Z[√D]の素数に関する考察

宮崎大学教育文化学部紀要　教育科学　第10号（2003）37－53頁

$Z[\sqrt{D}]$ の素数に関する考察

宇田　廣文

A study of prime numbers in $Z[\sqrt{D}]$

Hirohumi　Uda

1．はじめに

素数の概念は、整数の性質を理解する上で、また、初等整数論において重要で基本的な概念である。現在学校数学においては、中学３年で式の因数分解と絡めて導入され、根号の中を簡単にするときに利用される形で取り扱われているが、筆者は従前（平成４年以前）のように、中学１年で小学校とのつなぎ教材として、約数・倍数の観点から整数の性質として取り扱う方がよいと考えている。また、高等学校の数学Ａの「集合と論理」において、整数の約数の個数を求めるのに素因数分解が利用されている。このとき、素因数分解の一意性が働いているのであるが、それは潜在的（implicit）であり表面に出て来ず、あまり意識されていない。生徒の発達段階を考えるとそれはやむをえないことではあるが、指導する教師としては数学的素養として、一意性に対する意識を持っておく必要がある。ワイルズによって解決されたフェルマーの最終定理「$x^n+y^n=z^n$は$n\geqq 3$のとき、$x=y=z=0$以外に整数解を持たない。」が約400年間に亘り未解決であった要因の１つが、素因数分解の一意性が一般には成立しないことであった事実を考えると、その重要性が分かる。

素因数分解の一意性とは、次の初等整数論の基本定理の中に登場するものである。

《初等整数論の基本定理》

２以上の自然数は有限個の素数の積に分解され、しかもその表し方は素数の積の順序を無視すれば、一通りに定まる。つまり、次が成り立つ。

> p_1，p_2，……，p_n，q_1，q_2，……，q_mを素数とするとき、
> $p_1p_2\cdots\cdots p_n=q_1q_2\cdots\cdots q_m$　ならば、$m=n$ であり、順番を入れ替えることにより、$p_1=q_1$，$p_2=q_2$，……，$p_m=q_m$ とすることができる。

……（☆）

この（☆）を素因数分解の一意性と呼んでいる。この性質のお陰で、素因数分解をすることで約数の型が定まり、約数の個数が求められるのである。また、最大公約数や最小公倍数もその結果として求められることになる。

ところで、素因数分解の一意性を支えているものは、残念ながら素数の定義そのものではなく、素数の特徴付けともいえる素数の性質なのである。素数は一般に次のように定義される。

《素数の定義》
２以上の自然数ｐは（自然数の範囲で）１と自分以外に約数を持たないとき、素数（prime number）であるという。

この定義は、約数の視点（目）からみたものである。どんな自然数も１と自分自身を約数に持つので、１を除くと、常に２個以上の約数を持つことになる。そこで約数の個数が最小となる、即ち約数の個数が丁度２個であるものを素数と定義しているのである。

一方、約数と倍数は関係としてみると、相対的な概念である。例えば、３は12の約数であり、12は３の倍数である。これは、３と12を約数・倍数という目でみたとき、３を「主語」とすれば「約数」という用語が用いられ、12を「主語」とすれば「倍数」という用語が用いられるということで、どちらを主語とするかという問題であり、つまり、相対的な概念である。この関係は、一般に記号「３｜12」で表される。大小関係「３＜12」が３を「主語」とすれば「３は12より小さい」といい、12を「主語」とすれば「12は３より大きい」というのと同じことである。約数・倍数の概念は小学校６年で導入されるが、倍数はかけ算で約数はわり算でというように、別々に取り扱われている。導入の仕方としてはよいとしても、関係としての見方も育てる必要がある。

そこで、約数の視点で定義された素数を相対的な概念である倍数の視点でみると、次の素数の特徴付け（素数の定義と同値な性質）が得られる。

《素数の性質》
ｐを素数とする。ａ，ｂを整数とするとき
ｐ｜ａｂ ⇒ ｐ｜ａ または ｐ｜ｂ
ここで、 ｃ｜ｄ はｄがｃの倍数であることを意味する。

この素数の性質が、先の素因数分解の一意性を保証しているのである。この性質の証明には、小学校４年で学習される商と余りの考えが必要である。つまり、次の除法の原理がもとになっている。

《除法の原理》
整数ａ，ｂ（≠０）に対して
$$a = bq + r \quad 0 \leqq r < |b|$$
を満たす、整数ｑ，ｒが存在し、しかもただ一組存在する。
なお、ここでの整数は、負の整数も含むものとする。

この除法の原理は、整数の性質を考えていく上で最も基本的なものである。学校数学おいても、内容論的な面だけではなく、数学的な見方考え方の観点からも大切な内容である。

以上、素数と素因数分解の一意性の周辺を概観してきたが、先にも述べたように「一意性」は空気みたいなものである。つまり、空気が薄くなり呼吸が困難になって初めて空気のありがたさが分かるように、一意性もそれが成り立たない場面に遭遇して初めてその意義とよさを実感するのである。素因数分解の一意性が成り立たない例として、$a+b\sqrt{-5}$（a，bは整数）からなる数の世界（整域）で、$6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5})$がよく用いられる。

2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$はすべて素数であるが、明らかに一意性は満たしていない。

初等整数論の講義などでは、このような例をあげてそれ以上深入りしないのが、一般的である。また、先人たちは、一意性を克服するために、理想数（ideal number）を考え、それがイデアルの概念へ発達し、現在ではイデアル論的な解決をしている。さらに、素因数分解の一意性が成り立つような世界（UFD）に関する考察研究はよくなされているが、成り立たない世界における素数の考察は少ない。

