$a+b\sqrt{-6}$ の 世 界

——素因数分解の一意性について——

山　口　　格
（室蘭工業大学）

§ 1. 素因数分解の一意性は自明ではない

整数に関係のあることについて述べるので整数の性質を要約しておいた方が都合がよい。自然数 1, 2, 3, …の全体を **N**, 整数…, −2, −1, 0, 1, 2, …の全体を **Z** で表す。整数の間になりたつ加法, 乗法は周知のこととして省略するが、理論の出発点として自然数の集合 **N** に関する次の性質を承認することにする。

定理 1　**N** の任意の空でない部分集合 A はただ一つの最小数を含む, ここで m が A の最小数であるとは, $m\in$A で, 任意の $a\in$A に対して $m\leqq a$ であることを意味する。

定理 1 から数学的帰納法の原理が導かれる[(1)]。次に素数の定義を行う。

定義 1　自然数 $p>1$ が, ± 1, $\pm p$ 以外に約数をもたないとき, p を素数という。± 1, $\pm p$ (p 素数) 以外の整数を合成数という。

歴史的には上の定義が行なわれて来たが、最近は次の定義も見られるようになった。

定義 2　自然数 $p>1$ が, 任意の自然数 a, b に対して

$$p|ab \Rightarrow p|a \vee p|b$$

が成り立つとき, 素数という。

環論などとの関係を考えれば定義 2 が便利であるが, 当面は定義 1 で考えることにする。さて問題にしたいことは「素因数分解の一意性」についてである。つまり任意の自然数は素数の積に一意的に分解できるということを問題にしたい。このことは現在のカリキュラムでは中学校 1 年に扱うことになっている。例えばある教科書では

$36=2\times 18$　　$36=3\times 12$
$=2\times 2\times 9$　　$=3\times 2\times 6$
$=2\times 2\times 3\times 3$　　$=3\times 2\times 2\times 3$

という例を示したのち次のようになっている。「上のように素因数分解した結果は, 書き並べる順序を考えなければただ 1 通りになる。」しかしながら, このような経験的記述の信頼性は, はなはだぐらつきやすいものである。いま次のような例を考えよう,

$5063=61\times 83$

このような素因数分解が何かの方法でわかったとしよう，このとき 5063 を割切る素数はもはやこの他にはないということは明らかであろうか。

§ 2. $a+b\sqrt{6}$ の世界

上の中学校教科書にあるように先入観を排除するため，ここで別の数の世界を考察することにしよう。a, b は任意の整数をとることにして，$a+b\sqrt{6}$ の形をした数の全体を考える。この数の全体を $a+b\sqrt{6}$ の世界と名付けよう。この世界の数の間の演算は普通の実数の演算を行うこととする。そうすると $a+b\sqrt{6}$ の形の数の和，差，積はまた $a+b\sqrt{6}$ の形の数である。この数の世界は $b=0$ の場合，すなわち整数全体の集合 $\mathbf{Z}$ を含む集合である。この $a+b\sqrt{6}$ の世界で素因数分解を考えてみよう。素因数分解であるから乗法が問題である。乗法の例をいくつかあげてみよう[2]。

$$(3+\sqrt{6})(3-\sqrt{6})=9-6=3$$
$$(\sqrt{6}+2)(\sqrt{6}-2)=6-4=2$$
$$(3+\sqrt{6})(\sqrt{6}-2)=3\sqrt{6}-6+6-2\sqrt{6}=\sqrt{6}$$
$$(3-\sqrt{6})(\sqrt{6}+2)=\sqrt{6}$$
$$(3+\sqrt{6})(2+\sqrt{6})=12+5\sqrt{6}$$
$$(3-\sqrt{6})(\sqrt{6}-2)=12+5\sqrt{6}$$

このような計算は中学3年生には充分出来るはずである。さて因数分解にとりかかろう。

$$6=2\cdot 3=\sqrt{6}\cdot\sqrt{6} \tag{1}$$

この例をみると，6 は整数の分解 2•3 のほかに，$\sqrt{6}\cdot\sqrt{6}$ と全く別の形に書けることがわかる。素因数分解の一意性はこの $a+b\sqrt{6}$ の世界ではなりたたないのであろうか。早まった結論を出すのはやめてもう少しよく考えてみよう。$6=2\cdot 3$ の 2 と 3 は整数の世界ではもはやこれ以上分解出来ない数（すなわち素数）であったが，$a+b\sqrt{6}$ の世界では上の乗法の例にあるように

