４３「フェルマーの最終定理」

とうとうフェルマーの最終定理について書く時が来た。
多分これまでに書いた中でも最も困難な挑戦になるだろう。これまで難しかったのは、

２１「陽電子の予言」ディラック方程式

２６ ガロア補足

３７ 小林・益川理論　であった。

このテーマはさらに難しい。何故難しいのか？

数学は極めて抽象的な世界，無限の世界を扱う。

特に、現代数学は難しい記号ばかりである。
途中から、わけのわからない抽象的な記号の世界に入り込んで“ はい、証明終わり”となる。

それに「なぜ」が説明しにくい。

例えば、なぜそのような難問を解くのか？という問いに対して、納得させられそうな答えはなかなか見つからない。目的も説明しにくい。

しいて言えば「難しいからこそ挑戦したいのだ」というような答えになってしまう。

科学者なら、自分の研究が人を幸せにするということもあるだろう。しかし、数学者の研究が人の幸せに直接繋がるということは少ない。テクノロジーの底辺を支えているとは言えるだろうが。

むしろ数学はそういうことには関係ない、本質的な“真”とか“美”といったことに通じているような気がする。数学はもっと崇高で、芸術に近く、論理の芸術とでもいうべきものかも知れない。

フェルマーの最終定理とは、自然数 n≧3 に対して

$X^n+Y^n=Z^n$

を満たす自然数Ｘ，Ｙ，Ｚは存在しない、というものである。

ここでは、まだこの定理が正しいかどうかわからなかった時の言い方で、“フェルマー予想”と呼ぶ。

古代ギリシャ数学の源流「ディオファントス」の“算術”のラテン語訳本の欄外にフェルマーが書き込んだものだ。フェルマーは「この方程式の驚くべき証明を見つけたが、それを記すには余白が小さすぎる」と書き残した。それが１，６３７年のことである。

一般に数学の難問は、その問題の意味すら理解できないものが多い。

例えば、「単連結な 3 次元閉多様体は 3 次元球面 S^3 に同相である」というように。

これは最近解決されたポアンカレ予想という難問である。一体どんな意味なのだろうか？（注 1)。

しかし、このフェルマーの問題は、シンプルで小学生でも理解できる。そして、何となく解けそうな、n＝３，４あたりで１組ぐらい式を満たすＸ，Ｙ，Ｚがありそうな気もする。

例えば、

$3^3+4^3+5^3=6^3$ というような美しい式や、

$27^5+84^5+110^5+133^5=144^5$、

$2682440^4+15365639^4+18796760^4=20615673^4$ というものもある。

さらに$W^n+X^n+Y^n=Z^n$ という式では、１つＷという変数が増えるだけで n＝4 のとき無数に解があることがわかっている。

しかし、$X^n+Y^n=Z^n$だけはこれを満たす自然数X，Y，Zが存在しないことが、つい最近まで証明されず、３５０年以上経った１，９９４年、イギリスの数学者「アンドリュー・ワイルズ」によって、やっと証明されたのである。

フェルマーは本当に“証明を見つけた”のか？

現在では、フェルマーは証明したと勘違いしていたのだろうというのが共通認識のようだ。

というのは、

- フェルマーの残された書簡に、この最終定理に言及したものが見当たらないこと。もし、この定理が正しいと確信していたなら、必ず手紙に書いただろう。
- フェルマーの時代は記号法が未発達だった。例えば、文字指数X^nなどの表記法がない。従って、特定の指数について考えざるを得ないので、全ての指数 n についての証明は困難だろう。
- 後に続く大数学者、オイラーやガウスなどが証明に成功していない。記号法も整備され、新しい手法も導入されていたにもかかわらず、フェルマーに充分比肩し得る数学者達が証明できなかったのは不思議である。

さて、本論に入ろう。

証明の最後までたどり着くには相当長い説明となるが、途中で投げ出さないで是非終わりまで読んでほしい。

まず、オイラーは n＝3，n＝4 の場合を証明（n＝3：1,770 年，n＝4：1,738 年)。その前にフェルマー自身 n＝4 を証明していたようだ。

n = 3，4 が証明されたということは、その倍数 n = 6 , 9 , 12 , 15 、、、、n = 8 , 12 , 16 , 20 、、、、についても証明されたことになる。つまり、n は全ての素数についてだけ証明すれば良いのである。

・n = 5：ディリクレとルジャンドル（1,825 年）

・素数 p で 2p+1 も素数の場合（例えば、11,23,29,41,43･･･など）：ソフィ・ジェルマン（1,823 年）

・n = 14：ディリクレ（1,832 年）

・n=7：ラメ（1,839 年）

個々の指数を１つずつ証明していたのでは埒が明かない。この中で、ソフィ・ジェルマン（仏）は一般的な証明を目指したものとして評価に値する。

既に 200 年が経過し、初等的なアプローチでは行き詰まり新しいアイデアに基づく手法が必要である。

クンマー（独）は、素因数分解の一意性から発展させた、理想数（イデアル）の概念を導入することによって、その解決に接近した。素因数分解の一意性とは、整数の世界で最も重要な原理で、素因数分解がただ１通にしかできないということである。

例えば「6」は、6＝2×3 というように１通りにしか分解できない。2，3，5，7････など、素数は１と自分以外には割れない数の世界における原子である。

しかし、数の範囲を複素数まで広げると、$6=2\times3=\left(1+\sqrt{5}\right)\left(1-\sqrt{5}\right)$のように２通り、あるいはそれ以上の分解ができるようになる。原子核が陽子と中性子に分裂するのに似ている。

図１に数の体系図を示す。

数の概念を複素数よりさらに発展させたのがイデアルである。

クンマーのアイデアは、$X^n+Y^n=(X+Y)\ (X+\zeta Y)\ (X+\zeta^2 Y)\cdots\cdot(X+\zeta^{n-1} Y)$ というように因数分

解することである。このζは、n 乗すると 1 になる数（1 の n 乗根でζ＝cos[2π/n]＋i sin[2π/n]という複素数になる。

例えばn＝3 の場合、1 の 3 乗根であり　$\omega_1 = 1,\ \omega_2 = \dfrac{-1+i\sqrt{3}}{2},\ \omega_3 = \dfrac{-1-i\sqrt{3}}{2}$　となる。

n＝3,4,5,･･･と 1 つずつ証明するのではなく、すべての数について証明する方法が必要である。

実際はすべての数の必要はなく、すべて数は素数の組み合わせで作られるので、素数についてだけ証明できればよい。そのためにはどうすれば良いのか？

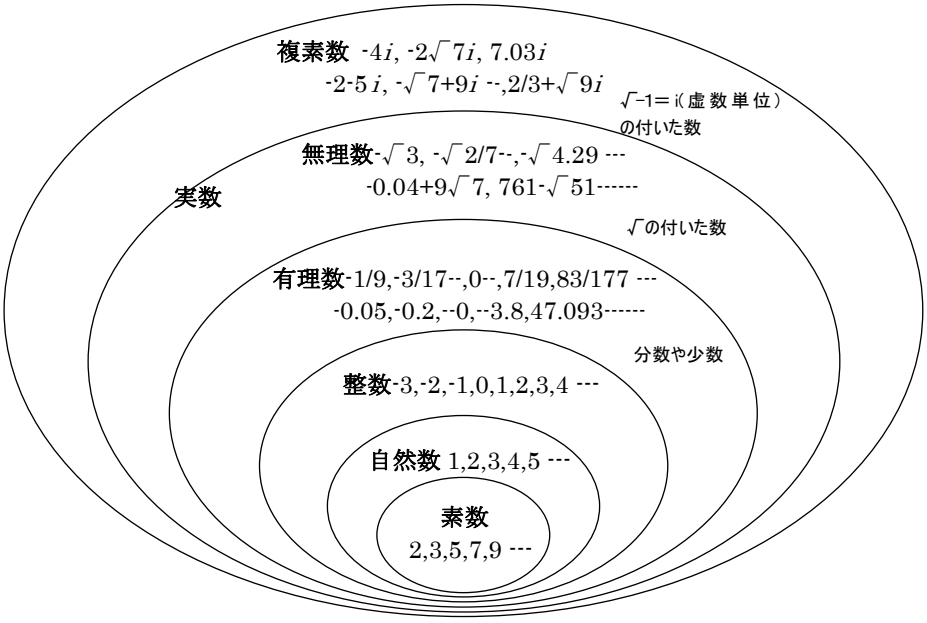


図 1　数の体系図

それには、楕円曲線の有理点が有限個しかないという楕円曲線の性質を利用するのである。

$X^n+Y^n=Z^n$ の両辺をZ^nで割ると、

$$\left(\frac{X}{Z}\right)^n+\left(\frac{Y}{Z}\right)^n = 1$$

$\dfrac{X}{Z}$ を 新たにX，　$\dfrac{Y}{Z}$ を 新たにYとおくと、

$X^n+Y^n=1$ とすることができる。これをフェルマーの方程式と呼んでいる。

X，Y，Zは自然数だから、

$\dfrac{X}{Z}$，$\dfrac{Y}{Z}$ は有理数（分数や少数）でなければならない。

従って、$X^n+Y^n=Z^n$を満たす自然数X，Y，Zを求めるという問題は、$X^n+Y^n=1$を満たす有理数X，Yを求めるという問題と同じである。

$X^n+Y^n=1$の描く曲線を曲線C_nと表すと、n＝2 のときは 2 次曲線（円，放物線，双曲線）となり、C_2を満足する有理数X，Yの組は無限に存在する。

n＝3 のときC_3は楕円曲線という曲線になる。まぎらわしいが、“楕円曲線”は“楕円”とは異なる。この楕円曲線の性質に対する研究が、フェルマー予想を解決に向けて大きく前進させるのである。

