研究レポート

3乗根を基底に持つ環の整数論

津山工業高等専門学校3年

一柳　浩輔

実験期間・データ収集機関　2021年4月～2021年9月

１．研究の目的と動機

整数全体の集合Zの素数について興味をもっていた。当然、素数は古くから研究されている。しかし、現在はリーマン・ゼータ関数などを用いた非常に難解な研究などが行われているようで、現在の自分の実力ではこのような研究は難しいと感じていた。そこで、部活動である数学クラブの担当をされている先生から拡張された整数について研究してみないかという提案があり研究が始まった。そして、$1, \sqrt[3]{2}, \sqrt[3]{4}$という３つの基底をもつ環

$$Z[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in Z\}$$

の素数を探索する研究に着手した。この研究をきっかけに、将来的にはn個の基底をもつ環の整数論へ拡張した一般理論を作ることを目指している。ここで、環とは足し算、引き算、掛け算が定義された集合のことである。

２．環$Z[\sqrt[3]{2}]$の素数を研究するということ

環$Z[\sqrt[3]{2}]$の整数$\eta = a + b\sqrt[3]{2} + c\sqrt[3]{4}$を考える。このとき、$\eta = \pm 1,\ \pm(1 - \sqrt[3]{2}),\ \pm(1 + \sqrt[3]{2} + \sqrt[3]{4})$などは、それぞれ逆数をもつ。代数学の環論において逆数をもつ数は単元と呼ばれる。さて、ηが素数であるとは、ηを割る$Z[\sqrt[3]{2}]$の整数ξがあったとき、すなわち$\xi|\eta$のとき、ξは単元またはη自身であるあるときをいう。

本研究の今回の目的は、環$Z[\sqrt[3]{2}]$の素数を探索するための方法論について研究することである。

通常の整数環Zにおいて、素数を探索する方法としては“エラトステネスのふるい”が古くから知られている。“ふるい”を作るときに大事なことは、素数かどうか調べたい数よりも“小さな数”が因数になっているかどうかを調べることである。環$Z[\sqrt[3]{2}]$の探索法について“ふるい”のような方法ができないかと考える場合、問題は環$Z[\sqrt[3]{2}]$の整数にはどのような大小関係があるのかである。

3. ノルムの定義

環のノルムとはその環の数の大小関係を調べるときに有用である。たとえば複素整数環の整数$\alpha = a + bi$については、αのノルム$N(\alpha)$は

$$N(\alpha) = \alpha\bar{\alpha} = a^2 - (bi)^2 = a^2 + b^2$$

と定義される。

Dを平方数ではない整数とする。このとき、二次の整数環$Z[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in Z,\}$の整数$\alpha = a + b\sqrt{D}$のノルムついては、以下のように定義される[1]。

定義１．　$Z[\sqrt{D}]$の整数$\alpha = a + b\sqrt{D}$について，αのノルム$N(\alpha)$は

$$N(\alpha) = \alpha\bar{\alpha} = a^2 - b^2D$$

ここで$\bar{\alpha} = a - b\sqrt{D}$で、これは$\alpha$の共役と呼ばれる。

$Z[\sqrt{D}]$の整数のノルム$N(\alpha)$は負の値をとることも許されている。しかし、$N(\alpha)N(\beta) = N(\alpha\beta)$が成り立つことから、$Z[\sqrt{D}]$の素数についての研究を行なうことができる。

それでは、$Z[\sqrt[3]{2}]$の整数$\eta = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ではどのように定義されるのであろうか。最初は、$Z[\sqrt[3]{2}]$の整数$\eta = a + b\sqrt[3]{2} + c\sqrt[3]{4}$について、

$$N(\eta) = a^3 + 2b^3 + 4c^3, \quad N(\eta) = a^3 - 2b^3 - 4c^3$$

などといった定義を考えた。しかし、これらの定義だと$N(\eta)$に等しいノルムをもつ整数が無限に存在する可能性がある。さらに、この定義には共役という概念を入れていないことも後々問題になりそうである。

実は、二次の整数環$Z[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in Z,\}$においては、$Z[\sqrt{D}]$の整数$\alpha$に対してシュプール$S(\alpha) = \alpha + \bar{\alpha}$という概念も定義されている。$Z[\sqrt{D}]$におけるノルム$N(\alpha) = \alpha\bar{\alpha}$とシュプール$S(\alpha) = \alpha + \bar{\alpha}$は、一体何を意味するのだろうか。

