2013年度藏野研究室卒業論文
“虚2次体の類数公式”

明治大学理工学部数学科
青木 省吾
荒井 悠介
達山 花純
戸塚 雄太
中ノ森 正貴
松並 奏史

平成26年2月26日

目 次

1　歴史・背景

定理 1.1 n を 3 以上の自然数とするとき、方程式

$$X^n + Y^n = Z^n$$

は非自明な整数解を持たない。

この定理は「Fermat[1]の最終定理」として知られ、およそ 360 年に渡り数学者達を悩ませ続けた。1630 年代に Fermat が古代ギリシャの数学者 Diophantus[2]の著作『算術』（Bachet[3]によって 1621 年に刊行されたギリシャ原典にラテン語訳が付されたもの）の中の方程式 $x^2 + y^2 = z^2$ の有理数解について論じられている部分の余白に Fermat の最終定理は書き残されたと言われている。この定理は 1994 年 9 月に Wiles[4]によって完全な証明が与えられたのだが、これに至るまでの多くの数学者達の努力は、大きく数学を発展させた。本論考では、そのうちの Kummer[5]の研究からそれを更に展開させた Dedekind[6]の研究の一端に触れる。

ζ_n を 1 の原始 n 乗根、つまり $\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ とおく。このとき Fermat の方程式 $x^n + y^n = z^n$ は

$$(x+y)(x+\zeta_n y)(x+\zeta_n^2 y)\cdots(x+\zeta_n^{n-1}y) = z^n$$

と「積=積」の形でかける為、

$$\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + \cdots + a_r\zeta_n^r \mid r \geq 0, a_0, \cdots, a_r \in \mathbb{Z}\}$$

内で整数環 $\mathbb{Z}$ と同様に「既約分解の一意性」が成立すれば、上の $x + \zeta_n^k y$ $(k = 0, 1, \cdots, n-1)$ や z を既約分解する事で、Fermat の最終定理は証明できる。しかし、実際には大抵の n に関して「既約分解の一意性」は $\mathbb{Z}[\zeta_n]$ で成り立たないのである。この「既約分解の一意性の不成立」は例えば、$\mathbb{Z}[\sqrt{-5}]$ のような世界でも生じてしまう。例えば 6 は $\mathbb{Z}[\sqrt{-5}]$ 内で、

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

[1]Pierre de Fermat (1601-1665) 国籍はフランス。職業は弁護士で数学は余暇に行ったものであると言われている。

[2]Diophantus (推定生年 200-214、推定没年 284-298) 古代ギリシャの数学者。彼の名にちなんだ Diophantus 方程式等の言葉もあり、「代数学の父」とも言われる。

[3]Claude-Gaspard Bachet de Mèziriac (1581-1638) フランスの数学愛好家。 1612 年に数学パズルに関する問題が書かれた Problèmes plaisants et delectables qui se font par les nombres を著した。この本は今でもペーパーバックで再販されている程の名著である。

[4]Andrew Wiles (1953-) イギリスの数学者。Oxford 大学教授。専門は整数論。

[5]Ernst Kummer (1810-1893) ドイツの数学者。Weierstrass、Kronecker とともに Berlin 大学の三大数学者として知られていた。最初は関数論を研究していたが、1840 年代から整数論を研究するようになった。

[6]Richard Dedekind (1831-1916) ドイツの数学者。実数の基礎付けを与えた Dedekind の切断でも知られる。Dirichlet の講義を元に作られた「整数論講義」の第二版補遺でイデアル等の基礎付けを与えた。

とかけるのだが、少し議論する事で 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ はどれもが $\mathbb{Z}[\sqrt{-5}]$ 内で同伴でない既約元であることがわかり、つまり少なくとも 6 は 2 通りの既約分解をもつ事が分かる。これを解消する為に Kummer はそれぞれを更に割り切るもの、つまり

$$2=\alpha^2,\ \ 3=\beta\gamma$$
$$1+\sqrt{-5}=\alpha\beta,\quad 1-\sqrt{-5}=\alpha\gamma$$

となるようなもの α, β, γ を**理想数** (complex ideal number) として導入した。この理想数を用いる事で「既約分解の一意性」（今の言葉でいうと、「整数環の素イデアル分解の一意性」）を示し、それを用いて Kummer は Fermat の最終定理を部分的に証明したのである。これは Kummer 以前の数学者たちの結果と比べて著しい進歩であった。この理想数の概念は後に Dedekind によって、**イデアル** (ideal) という概念として、厳密な定義が与えられた。

次の定理も、Fermat が『算術』の余白に残した命題である。

定理 1.2 N を平方数でない自然数とするとき、方程式

$$x^2-Ny^2=1$$

は無限個の自然数解を持つ。

例えば $N=2$ としたとき、

$$3^2-2\cdot 2^2=1,\quad 17^2-2\cdot 12^2=1\ ,\ \ 99^2-2\cdot 70^2=1$$

など、無限に自然数解を持つ。$x^2-Ny^2=1$ のような形をした方程式は Pell[7] 方程式と呼ばれる。ここで、

$$x^2-Ny^2=(x+\sqrt{N}y)(x-\sqrt{N}y)=1$$

と $\mathbb{Z}[\sqrt{N}]$ 内で表すことができ、これにより $x+\sqrt{N}y$ は $\mathbb{Z}[\sqrt{N}]$ 内の単元である事が分かる。後に示すが、$\mathbb{Z}[\sqrt{2}]$ の単元全体からなる集合（単数群）は $\{\pm(1+\sqrt{2})^n \mid n\in\mathbb{Z}\}$ となり、この集合が無限集合であることが、方程式 $x^2-2y^2=1$ が無限個の自然数解を持つ事の背後にある。この命題もまた、後に紹介する Dirichlet[8] の単数定理に深く関係しており、整数、有理数を超えた世界の一端を感じる事が出来る。

[7] John Pell (1611-1685) イングランドの数学者。Diophantus 方程式を好んで研究しており、よく講義でも扱っていた。他に Pell の名を冠する Pell 数というものがある。

[8] Gustav Peter Lejeune Dirichlet (1805-1859) ドイツの数学者。現代的形式の関数の定義 (関数を対応規則と解釈する方法) を与えた。また Fermat の最終定理の $n=5$ と $n=14$ の場合の証明を与えた。

最後にPythagoras[9]数に関するFermatの記述を紹介する。Fermatの方程式$x^n + y^n = z^n$において$n = 2$の場合、$x^2 + y^2 = z^2$の自然数解（Pythagoras数と言われる）は無数に存在する。Pythagoras数は古代から研究されていたのだが、次の定理のような素数とPythagoras数の関係を見出したのはFermatが初めてであった。

定理 1.3 *pが4で割ると1余る素数ならば、3辺の長さがどれも整数であり、かつ斜辺の長さがpであるような直角三角形が存在する。しかしpが4で割ると3余る素数であるときはそのような直角三角形は存在しない。*

この定理を示すには、次の命題が重要である。

命題 1.4 *pが4で割ると1余る素数なら*

$$p = x^2 + y^2$$

となる自然数$x,\ y$が存在する。しかしpが4で割ると3余る素数であるとき、$p = x^2 + y^2$をみたすx, yは、有理数すら存在しない。

この命題の証明ではGauss[10]の宝玉とも言われる「平方剰余の相互法則」の第一補充法則として知られる命題『pが4で割って1余る素数なら、$x^2 \equiv -1 \pmod{p}$を満たす整数xが存在し、pが4で割って3余る素数ならこのようなxは存在しない』が鍵となっている。この命題から少し議論を深める事でpが4で割って1余るような素数、例えば5や13のとき、

$$5 = 2^2 + 1^2 = (2 + i)(2 - i)$$
$$13 = 3^2 + 2^2 = (3 + 2i)(3 - 2i)$$

というように、$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$の中で「素数」としての性質を失ってしまうことが示される。それに対し4で割って3余るような素数は$\mathbb{Z}[i]$内でも「素数」としての性質を保ったままであることがわかる。更に$\mathbb{Z}[i]$は「素元分解の一意性」が成り立つ世界であることを用いて命題1.4は示され、

$$5^2 = (2 + i)^2(2 - i)^2 = 3^2 + 4^2$$
$$13^2 = (3 + 2i)^2(3 - 2i)^2 = 5^2 + 12^2$$

[9]Pythagoras (紀元前582-紀元前496) 古代ギリシャの数学者、哲学者。彼の数学や輪廻転生についての思想はPlatonにも大きな影響を与えた。Pythagoras教団を立ち上げ、そこでは数学における様々な定理が発見された。しかしこの時代に関する資料があまりにも少ない為、Pythagorasという人物の実在性を疑問視する声もある。

[10]Carl Friedrich Gauss (1777-1855) ドイツの数学者、天文学者、物理学者。近代数学のほぼ全ての分野に多大な影響を与えた。また代数学の基本定理を最初に証明したのもGaussである。1801年に出版されたDisquisitiones Arithmeticaeは、数論の分野で非常に重要なGaussの著作である。

というように命題 1.4 を用いて定理 1.3 を示す事が出来る。このように有理数の世界から少し広い世界にでる事で、この定理の本質を捉える事が出来る。

以上で見たように、Fermat が『算術』の余白に書き残したいくつもの命題は、一見すると整数もしくは有理数の世界だけでの話のように思えるが、その当時、つまり 17 世紀前半には考えられない程深遠な世界の一部を垣間みることの出来るものであった。このような理論は、後に「代数的整数論」として 1 つの大きな体系をなすのであった。

上で見たように代数体の整数環は一意分解整域である場合もあれば、そうでない場合もある。本論考では、「代数体の整数環はどのような場合に一意分解整域になるのか」ということを知る為の大きな手掛かりとなる代数体の**類数** (class number) を求める公式、すなわち**類数公式**を、特に代数体が虚 2 次体である場合のものを紹介することを目標とした。以下はその類数公式を理解する為に必要な理論をまとめたものである。

2　代数体、整数環

ここからの章では代数的整数論の核心的事項にふれる。この章では「代数体の整数環」について述べる。

定義 2.1 有理数体の有限次拡大体を、**代数体**(algebraic number field) と呼ぶ。

定義 2.2 代数体 K の部分集合 O_K を次のように定める。

ある $n > 0$ に対して $\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$ をみたす $c_1, \cdots, c_n \in \mathbb{Z}$ が存在するような K の元 α の全体の集合を O_K と書き、これを代数体 K の**整数環** (ring of integers) という。

定理 6.3.4 より O_K は K の部分環になる。

例えば、代数体 $K = \mathbb{Q}(\zeta_n)$ のときに $O_K = \mathbb{Z}[\zeta_n] = \{\sum_{k=0}^{n-1} a_k\zeta_n^k \mid a_k \in \mathbb{Z}\}$ となることが知られている。ζ_n とは 1 の原始 n 乗根 $\cos(2\pi/n) + i\sin(2\pi/n)$ の事であり、ζ_n^k は ζ_n の k 乗の意味である。この事を示すのは容易ではない。

