b\sqrt{-1} \mid a, b \in \mathbf{R}\}$ も体である。「完備化」という操作は、「数が小さい」ということが定義されている体に対して行なわれるもので、その結果として出てくるものは**「完備体」**になる。

さて、完備化というものを定義しよう。以下では、K を体とし、

$$|\sim|_K : K \to \mathbf{R}_{\geq 0} \stackrel{\text{def}}{=} \{x \in \mathbf{R} \mid x \geq 0\}$$

を、K 上で定義され、負でない実数に値をとる写像で、K に入っている数たちの大きさを測るものとしよう。つまり、$k \in K$ が小さいということは、$|k|_K$ という実数が小さいということで定義するのである。このような情報に対して、Cauchy（コーシー）数列を定義しよう：

Cauchy 数列とは、K の元たちの列 $\{k_n\}_{n=0,1,2,\ldots}$ で、任意の正の実数 $\epsilon > 0$ に対して、次の性質を満たす整数 N が必ず存在するもののことをいう：

$$\forall\, n, m \geq N,\ |k_n - k_m|_K < \epsilon$$

例えば、$K = \mathbf{R}, \mathbf{C}$ の場合、この概念は、大学の教養レベルの数学にも登場するが、実は、$\mathbf{R}$ や $\mathbf{C}$ だけではなく、任意の体に対して定義されるものである。その定義は、普通の言葉に直すと、N が大きくなるにつれて、その N から先の k_n たちはすべて互いに近くなっていく。つまり、N が大きくなると、密集してくるので、集積点、即ち**極限が存在する筈**の数列になるわけだが、与えられた体 K の中にその極限が実際に存在するかどうかは分からない。そこで、

そのような極限たちを、「人工的に」 K に付け加えたものとして

K の（$|\sim|_K$ に関する）完備化 $\widehat{K}$ を定義する。

ここで、この「人工的な極限たち」というのは、K の Cauchy 数列全体を、次の同値関係で割ったものである：二つの Cauchy 数列 $\{k_n\}_{n=0,1,\ldots}, \{k'_n\}_{n=0,1,\ldots}$ が、

$$\lim_{n\to\infty}(k_n - k'_n) = 0$$

（つまり、任意の正の実数 $\epsilon > 0$ に対して、$\forall n \geq N, |k_n - k'_n|_K < \epsilon$ が成り立つ整数 N が必ず存在する）を満たす時、その二つの Cauchy 数列を**同値**とみなす。この同値関係に関する同値類たちが、「人工的な極限たち」、即ち、完備体 $\widehat{K}$ を構成する「数たち」である。なお、数列に現れる元たち（$= k_n$ たち）ごとの加減乗除を行なうことによって、人工的な極限たちに対しても加減乗除を矛盾なく行なうことができるので、人工的な極限たち全体は、約束通り体になるのである。

本稿では、$\mathbf{Q}$ の整数論をテーマとしているので、$\mathbf{Q}$ の諸々の完備化たちを確認しておこう。体 $\mathbf{Q}$ が決まると、完備化を定義するのに、あとは、数の大きさを測る "$|\sim|$" を指定しなければならないが、その "$|\sim|$" に無限素点の $|\sim|_\infty$ をとると、実数の定義から簡単に確認できるように、完備化は実数体

$$\mathbf{R}$$

になる。例えば、1, 1.4, 1.41, 1.414, 1.4142, ... という $\sqrt{2}$ の十進法展開

$$\sqrt{2} = 1.4142\ldots$$

から決まる Cauchy 数列を考えることによって、$\sqrt{2}$ という数が $\mathbf{Q}$ の $|\sim|_\infty$ に関する完備化に入っていることが直ちに分かる。一方、完備化の距離 "$|\sim|$" として、p 進付値 $|\sim|_p$ を採用すると、p **進数体**と呼ばれる体

$$\mathbf{Q}_p$$

ができる。例えば、$p = 7$ の時、

$$\sqrt{2} = 3 + 1\cdot 7 + 2\cdot 7^2 + \ldots \in \mathbf{Q}_7$$

つまり、二乗したら 2 になる数が $\mathbf{Q}_7$ に入っていることは簡単に示せる。一般の p に対する $\mathbf{Q}_p$ の深い性質については、本稿では詳しく解説する余裕はないが、実数体を基にした「普通の解析」があるように、この p 進数体 $\mathbf{Q}_p$ を出発点とする「p **進解析**」という分野がある。p 進解析では、普通の解析に出てくる様々な馴染み深い対象たちの類似物がここ数十年で発見されていて、数論幾何全体の中でもますます重要になってきている。

完備体の重要な性質の一つとして、

多項式を「完備体の上で考える」（＝多項式の解を完備体の中に求める）と、完備化する前の体と較べて、非常に解き易くなる。

これは、要するに、完備体の定義から、完備化する前の体から見て解の近似にしかならないものを、完備体では「歴とした解」と（人工的に）認めているからである。以下では、多項式が一変数の場合に、この現象をもう少し詳しく検証していきたい。 まずは、無限素点の場合だが、$\mathbf{R}$ 上の一変数多項式で $\mathbf{R}$ に解を持たないものは、二次のものしかないことはごく初等的に証明できる。更に $i = \sqrt{-1}$ を $\mathbf{R}$ に添加して、