$$3=(3+\sqrt{6})(3-\sqrt{6})$$
$$2=(\sqrt{6}+2)(\sqrt{6}-2)$$

という分解をもつのである。したがって

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

という分解ができた。ところが $6=\sqrt{6}\cdot\sqrt{6}$ においても，先の乗法の例からわかるように

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

となる。さてここまで来ると，注意深く観察することによって，はじめの $6=2\cdot 3=\sqrt{6}\cdot\sqrt{6}$ という分解のほかに気がつかなかった分解がひそんでいたことがわかる。(2)の第一と第四，第二と第三の因数を組合せたものが(3)であるから，当然(2)の第一と第三，第二と第四の因数を組合わせた分解も存在するのである。それは乗法の例の最後の2つからもわかる。すなわち

$$6=(12+5\sqrt{6})(-12+5\sqrt{6})$$

が得られる。結局 6 の因数は $(\sqrt{6}+2)$, $(\sqrt{6}-2)$, $(3+\sqrt{6})$, $(3-\sqrt{6})$ の 4 つであることがわかった。

§ 3. $a+b\sqrt{-6}$ の世界

こんどは $a+b\sqrt{-6}$ という形の数の世界を考察しよう。前と同じく a, b は任意の整数である。$a+b\sqrt{6}$ の世界の計算ができた人は，この $a+b\sqrt{-6}$ の世界の計算も容易にできるはずである。これまでの 6 を -6 におきかえればよいのである。前節(1)に相当する分解は，今度の場合は

$$6=2\cdot 3=-\sqrt{-6}\cdot\sqrt{-6} \tag{4}$$

となる。ところが前節と同様に 2，3 及び $\sqrt{-6}$ をこの新しい数の世界で分解することを試みてもうまく行かないようである。ためしに前節の乗法を今度の場合に書きかえてみようとするとこのことはよくわかる。すなわち前の場合

$$(3+\sqrt{6})(3-\sqrt{6})=9-6=3$$

であったが，今度は

$$(3+\sqrt{-6})(3-\sqrt{-6})=9+6=15$$

となるのである。じつはこの $a+b\sqrt{-6}$ の世界では 2，3 および $\sqrt{-6}$ をこれ以上因数に分解することは不可能なのである。

このことを証明するためにノルムというものを導入する。$a+b\sqrt{-6}$ という数のノルムを

$$N(a+b\sqrt{-6})$$

と書いて次のように定義する。

$$N(a+b\sqrt{-6})=(a+b\sqrt{-6})(a-b\sqrt{-6})$$
$$=a^2+6b^2$$

これからわかることは，ノルムは 0 または正の整数である。ノルムには次の性質がある。

定理 2　2 つの数のノルムの積は，各数の積のノルムに等しい。すなわち 2 つの数を $a+b\sqrt{-6}$ および $c+d\sqrt{-6}$ とすれば

$$N(a+b\sqrt{-6})N(c+d\sqrt{-6})$$
$$=N((a+b\sqrt{-6})(c+d\sqrt{-6})) \tag{5}$$

である。

証明　$N(a+b\sqrt{-6})N(c+d\sqrt{-6})$
$=(a+b\sqrt{-6})(a-b\sqrt{-6})(c+d\sqrt{-6})(c-d\sqrt{-6})$
$=(a+b\sqrt{-6})(c+d\sqrt{-6})(a-b\sqrt{-6})(c-d\sqrt{-6})$
$=N((a+b\sqrt{-6})(c+d\sqrt{-6}))$

すなわち 4 つの括弧の順序を変えただけで証明ができたのである。

さて 2 がこの数の世界で因数に分解出来たとしよう。そうすると

$$2=(a+b\sqrt{-6})(c+d\sqrt{-6})$$

となるはずである。この両辺のノルムを取れば次のようになる。

$$N(2)=N((a+b\sqrt{-6})(c+d\sqrt{-6}))$$
$$=N(a+b\sqrt{-6})N(c+d\sqrt{-6}) \quad ((5)を用いた)$$
$$=(a^2+6b^2)(c^2+6d^2)$$

$N(2)=4$ であるから，これより

$$4=(a^2+6b^2)(c^2+6d^2)$$

を得る。右辺は2つの正の整数の積である。つまり4という整数は a^2+6b^2 の形の整数と c^2+6d^2 の形の整数の積に分解されることになる。ところが4を分解すると $2\cdot2$ か $4\cdot1$ かの何れかであるが。2は a^2+6b^2 の形には書けない。$4=4\cdot1$ は通常の整数論では因数に分解されたとみなされない。それと同じくこの世界でもやはり因数に分解されたとは見なさないのである。同様にノルムを用いて3も $\sqrt{-6}$ も分解不可能なことがすぐわかる。こうして

$$6=2\cdot3=-\sqrt{-6}\cdot\sqrt{-6} \tag{4}$$

というように，6という数が，いずれも分解不可能な因数からなる2通りの分解をもつことが示された。従って $a+b\sqrt{-6}$ の世界では素因数分解の一意性は成り立っていないことがわかったのである。