K が二次体の場合、O_K は次のようになる。

定理 2.3 m は 1 以外の平方数で割れず、1 でない整数とする。$K = \mathbb{Q}(\sqrt{m})$ とする。このとき,

$$O_K = \begin{cases} \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} & m \equiv 2, 3 \mod 4 \text{ のとき} \\ \mathbb{Z}\left[\dfrac{1+\sqrt{m}}{2}\right] = \left\{a + b\dfrac{1+\sqrt{m}}{2} \mid a, b \in \mathbb{Z}\right\} & m \equiv 1 \mod 4 \text{ のとき} \end{cases}$$

が成立する。

証明　m は 1 以外の平方数で割れない 1 でない整数, $K = \mathbb{Q}(\sqrt{m})$ とする。$K = \mathbb{Q} + \mathbb{Q}\sqrt{m}$ に注意する。

$\alpha = x + y\sqrt{m} \in K$ をとり $(x, y \in \mathbb{Q})$、それに対して $\alpha' = x - y\sqrt{m} \in K$ をとる。

最初に $\alpha \in O_K$ であることと、$\alpha + \alpha' = 2x$, $\alpha\alpha' = x^2 - my^2$ がともに $\mathbb{Z}$ に入る事が同値であることを示す。

まず $\alpha \in O_K$ と仮定する。このとき、$\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$ となる $c_1, \cdots c_n \in \mathbb{Z}$ が存在する。$\varphi(a + b\sqrt{m}) = a - b\sqrt{m}$ で定まる写像 φ が環準同型写像であることより $(\alpha')^n + c_1(\alpha')^{n-1} + \cdots + c_n = 0$ と書け、$\alpha' \in O_K$ がわかる。従って $\alpha + \alpha', \alpha\alpha' \in O_K$ となる。よって、$\alpha + \alpha'$, $\alpha\alpha'$ は、$O_K \cap \mathbb{Q}$ に入る。あと、$O_K \cap \mathbb{Q} = \mathbb{Z}$ を示せばよい。$a/b \in O_K \cap \mathbb{Q}$, $(a, b) = 1$ をとれば[11]、

$$(a/b)^n + d_1 (a/b)^{n-1} + \cdots + d_n = 0$$

を満たす $n > 1$, $d_1, \cdots, d_n \in \mathbb{Z}$ が存在するので、$a^n = -b(d_1 a^{n-1} + bd_2 a^{n-2} + \cdots + d_n b^{n-1})$ となる。このとき $(a, b) = 1$ より $b = \pm 1$ となる。従って $a/b \in \mathbb{Z}$ となるので $O_K \cap \mathbb{Q} = \mathbb{Z}$ である事がわかった。よって $\alpha + \alpha'$, $\alpha\alpha'$ は $O_K \cap \mathbb{Q} = \mathbb{Z}$ に属する。

逆に $\alpha + \alpha' \in \mathbb{Z}$, $\alpha\alpha' \in \mathbb{Z}$ と仮定する。$d_1 = -(\alpha + \alpha')$, $d_2 = \alpha\alpha'$ とすると $\alpha^2 + d_1\alpha + d_2 = 0$ を満たすので α は O_K に属する。

次に $x, y \in \mathbb{Q}$ に対して、

(1) $m \equiv 2, 3 \mod 4$ の場合は、$2x, x^2 - my^2 \in \mathbb{Z}$ である事と $x, y \in \mathbb{Z}$ が同値である

(2) $m \equiv 1 \mod 4$ の場合は、$2x, x^2 - my^2 \in \mathbb{Z}$ である事と $2x, 2y, x - y \in \mathbb{Z}$ であることが同値である

ことを示す。

ここで素数 p と有理数 $a \neq 0$ に対して、a の p 進付値を、次のように定義する。

定義 2.4 素数 p と有理数 $a \neq 0$ に対し、a の p 進付値 $\mathrm{ord}_p(t)$ を、$a = p^m \dfrac{u}{v}$, $m \in \mathbb{Z}$ かつ u, v は p で割れない整数と書いたときの m と定義する。つまり $\mathrm{ord}_p(a)$ は a が p の何乗できっかり割り切れるかをあらわす。$m < 0$ となることもある事に注意する。また、次が成り立つことに注意する。

(1) $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$

(2) $\mathrm{ord}_p(a + b) \geq \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$

(3) $\mathrm{ord}_p(a) \neq \mathrm{ord}_p(b)$ なら $\mathrm{ord}_p(a + b) = \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$

[11] $(a, b) = \gcd(a, b)$

定義 2.4 を使い、まず $x, y \in \mathbb{Q}$ で $2x, x^2 - my^2 \in \mathbb{Z}$ なら $2y \in \mathbb{Z}$ となることを示す。

p を奇素数とする。$x^2 - my^2 \in \mathbb{Z}$ より $\mathrm{ord}_p(x^2 - my^2) \geq 0$ である。また、$\mathrm{ord}_p(x^2) \geq 0$ より、$\mathrm{ord}_p(m) + 2\mathrm{ord}_p(y) < 0$ とすれば $\mathrm{ord}_p(x^2 - my^2) = \mathrm{ord}_p(m) + 2\mathrm{ord}_p(y) < 0$ となり矛盾する。従って $\mathrm{ord}_p(m) + 2\mathrm{ord}_p(y) \geq 0$ となる。$\mathrm{ord}_p(m) \leq 1$ より $2\mathrm{ord}_p(y) \geq -1$ である。よって $\mathrm{ord}_p(y) \geq 0$ である。

また $x^2 - my^2 \in \mathbb{Z}$ より $\mathrm{ord}_2(x^2 - my^2) \geq 0$ である。また $\mathrm{ord}_2(x) \geq -1$ なので、$\mathrm{ord}_2(x^2) = 2\mathrm{ord}_2(x) \geq -2$ となるから、$\mathrm{ord}_2(m) + 2\mathrm{ord}_2(y) < -2$ とすれば $\mathrm{ord}_2(x^2 - my^2) = \mathrm{ord}_2(m) + 2\mathrm{ord}_2(y) < -2$ となり矛盾する。従って $\mathrm{ord}_2(m) + 2\mathrm{ord}_2(y) \geq -2$ となる。$\mathrm{ord}_2(m) \leq 1$ より $2\mathrm{ord}_2(y) \geq -3$ よって $\mathrm{ord}_2(y) \geq -1$ である。有理数 z に対して、$z \in \mathbb{Z}$ であることと、任意の素数 p に対して $\mathrm{ord}_p(z) \geq 0$ であることは同値である。以上より $2y \in \mathbb{Z}$ となる。

(1) $m \equiv 2, 3 \mod 4$ の場合、$2x, x^2 - my^2 \in \mathbb{Z}$ である事と $x, y \in \mathbb{Z}$ が同値であることを示す。

$x, y \in \mathbb{Z}$ のとき $2x, x^2 - my^2 \in \mathbb{Z}$ となる事は明らかである。$2x, x^2 - my^2 \in \mathbb{Z}$ であり、$x, y \notin \mathbb{Z}$ と仮定する。x, y のどちらかが $\mathbb{Z}$ に含まれ、片方が $\mathbb{Z}$ に含まれないときは、$x^2 - my^2 \notin \mathbb{Z}$ となることは明らかである。どちらも $\mathbb{Z}$ に含まれないときは、$x = \dfrac{2x'+1}{2}$, $y = \dfrac{2y'+1}{2}$ $(x', y' \in \mathbb{Z})$ とかける。このとき $x^2 - my^2 = \alpha + \dfrac{1-m}{4} \notin \mathbb{Z}$ $(\alpha \in \mathbb{Z})$ となり矛盾する。

(2) $m \equiv 1 \mod 4$ の場合、$2x, x^2 - my^2 \in \mathbb{Z}$ である事と $2x, 2y, x - y \in \mathbb{Z}$ であることが同値であることを示す。

$2x, 2y, x - y \in \mathbb{Z}$ と仮定して、$2x$, $x^2 - my^2 \in \mathbb{Z}$ を示す。このとき $x, y \in \mathbb{Z}$、または $x = \dfrac{2x'+1}{2}$, $y = \dfrac{2y'+1}{2}$ $(x', y' \in \mathbb{Z})$ と書ける。$x, y \in \mathbb{Z}$ のときは明らかである。$x = \dfrac{2x'+1}{2}$, $y = \dfrac{2y'+1}{2}$ のときを考える。このとき、$x^2 - my^2 = \alpha + \dfrac{1-m}{4}$ $(\alpha \in \mathbb{Z})$ となり、$2x, x^2 - my^2 \in \mathbb{Z}$ を満たす。

次に $2x, x^2 - my^2 \in \mathbb{Z}$ と仮定する。x については $x = \dfrac{2x'+1}{2}$ 又は $x = x'$ $(x' \in \mathbb{Z})$ ととれる。y についても、$2y \in \mathbb{Z}$ より、$y = \dfrac{2y'+1}{2}$ 又は $y = y'$ $(y' \in \mathbb{Z})$ ととれる。$x - y \notin \mathbb{Z}$ と仮定すると、これを満たす組み合わせは $x = \dfrac{2x'+1}{2}, y = y'$ 又は $x = x', y = \dfrac{2y'+1}{2}$ である。しかしこのとき、それぞれ $x^2 - my^2 = \alpha + \dfrac{1}{4}$, $x^2 + my^2 = \beta + \dfrac{-m}{4}$ $(\alpha, \beta \in \mathbb{Z})$ とかけ $x^2 - my^2 \notin \mathbb{Z}$

となり仮定に矛盾する。

以上の事から $m \equiv 2, 3 \mod 4$ の時は、$x + y\sqrt{m} \in O_K$ である事と $x, y \in \mathbb{Z}$ であることが同値となり、$O_K = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$ が示された。
また、$m \equiv 1 \mod 4$ の時は、$x + y\sqrt{m} \in O_K$ であることと、$2x, 2y, x - y \in \mathbb{Z}$ が同値である。$2x, 2y, x - y \in \mathbb{Z}$ と仮定すると、$x, y \in \mathbb{Z}$ または $x = \dfrac{2x' + 1}{2}$, $y = \dfrac{2y' + 1}{2}$ $(x', y' \in \mathbb{Z})$ と書けるので、$x + y\sqrt{m}$ がそれぞれ $x - y + 2y\dfrac{1 + \sqrt{m}}{2}$, $x' - y' + (2y' + 1)\dfrac{1 + \sqrt{m}}{2}$ を満たす。よって $\alpha = x + y\sqrt{m} \in O_K$ である事と $\alpha = a + b\dfrac{1 + \sqrt{m}}{2}$ $(a, b \in \mathbb{Z})$ と書けることが同値となり、$O_K = \left\{a + b\dfrac{1 + \sqrt{m}}{2} \mid a, b \in \mathbb{Z}\right\}$ が示された。 **証明終**

定理 2.3 により、K が二次体であるときは O_K は有限生成 $\mathbb{Z}$-加群であり、特に O_K は Noether 環である。一般の代数体 K においても、定理 6.4.17 によって、O_K は有限生成 $\mathbb{Z}$-加群であり、Noether 環になる。

3 イデアル類群、単数群

定義 3.1 K を代数体とする。K の部分集合 $\mathfrak{a}$ が O_K の**分数イデアル**(fractional ideal) であるとは、次の同値な条件 (1), (2) をみたすことである。

