代数的整数論の道案内

村上友哉

2021 年 5 月 25 日

はじめに

この文書は, 代数的整数論をこれから勉強したい人や要点を速習したい人, あるいは勉強したけれど消化不良感がある人のための道案内として書かれたものです. 証明の細部には立ち入らず, なぜこのようなことを考えるのかというモチベーション, 理論の源泉となる具体的な計算例, 勉強する上で躓きやすいポイントを紹介することに重点を置きます. 他の本（例えば [雪 13a], [雪 13b], [ノ 12]）で勉強する際の副読本として利用してもらえればと思います.

この文書ではどのような前提知識を課すか, ということについて述べておきます. この文書を**読み始める**ための前提知識は特に課しません. と言うより, 前提知識が無くても読み始めることはできるように気を付けて書いた, と言う方が正確です. 実際, この文書では方程式の整数解のような中高生にも親しみやすい概念から話を進めていきます. 一方で, この文書を**読み進める**ための前提知識は色々と必要なものがあります. というのも, 代数的整数論について証明抜きで紹介していく以上, そこで用いられる理論（群論, 環論, 体論, 線形代数などなど）の助けを借りた説明になってしまうのはどうしても避けられないからです. ですが, それらの知識をまず身に付けてからこの文書を読む（あるいは代数的整数論を勉強する）というのではなく, まずはこの文書を読み進めてみて, どこかで知識の壁を感じたら一旦知識を補填して, そしてまたこの文章に戻る（あるいは代数的整数論の勉強に戻る）という風にするのが効率も良く身に付きやすい勉強法なのではないかと思います.

[工事中]

謝辞

この文書の内容は 2021 年 5 月から筆者が主催したセミナーに基づきます. 庄司幸弘さん, 前畑佑都さん, 田中拓弥さんにはセミナーに参加し質問やコメントを頂きました. 特に前畑佑都さんには演習問題の作成に役立つ計算例を提示して頂きました. 小野雅隆さんには数学的な誤りを, 川村悟史さんには数学的な誤りと誤植をご指摘頂きました. ここに感謝いたします.

目次

はじめに 1

第 1 章 代数的整数論とは？ 3
1.1 代数的整数論の研究対象 3
1.2 代数的整数論の目的 4

第 2 章 代数体の整数環の動機 6
2.1 Fermat の最終定理（$n = 3$）と一意分解整域 6
2.2 Pell 方程式と単元 8
2.3 代数体の整数環の定義と例 11

第 3 章 イデアルと Dedekind 環の動機 13
3.1 Fermat の最終定理（$n = 23$）と Kummer のアイデア 13
3.2 素イデアルであることの確認法 17
3.3 素イデアル分解の計算例 19
3.4 素数の分岐 21

第 4 章 23
4.1 23
4.2 23

第 5 章 24
5.1 24
5.2 24

第 6 章 25
6.1 25
6.2 25

参考文献 26

第 1 章

代数的整数論とは？

1.1　代数的整数論の研究対象

代数的整数論とは何か？

この問いに答えるのが本章の目的です.

さっそく答えを言ってしまうと,

代数的整数論とは, **代数的整数**の理論である

というのが一つの答えです. では**代数的整数**とは何か？ 定義を見てみましょう.

定義 1.1.1

複素数 α が**代数的整数**であるとは, ある整数係数多項式 $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ が存在して $f(\alpha) = 0$ を満たすことを言う.

定義のポイントは $f(x)$ が x^n から始まる多項式であるところです. このような多項式を**モニック多項式**と呼びます. この用語を用いると, 代数的整数とは「整数係数モニック多項式の根」のことだと言い換えることができます.

演習問題 1.1

代数的整数論の本で代数的整数の定義を確認しましょう.

では, この代数的整数という概念について理解を深めるために例を見ていきましょう.

例 1.1.2

整数は代数的整数である. また $\sqrt{2}, \sqrt{-1}, e^{2\pi\sqrt{-1}/5}$ は代数的整数である.

演習問題 1.2

例 1.1.2 で挙げた代数的整数の例について, それを根に持つような整数係数モニック多項式を挙げましょう.

演習問題 1.3

例 1.1.2 で挙げた以外の代数的整数の例を挙げましょう.

さて, 以上のことをまとめると

代数的整数論とは, $\sqrt{2}$ や $\sqrt{-1}$ などの代数的整数を研究する理論である

と述べることができます.

となると, 代数的整数は研究するに値する対象なのか, どのような応用があるかということが気になる方もいると思います. 実は, 代数的整数は方程式の整数解を調べるのに役立ちます. 詳しいことは次章以降で説明しますが, 核となるアイデアを具体例に沿って述べると, 例えば $x^2-2y^2=1$ という方程式は $\left(x-\sqrt{2}y\right)\left(x+\sqrt{2}y\right)=1$ という風に言い換えることができるので, $\sqrt{2}$ という数の性質からこの方程式を調べることができるのです. このため, 代数的整数論の応用として種々の方程式の整数解を求めることができます. このことについてはこの文書の随所で様々な具体例を示します.

1.2 代数的整数論の目的

前節では「代数的整数論では代数的整数を調べる」という話をしました. とは言ったものの, 実際の代数的整数論ではそこまで代数的整数や方程式それ自体をガシガシ弄るわけではありません. 実際の代数的整数論の主目的は, **代数体の整数環**の**素イデアル**の**分解**や**分布**を調べることです. …… 専門用語が色々出てきました. これらの専門用語の説明は後の章に回すことにして, ここではなぜ実際の代数的整数論が代数的整数ではなくそのような難しそうな概念（実際, これらは代数的整数よりも抽象度の高い概念です）を調べるのかということを説明してみたいと思います.

実は, より抽象度の高い概念を追求するということは数学ではよくあることです. このことを Galois 理論を例にとって説明してみたいと思います（Galois 理論を勉強したことが無い方は, 以下の話はそういうものかと読み流してください）.