楕円曲線は一般的に、$y^2+a_1y+a_3=x^3+a_2x^2+a_4x+a_6$ と表される。

$y=ax^3+bx^2+cx+d$ という 3 次曲線なら、高校で習ったという人もいると思うが、楕円曲線はこの y のところが y^2 に変わるだけなのに、多くの神秘的な性質が現れる。

つまり、(y の 2 次式) = (x の 3 次式) という式で表されるのだが、工夫して変数変換を行うことにより、この式は必ず、楕円曲線 $y^2=x^3+ax+b$ ----------①
という形に変形することができる。

曲線が楕円曲線であるとは、$y^2=x^3+ax+b$ と表され、少なくとも 1 つの有理点を持ち、その点は非特異点であることが必要である。非特異点とは、グラフに描くと尖ったり交差したりすることのない点である。

『楕円曲線において、有理数の点は有限個である』

これはモーデル・ファルティングスの定理といい、モーデルが予想を提起し、1，９８３年にファルティングスが証明した。(厳密にいうと、$X^n+Y^n=1$ などの式で表される曲線の複雑さは n によって変わり、それを表す“種数”という指数により決まる。その種数が 3 以上の場合について有理点が有限個であるという定理で、楕円曲線は種数 3 である) この定理から、フェルマーの方程式に解があるとすれば、その解は有限個である。無限にあるわけではなく有限ということが重要なのである。

ここで、フェルマー予想の解決に大きな役割を果たした日本人が登場する。

谷山豊と志村五郎である。1，９５５年９月、日光で開催された代数論的整数論の国際シンポジウムで、谷山豊は 1 つのアイデアを提示した。

『すべての楕円曲線はモジュラーである』

という、当時誰も思いつかなかった突拍子もない予想である。数学の言葉で正確に言えば「有理数体の楕円曲線のゼータ関数は、上半平面上の重み 2 のある保型形式のゼータ関数である」ということになるが、これを理解することがフェルマー予想を理解することになるので、これからゆっくり解りやすく書いていく。

まず“有理数体”とは、数の体系を示した図 1 において、有理数までを含む数（分数，少数など）の集まった「体」である。体とは、「26 ガロア補足」にあるように「数の集合で、その範囲で自由に四則演算ができる集合」のことである。

“ゼータ関数”とは、簡単にいえば素数のいろいろな性質を調べるのに便利な関数だと思っておけばよい。“上半平面”とは、$z=x+iy$（i は虚数単位）で表される複素平面（x 軸を実数軸，y 軸を虚数軸とした平面）で $y>0$ となる部分、つまり x 軸より上の部分である。

“重み２”とは、詳細は後でわかることになるが、例えば方程式は１次，２次、３次、、、と複雑になっていくが、とりあえずその複雑さが２次方程式程度のようなものと考えておけばよいだろう。

“保型形式”とは、一定の変数変換で不変な性質を持つ、複素数を変数とする関数のことで、楕円曲線の中で保型形式によって表されるものをモジュラー楕円曲線といい、全ての楕円曲線はモジュラー楕円曲線であるというのが谷山・志村予想である。このことは後でもっと詳しく書く。

「有理数体の楕円曲線のゼータ関数は、上半平面上の重み 2 のある保型形式のゼータ関数である」が突拍子もないとはどういうことなのか？

そもそも「楕円曲線のゼータ関数」とは、飛び飛びの数（離散数）を扱う整数論の世界から導かれるゼータ関数なのであるが、それが無限級数，微積分や連続した数（連続数）を扱う解析学の世界から導

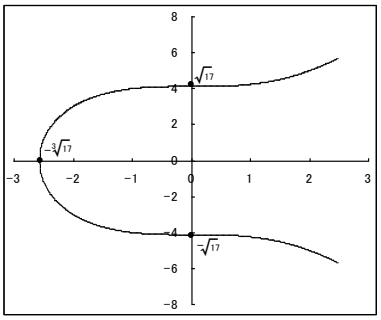
かれる「保型形式のゼータ関数」に一致することを予想したものだからである。

この谷山・志村予想は２，００１年には完全に証明されたが、最初は全く異なる分野が地下水脈で繋がっていたというような驚くべきものだったのである。

まず、楕円曲線（Elliptic Curve）について理解を深めていこう。（楕円曲線を「E：」と表す）

$E_1 : y^2=x^3+x$ ----------②

という楕円曲線（ ①式において a＝1，b＝0 の場合）について考えてみる。いきなりこの方程式の有理数解をすべて求めるのは難しい。



$y^2=x^3+x$ のグラフ

そのため、この方程式を合同式 $y^2\equiv x^3+x$ として扱い、まずこれを解くことからヒントを探してみる。

整数論において、割れるかどうか（整除性）は非常に重要なことで、それを扱う合同式は整数論にとって強力な道具である。

合同式は割ったときの余りに着目した計算で、a≡b（mod m）というように表し、a が m（modulus）を法として b と合同であるという。これは a－b が m で割れることをいう。

例えば、47≡35（mod 6）と書くと 47－35 が 6 で割れるので、47 と 35 は 6 を法として合同であるということである。

$y^2\equiv x^3+x \pmod p$として、素数 p（素数[prime number]は p という文字を使って表す）を法としていろいろな素数について解いてみる。整数係数の式を素数 p を法として考えることを、p を法として還元するという。

p＝2 のとき、

x，y を 0≦x,y≦1 の範囲で探すという問題なので、

x＝0 のとき y＝0、0≡0（mod 2） ---------- (0－0)/2＝0

x＝1 のとき、y＝0、$0\equiv 1^3+1=2$（mod 2） ---------- (0－2)/2＝－1

従って解は２つで、(0，0)（1，0）である。

p＝3 のとき、

x，y を 0≦x,y≦2 の範囲で探す。

x＝0 のとき y＝0、0≡0（mod 3） ---------- (0－0)/3＝0

x＝1 のとき解なし

x＝2 のとき y＝1、$1\equiv 2^3+2=10$（mod 3） ----------(1－10)/3=－3

y＝2、$4\equiv 2^3+2=10$（mod 3） ----------(4－10)/3=－2

従って、解は３つで（0，0）（2，1）（2，2）である。

このようにして、p＝5，7，11，13、、、、、と素数について地道に $y^2\equiv x^3+x \pmod p$を解き、その解の個数（N_p）を整理すると表１のようになる。

p	2	3	5	7	11	13	17	19	23	29
N_p	2	3	3	7	11	19	15	19	23	19
p	31	37	41	43	47	53	59	61	67	71
N_p	31	35	31	43	47	67	59	51	67	71

表１（楕円曲線 $E_1 : y^2=x^3+x$ に対する p を法とした解の個数 N_p ）

表１を見て何か気付かないだろうか？多くの素数について、N_p が p に等しくなっている。
p＝2，3，7，11，19，23，31，43，47，59，67，71 でN_p＝p であり、これらは 2 を除けばすべて 4 で割れば 3 余る数になっている。

よって p≡3（mod 4）のとき、楕円曲線$E_1: y^2=x^3+x$ は p を法として、ちょうどN_p＝p 個の点を持つということが言えそうである。

他の素数、つまり 4 で割れば 1 余る素数 p≡1（mod 4）はどうだろうか？

この場合のN_pは、p＝5 や 17 のようにN_p＜p，p＝13 や 53 のようにN_p＞p となっており、ランダムなように見える。それでも p が大きくなればN_pも大きくなり、N_pは p の周りをさまよっているように見える。そう考えると、p とN_pの差を調べることで何かわかるのではないか？

この差を $p-N_p=a_p$ として、p をもっと増やし $p\neq N_p$ となるものだけを表２に示す。

p	5	13	17	29	37	41	53	61	73	89
N_p	3	19	15	19	35	31	67	51	79	79
a_p	2	-6	2	10	2	10	-14	10	-6	10
$a_p/2$	1	-3	1	5	1	5	-7	5	-3	5
p	97	101	109	113	137	149	157	173	181	193
N_p	79	99	115	127	159	163	179	147	163	207
a_p	18	2	-6	-14	-22	-14	-22	26	18	-14
$a_p/2$	9	1	-3	-7	-11	-7	-11	13	9	-7

表２（楕円曲線$E_1: y^2=x^3+x$ に対する p を法とした解の個数 N_p と p 欠乏 a_p）

この a_p を楕円曲線$E_1: y^2=x^3+x$ に対する p 欠乏という。a_p はフロベニウス写像のトレース（用語説明省略）と呼んでいる。

表２には $a_p/2$ も加えてあるが、驚くことに $a_p/2\equiv1$（mod 4）となっているのである。
p≡1（mod 4）の素数は 2 つの平方数の和 $p=A^2+B^2$ とただ一通りに表すことができる。

つまり、A を正の奇数として $p=A^2+B^2$ に分解するとき、A≡1（mod 4）ならば $a_p=2A$ であり、A≡3（mod 4）ならば $a_p=-2A$ となる。

以上をまとめると、

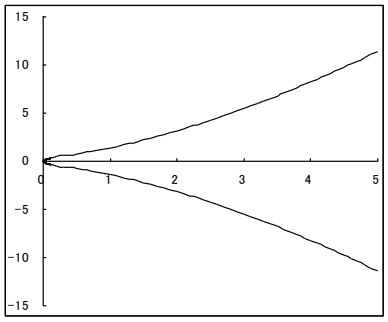
p≡3（mod 4）　4 で割って 3 余る素数のとき　N_p＝p である

p≡1（mod 4）　4 で割って 1 余る素数のとき、
A を奇数として必ず $p=A^2+B^2$（例えば $41=5^2+4^2$ のように）と 2 つの平方数の和として表せる。このとき $N_p=p\pm2A$ であり、A≡1（mod 4）のとき正、A≡3（mod 4）のとき負である