(1) O_K の 0 でない元 c があって、$c\mathfrak{a}$ は O_K の 0 でないイデアルになる。

(2) $\mathfrak{a}$ は K の 0 でない有限生成部分 O_K-加群である。

上の (1), (2) の同値性は、O_K が Noether 環であることからわかる。

定義 3.2 $K^\times$ の元 α に対し、分数イデアル αO_K を (α) と書く。(α) の形の分数イデアルを主分数イデアルという。

定義 3.3 K を代数体とする。K の分数イデアル $\mathfrak{a}, \mathfrak{b}$ に対し、$\displaystyle\sum_{i=1}^{n} a_i b_i$ $(n \geq 1, a_i \in \mathfrak{a}, b_i \in \mathfrak{b})$ の形の元全体を $\mathfrak{a}$ と $\mathfrak{b}$ の積と定義し、$\mathfrak{ab}$ と書く。$\mathfrak{ab}$ は O_K の分数イデアルである。

分数イデアル $\mathfrak{a}$ に対して、

$$(O_K : \mathfrak{a}) = \{x \in K \mid x\mathfrak{a} \subset O_K\}$$

と定めると、$(O_K : \mathfrak{a})$ も分数イデアルである。このとき、$\mathfrak{a} \cdot (O_K : \mathfrak{a}) = O_K$ となり、つまり、$(O_K : \mathfrak{a})$ はこの積に関して $\mathfrak{a}$ の逆元になることが知られている。つま

り今の場合、分数イデアル全体は、積に関して群となる。二つの主分数イデアルの積は主分数イデアルなので、主分数イデアル全体は、この群に関して部分群になっている。

定義 3.4 K を代数体とする。

(1) K の**イデアル類群**とは、O_K の分数イデアル全体が積についてなす群を主分数イデアル全体のなす部分群で割った商群のことである。K のイデアル類群を $Cl(K)$ または $Cl(O_K)$ と書く。またイデアル類群の位数を、その代数体の**類数**(class number) という。

(2) K の**単数群**とは、O_K の可逆元全体のなす乗法群 $O_K^\times$ のことである。

定理 4.1 によって、類数は有限である。

補題 3.5 K を代数体とすると次の (i), (ii), (iii) は同値。

(i) $Cl(K)$ は単位元のみからなる群。

(ii) O_K は主イデアル整域。

(iii) O_K は一意分解整域。

証明 (i) から (ii) を示す。I を O_K の分数イデアル全体のなす群とし、P を O_K の主分数イデアル全体のなす群とする。$Cl(K) = I/P$ であったので、

$$Cl(K) = I/P = \{\bar{e}\} \Leftrightarrow I = P$$

となる。O_K のイデアルは分数イデアルであるので、$I = P$ より (分数イデアルは主分数イデアルであり) O_K は主イデアル整域である。

(ii) から (iii) は一般に主イデアル整域であれば一意分解整域であることからわかる。

(iii) から (ii) を示す。後に示す事であるが、代数体の整数環の全てのイデアルは素イデアル分解が可能であることから、O_K のすべての素イデアルが主イデアルとなることを示せば十分である。

$\mathfrak{p}$ を O_K の (0) 以外の素イデアルとし、$\mathfrak{p}$ の 0 でない元 α をとる。O_K は一意分解整域であるので、

$$\alpha = q_1 q_2 \cdots q_n \qquad (q_i : O_K\text{の素元})$$

と書ける。$\mathfrak{p}$ が素イデアルであるので、$q_i \in \mathfrak{p}$ をみたす i が存在する。従って、

$$(q_i) \subseteq \mathfrak{p}$$

となる。また、Dedekind 整域では (0) 以外の素イデアルは極大イデアルであるので、

$$(q_i) = \mathfrak{p}$$

である。つまり O_K の全ての素イデアルは主イデアルである。

(ii) から (i) を示す前に、次の補題を示す。

補題 3.6 J を O_K の 0 でないイデアル全体の集合とする。$\mathfrak{a}, \mathfrak{b} \in J$ について、

$$\mathfrak{a} \sim \mathfrak{b} \overset{def}{\Leftrightarrow} \mathfrak{a} \text{ と } \mathfrak{b} \text{ は } O_K\text{-加群として同型}$$

と関係 $\sim$ を定める。このとき、$\sim$ は同値関係であり、

$$J/\sim \ \simeq \ Cl(K) \tag{♯}$$

である。

証明 まず、写像 f を $J \hookrightarrow I \to I/P = Cl(K)$ の合成射と置いたとき、$\mathfrak{a}, \mathfrak{b} \in J$ について,

$$f(\mathfrak{a}) = f(\mathfrak{b}) \Leftrightarrow \mathfrak{a} \sim \mathfrak{b} \tag{$*$}$$

を示す。

($\Rightarrow$) $f(\mathfrak{a}) = f(\mathfrak{b})$ より $\mathfrak{a} = (u)\mathfrak{b}$ となる $u \in K^\times$ が存在する。写像 g を $g : \mathfrak{b} \to \mathfrak{a}\ ;\ t \mapsto ut$ と定める。すると、明らかに g は O_K-加群の同型写像であるので、$\mathfrak{a} \sim \mathfrak{b}$ が言えた。

($\Leftarrow$) $\mathfrak{a} \sim \mathfrak{b}$ より、O_K-同型写像 $\varphi : \mathfrak{a} \to \mathfrak{b}$ がとれる。

任意の 0 でない $a, b \in \mathfrak{a}$ について、

$$\varphi(ab) = a\varphi(b) = b\varphi(a)$$

より、

$$\frac{\varphi(a)}{a} = \frac{\varphi(b)}{b}$$

が成立する。ここで、$\rho = \varphi(b)/b$ と定めると、任意の $a \in \mathfrak{a}$ に対し $\varphi(a) = a\rho$ と書ける。φ の全射性より $\rho\mathfrak{a} = \mathfrak{b}$ が成立し、$f(\mathfrak{a}) = f(\mathfrak{b})$ がわかる。以上で $(*)$ の証明は完了した。

ここで、任意の $\mathfrak{a} \in I$ に対して、$\mathfrak{a}$ が分数イデアルである事から $b\mathfrak{a} \in J$ をみたす $b \in O_K \backslash \{0\}$ が存在する。すると

$$f(b\mathfrak{a}) = \overline{b\mathfrak{a}} = \bar{\mathfrak{a}}$$

であるので、f が全射であることがわかる。f の全射性と $(*)$ より、(♯) が従う。

証明終

(ii) から (i) を示す。まず、任意の 0 でない二つの主イデアルは O_K-加群として同型であることを示す。(a) を 0 でない任意の主イデアルとし、

$$O_K \overset{\varphi_a}{\to} (a)$$

を、

$$\varphi_a(x) = xa$$

と定める。これは明らかに O_K-加群の同型写像である。同型という関係は同値関係なので、0 でないすべての主イデアルが O_K-加群として同型であることがわかった。すると、補題 3.6 より $J/\sim \simeq Cl(K)$ なので、$|J/\sim| = |Cl(K)|$ である。そして最初の議論から $|J/\sim| = 1$ となるので、$|Cl(K)| = 1$ となる。　　証明終

例 3.7 $\mathbb{Z}$ は一意分解環である。よって、$K = \mathbb{Q}$ のとき、$Cl(\mathbb{Q}) = \{\bar{e}\}$ であり、$\mathbb{Q}$ の単数群は $\mathbb{Z}^\times = \{\pm 1\}$ である。

イデアル類群と単数群の意味と重要性を述べる。

$a \in K^\times$ をとり、$a \mapsto (a)$ で定まる群準同型写像 $g : K^\times \to I$ を考える。すると、$\mathrm{Im}\, g = P$ であるので、

$$\mathrm{Coker}\ g = I/\mathrm{Im}\, g = I/P = Cl(K)$$

となる。また $\mathrm{Ker}\, g = O_K^\times$ に注意する。よって、

$$1 \longrightarrow O_K^\times \longrightarrow K^\times \xrightarrow{g} I \longrightarrow Cl(K) \longrightarrow 0$$

という完全列がある。一般に準同型写像 f に対し、

$$f \text{ が同型写像} \Leftrightarrow \mathrm{Ker}\, f = \mathrm{Coker} f = 0$$

であることから、イデアル類群や単数群は“数とイデアルのずれ”を表していると考えられる。また、イデアル類群は、補題 3.5 より“素元分解の法則の成り立たなさ”を表しているとも考えられる。そして、単数群についても素元分解に大きく影響する。例えば、$\mathbb{Z}[\sqrt{2}]$ における 7 の既約分解を考えると、

$$\begin{aligned} 7 &= (3+\sqrt{2})(3-\sqrt{2}) \\ &= (5+3\sqrt{2})(5-3\sqrt{2}) \\ &= (27+19\sqrt{2})(27-19\sqrt{2}) \\ &= \cdots \end{aligned} \tag{1}$$

このようにいくつもの既約分解を得るが、$3+\sqrt{2} = (5-3\sqrt{2})(1+\sqrt{2})^2$ からわかるように 7 のたくさんの既約分解 (1) は、$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$ の元をかけてずらしたものなので、同伴を除いて一意的である。このように、代数体 K のイデアル類群や単数群は、O_K における数の法則が $\mathbb{Z}$ における法則とどれくらい異なっているかを表していると考えられる。

4　代数的整数論の二大定理

ここでは、イデアル類群と単数群という代数体に関する 2 つの重要な群についての 2 つの定理を紹介する。定理の証明は容易でないため、ここでは与えない。

定理 4.1 (類数の有限性定理) 代数体のイデアル類群は有限群である。

次に Dirichlet の単数定理について述べるために必要な、実素点、複素素点の定義を述べる。

定義 4.2 K を代数体とする。

(1) K の実素点とは、K から $\mathbb{R}$ への環準同型のことである。

(2) K の複素素点とは、K から $\mathbb{C}$ への環準同型 σ のうち $\sigma(K) \subset \mathbb{R}$ とならないもののことである。ただし、そのような σ とその複素共役 $\overline{\sigma} : K \to \mathbb{C}$ (ただし、$x \mapsto \overline{\sigma(x)}$) は同じ複素素点を定めるとする。

定理 4.3 (Dirichlet の単数定理) 代数体の単数群は有限生成アーベル群である。さらに、代数体 K の実素点、複素素点の個数をそれぞれ r_1、r_2 とし、$r = r_1 + r_2 - 1$ とおくと、

$$O_K^\times \cong \mathbb{Z}^{\oplus r} \oplus \text{(有限巡回群)}$$

となる。ここで「有限巡回群」とは、K に属する 1 のベキ根全体のなす乗法群である。

以上の定理の証明を与えることはできないが、例をあげよう。

例 4.4 $K = \mathbb{Q}(\sqrt{2})$ のときを考える。このとき、定理 2.3 より $O_K = \mathbb{Z}[\sqrt{2}]$ である。$\sqrt{2}$ の最小多項式は $x^2 - 2$ であり、$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ となるので、$r_1 = 2, r_2 = 0$ である。Dirichlet の単数定理より、$r = r_1 + r_2 - 1 = 2 + 0 - 1 = 1$ とわかり、

$$O_K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

となる。以下、

$$O_K^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$$

であることを、証明する。(Dirichlet の単数定理から直ちにわかることではあるが、上の右辺の群は、$\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ と同型である)。