§ 4. 素因数分解の一意性の証明の歴史

今見たように $a+b\sqrt{-6}$ の世界では素因数分解の一意性は成りたたない。このことから整数の世界で素因数分解の一意性が成りたつことが明白とすることは疑問があるということがわかる。従ってもし整数の素因数分解に一意性が成りたつとすれば，それは整数に特有な性質に原因があって出て来ることと考えられる。

昔の人達はこのことをどう考えていたのだろうか。ユークリッド原論について述べたブルバキのコメントをみてみよう[3]。

「ただし，素因数分解の存在と一意性だけは，一般的な仕方では証明されていない。ユークリッドは実際には，どんな整数も素数で整除されること(7巻，命題31)，およびつぎの二つの命題（9巻，命題13と14）を証明している。すなわち

≪単位から出発し，望むだけの個数の数が，比が一定の（すなわち幾何）数列をなしていて，この単位のつぎの項が素数のとき，一番大きい項は，この数列に現われる項だけによって整除される≫（言いかえれば，整数の巾 p^n は，指数が n 以下の p の巾によってだけ整除される。）

≪ある数が，（与えられた）いくつかの素数で整除されるような，最小のもののとき，それは，はじめに除数（として与えられた）これら以外の，どんな素数でも整除されない≫（言いかえれば，たがいに異なる素数の積 $p_1\cdots p_k$ は，p_1，…，p_k 以外の素因子をもたない。）

そこで，ユークリッドが一般的定理を述べていないのは，単に整数の巾に対する適当な用語と記号法が欠けていたためらしい。この仮定を支持するものとして，完全数に関する定理の証明が，素因数分解の一意性の定理のもう一つの特別な場合に実はほかならないことを指摘することができる。」

ギリシャ時代の数学者はもちろん $a+b\sqrt{-6}$ の世界などは知らなかったにもかかわらず，素因数分解の一意性は証明しなければならないものだということを直観的に感じていたにちがいない。しかし19世紀初頭の頃には証明の必要性は忘れ去られていたようである。この頃ガウスが次のように述べている。

「任意の合成数が素因数へと分解できることは初等的考察から明らかであるが，これを多くの異なる方法で行うことはできないということは暗黙のうちに仮定されていて，一般には証明されていないのである。」このように素因数分解の一意性の定理の証明の重要性はガウスにより指摘され，その厳密な証明も彼の著書 Disquisitiones Arithmeticae (1801年) に述べられたので

あった[4]。

§ 5. 初等整数論の基本定理とその証明

今まで述べてきた素因数分解の一意性に関する命題を，初等整数論の基本定理とよんでいる。この節ではこの定理の証明を述べよう[5]。

定理 3　任意の整数 a と整数 $b>0$ に対して

$$a=bq+r,\quad 0\leqq r<b \tag{6}$$

となる整数 q，r がただ一組存在する。

証明　まず(6)をみたす整数 q，r の存在を示す。$a\geqq 0$ のとき，$(a+1)b>a$ であるから，a より大きい $mb(m\in\mathbf{N})$ の形の自然数全体の集合 $A=\{mb|mb>a\geqq 0, m\in\mathbf{N}\}$ は空集合ではない。したがって，A は定理 1 により最小数を含み，その最小数は $(q+1)b$，$q+1\in\mathbf{N}$，の形に表される。$(q+1)b$ は a より大きい $mb(m\in\mathbf{N})$ の形の整数の中で最小のものであるから $qb\leqq a<(q+1)b$ が成り立つ。($q+1=1$ のときは $q=0$ となるが，上の不等式はやはり成り立つ。)このとき $r=a-qb$ とおけば，$0\leqq r=a-qb<b$，$a=qb+r$ である。$a<0$ のときは，$-a>0$ であるから，$-a=bq'+r'$，$0\leqq r'<b$，となる q'，$r'\in\mathbf{Z}$ が存在する。$q=-(q'+1)$，$r=b-r'$ とおけば，$a=bq+r$，$0\leqq r<b$，となる。一意性については，$a=bq_1+r_1=bq_2+r_2$，$0\leqq r_1$，$r_2<b$ ならば $q_1=q_2$，$r_1=r_2$ である。実際，$(q_1-q_2)b=r_2-r_1$，$-b<r_2-r_1<b$ となるから，$r_2-r_1=0$。したがって $q_1-q_2=0$ である。 ■