次に楕円曲線、$E_2: y^2=x^3+17$ ----------③
でおなじことを行ったときの p，N_p，a_p を表３に整理して示す。

E_1では p≡3（mod 4），p≡1（mod 4）が意味を持っていたが、E_2では p≡2（mod 3）のとき N_p＝p となり、p≡1（mod 3）のとき $p=A^2+B^2$ と 2 つの平方数の和として表すことができる。

以上から、楕円曲線E_1，E_2とも p 欠乏は半分の素数に対し $a_p=0$，$p-(a_p/2)^2$ が平方数になるということが言えそうである。



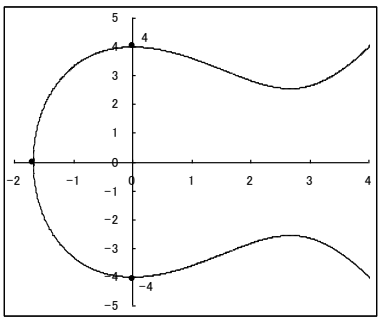
$y^2=x^3+17$ のグラフ

p	2	3	5	7	11	13	17	19	23	29
N_p	2	3	5	12	11	20	17	26	23	29
a_p	0	0	0	-5	0	-7	0	-7	0	0
p	31	37	41	43	47	53	59	61	67	71
N_p	42	48	41	56	47	53	59	48	62	71
a_p	-11	-11	0	-13	0	0	0	13	5	0
p	73	79	83	89	97	101	103	107	109	113
N_p	63	75	83	89	102	101	110	107	111	113
a_p	10	4	0	0	-5	0	-7	0	-2	0

表３（楕円曲線E_2：$y^2=x^3+17$ に対する
p を法とした解の個数 N_p と p 欠乏 a_p）

さらに楕円曲線、E_3：$y^2=x^3-4x^2+16$ ----------④
について同じようにやってみる。（E_3 は $x-4/3=X$ とおくと、$y^2=X^3-16/3X+(16-128/27)$とすることができるので、$y^2=x^3+ax+b$ の形になる）

表４に p，N_p，a_p をまとめる。



$y^2=x^3-4x^2+16$ のグラフ

p	2	3	5	7	11	13	17	19	23	29
N_p	2	4	4	9	10	9	19	19	24	29
a_p	0	-1	1	-2	1	4	-2	0	-1	0
p	31	37	41	43	47	53	59	61	67	71
N_p	24	34	49	49	39	59	54	49	74	74
a_p	7	3	-8	-6	8	-6	5	12	-7	-3
p	73	79	83	89	97	101	103	107	109	113
N_p	69	89	89	74	104	99	119	89	99	104
a_p	4	-10	-6	15	-7	2	-16	18	10	9

表４（楕円曲線E_3：$y^2=x^3-4x^2+16$ に対する
p を法とした解の個数 N_p と p 欠乏 a_p）

表４を見てわかることは、今までのパターンと違い $a_p=0$ となるケースが 2，19，29 と非常に少ないことである。p を 5,000 まで広げても $a_p=0$ となるのは 12 個しかないのである。

それらの数は $p\equiv 9 \pmod{10}$ となっているが、59，79，89，109 などの数は含まれていない。

また、$p=A^2+B^2$ となるパターンも現れない。さらに他のいろいろな楕円曲線について試してみても E_3 と同じようなものが多い。E_1，E_2 と E_3 は何が違うのだろうか？

実は E_1，E_2 は、特別なタイプの楕円曲線なのである。これらは虚数乗法もつ楕円曲線といい、$y^2=x^3+ax$（①式において $b=0$）や $y^2=x^3+b$（①式において $a=0$）といった比較的単純な楕円曲線がこの性質を持つが、楕円曲線全体の中ではごく少数派である。

そして虚数乗法を持つ楕円曲線だけ a_p の半分が 0 に等しく、虚数乗法もたない楕円曲線は、ごくわずかしか a_p が 0 にならないのである。

楕円曲線が虚数乗法をもつとは、その方程式がある特別な種類の変換を行っても変わらない性質を備えることをいう。例えば、（x，y）が方程式 E_1：$y^2=x^3+x$ の解であるとき、（$-x$，iy）もその解とな

る。従って、$(iy)^2=(-x)^3+(-x)$ はE_1の符号を変えれば一致する。

このように、方程式に対する $i=\sqrt{-1}$のような虚数の存在が「虚数乗法」という名の由来である。

さあ、ここまでくれば、楕円曲線のゼータ関数が導入できる。

ゼータ関数とは、素数が協力して作り出すもので、素数の秘密を解き明かすものと言われている。

素数 p に対して $a_p=p-N_p$（a_p は p 欠乏）とするとき、

$$L(s,E)=\prod_p (1-a_p p^{-s}+p^{1-2s})^{-1} \qquad \text{---------- ⑤}$$

を楕円曲線のゼータ関数と定義する。

⑤式において$\prod_p$ は、全ての素数 p（後に出てくる判別式Dを割らない素数）について（　）内を計算して出てきた数を全て掛け合わせることを示す。（　　）内は p と①式で示される楕円曲線 $y^2\equiv x^3+ax+b$（mod p）の p 欠乏から作られている。

Σが全ての和ならΠは全ての積である。また、(　　)$^{-1}$とは、(　　)の逆数 1／(　　)のことである。

方程式を素数 p ごとに、mod p で見ることによって得られるのが方程式のゼータ関数というわけだ。

つまり、$y^2\equiv x^3+ax+b$ という方程式を各素数 p で見て、mod p における解の個数の p に対する欠乏 a_p（$p-Np$）を数えて（　　）内を計算して出てきた数をすべて掛け合わせることにより、手がかりを得ようとするのである。$L(s,E)$は s の関数となる。

楕円曲線の方程式の各素数 p についての mod p の解の様子がわかれば、その楕円曲線の有理点の様子がわかる。楕円関数のゼータ関数というものは、mod p での解のありさまを素数 p たちについて統合して得られるもので、楕円曲線の有理点に関する何らかの調和した重要な情報が盛り込まれたものとなる。

ゼータ関数とは凄く神秘的ではないか！

⑤式の（　　）内を、$(1-x)^{-1}=1+x+x^2+x^3+\cdots\cdots$を使って書き直すと、

$(1-a_p p^{-s}+p^{1-2s})^{-1}=1+(a_p p^{-s}-p^{1-2s})+(a_p p^{-s}-p^{1-2s})^2+(a_p p^{-s}-p^{1-2s})^3+\cdots\cdots\cdots$

$=1+a_p p^{-s}+(a_p^{\,2}-p)\,p^{-2s}+\cdots\cdots\cdots$　から、これらを素数 p について掛け合わせれば、

$$L(s,E)=\sum_{n=1}^{\infty} a_n\cdot n^{-s} \qquad \text{---------- ⑥}$$

の形になることがわかる。

⑤⑥式は、⑦式に示すディリクレのＬ関数に通じている。ディリクレのＬ関数とは、

$$L(s,\chi)=\sum_{n=1}^{\infty} \chi(n)\cdot n^{-s}=\prod (1-\chi(p)p^{-s})^{-1} \qquad \text{---------- ⑦}$$

と定義され、ディリクレＬ関数の特別な場合が⑤⑥式のゼータ関数なのである。

⑦式は楕円曲線から作られるゼータ関数なので、楕円曲線のゼータ関数といい、$\overset{カイ}{\chi}(n)$をディリクレ指標と呼び、s を変数とする関数となる。

例えば、n を 4 で割った時の余りがどうなるかによって$\chi(n)$を、

n≡1（mod 4）のとき　1

n≡3（mod 4）のとき−1

n が偶数のとき　　0

とすると、

$$L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)\cdot n^{-s}=1-\frac{1}{3^s}+\frac{1}{5^s}-\frac{1}{7^s}+\frac{1}{9^s}-\frac{1}{11^s}+\frac{1}{13^s}-\cdots\cdots$$

ここで、s＝1 とすると、

$$L(1,\chi)=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\frac{1}{11}+\frac{1}{13}-\cdots\cdots=\frac{\pi}{4}$$

これは、ライプニッツの公式といい、整数（奇数）が集まって、不思議なことに整数に関係のない円周率πを作り出している。

楕円曲線のゼータ関数は、素数が自分を N（整数）で割った余りが何か、ということを主張し協力しながらできた関数といえる。

さて、虚数乗法を持たない楕円曲線（大多数の楕円曲線）について、これから凄いことが起こる。

E_3は虚数乗法を持たない楕円曲線であった。

$E_3: y^2=x^3-4x^2+16$　に対して、次の式が対応している。

$$q\prod_{n=1}^{\infty}\left[(1-q^n)(1-q^{11n})\right]^2 \qquad \text{----------⑧}$$

これを展開（n＝1，2，3 ‥‥として〔　　〕内を計算し全て掛け合わせる）すると、

$q\left[(1-q)(1-q^{11})\right]^2\cdot\left[(1-q^2)(1-q^{22})\right]^2\cdot\left[(1-q^3)(1-q^{33})\right]^2\cdot\left[(1-q^4)(1-q^{44})\right]^2\cdots\cdot$

この積は無限に続くが、最初の因数のいくつかを展開すると初めの方の項は定まり、続く何項かを展開したものを掛けても変わらなくなる。例えば、n＝23 まで掛け合わせると、

$$q-2q^2-q^3+2q^4+q^5+2q^6-2q^7-2q^9-2q^{10}+q^{11}-2q^{12}+4q^{13}$$
$$+4q^{14}-q^{15}-4q^{16}-2q^{17}+4q^{18}+2q^{20}+2q^{21}-2q^{22}-q^{23}+\cdots\cdot \qquad \text{----------⑨}$$