そこで本稿では、身近な数環である$Z[\sqrt{D}]=\{a+b\sqrt{D}\mid a，bは整数\}$を用いて、初等的手法で素数を考察整理することと、大学における整数論や環論の題材の一助とすることを目的とする。従って以後は、数学的に考察をしていく。

2．準　　備

ここでは、環論的な準備をする。

2．1　数　環

複素数体Cの部分集合Rは次の条件を満たすとき、数環（number ring）という。

1）$Z\subseteq R$　ここで、Zは整数全体の集合を表す。

2）$a，b\in R$ に対し、$a\pm b$，$ab\in R$（和・差・積で閉じている。）

整数全体の集合Z、有理数全体の集合Q、実数全体の集合R、複素数全体の集合Cは数環の代表的な例である。

また、Dを非平方数とするとき、$Z[\sqrt{D}]=\{a+b\sqrt{D}\mid a，bは整数\}$は数環である。

特に、$Z[\sqrt{-1}]$はガウスの整数環と呼ばれているものである。

2．2　単　元

数環Rの要素αは$\alpha\beta=1$となるRの要素βが存在するときに、Rの単元（unit）であるという。そして、Rの単元全体を$R^{\times}$で表す。$R^{\times}$は積で群をなす。

例えば、$Z^{\times}=\{1，-1\}$，$Q^{\times}=Q-\{0\}$，$R^{\times}=R-\{0\}$，$C^{\times}=C-\{0\}$，

また、$Z[\sqrt{-1}]^{\times}=\{1，-1，\sqrt{-1}，-\sqrt{-1}\}$，そしてD≦－2のとき，

$Z[\sqrt{D}]^{\times}=\{1，-1\}$　となる。

このように、D＜0のときは、単元は容易に分かるが、D＞0となると事情は一変する。

例えば、$Z[\sqrt{2}]$においては、$Z[\sqrt{2}]^{\times}=\{\pm(1+\sqrt{2})^{n}\mid nは整数\}$となる。

2.3 約元・倍元・同伴

数環Rの要素α，β（$\neq 0$）に対して、$\alpha=\beta\gamma$となるRの要素γが存在するとき、$\beta \mid \alpha$とかき、αはβの倍元であるといい、また、βはαの約元であるという。

約元・倍元に関する基本的な性質として、次は大切である。

数環Rの0でない要素α，β，γに対して

1）$1 \mid \alpha$，$\alpha \mid \alpha$

2）$\alpha \mid \beta$，$\beta \mid \alpha$ ならば $\beta=\varepsilon\alpha$となるRの単元εが存在する。

3）$\alpha \mid \beta$，$\beta \mid \gamma$ ならば $\alpha \mid \gamma$

4）$\alpha \mid \beta$，$\alpha \mid \gamma$ ならば Rの任意の要素σ，τに対して $\alpha \mid \beta\sigma+\gamma\tau$

数環Rの0でない要素α，βが$\alpha \mid \beta$，$\beta \mid \alpha$を満たすとき、αとβは同伴である（associate）といい、$\alpha \sim \beta$で表す。2）より、同伴な元は単元倍の違いだけであることが分かる。また、この関係$\sim$は、同値関係である。このことは、約元・倍元という目で見たとき、同伴な元は区別できないということを意味している。

例えば、2と同伴な元は、Zにおいては2，-2、また、$\mathbb{Z}[\sqrt{-1}]$においては2，-2，$2\sqrt{-1}$，$-2\sqrt{-1}$であるが、それぞれにおいて約元・倍元という目で見たときそれらは区別できない。

2.4 既約元・素元

素数の定義を一般化したものとして既約元の概念があり、素数の性質を一般化したものとして素元の概念がある。即ち、以下のように定義される。

《既約元（irreducible element）》
数環Rの0でも単元でもない要素πは次の条件を満たすとき、Rの既約元という。
Rの要素αに対し、 $\alpha \mid \pi \Rightarrow \alpha \in R^{\times}$ または $\alpha \sim \pi$

《素元（prime element）》
数環Rの0でも単元でもない要素πは次の条件を満たすとき、Rの素元という。
Rの要素α，βに対し、 $\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha$ または $\pi \mid \beta$

数環の既約元、素元はそれぞれ既約数、素数と呼ぶこともあるが、ここでは整数における素数の意味との混同を避けるために既約元、素元を用いることにする。

先述のように整数の世界では、既約元と素元は同じ概念になるが一般には同じではない。ここに、一意性が成り立たない要因がある。既約元と素元が同じ概念になる数環としては、Z，$\mathbb{Z}[\sqrt{-1}]$，$\mathbb{Z}[\sqrt{2}]$などあるが、本稿では触れない。

既約元と素元が同じ概念にはならない例としては、はじめにで述べた例がそうである。即ち、数環$\mathbb{Z}[\sqrt{-5}]$において、$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$より$2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$であるが、$2 \nmid 1+\sqrt{-5}$，$2 \nmid 1-\sqrt{-5}$であるから2は$\mathbb{Z}[\sqrt{-5}]$の素元ではない。（ここで、記号$\alpha \nmid \beta$は$\alpha$が$\beta$の約元でないことを示す。）また、2が$\mathbb{Z}[\sqrt{-5}]$の既約元であること

も容易に分かる（詳細は、後述）。一般には、次が成り立つ。

1）素元は既約元である。

従って、一般には「素元」の概念が「既約元」の概念より強いということになる。

2．5　イデアル

倍数の概念を一般化したものとしてイデアルの概念がある。数環Rの空でない部分集合Iは次の条件を満たすとき、Rのイデアル（ideal）であるという。

1）α，$\beta \in I$ に対し、$\alpha \pm \beta \in I$

2）$\alpha \in I$，$\gamma \in R$ に対し、$\alpha\gamma \in I$

特に、Rの任意の要素αに対し、αの倍元全体 $\{\alpha\gamma \mid \gamma \in R\}$ はRのイデアルである。これをαで生成されたRの単項イデアル（principal ideal）といい、(α)で表す。