19 世紀の数学者 Galois によって見出された Galois 理論は,

方程式 $x^n+a_1x^{n-1}+\cdots+a_n=0$（ただし $a_i\in\mathbb{Q}$）
を調べる代わりに
体 $\mathbb{Q}(\alpha)$（ただし α は方程式 $x^n+a_1x^{n-1}+\cdots+a_n=0$ の解の 1 つ）やその **Galois 群**
を調べる！

というパラダイムシフト（視点の転換）を引き起こしました. つまり, 方程式を調べたければ, (数学的により洗練された対象である）体やその Galois 群を代わりに調べれば良い, という革命的な視点を提供したのです. この革命が当時の数学界に与えた反響が非常に大きかったことは想像に難くないですが, Galois 理論が定着するにつれ, いつしか興味は方程式から（より本質的な対象である）体へと移っていきました. Galois 理論の教科書に「これって方程式とどう関係するの？」と首をかしげたくなるような命題がつらつらと並んでいるのはそのためです.

実は, 代数的整数論でも Galois 理論と同じようなパラダイムシフトが起こっています. つまり

代数的整数（例えば $\sqrt{2}$）
を調べる代わりに
代数体の整数環（例えば $\mathbb{Z}[\sqrt{2}]$）やその**素イデアル**
を調べる！

という視点の切り替えがあったのです. これにより, いつしか興味は方程式の整数解から（より数学的に洗練されていて本質的な対象である）**代数体の整数環**やその**素イデアル**へと移りました. このような背景から代数的整数論では代数体の整数環や素イデアルといったより抽象的な概念を調べていて, そのために代数的整数論の教科書は内容が厳つくなってしまうのです. その一方で抽象度が高い概念を調べるがゆえに, 理論が美しく整然としているのもまた事実です.

第 2 章

代数体の整数環の動機

1.1 節の最後で

> 代数的整数は方程式の整数解を調べるのに役立ち, そのため代数的整数論の応用として種々の方程式の整数解を求めることができる

ということを述べました. 一方 1.2 節では

> 実際の代数的整数論で調べるのは代数体の整数環などのより抽象的な概念である

ということを述べました. これらのことを踏まえて, 本章では

> なぜ代数体の整数環を考えるのか？

という問いに答えたいと思います. 本章の目的は,

> 代数体の整数環を調べると嬉しいことが色々あるんだな, じゃあ一丁, 調べてやりますか

という気持ちになってもらうことです. そのためにまず 2.1 節で Fermat の最終定理, 2.2 節で Pell 方程式について考察して, 代数体の整数環というものを考えるとこれらの方程式の整数解を見通し良く決定できることを紹介します. その後 2.3 節で代数体の整数環の定義と例について見ていくことにします.

2.1 Fermat の最終定理（$n = 3$）と一意分解整域

本節では Fermat の最終定理の $n = 3$ の場合, つまり次の事実の見通しの良い証明について検討します.

定理 2.1.1

$x^3 + y^3 = z^3$ を満たす自然数の組 $(x, y, z) \in \mathbb{Z}_{>0}^3$ は存在しない.

ここでは [雪 13a, 系 8.7.6] の証明を念頭に置いて話を進めていきますが, 証明を読んでいなくて

も問題ありません.

証明の方針は解 $(x,y,z)\in\mathbb{Z}^3_{>0}$ が存在すると仮定して無限降下法で矛盾を導くというものですが, 実際に矛盾を導くための核となるアイデアは以下の通りです.

【アイデア】

まず $\gcd(x,y,z)=1$ として良いことに注意する. ここで $\zeta_3=(-1+\sqrt{-3})/2$ とおくと

$$z^3=x^3+y^3=(x+y)(x+\zeta_3 y)(x+\zeta_3^2 y)$$

と因数分解できる. このとき各 $i\in\{0,1,2\}$ に対し整数 $u_i,v_i\in\mathbb{Z}$ が存在して

$$x+\zeta_3^i y=(u_i+\zeta_3 v_i)^3$$

と書けるのではないか？

最後の推論がこのアイデアの核心的な部分で, これは次の整数の性質からの類推です.

補題 2.1.2

どの 2 つも互いに素な 3 つの自然数の積が立方数なら, それらは全て立方数である. すなわち, 自然数 $n_1,n_2,n_3,N\in\mathbb{Z}_{>0}$ が

$$\gcd(n_1,n_2)=\gcd(n_2,n_3)=\gcd(n_3,n_1)=1,\quad n_1n_2n_3=N^3$$

を満たすなら, 各 $i\in\{1,2,3\}$ に対し整数 $u_i\in\mathbb{Z}$ が存在して $n_i=u_i^3$ を満たす.

代数的整数論とは少し外れますが, 理解の助けにするために証明をつけておきます. 整数問題に自信のある方はぜひ自力での証明に挑戦してみてください.

証明. 各 $i\in\{1,2,3\}$ に対し $n_i=p_{i,1}^{e_{i,1}}\cdots p_{i,r_i}^{e_{i,r_i}}$ を素因数分解とすると, $\gcd(n_1,n_2)=\gcd(n_2,n_3)=\gcd(n_3,n_1)=1$ より

$$N^3=\left(p_{1,1}^{e_{1,1}}\cdots p_{1,r_1}^{e_{1,r_1}}\right)\left(p_{2,1}^{e_{2,1}}\cdots p_{2,r_2}^{e_{2,r_2}}\right)\left(p_{3,1}^{e_{3,1}}\cdots p_{3,r_3}^{e_{3,r_3}}\right)$$

は N^3 の素因数分解である. よって全ての $e_{i,j}$ は 3 の倍数なので, n_1,n_2,n_3 は全て立方数である. □

証明のポイントは整数が素因数分解できることにあります. そこで, 上に述べたアイデアを正当化させるには $x+y\zeta_3$（ただし $x,y\in\mathbb{Z}$）という数の体系に対して素因数分解を樹立する必要が出てきます. ここで

$$\mathbb{Z}[\zeta_3]:=\{x+y\zeta_3\mid x,y\in\mathbb{Z}\}$$

とおくと, これは足し算と掛け算で閉じており, **環**と呼ばれる数学的対象になっていることが分かります. このとき $\mathbb{Z}[\zeta_3]$ という数の体系に対する素因数分解は, 環論の用語を用いることで次のように定式化することができます.