証明 $O_K = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ に注意する。ここで、

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$$

となることを証明する。

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

より、$1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ である。よって、任意の n に対して、$\pm(1 + \sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^\times$ となる。このことより、$\{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\} \subset \mathbb{Z}[\sqrt{2}]^\times$ となる。

逆に、任意の元 $\alpha \in \mathbb{Z}[\sqrt{2}]^\times$ をとる。$-1 \in \mathbb{Z}[\sqrt{2}]^\times$ より、必要なら -1 倍することにより $\alpha > 0$ ととることができる。また、$0 < \beta \leq \alpha < (1+\sqrt{2})\beta$ を満たす $\beta \in \{(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$ が存在することがわかる。特に $\beta \in \mathbb{Z}[\sqrt{2}]^\times$ に注意すると、$1 \leq \dfrac{\alpha}{\beta} < 1+\sqrt{2}$ であり、$\dfrac{\alpha}{\beta} \in \mathbb{Z}[\sqrt{2}]^\times$ である。ここで、$\dfrac{\alpha}{\beta} \neq 1$、つまり、$1 < \dfrac{\alpha}{\beta} < 1+\sqrt{2}$ と仮定する。$\dfrac{\alpha}{\beta} = x + y\sqrt{2}$ $(x, y \in \mathbb{Z})$ とおくと、$(x+y\sqrt{2})(a+b\sqrt{2}) = 1$ を満たすような a、$b \in \mathbb{Z}$ が存在する。よって、$(ax+2by) + (bx+ay)\sqrt{2} = 1$ となり、1 と $\sqrt{2}$ の $\mathbb{Q}$ 上の線形独立性により、$ax + 2by = 1$ かつ $bx + ay = 0$ である。よって、$-bx - ay = 0$ であるので、

$$(x - y\sqrt{2})(a - b\sqrt{2}) = (ax + 2by) + (-bx - ay)\sqrt{2} = 1 + 0 \times \sqrt{2} = 1$$

であるので、

$$(x + y\sqrt{2})(x - y\sqrt{2})(a + b\sqrt{2})(a - b\sqrt{2}) = (x^2 - 2y^2)(a^2 - 2b^2) = 1$$

である。従って

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

となる。故に、$x - y\sqrt{2} = \dfrac{\pm 1}{x + y\sqrt{2}}$ となるが、$\dfrac{\alpha}{\beta} = x + y\sqrt{2} > 1$ より、$-1 < x - y\sqrt{2} = \dfrac{\pm 1}{x + y\sqrt{2}} < 1$ となる。各辺に、$1 < x + y\sqrt{2} < 1 + \sqrt{2}$ を加えると、$0 < 2x < 2 + \sqrt{2}$ となり、$x = 1$ を得る。$1 < x + y\sqrt{2} < 1 + \sqrt{2}$ に $x = 1$ を代入し、$1 < 1 + y\sqrt{2} < 1 + \sqrt{2}$ より $0 < y\sqrt{2} < \sqrt{2}$ となるが、これは $y \in \mathbb{Z}$ に矛盾する。よって $\dfrac{\alpha}{\beta} = 1$ であり、$\alpha = \beta \in \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$ となる。 **証明終**

5 虚二次体の類数公式

定義 5.1 p を奇素数とし、a を p で割れない整数とする。平方剰余記号 $\left(\dfrac{a}{p}\right) \in \{\pm 1\}$ を、次のように定める。$\mathbb{F}_p$ において a の平方根が存在するとき（すなわち $x^2 \equiv a \pmod{p}$ となる整数 x が存在するとき）$\left(\dfrac{a}{p}\right) = 1$ と定め、存在しないとき $\left(\dfrac{a}{p}\right) = -1$ とする。

注意 5.2 $a, b \in \mathbb{Z}$ がどちらも p で割れない整数とすると

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

が成り立つ。これは、乗法群 $\mathbb{F}_p^\times$ の部分群 $\{a^2 \mid a \in \mathbb{F}_p^\times\}$ を考えれば、明らかである。

Gauss による平方剰余の相互法則を紹介する。ここでは証明しない。

定理 5.3　(1) q を p と異なる奇素数とするとき、

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

が成立する。

(2) 奇素数 p に対して、次が成立する[12]。

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod 4 \text{ のとき} \\ -1 & p \equiv 3 \pmod 4 \text{ のとき} \end{cases}$$

以下、K を虚 2 次体（$\mathbb{R}$ に入らない $\mathbb{Q}$ 上の 2 次拡大体）とする。すなわち $K = \mathbb{Q}(\sqrt{m})$ で、m は 1 以外の平方数でわりきれない整数で $m < 0$ としてよい。ここで、

$$N = \begin{cases} |m| & m \equiv 1 \pmod 4 \text{ のとき} \\ |4m| & m \equiv 2, 3 \pmod 4 \text{ のとき} \end{cases}$$

とおく。

定義 5.4 環 $\mathbb{Z}/N\mathbb{Z}$ の可逆元全体の乗法群 $(\mathbb{Z}/N\mathbb{Z})^\times$ から 0 でない複素数全体の乗法群 $\mathbb{C}^\times$ への群準同型

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

を、(mod N の)**Dirichlet 指標**という。

Dirichlet 指標 χ で、m を割らない全ての奇素数 p について

$$\chi(p \bmod N) = \left(\frac{m}{p}\right) \qquad (\#)$$

をみたすものが、ただ一つ存在する。(存在すれば、一意性は、$(\mathbb{Z}/N\mathbb{Z})^\times$ が N と互いに素な素数の類で生成されることから明らかであろう。)

実際 χ は、次のように具体的にあらわされる。

N と互いに素な整数 a に対し、

$$\left(\prod_l \left(\frac{a}{l}\right)\right) \cdot \theta(a) \qquad (*)$$

を考える。ただし、l は m を割りきる奇素数すべてをわたり、$\theta(a)$ は以下のように定める。

[12] この式は、平方剰余の第一補充法則、あるいは Euler の基準と呼ばれる。

(1) $m \equiv 1 \pmod 4$ の場合、$\theta(a) = 1$。

(2) $m \equiv 3 \pmod 4$ の場合、$a \equiv 1 \pmod 4$ なら $\theta(a) = 1$、$a \equiv 3 \pmod 4$ なら $\theta(a) = -1$。

(3) m が偶数の場合。$a \equiv 1, 1-m \pmod 8$ なら $\theta(a) = 1$、そうでなければ $\theta(a) = -1$。

式 $(*)$ に出てくる a に対して $\left(\frac{a}{l}\right)$ や $\theta(a)$ を対応させる写像は、$(\mathbb{Z}/N\mathbb{Z})^\times$ から $\mathbb{C}^\times$ への群準同型、つまり Dirichlet 指標になる。よって、$(*)$ 自身も、Dirichlet 指標になる。

この式が $(\#)$ を満たすことを示せばよい。

(1) の場合に、$(*)$ が $(\#)$ を満たすことを示す。すなわち、$m \equiv 1 \pmod 4$ であるとき

$$\left(\frac{m}{p}\right) = \prod_l \left(\frac{p}{l}\right) \qquad (+)$$

とかける事を示す。$m = -l_1 l_2 \cdots l_s$ とする（l_i は奇素数）。平方剰余の相互法則を用いると

$$\left(\frac{m}{p}\right) = \left(\frac{-\,l_1 l_2 \cdots l_s}{p}\right) = (-1)^{\frac{p-1}{2}(1+\frac{l_1-1}{2}+\cdots+\frac{l_s-1}{2})} \cdot \left(\frac{p}{l_1}\right) \cdots \left(\frac{p}{l_s}\right)$$

となる。$l_1 l_2 \cdots l_s = -m$ より、$l_1 l_2 \cdots l_s \equiv 3 \pmod 4$ である。よって $l_1 l_2 \cdots l_s$ の中に $l_i \equiv 3 \pmod 4$ となるような i は奇数個あり、他は全て $l_j \equiv 1 \pmod 4$ となる。$l_j \equiv 1 \pmod 4$ のときに $\frac{l_j-1}{2}$ は偶数、$l_i \equiv 3 \pmod 4$ のときに $\frac{l_i-1}{2}$ は奇数になることに注意すると、$\frac{l_1-1}{2}, \ldots, \frac{l_s-1}{2}$ の中に奇数は奇数個あることがわかる。よって $\frac{l_1-1}{2} + \cdots + \frac{l_s-1}{2}$ は奇数になり、それに 1 を加えているので $1 + \frac{l_1-1}{2} + \cdots + \frac{l_s-1}{2}$ は偶数になる。これで $(+)$ が示された。

(2), (3) も同様に証明できる。

定義 5.5 N を自然数、χ を $(\bmod N$ の$)$Dirichlet 指標としたとき、

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

とおいて、これを (χ についての)**Dirichlet L 関数**という。ただしここで $\chi(n)$ は n と N が互いに素なときは $\chi(n \mod N)$ を表すが、n と N が互いに素でないときは 0 を表す。

次の定理が虚 2 次体の類数公式と呼ばれるものである。

定理 5.6 (虚 2 次体の類数公式) K を虚 2 次体とし、m, N を上のとおりとする。χ は、(#) をみたす Dirichlet 指標とする。h_K を K の類数とし、w_K を K に含まれる 1 のベキ根の個数とする。このとき

$$h_K = \frac{w_K}{2} L(0,\chi) = \frac{w_K\sqrt{N}}{2\pi} L(1,\chi)$$

が成立する。

定理の証明は省略する。

命題 5.7 w_K は $K = \mathbb{Q}(\sqrt{-1})$ のとき 4、$K = \mathbb{Q}(\sqrt{-3})$ のとき 6、K がその他の虚 2 次体のときは 2 である。

証明 $K = \mathbb{Q}(\sqrt{m})$ とする。$(m \in \mathbb{Z},\, m < 0)$、また $\alpha \in K$ について $N(\alpha)$ は α の複素数としてのノルムをあらわすものとすると、

$$N(\alpha) = 1 \Leftrightarrow \alpha \text{ は } K \text{ に属する 1 のベキ根}$$

が成り立つ。$\Longleftarrow$ は明らかである。$\Longrightarrow$ は、O_K に中には、ノルムが 1 の元は高々有限個であることから従う。

よって、w_K の値を求めるには $N(\alpha) = 1$ となる $\alpha \in K$ の個数を求めればよい。また、α が 1 のベキ根であれば $\alpha \in O_K^\times$ であることに注意する。

Case 1. $m \equiv 2, 3 \pmod 4$ のときを考える。定理 2.3 より $O_K = \mathbb{Z}[\sqrt{m}]$ となる。$\alpha = a + b\sqrt{m} \in O_K$ を 1 のベキ根とする $(a, b \in \mathbb{Z})$。ここで $n = -m > 0$ とおくと、$N(\alpha) = a^2 - b^2 m = a^2 + b^2 n$ となる。

(1) $m = -1$ の場合、$N(\alpha) = a^2 + b^2 = 1$ より $\alpha = \pm 1, \pm i$ のいずれかである。従って $w_K = 4$ である。

