有限体と方程式の解の数*

大坪紀之†

1 序

フェルマー方程式

$$x^N + y^N = 1$$

の有理数解は, $N \geq 3$ の時, 自明なものしかない. このフェルマー予想は 1994 年, ワイルズによって証明された. しかしこの魅力的な方程式は, まだまだその輝きを放ち続けるであろう. 一方, この方程式の有限体における解の個数は 1949 年, ヴェイユによって計算され, 同時に提出されたヴェイユ予想はその後の数論幾何学の発展の原動力となってきた.

この講義では有限体を紹介し, 有限体における方程式の解の個数を数える. そこには驚くべき規則性があり, それがヴェイユ予想によって美しく記述されることを述べる. その背後には代数多様体 (より一般にスキーム) という幾何学的対象と, それらのコホモロジー群という代数学的対象が隠れているが, そこまでは立ち入ることができない. 諸君の今後の勉強に期待する.

2 有限体

2.1 合同数

以下, N は 2 以上の自然数とする.

定義 2.1. 整数 a, b が N **を法として合同**とは, $a - b$ が N で割り切れることである. 言い換えると, a, b を N で割った余りが等しいことである. この時, $a \equiv b \pmod{N}$ と書く.

整数 a に対して, $a \equiv b \pmod{N}$ となる $b \in \{0, 1, \ldots, N-1\}$ がただ 1 つ存在する. この b は a を N で割った余りである.

*日本数学オリンピック夏季セミナー (2010 年 8 月 25 日, 清里) における講演のノート.

†千葉大学大学院理学研究科, otsubo@math.s.chiba-u.ac.jp

定義 2.2. 整数の集合 $\mathbb{Z}$ から, N を法として合同な整数を同一視することによって得られる集合を $\mathbb{Z}/N\mathbb{Z}$ と書く. 整数 a から (同一視によって) 得られる $\mathbb{Z}/N\mathbb{Z}$ の元を $\overline{a}$ と書く.

つまり, $a \equiv b \pmod{N}$ の時, またその時に限り, $\mathbb{Z}/N\mathbb{Z}$ において $\overline{a} = \overline{b}$ である. 例えば,

$$\cdots \overline{-2N} = \overline{-N} = \overline{0} = \overline{N} = \overline{2N} = \cdots$$

$$\cdots \overline{-2N+1} = \overline{-N+1} = \overline{1} = \overline{N+1} = \overline{2N+1} = \cdots$$

である. 上の注意より,

$$\mathbb{Z}/N\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{N-1}\}$$

であり, これは N 個の元からなる集合である.

定義 2.3. $\mathbb{Z}/N\mathbb{Z}$ 上の和と積をそれぞれ

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{ab}$$

で定める.

$\mathbb{Z}/N\mathbb{Z}$ の元をいつも $\{0, 1, \ldots, N-1\}$ を用いて表すことにすると,

$$\overline{a} + \overline{b} = \overline{a+b \text{ を } N \text{ で割った余り}}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b \text{ を } N \text{ で割った余り}}$$

である. 例えば, $N = 10$ の時,

$$\overline{3} + \overline{9} = \overline{12} = \overline{2}, \quad \overline{4} \cdot \overline{5} = \overline{20} = \overline{0}$$

である.

命題 2.4. 上の和と積に関して $\mathbb{Z}/N\mathbb{Z}$ は可換環である.

可換環の定義はすぐ後で述べる. 命題は各自証明せよ.

2.2 環と体

定義 2.5. 集合 K に和と積が定義されていて, 次の条件 (i) - (vii) を満たすとき, これを**環** (かん, ring) という. さらに条件 (viii) - (ix) を満たすとき, これを**体** (たい, field) という.

(i) 任意の $a, b, c \in K$ に対して $(a+b)+c = a+(b+c)$ (和の結合法則).

(ii) ある元 $0 \in K$ が存在して, 全ての $a \in K$ に対して $0 + a = a + 0 = a$ (零元の存在).

(iii) 各 $a \in K$ に対して, $a' + a = a + a' = 0$ となる $a' \in K$ が存在 (マイナス元の存在).

(iv) 任意の $a, b \in K$ に対して $a + b = b + a$ (和の可換性).

(v) 任意の $a, b, c \in K$ に対して $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (積の結合法則).

(vi) ある元 $1 \in K$ が存在して, 全ての $a \in K$ に対して $1 \cdot a = a \cdot 1 = a$ (単位元の存在).

(vii) 任意の $a, b, c \in K$ に対して $a \cdot (b+c) = a \cdot b + a \cdot c$, $(a+b) \cdot c = a \cdot c + b \cdot c$. (分配法則)

(viii) 各 $a \in K$, $a \neq 0$ に対して, $a' \cdot a = a \cdot a' = 1$ となる $a' \in K$ が存在 (逆元の存在).

(ix) 任意の $a, b \in K$ に対して $a \cdot b = b \cdot a$ (積の可換性).

注 2.6. 通常, 環と言うときは積の可換性 (ix) は仮定せず, これを満たす環を可換環と呼ぶ. 一方, 体と言うときはこれを仮定し, 可換ではない体のことを斜体と呼ぶ. また, 環の定義で単位元の存在 (vi) を仮定しないこともある.

注 2.7. 零元, 単位元は存在すれば一意的である (証明せよ). a のマイナス元, 逆元も存在すれば一意的であり (証明せよ), これをそれぞれ $-a$, a^{-1} と書く.

