代数的整数論の道案内

村上友哉

2021 年 5 月 15 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], [J.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。セミナーに参加し質問やコメントを下さった庄司幸弘さん、前畑佑都さん、田中拓弥さんに感謝いたします。

目次

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 $x^n + a_1 x^{n-1} + \cdots + a_n = 0$（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 $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ 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

$x^3 + y^3 = z^3$ の整数解は $(x, y, z) = (0, 0, 0)$ のみである.

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 $(x,y,z) \neq (0,0,0)$ 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 $\omega=(-1+\sqrt{-3})/2$ とおくと

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

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

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

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 $x+y\omega$（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

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

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 $\mathbb{Z}[\omega]$ 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]

$\mathbb{Z}[\omega]$ 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 $\mathbb{Z}[\omega]$ 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) $\alpha, \beta \in \mathbb{Z}[\omega]$ に対し $\alpha\beta \in \mathbb{Z}[\omega]$ を示せ。

(ii) 数学書で**環**の定義を確認し、$\mathbb{Z}[\omega]$ 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 2.3.4 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、$\omega = (-1 + \sqrt{-3})/2$ とおくとき代数体 $\mathbb{Q}(\omega)$ の整数環は $\mathbb{Z}[\sqrt{3}]$ ではなく $\mathbb{Z}[\omega]$ 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。環論の用語を使うと、代数体の整数環とは代数的整数のなす整閉整域だと換言することもできます。

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も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がスキーム論の観点から理解することができる。

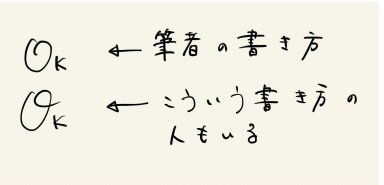

図 2.1: 手書きの $\mathcal{O}_K$

第 3 章

イデアルと Dedekind 環の動機

3.1 Fermat の最終定理（$n = 23$）

3.2 Kummer のアイデア：イデアルの分解と類数

3.3 Dedekind 環のこころ

3.4 素イデアル分解の計算例

第 4 章

4.1

4.2

第 5 章

5.1

5.2

参考文献

[J.12] ノイキルヒ J. 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.