複素数体 $\mathbf{C}$ 上で考えると、任意の一変数多項式

$$X^n + c_{n-1} \cdot X^{n-1} + \ldots + c_1 \cdot X + c_0 = 0$$

は、必ず複素数体に解を持つ。

（ただし、$c_0, \ldots, c_{n-1} \in \mathbf{C}$。）このように、一変数多項式が必ず解を持つような体のことを、**（代数的）閉体**という。つまり、有理数体 $\mathbf{Q}$ を無限素点で完備化すると、「閉体の一歩手前」の体（$= \mathbf{R}$）ができる。

一方、p 進数体 $\mathbf{Q}_p$ の方だが、閉体にはならないし、閉体の一歩手前ともいえないが、ある一変数多項式 $X^n + c_{n-1} \cdot X^{n-1} + \ldots + c_1 \cdot X + c_0 = 0$（ただし、$c_0, \ldots, c_{n-1} \in \mathbf{Q}_p$）が解を持っている時、この多項式に「十分近い」$n$ 次の一変数多項式（＝その係数が $c_0, \ldots, c_{n-1}$ に、$| \sim |_p$ に関して十分近い）は、必ず解を持つという性質が成り立つ。証明が（代数方程式の数値解法の基本的な手法である）Newton（ニュートン）の反復法にルーツを持つこの性質は、**「Hensel（ヘンゼル）の補題」**と呼ばれ、p 進数体 $\mathbf{Q}_p$ を出発点とする研究では非常に重要である。

(B.) 完備体上の多項式が定める図形

上の話では、体を完備化すると、（少なくとも一変数）多項式が、$\mathbf{Q}$ の時と較べて非常に解き易くなるという現象を見てきたが、実は、多変数の多項式の場合でも似たような現象が起こる。多変数の多項式だと、その多項式によって代数多様体＝幾何学的な図形が定まるので、**基礎体**（＝係数が入っていたり、多項式の解を求めたりする体）によって、その図形の点たちの様子が変わってくる。その変わり方が大体どのようなものかというと、基礎体が有理数体 $\mathbf{Q}$ の場合は、ちょうど実軸の中に入っている有理数点（図3を参照）のように、（完備体を基礎体にとる場合に対応する）滑らかで一様な実軸全体と較べて、ぽつぽつと点在していて黒い連続体の夜空にちらばる星々のような恰好をしている。

しかも、考えている多項式の次数が上がると、$\mathbf{Q}$ が基礎体の時は完備体上で考えた場合と較べて点が更に珍しくなって、フェルマの方程式 $x^n+y^n=1 \quad (n \geq 3)$ のように完全かほとんど完全になくなってしまうことまである。つまり、基本的な傾向としては、完備体を基礎体にとると多項式が定める図形が**滑らかで一様な物質**でできているかのような様子を呈してくる。この現象は一変数多項式が完備体の上では非常に解き易くなるという現象と密接に関係していて、正にその現象の多変数版といってもよい。

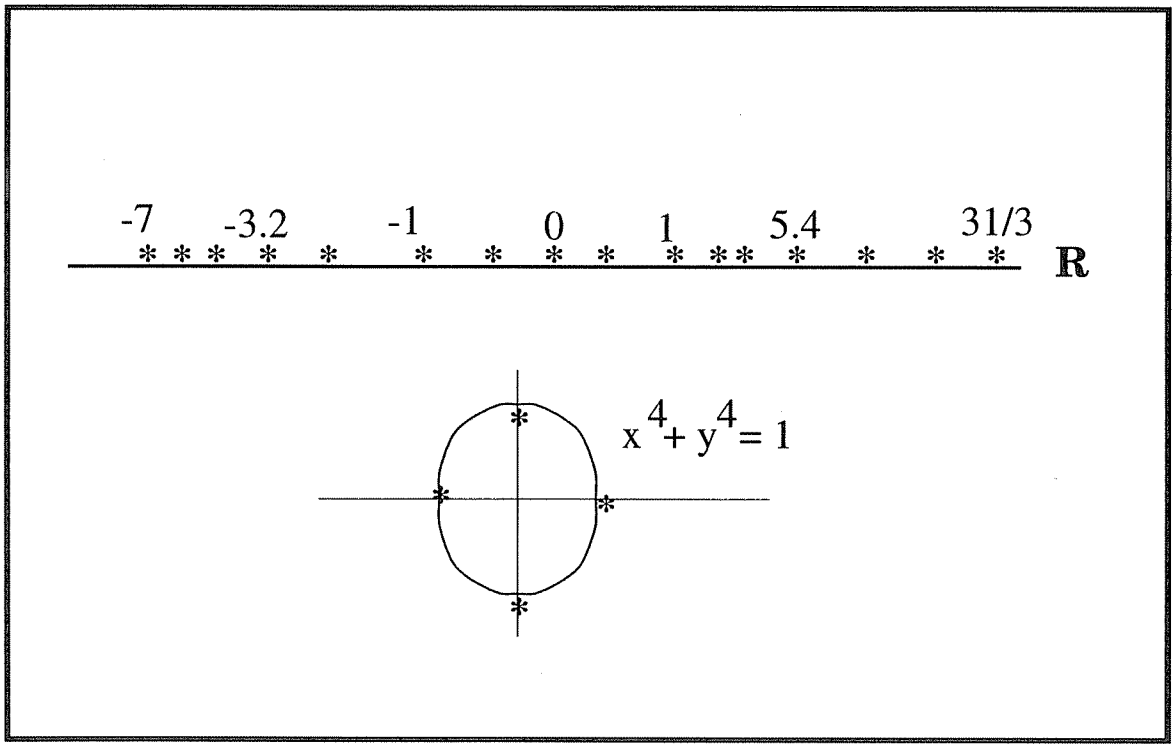

図３：有理数体上の点は珍しい。

次に、複素数体 $\mathbf{C}$ 上の d 次二変数多項式

$$\sum_{i+j \leq d} c_{i,j} \cdot X^i \cdot Y^j = 0$$

（ここで、$c_{i,j}$ たちはすべて複素数）について考えよう。この多項式が定める代数多様体の点は、多項式を満たす複素数の組 (X, Y) 全体である。この場合、基礎体としている複素数体は閉体なので、定まる代数多様体が非常に分かりやすい構造をしているはずである。実際、この場合、対応する代数曲線＝一次元