(2) $m < -1$ の場合を考える。今、$b \neq 0$ と仮定する。すると

$$1 < b^2 n \leqq a^2 + b^2 n = N(\alpha)$$

となり、これは α が 1 のベキ根であることに矛盾する。 よって $b = 0$ である。従って $\alpha = \pm 1$ のいずれかである。従って $w_K = 2$ である。

Case 2. $m = 1 \pmod 4$ のとき。定理 2.3 より $O_K = \mathbb{Z}\left[\dfrac{1+\sqrt{m}}{2}\right]$ となる。$\alpha = a + b\frac{1+\sqrt{m}}{2} \in O_K$ を 1 のベキ根とする $(a, b \in \mathbb{Z})$。ここで $n = -m > 0$ とおくと $N(\alpha) = (a + \frac{1}{2}b)^2 + (\frac{b}{2})^2 n$ とかける。

(1) $m=-3$ の場合、$N(\alpha)=(a+\frac{1}{2}b)^2+\frac{3}{4}b^2=1$ となる。よって、$b=0,\pm1$ である。すると、α は $\pm1,\ \pm\dfrac{1+\sqrt{-3}}{2},\ \pm1\mp\dfrac{1+\sqrt{-3}}{2}$ のいずれかである。従って $w_K=6$ である。

(2) $m<-3$ とする。$m\equiv1\pmod 4$ より $m\leqq-7$ である。よって $b\neq0$ とすると

$$N(\alpha)=(a+\frac{1}{2}b)^2+\frac{n}{4}b^2\geq\frac{n}{4}b^2>1$$

となり α が1のベキ根であることに矛盾する。よって $b=0$ であり、$N(\alpha)=a^2$ より、α は ±1 のいずれかである。従って $w_K=2$ である。

証明終

補題 5.8 N を自然数とし、

$$\chi:(\mathbb{Z}/N\mathbb{Z})^\times\to\mathbb{C}^\times$$

を、$(\#)$ をみたす Dirichlet 指標とすると、

$$L(0,\chi)=-\frac{1}{N}\sum_{a=1}^{N}a\chi(a)$$

が成り立つ。

補題 5.8 を認めると、定理 5.6 は次のように書き換えられる。

系 5.9 K, m, N を上のとおりとする。χ は、$(\#)$ をみたす Dirichlet 指標とするとき、

$$h_K=-\frac{w_K}{2N}\sum_{a=1}^{N}a\chi(a)$$

が成立する。

例として、$\mathbb{Q}(\sqrt{-1})$ と $\mathbb{Q}(\sqrt{-3})$ の類数を系 5.9 を用いて求める。

$K=\mathbb{Q}(\sqrt{-1})$ とおく。すると $w_K=4$, $m=-1\equiv3\pmod 4$ なので $N=|4m|=4$ である。従って、

$$h_K=-\frac{4}{2\times4}\sum_{a=1}^{4}a\chi(a)=-\frac{1}{2}(1\cdot\chi(1)+3\cdot\chi(3))$$

である。また $\chi(1)=1$, $\chi(3)=\left(\dfrac{-1}{3}\right)=\left(\dfrac{2}{3}\right)=-1$ より、

$$h_K=-\frac{1}{2}(1\cdot1+3\cdot(-1))=1$$

である。

次に $K=\mathbb{Q}(\sqrt{-3})$ とする。$w_k=6,\ m=-3\equiv 1\pmod 4$ なので $N=3$ である。従って、

$$h_k=-\frac{6}{2\times 3}\sum_{a=1}^{3}a\chi(a)=-(1\chi(1)+2\chi(2))$$

である。このとき、式 $(*)$ により、$\chi(a\pmod 3)=\left(\dfrac{a}{3}\right)$ なので、$\chi(1)=1,\chi(2)=\left(\dfrac{2}{3}\right)=-1$ である。よって、$h_k=1$ となる。

次に、$\mathbb{Q}(\sqrt{-1})$ と $\mathbb{Q}(\sqrt{-3})$ の類数を定理 5.6 を用いて求める。

$K=\mathbb{Q}(\sqrt{-1})$ とおく。すると

$$h_K=\frac{w_K\sqrt{N}}{2\pi}L(1,\chi)=\frac{4}{\pi}\cdot L(1,\chi)$$

となる。ここで、

$$L(1,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots=\frac{\pi}{4}$$

となる[13]ので $h_K=1$ である。

続いて $K=\mathbb{Q}(\sqrt{-3})$ とする。

$$h_K=\frac{6\times\sqrt{3}}{2\pi}\cdot L(1,\chi)=\frac{3\sqrt{3}}{\pi}\cdot L(1,\chi)$$

より、$L(1,\chi)=\dfrac{\pi}{3\sqrt{3}}$ となることが、$\mathbb{Q}(\sqrt{-3})$ の類数が 1 であることからわかる。

なお、$L(1,\chi)$ が正確に $\dfrac{\pi}{3\sqrt{3}}$ であることを知らなくても、上の $h_K=\dfrac{3\sqrt{3}}{\pi}\cdot L(1,\chi)$ から $h_K=1$ を得ることが可能である。なぜなら

$$L(1,\chi)=1-\frac{1}{2}+\frac{1}{4}-\frac{1}{5}+\cdots<1$$

より、

$$h_K=\frac{3\sqrt{3}}{\pi}\cdot L(1,\chi)<\frac{3\sqrt{3}}{\pi}<2$$

である。ところが h_K は自然数であるため、これから $h_K=1$ を得る。

このように、虚 2 次体の類数公式 $h_K=\dfrac{w_K\sqrt{N}}{2\pi}L(1,\chi)$ から、無限級数 $L(1,\chi)$ のある程度の近似計算をすれば、h_K を求めることができる。

[13] ライプニッツの公式である。$\arctan(x)$ の導関数を用いて示す事が出来る。

類数が 1 の虚 2 次体が、

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163})$$

の 9 個だけであることが、1967 年に Baker と Stark によって証明されている。

6 可換環論からの準備

6.1 代数系

定義 6.1.1 加法と乗法の定められた空でない集合 A が **(可換) 環**であるとは、次の条件を満たすことをいう

(1) R は加法に関して Abel 群をなす

(2) $\forall a, b, c \in A$ に対し

$$(ab)c = a(bc)$$

(3) $\forall a, b, c \in A$ に対し

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

(4) $\forall a \in A$ に対し

$$ax = xa = a$$

となる $x \in A$ が存在する

(5) $\forall a, b \in A$ に対し

$$ab = ba$$

注意 6.1.2 定義 6.1.1(4),(5) は環の定義において必ずしも課される条件ではないが、以下では (1)∼(5) の成り立つ環のみを考察する。

(1) 定義 6.1.1(4) における x は存在するならば唯一つ定まる (証明はモノイドの単位元の一意性と同様である)。そこでこの x を 1 と書き、A の乗法に関する**単位元**という。

(2) 加法に関する単位元は 0 と書き、A の**零元**という。

(3) 環 A において $1 = 0$ が成り立つとき、任意の $a \in A$ に対して $a = a1 = a0 = 0$ が成り立つので $A = \{0\}$ である。このような環を**零環**という。以下では環は零環ではない、つまり、$1 \neq 0$ であることは常に仮定する。

定義 6.1.3 環 A の部分集合 B が次の条件を満たすとき、B は A の**部分環**であるという。

(1) $a, b \in B \Longrightarrow a+b, -a, ab \in B$

(2) $1 \in B$

定義 6.1.4 A は環とする。

(1) $a \in R$ が乗法に関する逆元を持つとき、すなわち $ax = xa = 1$ となる $x \in A$ が存在するとき、a は A の**単元**あるいは**単数**であるという。

(2) A の 0 でない任意の元が単元であるとき、A は**体**であるという。

(3) 体 A の部分環 B が再び体となる、すなわち、

$$a \in B \Longrightarrow a^{-1} \in B$$

となるとき、B は A の**部分体**であるという。

注意 6.1.5 モノイドの場合と同様に、与えられた元 $a \in A$ の逆元は存在するならば一意に定まる。そこで a の逆元を a^{-1} と書く。また、A の単元全体の集合は A の乗法によって群をなす。この群を A の**乗法群**あるいは**単数群**などといい、$A^{\times}$ と書く。

定義 6.1.6 A を環、M を Abel 群とする (M の演算も $+$ によって表す)。このとき、M が ***A*-加群**であるとは A の作用、すなわち写像 $\mu : A \times M \to M$ が与えられており、任意の $a, b \in A, x, y \in M$ に対して次が成立することをいう。($\mu(a, x)$ を ax と書くことにする)

(1) $(a+b)x = ax + bx$

(2) $a(x+y) = ax + ay$

(3) $a(bx) = (ab)x$

(4) $1x = x$

定義 6.1.7 A-加群 M の部分群 N が任意の $a \in A$ と $x \in N$ に対して $ax \in N$ となるとき、N を M の**部分*A*-加群**という。

定義 6.1.8 環 A の積は、A の A 自身への作用と見做せる。このとき、A の部分 A-加群のことを A の**イデアル**という。

注意 6.1.9 イデアルは大文字 $I, J, \cdots$ や、ドイツ文字 $\mathfrak{a}, \mathfrak{b}, \cdots$ などで表す。

命題 6.1.10 環 A のイデアル $\mathfrak{a}$ に対して次が成り立つ。

(1) $1 \in \mathfrak{a} \Longrightarrow \mathfrak{a} = A$

(2) $\mathfrak{a}$ が A の単元を含む $\Longrightarrow \mathfrak{a} = A$

証明

(1) $\forall a \in A$ に対し、$a = a1 \in \mathfrak{a}$ が成り立つので $A \subseteq \mathfrak{a}$。

(2) $x \in \mathfrak{a} \cap A^\times$ をとると、$x^{-1} \in A$ より $x^{-1}x = 1 \in \mathfrak{a}$ となり (1) より $\mathfrak{a} = A$ が成り立つ。

証明終

この命題から次が直ちにわかる。

系 6.1.11 環 A に対して、A が体であることと、A のイデアルは $\{0\}$ と A 自身のみであることは同値である。

次の性質は加群の定義から明らかである。

命題 6.1.12 A を環とする。M を A-加群、$(M_i)_{i\in I}$ を M の A-部分加群の族、$\mathfrak{a}$ を A のイデアルとするとき、次は A-加群である。

(1) $\displaystyle\bigcap_{i\in I} M_i$

(2) $\displaystyle\sum_{i\in I} M_i = \{\sum_{\text{有限和}} x_i \mid x_i \in M_i\}$

(3) $\mathfrak{a}M = \{\displaystyle\sum_{\text{有限和}} a_i x_i \mid a_i \in \mathfrak{a},\ x_i \in M\}$

注意 6.1.13 命題 6.1.12(3) より、M として特に A のイデアル $\mathfrak{b}$ をとると、イデアルの積

$$\mathfrak{a}\mathfrak{b} = \{\sum_{\text{有限和}} ab \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\}$$

が定義でき、$\mathfrak{a}\mathfrak{b}$ は A のイデアルとなる。
同様に有限個の A のイデアル $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_\mathfrak{n}$ の積 $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n$ が定義できる。