定理 2.1.3: [雪 13a, 定理 8.6.1]

$\mathbb{Z}[\zeta_3]$ は**一意分解整域**である.

そしてこの性質を用いることで, 上で述べたアイデアを遂行して Fermat の最終定理の $n = 3$ の場合に証明を与えることができるのです.

以上の議論では,

方程式の代わりに**環**を調べる！

というパラダイムシフトが起こっています. そして実のところ, ここで登場した $\mathbb{Z}[\zeta_3]$ という環は代数体の整数環の例になっています.

以上が, 方程式の整数解の研究に代数体の整数環が役立つことの第一の例です.

演習問題 2.1

(i) $\alpha, \beta \in \mathbb{Z}[\zeta_3]$ に対し $\alpha\beta \in \mathbb{Z}[\zeta_3]$ を示せ.

(ii) 数学書で**環**の定義を確認し, $\mathbb{Z}[\zeta_3]$ が環をなすことを確認せよ.

2.2 Pell 方程式と単元

次に, 方程式の整数解の研究に代数体の整数環が役立つことの第二の例である Pell 方程式について述べたいと思います. Pell 方程式とは, 平方数でない $d \in \mathbb{Z}_{>0}$ に対する $x^2 - dy^2 = \pm 1$ という形の方程式を指します. ここでは $d = 2$ の場合を考察してみます.

$x^2 - 2y^2 = -1$ という方程式は, いくつか代入してみることで $(x, y) = (1, 1)$ という解を持つことが分かります. 同様に $x^2 - 2y^2 = 1$ という方程式は $(x, y) = (3, 2)$ という解を持つことが分かります. これらの他にはどのような解があるでしょうか？

実は, これらの解から新しい解を作ることができます. そのためには, 1.1 節の最後に少しだけ述べた

$$\pm 1 = x^2 - 2y^2 = \left(x - \sqrt{2}y\right)\left(x + \sqrt{2}y\right)$$

という因数分解を用いることで計算の見通しが立ちやすくなります. 例えば

$$-1 = (-1)^3 = \left(1 - \sqrt{2}\right)^3 \left(1 + \sqrt{2}\right)^3 = \left(11 - 5\sqrt{2}\right)\left(11 + \sqrt{2}\right),$$
$$1 = 1^2 = \left(3 - 2\sqrt{2}\right)^2 \left(3 + 2\sqrt{2}\right)^2 = \left(17 - 12\sqrt{2}\right)\left(17 + 12\sqrt{2}\right),$$

と計算できるので, $x^2 - 2y^2 = -1$ の解として $(x, y) = (11, 5)$ が, $x^2 - 2y^2 = 1$ の解として $(x, y) = (17, 12)$ があることが分かります. ここで

$$1 = (-1)^2 = \left(\left(1 - \sqrt{2}\right)\left(1 + \sqrt{2}\right)\right)^2 = \left(3 - 2\sqrt{2}\right)\left(3 + 2\sqrt{2}\right)$$

であることに注意すると, 結局 $\left(1 + \sqrt{2}\right)^n$ を計算することにより, n が奇数の時は $x^2 - 2y^2 = -1$

の解が, n が偶数の時は $x^2-2y^2=1$ の解が得られることが分かります. 以上の計算はもちろん $\sqrt{2}$ を出さずに行うこともできますが, $\sqrt{2}$ を出した方が見通しが良いように思います.

さて, ここで

$$\left(1+\sqrt{2}\right)^n \text{ を計算することで方程式 } x^2-dy^2=\pm 1 \text{ の}\textbf{全ての}\text{解を得られるか？}$$

という疑問が浮かび上がりますが, 答えは「YES」です. 実際, 次の定理が成り立ちます.

定理 2.2.1

方程式 $x^2-2y^2=1$, $x^2-2y^2=-1$ の解全体の集合はそれぞれ

$$\left\{(x,y)\in\mathbb{Z}^2 \;\middle|\; x+\sqrt{2}y=\pm\left(1+\sqrt{2}\right)^n, n\in\mathbb{Z} \text{ は偶数}\right\},$$
$$\left\{(x,y)\in\mathbb{Z}^2 \;\middle|\; x+\sqrt{2}y=\pm\left(1+\sqrt{2}\right)^n, n\in\mathbb{Z} \text{ は奇数}\right\}$$

と表される.

この定理は次のように一般化されます.

定理 2.2.2

平方数でない $d\in\mathbb{Z}_{>0}$ に対し, 方程式 $x^2-dy^2=\pm 1$ の解全体の集合はある整数の組 (x_0,y_0) を用いて

$$\left\{(x,y)\in\mathbb{Z}^2 \;\middle|\; x+\sqrt{d}y=\pm\left(x_0+\sqrt{d}y_0\right)^n, n\in\mathbb{Z}\right\}$$

と表される.

注意 2.2.3

平方数でない $d\in\mathbb{Z}_{>0}$ に対し, 一般には方程式 $x^2-dy^2=-1$ には解が無いことがあるため, **定理 2.2.2** では**定理 2.2.1** とは少し異なる書き方をした. なお, 方程式 $x^2-dy^2=1$ には常に無限個の解が存在する.

では, これらの定理はどのように示されるのでしょうか. **定理 2.2.1** は初等的に示すことができるのですが, **定理 2.2.2** の証明は難しいです（これは $\mathbb{Z}[\sqrt{2}]$ が単項イデアル整域（より強く Euclid 整域）であることと, 一般に $\mathbb{Z}[\sqrt{d}]$ は単項イデアル整域とは限らないことの現れです）. 証明のためにどのようにアプローチするかというと, ここでも方程式 $x^2-dy^2=\pm 1$ の代わりに**環** $\mathbb{Z}[\sqrt{d}]$ を考察するのです. そして, $\mathbb{Z}[\sqrt{d}]$ は $d\equiv 2,3$ のときには**代数体の整数環**という対象になっているのです（$d\equiv 1$ の場合は代数体の整数環より少し広いクラスである代数体の整環と呼ばれるものになっていて, 代数体の整数環と並行した議論がある程度できます）.