定理 4　整数 a，b の積 ab がある素数 p で割りきれるならば，a または b の少なくとも一方は p で割りきれる。すなわち

$$p|ab \Rightarrow p|a \text{ または } p|b。$$

証明　a と p との最大公約数を $(a,\ p)$ と書くとき，$(a,\ p)$ は p の約数であるから p または 1 である。$(a,\ p)=p$ のとき，$p|a$。$(a,\ p)=1$ ならば $ax+py=1$ となる x，$y\in Z$ が存在する。このとき $b=abx+pby$ であり $p|ab$ より $p|b$。 ■

上の証明で $(a,\ p)=1$ のとき $ax+py=1$ となる x，$y\in Z$ をみつけるには，定理 3 を何回かくりかえし用いるのである。定理 3 を用いて最大公約数を求める（ユークリッド互除法とよばれる）計算を逆にたどるのである。

定理 5　（初等整数論の基本定理）任意の自然数 $a>1$ は

$$a=p_1\cdots p_k\ (\text{ただし，}p_1,\ \cdots,\ p_k\text{ は必ずしも異ならない素数})$$

の形に順序を除いて一意的に表される。ここで、順序を除いて一意的というのは

$$a=p_1\cdots p_k=q_1\cdots q_k\ (q_1,\ \cdots,\ q_k\text{ は必ずしも異ならない素数})$$

であれば，$k=l$ であり，適当な番号をつけかえれば $p_1=q_1$，$\cdots$，$p_k=q_k$ となることである。

証明　$a>1$ についての数学的帰納法により証明する。

(i) まず，$a>1$ が素数の積として表わされること，すなわち

$$a=p_1\cdots p_k$$

となることを証明する。$a=p$ が素数なら $k=1, p_1=p$ として正しい。a が合成数ならば $a=a_1a_2$，$a_1>1$，$a_2>1$，と表される。$a_1<a$，$a_2<a$ については a_1，a_2 が素数の積として表されるから，a もそれら素数の積となる。

(ii) $a=p_1\cdots p_k=q_1\cdots q_l$ とする。$p_1|q_1\cdots q_l$ であるから，ある番号 i に対しては $p_1|q_i$。q_i は素数であるから $p_1=q_i$。番号をつけかえたと考えて $i=1$ とする。$p_1=q_1$。このとき $1<a/p_1$ ならば $a/p_1=p_2\cdots p_k=q_2\cdots q_l$。$a/p_1<a$ については数学的帰納法の仮定により，$k=l$，適当に番号をつけかえて $p_2=q_2$，…，$p_p=q_k$。 ■

この素因数分解の一意性の定理の証明の核心部分は(ii)のはじめの部分の

$$p_1|q_1\cdots q_l \Rightarrow p_1|q_i$$

であり，この部分に定理4が用いられている。定理4の証明には定理3，すなわちユークリッド互除法を用いている。この定理3がなりたつことが，整数全体の集合 Z の大きな特徴であり，他の数の世界と異なっているところである。$a+b\sqrt{-6}$ の世界で素因数分解の一意性が成り立たないのは，つまるところ定理4が成り立たないからである。

§ 6. ユークリッド環について[6]

有理整数環 $\mathbf{Z}$ において素因数分解の一意性が成りたつのは，前述したように，割り算定理「Z の任意の a と $b\neq 0$ とに対し，適当な整数 q，r が存在して，$a=bq+r$，$|r|<|b|$ が成り立つ」から由来する。それゆえ，もし任意の環 $\mathbf{O}$ において割り算定理の適当な類推が成り立てば，環 $\mathbf{O}$ においても $\mathbf{Z}$ と全く同様に，素因数分解の一意性を証明しうるであろう。そこで次の定義をしよう。

定義3 環 $\mathbf{O}$ において割り算(剰余を伴う)が可能であるとは，零と異なる $\alpha\in\mathbf{O}$ に関数 $\|\alpha\|$ が定義され，その値は非負な整数で，かつ次の条件をみたしていることである。