となり、q^{23}の項まではこれ以上掛けても不変である。

この係数とE_3に対する p 欠乏をまとめた表 4 のa_pを比べてみると、驚くことに⑨式の q の素数乗に対応する項の係数がa_pの値と完全に一致している。

そして、このパターンはすべての素数で成り立つのである。

今から６０前に、谷山豊は「すべての楕円曲線はモジュラーである」という予想を立てた。その後志村五郎が、その予想を「すべての楕円曲線はモジュラー性パターンを表すはずだ」と精密化した。

谷山・志村予想、すべての楕円曲線はモジュラー性パターンを表すとは、

無限級数　$c_1q+c_2q^2+c_3q^3+c_4q^4+\cdots\cdot$

の q の素数乗に対する項の係数c_pが楕円曲線の p 欠乏a_pに等しいことから、この式が持つある種の変換に対する対称性（これを保型性という）を持つことを意味するのである。

上半平面にある複素数 z（＝x＋iy ： y＞0）の指数関数$e^{2\pi iz}$を q(z)とすると $q(z)=e^{2\pi iz}$

$e^{2\pi i}=\cos 2\pi+i\sin 2\pi$，$\cos 2\pi=1$，$\sin 2\pi=0$ だから $e^{2\pi i}=1$、$q(z)=e^{2\pi i}\cdot e^{2\pi iz}=e^{2\pi i(z+1)}=q(z+1)$

となり、q(z)は周期 1 の周期関数である。

すべての周期関数はフーリエ級数を用いて表せるので、次式のように表すことができる。

$$f(z)=\sum_{n=1}^{\infty} c_n q^n \qquad \text{----------⑩}$$

⑩式は $n<0$ のとき $c_n=0$，さらに $n=0$ のとき $c_0=0$ が成り立つ尖点形式（カスプ形式という）が満たされるとして、フーリエ級数のΣにおいて、

$\sum_{n=-\infty}^{\infty} \rightarrow \sum_{n=1}^{\infty}$　としたものである。

ここで、$f(z)$は正則関数（複素数の関数として微分できる、つまりグラフで描けば滑らかな曲線となる）である。

$f(z)$が、$ad-bc=1$ となる整数 a，b，c，d に対し、$z\rightarrow \frac{az+b}{cz+d}$ という変換で、

$$f\left(\frac{az+b}{cz+d}\right)=(cz+d)\, f(z) \qquad \text{----------⑪}$$

が成り立つとき、$f(z)$は重み 1 の保型形式であるという。

$f(z)$が $z\rightarrow \frac{az+b}{cz+d}$ という変換を行っても型が保たれることから「保型形式」と呼んでいる。

さらに、上半平面上の重み k（整数），レベルN（自然数）の保型形式とは、

$$f\left(\frac{az+b}{cz+d}\right)=(cz+d)^k\, f(z) \qquad \text{----------⑫}$$

という変換が成り立つことをいう。(⑫式には、さらに c は N の倍数など細かい条件が存在するが省略)

重み k やレベルNについて、フェルマー予想の証明には $k=2$，$N=2$ で充分なので説明は省略する。

さあ、これでやっと保型形式のゼータ関数を定義できる。

保型形式のゼータ関数$L(s,F)$の定義。

⑩式に示す上半平面上における保型形式

$$f(z)=\sum_{n=1}^{\infty} c_n q^n$$

に対し、そのゼータ関数を

$$L(s,F)=\sum_{n=1}^{\infty} c_n n^{-s} \qquad \text{----------⑬}$$

と定義する。定義するといっても⑩式において $q^n\rightarrow n^{-s}$ と入れ替えるだけなのだ。

これは s（s は複素数）の実部が充分大きいとき収束して正則関数となる。

これから多くの $f(z)$について次式が導かれる。（これは⑤式から⑥式を導いた逆の計算で導ける）

$$L(s,F)=\prod_{p}(1-a_p p^{-s}+p^{k-1-2s})^{-1} \qquad \text{----------⑭}$$

ここで、k は重みを示す。

この⑭式は⑤式と非常に似ており、谷山・志村予想「有理数体の楕円曲線のゼータ関数は、上半平面上の重み２のある保型形式のゼータ関数である」のとおり、$k=2$ のとき一致することに気付くだろう。

谷山・志村予想の不思議さは、このように元来全く関係のない、楕円曲線から作られるゼータ関数と保型形式から導かれるゼータ関数とが一致してしまうところである。

楕円曲線というのは、まだ完全に解明されていないのであるが、それから導かれるゼータ関数がとても深いところまで解っている保型形式の理論に置き換えられてしまうのである。

さあ、いよいよこれからフェルマー予想の証明の最終段階に入る。

フェルマー予想の証明に関して、最も画期的な進展をもたらしたのが、ゲルハルト・フライ（ドイツ）である。フライは、フェルマー予想を谷山・志村予想を証明することに帰着させた。

フライのアイデアは次のようなものだ。

フェルマー予想が誤りだとすると、少なくとも１組の整数解が存在するはずである。その解を a，b，c とすると、$a^n+b^n=c^n$ となる。

ここで、次のような楕円曲線に着目する。

$$y^2=x(x-a^n)(x+b^n) \qquad \text{----------⑮}$$

この曲線をフライに敬意を表してフライ曲線と呼んでいる。

３次方程式 $x^3+ax^2+bx+c=0$ の３つの根を α，β，γ とすると、この方程式の判別式Ｄは、$D=\{(\beta-\alpha)(\gamma-\beta)(\alpha-\gamma)\}^2$ である。判別式とはその方程式がどのような根（実根，虚根，重根）を持つのかを判別するためのもので、フライ曲線の判別式は $\alpha\to0$，$\beta\to a^n$，$\gamma\to-b^n$ から、

$D=\{a^n\cdot b^n\cdot(a^n+b^n)\}^2$、$a^n+b^n=c^n$ だから $D=(a^n\cdot b^n\cdot c^n)^2=(abc)^{2n}$ となる。

つまり、判別式は自然数 abc の 2n 乗である。

判別式を考えるとき、素数 p が判別式Ｄを割らなければ mod p で考えた曲線、

$y^2\equiv(x-\alpha)(x-\beta)(x-\gamma)$（mod p）の右辺の３つの因数は異なる。

同じように mod p で考えたときに因数が重なることがある場合などの判別も可能となる。

根 α，β，γ のうち、２つが同じ場合や３つすべてが同じ場合、つまり方程式が $(x-\alpha)^2(x-\beta)=0$ や $(x-\alpha)^3=0$ のとき、判別式Ｄは 0 となってしまう。判別式が 0 とならない楕円曲線を「安定」であるといい、従ってフライ曲線は安定である。

このフライ曲線をもとに導かれたゼータ関数は、谷山・志村予想により、重さ２，レベル２の保型形式になる。そこで、楕円曲線の判別式が２ｎ乗数であるという特殊性を使えば、重さが２でレベルが２の保型形式が存在するということが証明されてしまう。

しかし、保型形式の理論によれば、そのような関数は存在しないことがわかっているので、谷山・志村予想が正しければフェルマー予想も正しいことになるのである。

フライは、判別式が 2n 乗となるような珍しい曲線は存在しないことを示唆した。この曲線は非常に奇妙であり、その p 欠乏はモジュラー性パターンを表さないはずだと予想した。

フライの予想はジャン・ピエール・セールによって精密化され、１，９８６年にケネス・リベットがモジュラー性予想（谷山・志村予想）に反することを証明した。

つまり、リベットは $a^n+b^n=c^n$ が $abc\neq0$ を満たす解をもつとき、フライ曲線がモジュラー性を持たないことを証明したのである。

このリベットの成果に促されてアンドリュー・ワイルズは、すべての（厳密にはほとんどの）楕円曲線がモジュラー性パターンを表すということを証明するために、社会から隔絶し独りこの難問と格闘し

た。そして６年後、遂にすべての安定・半安定な楕円曲線がモジュラーであることを証明したのである。

半安定とは、すべての悪い素数 $p \geqq 3$ に対して、p 欠乏 a_p が ± 1 に等しいことをいい、悪い素数とは楕円曲線を mod p で見たときに三重根となる素数をいう。フェルマー予想の証明にはこれで充分であった。なぜなら、フライ曲線は少なくとも半安定であることが示せるからである。(⑮式で仮定した曲線は安定であるが、存在しない曲線に対する判定であったため)

例えば方程式 $y^2=x^3+1$ を mod 3 でみると、$x^3+1=x^3+1+(3x^2+3x) =(x+1)^3 \pmod 3$となるので三重根となる 3 は悪い素数である。

“悪い”は舌足らずで“都合悪い”の方が適切な言葉だろう。数学者は次々と新しい用語を作るが、時にその決め方に適切さを欠くように感じることがある。

アンドリュー・ワイルズによる、谷山・志村予想の証明を以下に書く。

ここからはとても難しい。正直言って、私もほとんど理解不能である。だから当然のこと、分りやすい説明は困難だ。こんな筋道で証明がなされた、ということを知ってもらえれば満足である。

楕円曲線と保型形式を同じ土俵で比較するため、「ガロア表現」というものを使う。表面的にはガロア表現と結びつかないと思われるところを、ワイルズはガロア表現が有効なアプローチになるはずであると見抜いた。

楕円曲線から生まれるガロア表現と、保型形式から生まれるガロア表現を比較する。

整数論においてはガロア理論が大活躍する。ここでは、どうしてもガロア理論を説明しなくてはならない。ガロア理論の真髄は、色々な数の集合である「体」という難しく捉え難いものを、有限な「群」という、より分りやすい対象を見ることによって把握できるようにした「体」と「群」の対応の見事さである。「群」には基本的に演算が１種しかないのに対し、「体」には四則演算が絡み合う複雑さがある。