私は、$\alpha = a + b\sqrt{D}$を解にもつ２次方程式にヒントがあると考えた。なぜならば、$N(\alpha)$も$S(\alpha)$もどちらも２次方程式の解と係数の関係式に見えるからである。すなわち、$\alpha = a + b\sqrt{D}$を解にもつ最高次数の係数が１であるZ係数の２次方程式（モニックなZ係数の２次方程式という）は

$$t^2 - S(\alpha)t + N(\alpha) = 0$$

であるということに気がついた。

定義２．$\eta = a + b\sqrt[3]{2} + c\sqrt[3]{4}$について、$\eta$を解にもつモニックな$Z$係数の３次方程式を

$$t^3 + S_1(\eta)t^2 + S_2(\eta)t + S_3(\eta) = 0$$

とし、左辺を単にηを解にもつZ係数の3次式という。

定義３．ηを解にもつZ係数の3次式の残りの２つの解η', η''を、ηの共役という。

さて、$\eta - a = b\sqrt[3]{2} + b\sqrt[3]{4}$の両辺を３乗して

$$\begin{aligned}\eta^3 - 3a\eta^2 + 3a^2\eta + a^3 &= 2b^3 + 4c^3 + 6bc\left(b\sqrt[3]{2} + c\sqrt[3]{4}\right)\\ &= 2b^3 + 4c^3 + 6bc(\eta - a)\end{aligned}$$

を得る。よって、

$$\eta^3 - 3a\eta^2 + (3a^2 - 6bc)\eta + a^3 - 2b^3 - 4c^3 + 6abc = 0$$

を得る。したがって、$\eta = a + b\sqrt[3]{2} + c\sqrt[3]{4}$を解にもつ$Z$係数の3次式は

$$t^3 - 3at^2 + (3a^2 - 6bc)t + a^3 - 2b^3 - 4c^3 + 6abc$$

である。

定義４． $\eta = a + b\sqrt[3]{2} + b\sqrt[3]{4}$について

$$S_1(\eta) = -3a,\quad S_2(\eta) = 3a^2 - 6bc,\quad S_3(\eta) = a^3 - 2b^3 - 4c^3 + 6abc$$

とし、$S_i(x)$を第iシュプールという。さらに、ノルム$N(\eta)$を

$$N(\eta) = |S_1(\eta)| + |S_2(\eta)| + |S_3(\eta)|$$

と定義する。

（注意）$N(\eta) = |S_3(\eta)|$と考えることもできるが、これだと同じノルムに無限個の整数をもつ可能性があるため、ノルムを上の定義４にした。

さて、$\eta = 1 + \sqrt[3]{2}$のノルム$N(\eta)$を求める。$S_1(\eta) = -3, S_2(\eta) = 3,\quad S_3(\eta) = 1$であり、

$$N(\eta) = 7$$

である。同様にして$0 \le N(\eta) \le 10$について以下を得る。

（0）$N(\eta) = 0$の場合：$\eta = 0$

（1）$N(\eta) = 1$の場合：なし

（2）$N(\eta) = 2$の場合：$\eta = \pm\sqrt[3]{2}$

（3）$N(\eta) = 3$の場合：なし

（4）$N(\eta) = 4$の場合：$\eta = \pm\sqrt[3]{4}$

（5）$N(\eta) = 5$の場合：なし

（6）$N(\eta) = 6$の場合：なし

（7）$N(\eta) = 7$の場合：$\eta = \pm 1,\ \pm\left(1 + \sqrt[3]{2}\right),\ \pm\left(1 + \sqrt[3]{2} + \sqrt[3]{4}\right)$

（8）$N(\eta) = 8$の場合：$\eta = \pm\left(\sqrt[3]{2} - \sqrt[3]{4}\right),\ \pm\left(2 + \sqrt[3]{2} + 2\sqrt[3]{4}\right)$

（9）$N(\eta) = 9$の場合：$\eta = \pm\left(1 - \sqrt[3]{2}\right),\ \pm\left(1 + \sqrt[3]{4}\right)$