1) もし $\alpha\neq 0$ が β で整除されれば，

$$\|\alpha\|\geqq\|\beta\|:$$

2) $\mathbf{O}$ の任意の元 α と $\beta\neq 0$ とに対し，適当な γ と ρ が存在して $\alpha=\beta\gamma+\rho$ が成り立ち，ここで $\rho=0$ であるかまたは $\|\rho\|<\|\beta\|$。環 $\mathbf{O}$ はこのとき Euclid 環とよばれる。

有理整数に対する素因数分解の一意性の証明で使った性質は，環の一般的な性質以外は，割り算定理だけである。それゆえこの証明を一語一語くり返せば，次の結果に到達する。

定理6 Euclid 環では，各元は素元の積に一意的に分解される。

実2次体 $\mathbf{R}(\sqrt{d})$ の極大整環のうちでノルムについて割り算の成り立つものは，d が次の16個のうちどれかと一致するときだけである。

$$d=2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73$$

これと反対に，代数的数体の極大整環において素因数への分解が一意的とは限らない例は多

くある。たとえば体 $\mathbf{R}(\sqrt{-5})$ をとる。この体の極大整環に属する数は，x, y を有理整数として，$\alpha=x+y\sqrt{-5}$ の形をしている。このノルムは $\mathrm{N}(\alpha)=x^2+5y^2$。ここで 21 は次の分解をもつ。

$$21=3\cdot 7$$

$$21=(1+2\sqrt{-5})(1-2\sqrt{-5})$$

両式の右辺にある因数はすべて素であることは $a+b\sqrt{-6}$ の世界の場合と同様にしてすぐ確かめられる。また体 $\mathbf{R}(\sqrt{-23})$ の極大整環において次の素因数分解が成り立つ。

$$6=2\cdot 3$$

$$6=\frac{1+\sqrt{-23}}{2}\cdot\frac{1-\sqrt{-23}}{2}$$

$$27=3\cdot 3\cdot 3$$

$$27=(2+\sqrt{-23})(2-\sqrt{-23})$$

等々このような例は多数あげることができる。

§ 7. 素元分解整域

数論の問題が今日の（抽象）代数学の出発点のひとつであった。例えば 19 世紀におけるフェルマーの大定理をめぐってのクンマーの円分整数の理論は素因数分解の一意性そのものが問題にされたのである[7]。

ここでは整数環 $\mathbf{Z}$ での素因数分解をより一般化した代数学の概念を述べよう。

$\mathbf{R}$ を整域とする。すなわち，$\mathbf{R}$ は単位元 1 をもつ可換環[8] で，$\mathbf{R}$ の元 a, b に対して，“$ab=0\Rightarrow a=0$ または $b=0$” が成り立つ。

$\mathbf{R}$ の二元 a, b に対して $a=bc$ となる $c\in\mathbf{R}$ が存在するとき，a は b の倍元，b は a の約元であるといい，$b|a$ とかく，$b|a$ かつ $a|b$ であるとき a, b は同伴であるといい，a は b の（b は a の）同伴元であるという。a, b が同伴であるための心要十分条件は $a=be$ となる単元（正則元 e）[9] が存在することである。

整数環 $\mathbf{Z}$ においては，a, b が同伴である必要十分条件は $a=\pm b$ である。

$\mathbf{R}$ の元 $q(\neq 0)$ が単元でなく，かつ q の約元は単元または同伴元に限るとき，q を $\mathbf{R}$ の既約元という，また $\mathbf{R}$ の元 $p(\neq 0)$ が単元でなく，かつ $p|ab$ (a, $b\in\mathbf{R}$) ならば $p|a$ または $p|b$ となるとき，p を $\mathbf{R}$ の素元という。（§ 1，定義 2 である。）

定理 7　整域 $\mathbf{R}$ において素元は既約元である。

証明　p を $\mathbf{R}$ の素元として，$p=bc$ (b, $c\in\mathbf{R}$) とする，素元の定義から，$p|b$ または $p|c$ となる。$p|b$ のとき，$b=pb'$ ($b'\in\mathbf{R}$) である。$p=bc=pb'c$。これより $p(1-b'c)=0$。$p\neq 0$ で，$\mathbf{R}$ が整域であるから $1-b'c=0$。これより $b'c=1$ すなわち b', c は単元である。従って b は p の同伴元且つ c は単元である。$p|c$ のときも同様に b は単元，c は p の同伴元になる。p の約元が単元または p の同伴元であることから，p は既約元である。 ■