それでは, Pell 方程式を環の言葉で翻訳してみましょう. 以下では平方数でない $d\in\mathbb{Z}_{>0}$ を固定

して議論することにします. まずノルム写像を

$$\begin{array}{rccc} N\colon & \mathbb{Z}[\sqrt{d}] & \longrightarrow & \mathbb{Z} \\ & x+\sqrt{d}y & \longmapsto & \left(x-\sqrt{d}y\right)\left(x+\sqrt{d}y\right) \end{array}$$

によって定めます. このとき

$$\begin{array}{ccc} \{(x,y)\in\mathbb{Z}^2 \mid x^2-dy^2=\pm 1\} & \longrightarrow & \{\alpha\in\mathbb{Z}[\sqrt{d}] \mid N(\alpha)=\pm 1\} \\ (x,y) & \longmapsto & x+\sqrt{d}y \end{array}$$

は全単射であることがノルム写像の定義から従います. このようにして Pell 方程式の解集合を環 $\mathbb{Z}[\sqrt{d}]$ とノルム写像の言葉で翻訳することができました.

ここからは環サイドから考察していくことにしましょう. まず, 代数的整数論の基礎事項から次の事実を示すことができます.

補題 2.2.4

$$\{\alpha\in\mathbb{Z}[\sqrt{d}] \mid N(\alpha)=\pm 1\}=\mathbb{Z}[\sqrt{d}]^\times.$$

ここで $\mathbb{Z}[\sqrt{d}]^\times$ は環 $\mathbb{Z}[\sqrt{d}]$ の単元全体のなす集合を表します. このようにして, Pell 方程式の解集合を環 $\mathbb{Z}[\sqrt{d}]$ の単元という理論的により洗練された対象で置き換えることができました.

演習問題 2.2

環の単元の定義を, 何も見ずノートに書けるようになりましょう.

次に, **Dirichlet の単数定理**という代数的整数論の偉大な結果から次が従います.

定理 2.2.5

ある単数 $\varepsilon_0\in\mathbb{Z}[\sqrt{d}]^\times$ が存在して

$$\mathbb{Z}[\sqrt{d}]^\times=\{\pm\varepsilon_0^n \mid n\in\mathbb{Z}\}$$

が成り立つ.

以上の事実から**定理 2.2.2** が従います.

演習問題 2.3

上で述べた事実の帰結として**定理 2.2.2** が得られることを示しましょう.

ここでの議論は

- まず Pell 方程式を環論的に言い換え,
- 次に代数的整数論の力を使って環を調べる

と要約することができます. ポイントは, 方程式の代わりに代数体の整数環（と整環）というより洗練された対象を考察するという部分です. 2.1 節と同様, 方程式の整数解の研究に代数体の整数環が役立つことを見て取ることができました.

演習問題 2.4

Pell 方程式 $x^2 - 3y^2 = \pm 1, x^2 - 27dy^2 = \pm 1$ の解を調べるにはそれぞれどのような環を調べることが有効か述べましょう.

2.3 代数体の整数環の定義と例

2.1, 2.2 節では代数体の整数環を研究することで嬉しいこと（方程式の整数解について理解できること）があると述べました. ですがまだ代数体の整数環の定義を述べていませんでしたので, ここで述べたいと思います.

まず代数体の定義を与えます.

定義 2.3.1

代数体とは $\mathbb{Q}$ の有限次拡大体（となる $\mathbb{C}$ の部分体）のことである.

例 2.3.2

$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(e^{2\pi\sqrt{-1}/5})$ は代数体である.

演習問題 2.5

例 2.3.2 で述べた以外の代数体の例を挙げよ.

次に代数体の整数環の定義を述べます.

定義 2.3.3

代数体 K の整数環 $\mathcal{O}_K$ を

$$\mathcal{O}_K := \{\alpha \in K : \text{代数的整数}\}$$

と定義する.

例 2.3.4

代数体 $\mathbb{Q}(\sqrt{2})$ の整数環は $\mathbb{Z}[\sqrt{2}]$ である. また代数体 $\mathbb{Q}(\sqrt{-3})$ の整数環は $\mathbb{Z}[\sqrt{-3}]$ ではなく $\mathbb{Z}[(-1+\sqrt{-3})/2]$ である. しかしこれらの事実を証明するには, 代数体の全ての元に対しそれが代数的整数かどうか判定する必要があるので少々努力を要する.

つまり代数体 K の整数環とは, K の元のうち代数的整数であるものを取れるだけとってきたものだということができます.

注意 2.3.5

$\mathcal{O}$（カリグラフィーの O）とは不思議な記号だが, 実はこの記号は複素多様体論で正則関数のなす環を表すのに用いられ, その記号法はここで述べた代数体の整数環の記号と整合性があることをスキーム論の観点から理解することができる.

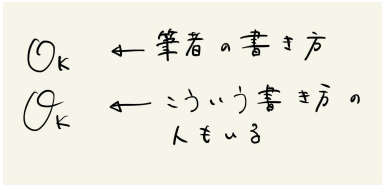

図 2.1: 手書きの $\mathcal{O}_K$

第 3 章

イデアルと Dedekind 環の動機

前章では, 方程式の整数解を調べるには代数体の整数環を調べることが有効であるということを述べました. しかしながら, 様々な種類の方程式の整数解を調べるためには一筋縄ではいかず, 代数体の整数環のより深い性質を理解することが必要になってきます.

本章では, 3.1 で一筋縄ではいかない方程式の例として $n = 23$ の場合の Fermat の最終定理を紹介したのち, それを攻略するための Kummer の革命的な 3 つのアイデアについて説明します. Kummer のアイデアの主要部の一つに**素イデアル分解**というものがあるのですが, 3.3 節ではこの素イデアル分解について例と演習問題を通じて計算法を習得してもらいます. 3.4 節では, 3.3 節でみた素イデアル分解の様子に「分岐」や「不分岐」などの名前が付けられていることを紹介します.