の代数多様体は**滑らかな曲面**になる（図4を参照）。その曲面は、（欠けている「無限遠点」を付け加えたり、少し尖っているところを滑らかにしたりするという簡単な技術的操作をすることを除けば）あるいは**球面**になるか、あるいは**球面に幾つかの「ハンドル」**（＝‘取っ手’）を施したものになるか、ということが知られている。その付け加わるハンドルの数は、曲面の**種数**（英語名：genus）と呼ばれる多様体の基本的な不変量になる。出発した多項式の係数たち $c_{i,j}$ の多くがゼロになったり、その他の意味で退化になったりしない「一般的な場合」には、種数は、次の公式によって多項式の次数 d から簡単に求まる：

$$\text{種数} = \frac{1}{2}(d-1)(d-2)$$

本稿では、特に $d = 3$、種数＝1の場合に注目して話を進めていきたい。この場合には対応する代数多様体は**楕円曲線**と呼ばれ、数論幾何では非常に重要な研究対象となっている。楕円曲線には様々な特別な性質が見られるが、中でも取り分け重要なのは**加群構造**の存在である。「加群構造」が入っている代数多様体の場合、その点たちに対して、普通の数と同様に矛盾なく足し算と引き算ができる。この足し算と引き算のような操作のことを**「群演算」**という。このように点に対して矛盾を発生しない群演算が定義可能な種数の曲面は、（曲面から点を抜いたりしない限り）種数1だけしかない。点を抜くことを許せば、楕円曲線の場合以外にも、種数0の曲面＝球面から1点を抜いてできる

$$\mathbf{G}_{\mathrm{a}} \stackrel{\mathrm{def}}{=} V(Y = 0)$$

（＝複素数体上では「平面」）と、2点を抜いてできる

$$\mathbf{G}_{\mathrm{m}} \stackrel{\mathrm{def}}{=} V(XY - 1 = 0)$$

（＝複素数体上では「平面」から原点を除いてできる多様体）にも加群構造が入る。$\mathbf{G}_{\mathrm{a}}$ の場合、点は基礎体 K と同じ集合になって、群演算も体 K の普通の足し算と引き算になる。$\mathbf{G}_{\mathrm{m}}$ の場合、点は基礎体 K の零でない元たちからなる集合 $K^{\times}$ になって、群演算は体 K の普通の掛け算と割り算に当たる。

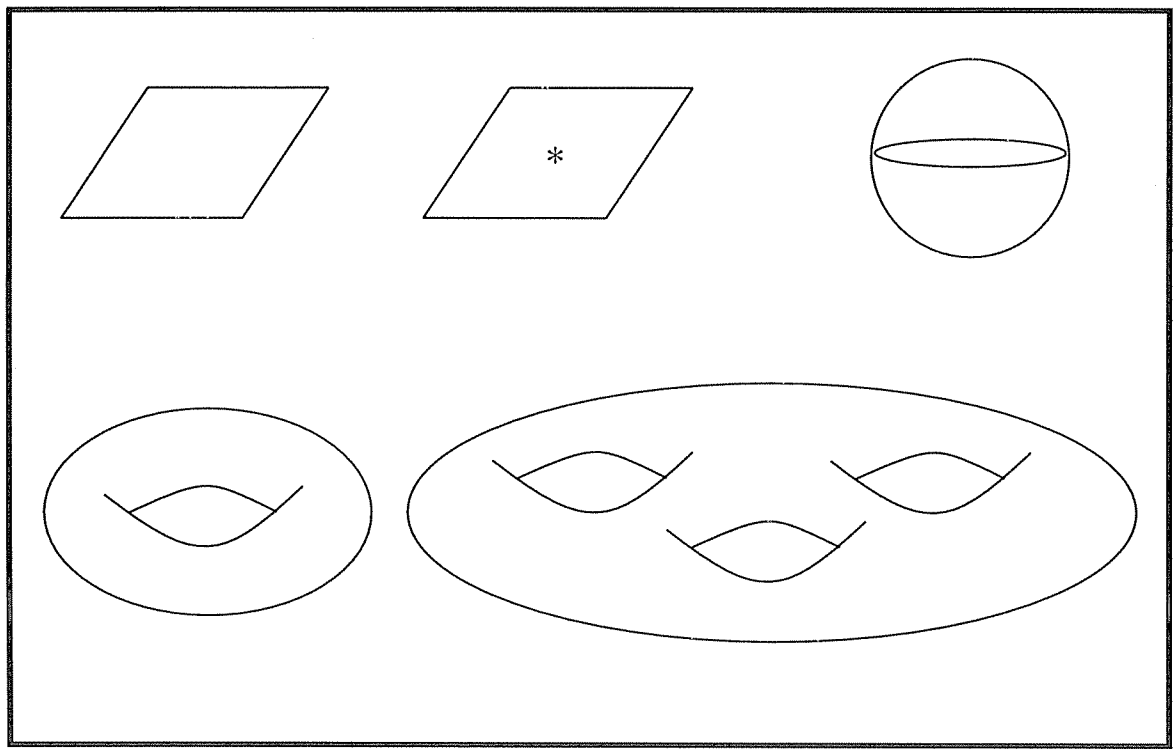

図４：完備化すれば、滑らかな物質でできたつるつるした表面の幾何的対象が誕生。（複素平面＝$\mathbb{G}_{\mathrm{a}}$、複素平面マイナス原点＝$\mathbb{G}_{\mathrm{m}}$、種数０の曲面、楕円曲線＝種数１の曲面、種数３の曲面。）