例 2.8. 環の例:

$\mathbb{Z} =$ (整数全体), $\mathbb{Q} =$ (有理数全体), $\mathbb{R} =$ (実数全体), $\mathbb{C} =$ (複素数全体),

$\mathbb{Z}[T]$, $\mathbb{Q}[T]$ (それぞれ $\mathbb{Z}$-, $\mathbb{Q}$-係数の 1 変数多項式全体),

$\mathbb{Z}/N\mathbb{Z}$, $M_n(\mathbb{R}) =$ ($\mathbb{R}$-係数 $n \times n$ 行列全体), (関数 $f \colon \mathbb{R} \to \mathbb{R}$ 全体).

これらのうち, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は体である. $\mathbb{Z}/N\mathbb{Z}$ が体かどうかは下で述べる. その他の環が体でない理由を考えよ. これらのうち, $M_n(\mathbb{R})$ だけが可換でない.

定義 2.9. 可換環 K の元 a が**零因子**であるとは, ある $b \neq 0$ に対して $a \cdot b = 0$ となることである.

命題 2.10. 体は 0 以外の零因子をもたない.

証明. $a \cdot b = 0$, $b \neq 0$ とすると b^{-1} が存在し, $a = a \cdot 1 = a \cdot (b \cdot b^{-1}) = (a \cdot b) \cdot b^{-1} = 0 \cdot b^{-1} = 0$. □

命題 2.11. $\mathbb{Z}/N\mathbb{Z}$ が体になる必要十分条件は N が素数であることである.

証明. $\mathbb{Z}/N\mathbb{Z}$ が体だと仮定し, $N = mn$ (m, n は自然数) とする. このとき, $\mathbb{Z}/N\mathbb{Z}$ において

$$\overline{m} \cdot \overline{n} = \overline{N} = \overline{0}$$

である. 体に零因子は存在しないから, $\overline{m} = \overline{0}$ または $\overline{n} = \overline{0}$, つまり $m = N$ または $n = N$ である. よって N は素数である.

逆に N を素数とすると, n=1, 2, …, $N-1$ は N と互いに素であり,

$$kn + lN = 1$$

となる整数 k, l が存在する. このとき,

$$\overline{1} = \overline{kn + lN} = \overline{k} \cdot \overline{n} + \overline{l} \cdot \overline{N} = \overline{k} \cdot \overline{n} + \overline{l} \cdot \overline{0} = \overline{k} \cdot \overline{n}.$$

つまり, $\overline{n}$ には逆元 $\overline{k}$ が存在する. よって $\mathbb{Z}/N\mathbb{Z}$ は体である. □

問 2.12. $\mathbb{Z}/7\mathbb{Z}$ の 0 でない各元に対し逆元を求めよ. $\mathbb{Z}/10\mathbb{Z}$ の元で逆元が存在するものを求めよ.

2.3 有限体 $\mathbb{F}_p$

定義 2.13. 有限個の元からなる体のことを**有限体**という.

定義 2.14. 命題 2.11 より, 素数 p に対して $\mathbb{Z}/p\mathbb{Z}$ は有限体であり, これを $\mathbb{F}_p$ と書く. 以下, $\overline{a}$ のことを単に a と書く. つまり, $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ であり, $\mathbb{F}_p$ においては $p = 0$, $p - 1 = -1$ などである.

命題 2.15 (フェルマーの小定理)**.** 任意の $a \in \mathbb{F}_p$, $a \neq 0$ に対して $a^{p-1} = 1$. 任意の $a \in \mathbb{F}_p$ に対して $a^p = a$.

注 2.16. これは言い換えると, 任意の整数 a に対して $a^p \equiv a \pmod{p}$, つまり $p \mid a^p - a$ ということである.

証明. 任意の a, $b \in \mathbb{F}_p$ に対して $(a+b)^p = a^p + b^p$ である. なぜなら, $1 \leqq k \leqq p-1$ に対して 2 項係数 ${}_pC_k$ は p の倍数だからである. 従って, $a = \overline{n}$ である自然数 n に対して

$$a^p = (\underbrace{1 + \cdots + 1}_{n \text{ 回}})^p = \underbrace{1^p + \cdots + 1^p}_{n \text{ 回}} = a.$$

□

定義 2.17. 体 K に対して, 集合 $K - \{0\}$ とその上の積のみを考えたものを K^* と書き, K の**乗法群**と呼ぶ.

定理 2.18. $\mathbb{F}_p$ の乗法群 $\mathbb{F}_p^*$ は位数 $p-1$ の**巡回群**である. つまり, ある $\alpha \in \mathbb{F}_p$ に対して

$$\mathbb{F}_p^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{p-2}\}$$

である.

注 2.19. $\alpha^i \cdot \alpha^j = \alpha^{i+j}$ であり, α^i は i を $p-1$ で割った余りにのみによることに注意. 特に, 任意の i に対して $(\alpha^i)^{p-1} = 1$ であり, この定理は命題 2.15 を含んでいる.

注 2.20. この定理は

$$\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

と書ける. ただし, 右辺は積を忘れて和のみ考えており, 記号 $\simeq$ の意味は, 全単射でありかつ左辺の積が右辺の和に対応しているということである. 定理の α を 1 つ選び α^i と $\overline{i}$ を対応させればよい.

証明. 命題 2.15 より, $\mathbb{F}_p^*$ の元は方程式 x^{p-1} の解である. よって以下の一般的な命題から従う (なぜか考えよ). □

命題 2.21. 体 K における d 次方程式

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0$$

の解の個数は高々 d 個である.