整数環Zのイデアルはすべて単項イデアルであることが、除法の原理を用いることにより分かる。このような数環は一般に単項イデアル整域（ＰＩＤ）と呼ばれている。先の$Z[\sqrt{-1}]$，$Z[\sqrt{2}]$ などもその仲間である。また、数環$Z[\sqrt{-5}]$はＰＩＤではない。このことも既約元と素元は同じ概念にならないことと関係しているがここでは深入りしない。

素元の概念をイデアル化したものとして、素イデアルがある。

> 素イデアル（prime ideal）
> 数環RのRと異なるイデアルPは、次の条件を満たすとき、Rの素イデアルであるという。
> α，$\beta \in R$ に対し、　$\alpha\beta \in P \Rightarrow \alpha \in P$　または　$\beta \in P$

特に、素元はイデアルを用いて表現すれば、次のようになる。

3）数環Rの０でも単元でもない要素πに対して、次が成り立つ。

πはRの素元である。$\Leftrightarrow$（π）はRの素イデアルである。

さらに、次の性質が成り立つ。

4）数環$R \subseteq S$があるとき、Sのイデアル I に対し、$I \cap R$はRのイデアルになる。

特に、PがSの素イデアルであるとき、$P \cap R$はRの素イデアルになる。

2．6　ノルム

未知のものを考察するとき、何らかの方法（関数の考えなど）を用いて、既知の世界に帰着させて考察することは、有効な数学的な考え方の一つである。ここでも、数環$Z[\sqrt{D}]$での考察を整数環Zでの考察に帰着させていく。そのための手段としてノルムの考えがある。

まず、共役複素数の概念を一般化した共役元の概念を定義する。

整数Dを非平方数としておく。数環$Z[\sqrt{D}]$の要素$\alpha = a + b\sqrt{D}$（a，b$\in$Z）に対し、$a - b\sqrt{D}$ をαの共役元（cojugate element）といい、$\overline{\alpha}$で表す。

さらに、$\alpha\overline{\alpha} = a^2 - Db^2$を$\alpha$のノルム（norm）といい、$N(\alpha)$で表す。

定義からNは数環$Z[\sqrt{D}]$からZへの関数であり、次の性質が成り立つ。

1）$\alpha \in Z[\sqrt{D}]$に対し、　　$N(\alpha) = N(\overline{\alpha})$

2） α，$\beta \in Z[\sqrt{D}]$に対し、 $N(\alpha\beta)=N(\alpha)N(\beta)$

3） $\alpha \in Z[\sqrt{D}]$に対し、 $\alpha \in Z[\sqrt{D}]^{\times} \Leftrightarrow N(\alpha)=\pm 1$

4） α，$\beta \in Z[\sqrt{D}]$に対し、 $\alpha \sim \beta \Rightarrow N(\alpha)=\pm N(\beta)$

2．7 その他

以下で用いる次の記号を導入しておく。

自然数nと整数a，bに対し、$n \mid a-b$のとき $a \equiv b \pmod{n}$ で表す。

また、素数pとpと互いに素である整数aに対し、$x^2 \equiv a \pmod{p}$ が整数解を持つとき、$\left(\frac{a}{p}\right)=1$、そうでないとき $\left(\frac{a}{p}\right)=-1$ で表す。

3．既 約 元

以下本稿では、Dは非平方数としておく。

ある整数が素数かどうかを判定する方法としては現在数多くのものが知られているが、最も素朴で基本的なものは次の判定法であろう。

> 《素数の判定法》 nを2以上の自然数とする。このとき，
> 自然数nは$\sqrt{n}$ 以下の素数で割れなければ、素数である。

100以下の24個の奇素数を用いると10000以下の素数が決定できるように、数が小さいときは有効な方法である。

素数の定義に準じて約元の観点で定義された既約元についても同様に、次の判定法が考えられる。

> 《既約元の判定法》
> 数環$Z[\sqrt{D}]$ の0でも単元でもない要素πは、次の条件を満たせば既約元である。
> (※) $N(\pi)$の± 1，$\pm N(\pi)$ と異なる任意の約数nに対して、
> 不定方程式$x^2-Dy^2=n$が整数解を持たない。

このことは、2．6の2）が、

1） α，$\beta \in Z[\sqrt{D}]$に対し、$\alpha \mid \beta$ ならば $N(\alpha) \mid N(\beta)$ を意味していることから分かる。

例えば、数環$Z[\sqrt{-5}]$においては、$N(a+b\sqrt{-5})=a^2+5b^2 \geqq 0$ （a，bは整数）だから、約数は正の約数のみ考えればよい。

$N(2)=4$，$N(3)=9$，$N(1\pm\sqrt{-5})=6$であり、$x^2+5y^2=2$，3を満たす整数解は存在しないので、2，3，$1+\sqrt{-5}$ ，$1-\sqrt{-5}$ は$Z[\sqrt{-5}]$の既約元であることが分かる。

また、1）の逆は、次の例から分かるように一般には正しくない。

数環$Z[\sqrt{-5}]$において、$N(3)=9$，$N(1+4\sqrt{-5})=81$で、$9 \mid 81$であるが、
$Z[\sqrt{-5}]$において、$3 \nmid 1+4\sqrt{-5}$ である。
上記の判定法からすぐ分かることに、次の３つがある。

２）πを数環$Z[\sqrt{D}]$の既約元とする。このとき、数環$Z[\sqrt{D}]$の任意の単元εに対して、
$\varepsilon\pi$，$\varepsilon\bar{\pi}$は数環$Z[\sqrt{D}]$の既約元である。