楕円曲線の場合、群演算を具体的に表示することはもう少し難しくなるので、ここでは次のことを指摘するにとどめる：三次式で定義される楕円曲線と、任意の直線の交わる（重複度込みで勘定した時の）三点 A, B, C の（楕円曲線の群演算に関する）和

$$A + B + C$$

は、必ず０（＝楕円曲線の群演算に関する「原点」）になる（図５を参照）。

IV. 一意化： 多項式の解の標準的な名簿

(A.) 幾つかの具体例

前節の完備化の話では、有理数体のような体ではなく、その完備化の上で多項式を考えると解き易くなる、つまり、多項式が定める代数多様体がたくさんの点を持つという現象を検証してきたが、点が多くなったのであれば、

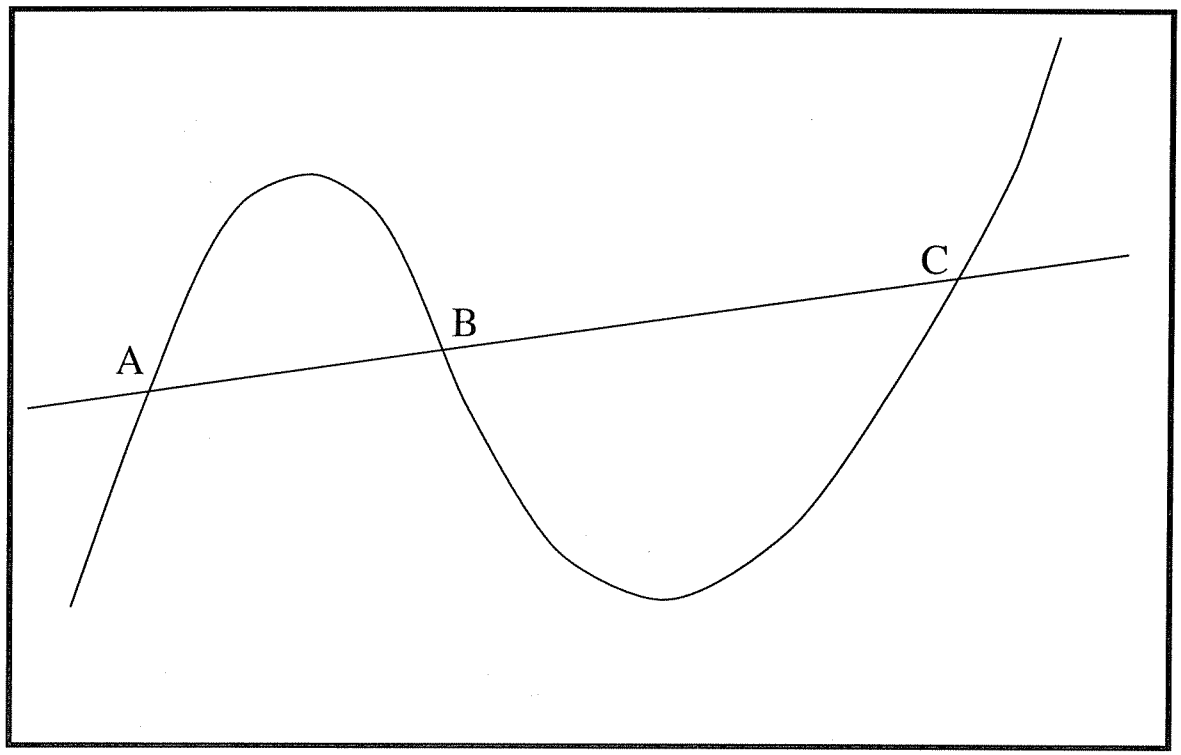

図５：三次式で定義される曲線と直線が交わる三点。

その点たちを整理して、自然な名前を付けたり、点たちの名簿を作ったりしたくなる。そのような点の**名簿＝リスト＝カタログ**が、**一意化**である。

代数多様体の一意化で、ある意味ではもっとも簡単かつ基本的な例は、複素数体上の

$$\mathbf{G}_{\mathrm{m}} \stackrel{\mathrm{def}}{=} V(XY-1=0)$$

の一意化である。この場合、指数関数 exp を使うことによって、$\mathbf{G}_{\mathrm{m}}$ を $\mathbf{C}$ で一意化することができる：

$$\exp : \mathbf{C} \to \mathbf{G}_{\mathrm{m}}$$

$$z \mapsto (X,Y) = (\exp(z), \exp(-z))$$

この一意化は、言い換えれば $\mathbf{G}_{\mathrm{m}}$ の複素数体上の点たちにいわば「番号を振る」という作業に当たるもので、番号に相当するものは、$\mathbf{C}$ の元である。その $\mathbf{C}$ の元 z に対して、$X = \exp(z)$, $Y = \exp(-z)$ という $\mathbf{G}_{\mathrm{m}}$ の点を対応させていくわけである。

