５４「イデアル」

イデアルについては、**「４３ フェルマーの最終定理」**で少し触れた。

クンマー（ドイツ 1,810～1,893）は、フェルマーの方程式を解くために素因数分解の一意性（素因数分解がただ一通りにしかできない）から出発した。どんな自然数（1，2，3，‥‥）も 6＝2×3，15＝3×5，78＝2×3×13 のように、ただ一通りに素数の積で表せる。

クンマーはフェルマーの方程式 $x^n+y^n=z^n$ の左辺を、

① $x^n+y^n=(x+y)(x+\zeta y)(x+\zeta^2 y)\cdots\cdots(x+\zeta^{n-1} y)=\prod_{k=0}^{n-1}(x+\zeta^k y)$

というように因数分解することで解けるはずだと考えた。

（ここで$\prod$は各項の積を表し、ζ，ζ^2，ζ^3‥‥‥，ζ^{n-1} は n 乗すると 1 になる数（1 の n 乗根）で、$\zeta=\cos\left(\frac{2\pi}{n}\right)+i\sin\left(\frac{2\pi}{n}\right)$という複素数で表される）

ところが、図１「数の体系図」に示すように数の範囲を広げ複素数の範囲で考えると、$6=2\times3=(1+\sqrt{-5})(1-\sqrt{-5})$，$15=3\times5=3\times(2+\sqrt{-1})(2-\sqrt{-1})$，$78=2\times3\times13=2\times3\times(4+\sqrt{-1})(4-\sqrt{-1})$というように、２通りあるいはそれ以上に分解してしまう。つまり、自然数の世界の因数分解の一意性が複素数の世界では成立しなくなってしまうのである。

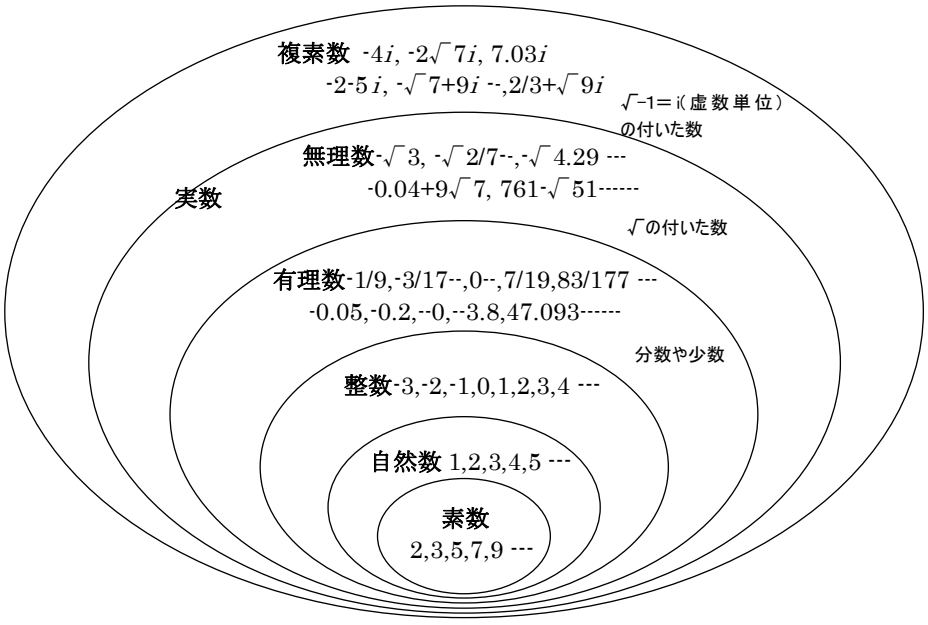


図１ 数の体系図

①の右辺 $\prod_{k=0}^{n-1}(x+\zeta^k y)$ は変幻自在の世界で、

② $a_0+a_1\zeta_n+a_2\zeta^2_{n-1}+a_3\zeta^3_{n-2}+\cdots\cdots+a_k\zeta^k_{n-k}$ （a_0，a_1，$a_2\cdots\cdots a_k$ は整数）