3.1 Fermat の最終定理（$n = 23$）と Kummer のアイデア

本節では, 2 章で述べたやり方では攻略できないような方程式の例である Fermat の最終定理の $n = 23$ の場合と, Kummer による攻略法について紹介します. なお, 以下で述べる証明の方針は [雪 13a, 定理 8.11.15] に基づきます.

まず, Fermat 方程式が自明解しか持たないことを示すには n が 4 か素数の場合に考えれば十分であることに注意します. $n = 4$ の場合は初等的に証明できるので, n が 3 以上の素数 p の場合に議論すれば十分です.

さて, 2.1 節では, Fermat 方程式 $x^p + y^p = z^p$ に対して $p = 3$ の場合に解を調べるために環 $\mathbb{Z}[\zeta_3]$ が一意分解整域であることを用いた議論をしました. となると他の素数 p ではどうなるか気になるところです. 実は, この議論は $p \leq 22$ では機能するものの $p = 23$ では機能しなくなります. このようなことが起こるのは $\zeta_{23} := e^{2\pi\sqrt{-1}/23}$ とおくとき環 $\mathbb{Z}[\zeta_{23}]$ が一意分解整域でないためです. では, 環 $\mathbb{Z}[\zeta_p]$ が一意分解整域でないときに Fermat 方程式 $x^p + y^p = z^p$ にアタックするにはどうすれば良いのでしょうか. Kummer は次の攻略法を考えました.

(i) 環 $\mathbb{Z}[\zeta_p]$ において, 数より細かい分解である**素イデアル分解**を考える.

(ii) イデアルのなす**イデアル類群**の位数が p で割れるときに, 群論的な操作から $p = 3$ の場合と同様の議論が回ることを示す.

(iii) (ii) の条件がいつ成り立つかの判定法を与え, $p = 23$ のときにはその条件が満たされることを示す.

この攻略法について順を追って解説していきます.

3.1.1 (i) について

まず (i) について, $\mathbb{Z}[\zeta_{23}]$ より簡単な一意分解整域でない環である $\mathbb{Z}[\sqrt{-5}]$ を例にとって説明してみます.

一意分解整域でない環では,「素因数分解」はできるかもしれませんが「素因数分解の一意性」は成り立ちません. 例えば, 環 $\mathbb{Z}[\sqrt{-5}]$ において

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{3.1.1}$$

という等式が成り立ちますが, ここで $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ はどの二つも同伴でない素元です. つまり, 環 $\mathbb{Z}[\sqrt{-5}]$ において数 6 は $2 \cdot 3$ と $(1 + \sqrt{-5})(1 - \sqrt{-5})$ という二通りの「素因数分解」を持ってしまうのです. そこでどうするかというと, Kummer は

幾通りにも分解できるなら, もっと分解してしまえ！

というアイデアを提起しました. この発想は, 物理学でかつて物質の基本単位と考えられていた原子について, より深い現象に説明を付けるために原子を更に電子・陽子・中性子という構成要素に分解したことに似ているかもしれません.

Kummer は式 (3.1.1) において

$$6 = I_1 I_2 I_3 I_4, \quad I_1 I_2 = 2, \quad I_3 I_4 = 3, \quad I_1 I_3 = 1 + \sqrt{-5}, \quad I_2 I_4 = 1 - \sqrt{-5}$$

を満たすような**理想数 (ideal number)** I_1, I_2, I_3, I_4 があると考えたのです. すると, 式 (3.1.1) の分解は実際には $6 = I_1 I_2 I_3 I_4$ というただ一つの分解が二通りに顕現していたのだとみなすことができるのです.

すると次は, この「理想数」を数学的にどのように定式化するかということが問題になります. Kummer 流の定式化がどのようなものだったのか筆者は知らないのですが, 実際のところ「理想数」は「最大公約数の拡張概念」だと考えることができます. 例えば

- I_1 は 2 と $1 + \sqrt{-5}$ の「最大公約数」,
- I_2 は 2 と $1 - \sqrt{-5}$ の「最大公約数」,
- I_3 は 3 と $1 + \sqrt{-5}$ の「最大公約数」,
- I_4 は 3 と $1 - \sqrt{-5}$ の「最大公約数」

と考えるのです. この「最大公約数の拡張概念」は現代的な用語を使えば「環 $\mathbb{Z}[\sqrt{-5}]$ の部分 $\mathbb{Z}[\sqrt{-5}]$ 加群」がまさにそれになっていることが分かり, Kummer の発見にちなんで「**イデアル (ideal)**」という名前が付けられています. 整数 a, b の最大公約数を (a, b) と表すことがあります

が, それに倣って上のイデアルたちは

$$I_1 = (2, 1+\sqrt{-5}), \quad I_2 = (2, 1-\sqrt{-5}), \quad I_3 = (3, 1+\sqrt{-5}), \quad I_4 = (3, 1-\sqrt{-5})$$

という記号で表されます. また, 上の分解は

$$\text{イデアル } 6\mathbb{Z}[\sqrt{-5}] \text{ の}\textbf{素イデアル分解}\ 6\mathbb{Z}[\sqrt{-5}] = I_1 I_2 I_3 I_4$$

という形で数学的な定式化がなされています. この素イデアル分解については次節で詳しく説明することにします.

演習問題 3.1

(i) $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ が $\mathbb{Z}[\sqrt{-5}]$ の素元であることを示しましょう.
(ii) 数学書で「同伴」の定義を確認しましょう.
(iii) $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$ を示しましょう.
(iv) 数学書で「一意分解整域」の定義を確認しましょう.
(v) 式 (3.1.1) から, 環 $\mathbb{Z}[\sqrt{-5}]$ が一意分解整域でないことを示しましょう.

演習問題 3.2

(i) $1 \pm \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ を示しましょう.
(ii) 等式

$$4 = 2^2 = (2\sqrt{2}+2)(2\sqrt{2}-2)$$

は環 $\mathbb{Z}[\sqrt{2}]$ が一意分解整域であるという事実と矛盾しないことに, 納得できる説明を付けましょう.