楕円曲線の場合でも、**楕円関数**という特別な関数による一意化がある。楕円関数の中でもっとも基本的なものはWeierstrass （ワイエルシュトラス）$\wp$（ペー）-関数と呼ばれ、次のような形をしている：まず、**周期**と呼ばれる複素数τを固定しておく。なお、慣例に従って、τの虚部（＝複素数$\tau = a + ib$ $(a, b \in \mathbf{R})$と書いた時、bのこと）が正であると仮定する。そうしたとき、複素数zに対して、$\wp$-関数を

$$\wp(z) \stackrel{\text{def}}{=} \frac{1}{z^2} + \sum_{n,m \in \mathbf{Z},\ (n,m) \neq 0} \left(\frac{1}{(z - n - m\tau)^2} - \frac{1}{(n + m\tau)^2} \right)$$

で定義する。更に、複素定数$g_2, g_3 \in \mathbf{C}$を

$$g_2 \stackrel{\text{def}}{=} 60 \sum_{(n,m) \neq 0} \frac{1}{(n + m\tau)^4}; \quad g_3 \stackrel{\text{def}}{=} 140 \sum_{(n,m) \neq 0} \frac{1}{(n + m\tau)^6}$$

（ただし、$\sum$のn, mは、$(0,0)$以外のすべての整数の対を走るとする）と定義すると、$\wp(z)$とその微分$\wp'(z) \stackrel{\text{def}}{=} d\wp(z)/dz$は次の関係式を満たす：

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

つまり、言い換えれば、$(X, Y) = (\wp(z), \wp'(z))$という点は

$$Y^2 = 4X^3 - g_2X - g_3$$

という三次式が定義する楕円曲線の上にのっているということである。実は、ここでは証明しないが、この楕円曲線の複素数体上のすべての点は、適当な複素数zに対して$(\wp(z), \wp'(z))$という形に書ける。しかも、座標変換を除けば、任意の楕円曲線が、適当なτに対して$V(Y^2 = 4X^3 - g_2X - g_3)$という形に書けることが知られているので、これで、Weierstrass $\wp$-関数（とその微分）によって、任意の楕円曲線が一意化される＝すべての複素数体上の点に$(\wp(z), \wp'(z))$というラベルが付けられる：

$$(\wp(-), \wp'(-)) : \mathbf{C} \to E \stackrel{\text{def}}{=} V(Y^2 = 4X^3 - g_2X - g_3)$$

$$z \mapsto (\wp(z), \wp'(z))$$

ことが分かる。

実は、III., (B.) に出てきたような種数がもっと高い代数曲線も自然に一意化される。種数が 2 以上の時は、複素平面 $\mathbf{C}$ 全体ではなく、「**上半平面**」と呼ばれるその上半部分 $\mathfrak{H} \stackrel{\text{def}}{=} \{z \in \mathbf{C} \mid \text{虚部}(z) > 0\}$ によって一意化される。この事実は、**Köbe（ケーベ）の一意化定理**と呼ばれ、複素数体上の代数曲線に関する非常に基本的な結果である。