ガロア理論の要点を述べるだけでも長くなるので、詳細は巻末の「注２」を参照していただきたい。また、**「６ ガロア」「２６ ガロア補足」**も参考になると思う。

ここで、さらに代数の世界と解析の世界の間に、ゼータ関数を通して繋げる「非可換類体論」という重要な理論があるので、それを説明しなければならない。

その前に「類体論」とは、

「4 で割ると 1 余る素数は x^2+y^2（x，y は整数）の形に表せる。4 で割ると 3 余る素数はそのように表せない」

「8 で割ると 1 または 7 余る素数は x^2-2y^2（x，y は整数）の形に表せる。8 で割ると 3 または 5 余る素数はそのように表せない。8 で割ると 1 または 3 余る素数は x^2+2y^2（x，y は整数）の形に表せる。8 で割ると 5 または 7 余る素数はそのように表せない。」といったような法則。

ある数を素数 p で割った剰余（余り）の集合 $\mathbf{F}_p$ において、与えられた整数がその中で何かの平方数になっているか（平方根を持つか）どうかを考える『平方剰余の相互法則』

あるいは有理数体 $\mathbf{Q}$ においてその拡大体、

例えば $\mathbf{Q}(\sqrt{2})$（有理数全体を含む体 $\mathbf{Q}$ に $\sqrt{2}$ を付加した体）において、「8 で割ると 1 または 7 余る素数は、$7=(3+\sqrt{2})(3-\sqrt{2})$のように 2 つに分解し、8 で割ると 3 または 5 余る素数は分解できない」

$\mathbb{Q}(\sqrt{3})$において、「12 で割ると 1 または 11 余る素数は、$11=(2\sqrt{3}+1)(2\sqrt{3}-1)$のように 2 つに分解し、12 で割ると 5 または 7 余る素数は分解できない」などの素数の分解に関する法則。

といったような素数の性質を体系化した理論が類体論で、高木貞治により確立された整数論における大理論である。素数をある数で割った余りで「類別」することで、素数の分解の法則が決まる数の集合（体）を「類体」と呼ぶことから類体論といっている。

この理論は、ガロア群（後述）が可換群（乗法に関する交換則 xy＝yx が成り立つ群をいう）である場合には成り立つが、非可換群のときは成り立たない。

非可換群の場合における素数の分解は、非可換類体論（ガロア群が非可換群であっても通用する類体論の拡張版）によって扱うことになる。

非可換類体論において、図２のように代数的対象⇔解析的対象という、お互いの間の大きな溝を越える不思議な対応がある。非可換類体論は、代数的な対象が素数の世界を通って行くとき、各素数ごとに調和のある姿を導き出す。

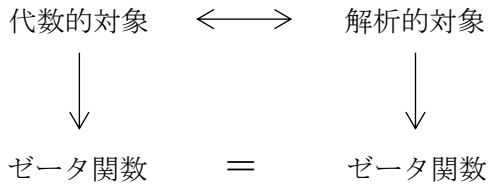


図２ 非可換類体論における対応

非可換類体論では「代数的対象⇔解析的対象」において、代数的対象の方にガロア理論が現れ、ガロア理論が活躍する。図２を書き直すと図３のようになる。

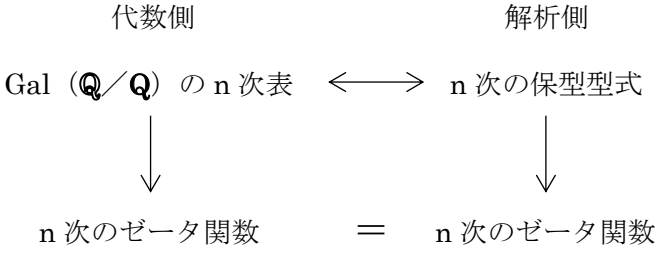


図３ 非可換類体論における対応

$\overline{\mathbb{Q}}$は有理数の集合$\mathbb{Q}$に、あらゆる代数的数を加えて得られる体で、代数的数全体を表す体である。

代数的数とは方程式の解になりうる数で、$\sqrt{2}$ や ζ_N（1 の N 乗根）などが含まれるが、π や e などの超越数（代数方程式の解となり得ない数を超越数という）は含まない。

$\overline{\mathbb{Q}}$は$\mathbb{Q}$のいろいろな拡大体（$\mathbb{Q}(\sqrt{2})$のように、体にいろいろな数を追加してさらに大きな体にしたもの）が合わさって総まとめした大きな拡大体になっている。この拡大体に対して Gal（$\overline{\mathbb{Q}}/\mathbb{Q}$）と書いて、$\overline{\mathbb{Q}}$の$\mathbb{Q}$上のガロア群と呼ぶ。

n 次表現とは何か？

群Ｇの n 次表現とは、ある体Ｆについて群の演算で保つ写像（変換と同じような意味と考えてよい）$G \to GL_n(F)$のことをいう。$GL_n(F)$は、体Ｆの元を成分とする n 次正方行列全体が、乗法に対してなす群を表す。群の演算を保つとは、その写像 ρ が $\rho(\sigma\cdot\tau)=\rho(\sigma)\cdot\rho(\tau)$という演算（群の元 σ と τ の

積の写像は、σの写像とτの写像の積に等しい）を満たすことをいう。

Gがガロア群のとき、Gのn次表現をn次ガロア表現という。フェルマー予想の証明においては、２次ガロア表現、つまり２次の非可換類体論で考えればよい。

$\mathbb{Q}$ 上の楕円曲線Eから Gal（$\overline{\mathbb{Q}}/\mathbb{Q}$）の２次ガロア表現 ρ_E

$$\rho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(F) = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} ; a, b, c, d / F, ad-bc \neq 0 \right]$$

が得られる。この$GL_2(F)$は複素数体$\mathbb{C}$の$GL_2(F)$ではなく、L進数体（‥‥−2,−1, 0, 1, 2, 3‥‥という数の体系ではなく、全く異なった観点に立って作られた数の体系）というもののGL$_2$(F)であり、このガロア表現は楕円曲線Eの等分点へのガロア群 Gal（$\overline{\mathbb{Q}}/\mathbb{Q}$）の作用から得られる。

ガロア表現は、ガロア群の絡み合う様子が行列の形として表されたもので、ワイルズは楕円曲線の等分点から導かれる $\mathbb{Q}$ のガロア拡大での素数の運命を、このガロア群を用いて考察したのである。

ガロア表現 ρ_E からゼータ関数L(s,E)が生まれ、保型形式のゼータ関数に一致する。そのゼータ関数は⑦式ディリクレのL関数 $\prod_p (1-\chi(p)p^{-s})^{-1}$ に似た形の、$\prod_p$ (pの運命を表す式, p^{-s}のn次式)$^{-1}$ であり、$\prod_p$〔(1−$\phi_p \cdot p^{-s}$) の行列式〕$^{-1}$ という形で表される。ここにϕ_pは、ガロア拡大における素数の運命に関わるn次正方行列で、「pのフロベニウス置換」と呼ばれる Gal（$\overline{\mathbb{Q}}/\mathbb{Q}$）の元の、ガロア表現による写像として出てくる行列である。

楕円曲線から生ずる２次ガロア表現の場合、この無限積は楕円曲線のゼータ関数に一致する。

楕円曲線Eに対する保型形式をFと書くと、谷山・志村予想は、

$$\begin{array}{ccc} \rho_E & \longleftrightarrow & F \\ \downarrow & & \downarrow \\ L(s,E) & = & L(s,F) \end{array}$$

という対応を示したものである。

ワイルズの論文は次の２編からなる。

（１） Modular elliptic curves and Fermat's last theorem
　　モジュラー楕円曲線とフェルマーの最終定理

（２） Ring theoretic properties of the certain Hecke algebras
　　ある種のヘッケ環の環論的性質（リチャード・テイラーとの共著）

（１）は、楕円曲線のセルマー群と呼ばれるある群の大きさが求められれば、少なくとも半安定な楕円曲線に対して谷山・志村予想が成り立つことを証明したものである。

それは、楕円曲線に伴う２次のガロア表現が保型形式に伴うガロア表現と一致することを証明する、という形をとっている。楕円曲線を直接捉えるのではなく、楕円曲線の等分点へのガロア群の作用という代数論的な性質を調べることで目的を達成しようというものである。

セルマー群とは、この場合楕円曲線の有理点から作られる群で、幾何学で言う曲線や曲面の“ねじれ”、あるいはその上で起きる現象が引き起こす“ねじれの総体”（ホモロジー群，コホモロジー群と呼ぶ）に類似したものである。セルマー群は、素数全体が作る空間やその上で起きる現象に対し、ねじれを定義したものでエタール・コホモロジーと呼ばれ、それらの幾何的構造などを反映する群である。

セルマー群はその現象のエタール・コホモロジーとして定義される。

ワイルズにとって証明したいのは「楕円曲線は、少なくとも半安定ならばモジュラーである」という命題である。そのためには、いろいろな素数に関してガロア表現を考察し、そこからEがモジュラーであるということを導くのが普通のやり方に思える。

しかし、ワイルズのとった道はそうではなかった。たった１つの素数に対してガロア表現を考察し、それがモジュラーならば楕円曲線もモジュラーになることを証明し、それを他の素数についても自動的に成り立つようにしようというのである。