演習問題 3.3

(i) 等式

$$4 = 2^2 = (1+\sqrt{-3})(1-\sqrt{-3})$$

を用いて, 環 $\mathbb{Z}[\sqrt{-3}]$ が一意分解整域でないことを示しましょう.
(ii) 数学書で「一意分解整域は整閉整域である」という命題の証明を追いましょう.
(iii) 環 $\mathbb{Z}[\sqrt{-3}]$ の整閉包が $\mathbb{Z}[(-1+\sqrt{-3})/2]$ であることを示し, 環 $\mathbb{Z}[\sqrt{-3}]$ が一意分解整域でないことを帰結しましょう.

演習問題 3.4

環 $\mathbb{Z}[\sqrt{-5}]$ において, イデアルの等式 $(2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5})$ が成り立つことを示しましょう.

3.1.2 (ii) について

次に (ii) について説明します. (i) のアイデアだけで十分驚嘆に値しますが, Kummer はここから更に歩みを進めました.

一意分解整域とは限らない環 $\mathbb{Z}[\zeta_p]$ に対し, イデアルの「類」からなる「**イデアル類群** $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$」というものを考察することで Fermat 方程式 $x^p + y^p = z^p$ にアタックしようと考えたのです（なお, イデアル類群それ自体は Kummer 以前に Gauss によって二次体の整数環の場合に研究されていました）.

イデアルは通常の数よりも細かい分解ができることが大きな特長ですが, 一方で数ではない（実際, 数学的には加群として定式化されていました）ので方程式への翻訳が難しいという問題点があります. 一方でイデアルの中でも「**単項イデアル**」と呼ばれるものは数に近い性質を持ち, 方程式への翻訳も行いやすい概念です. 実はイデアル類群の単位元がこの単項イデアル全体のなす集合になっているので, あるイデアルがイデアル類群で 1 になるということはそのイデアルが単項であることを意味し, 従って方程式の言葉に翻訳できるということが分かるのです.

Kummer は環 $\mathbb{Z}[\zeta_p]$ のイデアル類群 $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ に対し次の群論における補題を適用しました（Kummer の時代にはまだ群論は整備されていなかったと思われるので, 正確に述べると「Kummer のアイデアでは本質的に以下の群論の補題を用いている」となります）.

補題 3.1.1

有限群 G と素数 p に対し, p が G の位数を割らないなら G の位数 p の元は存在しない. すなわち, $g \in G$ が $g^p = 1$ を満たすなら $g = 1$ が成り立つ.

2.1 節で紹介した, 環 $\mathbb{Z}[\zeta_3]$ を用いて Fermat 方程式 $x^3 + y^3 = z^3$ を調べたことと同様の議論をイデアルに対して行うことで, Fermat 方程式 $x^p + y^p = z^p$ に対し I^p が単項イデアルになるようなイデアル I を構成できます. I^p が群 $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ の中で 1 となることを意味するので, もし p **がイデアル類群** $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ **の位数を割らない**なら**補題 3.1.1** から I は群 $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ の中で 1 に等しい, すなわち単項イデアルであることが従います. ここから単項イデアルは方程式への翻訳が行いやすいことを利用して, Fermat 方程式 $x^p + y^p = z^p$ は自明な解しか持たないことを示すことができるのです.

ここで登場した

$$p \text{ がイデアル類群 } \mathrm{Cl}(\mathbb{Z}[\zeta_p]) \text{ の位数を割らない}$$

という条件を見たす素数には**正則素数**という名前が付けられています. 以上の議論から, 結局 Kummer は次を示したことになります.

定理 3.1.2: Kummer

p が正則素数なら Fermat 方程式 $x^p + y^p = z^p$ の解は $xyz = 0$ を満たす.

演習問題 3.5

補題 3.1.1 の証明を与えましょう.

3.1.3 (iii) について

(ii) では正則素数 p に対しては Fermat の最終定理が解決されることを見ました. 次の問題はいつ p が正則素数になるかということです. 特に 23 が正則素数であることが分かれば, $p = 23$ の場合に Fermat の最終定理が解決したことになります.

実は, Kummer は正則素数の判定法も与えています. その抜かりなさには畏敬の念すら覚えます.

Kummer は Bernoulli 数という数列を用いた正則素数の判定法を与えました. Bernoulli 数は Riemann ゼータ関数の正の偶数点での値に現れる数列です. ここで Kummer の判定法の詳細は述べませんが, 例えば Kummer の判定法によると

$$\zeta(12) = \sum_{n=1}^{\infty} \frac{1}{n^{12}} = \frac{691}{638512875}\pi^{12}$$

という等式から 691 が正則素数**ではない**ことが従います.

3.2 素イデアルであることの確認法

これから代数体の整数環における素イデアル分解の計算について紹介しますが, その準備段階としてまずはイデアルが素イデアルであるかどうかの確認のやり方について述べたいと思います. 計算のために必要となるので, 本節以降では環準同型定理までの環論の知識は仮定することにします.

イデアルが素イデアルであるかどうかを確認するには, 次の環論の命題を使います.

命題 3.2.1

環 A のイデアル I に対し以下が成り立つ.

(i) I が素イデアルであることは A/I が整域であることと同値である.
(ii) I が極大イデアルであることは A/I が体であることと同値である.

環論では素イデアルと極大イデアルは明確に区別されますが, 代数的整数論では**素イデアルと言ったら極大イデアルのこと**を指します. これはややこしい用語法ですが, 歴史的な事情があることと, 次の命題が成り立つことから正当化されます.

命題 3.2.2

代数体の部分環において, 0 でない素イデアルは極大イデアルである.

注意 3.2.3

可換環論の用語を使うと, **命題 3.2.2** における「0 でない素イデアルは極大イデアルである」という条件は「Krull 次元が 1 である」と言い換えることができる.

この文書でも, 代数体の部分環において素イデアルと言ったら極大イデアル（つまり 0 でない素イデアル）のことを指すことにします.