整数環 $\mathbf{Z}$ においては

(i)　p は素数である

(ii)　p は $\mathbf{Z}$ の既約元である

(iii) p は $\mathbf{Z}$ の素元である

という三つの命題は同値であるが，一般に整域 $\mathbf{R}$ においては，定理 7 の逆がなりたたない例が知られている。すなわち一般の整域においては既約元は素元であるとは限らない。§3 において述べた $\mathbf{R}=\mathbf{Z}+\sqrt{-6}\,\mathbf{Z}=\{a+b\sqrt{-6}\mid a, b\in\mathbf{Z}\}$ で $\mathbf{R}$ の元 6 は

$$6=2\cdot 3=-\sqrt{-6}\cdot\sqrt{-6}$$

と表わされるが，2，3，$\pm\sqrt{-6}$ はみな既約元である。

整数環 $\mathbf{Z}$ における整除の理論の基本定理は定理 3 であった。それは

「任意の整数 a と $b(\neq 0)$ に対して

$$a=bq+r$$

となる q，$r\in\mathbf{Z}$，$0\leqq r<|b|$，が存在する」

であった[10]。一般に，整域 $\mathbf{R}$ の各元 $a\neq 0$ に整数 $\lambda(a)\geqq 0$ が対応して

(1) 任意の a，$b\in\mathbf{R}$，$b\neq 0$，に対して

$$a=bq+r$$

で $r=0$ または $\lambda(r)<\lambda(b)$ をみたす q，$r\in\mathbf{R}$ が存在する。

(2) $a\neq 0$，$b\neq 0$ に対して $\lambda(ab)\geqq\lambda(a)$ をみたすとき，$\mathbf{R}$ をユークリッド整域という。整数環 $\mathbf{Z}$ は，$\lambda(b)=|b|$ とおくことでユークリッド整域になる。

可換環 $\mathbf{R}$ において，$\mathbf{R}$ の部分集合 $\mathfrak{a}$ $(\neq\phi)$ が

(1) $\mathfrak{a}\ni a$，$b\Rightarrow a+b\in\mathfrak{a}$

(2) $\mathbf{R}\ni\lambda$，$\mathfrak{a}\ni a\Rightarrow\lambda a\in\mathfrak{a}$

をみたすとき，$\mathfrak{a}$ を $\mathbf{R}$ のイデアルという。

単位元 1 をもつ可換環 R の元 a_1，$\cdots a_s$ に対して，$r_1a_1+\cdots+r_sa_s$ $(r_i\in\mathbf{R},\ i=1,\ \cdots,\ s)$ の形の元全体を $(a_1,\ \cdots,\ a_s)$ で表わすと，$(a_1,\ \cdots,\ a_s)$ は R のイデアルである。これを元 a_1，$\cdots$，a_s により生成されるイデアルという。とくに一つの元 a により生成されるイデアル (a) を a により生成される単項イデアルという。

$\mathbf{R}$ のイデアルは単項イデアルとは限らないが，とくに $\mathbf{R}$ のイデアルがすべて単項イデアルであるような環 R を単項イデアル環という。

定理 8[11]　ユークリッド整域は単項イデアル整域である。

証明　ユークリッド整域 $\mathbf{R}$ の任意のイデアルを $\mathfrak{a}$ とする。$\mathfrak{a}=(0)$ なら $\mathfrak{a}$ は単項イデアルである。$\mathfrak{a}\neq(0)$ のとき，$\{\lambda(x)|x\in\mathfrak{a},\ x\neq 0\}$ は $\mathbf{N}\cup\{0\}$ の空でない部分集合であるから最小値が存在（定理 1）する。その最小値を与える $\mathfrak{a}$ の元を $a(\neq 0)$ とすれば $a=(a)$ である。実際，$\mathfrak{a}\ni{}^{\forall}b$ に対し，$b=aq+r$，$r\neq 0$，$\lambda(r)<\lambda(a)$ ならば $r=b-ag\in\mathfrak{a}$ であるから，a の最小性に反する。よって $r=0$，$b=aq$ となり $\mathfrak{a}\subseteq(a)$，$(a)\subseteq\mathfrak{a}$ はイデアルの定義より明かであるから $\mathfrak{a}=(a)$ である。 ■

整数環 $\mathbf{Z}$ は単項イデアル整域である。一般に，単位元をもつ可換環 $\mathbf{R}$ において，元 b が元 a_1，$\cdots$，a_r の約元であるとき，b を a_1，$\cdots a_r$ の公約元という。また，$d(\neq 0)$ が a_1，$\cdots$，a_r の公約元であり，a_1，$\cdots$，a_r の任意の公約元は d の約元であるとき，d を a_1，$\cdots$，a_r の最大公約元という。最大公約元は一般に存在するとは限らない。公倍元，最小公倍元も同様に定義する。