３）πを数環$Z[\sqrt{D}]$の要素とするとき、
$N(\pi)$が$\pm p$（pは素数）ならば、πは数環$Z[\sqrt{D}]$の既約元である。
なお、後でこの場合には実はπは素元になっていることを示す。

４）pを素数とするとき、
$x^2-Dy^2=\pm p$が整数解を持たないならば、pは数環$Z[\sqrt{D}]$の既約元である。

さらに、２以上の自然数が有限個の素数の積として表すことができることが示せるのと同様に、数環$Z[\sqrt{D}]$の０でも単元でもない任意の要素が既約元の有限個の積として表すことができることも、ノルムを通しての整数での考察から示すことができる。従って、整数環との異同は一意性が成り立つのか、それとも成り立たないのかである。それは突き詰めれば、素元と既約元の問題に帰着される。

４．例

数環$Z[\sqrt{D}]$の素元を一般的に考察する前に、具体的な例で素元性の検討を試みる。例を地道に考察することは、素元の具体的な例を豊富にすること（外延を明確にすること）は勿論のこと、帰納的な考え方や類推的な考え方などの考え方を養うとともに、その構造などを明らかにすること（内包を明らかにすること）になる。概念理解には、多くの例に当たり具体的に体験的に実感していくことが重要である。

ここでは、$3+2\sqrt{-5}$ を例に取り、これが数環$Z[\sqrt{-5}]$ の素元であることを示していく。

実は、この $3+2\sqrt{-5}$ は数環$Z[\sqrt{-5}]$ において、$\sqrt{-5}$ の次にそのノルムが小さい素元である。

まず、$\pi=3+2\sqrt{-5}$　とおくと、そのノルムは$N(\pi)=29$である。

そこで、　α，$\beta \in Z[\sqrt{-5}]$ に対し、　$\pi \mid \alpha\beta$と仮定する。

このとき、　$N(\pi) \mid N(\alpha\beta)$　　よって　$N(\pi) \mid N(\alpha)N(\beta)$ となる。

$N(\pi)=29$　は素数だから、　$29 \mid N(\alpha)$　または　$29 \mid N(\beta)$ であることが分かる。

今、$29 \mid N(\alpha)$ としておく。（一般性は失われない。即ち、$29 \mid N(\beta)$のときも同様。）

そこで、$\alpha=a+b\sqrt{-5}$（a，$b \in Z$）とおくと、

$29 \mid N(\alpha)$　だから　$a^2+5b^2 \equiv 0 \pmod{29}$ である。

今、$13^2 \equiv -5 \pmod{29}$ を使うと（因数分解を可能にするためのテクニック！）

$a^2-13^2b^2 \equiv 0 \pmod{29}$ となる。

よって、$29 \mid a+13b$　または　$29 \mid a-13b$　であることが分かる。

(1) $29 \mid a+13b$ のとき $a+13b=29m$ $(m \in Z)$ とおく。

$\alpha = a+b\sqrt{-5} = 29m-b(13-\sqrt{-5})$

$29=(3+2\sqrt{-5})(3-2\sqrt{-5})$

$13-\sqrt{-5}=(3+2\sqrt{-5})(1-\sqrt{-5})$

これから $3+2\sqrt{-5} \mid \alpha$ 即ち $\pi \mid \alpha$ であることが分かる。

(2) $29 \mid a-13b$ のとき $a-13b=29m$ $(m \in Z)$ とおく。

$\alpha = a+b\sqrt{-5} = 29m+b(13+\sqrt{-5})$

(注意：(1)と同様にすると $\bar{\pi}=3-2\sqrt{-5}$ とおくと $\bar{\pi} \mid \alpha$)

1) $29 \mid b$ のとき

$29 \mid \alpha$ となり $\pi \mid 29$ だから $\pi \mid \alpha$ であることが分かる。

2) $29 \nmid b$ のとき

まず、次を示す。

$\gamma \in Z[\sqrt{-5}]$ に対し、 $\pi \mid b\gamma \Rightarrow \pi \mid \gamma$ (☆)

$\gamma = c+d\sqrt{-5}$, $b\gamma = \pi\delta$, $\delta = x+y\sqrt{-5}$ $(c, d, x, y \in Z)$ とおくと、

$bc=3x-10y$, $bd=2x+3y$

これから、 $29x=b(3c+10d)$, $29y=b(-2c+3d)$

$29 \nmid b$ だから $x=be$, $y=bf$ $(e, f \in Z)$

と表すことができる。

よって、$\gamma=\pi(e+f\sqrt{-5})$ 即ち $\pi \mid \gamma$ となり、(☆) が成り立つ。

さて、$\alpha\beta=29m\beta+b(13+\sqrt{-5})\beta$

$13+\sqrt{-5}=(3+2\sqrt{-5})(2-\sqrt{-5})-3$

従って、$\pi \mid 3b\beta$ であることが分かる。

$29 \nmid 3b$ だから (☆) より $\pi \mid \beta$ となる。

よって、$\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha$ または $\pi \mid \beta$

以上により、$\pi=3+2\sqrt{-5}$ は 数環 $Z[\sqrt{-5}]$ の素元である。

このように、ある要素が素元であるかどうかを調べるには、地道な計算が必要である。そしてそこには、共役元との関係の考察の必要性や因数分解へ持っていくことの必要性など、一般の場合の考察への情報が内在している。もし、素元の一般的な判定法があれば、煩雑な計算は省くことができる。そこに、数学的なそして理論的な考察の意味と意義の一端がある。一方、理論だけに頼ると具体性のない無味乾燥なものになりかねないので、前述のように具体例の考察が欠かせないのである。