代数的整数論における「素イデアル」の用法

代数的整数論で極大イデアルを素イデアルと呼ぶのは, 環論に親しんだ身からすると座りが悪い用法に思われます. 一方で素イデアルは素数の拡張概念だという立場からすると自然な用法に思われます. また「素因数分解」の拡張である「素イデアル分解」を「極大イデアル分解」と呼ぶのもまた気持ちが良くない気がします.

歴史的な順序がどうだったのか筆者は知らないのですが, このような状況は, かつて「ケータイ」と呼んでいたものがスマホの登場とともに「ガラケー」と呼ばれるようになったことに似ているかもしれません（このような単語をレトロニムと呼びます）.

それでは, 実際に素イデアルかどうかを判定してみましょう.

命題 3.2.4

環 $\mathbb{Z}[\sqrt{-5}]$ のイデアル $I = (2, 1+\sqrt{-5})$ は素イデアルである.

証明. 環の同型

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{-5}] & \xrightarrow{\sim} & \mathbb{Z}[t]/(t^2+5) \\ x+y\sqrt{-5} & \longmapsto & \overline{x+yt} \end{array}$$

において I は $\mathbb{Z}[t]/(t^2+5)$ のイデアル $(2, 1+t, t^2+5)/(t^2+5)$ に対応するので

$$\mathbb{Z}[\sqrt{-5}]/I \cong \frac{\mathbb{Z}[t]/(t^2+5)\mathbb{Z}[t]}{(2,1+t,t^2+5)/(t^2+5)\mathbb{Z}[t]} \cong \mathbb{Z}[t]/(2,1+t,t^2+5)$$

が成り立つ. ここで $t^2+5 = (t+1)^2 + 2(-t+2)$ より, $\mathbb{Z}[t]$ のイデアルとして $(2,1+t,t^2+5) = (2,1+t)$ なので

$$\mathbb{Z}[\sqrt{-5}]/I \cong \mathbb{Z}[t]/(2,1+t) \cong \frac{\mathbb{Z}[t]/2\mathbb{Z}[t]}{(2,1+t)/2\mathbb{Z}[t]} \cong \mathbb{F}_2[t]/(1+t) \cong \mathbb{F}_2$$

を得る. これは体なので**命題 3.2.1** より I は素イデアルである. □

注意 3.2.5

上の証明において, $\mathbb{Z}[t]$ のイデアルを (t^2+5) と表したり $(t^2+5)\mathbb{Z}[t]$ と表したりしましたが, これらは同じイデアルを指します. 前者は記号が簡単で, 後者はどの環のイデアルなのかが分かりやすい記法です. 後者の記法はイデアルが $\mathbb{Z}[t]$ 加群であることを強調した書き方であると述べることもできます.

上の議論のアイデアは以下のようにまとめられます.

【アイデア】

環の同型

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{-5}] & \xrightarrow{\sim} & \mathbb{Z}[t]/(t^2+5) \\ x+y\sqrt{-5} & \longmapsto & \overline{x+yt} \end{array}$$

におけるイデアルの対応を見る.

演習問題 3.6

環 $\mathbb{Z}[\sqrt{-5}]$ において, 以下のイデアルが素イデアルであることを示しましょう.

(i) $(3, 1+\sqrt{-5})$.
(ii) $(\sqrt{-5})$.（ヒント：$\mathbb{Z}[t]$ のイデアルの等式 $(t, t^2+5) = (t, 5)$ を使います.）
(iii) (11).（ヒント：t^2+5 が $\mathbb{F}_{11}[t]$ の既約多項式であることを示します.）

演習問題 3.7

(i) 環 $\mathbb{Z}[\sqrt{2}]$ においてイデアル $(\sqrt{2}), (3), (3+\sqrt{2})$ が素イデアルであることを示しましょう.
(ii) 環 $\mathbb{Z}[\sqrt{2}]$ においてイデアル $(3+2\sqrt{2})$ が素イデアルでないことを示しましょう（ヒント：$1+\sqrt{2}$ は単元です）.

演習問題 3.8

環 $\mathbb{Z}[(-1+\sqrt{-3})/2]$ においてイデアル $(2), (\sqrt{-3}), ((5+\sqrt{-3})/2)$ が素イデアルであることを示しましょう.

3.3 素イデアル分解の計算例

それではいよいよ素イデアル分解の計算をやってみましょう. ポイントは前節で登場した環同型 $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[t]/(t^2+5)$ と**中国剰余定理**です.

演習問題 3.9

数学書で中国剰余定理の主張を確認しましょう.

それでは計算してみます.

命題 3.3.1

環 $\mathbb{Z}[\sqrt{-5}]$ のイデアルの等式 $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$ が成り立つ.

証明.

$$\mathbb{Z}[\sqrt{-5}]/(3) \cong \frac{\mathbb{Z}[t]/(t^2+5)\mathbb{Z}[t]}{(3,t^2+5)/(t^2+5)\mathbb{Z}[t]} \cong \mathbb{Z}[t]/(3,t^2+5)$$

が成り立つ. ここで $t^2+5=(t+1)(t-1)+2\cdot 3$ より, $\mathbb{Z}[t]$ のイデアルとして $(3,t^2+5)=(3,(t+1)(t-1))$ なので

$$\mathbb{Z}[\sqrt{-5}]/(3) \cong \mathbb{Z}[t]/(3,(t+1)(t-1)) \cong \frac{\mathbb{Z}[t]/3\mathbb{Z}[t]}{(3,(t+1)(t-1))/2\mathbb{Z}[t]} \cong \mathbb{F}_3[t]/(t+1)(t-1)$$

を得る. 中国剰余定理より

$$\mathbb{Z}[\sqrt{-5}]/(3) \cong \mathbb{F}_3[t]/(t+1)\times\mathbb{F}_3[t]/(t-1)$$

が成り立つ. 上の計算を逆に辿ることで環同型

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{-5}]/(3) & \xrightarrow{\sim} & \mathbb{Z}[\sqrt{-5}]/(3,1+\sqrt{-5})\times\mathbb{Z}[\sqrt{-5}]/(3,1-\sqrt{-5}) \\ \alpha & \longmapsto & (\overline{\alpha},\overline{\alpha}) \end{array}$$