（10）$N(\eta) = 10$の場合：なし

４．同じノルムをもつ整数の個数

環$Z\left[\sqrt[3]{2}\right]$の整数$\eta$についてそのノルム$N(\eta)$と同じノルムをもつ整数は有限個しかないことを証明した。

定理 1. $\eta = a + b\sqrt[3]{2} + c\sqrt[3]{4}$について

$$|a| \leq \frac{1}{3}N(x) \qquad \dots(a)$$

$c = 0$ならば

$$|b| \leq \frac{1}{18}N(\eta) + \frac{1}{6}N(\eta) \qquad \dots(b)$$

$b = 0$ならば

$$|c| \leq \frac{1}{18}N(\eta) + \frac{1}{6}N(\eta) \qquad \dots(c)$$

$c \neq 0$ならば

$$|b| \leq \sqrt[3]{\frac{1}{2}N(\eta) + \frac{1}{54}N(\eta)^3} \qquad \dots(d)$$

$b \neq 0$ならば

$$|c| \leq \sqrt[3]{\frac{1}{2}N(\eta) + \frac{1}{54}N(\eta)^3} \qquad \dots(e)$$

（証明）不等式(a)について、

$$N(\eta) \geq S_1(\eta) = 3|a|$$

より、不等式(a)は明らかに成り立つ。

三角不等式より

$$N(\eta) \geq |S_2(\eta)| = |3a^2 - 6bc| \geq |6bc| - |3a^2|$$

$$|6bc| \leq N(\eta) + |3a^2| \leq N + 3 \times \frac{1}{9}N(\eta)^2 \leq \frac{1}{3}N(\eta)^2 + N(\eta) \qquad \dots(A)$$

が成り立つ。また、

$$N(\eta) \geq |S_3(\eta)| \geq |a^3 - 2b^3 - 4c^3| - |6ac|$$

$$|a^3 - 2b^3 - 4c^3| \leq N[\eta] + |6abc| = \frac{1}{9}N(\eta)^3 + \frac{1}{3}N(\eta)^2 + N(\eta)$$

である。

$$|a^3 - (2b^3 + 4b^3)| \geq |2b^3 + 4b^3| - |a^3|$$

$$|2b^3 + 4b^3| \leq \frac{1}{9}N(\eta)^3 + \frac{1}{3}N(\eta)^2 + \frac{4}{3}N(\eta) \qquad \dots(B)$$

$c \neq 0$のとき、(A)より

$$|b| \leq \frac{1}{6|c|}\{\frac{1}{3}N(\eta)^2 + N(\eta)\} \leq \frac{1}{18}N(\eta)^2 + \frac{1}{6}N(\eta)$$

$c=0$のとき、(B)より

$$|2b^3| \leq \frac{1}{9}N(\eta)^3+\frac{1}{3}N(\eta)^2+\frac{4}{3}N(\eta)$$

$$|b^3| \leq \frac{1}{18}N(\eta)^3+\frac{1}{6}N(\eta)^2+\frac{2}{3}N(\eta)$$

$$|b| \leq \sqrt[3]{\frac{1}{18}N(\eta)^3+\frac{1}{6}N(\eta)^2+\frac{2}{3}N(\eta)}$$

$t\neq 0$のとき、(A)より

$$|c| \leq \frac{1}{6|b|}\{\frac{1}{3}N(\eta)^2+N(\eta)\} \leq \frac{1}{18}N(\eta)^2+\frac{1}{6}N(\eta)$$

$t=0$のとき、(B)より

$$|4c^3| \leq \frac{1}{9}N(\eta)^3+\frac{1}{3}N(\eta)^2+\frac{4}{3}N(\eta)$$

$$|c^3| \leq \frac{1}{36}N(\eta)^3+\frac{1}{12}N(\eta)^2+\frac{1}{3}N(\eta)$$

$$|b| \leq \sqrt[3]{\frac{1}{36}N(\eta)^3+\frac{1}{12}N(\eta)^2+\frac{1}{3}N(\eta)}$$

よって、定理３の不等式$(b),(c),(d),(e)$はすべて示された。（証明終）

定理１から次の系が得られる。

系１． 任意の$N(\eta)$について、$N(\eta)>N(\xi)$となるξは有限個しかない。

５．$Z[\sqrt[3]{2}]$における割り算について

$Z[\sqrt[3]{2}]$の整数$\eta=a+b\sqrt[3]{2}+c\sqrt[3]{4}$が素数であるかどうかを確かめるためには、$Z[\sqrt[3]{2}]$の割り算について調べておく必要がある。