5．素　　元

この節で、いよいよ数環 $Z[\sqrt{D}]$ の素元を以下の手順を踏んで決定していく。

まず、数環 $Z[\sqrt{D}]$ の素元と素数との関係を調べる。ここでは、整数環Zのイデアルがすべて単項イデアルであること（即ち、ZはＰＩＤ）が本質的である。

5．1　$Z[\sqrt{D}]$ の素元をπとするとき、$(\pi)\cap Z=(p)$ を満たす素数pが存在する。
さらに、このとき　$N(\pi)=\pm p,\ \pm p^2$　が成り立つ。

実際、πを数環$Z[\sqrt{D}]$の素元であるとすると、2．5の3）より、単項イデアル（π）は数環$Z[\sqrt{D}]$ の素イデアルである。従って、2．5の4）より（π）$\cap$ZはZの素イデアルである。

よって、$(\pi)\cap Z=(p)$ を満たす素数pが存在する。
（注意：$0\neq N(\pi)\in Z$より　$(\pi)\cap Z\neq(0)$）
一方、$p\in(\pi)\cap Z$から　$p=\pi\tau$となる　$\tau\in Z[\sqrt{D}]$ が存在する。
故に、$p^2=N(\pi)N(\tau)$
また、　$N(\pi)\in(\pi)\cap Z=(p)$　より　　$p\mid N(\pi)$
従って、$N(\pi)=\pm p,\ \pm p^2$　が成り立つことが分かる。

5．2　逆に、$\pi\in Z[\sqrt{D}]$ に対して、$(\pi)\cap Z=(p)$ を満たす素数pが存在するならば、πは数環$Z[\sqrt{D}]$ の既約元であるか、またはpと同伴である。

実際、$(\pi)\cap Z=(p)$ を満たす素数pが存在すると仮定すると、$(\pi)\cap Z=(p)$ から　πは単元ではないことが分かる。　従って、$N(\pi)\neq\pm1$　である。
また、仮定より、$p=\pi\tau$となる　$\tau\in Z[\sqrt{D}]$ が存在する。
よって、$p^2=N(\pi)N(\tau)$ であるから、$N(\pi)=\pm p,\ \pm p^2$となることが分かる。
そこで、2つの場合に分けて考察する。

① $N(\pi)=\pm p$のとき

既約元の判定法により、πが数環$Z[\sqrt{D}]$ の既約元であることは明らかである。(cf.3．4))

しかし、ここでは計算するという立場から、具体的な計算を示しておく。

今、$\alpha\mid\pi$（$\alpha\in Z[\sqrt{D}]$）と仮定すると、$\pi=\alpha\beta$となる　$\beta\in Z[\sqrt{D}]$が存在する。
すると、$N(\pi)=N(\alpha)N(\beta)$で$N(\pi)=\pm p$だから、

$$N(\alpha)=\pm1\quad\text{または}\quad N(\beta)=\pm1$$

であることが分かる。従って、πは$Z[\sqrt{D}]$ の既約元である。

② $N(\pi)=\pm p^2$　のとき

$p=\pi\tau$から、$N(\tau)=\pm1$　となるので、πはpと同伴である。

以上により、素数pがいつ数環$Z[\sqrt{D}]$ の素元になるかということと、$N(\pi)=\pm p$となるπは素元かということを見ていけば、数環$Z[\sqrt{D}]$の素元を決定することができる。

5．3　素数pの素元性

素数pが、数環$Z[\sqrt{D}]$においていつ素元になるのかについては、数論的にもイデアル論的にもよく知られていることである。ここでは、ノルムの有効性と合同式のよさをみるために、また、素元の定義の強みを感得するために手順をおって具体的に示していく。

まず、次の同値な命題が成り立つ。

$p \mid N(\alpha) \Rightarrow \pi \mid \alpha$ または $\bar{\pi} \mid \alpha$

実際に2つの場合が生じる例をあげておく。

例 $\pi = 3 + 2\sqrt{-5}$ とすると、$N(\pi) = 29$である。

$\alpha = -4 + 7\sqrt{-5}$ とおくと $N(\alpha) = 261 = 29 \times 9$

今、$3 \times 7 - 2 \times (-4) = 29$ だから $\pi \mid \alpha$

実際 $\alpha = \pi(2 + \sqrt{-5})$

また、$\beta = 16 - \sqrt{-5}$ とおくと $N(\alpha) = 261 = 29 \times 9$

$3 \times (-1) + 2 \times 16 = 29$ だから $\bar{\pi} \mid \beta$

実際 $\beta = \bar{\pi}(2 + \sqrt{-5})$

3）における考察と例から、目的であるπの素元性を示すためには、$\bar{\pi}$の処理が必要であることが分かった。そこで、次にその処理のために2つの準備をする。

4）$p = 2$ または $p \mid D \Rightarrow \pi \sim \bar{\pi}$

① $p = 2$ とする。このとき、 $a^2 - Db^2 = \pm 2$ であるから、

$$\frac{a + b\sqrt{D}}{a - b\sqrt{D}} = \frac{(a^2 + Db^2) + 2ab\sqrt{D}}{\pm 2} = \frac{\pm 2 + 2Db^2 + 2ab\sqrt{D}}{\pm 2} \in Z[\sqrt{D}]$$

故に $(\pi) \subseteq (\bar{\pi})$ であることが分かる。

逆も同様にして示すことができるので、$(\pi) = (\bar{\pi})$ となる。

即ち、$\pi \sim \bar{\pi}$ であることになる。

② $p \mid D$ でpを奇素数としておく。

このとき、$a^2 - Db^2 = \pm p$ より $p \mid a$ がまず分かる。

$$\frac{a + b\sqrt{D}}{a - b\sqrt{D}} = \frac{(a^2 + Db^2) + 2ab\sqrt{D}}{\pm p} \in Z[\sqrt{D}]$$