命題 6.1.14 M を A-加群、N を M の部分 A-加群とする。このとき M が Abel 群であることから剰余群 M/N が定義できるが、$\overline{x} \in M/N, a \in A$ に対して

$$a\overline{x} = \overline{ax}$$

と定めると、これは well-defined な A の M/N への作用であり、したがって M/N も A-加群の構造を持つ。
また、$\mathfrak{a}$ を A のイデアルとするとき、$\overline{x}, \overline{y} \in A/\mathfrak{a}$ に対し

$$\overline{x} \cdot \overline{y} = \overline{xy}$$

と定めると $\cdot$ は $A/\mathfrak{a}$ 上の well-defined な演算であり、$A/\mathfrak{a}$ はこの演算を積として環をなす。

証明　作用と積の well-defined 性のみを示す。
$\overline{x} = \overline{x'}$ とすると $x - x' = \alpha$ となる $\alpha \in \mathfrak{a}$ が存在する。このとき

$$a\overline{x} = \overline{ax} = \overline{a(\alpha + x')} = \overline{a\alpha + ax'} = \overline{ax'} = a\overline{x'}$$

となる。
同様に $\overline{x} = \overline{x'}, \overline{y} = \overline{y'}$ とすると $x - x' = \alpha, y - y' = \beta$ となる $\alpha, \beta \in \mathfrak{a}$ が存在し

$$\overline{x} \cdot \overline{y} = \overline{xy} = \overline{(\alpha + x')(\beta + y')} = \overline{\alpha\beta + \alpha y' + \beta x' + x'y'} = \overline{x'y'} = \overline{x'} \cdot \overline{y'}$$

が成立する。　**証明終**

定義 6.1.15　命題 6.1.14 で定義された A-加群 M/N を M の N による**剰余加群**、環 $A/\mathfrak{a}$ を A の $\mathfrak{a}$ による**剰余環**という。

定義 6.1.16　A, B を環とする。このとき、写像 $\phi : A \to B$ が環の**準同型写像**であるとは、次の条件を満たすことである。

(1) $\forall a, b \in A$ に対し、$\phi(a + b) = \phi(a) + \phi(b)$

(2) $\forall a, b \in A$ に対し、$\phi(ab) = \phi(a)\phi(b)$

(3) $\phi(1) = 1$

命題 6.1.17　環の準同型写像 $\phi : A \longrightarrow B$ に対して次が成り立つ。

(1) $\phi(0) = 0$

(2) $\phi(-a) = -\phi(a)$

(3) $\phi(a^{-1}) = \phi(a)^{-1}$　(ただし、$a \in A^{\times}$ とする)

証明

(1) $\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0)$ より $\phi(0) = \phi(0) - \phi(0) = 0$

(2) (1) より $0 = \phi(0) = \phi(a - a) = \phi(a) + \phi(-a)$ なので $\phi(-a) = -\phi(a)$

(3) $1 = \phi(1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$ より $\phi(a^{-1}) = \phi(a)^{-1}$

証明終

定義 6.1.18 M, M' を A-加群とする。このとき、写像 $\phi : M \to M'$ が ***A*-加群の準同型写像**あるいは ***A*-線形写像**であるとは、次の条件を満たすことである。

(1) $\forall x, y \in M$ に対し、$\phi(x + y) = \phi(x) + \phi(y)$

(2) $\forall x \in M, \forall a \in A$ に対し、$\phi(ax) = a\phi(x)$

命題 6.1.19 命題 6.1.17 と同様に A-線形写像 $\phi : M \longrightarrow N$ に対して次が成り立つ。

(1) $\phi(0) = 0$

(2) $\phi(-a) = -\phi(a)$

次の性質は準同型写像の定義から明らかである。

命題 6.1.20 $\iota : A \longrightarrow A$ を環 A 上の恒等写像とするとき、ι は環準同型写像である。
また、$f : A \longrightarrow B,\ g : B \longrightarrow C$ を環準同型写像とするとき、合成写像 $g \circ f$ は環準同型写像である。

注意 6.1.21 命題 6.1.20 と同様に、加群の場合にも、恒等写像が線形写像であること、線形写像の合成が再び線形写像となることがわかる。

命題 6.1.22 A を環、$\mathfrak{a}$ を A のイデアル、M を A-加群、N を M の部分 A-加群とする。このとき、自然な写像

$$\phi : A \ni a \longmapsto \overline{a} \in A/\mathfrak{a}$$
$$\psi : M \ni x \longmapsto \overline{x} \in M/N$$

を考えると、ϕ は全射な環準同型写像、ψ は全射な A-線形写像である。

証明 $A/\mathfrak{a}$ および M/N での演算、作用の定義から明らかである。 証明終

命題 6.1.23 $\phi : A \to B$ を環の準同型写像とする。このとき

$$\mathrm{Ker}\,\phi = \{a \in A \mid \phi(a) = 0\}$$
$$\mathrm{Im}\,\phi = \{\phi(a) \in B \mid a \in A\}$$

と定めると、$\mathrm{Ker}\,\phi$ は A のイデアル、$\mathrm{Im}\,\phi$ は B の部分環となる。

証明 $x, y \in \mathrm{Ker}\,\phi$ および $a \in A$ を任意にとると

$$\phi(x-y) = \phi(x) - \phi(y) = 0 - 0 = 0$$
$$\phi(ax) = \phi(a)\phi(x) = \phi(a)0 = 0$$

が成り立つので $x-y, ax \in \mathrm{Ker}\,\phi$、すなわち $\mathrm{Ker}\,\phi$ は A のイデアルである。
$\alpha, \beta \in \mathrm{Im}\,\phi$ を任意にとると $\phi(x) = \alpha, \phi(y) = \beta$ となる $x, y \in A$ が存在する。このとき

$$\alpha - \beta = \phi(x) - \phi(y) = \phi(x-y) \in \mathrm{Im}\,\phi$$
$$\alpha\beta = \phi(x)\phi(y) = \phi(xy) \in \mathrm{Im}\,\phi$$

である。また、明らかに $\phi(1) = 1 \in \mathrm{Im}\,\phi$ であるから、$\mathrm{Im}\,\phi$ は B の部分環となる。 **証明終**

定義 6.1.24 命題 6.1.23 の $\mathrm{Ker}\,\phi$ を ϕ の**核**、$\mathrm{Im}\,\phi$ を ϕ の**像**という。

線形写像に対しても、同様に核と像の概念が定義される。

定義 6.1.25 $\phi : M \to N$ を A-線形写像とする。このとき ϕ の**核** $\mathrm{Ker}\,\phi$, **像** $\mathrm{Im}\,\phi$ を

$$\mathrm{Ker}\,\phi = \{x \in M | \phi(x) = 0\}$$
$$\mathrm{Im}\,\phi = \{\phi(x) \in N | x \in M\}$$

と定めると、$\mathrm{Ker}\,\phi$ は M の部分 A-加群、$\mathrm{Im}\,\phi$ は N の部分 A-加群となる。

証明 $\mathrm{Ker}\,\phi$ については環の場合と同様。
$\mathrm{Im}\,\phi$ についても $\alpha, \beta \in \mathrm{Im}\,\phi$、$a \in A$ を任意にとったとき $\phi(x) = \alpha, \phi(y) = \beta$ となる $x, y \in A$ が存在することから

$$\alpha - \beta = \phi(x) - \phi(y) = \phi(x-y) \in \mathrm{Im}\,\phi$$
$$a\alpha = a\phi(x) = \phi(ax) \in \mathrm{Im}\,\phi$$

が成り立つ。 **証明終**

命題 6.1.26 $f : A \longrightarrow B$ を環の準同型写像とするとき

$$f \text{ が単射} \iff \mathrm{Ker}\, f = \{0\}$$

同様に、$\phi : M \longrightarrow N$ を A-線形写像とするとき

$$\phi \text{が単射} \iff \mathrm{Ker}\,\phi = \{0\}$$

が成り立つ。

証明 前者を示す。
($\Rightarrow$) $x \in \mathrm{Ker}\, f$ を任意にとると、$f(x) = 0$ であるが $f(0) = 0$ でもあるので $f(x) = f(0)$。f が単射なので $x = 0$。
($\Leftarrow$) $f(x) = f(y)$ と仮定すると、f が準同型写像であることから $f(x-y) = 0$、すなわち $x - y \in \mathrm{Ker}\, f$ が成り立つ。よって $x - y = 0$ で f は単射となる。 **証明終**

命題 6.1.27 $\phi : M \longrightarrow N$ を A-線形写像、L を N の部分 A-加群とする。このとき、$\phi^{-1}(L)$ は M の部分 A-加群である。

証明 $x, y \in \phi^{-1}(L)$ を任意にとると、$\phi(x), \phi(y) \in L$ であるから $\phi(x-y) = \phi(x) - \phi(y) \in L$ より $x - y \in \phi^{-1}(L)$。
また、$a \in A$ を任意にとると $\phi(ax) = a\phi(x) \in L$ より $ax \in \phi^{-1}(L)$ を得る。 **証明終**

命題 6.1.28 $\phi : A \longrightarrow B$ を環の準同型写像、$\mathfrak{b}$ を B のイデアルとすると、$\phi^{-1}(\mathfrak{b})$ は A のイデアルである。

証明 和と差について閉じていることは命題 6.1.27 の証明と同様である。
$\alpha \in A$ を任意にとると、任意の $a \in A$ に対し $\phi(\alpha a) = \phi(\alpha)\phi(\alpha) \in \mathfrak{b}$ が成り立つので、$\alpha a \in \phi^{-1}(\mathfrak{b})$ となる。 **証明終**

命題 6.1.29 $\phi : A \to B$ を環の準同型写像、$\mathfrak{a}$ を A のイデアルとする。このとき、ϕ が全射ならば、$\phi(\mathfrak{a})$ は B のイデアルである。

証明 $\alpha, \beta \in \phi(\mathfrak{a})$ を任意にとると、$\phi(x) = \alpha, \phi(y) = \beta$ となる $x, y \in \mathfrak{a}$ が存在する。このとき、$x - y \in \mathfrak{a}$ であるので、

$$\alpha - \beta = \phi(x) - \phi(y) = \phi(x - y) \in \phi(\mathfrak{a})$$

が成り立つ。また、任意の $b \in B$ に対して $\phi(a) = b$ となる $a \in A$ が存在するので、

$$b\alpha = \phi(a)\phi(x) = \phi(ax) \in \phi(\mathfrak{a})$$

が成り立つ。 **証明終**

次の定理は、対応定理と呼ばれる。

定理 6.1.30 A を環、$\mathfrak{a}$ を A のイデアルとする。このとき

$$\mathscr{X} = \{\mathfrak{b} \mid \mathfrak{b} \text{ は } A \text{ のイデアルで } \mathfrak{a} \subseteq \mathfrak{b}\}$$
$$\mathscr{Y} = \{\mathfrak{c} \mid \mathfrak{c} \text{ は } A/\mathfrak{a} \text{ のイデアル }\}$$

とおくと、$\mathscr{X}$ と $\mathscr{Y}$ の間には、包含関係を保つ全単射が存在する。
同様に、M を A-加群、N を M の部分 A-加群とするとき

$$\mathscr{S} = \{L \mid L \text{ は } M \text{ の部分 } A\text{–加群で } N \subseteq L\}$$
$$\mathscr{T} = \{K \mid K \text{ は } M/N \text{ の部分 } A\text{–加群 }\}$$