定理２． $\xi=s+t\sqrt[3]{2}+u\sqrt[3]{4},\ \ \eta=a+b\sqrt[3]{2}+c\sqrt[3]{4}$について$\eta|\xi$であるための必要十分条件は

$$\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}=\begin{pmatrix} s \\ t \\ u \end{pmatrix}$$

が整数解x,y,zを持つことである。

(証明)

$$s+t\sqrt[3]{2}+u\sqrt[3]{4}=\left(a+b\sqrt[3]{2}+c\sqrt[3]{4}\right)\left(x+y\sqrt[3]{2}+z\sqrt[3]{4}\right)$$
$$=(ax+2bz+2cy)+(ay+bx+2cz)\sqrt[3]{2}+(az+by+cx)\sqrt[3]{4} \quad \dots(3)$$

逆に、次のような除算

$$\frac{s+t\sqrt[3]{2}+\sqrt[3]{4}}{a+b\sqrt[3]{2}+c\sqrt[3]{4}}$$

について考える。その時、(3)式より

$$s=ax+2bz+2cy,\quad t=(ay+bx+cz)\sqrt[3]{2},\quad u=(az+by+cx)\sqrt[3]{4}$$

を得る。つまり、$a+b\sqrt[3]{2}+c\sqrt[3]{4}$が$s+t\sqrt[3]{2}+\sqrt[3]{4}$を割切るとき

$$\begin{cases} ax+2bz+2cy=s \\ ay+bx+2cz=t \\ az+by+cx=u \end{cases}$$

を満たすx,y,zは整数解でなければならない。すなわち、

$$\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}=\begin{pmatrix} s \\ t \\ u \end{pmatrix}$$

を満たすx,y,zは整数解でなければならない。(証明終)

改めて$x=a+b\sqrt[2]{2}+c\sqrt[3]{4}$における素数を定義する。

定義. 4　$x,p\in Z\left[\sqrt[3]{2}\right]$かつ$N(x)<N(p)$とする。$x|p$で$x$が単元に限るとき、$p$は素数という。

たとえば、$\xi=3$が素数かどうか判定する。このとき、$N(\xi)=63$である。一方、$\eta=1+\sqrt[3]{2}$は$N(\eta)=7$である。したがって、$N(\eta)<N(\xi)$である。そこで、連立方程式

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}=\begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}$$

を考えると、$x=1,y=-1,z=1$が得られる。したがって、定理 2 より$\xi=3$は素数でない。

$0\le N(\eta)\le 10$について以下の素数のリストを得る。

(1) $N(\eta)=2$の場合：$\eta=\pm\sqrt[3]{2}$
(2) $N(\eta)=7$の場合：$\eta=\pm\left(1+\sqrt[3]{2}\right)$
(3) $N(\eta)=8$の場合：$\eta=\pm\left(2+\sqrt[3]{2}+2\sqrt[3]{4}\right)$
(4) $N(\eta)=9$の場合：$\eta=\pm\left(1+\sqrt[3]{4}\right)$

単位元について、次の予想が得られている。

予想. 1　単元は$\pm 1, \pm\left(1+\sqrt[3]{2}\right), \pm\left(1+\sqrt[3]{2}+\sqrt[3]{4}\right)$の 6 個だけである。

6．今後の研究について

今回の研究では環$Z[\sqrt[3]{2}]$における素数を調べるための道具を準備することができた。すなわち、環$Z[\sqrt[3]{2}]$の整数のノルムを定義することができ、さらに 2 つの整数の割り算が環$Z\left[\sqrt[3]{2}\right]$内で可能かどうかを調べるための定理も証明することができた。

今後は、本格的に環$Z[\sqrt[3]{2}]$における素数を調べ、素数に関する何らかの法則（たとえば環$Z\left[\sqrt[3]{2}\right]$は一意分解整域となっているかどうかなど）を研究したいと考えている。また、今回のノルムの定義は、より一般的な環でも扱うことができると考えている。したがって、より一般的な環論における素数の研究に応用できるとも考えている。

参考文献

[1]　武隈良一，2 次体の整数論，槇書店, 1966