（１）で残ったのは、セルマー群の大きさを求めることであった。

１，９９３年の論文では、それを群の位数間の不等式にまで還元し、その不等式をロシアの数学者コリヴァギン（彼は楕円曲線上に有理点が無数に存在するためには、Ｌ関数：Ｌ（1，Ｅ）＝0となることが必要条件であるという難問[バーチ・スゥインナートン＝ダイヤー予想]解決のための大発見をし急進展させた）が発明したオイラー・システムと呼ばれる考え方により証明しようとした。

しかし、その証明の中に大きな欠陥が見つかったのである。

谷山・志村予想をセルマー群の元の数に還元する基本的な部分は正しかったのだが，セルマー群の位数の正確な上限を求める計算が完全ではなかったのである。

ワイルズは、もともとヘッケ環を利用する方法を考えており、そのためにオイラー・システムを利用すればうまくいくと考えていた。しかし思うように行かず、結局オイラー・システムによる方法を改め、当初考えていたヘッケ環の様子を直接調べるやり方で、再度フラッハの理論を一般化する試みを行うなかで、遂にセルマー群の大きさを求めることに成功し難局を乗り越えたのだった。

論文（２）において、ヘッケ環（Ｔ）というのは、保型形式のなす空間に作用するヘッケ作用素と呼ばれる作用素に加算，乗算を定義して得られる体系である。ヘッケ作用素とは、その固有値λ_n（説明省略）からオイラー積を持つゼータ関数 $\sum_{n=1}^{\infty} \lambda_n n^{-s}$が得られる作用素（ゼータ関数を生む作用素）である。ヘッケ環には保型形式の重要な性質が隠されていることが知られていた。

ワイルズは、そのヘッケ環が「完全交差性（説明省略）」という、環として非常に良い性質を持つことを示し、着目する楕円曲線に伴う２次のガロア表現 Gal（$\mathbb{Q}$／$\mathbb{Q}$）→GL_2(F)が、全てヘッケ環（Ｔ）を通して捉えられることを示した。

群演算を保つ写像：Gal（$\mathbb{Q}$／$\mathbb{Q}$）→GL_2(T)

GL_2(T)はＴの元を成分とする２次正方行列全体のなす群で、Gal（$\mathbb{Q}$／$\mathbb{Q}$）→GL_2(F)は、環構造を保つある写像Ｔ→Ｆから、Gal（$\mathbb{Q}$／$\mathbb{Q}$）→GL_2(T)→GL_2(F)というように合成として得られることになる。楕円曲線に伴う２次ガロア表現が、保型形式に関係したヘッケ環で捉えられるということは、谷山・志村予想が正しいことを意味するのである。

ワイルズが証明したのは、有理数体$\mathbb{Q}$上の楕円曲線Ｅ（係数が有理数である楕円曲線）に対し、上半平面上の重み２の保型形式Ｆで、

$L(s,E)=L(s,F)$

となるものが存在するということを、半安定の楕円曲線について成立することを示したのである。

ワイルズは谷山・志村予想の大きな部分を証明したことにより、その副産物としてフェルマー予想を証明した。この証明により、楕円曲線のゼータ関数$L(s,E)$は、保型形式のゼータ関数となり、従って複

素平面全体に解析接続（上半平面でのみ定義されていた保型形式が、複素平面全体でそれに一致するものが存在することをいう）されることが初めて証明されたことになる。

この小文は数学の論文ではない。用語の定義や表示方法などに厳密性を欠くことについては、お許しいただきたい。

最後に、この想像を超える、抽象的で不可思議な理論を理解できる頭脳とは、どのようなものなのだろう？私の頭脳と入手可能な文献や資料からは、これ以上の説明は困難である。

（注１）

これは、位相幾何学（トポロジー）の問題である。「3 次元閉多様体」とは『3 次元空間において、破れた穴の空いていない複雑な形をした立体』、「短連結」とは『輪になった紐を縮めていって 1 点にすることができるというような意味』、「3 次元球面 S^3 に同相」とは『3 次元の球そのものである』ということである。

例えば、船に乗って地球を一周したとき、我々は地球が球体ということを知っているが、それはドーナツ型かも知れない。ドーナツ型でも一周することができるからである。ぐるっと一周しても自分がいるのが球なのかドーナツなのかわからない。その立体から離れて見ない限り分らないのだ。

ところが、もしその曲面上でどのように掛けた輪も縮めて 1 点にできれば、それはドーナツ型（もっと複雑な形かもしれない）ではなく球しかありえない。このことを証明せよというのがポアンカレ予想である。

（注２）

ガロア理論（要点のみ）

四則演算の定義された集合を体と呼ぶ。ガロア理論は群と体についての奥深い理論である。

円分体の例を用いてガロア理論とガロア群の要点を説明する。

自然数 N に対し、ζ_N で複素平面（図 A）に記した位置にある複素数をあらわす。これを円分体といい ζ_N は 1 の N 乗根であり、ζ_N（$0 \leqq a \leqq N-1$）が 1 のすべての N 乗根になる。例えば N＝12 の場合を考える。図 B において、有理数体 $\mathbf{Q}$（有理数全体を含む数の集合）と 1 の 12 乗根 ζ_{12} から四則演算によって作られる数全体がなす体を、$\mathbf{Q}(\zeta_{12})$ と書く。

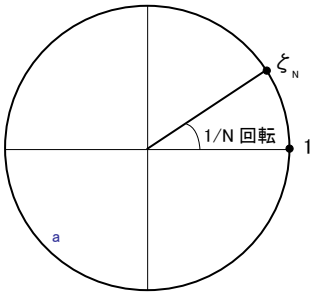


図 A 複素平面における1の N 乗根

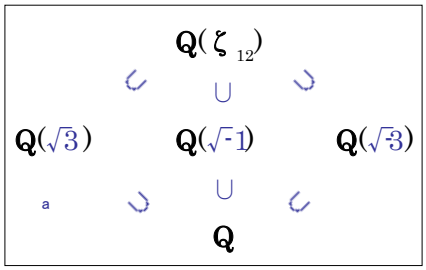


図 B 部分体の包含関係

ζ_{12} を ζ_{12}^{0} から ζ_{12}^{11} まで書くと表 A のようになる。

図 A の半径 1 の円において、ζ_{12} は円周の１２等分点を複素数で表したものである。

各点は、$\cos(2n\pi/12)+i\sin(2n\pi/12)$ において、n＝0, 1, 12------, 11 とすることにより得られる。

1の12乗根の記号	角度 $\pi=180^\circ$	1の12乗根の値	1の3乗根の場合	1の4乗根の場合
ζ_{12}^{0}	0	1	ζ_{3}^{0}	ζ_{4}^{0}
ζ_{12}^{1}	$\pi/6$	$\sqrt{3}/2+1/2\,i$		
ζ_{12}^{2}	$\pi/3$	$1/2+\sqrt{3}/2\,i$		
ζ_{12}^{3}	$\pi/2$	i		ζ_{4}^{1}
ζ_{12}^{4}	$2\pi/3$	$-1/2+\sqrt{3}/2\,i$	ζ_{3}^{1}	
ζ_{12}^{5}	$5\pi/6$	$-\sqrt{3}/2+1/2\,i$		
ζ_{12}^{6}	π	-1		ζ_{4}^{2}
ζ_{12}^{7}	$7\pi/6$	$-\sqrt{3}/2-1/2\,i$		
ζ_{12}^{8}	$4\pi/3$	$-1/2-\sqrt{3}/2\,i$	ζ_{3}^{2}	
ζ_{12}^{9}	$3\pi/2$	$-i$		ζ_{4}^{3}
ζ_{12}^{10}	$5\pi/3$	$1/2-\sqrt{3}/2\,i$		
ζ_{12}^{11}	$11\pi/6$	$\sqrt{3}/2-1/2\,i$		

表A 1の12乗根

表Aのζ_{12}^{0}からζ_{12}^{11}を見ると、1の12乗根の中に有理数以外の数として、$\sqrt{3}$，$\sqrt{-1}(=i)$，$\sqrt{-3}(=\sqrt{3}i)$がある。

これから、$\mathbf{Q}(\zeta_{12})$には、$\mathbf{Q}(\sqrt{3})=\{a+b\sqrt{3}:a,\ b\in\mathbf{Q}\}$

$\mathbf{Q}(\sqrt{-1})=\{a+b\sqrt{-1}:a,\ b\in\mathbf{Q}\}$

$\mathbf{Q}(\sqrt{-3})=\{a+b\sqrt{-3}:a,\ b\in\mathbf{Q}\}$

などの体が含まれていることになる。

さて、$\mathbf{Q}(\zeta_{12})$に含まれる体は、体$\mathbf{Q}(\sqrt{3})$，$\mathbf{Q}(\sqrt{-1})$，$\mathbf{Q}(\sqrt{-3})$の他にも存在するだろうか？「他には存在しない」というのが正解なのだが、どのようにしてそんなことがわかるのだろうか？

ガロア理論は、どのように体が存在しているかがすべてわかる理論なのである。

$\mathbf{Q}(\zeta_{12})$に入る前に簡単な例として、複素数体$\mathbf{C}$（全ての複素数を含む数の集合）における共役写像（複素数の虚数部分の符号を反転させる変換λ）：$\lambda(x+yi)=x-yi$（x,yは実数）について説明する。

λは四則演算を保ち（複素数α，βに対し$\lambda(\alpha+\beta)=\lambda(\alpha)+\lambda(\beta)$，$\lambda(\alpha\,\beta)=\lambda(\alpha)\lambda(\beta)$が成立する）。また$\lambda$は実数を動かさない。

これを計算で示す。

加算について、$\lambda\{(\alpha_1+\alpha_2 i)+(\beta_1+\beta_2 i)\}=\lambda\{(\alpha_1+\beta_1)+(\alpha_2+\beta_2)\,i\}=(\alpha_1+\beta_1)-(\alpha_2+\beta_2)\,i$