とおくと、$\mathscr{S}$ と $\mathscr{T}$ の間には、包含関係を保つ全単射が存在する。

証明　前者のみ示す。

$\pi : A \to A/\mathfrak{a}$ を自然な写像とすると、命題 6.1.28 および命題 6.1.29 より、写像 $F : \mathscr{X} \to \mathscr{Y}$ と $G : \mathscr{Y} \to \mathscr{X}$ を

$$F(\mathfrak{b}) = \pi(\mathfrak{b})$$
$$G(\mathfrak{c}) = \pi^{-1}(\mathfrak{c})$$

と定めることができる。これが、

$$\mathfrak{b} \subseteq \mathfrak{b}' \Longrightarrow F(\mathfrak{b}) \subseteq F(\mathfrak{b}')$$
$$\mathfrak{c} \subseteq \mathfrak{c}' \Longrightarrow G(\mathfrak{c}) \subseteq G(\mathfrak{c}')$$

かつ、$G \circ F = id_{\mathscr{X}}$, $F \circ G = id_{\mathscr{Y}}$ を満たすことは明らかである。　　**証明終**

次の定理は、準同型定理と呼ばれる。

定理 6.1.31　$f : A \longrightarrow B$ を環の準同型写像、$\mathfrak{a}$ を $\mathfrak{a} \subseteq \operatorname{Ker} f$ であるような A のイデアル、$\pi : A \longrightarrow A/\mathfrak{a}$ を自然な写像とする。このとき、$g \circ \pi = f$ となる環準同型写像 $g : A/\mathfrak{a} \to B$ が唯一つ存在する。また、このとき

$$g \text{が単射} \Longleftrightarrow \mathfrak{a} = \operatorname{Ker} f$$

が成り立つ。
同様に、$\phi : M \longrightarrow N$ を A-線形写像、L を $L \subseteq \operatorname{Ker} \phi$ であるような M の部分 A-加群、$\pi : M \longrightarrow M/L$ を自然な写像とすると、$\psi \circ \pi = \phi$ となる A-線形写像 $\psi : M/L \longrightarrow N$ が唯一つ存在し

$$\psi \text{が単射} \Longleftrightarrow L = \operatorname{Ker} \phi$$

が成り立つ。

証明　前者のみ示す。

まず、π が全射であるので、$g \circ \pi = f$ となる g は存在するならば一意に定まることがわかる。

次に、$A/\mathfrak{a}$ において、$\overline{a} = \overline{a'}$ ならば、$a - a' \in \mathfrak{a} \subseteq \operatorname{Ker} f$ であるので、$f(a) = f(a')$ となることに注意すれば、$g : A/\mathfrak{a} \to B$ を

$$g(\overline{a}) = f(a)$$

と定めてよいことがわかる。これは、明らかに $g \circ \pi = f$ を満たす。
さらに、このとき、

$$\overline{a} \in \operatorname{Ker} g \Longleftrightarrow a \in \operatorname{Ker} f$$

であるから

$$g \text{が単射} \iff \forall \overline{a} \in \operatorname{Ker} g,\ \overline{a} = 0 \iff \forall a \in \operatorname{Ker} f,\ a \in \mathfrak{a}$$

が成り立つ。すなわち $\operatorname{Ker} f \subseteq \mathfrak{a}$ となるので

$$g \text{が単射} \iff \mathfrak{a} = \operatorname{Ker} f$$

が成り立つ。 **証明終**

定義 6.1.32 A を環、$x \in A$ とする。

$$0 \neq \exists y \in A \ s.t.\ xy = 0$$

が成り立つとき、x は A の**零因子**であるという。零因子でない元のことを**非零因子**という。また、$x^n = 0$ となる $n \in \mathbb{N}$ が存在するとき x は A の**ベキ零元**であるという。

定義 6.1.33 環 A のベキ零元全体の集合を $\mathfrak{N}_A$ と書き、A の**ベキ零根基**という。

命題 6.1.34 環 A の単元は非零因子である。

証明 $x \in A^\times$ が A の零因子であったとすると $xy = 0$ をみたす $y \in A \setminus \{0\}$ が存在するが、$x^{-1} \in A$ より

$$y = 1y = x^{-1}xy = 0$$

となり y の取り方に反する。 **証明終**

定義 6.1.35 環 A が 0 以外の零因子を持たないとき、すなわち $\forall x, y \in A$ に対して

$$xy = 0 \Longrightarrow x = 0 \text{ または } y = 0$$

が成り立つとき、A は**整域**であるという。

命題 6.1.34 より次がしたがう。

系 6.1.36 体は整域である。

定義 6.1.37 環 A のイデアル $\mathfrak{p}(\neq A)$ は次の条件を満たすとき、A の**素イデアル**という。

$$xy \in \mathfrak{p} \Longrightarrow x \in \mathfrak{p} \text{ または } y \in \mathfrak{p}$$

また、環 A のイデアル $\mathfrak{m}(\neq A)$ は次の条件を満たすとき、A の**極大イデアル**という。

$$A \text{のイデアル} \mathfrak{a} \text{に対し } \mathfrak{m} \subseteq \mathfrak{a} \Longrightarrow \mathfrak{a} = A \text{ または } \mathfrak{a} = \mathfrak{m}$$

注意 6.1.38 環 A の素イデアル全体の集合を、Spec$A$ によって表す。

命題 6.1.39 A を環とするとき、次が成り立つ。

$$\mathfrak{p} \text{ が } A \text{ の素イデアル} \iff A/\mathfrak{p} \text{ が整域}$$
$$\mathfrak{m} \text{ が } A \text{ の極大イデアル} \iff A/\mathfrak{m} \text{ が体}$$

証明

$$\begin{aligned}
\mathfrak{p} \text{ が } A \text{ の素イデアル} &\iff x, y \in A \text{ が } xy \in \mathfrak{p} \text{ を満たすとき、} x \in \mathfrak{p} \text{ または } y \in \mathfrak{p} \\
&\iff \overline{x}, \overline{y} \in A/\mathfrak{p} \text{ が} \overline{x}\overline{y} = \overline{0} \text{を満たすなら、} \overline{x} = \overline{0} \text{ または } \overline{y} = \overline{0} \\
&\iff A/\mathfrak{p} \text{ が整域} \\
\mathfrak{m} \text{ が } A \text{ の極大イデアル} &\iff \mathfrak{m} \text{ を真に含むイデアルは } A \text{ のみ} \\
&\iff A/\mathfrak{m} \text{ のイデアルは } \{\overline{0}\}, A/\mathfrak{m} \text{ のみ (定理 6.1.30 より)} \\
&\iff A/\mathfrak{m} \text{ は体 (命題 6.1.11 より)}
\end{aligned}$$

証明終

体が整域であることから次がしたがう。

系 6.1.40 極大イデアルは素イデアルである。

系 6.1.41 体からの環準同型写像は単射である。すなわち F が体、B を環、$f : F \longrightarrow B$ が環準同型写像ならば、f は単射である。

証明 $f(1) = 1$ より、Ker f は F 自身と異なる F のイデアルである。したがって Ker $f = 0$ なので f は単射である。 **証明終**

定理 6.1.42 環 A の任意の真のイデアル $\mathfrak{a}$ に対し、$\mathfrak{a} \subseteq \mathfrak{m}$ となる A の極大イデアル $\mathfrak{m}$ が存在する。

証明 A が Noether 環である場合には、Noether 環の定義 (命題 6.4.1) より直ちにこのような極大イデアルの存在が言える。A が Noether 環とは限らない場合には、Zorn の補題を適用する必要がある。

Σ を $\mathfrak{a}$ を含む A の真のイデアル全体の集合とし、包含関係による順序を導入する。このとき、$\mathfrak{a} \in \Sigma$ であるので $\Sigma \neq \emptyset$ である。そこで、

$$\mathscr{I} = \{\mathfrak{a}_i \mid i \in I\}$$

を Σ の全順序部分集合とすると、

$$\bigcup_{i \in I} \mathfrak{a}_i$$

は A のイデアルとなる。実際、$x, y \in \cup\mathfrak{a}_i$ を任意にとると、$\mathscr{I}$ が全順序集合であることから、

$$x, y \in \mathfrak{a}_j$$

となる $j \in I$ が存在する。したがって任意の $a \in A$ に対し

$$x - y, ax \in \mathfrak{a}_j \subseteq \bigcup_{i \in I} \mathfrak{a}_i$$

が成り立つ。
また、任意の $i \in I$ に対して $1 \notin \mathfrak{a}_i$ であることから $1 \notin \cup\mathfrak{a}_i$、すなわち $\cup\mathfrak{a}_i \neq A$ であり $\cup\mathfrak{a}_i \in \Sigma$ となる。したがって、$\cup\mathfrak{a}_i$ は $\mathscr{I}$ の上界となる。ゆえに、Σ は帰納的順序集合となるので Zorn の補題を適用することができ、Σ の極大元、すなわち $\mathfrak{a}$ を含む A の極大イデアルの存在が言える。 **証明終**

定義 6.1.43 極大イデアルを唯一つしか持たない環を**局所環**という。

系 6.1.44 A を環とするとき、A が局所環であることと、A の非単元全体の集合 $A \setminus A^\times$ がイデアルとなることは同値である。

証明 A が局所環であるとし、$\mathfrak{m}$ をその唯一の極大イデアルとすると、定理 6.1.42 より任意の非単元 x に対し x で生成された単項イデアル (定義 6.1.48 参照) は $\mathfrak{m}$ に含まれるので、$A \setminus A^\times \subseteq \mathfrak{m}$ である。一方 $\mathfrak{m} \subsetneqq A$ より $\mathfrak{m} \subseteq A \setminus A^\times$ は明らかに成り立つ。したがって、$A \setminus A^\times = \mathfrak{m}$ である。
逆に、$A \setminus A^\times$ が A のイデアルとなったとすると、A の任意の真のイデアルは非単元のみからなるので $A \setminus A^\times$ に含まれる。よって、$A \setminus A^\times$ が A の唯一の極大イデアルとなる。 **証明終**

命題 6.1.45 $f : A \longrightarrow B$ を環準同型写像、$\mathfrak{p}$ を B の素イデアルとするとき、$f^{-1}(\mathfrak{p})$ は A の素イデアルである。

証明 $1 \notin \mathfrak{p}$ より $1 \notin f^{-1}(\mathfrak{p})$ なので $f^{-1}(\mathfrak{p}) \neq A$ である。
$xy \in f^{-1}(\mathfrak{p})$ とすると $f(x)f(y) = f(xy) \in \mathfrak{p}$ より $f(x) \in \mathfrak{p}$ または $f(y) \in \mathfrak{p}$ である。すなわち

$$x \in f^{-1}(\mathfrak{p}) \text{ または } y \in f^{-1}(\mathfrak{p})$$

が成り立つ。 **証明終**

命題 6.1.46 $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ を環 A のイデアル、$\mathfrak{p}$ を A の素イデアルとし

$$\bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{p}$$

とすると、$\mathfrak{a}_i \subseteq \mathfrak{p}$ となる i が存在する。特に $\mathfrak{p} = \cap\mathfrak{a}_i$ ならば、$\mathfrak{p} = \mathfrak{a}_i$ となる i が存在する。