注 2.22. これは一般の環では成り立たない. 例えば, $\mathbb{Z}/8\mathbb{Z}$ における 2 次方程式 $x^2 = \overline{1}$ の解は $x = \overline{1}, \overline{3}, \overline{5}, \overline{7}$ の 4 つである.

証明. 一般の体でも剰余の定理が成り立つ (確かめよ). 相異なる解 $\alpha_1, \alpha_2, \ldots, \alpha_{d+1}$ が存在したとすると

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = (x-\alpha_1)\cdots(x-\alpha_d)$$

であるが, 右辺に $x = a_{d+1}$ を代入しても 0 にならない. なぜなら $\alpha_{d+1} - \alpha_i \neq 0$ $(i = 1, \ldots, d)$ であり, 体 K には零因子がないからである. □

問 2.23. 定理 2.18 のような α を**原始根**と言う. 小さい素数 p に対して $\mathbb{F}_p^*$ の原始根を求めよ.

3 方程式の解の数

ここで方程式というのは代数方程式, つまり $f(x_1, x_2, \ldots, x_n)$ を n 変数の多項式として

$$f(x_1, x_2, \ldots, x_n) = 0$$

のことである. その解全体の集合を考える. 実数 $\mathbb{R}$-係数の方程式を考えると, これは n 次元空間内の (一般には) $n-1$ 次元の「図形」を定める. 例えば, 平面上の曲線, 3 次元空間内の曲面などである.

このような図形を一般化したものを**代数多様体**という. 代数方程式の解のことを, 対応する代数多様体の**点**という. 一般には, 上のような方程式いくつ

かの共通解を考える．それをアフィン代数多様体という．一般の代数多様体はアフィン代数多様体の「貼り合わせ」で定義される．

多項式 $f(x_1, \ldots, x_n)$ が $\mathbb{F}_p$-係数だとして方程式 $f = 0$ の $\mathbb{F}_p$ における解を考える．各 x_i の取りうる値は p 個なので, $(x_1, \cdots, x_n)$ の取りうる値は p^n 個である．いずれにせよ有限個なので, 実際に f に代入することで, 全ての解を求めることができる．

3.1 べき根の場合

定義 3.1. 体 K において 1 の N **乗根** (または N べき根) とは, N 乗すると 1 になる元のこと, つまり $x^N = 1$ の解のことである．命題 2.21 より, K に含まれる 1 の N 乗根は高々 N 個である．**原始** N 乗根とは, N 乗して初めて 1 になる元のことである．

例 3.2. $K = \mathbb{C}$ のとき, 1 の N 乗根は

$$e^{\frac{2\pi i}{N}n} = \cos\frac{2\pi n}{N} + i\sin\frac{2\pi n}{N} \quad (n = 0, 1, \ldots, N-1)$$

である．原始 N 乗根なのは n が N と互いに素な時である．後のために

$$\zeta_N = \cos\frac{2\pi}{N} + i\sin\frac{2\pi}{N}$$

とおく．

例 3.3. 定理 2.18 より, $\mathbb{F}_p^*$ は 1 の $p-1$ 乗根全体である．

それでは, 一般のべき根の方程式

$$x^N = u \quad (u \in \mathbb{F}_p^*) \tag{1}$$

を考えよう．ただし, 簡単のため, 自然数 N は $p-1$ の約数だと仮定する．この時, 1 の N 乗根はすべて $\mathbb{F}_p^*$ に含まれることに注意．$p - 1 = Nd$, α を $\mathbb{F}_p$ の原始根の 1 つとすると, α^d は 1 の原始 N 乗根であり, 1 の N 乗根全体は $\{1, \alpha^d, \alpha^{2d}, \ldots, \alpha^{(N-1)d}\}$ である．

補題 3.4. 上の仮定のもとで, 方程式 (1) の $\mathbb{F}_p$ における解の個数は N か 0 である．

証明. 解 $x = \beta$ が存在したとすると, 1 の N 乗根 γ に対して, $(\beta\gamma)^N = \beta^N\gamma^N = u \cdot 1 = u$ なので $x = \beta\gamma$ も解である．異なる γ に対しては $\beta\gamma$ も異なるので N 個の解を持つ．命題 2.21 より, これが全てである． □

定義 3.5. 乗法群 $\mathbb{F}_p^*$ の**指標**とは, 写像

$$\psi\colon \mathbb{F}_p^* \to \mathbb{C}^*$$

で, 任意の $a, b \in \mathbb{F}_q^*$ に対して $\psi(ab) = \psi(a)\psi(b)$ を満たすものことである．

原始根 α を 1 つ固定すると, $\psi(\alpha^i) = \psi(\alpha)^i$ なので, 指標は α の値のみで決まる. また, $\psi(\alpha)^{p-1} = \psi(\alpha^{p-1}) = \psi(1) = 1$ なので, $\psi(\alpha)$ は ($\mathbb{C}$ における) 1 の $p-1$ 乗根でなければならない.

問 3.6. $\psi(1) = 1$ を証明せよ. ここで, 最初の 1 は $\mathbb{F}_p$ の単位元, 次の 1 は $\mathbb{C}$ の単位元であることに注意.

定義 3.7. 原始根 $\alpha \in \mathbb{F}_p^*$, 1 の原始 N 乗根 $\zeta_N \in \mathbb{C}^*$ に対して, 指標 $\chi\colon \mathbb{F}_p^* \to \mathbb{C}^*$ を $\chi(\alpha^i) = \zeta_N^i$ で定義する.

注 3.8. χ は位数 N の指標, つまり N 乗して初めて自明になる指標である. 位数が N を割る指標の全体は $\{\chi^a \mid 0 \leqq a < N\}$ である.