故に $(\pi) \subseteq (\bar{\pi})$ であることが分かる。

逆も同様にして示すことができるので、$(\pi) = (\bar{\pi})$ となる。

即ち、$\pi \sim \bar{\pi}$ であることになる。

5）pを奇素数とし、$p \nmid D$ としておく。

$\alpha = c + d\sqrt{D}$ $(a, b \in Z)$ とするとき、次が成り立つ。

$\pi \mid \bar{\pi}\alpha \Rightarrow \pi \mid \alpha$

（このことは、πの素元性が分かれば当然の性質であるが、実際はこの性質がπの素元性の一翼を担っているのである。）

さて今、$\pi \mid \bar{\pi}\alpha$ と仮定する。このとき、

$\bar{\pi}\alpha = \pi\beta$ $\beta = x + y\sqrt{D}$ $(x, y \in Z)$

と表すことができる。計算すると、

$$ac - Dbd = ax + Dby \quad \cdots\cdots ①$$

$$ad - bc = ay + bx \quad \cdots\cdots ②$$

さらに次の計算をする。

①×a＋②×Dbから

$$\pm pc=(a^2+Db^2)x+2Daby=\pm px+2Db(bx+ay)$$

①×b＋②×aから

$$\pm pd=2abx+(a^2+Db^2)y=\pm py+2b(ax+Dby)$$

仮定より、pは奇素数で $p\nmid D$ 、$p\nmid b$ であるから

$$bx+ay\equiv 0 \pmod p$$

$$ax+Dby\equiv 0 \pmod p$$

よって、$\dfrac{c+d\sqrt{D}}{a+b\sqrt{D}}=\dfrac{x+y\sqrt{D}}{a-b\sqrt{D}}=\dfrac{(ax+dby)+(bx+ay)\sqrt{D}}{a^2-Db^2}=\in Z[\sqrt{D}]$

故に、$\pi\mid\alpha$ であることが示された。

以上の準備のもと、πの素元性を次に示す。

6）$N(\pi)=\pm p$（pは素数）ならば π は数環$Z[\sqrt{D}]$の素元である。

実際、$\pi\mid\alpha\beta$ （α，$\beta\in Z[\sqrt{D}]$）と仮定する。

このとき、$N(\pi)\mid N(\alpha)\,N(\beta)$，$N(\pi)=\pm p$ だから

$p\mid N(\alpha)$ または $p\mid N(\beta)$

今、$p\mid N(\alpha)$ とする。さらに、

$|N(\alpha)|=p^m q$ で $p\nmid q$，$m\geqq 1$ としておく。

先の3）より $\pi\mid\alpha$ または $\bar{\pi}\mid\alpha$ であることが分かる。

そこで、もし、$p=2$ あるいは $p\mid D$のときは、4）から $\pi\mid\alpha$は分かる。

従って、以後、p を奇素数とし、$p\nmid D$ としておく。

もし、$\pi\mid\alpha$ ならば $\pi\mid\alpha$ または $\pi\mid\beta$ であることは明らかである。

そこで、$\pi\nmid\alpha$ と仮定する。 このとき、必然的に $\bar{\pi}\mid\alpha$ となる。

$m\geqq 2$ のときは5）を繰り返して用いることにより、 $\bar{\pi}^m\mid\alpha$ が分かる。

即ち、$\alpha=\bar{\pi}^m\alpha_1$（$\alpha_1\in Z[\sqrt{D}]$） $|N(\alpha_1)|=q$ $p\nmid q$

と表すことができる。

すると、上の5）から $\pi\mid\alpha_1\beta$ である。

このとき、$N(\pi)\mid N(\alpha_1)\,N(\beta)$，$N(\pi)=\pm p$ だから$p\mid N(\alpha_1)\,N(\beta)$

仮定より、$p\nmid q$だから $p\mid N(\beta)$

そこでまた、$\pi\nmid\beta$と仮定すると 同様にして、

$\beta=\bar{\pi}^n\beta_1$（$\beta_1\in Z[\sqrt{D}]$） $|N(\beta_1)|=r$ $p\nmid r$

と表すことができる。

従ってまた、$\pi\mid\bar{\pi}^n\alpha_1\beta_1$ だから5）から $\pi\mid\alpha_1\beta_1$

すると $p\mid N(\alpha_1)\,N(\beta_1)$ となるが、これは $p\nmid q$，$p\nmid r$に矛盾する。

従って、$\pi\mid\alpha$ または $\pi\mid\beta$ であることが分かる。

故に、π は数環$Z[\sqrt{D}]$の素元である。

5．5 $Z[\sqrt{D}]$ の素元

以上の考察により、数環$Z[\sqrt{D}]$の素元は次の２つのタイプがあることが分かった。

(1) 素数pがそのまま 数環$Z[\sqrt{D}]$ の素元である。
これは、$x^2 \equiv D \pmod{p}$ が整数解を持たないときであり、そのときに限る。
非平方数Dが与えられたとき、$p \nmid D$となる素数pがいつ $(\frac{D}{p}) = -1$ となるかは
平方剰余の理論により容易に決定できるので、pの素元性も決定できる。

(2) $N(\pi) = \pm p$ となる数環$Z[\sqrt{D}]$ の要素 π は素元である。
$\pi = a + b\sqrt{D}$ $(a, b \in Z)$ とおくと、$a^2 - Db^2 = \pm p$
即ち、$x^2 - Dy^2 = \pm p$ が整数解を (x, y) を持つとき，そのときに限り、pは2つの素元の積に分解できる。