と表される数（代数的整数）なのであった。

例えば 31 は、$31=(3+\sqrt[3]{2}^2)(3+3\sqrt[3]{2}+\sqrt[3]{2}^2)(3-3\sqrt[3]{2}+\sqrt[3]{2}^2)$　　無理数の世界で因数分解

$31=(2+\zeta_5)(2+\zeta^2_5)(2+\zeta^3_5)(2+\zeta^4_5)$　　複素数の世界で因数分解

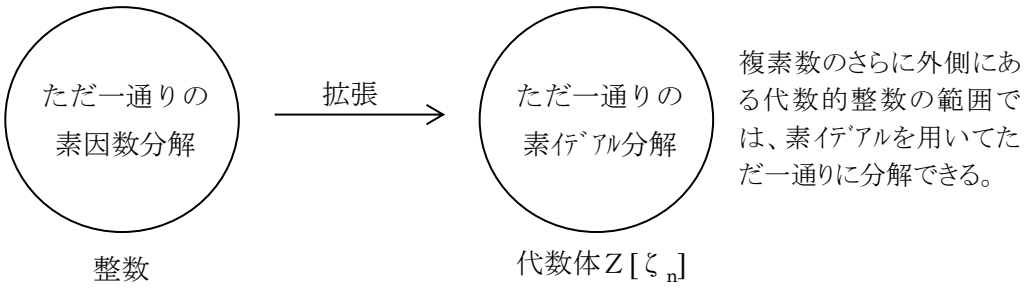
ここでζ_5，ζ^2_5，ζ^3_5，ζ^4_5について○＋○i という形で示すと

$\zeta_5=0.3090+0.9510i$　　$\zeta^2_5=-0.8090+0.5877i$

$\zeta^3_5=-0.8090-0.5877i$　　$\zeta^4_5=0.3090-0.9510i$　　である。

このように２通り、あるいはそれ以上に分解できしまう。実は“２”も分解できて、$2=\sqrt{-1}(1-\sqrt{-1})^2$ となる。

クンマーは、このように無理数や複素数の世界に入ると、素因数分解の一意性が成立しないことに気付き、これを乗り越えようと“イデアルの概念”を導入してフェルマーの方程式に迫った。その考え方は、素因数分解の一意性を代数体（②式に示すような数の集合で代数方程式の解となる数を含む集合）へと拡張し一般化したものである。クンマーは代数体の世界における素因数分解一意性の障害となるものが、$Z[\zeta_n]$（整数に代数的整数を加えた数の集合[足し算，引き算，掛け算が自由にできる]）のイデアル類群という「群」であることを発見した。$Z[\zeta_n]$における基本原則は、ただ一通りの素イデアル分解ができることである。



素イデアルとはどのようなものなのか？

例えば、$6=2\times3=(1+\sqrt{-5})(1-\sqrt{-5})$において、p，q，q′という新しい数（素イデアル）を考える。

すると「６」は表１のように素イデアルに分解できる。

２乗することによって 2 になるイデアルという世界に存在する“p”という数（素イデアル）（勿論 $\sqrt{2}$ではない）	$2=p^2$
p，q，q' は演算すると右のようになる数（素イデアル）	$3=qq'$
	$(1+\sqrt{-5})=pq$
	$(1-\sqrt{-5})=pq'$

表１　「６」の素イデアル分解

このような素イデアルを使うと、$6=p^2\cdot(qq')=(pq)\cdot(pq')$と書くことができ、素イデアルによって一意的に分解され、ただまとめ方の違いに過ぎないと考えることができる。p は 2 と$(1+\sqrt{-5})$と$(1-\sqrt{-5})$の、q は 3 と$(1+\sqrt{-5})$の、q′は 3 と$(1-\sqrt{-5})$のイデアルの世界における最大公約数のようなもの（素イデアル）と考えられる。

そしてクンマーは、フェルマーの方程式に対して「p を素数とするとき、もし$Z[\zeta_n]$のイデアル類群の位数（イデアル類群の元の個数）が p で割れなければ、$x^p+y^p=z^2$ をみたす自然数 x，y，z は存在し