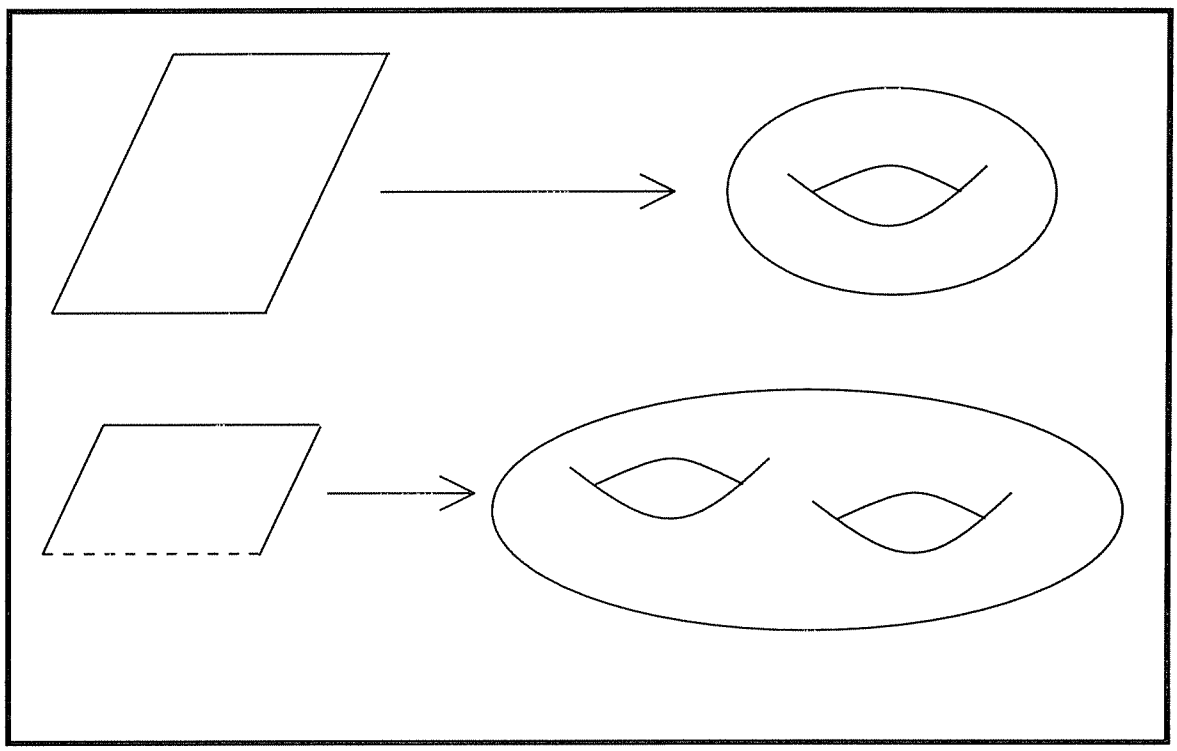

図６：完備化してできる代数多様体の点には、複素平面や上半平面のような単純な幾何的対象上で定義される一意化写像による自然な「名前」が付いている。

今まで、複素数体という「無限素点系」の体の上で一意化という現象を紹介してきたが、実は、p 進数体の上でも、$\mathbf{G}_{\mathrm{m}}$ や楕円曲線、更に種数が高い代数曲線に対する自然な一意化が知られている。p 進の場合は、技術的には複素数体の場合より遥かに難しくなるので、ここでは、$\mathbf{G}_{\mathrm{m}}$ の一意化を定義する指数関数の巾級数展開

$$\exp(z) = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \ldots + \frac{z^n}{n!} + \ldots$$

が、(少なくとも p が奇数なら) $|z|_p < 1$ を満たす p 進数 $z \in \mathbf{Q}_p$ を代入した時でも $|\sim|_p$ に関して**収束**することを指摘するにとどめる。

(B.) 一意化の概念と Hodge (ホッジ) 理論

一意化理論、即ち、完備体上の代数多様体の点の自然な列挙方法は、もう少し加工して見ると、次のように解釈することもできる。(A.) で紹介したような自然な一意化による点への「番号の振り方＝名前の付け方」は、決して勝手なものではなく、代数多様体の、一つの**図形としての幾何学や対称性**と深く関係している。この視点を追究すると、一意化というものの本質が、

多項式の解 $\Longleftrightarrow$ 対応する図形の幾何学 / 対称性

つまり、多項式の解と、多項式が定める図形の幾何学や対称性の間の一種の同値性を主張しているところにあると見ることができる。**Hodge (ホッジ) 理論**では、このような同値性は更に高いレベルにまで磨き上げられていて、「点」以外の代数多様体に付随する様々な構造や不変量に対して、多項式系のものと、代数多様体の**位相**＝図形の幾何学や対称性によるものの間に一種の同値性が成り立つことが知られている。言い換えれば、上で紹介した**一意化の例は Hodge 理論の原型**ともいえる。

ただし、現時点では、複素数体や p 進数体のような**完備体**の上では Hodge 理論はかなり高度なレベルに発展しているが、有理数体 $\mathbf{Q}$ のような**「大域体」**の上では同様な一意化理論や Hodge 理論はまだ発見されていない。そのような**大域的な Hodge 理論**の構築は、現代数論幾何の大きな課題といえよう。実際、思い出してみれば、有理数体 $\mathbf{Q}$ 上で完璧な一意化理論があったら、それは要するに有理数体上の多項式の解を列挙する組織的な方法が見つかったことになるので、I.,(A.), で紹介した数論幾何の元々の動機付けである「多項式の有理数解を理解せよ」という問題を事実上解決したことになる。

V. 現代数論幾何を代表する結果の紹介

(A.) 有理点の有限性定理

代数多様体の **Q-有理点** (＝有理数体 $\mathbf{Q}$ 上の点) は、一般にはどちらかというと珍しいものだということを、III., (B.), の議論でも指摘したが、現代数論幾何の大きな勝利の一つは、その「経験則」に厳密な数学的基礎付けを与えることができたことにある。有理点が珍しいという感覚には色々な精密化の仕

方があるが、恐らくもっとも基本的なのは、「有理点は有限個しかない」というものであろう。種数が2以上の時は、このことは二十世紀初頭にMordell（モルデル）によって予想され、ついに１９８３年にFaltings（ファルティングス）によって証明された。

定理（Faltings） 種数2以上の有理数体$\mathbf{Q}$上の代数曲線の有理点の個数は有限である。

この定理の証明は、スキーム論の恰好の応用であり、有理数体という大域的な体に関するものでありながら、「局所体」＝完備体上のHodge理論を適用した後、そうして得た局所的な情報を、積公式を使って張り合わせて大域的な結果を導くという論法の典型的な例でもある。ただし、有理点の有限性を直接証明する代わりに、**「アーベル多様体のTate（テート）予想」**を先に証明して、そのTate予想を使って有理点の有限性を導くのである。アーベル多様体とは、楕円曲線の高次元版ともいえる非常に特別な種類の代数多様体のことである。「Parshin（パルシン）のトリック」と呼ばれるある簡単な操作をすると、与えられた代数曲線の有理点が、ある条件を満たす「アーベル多様体」と1対1に対応しているが分かるので、有理点の有限性をいうには、そのようなアーベル多様体の有限性をいえば十分だが、そちらの方の有限性は、Tate予想を用いて証明することができる。Tate予想については、一次元のアーベル多様体である楕円曲線の場合に、次節で詳しく説明する。

因みに、楕円曲線の有理点だが、種数が2以上の場合と違ってその数は必ずしも有限ではない。ただし、任意の有理点ではなく、**等分点**という特殊なタイプの有理点に限定すれば、有限性はいえる。「等分点」とは、$N\cdot\tau=0$（つまり、楕円曲線の加群構造では、τをN回足したら、0になる）となる自然数$N\neq 0$が存在するような点τのことである。$N\cdot\tau=0$を満たす等分点τを、N等分点という。