また、合同式$x^2 \equiv D \pmod{p}$ は整数解を持つが、不定方程式$x^2 - Dy^2 = \pm p$ が整数解を (x, y) を持たないときは，pは既約元ではあるが素元ではない。

6．終わりに

素因数分解の一意性は整数論において極めて重要な性質である。それが成り立つか成り立たないかの要因は素数の性質にある。そこで、数環$Z[\sqrt{D}]$ を用いて素数の定義と素数の性質を初等的に考察してきた。既約元や素元の概念は、環論的にはよく知られたものである。また、数環$Z[\sqrt{D}]$ も数論においてもイデアル論においてもよく知られたものである。しかし、既約元や素元そのものに焦点を当てた考察は必ずしも多くはない。そこに焦点を当てて初等的に整理したのが本稿である。その内容としては次などがある。

1）素数の定義と性質を約数・倍数の見方の違いとして捉えたこと
2）既約元の判定法を示せたこと
これには、約数の目で見るという見方が関係していた。
3）数環$Z[\sqrt{D}]$ の素元を初等的に決定したこと

また、本稿では、教授学的な立場からもアイデアやポイントそして具体例などを提示した。特に、数論などでよく用いられるノルムの有用性を、数学的な見方考え方の視点から具体的に示してきた。即ち、未知の事象の考察を既知の事象での考察に変換することで、考察の道具を得ることができ、課題解決や構造把握に繋げられることを示した。

一方、それにも限界がある。間接的な考察になるため、有効に働かない場面が生じてくる。例えば、既約元の判定法は、素数の判定法と違って、十分条件ではあるが必要条件ではない。従って、一般にはエラトステネスの篩の適用はできなくなる。必要条件でないことを示す例としては、次をあげることができる。

例 数環$Z[\sqrt{-7}]$において、$\pi = 1 + \sqrt{-7}$ とおくと、πは数環$Z[\sqrt{-7}]$の既約元である。
実際、数環$Z[\sqrt{-7}]$の要素αに対し、$\alpha \mid \pi$と仮定すると、$N(\alpha) \mid N(\pi)$となる。
一方、$N(\pi) = 8$だから、$N(\alpha) = 1, 2, 4, 8$であることになる。

① $N(\alpha) = 1$のときは、αは単元である。
② $N(\alpha) = 2$のときは、αは存在しない。
③ $N(\alpha) = 4$のときは、$\alpha = \pm 2$である。
④ $N(\alpha) = 8$のときは、αはπと同伴である。

また、$2 \nmid 1+\sqrt{-7}$ は明らかであるので、以上より、π が数環 $Z[\sqrt{-7}]$ の既約元であることが分かる。さらに、これらの考察は、$N(\pi)=8$ の約数である4に対して、ノルムが4となる数環 $Z[\sqrt{-7}]$ の要素、± 2 が存在するので、既約元の判定法が必要条件ではないことを示している。

さらに、ノルムの相等性が既約性を保つとは限らない。即ち、数環 $Z[\sqrt{-D}]$ の2つの要素 α, β が $N(\alpha)=N(\beta)$ を満たすとき、α が既約元だからといって、β も既約元であるとは限らない。例えば、数環 $Z[\sqrt{-14}]$ において、9と $5+2\sqrt{-14}$ を考えるとよい。9は明らかに既約元ではないが、$5+2\sqrt{-14}$ は既約元であることが簡単な考察で容易に分かる。しかし、$N(9)=N(5+2\sqrt{-14})=81$ であり、両者のノルムは等しい。

上の例などからも分かるように、その原因は、$\alpha \mid \beta$ と $N(\alpha) \mid N(\beta)$ が同値でないことに起因している。従って、既約元の判定法を必要条件を満たすようにすると、次のようになる。

《既約元の判定法（精緻化）》
数環 $Z[\sqrt{D}]$ の0でも単元でもない要素 π は、次の条件を満たせば既約元である。
(※※) $N(\pi)$ の ± 1, $\pm N(\pi)$ と異なる任意の約数を n とするとき、
$N(\alpha)=n$ となる任意の $\alpha \in Z[\sqrt{D}]$ に対して、$\alpha \nmid \pi$ である。

これは、既約元の定義をノルムを用いて、整数の世界で表現し直したものであるが、整数の世界だけでは既約元の判定ができないことを示している。

事象の考察には様々な道具が用いられるが、そこには常に有効性と限界があるということを念頭に置くことの大切さを、このことは示唆している。そのことを実感するためには、多くの事例での数学的考察を通した体験的認識が必要であることはいうまでもない。

一方、既約元と素元が一致しない数環（ＰＩＤでない数環）においても、既約元の判定法が必要十分条件になるものもある。例えば、数環 $Z[\sqrt{-5}]$、$Z[\sqrt{-13}]$ などがそうである。

そこで、終わりに参考資料として、数環 $Z[\sqrt{-5}]$ における既約元と素元の例をあげておく。

なお、数環 $Z[\sqrt{-13}]$ についても同様な結果を示すことができる。

参 考 文 献

1．武隈良一　1966　2次体の整数論　槙書店.
2．David A. Cox,　1989　Primes of the form x^2+ny^2, John Wiley & Sons.
3．河田敬義　1978　岩波講座基礎数学「数論Ⅰ」　岩波書店.