ない」ことを証明した。

イデアル類群とは「イデアルの世界」と「数の世界」のずれを捉えるもので、イデアル類群の位数が大きければ数の世界とのずれが大きく考察が難しくなる。

例えば $Q[\sqrt{-5}]$（有理数[分数，少数までを含む数の集合]に$\sqrt{-5}$ を加えた数の集合）のイデアル類群は、単位元$\left[\left(\frac{b_1}{a_1},\ \frac{2b_1}{a_1},\ \frac{3b_1}{a_1}\cdots\cdot\frac{nb_1}{a_1}\right),\ \left(\frac{b_2}{a_2},\ \frac{2b_2}{a_2},\ \frac{3b_2}{a_2}\cdots\cdot\frac{nb_2}{a_2}\right),\ \cdots\cdot\right]$ など分数イデアルの集まりと、

〔c_1，c_2，c_3，$\cdots\cdot c_n$，$d_1\pm\sqrt{-5}$，$d_2\pm\sqrt{-5}$，$d_3\pm\sqrt{-5}$，$\cdots\cdot d_n\pm\sqrt{-5}$ 〕など整数，整数$\pm\sqrt{-5}$を含む２つの元からなる群である。

代数体のイデアル類群は必ず有限個の元からなり、イデアル類群の元の個数をその代数体の位数と呼ぶ。$\mathbf{Q}$（有理数体）の位数は１，$\mathbf{Q}[\sqrt{-5}]$の位数は２である。$\mathbf{Q}[\zeta_n]$の位数を示すと表２のようになる。

n	1～22	23	24～28	29	30	31	32～36	37	38	39
$\mathbf{Q}[\zeta_n]$の位数	1	3	1	8	1	9	1	37	1	2

表２ $\mathbf{Q}[\zeta_n]$ におけるイデアル類群の位数

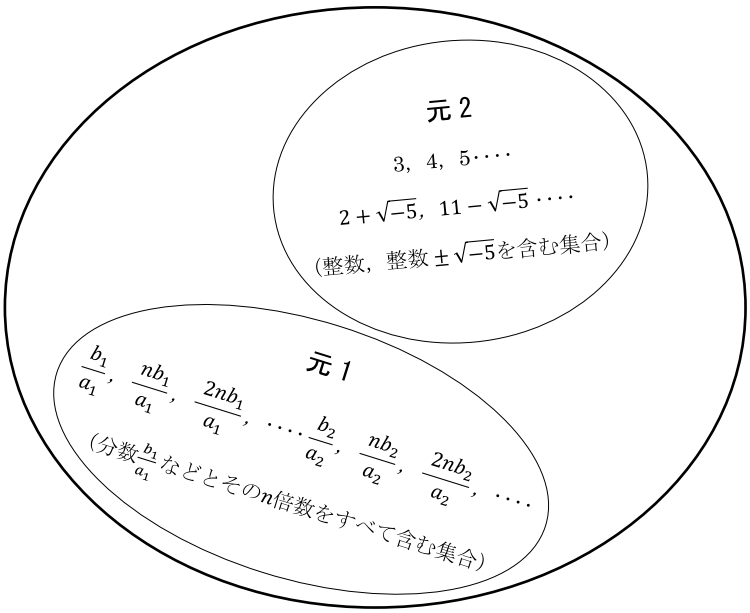


図２ $\mathbf{Q}[\sqrt{-5}]$のイデアル類群の元

表２において、位数が１の n については、ただ一通りの因数分解となるが、１以外では因数分解の一意性は成り立たない。このイデアル類群の考え方から、クンマーは n が３以上の素数で、$\mathbf{Q}[\zeta_n]$の位数が n の倍数でなければ $x^n+y^n=z^n$ を満たす自然数は x，y，z は存在しないことを証明したのである。表１でいえば n＝37 のとき位数が 37 で n の倍数となっているので、$x^{37}+y^{37}=z^{37}$ についての自然数解の有無はこの定理からはいえない。「37」は非正則素数と呼ばれ、100 以下では 37 の他に「59」「67」がこれにあたる。このようにクンマーの導入したイデアルの概念により、フェルマーの方程式は多くの n について証明されたことになる。（２０１３．１２．２３）