定理 3.9. 方程式 (1) の $\mathbb{F}_p$ における解の個数は

$$\sum_{0 \leqq a < N} \chi^a(u)$$

である.

証明. 方程式 (1) が解 $x = \beta$ を持てば, $\chi(u) = \chi(\beta^N) = \chi(\beta)^N = 1$ なので, $\sum_{0 \leqq a < N} \chi^a(u) = N$. 解を持たないとすると, $u = \alpha^i$ ($i \in \{0, 1, \ldots, p-2\}$) と書いた時, $i \notin \{0, N, \ldots, (d-1)N\}$. よって $\chi(u) \neq 1$, つまり, $\chi(u)$ は N のある約数 $N' \neq 1$ に対して 1 の原始 N'-乗根である. $\sum_{0 \leqq a < N} \chi^a(u) = 0$ であることは次から従う. □

補題 3.10. $1 + \zeta_N + \zeta_N^2 + \cdots + \zeta_N^{N-1} = 0$.

証明. $x^N - 1 = (x-1)(x-\zeta_N)\cdots(x-\zeta_N^{N-1})$ で x の係数を比べよ. □

3.2 楕円曲線の場合

多少不正確であるが以下のように定義する.

定義 3.11. 楕円曲線とは, 3 次方程式

$$y^2 = x^3 + Ax + B \tag{2}$$

ただし $4A^3 + 27B^2 \neq 0$, で定義される平面内の曲線のことである.

注 3.12. 条件 $4A^3 + 27B^2 \neq 0$ は $x^3 + Ax + B$ が重根を持たないことと同値であり, これは曲線が「滑らか」であることを意味する. 実平面上で $y^2 = x^3 - 3x + 2$, $y^2 = x^3$ のグラフを描いてみよ.

定義 3.13. 方程式 (2) の $\mathbb{F}_p$ における解の個数を N_p と書く.

明らかに $N_p \leqq p^2$ であるが, さらに, 次のような「確率的」な考察ができる. p を奇素数とすると, y が $\mathbb{F}_p^*$ を動く時, y^2 は $\mathbb{F}_p^*$ の半分の値を動き, $(-y)^2 = y^2$ なので, 各値につきそのような y は 2 個ある. 従って, x が動く時 $x^3 + Ax + B$ が偏りのない値をとるとすると, N_p は「だいたい p」であることになる.

実際それは正しい. 次の定理は後で述べるヴェイユ予想の特別な場合である.

定理 3.14 (Hasse)**.**

$$|p - N_p| \leqq 2\sqrt{p}.$$

例 3.15. 以下では次の例を考えよう:

$$y^2 = x^3 + x + 1.$$

これを $\mathbb{F}_p$-係数の方程式と見て, $\mathbb{F}_p$ における解を求めるのである. ただし, 滑らかであるための条件より, $\mathbb{F}_p$ において $31 \neq 0$, つまり $p \neq 31$ である.

$p = 2$ の時, 解は $(x, y) = (0, 1), (1, 1)$ の 2 個.

$p = 3$ の時, 解は $(x, y) = (0, 1), (0, 2), (1, 0)$ の 3 個.

$p = 5$ の時, 解は $(x, y) = (0, 1), (0, 4), (2, 1), (2, 4), (3, 1), (3, 4), (4, 2), (4, 3)$ の 8 個.

$p = 7$ の時,

x	0	1	2	3	4	5	6
$x^3 + x + 1$	1	3	4	3	6	5	6

y	0	1	2	3	4	5	6
y^2	0	1	4	2	2	4	1

より, 解は $(x, y) = (0, 1), (0, 6), (2, 2), (2, 5)$ の 4 個.

問 3.16. 上の例で, $p = 11, 13$ の時に解を求めよ.

小さな p に対して解の個数 N_p を求めると下の表のようになる. ただし, $a_p = p - N_p$ とおいた. 表から, p に比べて $|a_p|$ が小さいことが見てとれる. この範囲で $|a_p|$ が定理の上界 $2\sqrt{p}$ に最も近づくのは $p = 163$ の時で, $2\sqrt{163} - a_{163} = 0.53\cdots$ である.

p	N_p	$\lvert a_p\rvert$	p	N_p	$\lvert a_p\rvert$	p	N_p	$\lvert a_p\rvert$
2	2	0	101	104	3	229	231	2
3	3	0	103	86	17	233	236	3
5	8	3	107	104	3	239	261	22
7	4	3	109	122	13	241	219	22
11	13	2	113	124	11	251	281	30
13	17	4	127	125	2	257	248	9
17	17	0	131	127	4	263	259	4
19	20	1	137	125	12	269	293	24
23	27	4	139	125	14	271	273	2
29	35	6	149	135	14	277	255	22
37	47	10	151	153	2	281	288	7
41	34	7	157	170	13	283	263	20
43	33	10	163	188	25	293	267	26
47	59	12	167	143	24	307	300	7
53	57	4	173	171	2	311	314	3
59	62	3	179	179	0	313	345	32
61	49	12	181	189	8	317	332	15
67	55	12	191	216	25	331	341	10
71	58	13	193	200	7	337	351	14
73	71	2	197	221	24	347	331	16
79	85	6	199	217	18	349	335	14
83	89	6	211	222	11	353	357	4
89	99	10	223	243	20	359	350	9
97	96	1	227	227	0	367	345	22

3.3 フェルマー方程式

ここで, フェルマー方程式

$$x^N + y^N = 1 \tag{3}$$

を考えよう. §3.1 と同様, 簡単のために $N \mid p-1$ を仮定する. また, N が奇数であることも仮定する.