$=(\alpha_1-\alpha_2 i)+(\beta_1-\beta_2 i)=\lambda(\alpha_1+\alpha_2 i)+\lambda(\beta_1+\beta_2 i)$

乗算について、$\lambda\{(\alpha_1+\alpha_2 i)\cdot(\beta_1+\beta_2 i)\}=\lambda\{(\alpha_1\beta_1-\alpha_2\beta_2)+(\alpha_1\beta_2+\alpha_2\beta_1)\,i\}$

$=(\alpha_1\beta_1-\alpha_2\beta_2)-(\alpha_1\beta_2+\alpha_2\beta_1)\,i=\alpha_1(\beta_1-\beta_2 i)-\alpha_2(\beta_1-\beta_2 i)\,i$

$=(\alpha_1-\alpha_2 i)\cdot(\beta_1-\beta_2 i)=\lambda(\alpha_1+\alpha_2 i)\cdot\lambda(\beta_1+\beta_2 i)\}$

$\mathbf{C}$から$\mathbf{C}$への四則演算を保ち、実数を動かさない写像は、この共役写像λと恒等写像（$\mathbf{C}$の元をまったく動かさない写像）の2つのみである。これを自己同型写像という。

そしてこれらの写像でまったく動かされない $\mathbf{C}$ の元全体は、実数体 $\mathbf{R}$（図１で無理数の枠に囲まれる数全体の集合）に一致する。この $\mathbf{C}$（複素数体）と $\mathbf{R}$（実数体）のあいだで起こったことと同じことを、$\mathbf{Q}(\zeta_{12})$ と $\mathbf{Q}$ のあいだで考える。

$\mathbf{Q}(\zeta_{12})$ から $\mathbf{Q}(\zeta_{12})$ への、四則演算を保ち $\mathbf{Q}$ の元を動かさない写像全体をガロア群といい、

Gal（$\mathbf{Q}(\zeta_{12})/\mathbf{Q}$）と書く。

$\mathbf{C}$ と $\mathbf{R}$ については、Gal（$\mathbf{C}/\mathbf{R}$）＝{λ(共役写像), 恒等写像}であったが、Gal（$\mathbf{Q}(\zeta_{12})/\mathbf{Q}$）はもう少し複雑になり、次のようになる。

a を N と互いに素な整数（N と共通の素因数を持たない整数）とすると、Gal（$\mathbf{Q}(\zeta_{12})/\mathbf{Q}$）の元の中に唯一つ、$\sigma_a(\zeta_{12})=\zeta_{12}^{\,a}$ をみたす σ_a という元が存在する。そして Gal（$\mathbf{Q}(\zeta_{12})/\mathbf{Q}$）の元はこういう σ_a のみで、それ以外にはない。σ_a と他の元 σ_b は、$a\equiv b \pmod N$ の時、その時に限り一致する。

ζ_{12} においてガロア群は、Gal（$\mathbf{Q}(\zeta_{12})/\mathbf{Q}$）＝$\{\sigma_1,\ \sigma_5,\ \sigma_7,\ \sigma_{11}\}$である。（これらの 4 個の元は互いに異なる）具体的な $\sigma_1,\ \sigma_5,\ \sigma_7,\ \sigma_{11}$ は以下の通りである。

σ_1 は恒等写像	$\sqrt{3}/2+1/2\,i \rightarrow \sqrt{3}/2+1/2\,i$
σ_5 は無理数$\sqrt{3}$ の符号を反転させる共役写像	$\sqrt{3}/2+1/2\,i \rightarrow -\sqrt{3}/2+1/2\,i$
σ_7 は無理数$\sqrt{3}$ 及び複素数の虚数部分の符号を反転させる共役写像	$\sqrt{3}/2+1/2\,i \rightarrow -\sqrt{3}/2-1/2\,i$
σ_{11} は複素数の虚数部分の符号を反転させる共役写像	$\sqrt{3}/2+1/2\,i \rightarrow \sqrt{3}/2-1/2\,i$

また、これらの写像が四則演算を保つことを末尾に示す。

Gal（$\mathbf{Q}(\zeta_N)/\mathbf{Q}$）は、写像の合成[$\circ$]について「群」になる。

$\sigma_a\circ\sigma_b=\sigma_{ab}$ で、

$$(\sigma_a\circ\sigma_b)(\zeta_N)=\sigma_a(\sigma_b(\zeta_N))=\sigma_a(\zeta_N^{\,b})=\sigma_a(\zeta_N)^b=(\zeta_N^{\,a})^b=\zeta_N^{\,ab}$$

であるから、例えば Gal（$\mathbf{Q}(\zeta_{12})/\mathbf{Q}$）において、

$\sigma_5\circ\sigma_5=\sigma_{25}=\sigma_1$,　$\sigma_5\circ\sigma_7=\sigma_{35}=\sigma_{11}$

などが成りたつ。それらを全てまとめると表Ｂ，Ｃのようになる。

	σ_1	σ_5	σ_7	σ_{11}
σ_1	σ_1	σ_5	σ_7	σ_{11}
σ_5	σ_5	σ_1	σ_{11}	σ_7
σ_7	σ_7	σ_{11}	σ_1	σ_5
σ_{11}	σ_{11}	σ_7	σ_5	σ_1

表B ガロア群 Gal($\mathbf{Q}(\zeta_{12})/\mathbf{Q}$)写の合成に対して群になる

	σ_1	σ_5
σ_1	σ_1	σ_5
σ_5	σ_5	σ_1

	σ_1	σ_7
σ_1	σ_1	σ_7
σ_7	σ_7	σ_1

	σ_1	σ_{11}
σ_1	σ_1	σ_{11}
σ_{11}	σ_{11}	σ_1

表C ガロア群 Gal($\mathbf{Q}(\zeta_{12})/\mathbf{Q}$)の部分群

ガロア理論の基本定理によれば、Gal（$\mathbf{Q}(\zeta_N)/\mathbf{Q}$）の部分群（部分集合でかつ写像の合成[$\circ$]について群になっているもの）と、$\mathbf{Q}(\zeta_N)\supseteq\mathbf{M}\supseteq\mathbf{Q}$ となる体 $\mathbf{M}$ とは１対１に対応する。

例えば、Gal（$\mathbf{Q}(\zeta_N)/\mathbf{Q}$）の部分群は表 C 及び図 C に書いた、$\{\sigma_1,\ \sigma_5\}$, $\{\sigma_1,\ \sigma_7\}$, $\{\sigma_1,\ \sigma_{11}\}$しかない。

１対１対応があるということは、$\mathbf{Q}(\zeta_{12})\supseteq\mathbf{M}\supseteq\mathbf{Q}$ となる体 $\mathbf{M}$ は、図 B に登場したもの以外にはないこ

とがわかる。$\mathbf{Q}(\zeta_{12})$に含まれる体は必ず $\mathbf{Q}$ を含んでしまうので、$\mathbf{Q}(\zeta_{12})$に含まれる体は図 B に登場したものしかないことがわかるのである。

ガロア理論というのは、このような 1 対 1 対応の存在をいうものである。$\mathbf{K}$ を体、$\mathbf{k}$ をその部分体とする。そして後でふれる、「$\mathbf{K}$ が $\mathbf{k}$ の有限次ガロア拡大である」という条件が成立するとき、$\mathbf{K}$ から $\mathbf{k}$ への、四則演算を保ち $\mathbf{k}$ の元を動かさない写像全体を Gal（$\mathbf{K}$／$\mathbf{k}$）と書く。

これは合成[○]について有限群（有限個の元からなる群）になるが、Gal（$\mathbf{K}$／$\mathbf{k}$）を $\mathbf{K}$ の $\mathbf{k}$ 上のガロア群と呼ぶ。ガロア理論の主定理は、「Gal（$\mathbf{K}$／$\mathbf{k}$）の部分群 $\mathbf{H}$ と、$\mathbf{K}\supseteq\mathbf{M}\supseteq\mathbf{k}$ となる体 $\mathbf{M}$ が、次の対応で 1 対 1 に対応する」というものである。

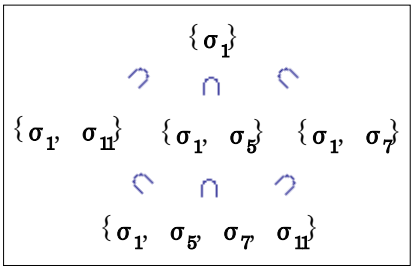


図 C 群の包含関係

これにより、どのように体が存在しているかがすべて分るのである。$\mathbf{H}$ に対し $\mathbf{M}$ は、$\mathbf{H}$ のすべての元で動かされない $\mathbf{K}$ の元全体、逆に $\mathbf{M}$ に対し $\mathbf{H}$ は、$\mathbf{M}$ のすべての元を動かさない Gal（$\mathbf{K}$／$\mathbf{k}$）の元全体。「$\mathbf{K}$ が $\mathbf{k}$ の有限次ガロア拡大である」という条件は、$\mathbf{k}$ が $\mathbf{Q}$ を含む体である場合は次の通りとなる。

「k の元を係数とする或る多項式

$f(x)=x^n+a_1x^{n-1}+\cdots\cdots\cdots+a_n$（$n\geqq 1$，$a_1$，----，$a_n\in\mathbf{k}$）

があって、$\mathbf{K}$ は $\mathbf{k}$ と $f(x)=0$ のすべての根から、四則演算によって得られるもの全体がなす体である」

例えば $\mathbf{Q}(\zeta_N)$が Q の有限次ガロア拡大であることは、$\mathbf{K}=\mathbf{Q}(\zeta_N)$，$\mathbf{k}=\mathbf{Q}$，$f(x)=x^N-1$、としてみればわかる。なお図 B と図 C の間では、対応する場所にある体と群が、ちょうどガロア理論によって対応する体と群になっている。