定理（Mordell-Weil） 有理数体$\mathbf{Q}$上の楕円曲線の等分点の個数は有限である。

この定理は、二十世紀初頭にはじめて証明され、上のFaltingsの定理から導くこともできる。

(B.) Tate（テート）予想

有理数体$\mathbf{Q}$上の楕円曲線Eを複素数体上で見ると、トーラスの形をしていて、IV., (A.), で紹介した$\wp$-関数による一意化を使えば、このトーラスを、

$0, 1, \tau, 1+\tau$ という四つの点を頂点にもつ平行四辺形（ただし、平行四辺形の上下または左右の二辺を同一視する）と見ることができる。この平行四辺形を採用したのは、複素平面 $\mathbf{C}$ 全体の上で定義されている一意化写像 $(\wp(-), \wp'(-))$ をこの平行四辺形に制限すると、写像は楕円曲線の（複素数体上の）**すべての点をちょうど一回だけ覆う**からである（図7を参照）。すると、等分点たちは、

$$a + b\tau \in \mathbf{C}$$

（ただし、$a, b \in \mathbf{Q}; 0 \leq a, b \leq 1$）という形に書ける点たちに対応する。

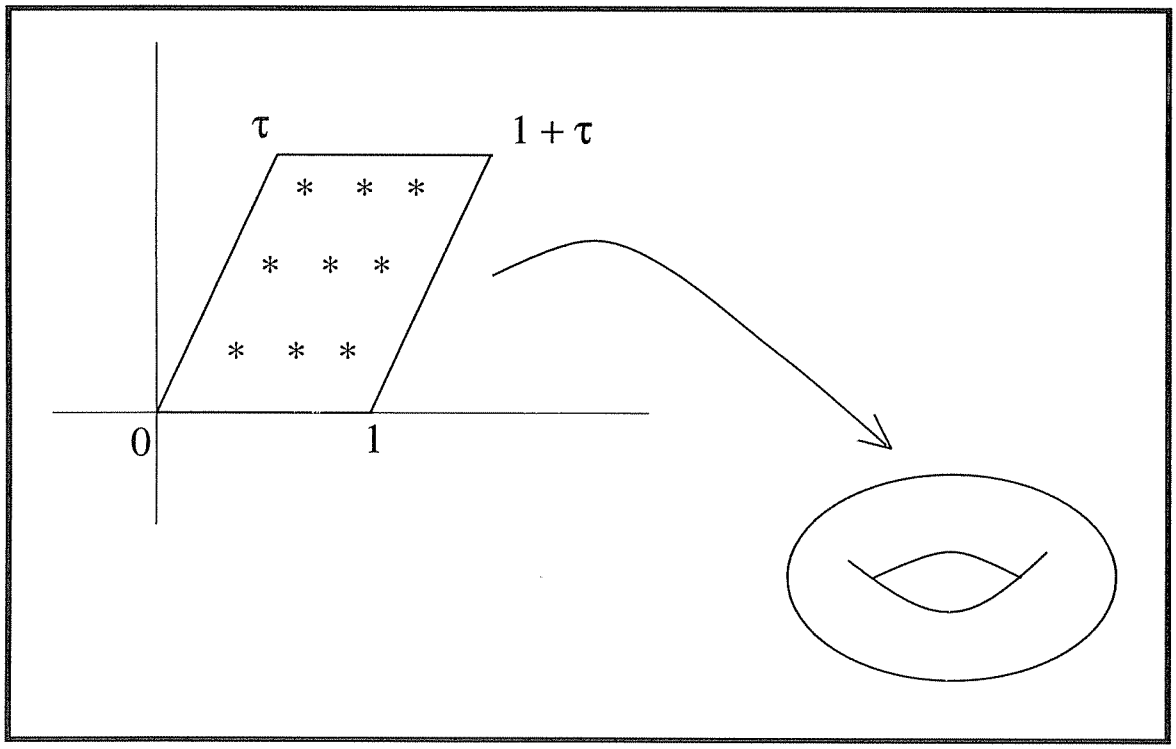

図7：一意化から見た等分点たち。

ただし、複素数体の上で考えないと存在しない一意化に関して等分点の座標が、$a + b\tau \in \mathbf{C}$（ただし、$a, b \in \mathbf{Q}$）のような簡単な形をしていても、元々楕円曲線を有理数体上で定義するために使った三次式

$$\sum_{i+j \leq 3} c_{i,j} \cdot X^i \cdot Y^j = 0$$

から譲り受ける X と Y という座標では、等分点は一般にはこのような簡単な形には書けない。等分点をこの X と Y という座標で記述しようとすると、一般にはいろいろな複素数（実は、代数的数だが）が必要になってくるが、これらの複素数を含む $\mathbf{C}$ の中の最小の部分体（＝これらの数を含み、かつ加減乗除について閉じている最小の集合）を、

$$\mathbf{Q}(E[\infty])$$

と書くことにする。同様に、すべての等分点ではなく、（自然数 N に対して）N 等分点の座標に出てくる数を含む $\mathbf{C}$ の最小の部分体を

$$\mathbf{Q}(E[N])$$

と書く。すると、もっとも基本的な場合には Tate 予想は次のことを主張している：

定理（Faltings） 有理数体 $\mathbf{Q}$ 上の二つの楕円曲線 E, E' に対して、E と E' が「同型」（＝座標変換を除いて同じ三次式で定義される）になるためには、すべての自然数 N に対して $\mathbf{Q}(E[N])$ と $\mathbf{Q}(E'[N])$ が（$\mathbf{C}$ の部分体として）一致することは、（本質的に有限個しかない）ある例外的な E と E' を除いて必要かつ十分である。