定理9　単項イデアル整域 $\mathbf{R}$ においては，$\mathbf{R}$ の元 $a_1, \cdots, a_r$ の最大公約元 d，最小公倍元 m が存在する。

証明　$\mathbf{R}$ のイデアルはすべて単項イデアルであるから $(a_1, \cdots, a_r)=(d)$ となる $d\in\mathbf{R}$ が存在する。この d が一つの最大公約元である。最小公倍元については $(a_1)\cap\cdots\cap(a_r)=(m)$ となる $m\in\mathbf{R}$ がそうである。■

d, d' を $a_1, \cdots, a_r$ の最大公約元とすれば，$d'=d\varepsilon$，ε は単元である。m についても同様である。

系　単項イデアル整域 $\mathbf{R}$ の元 $a_1, \cdots, a_r$ の最大公約元を d とすれば，$(a_1, \cdots, a_r)=(d)$ であり，$a_1x_1+\cdots+a_rx_r=d$ となる $x_1, \cdots, x_r\in\mathbf{R}$ が存在する。

定理10　単項イデアル整域の元 p に対して次の二つの命題は同値である。

(i)　p は素元である。

(ii)　p は既約元である。

証明　(i)⟹(ii)は一般の整域について成り立つ。(定理7)。(ii)⟹(i)。p を既約元として，$p|ab$ とする，a, p の最大公約元を d とすれば $d|p$ であるから d は $p\varepsilon$（ε は単元）の形の元または単元である。$d=p\varepsilon$ のとき $d|a$ でもあるから $p|a$。次に d が単元のとき，d は a, p の最大公約元であるから $ax+py=d$ となる x, $y\in\mathbf{R}$ をとれば，$d^{-1}ax+d^{-1}py=1$，これより $b=ab(d^{-1}x)+p(bd^{-1}y)$，$p|ab$，より $p|b$。よって p は素元である。■

整域 $\mathbf{R}$ において，$\mathbf{R}$ の単元でない元 $a(\neq0)$ はすべて有限個の素元の積 $a=p_1\cdots p_r$（p_i 素元）として表されるとき，$\mathbf{R}$ を素元分解整域という。整数環 $\mathbf{Z}$ は素元分解整域である。素元分解整域 $\mathbf{R}$ において $a=p_1\cdots p_r=q_1\cdots q_s$（$p_i$, q_i 素元）を二通りの素元の積とすれば，$r=s$ でありかつ q_i の順序を適当に並べかえれば p_i と q_i $(i=1, \cdots, r)$ は同伴となる。(§5，定理5の証明と同様にして証明できる。) それゆえ，素元分解整域のことを一意分解整域ともいう。

定理11　単項イデアル整域 $\mathbf{R}$ は素元分解整域である。

証明　$\mathbf{R}$ において既約元は素元であるから(定理10)，単元でない元 $a(\neq0)$ が有限個の既約元の積となることを示せばよい。a が有限個の既約元の積として表されないとすれば，a は既約元ではないから $a=a_1a_1'$，$(a_1)\neq(1)$，$(a_1')\neq(1)$ と分解され，a_1, a_1' の少なくとも一方は既約元でない。a_1 が既約元でなければ，$a_1=a_2a_2'$，$(a_2)\neq(1)$，$(a_2')\neq(1)$，a_2, a_2' のうち少なくとも一つは既約元でない，と分解される。このように続ければ，真に増大するイデアルの増大列

$$(a)\subsetneqq(a_1)\subsetneqq\cdots\subsetneqq(1)=\mathbf{R}$$

が得られる。このとき和集合 $\cup(a_i)$ もイデアルであるから，仮定により単項イデアル (b) である。$\cup(a_i)=(b)$ とすれば，b はある (a_n) に含まれるから $(a_n)=(a_{n+1})=\cdots$ となり，$(a_n)\subsetneqq(a$

$n+1$)$\subsetneq\cdots$に矛盾する。したがって，$\mathbf{R}$ の単元でない元 $a(\neq 0)$ はすべて有限個の既約元(したがって素元) の積として表される。 ■

§ 8. 多項式環

k を体とする[12]。a_0, …, $a_n \in k$ とするとき

$$f=f(X)=a_0+a_1X+\cdots+a_nX^n$$

の形の式を k の元を係数とする変数 X の多項式といい[13], $a_n\neq 0$ ならば n をその次数といって $\deg f$ で表す。k の元を係数とする変数 X の多項式全体の集合を $k[X]$ で表せば，多項式の通常の加法，乗法に関して $k[X]$ は整域となる。$k[X]$ を体 k の元を係数とする一変数 X の多項式環という。