を得る. 等式 $3-(1+\sqrt{-5})-(1-\sqrt{-5})=1$ よりイデアル $(3,1+\sqrt{-5})$ と $(3,1-\sqrt{-5})$ は互いに素なので, 中国剰余定理より環同型

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{-5}]/(3) & \xrightarrow{\sim} & \mathbb{Z}[\sqrt{-5}]/(3,1+\sqrt{-5})(3,1-\sqrt{-5}) \\ \alpha & \longmapsto & \overline{\alpha} \end{array}$$

を得る. この同型写像からイデアルの等式 $(3)=(3,1+\sqrt{-5})(3,1-\sqrt{-5})$ が従う. □

演習問題 3.10

環 $\mathbb{Z}[\sqrt{-5}]$ において, イデアルの等式 $(2)=(2,1+\sqrt{-5})^2$ を示しましょう.

演習問題 3.11

環 $\mathbb{Z}[\sqrt{-10}]$ において, イデアルの等式 $(7)=(7,2+\sqrt{-10})(7,2-\sqrt{-10})$ を示しましょう.

演習問題 3.12

環 $\mathbb{Z}[\sqrt{-5}]$ において, イデアル $(5),(7),(11)$ を素イデアル分解しましょう.

演習問題 3.13

環 $\mathbb{Z}[\sqrt{-10}]$ において, イデアル (13) を素イデアル分解しましょう.

演習問題 3.14

環 $\mathbb{Z}[\sqrt{2}]$ において, $1+\sqrt{2}$ が単元であることに注意しながら以下の問いに答えましょう.

(i) 素数 $2,3,5,7$ を素元分解しましょう.
(ii) イデアル $(2),(3),(5),(7)$ を素イデアル分解しましょう.

演習問題 3.15

環 $\mathbb{Z}[(-1+\sqrt{-3})/2]$ において, イデアル $(2),(3),(5),(7)$ を素イデアル分解しましょう.

演習問題 3.16

(i) 環 $\mathbb{Z}[\sqrt{-3}]$ において, イデアル $(3),(5),(7)$ を素イデアル分解しましょう.

(ii) 環 $\mathbb{Z}[\sqrt{-3}]$ において, イデアルの等式 $(2,1+\sqrt{-3})^2 = (2)(2,1+\sqrt{-3})$ を示しましょう.

(iii) 環 $\mathbb{Z}[\sqrt{-3}]$ が Dedekind 環でないことを示しましょう.

3.4 素数の分岐

前節では, 素数 p に対して代数体の整数環のイデアル (p) がどのように素イデアル分解するかについて, 色々な現象を垣間見ることができました. それらの現象には以下のように名前が付けられています.

定義 3.4.1

- 素数 p.
- 代数体 K,
- K の整数環 $\mathcal{O}_K$
- K の拡大次数 $n := [K:\mathbb{Q}]$

に対し以下の用語を定義する.

(i) 素数 p が K で**分岐**するとは, $\mathcal{O}_K$ の相異なる素イデアル $\mathfrak{p}_1,\dots,\mathfrak{p}_g$ と整数 $e_1,\dots.e_g$ によって $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$ と素イデアル分解されるとき, ある番号 $1 \le i \le g$ が存在して $e_i \ge 2$ が成り立つことを言う.

(ii) 素数 p が K で**完全分岐**するとは, $\mathcal{O}_K$ の素イデアル $\mathfrak{p}$ によって $p\mathcal{O}_K = \mathfrak{p}^n$ と素イデアル分解されることを言う.

(iii) 素数 p が K で**不分岐**であるとは, 分岐しないことを言う. すなわち, $\mathcal{O}_K$ の相異なる素イデアル $\mathfrak{p}_1,\dots,\mathfrak{p}_g$ によって $p\mathcal{O}_K = \mathfrak{p}_1\cdots\mathfrak{p}_g$ と素イデアル分解されることを言う.

(iv) 素数 p が K で**完全分解**するとは, $\mathcal{O}_K$ の相異なる素イデアル $\mathfrak{p}_1,\dots,\mathfrak{p}_n$ によって $p\mathcal{O}_K = \mathfrak{p}_1\cdots\mathfrak{p}_n$ と素イデアル分解されることを言う.

(v) 素数 p が K で**惰性**するとは, $p\mathcal{O}_K$ が $\mathcal{O}_K$ の素イデアルであることを言う.

注意 3.4.2

完全分岐は分岐の特別な場合であり、完全分解と惰性は不分岐の特別な場合である.

例 3.4.3

代数体 $\mathbb{Q}(\sqrt{-5})$ において $2, 5$ は完全分岐し, $3, 7$ は完全分解し, 11 は惰性する.

演習問題 3.17

代数体 $\mathbb{Q}(\sqrt{-10})$ において素数 $2, 3, 5, 7, 11, 13$ が分岐, 完全分岐, 不分岐, 完全分解, 惰性のどれにあたるか判定せよ.

注意 3.4.4

「分岐」という一見すると奇妙に思われる用語は, 恐らく Riemann 面の理論に由来する. これは安直には, 例えば素イデアル分解 $p\mathcal{O}_K = \mathfrak{p}^2$ を, 分枝を持つ複素関数 $\sqrt{z}$ の類似物とみなすことよる.「分岐」という用語に限らず, 代数的整数論と Riemann 面の理論には様々なアナロジーが成り立っており, それらはスキーム論によって統一される.

第 4 章

4.1

4.2

第 5 章

5.1

5.2

第 6 章

6.1

6.2

参考文献

[ノ 12] ノイキルヒ. 代数的整数論. 丸善出版, 7 2012.

[雪 13a] 雪江明彦. 整数論 1: 初等整数論から p 進数へ. 日本評論社, 8 2013.

[雪 13b] 雪江明彦. 整数論 2: 代数的整数論の基礎. 日本評論社, 10 2013.