この時, $\mathbb{F}_p$ は 1 の N 乗根を全て含むので, $x=0$, $y=0$ なる解はそれぞれ

N 個ずつある. それ以外の解を数えると, 定理 3.9 より,

$$\begin{aligned}
&\sharp\{(x,y) \mid x,y \in \mathbb{F}_p^*, x^N + y^N = 1\} \\
&\quad = \sum_{u,v \in \mathbb{F}_p^*, u+v=1} \sharp\{x \in \mathbb{F}_p^* \mid x^n = u\}\sharp\{y \in \mathbb{F}_p^* \mid y^n = v\} \\
&\quad = \sum_{u,v \in \mathbb{F}_p^*, u+v=1} \sum_{0 \leqq a < N} \chi^a(u) \sum_{0 \leqq b < N} \chi^b(v) \\
&\quad = \sum_{0 \leqq a,b < N} \sum_{u,v \in \mathbb{F}_p^*, u+v=1} \chi^a(u)\chi^b(v).
\end{aligned}$$

定義 3.17. 整数 $0 \leqq a, b < N$ に対して**ヤコビ和**を以下で定義する:

$$j^{a,b} = -\sum_{u,v \in \mathbb{F}_p^*, u+v=1} \chi^a(u)\chi^b(v).$$

これは $\mathbb{Q}(\zeta_N) \subset \mathbb{C}$ の元であることに注意.

補題 3.18. (i) $a = b = 0$ の時, $j^{a,b} = 2 - p$.

(ii) $a = 0, b \neq 0$ または $a \neq 0, b = 0$ の時, $j^{a,b} = 1$.

(iii) $a \neq 0, b \neq 0, a + b = N$ の時, $j^{a,b} = 1$.

問 3.19. 上の補題を証明せよ.

以上を合わせると次を得る.

定理 3.20. 上の仮定のもとで, (3) の $\mathbb{F}_p$ における解の個数は

$$p + 1 - \sum_{0 < a,b < N, a+b \neq N} j^{a,b} - N$$

である.

問 3.21. $N = 3$, $p = 7$ の場合に (3) の $\mathbb{F}_p$ における解を求めよ. 一方, ヤコビ和をすべて計算し, 上の定理が成り立つことを確かめよ.

4 ヴェイユ予想

今までは方程式を決めて素数 p を動かしてきたが, ここでは素数 p も固定して, $\mathbb{F}_p$ を含む全ての有限体について考える.

4.1 一般の有限体

命題 4.1. K を体とする時, K は有理数体 $\mathbb{Q}$ を含むか, あるただ 1 つの素数 p に対して $\mathbb{F}_p$ を含む.

証明. $\underbrace{1+\cdots+1}_{n\text{ 回}} = 0$ となる最小の p を考える. そのような p がない場合は K は $\mathbb{Z}$ を含み, よって $\mathbb{Q}$ を含む. そのような p がある場合は, p は素数である. なぜなら, $p = mn$, $m, n \neq 1$ ならば

$$0 = \underbrace{1+\cdots+1}_{p\text{ 回}} = (\underbrace{1+\cdots+1}_{m\text{ 回}}) \cdot (\underbrace{1+\cdots+1}_{n\text{ 回}})$$

であり, K には零因子はないので $\underbrace{1+\cdots+1}_{m\text{ 回}} = 0$ または $\underbrace{1+\cdots+1}_{n\text{ 回}} = 0$ である. これは p の最小性に矛盾する. □

定義 4.2. 体 K が $\mathbb{F}_p$ を含む時, K の**標数**が p であるという. $\mathbb{Q}$ を含むときの標数は 0 と定める.

有限体は $\mathbb{Q}$ を含みえないので, その標数はある素数 p である.

問 4.3. 有限体の位数 (元の数) は標数 p のべき (ある自然数 n に対して p^n) であることを示せ.

定義 4.4. $\mathbb{F}_p$ に $\mathbb{F}_p$-係数多項式の根を全てつけ加えて得られる体を $\mathbb{F}_p$ の**代数閉包**と呼び, $\overline{\mathbb{F}_p}$ と書く.

命題 4.5. 自然数 n に対して

$$\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$$

とおくとき, これは p^n 個の元からなる有限体である.

証明. $x, y \in \mathbb{F}_{p^n}$ ならば,

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} = x + y,\ (xy)^{p^n} = x^{p^n} y^{p^n} = xy$$

なので $x+y$, $xy \in \mathbb{F}_{p^n}$. よって $\mathbb{F}_{p^n}$ には和と積が定義される. $0, 1 \in \mathbb{F}_{p^n}$ は明らか.

$$(-x)^{p^n} = (-1)^{p^n} \cdot x^{p^n} = -1 \cdot x = -x$$

よりマイナス元が存在 ($p = 2$ の時は $-1 = 1$ であることに注意). $x \in \mathbb{F}_{p^n}^*$ とすると $x^{p^n-1} = x \cdot x^{p^n-2} = 1$, よって逆元 $x^{-1} = x^{p^n-2} \in \mathbb{F}_{p^n}^*$ が存在. □

次の定理は難しいことではないが, ここでは証明しない.

定理 4.6. 任意の有限体はある $\mathbb{F}_{p^n}$ と同形である.

問 4.7. $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ である必要十分条件は m が n を割り切ることである. これを示せ.