Gal（$\mathbf{C}$／$\mathbf{R}$）の元の個数は 2 であるが、これは $\mathbf{C}$ の元が $a+bi$（a，$b\in\mathbf{R}$）というように、2 個の $\mathbf{R}$ の元を使ってあらわされることと関係している。

一般に $\mathbf{K}$ が $\mathbf{k}$ の有限次ガロア拡大であるとき、Gal（$\mathbf{K}$／$\mathbf{k}$）の元の個数は $\mathbf{K}$ と $\mathbf{k}$ 点の間の拡大次数と呼ばれ、［$\mathbf{K}:\mathbf{k}$］と書かれる次の数に一致する。$\mathbf{K}$ の元 a_1，a_2 ------，a_n を適当にとれば、$\mathbf{K}$ のどの元もただひととおりに、

$a_1\alpha_1+a_2\alpha_2+\cdots\cdots+a_n\alpha_n$　（a_1，a_2 ------，$a_n\in\mathbf{k}$）

の形に書くことができる。拡大次数［$\mathbf{K}:\mathbf{k}$］とはこの n のことをいう。（つまり $\mathbf{K}$ の元を n 個の $\mathbf{k}$ の元を使ってあらわすことができる）

例えば、$\mathbf{Q}(\sqrt{3})$ の元は、ただひととおりに $a+b\sqrt{3}$（a，$b\in\mathbf{Q}$）の形にあらわされるから、

［$\mathbf{Q}(\sqrt{3})$：$\mathbf{Q}$］＝2

Gal（$\mathbf{K}$／$\mathbf{k}$）の部分群 $\mathbf{H}$ と、$\mathbf{K}\supseteq\mathbf{M}\supseteq\mathbf{k}$ となる体 $\mathbf{M}$ が対応している時、

［$\mathbf{M}:\mathbf{k}$］＝（Gal（$\mathbf{K}$／$\mathbf{k}$）の元の個数）÷（$\mathbf{H}$ の元の個数），

［$\mathbf{K}:\mathbf{M}$］＝$\mathbf{H}$ の元の個数、が成立する。

σ_1, σ_5, σ_7, σ_{11} について、それぞれが四則演算を保つことを以下に示す。

加算については成立することが明らかなので、σ_1, σ_5, σ_7, σ_{11} の乗算について、

$\sigma_{1/5/7/11}(\alpha\ \beta)=\sigma_{1/5/7/11}(\alpha)\cdot\sigma_{1/5/7/11}(\beta)$が成立することを計算で確認する。

α ：$a_1+b_1\sqrt{3}+c_1i+d_1\sqrt{3}i$,

β ：$a_2+b_2\sqrt{3}+c_2i+d_2\sqrt{3}i$ とする。

σ_1（恒等写像：$\sqrt{3}/2\ +1/2\,i\rightarrow\ \sqrt{3}/2\ +1/2\,i$）

$\rightarrow(a_1+b_1\sqrt{3}+c_1i+d_1\sqrt{3}i)\cdot(a_2+b_2\sqrt{3}+c_2i+d_2\sqrt{3}i)$

σ_5（無理数$\sqrt{3}$の符号を反転させる共役写像：$\sqrt{3}/2\ +1/2\,i\rightarrow-\sqrt{3}/2\ +1/2\,i$）については、

$\rightarrow(a_1-b_1\sqrt{3}+c_1i-d_1\sqrt{3}i)\cdot(a_2-b_2\sqrt{3}+c_2i-d_2\sqrt{3}i)$

σ_7（無理数$\sqrt{3}$及び複素数の虚数部分の符号を反転させる共役写像：$\sqrt{3}/2\ +1/2\,i\rightarrow-\sqrt{3}/2-\ 1/2\,i$）

$\rightarrow(a_1-b_1\sqrt{3}-c_1i+d_1\sqrt{3}i)\cdot(a_2-b_2\sqrt{3}-c_2i+d_2\sqrt{3}i)$

σ_{11}（複素数の虚数部分の符号を反転させる共役写像）

$\rightarrow(a_1+b_1\sqrt{3}-c_1i-d_1\sqrt{3}i)\cdot(a_2+b_2\sqrt{3}-c_2i-d_2\sqrt{3}i)$

をそれぞれ計算した時の、以下の各項（４種類）の符号をまとめて表 D に示す

・有理数項（$a_1\,a_2$, b_1b_2, c_1c_2, d_1d_2 の項）

・$\sqrt{3}$ の項（$a_1\,b_2$, a_2b_1, c_1d_2, c_2d_1 の項）

・i の項（$a_1\,c_2$, a_2c_1, b_1d_2, b_2d_1 の項）

・$\sqrt{3}i$ の項（$a_1\,d_2$, a_2d_1, b_1c_2, c_2d_1 の項）

	σ_1				σ_5				σ_7				σ_{11}			
有理数項	a_1a_2	b_1b_2	c_1c_2	d_1d_2	a_1a_2	b_1b_2	c_1c_2	d_1d_2	a_1a_2	b_1b_2	c_1c_2	d_1d_2	a_1a_2	b_1b_2	c_1c_2	d_1d_2
	＋	＋	－	－	＋	＋	－	－	＋	＋	－	－	＋	＋	－	－
√3の項	a_1b_2	a_2b_1	c_1d_2	c_2d_1	a_1b_2	a_2b_1	c_1d_2	c_2d_1	a_1b_2	a_2b_1	c_1d_2	c_2d_1	a_1b_2	a_2b_1	c_1d_2	c_2d_1
	＋	＋	－	－	－	－	＋	＋	－	－	＋	＋	＋	＋	－	－
iの項	a_1c_2	a_2c_1	b_1d_2	b_2d_1	a_1c_2	a_2c_1	b_1d_2	b_2d_1	a_1c_2	a_2c_1	b_1d_2	b_2d_1	a_1c_2	a_2c_1	b_1d_2	b_2d_1
	＋	＋	＋	＋	＋	＋	＋	＋	－	－	－	－	－	－	－	－
√3iの項	a_1d_2	a_2d_1	b_1c_2	c_2d_1	a_1d_2	a_2d_1	b_1c_2	c_2d_1	a_1d_2	a_2d_1	b_1c_2	c_2d_1	a_1d_2	a_2d_1	b_1c_2	c_2d_1
	＋	＋	＋	＋	－	－	－	－	＋	＋	＋	＋	－	－	－	－

表 D〔$\sigma_{1/5/7/11}(\alpha)\cdot\sigma_{1/5/7/11}(\beta)$を計算した時の各項符号のまとめ〕

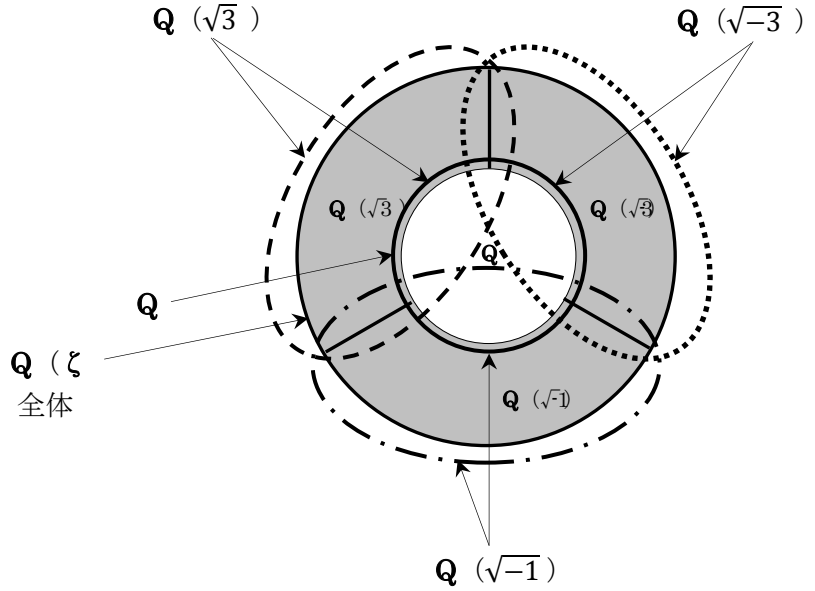
表 D は、σ_1 に対し符号が反転している部分を ▭ で示している。

表中の σ_5, σ_7, σ_{11} は、$\sigma_{5/7/11}(\alpha)\cdot\sigma_{5/7/11}(\beta)$を計算結果した時の各項の符号を示している。

一方、$\sigma_{1/5/7/11}(\alpha\ \beta)$は$\sigma_1$（恒等写像）の対応する項の符号を反転したものに対応するので、

$\sigma_{1/5/7/11}(\alpha\ \beta)=\sigma_{1/5/7/11}(\alpha)\cdot\sigma_{1/5/7/11}(\beta)$が確認されるだろう。

$\mathbf{Q}(\zeta_{12})$，$\mathbf{Q}$に対する、$\mathbf{Q}(\sqrt{3})$，$\mathbf{Q}(\sqrt{-1})$，$\mathbf{Q}(\sqrt{-3})$の関係を図で示す。



参考文献

１．フェルマーの最終定理・佐藤－テイト予想解決への道（類体論と非可換類体論１）　加藤和也

２．解決！フェルマーの最終定理　　加藤和也

３．フェルマーの大定理（第３版）　足立恒雄

４．フェルマーの大定理が解けた！　足立恒雄

５．はじめての数論 第３版（訳本）　ジョセフ・H. シルヴァーマン

６．体とガロア理論（岩波基礎数学選書）　藤崎源二郎

（２０１３．０４．１０）