参 考 資 料

数環Z[$\sqrt{-5}$]における既約元・素元

これまでの考察をもとに、数環Z[$\sqrt{-5}$]における既約元・素元を参考として決定する。
まず、よく知られた次の事実をあげておく。

p（≠2，5）を奇素数とするとき、

① $(\frac{-5}{p})=-1 \Leftrightarrow p\equiv 11,\ 13,\ 17,\ 19 \pmod{20}$

② $(\frac{-5}{p})=1 \Leftrightarrow p\equiv 1,\ 3,\ 7,\ 9 \pmod{20}$

さらに、 $x^2+5y^2=p$ が整数解を持つ $\Leftrightarrow$ $p\equiv 1,\ 9 \pmod{20}$
$x^2+5y^2=2p$ が整数解を持つ $\Leftrightarrow$ $p\equiv 3,\ 7 \pmod{20}$

従って、本論から次が分かる。

1）±2は、数環Z[$\sqrt{-5}$]において既約元であるが、素元ではない。

2）$\pm\sqrt{-5}$ は、数環Z[$\sqrt{-5}$]において素元である。

3）奇素数pがp≡11，13，17，19（mod 20）を満たすとき、
±p は、数環Z[$\sqrt{-5}$] において素元である。

4）奇素数pが p≡1，3，7，9（mod 20）を満たすとき、
±p は、数環Z[$\sqrt{-5}$]において既約元であるが素元ではない。

5）奇素数pが p≡1，9（mod 20）を満たすとき、$N(a+b\sqrt{-5})=p$（a，bは整数）とすると、$a+b\sqrt{-5}$ は数環Z[$\sqrt{-5}$]において素元である。

6）奇素数pが p≡3，7（mod 20）を満たすとき、$N(a+b\sqrt{-5})=2p$（a，bは整数）とすると、$a+b\sqrt{-5}$ は数環Z[$\sqrt{-5}$]において既約元であるが素元ではない。
さらに、次が分かる。

7）奇素数p，qがp，q≡3，7（mod 20）を満たすとする。（p＝qも含む。）
このとき、$\pi=a+b\sqrt{-5}$（a，bは整数）で$N(\pi)=pq$となるものが存在する。
さらに、πは数環Z[$\sqrt{-5}$]において既約元であるが素元ではない。
実際、②から $x^2+5y^2=2p$ を満たす整数解（c，d）と $x^2+5y^2=2q$ を満たす整数解（e，f）が存在する。即ち、$c^2+5d^2=2p$，$e^2+5f^2=2q$ ここで、p，qは奇素数であるので、c，d，e，fはともに奇数であることが分かる。
一方、$(ce+5df)^2+5(cf-de)^2=(c^2+5d^2)(e^2+5f^2)=4pq$
c，d，e，fはともに奇数であるから、ce＋5df，cf－deはともに偶数である。
よって、ce＋5df＝2a，cf－de＝2b（a，bは整数）とおくと $a^2+5b^2=pq$ となる。
また、このとき、$\pi=a+b\sqrt{-5}$ が数環Z[$\sqrt{-5}$]において既約元であることは、既約元の判定法から明らかである。

このように、①，②のお陰で、数環Z[$\sqrt{-5}$]の既約元と素元を求めることができる。

逆に、数環Z[$\sqrt{-5}$]の既約元と素元は上の1）から7）のタイプに限られることも示すことができる。ノルムが7）のタイプの相異なる素数の積である場合を除くと、初等的な考察で処理できるが、ノルムが7）のタイプの相異なる素数の積である場合の初等的考察の仕方を筆者は持っていない。その処理は、数環Z[$\sqrt{-5}$]の類数が2であることと、数環Z[$\sqrt{-5}$]がデデキント整域（各イデアルが素イデアルの積に一意的に分解できる数環）であることを用いるとできるが、ここでは「初等的に」を考察の1つのキーワードとしてきたので深入りしない。

解決の難しさの原因は、因数分解の一意性が使えないところにある。このような場面の考察を通して、一意性などのよさを実感していくのである。最後に、$N[\pi] \leqq 510$ となるものを以下の表にあげる。$\pi = a + b\sqrt{-5}$ とおくとき、π が既約元か素元ならば、$\pm\pi$，$\pm\bar{\pi}$ もそうである。そこで、表は（a，b）（$a \geqq 0$，$b \geqq 0$）で示す。また、表で既約元は、素元でない既約元を意味する。

$N[\pi]$	既約元	素元
4	(2, 0)	
5		(0, 1)
6	(1, 1)	
9	(3, 0)	
	(2, 1)	
14	(3, 1)	
21	(4, 1)	
	(1, 2)	
29		(3, 2)
41		(6, 1)
46	(1, 3)	
49	(7, 0)	
	(2, 3)	
61		(4, 3)
69	(8, 1)	
	(7, 2)	
86	(9, 1)	
89		(3, 4)
94	(7, 3)	
101		(9, 2)
109		(8, 3)
121		(11, 0)
129	(7, 4)	
	(2, 5)	
134	(3, 5)	
141	(11, 2)	
	(4, 5)	
149		(12, 1)
161	(9, 4)	
	(6, 5)	
166	(11, 3)	
169		(13, 0)
181		(1, 6)
201	(14, 1)	
	(11, 4)	
206	(9, 5)	
214	(13, 3)	

$N[\pi]$	既約元	素元
229		(7, 6)
241		(14, 3)
249	(13, 4)	
	(2, 7)	
254	(3, 7)	
269		(12, 5)
281		(6, 7)
289		(17, 0)
301	(16, 3)	
	(11, 6)	
309	(17, 2)	
	(8, 7)	
321	(14, 5)	
	(1, 8)	
326	(9, 7)	
329	(18, 1)	
	(3, 8)	
334	(17, 3)	
349		(13, 6)
361		(19, 0)
381	(19, 2)	
	(16, 5)	
389		(12, 7)
401		(9, 8)
409		(2, 9)
421		(4, 9)
446	(21, 1)	
449		(18, 5)
454	(7, 9)	
461		(21, 2)
469	(17, 6)	
	(8, 9)	
489	(22, 1)	
	(13, 8)	
501	(16, 7)	
	(1, 10)	
509		(3, 10)