注 4.8. $\mathbb{F}_{p^n}$ の定義と命題 2.21 より, $\mathbb{F}_{p^n}^*$ は 1 の $p^n - 1$ 乗根全体であり, 巡回群である.

例 4.9. $\mathbb{F}_9$ は $\mathbb{F}_3$ に 1 の 8 乗根をつけ加えた体だが, $\mathbb{F}_3$-係数の多項式として

$$T^8 - 1 = (T-1)(T+1)(T^2+1)(T^2-T-1)(T^2-T+1)$$

と因数分解できる. $(T^2-T-1)(T^2-T+1)$ の 4 つの根が 1 の原始 8 乗根である. 例えば, T^2-T-1 の根の 1 つを α としよう. この時,

$$\mathbb{F}_9 = \{x + y\alpha \mid x, y \in \mathbb{F}_3\}$$

であり, 和と積は

$$\begin{aligned}(x+y\alpha) + (x'+y'\alpha) &= (x+x') + (y+y')\alpha \\ (x+y\alpha)(x'+y'\alpha) &= (xx'+yy') + (xy'+x'y+yy')\alpha\end{aligned}$$

となる

問 4.10. $\mathbb{F}_{25}$ や $\mathbb{F}_{27}$ に対して上の例と同様の考察をせよ.

4.2 ゼータ関数

X を $\mathbb{F}_p$ 上の代数多様体とする. ここでは, ある 1 つの方程式

$$f(x_1, x_2, \ldots, x_n) = 0$$

の解の集合のことと思ってよい.

前節では方程式の $\mathbb{F}_p$ における解の個数を計算したが, ここではさらに, 全ての n に対して $\mathbb{F}_{p^n}$ における解を考える. これは代数多様体 X の $\mathbb{F}_{p^n}$ **に値を持つ点**とも言い換えられる. それら全体の集合を $X(\mathbb{F}_{p^n})$ と書く.

定義 4.11. K を体とするとき, K-係数の**形式的べき級数**とは

$$f(T) = a_0 + a_1 T + \cdots + a_n T^n + \cdots \quad (a_i \in K)$$

の形の式のことである. 2 つの形式的べき級数の和, 積が自然に定義され, 形式的べき級数全体は環になる. さらに, 2 つの形式的べき級数 $f(T)$, $g(T)$ の合成

$$(g \circ F)(T) = g(f(T))$$

が定義される.

形式的べき級数 $f(T)$ は数列 $\{a_n\}$ と 1 対 1 に対応している. この $f(T)$ を $\{a_n\}$ の**母関数**という. 積や合成を考えられることによって, 形式的べき級数には単なる数列よりも豊かな構造が入る. また微分も通常のように定義される. $f(T)$ から a_n を思い出すには, n 回微分して $T=0$ を代入すればよい.

例 4.12. $1+T+T^2+\cdots$ は $1-T$ の逆元である.

例 4.13. 指数, 対数を以下のように定義する:

$$\exp(T)=\sum_{n\geqq 0}\frac{T^n}{n!},\quad \log(1-T)=-\sum_{n\geqq 1}\frac{T^n}{n}.$$

この時,

$$\exp(\log(1-T))=1-T,\quad \log(\exp(T))=T.$$

これらを確かめよ.

定義 4.14. $N_n=\sharp X(\mathbb{F}_{p^n})$ とし,

$$Z(X,T)=\exp\left(\sum_{n\geqq 1}\frac{N_n}{n}T^n\right)$$

とおく. これを X の**ゼータ関数** (合同ゼータ関数) という.

これもまた, $\{N_n\}$ の母関数の一種である. 定義から, $Z(X,T)$ は $\mathbb{Q}$-係数の形式的べき級数である.

例 4.15. 1 点を考えると, $N_n=1$ なので, 例 4.13 より

$$Z(X,T)=\frac{1}{1-T}$$

である. 直線の方程式 $y=ax+b$ $(a,b\in\mathbb{F}_p)$ や, 放物線の方程式 $y=ax^2+bx+c$ $(a\neq 0,b,c\in\mathbb{F}_p)$ を考えると, $N_n=p^n$ である. よって, 同様に

$$Z(X,T)=\frac{1}{1-pT}$$

である. これらは有理式 (多項式の商) である.

ある実数が有理数であるための必要十分条件は, それを少数展開した時に, ある所から先は循環するということであった. 同様に, ある形式的べき級数が有理式になるためには, その係数列が強い規則性を持つことが必要である.

4.3 ヴェイユ予想

ここで, X は $\mathbb{F}_p$ 上の d 次元の代数多様体であり, **射影的**かつ**滑らか**という条件をみたすものとする. これらの正確な定義を述べる時間はないが, 楕円曲線の射影化を説明しよう.

方程式 (2) において $x = X/Z$, $y = Y/Z$ を代入すると

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

が得られる. 点 (x, y) のかわりに比 $(X : Y : Z)$ を考える. ただし $X = Y = Z = 0$ は考えない. $Z \neq 0$ ならば $(X : Y : Z) = (x : y : 1)$ なので新しい点はない. $Z = 0$ を代入すると $X = 0$ なので, 新しい点 $(0 : 1 : 0)$ が加わる. これを**無限遠点**と呼ぶ. 同様に, §3.3 の仮定のもとでは, フェルマー曲線の射影化

$$X^N + Y^N = Z^N$$

には無限遠点が N 個あることが分かる.