E と E' が同型な時は、$\mathbf{Q}(E[N])$ と $\mathbf{Q}(E'[N])$ が一致することを証明することは簡単だが、逆は難しいので、以下では逆に関する Faltings の証明を大部簡略化された形で紹介する。すべての自然数 N に対して、この二つの部分体が一致することを仮定しよう。すると、E と E' が同型になることを証明するということを、「よい座標 X, Y」を選んだ時、それぞれの定義式の係数が一致するかどうかという問題に解釈することができる。これらの係数は、全部有理数なので、積公式から分かるように（II., (B.), の例を参照）その係数が、多くの付値 $|\sim|_p$ や $|\sim|_\infty$ に関して十分に近いことさえ言えれば、完全に一致してしまうことが分かる。ところが、すべての自然数 N に対して部分体 $\mathbf{Q}(E[N])$ と $\mathbf{Q}(E'[N])$ が一致するという条件を p 進数体上の Hodge 理論を使って解釈すると、多くの p 進素点では E と E' の定義方程式の係数が近いことが出る。これで証明は完結する。

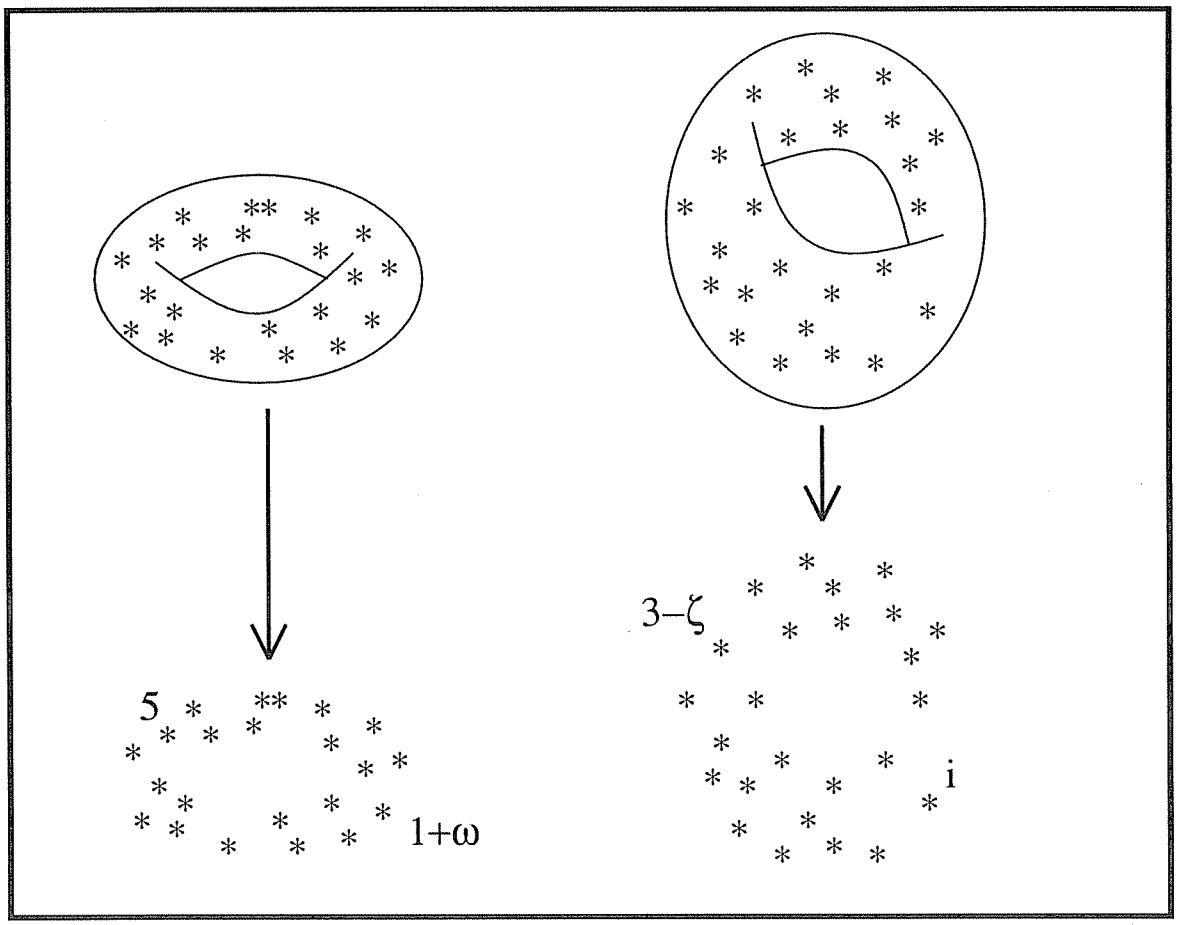

図８：「楕円曲線の身元は、その等分点の座標に登場する数たちに筒抜け。」
（ここで、$\omega = \frac{1}{2}(1+\sqrt{-3}), \zeta = \frac{1}{\sqrt{2}}(1+\sqrt{-1})$。）

参考文献

[1] 望月新一、「基本群に映る双曲的代数曲線の構造」、数理科学 **36** 巻７号（１９９８）、４１～４７頁。

[2] 望月新一、「モチーフ — 代数多様体の数論的骨格 — 」、数学セミナー **38** 巻５号（１９９９）、３０～３１頁。

[3] 中村博昭、「グロタンディークのガロア理論」、数学セミナー **35** 巻９号（１９９６）、２４～２５頁。