定理 12 f, $g\in k[X]$, $g\neq 0$ に対して

$$f=gq+r \quad r=0 \text{ または } \deg r<\deg g$$

をみたす q, $r\in k[X]$ がただ一組存在する。

$\lambda(f)=\deg f$ とおいて，この定理は，$k[X]$ がユークリッド整域であることを示している。定理 12 は整数環 Z における定理 3 と同じ役割をはたしている。$k[X]$ はユークリッド整域であるから，単イデアル整域であり（定理 8），したがって素元分解整域（定理 11）である。

定理 13 体 k の元を係数とする 0 でない多項式 $f(X)$ は，$f(X)=ap_1(X)\cdots p_r(X)$ の形に定数と既約多項式 $p_i(X)$ の積に分解される。このとき多項式環 $k[X]$ のイデアル $(p_1(X)$, …, $(p_r(X))$ は順序を除いて一意的に定まる。

注

(1) 定理 1 は数学的帰納法と同値である。山口格：「数学的帰納法について――数学教育の立場からの考察――」，北海道大学教育学部教育方法学研究室「教授学の探究」第 5 号（1987 年）

(2) ここで使う例は次の書物からとった Rademacher • Toeplitz：「Von Zahlen und Figuren」Springer (1968).

(3) ブルバキ：「数学史」p. 103～104。東京図書（1970 年）。

(4) C. F. Gauss: Werke I. Olms Verlag. (1863 年)。復刻版（1981 年）。および，足立恒雄：「フェルマーの大定理――整数論の源流――」。日本評論社（1984 年）。

(5) 藤崎源二郎，森田康夫，山本芳彦：「数論への出発」，日本評論社（1980 年），第 1 章によった。

(6) この節では代数学の用語を説明なしに用いる。
くわしくは，ボレビッチ・シャハレビッチ：「整数論」(上)，佐々木義雄訳，吉岡書店，1971 年，をみよ。

(7) このことについては，足立恒雄：「フェルマーの大定理――整数論の源流――」，日本評論社，1984 年，をみよ。

(8) 可換環の定義。空集合でない集合 $\mathbf{R}$ で二種類の演算，加法 $(a, b)\to a+b$ と，乗法 $(a, b)\to ab$ が定義されていて，次の条件がみたされるとき，$\mathbf{R}$ はこれらの演算に関して環であるという。

1) $\mathbf{R}$ は加法に関してアーベル群である。すなわち $\mathbf{R}$ の任意の元 a, b, c に対して

$$(a+b)+c=a+(b+c) \text{（結合法則）}$$

が成り立ち，さらに $\mathbf{R}$ の任意の元 a に対して $a+0=0+a=a$ が成り立つ単位元 $0\in\mathbf{R}$ が存在し，$a+x=x+$

$a=0$ となる逆元 x（これを $-a$ と書く）$\in \mathbf{R}$ が存在する。そしてつねに $a+b=b+a$（交換法則）が成り立つ。

2) $\mathbf{R}$ の任意の元 a, b, c に対して結合法則

$(ab)c=a(bc)$

が成り立つ。

3) $\mathbf{R}$ の任意の元 a, b, c に対して，分配法則

$a(b+c)=ab+ac$, $(a+b)c=ac+bc$

が成り立つ。

環 R において，乗法に関して交換法則 $ab=ba$ が成り立つとき，$\mathbf{R}$ を可換環という。

(9) 一般に，乗法の単位元 1 をもつ環 $\mathbf{R}$ において，元 a が乗法に関して逆元 a^{-1}（$aa^{-1}=a^{-1}a=1$）をもつとき，a を正則元，単元，可逆元などとよぶ。a の逆元は存在すればただ一つである。

(10) 定理 3 では $b>0$ としておいたが，ここでは $b\neq 0$ としたので $0\leqq r<|b|$ と b に絶対値がつく。

(11) 定理 8～定理 11 の記法は(5)によった。

(12) 単位元をもつ可換環 $k(\neq\{0\})$ において，0 以外の任意の元 a が乗法の逆元 $a^{-1}\in k$, $aa^{-1}=1$ をもつとき，k は体であるという。

(13) これでは実は多項式の定義になっていない。多項式の定義をきちんとした形で述べるのは意外に面倒であるから，ここでは省略する。次の本を参照せよ。藤崎源二郎：「代数的整数論入門（上）」，裳華房（1975 年）。