定理 4.16 (ヴェイユ予想, Dwork, Grothendieck, Deligne の定理)**.**

(i) $\mathbb{Z}$-係数の多項式 $P_i(T)$ を用いて

$$Z(X, T) = \frac{P_1(T) \cdots P_{2d-1}(T)}{P_0(T)P_2(T) \cdots P_{2d}(T)}$$

と書ける. ただし $P_i(T)$ は次の条件で特徴づけられる.

(ii) $P_i(T)$ の根の逆数は絶対値が $\sqrt{p}^i$.

まず (i) は, べき級数として定義されたゼータ関数が有理式であることを言っている. それは, 例 4.15 でも見たように, 数列 $\{N_n\}$ には大きな規則性があることを意味している.

次に, (ii) はリーマン予想の類似と呼ばれる. その理由を曲線 $(d = 1)$ の場合に説明しよう. 曲線の場合は $P_0(T) = 1 - T$, $P_2(T) = 1 - pT$ であり, $P_1(T)$ が問題になる. ここで s を複素数として

$$\zeta(X, s) = Z(X, p^{-s})$$

とおくとき (ii) は, $\zeta(X, s) = 0$ ならば s の実数部分は $1/2$ であることを意味している. 未だ未解決のリーマン予想とは, (全複素平面に解析接続された) リーマン・ゼータ関数

$$\zeta(s) = \sum_{n \geqq 1} \frac{1}{n^s}$$

の零点の実数部分が $1/2$ である, というものだったことを思い出そう.

注 4.17. 曲線には**種数**という非負整数 g が対応するが, $P_1(T)$ の次数は $2g$ である. 例 4.15 の場合は $g = 0$, 楕円曲線は $g = 1$ の曲線である.

上の (i), (ii) のほかに, 関数等式とベッチ数の一致というのもあるのだが, ここでは割愛する.

4.4 楕円曲線の場合

X を式 (1) で定義される $\mathbb{F}_p$ 上の楕円曲線を射影化したものとする.

$$a_n = p^n + 1 - N_n$$

とおく. 無限遠点が 1 点加わっているので, ここでの N_n は (1) の解の数 $+1$ であることに注意. また, p は固定しているので記号から省略している. 前節で a_p と書いていたものがここでは a_1 であることに注意.

この場合のヴェイユ予想は次のように書ける.

定理 4.18 (ヴェイユ予想, 楕円曲線の場合)**.**

(i)
$$Z(X,T) = \frac{1 - a_1 T + pT^2}{(1-T)(1-pT)}.$$

(ii) $1 - a_1 T + pT^2 = (1-\alpha T)(1-\beta T)$ $(\alpha, \beta \in \mathbb{C})$ と分解した時, $|\alpha| = |\beta| = \sqrt{p}$ である.

まず (i) だが, これは

$$-\exp\left(\sum_{n \geqq 1} \frac{a_n}{n} T^n\right) = 1 - a_1 T + pT^2$$

と同値である. 驚くべきなのは, 左辺はすべての a_n の情報を持っているのに対し右辺には a_1 のみしか現れない, つまり a_1 から全ての a_n が求まるということである. 実際,

$$-\log(1-\alpha T)(1-\beta T) = \sum_{n \geqq 1} \frac{\alpha^n + \beta^n}{n} T^n,$$

よって

$$a_n = \alpha^n + \beta^n$$

である. 対称式は基本対称式で書けるが, $\alpha + \beta = a_1$, $\alpha\beta = p$ なので, 全ての a_n, よって N_n が a_1 から求まるのである.

問 4.19. 例 3.15 において $p = 3$ の場合に N_2, N_3 などを求めてみよ. 例 4.9 を用いて $X(\mathbb{F}_9)$ を求め, N_2 が上の値になることを確かめよ.

次に定理の (ii) だが, これは

$$|a_1| \leqq 2\sqrt{p}$$

と同値である (証明せよ). 従って, 定理 3.14 はヴェイユ予想の特別な場合であった. しかしながら, 定量的な前者の不等式に比べ, 後者の定式化の方が定性的で問題の本質が現れている. 定理 4.16 (ii) で $\sqrt{p}$ の肩に現れる i は**重さ** (weight) と呼ばれ, とても重要な概念である.

注 4.20. 有名なラマヌジャン予想は

$$q\prod_{n\geqq 1}(1-q^n)^{24}=\sum_{n\geqq 1}a_nq^n$$

によって定まる整数列 $\{a_n\}$ は任意の素数 p に対して $|a_p|\leqq 2\sqrt{p}^{11}$ を満たす (重さが 11 である), というものである. これはドリーニュによりヴェイユ予想に帰着されて証明された.

4.5 フェルマー曲線の場合

再びフェルマー方程式 (3) を考える. これが定める代数多様体がフェルマー曲線である. それを射影化したものをここでは X と書く.

$\mathbb{F}_{p^n}^*$ の元 x に対して $x^{\frac{p^n-1}{p-1}}$ は $\mathbb{F}_p^*$ の元である. よって, χ との合成

$$\chi_n\colon \mathbb{F}_{p^n}^*\to\mathbb{F}_p^*\to\mathbb{C}^*$$

を考えると, これは $\mathbb{F}_{p^n}^*$ の指標である. ヤコビ和を同様にと定義する:

$$j_n^{a,b}=-\sum_{u,v\in\mathbb{F}_{p^n}^*}\chi_n^a(u)\chi_n^b(v).$$

定理 3.20 において p を p^n で置き換えたものが成り立ち, フェルマー曲線は N 個の無限遠点を持つので,

$$N_n=p^n+1-\sum_{0<a,b<N,a+b\neq N}j_n^{a,b}$$

となる. さらに次が成り立つ.

定理 4.21 (Davenport-Hasse)**.**

$$j_n^{a,b}=(j^{a,b})^n.$$

よって次が従う.

系 4.22.

$$Z(X,T)=\frac{\prod_{0<a,b<N,a+b\neq N}(1-j^{a,b}T)}{(1-T)(1-pT)}.$$

問 4.23. ヴェイユ予想 (i)

$$\prod_{0<a,b<N,a+b\neq N}(1-j^{a,b}T)\in\mathbb{Z}[T]$$

を示せ. ガロワ群 $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})\simeq(\mathbb{Z}/N\mathbb{Z})^*$ の作用を考えればよい.

系より, この場合のヴェイユ予想 (ii) は次と同値である.

定理 4.24. 任意の $0 < a, b < N$, $a + b \neq N$ に対して

$$|j^{a,b}| = \sqrt{p}.$$

証明. ガウス和を用いて証明されることが多いが, 直接的な証明を与える.

$$|j^{a,b}|^2 = \sum_{u\neq 0,1} \chi^a(u)\chi^b(1-u) \sum_{v\neq 0,1} \chi^{-a}(v)\chi^{-b}(1-v) = \sum_{u,v\neq 0,1} \chi^a(\tfrac{u}{v})\chi^b(\tfrac{1-u}{1-v}).$$

ここで $w = u/v$ とおくと,

$$|j^{a,b}|^2 = \sum_{v\neq 0,1, w\neq 0,1/v} \chi^a(w)\chi^b(\tfrac{1-vw}{1-v}) = \sum_{w\neq 0} \chi^a(w) \sum_{v\neq 0,1,1/w} \chi^b(\tfrac{1-vw}{1-v}).$$

$w = 1$ の時, $\sum_{v\neq 0,1,1/w} \chi^b(\frac{1-vw}{1-v}) = \sum_{v\neq 0,1} \chi^b(1) = p - 2$. $w \neq 0, 1$ の時, $x = \frac{1-vw}{1-v}$ とおくと

$$\sum_{v\neq 0,1,1/w} \chi^b(\tfrac{1-vw}{1-v}) = \sum_{x\neq 0,1,w} \chi^b(x) = -1 - \chi^b(w).$$

ここで, 仮定 $b \neq 0$ と補題 3.10 を用いた. 以上より,

$$|j^{a,b}|^2 = p - 2 - \sum_{w\neq 0,1} \chi^a(w) - \sum_{w\neq 0,1} \chi^{a+b}(w).$$

仮定 $a \neq 0$, $a + b \neq N$ と補題 3.10 より

$$\sum_{w\neq 0,1} \chi^a(w) = \sum_{w\neq 0,1} \chi^{a+b}(w) = -1.$$

よって証明された. □

注 4.25. 上の積に現れる (a, b) は $2g = (N - 1)(N - 2)$ 個ある. 楕円曲線の場合は N_1 から全ての N_n が分かったが, 今の場合は $N_1, \ldots, N_g$ から全ての N_n が分かる.

4.6 証明について

グロタンディークとドリーニュによるヴェイユ予想の証明において最も重要なのは, 多項式 $P_i(T)$ を線形写像の固有多項式ととらえることである.

その線形空間とは i-次の ℓ-進エタール・コホモロジー群とよばれる $\mathbb{Q}_\ell$-線形空間である (素数 ℓ に対して $\mathbb{Q}_\ell$ は $\mathbb{Q}$ の ℓ-進完備化という標数 0 の体である). この ℓ-進コホモロジーの特徴のひとつは, 有限体上の多様体という標数 p の対象に, 標数 0 の線形空間を対応させることである. またこのコホモロジーは位相多様体に対する特異コホモロジーの類似であり, さまざまな良い性質を満たす.

その線形空間に作用する線形写像はフロベニウス自己同形

$$F\colon \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}\ ; \quad F(x) = x^p$$

から誘導される写像である. ℓ-進コホモロジーのもうひとつの特徴は, ガロワ群 $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ が作用することだが, フロベニウス F はその「生成元」である. 有限体 $\mathbb{F}_{p^n}$ は F^n で固定される $\overline{\mathbb{F}_p}$ の部分体であった. 従って, $X(\mathbb{F}_{p^n})$ は F^n による固定点である. 古典的なレフシェッツ固定点定理にはその ℓ-進類似があり, 定理 4.16 (i) はその帰結である.

ドリーニュによるリーマン予想の類似 (定理 4.16 (ii)) の証明は, いくつかの代数幾何的な技術を組み合わせてなされる. そこで重要なのは, 個々の多様体を考えるだけでなく, 多様体の族や多様体の積たちを同時に考え, それらのコホモロジー群とそこへのフロベニウス作用の重さの関係を調べることである.

参考文献

[1] Deligne, P.: La conjecture de Weil I. Publ. Math. IHES **43** (1974), 273-307. (ヴェイユ予想の証明が完結した論文)

[2] Hartshorne, R.: Algebraic geometry. Springer GTM **52**, 1977. (代数幾何学の標準的な教科書, 和訳あり)

[3] Milne, J. S.: Étale cohomology. Princeton Univ. Press, 1980. (エタール・コホモロジーの教科書)

[4] Silverman, J. H.: The arithmetic of elliptic curves (2nd edition). Springer GTM **106**, 2009. (楕円曲線の標準的な教科書, 和訳あり)

[5] Weil, A.: Number of solutions of equations in finite fields. Bull. Amer. Math. Soc. **55** (1949), 497-508. (ヴェイユ予想が提出された論文)