証明 対偶を示す。任意の i に対し $\mathfrak{a}_i \subsetneqq \mathfrak{p}$ であると仮定すると、各 i に対して $x_i \in \mathfrak{a}_i$ かつ $x_i \notin \mathfrak{p}$ となる x_i が存在する。したがって $\Pi x_i \in \Pi \mathfrak{a}_i \subseteq \cap \mathfrak{a}_i$ が成り立つ。しかし、$\mathfrak{p}$ が素イデアルであるので、x_i のとりかたから $\Pi x_i \notin \mathfrak{p}$ である。ゆえに、$\cap \mathfrak{a}_i \not\subseteq \mathfrak{p}$ である。
$\mathfrak{p} = \cap \mathfrak{a}_i$ であるとき、任意の j に対して $\mathfrak{p} \subseteq \mathfrak{a}_j$ であることに注意すれば、主張は明らかである。 **証明終**

定義 6.1.47 M を A-加群、L を M の部分集合とする。このとき

$$AL = \{ \sum_{\text{有限和}} a_i x_i \mid a_i \in A, x_i \in L \}$$

とおくと AL は M の部分 A-加群である。この加群のことを A 上 L によって**生成された加群**という。
特に、L が有限集合 $\{x_1, x_2, \cdots, x_n\}$ であるとき

$$AL = Ax_1 + Ax_2 + \cdots + Ax_n$$

と書き、L は A 上有限生成であるという。

定義 6.1.48 環 A 上で、$x_1, x_2, \cdots, x_n \in A$ で生成されるイデアルは $(x_1, x_2, \cdots, x_n)$ と表される。特に、唯一つの元 x で生成されるイデアル (x) のことを**単項イデアル**という。
また、任意のイデアルが単項イデアルであるような整域のことを、**単項イデアル整域**あるいは **PID** という。

注意 6.1.49 命題 6.1.12(3) において、環 A のイデアル $\mathfrak{a}$ と A-加群 M との積 $\mathfrak{a}M$ が定義されたが、$\mathfrak{a}$ が単項イデアル (a) であるとき、$(a)M$ を aM と表す。

定義 6.1.50 $(M_i)_{i \in I}$ を A-加群の族とするとき、$(M_i)_{i \in I}$ の群としての直和

$$\bigoplus_{i \in I} M_i = \{ (x_i)_{i \in I} \mid x_i \in M_i \text{ ただし、有限個の } i \text{ を除いて } x_i = 0 \}$$

に対し、成分ごとに A の作用を定める。すなわち、$a \in A$ に対し、

$$a(x_i)_{i \in I} = (ax_i)_{i \in I}$$

と定めると、$\oplus M_i$ は明らかに A-加群の構造を持つ。この加群を $(M_i)_{i \in I}$ の**直和**という。

定義 6.1.51 環 A の (任意個の) 直和

$$A^{\oplus I}$$

と同型な A-加群のことを**自由 A-加群**という。特に、添字集合 I が有限集合 $\{1, 2, \cdots, n\}$ であるとき、$A^{\oplus I}$ を A^n と書く。

命題 6.1.52 A 加群 M について、M が有限生成 A-加群であることと、M がある自由 A-加群の剰余加群と同型となることは同値である。

証明 $M = x_1M + \cdots + x_nM$ とするとき、写像 $\phi : A^n \to M$ を $\phi((a_1, \cdots, a_n)) = a_1x_1 + \cdots + a_nx_n$ によって定めると、ϕ は明らかに A-線形写像であり、かつ全射である。よって、M は $A^n/\operatorname{Ker}\phi$ と同型である。

逆に、全射な A-線形写像 $\phi : A^n \to M$ が存在したとする。このとき、$e_i = (0, \cdots, 0, 1, 0, \cdots, 0))$(第 i 成分が 1 で、それ以外の成分は 0) とおくと、$A^n = e_1A + \cdots + e_nA$ より、

$$M = \phi(A^n) = \phi(e_1)A + \cdots + \phi(e_n)A$$

を得る。 **証明終**

命題 6.1.53 M を有限生成 A-加群、$\mathfrak{a}$ を A のイデアルとする。このとき M の A-加群の自己準同型写像 ϕ が $\phi(M) \subseteq \mathfrak{a}M$ を満たすとすると、

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

となるような $n \in \mathbb{N},\ a_i \in \mathfrak{a}$ が存在する。

証明 $M = Ax_1 + Ax_2 + \cdots + Ax_n$ とすると、各 x_i に対し $\phi(x_i) \in \mathfrak{a}M$ であるので、$\phi(x_i) = \Sigma_{j=1}^n a_{ij}x_j$ となる $a_{ij} \in \mathfrak{a}$ が存在する。すなわち

$$\phi(x_i) - \sum_{j=1}^{n} a_{ij}x_j = 0$$

が成り立つ。
ここで、A 上の一変数多項式環 $A[t]$ の M への作用を $\alpha \in M$ に対して $(\Sigma a_it^i)\alpha = \Sigma a_i\phi^i(\alpha)$ と定めると、これは明らかに well-difined な $A[t]$ から M への作用となる。すると、いま

$$\sum_{j=1}^{n}(\delta_{ij}t - a_{ij})x_j = 0$$

が成り立っている。すなわち、$P = (\delta_{ij}t - a_{ij}),\ \boldsymbol{x} = {}^t(x_1, x_2, \cdots, x_n)$ とおくと

$$P\boldsymbol{x} = \mathbf{0}$$

であるから、P の余因子行列 $P^{(c)}$ を左から掛けて ($A[t]$ が可換環であることに注意)

$$P^{(c)}P\boldsymbol{x} = (\det P)I\boldsymbol{x} = (\det P)\boldsymbol{x} = \mathbf{0}$$

が成り立つ。つまり各 i に対して $(\det P)x_i = 0$ が成り立っているが、$x_1, x_2, \cdots, x_n$ は M を生成するので、$\det P \in A[t]$ は任意の $x \in M$ に対して $(\det P)x = 0$ をみたすことがわかる。

P の (i,j)-成分が $\delta_{ij}t - a_{ij}$ であることに注意すれば、$\det P$ は t に関する n 次の monic 多項式であり、$n-1$ 次以下の係数がすべて $\mathfrak{a}$ に属することもわかる。すなわち、M から M への A-線形写像として

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

が成り立つ。 **証明終**

命題 6.1.54 環 A のベキ零根基 $\mathfrak{N}_A$ は A の素イデアル全体の共通部分と等しい。したがって $\mathfrak{N}_A$ は A のイデアルである。

証明 $\mathfrak{N}' = \bigcap_{\mathfrak{p}\in \mathrm{Spec}A} \mathfrak{p}$ とおく。$x \in \mathfrak{N}_A$ をとると、$x^n = 0$ となる $n \in \mathbb{N}$ が存在するから、任意の素イデアル $\mathfrak{p}$ に対して $x^n \in \mathfrak{p}$ となる。すると $\mathfrak{p}$ が素イデアルであることから

$$\begin{aligned} x^n \in \mathfrak{p} &\Longleftrightarrow x^{n-1} \in \mathfrak{p} \\ &\Longleftrightarrow \cdots \\ &\Longleftrightarrow x \in \mathfrak{p} \end{aligned}$$

となるので $x \in \mathfrak{N}'$ が成り立つ。
逆に、$x \notin \mathfrak{N}_A$ とし、A のイデアルの集合 Σ を

$$\Sigma = \{\mathfrak{a} \mid \mathfrak{a} \text{ は } A \text{ のイデアルで } \forall n \in \mathbb{N}, x^n \notin \mathfrak{a}\}$$

と定めると、$(0) \in \Sigma$ より $\Sigma \neq \emptyset$ であり、包含関係に関する帰納的順序集合となることがわかる。したがって、Σ に Zorn の補題を適用することができる。そこで $\mathfrak{a}$ を Σ の極大元のひとつとする。
$a, b \in A$ に対して $a, b \notin \mathfrak{a}$ と仮定すると

$$\mathfrak{a} \subsetneqq \mathfrak{a} + (a) \text{ かつ } \mathfrak{a} \subsetneqq \mathfrak{a} + (b)$$

であるが、$\mathfrak{a}$ の極大性から $\mathfrak{a} + (a), \mathfrak{a} + (b) \notin \Sigma$ である。したがって

$$\exists m, n \in \mathbb{N}\ s.t.\ x^m \in \mathfrak{a} + (a),\ x^n \in \mathfrak{a} + (b)$$

が成り立つ。したがって $x^{m+n} \in \mathfrak{a} + (ab)$ であるから、$\mathfrak{a} + (ab) \notin \Sigma$ となる。
よって $\mathfrak{a} \in \Sigma$ なので $ab \notin \mathfrak{a}$ となることがわかる。すなわち

$$a \notin \mathfrak{a} \text{ かつ } b \notin \mathfrak{a} \Longrightarrow ab \notin \mathfrak{a}$$

が言えた。対偶をとれば $\mathfrak{a}$ が素イデアルであることがわかる。
以上より、Σ の定め方から $x \notin \mathfrak{a}$ であり、$\mathfrak{a}$ が素イデアルであることから $x \notin \mathfrak{N}'$ が成り立つ。 **証明終**

命題 6.1.55 環 A のイデアル $\mathfrak{a}$ に対して

$$r(\mathfrak{a}) = \{x \in A \mid \exists n \in \mathbb{N}\ s.t.\ x^n \in \mathfrak{a}\}$$

とおくと、$r(\mathfrak{a})$ は A のイデアルである。

証明　$x, y \in r(\mathfrak{a})$ をとると、$x^n, y^m \in \mathfrak{a}$ となる $n, m \in \mathbb{N}$ が存在する。よって、$l = \max\{n, m\}$ とおけば $(x-y)^{2l} \in \mathfrak{a}$、すなわち $x - y \in r(\mathfrak{a})$ を得る。また、任意の $a \in A$ に対して、$(ax)^n$ を考えれば、明らかに $ax \in r(\mathfrak{a})$ が成り立つ。　**証明終**

定義 6.1.56 命題 6.1.55 で定義されたイデアル $r(\mathfrak{a})$ のことを、$\mathfrak{a}$ の**根基**という。

命題 6.1.57 環 A のイデアル $\mathfrak{a}$ の根基 $r(\mathfrak{a})$ は、$\mathfrak{a}$ を含むような全ての A の素イデアルの共通部分と等しい。

証明　定理 6.1.30 より、$A/\mathfrak{a}$ のイデアルと A のイデアルで $\mathfrak{a}$ を含むものの間には、1 対 1 の対応が存在する。このとき

$$\begin{aligned} x \in r(\mathfrak{a}) &\Longleftrightarrow \exists n \in \mathbb{N}\ s.t.\ x^n \in \mathfrak{a} \\ &\Longleftrightarrow A/\mathfrak{a} \text{ において } \exists n \in \mathbb{N}\ s.t.\ \overline{x}^n = \overline{0} \\ &\Longleftrightarrow \overline{x} \in \mathfrak{N}_{A/\mathfrak{a}} \end{aligned}$$

であるから、定理 6.1.30 において $r(\mathfrak{a})$ は $\mathfrak{N}_{A/\mathfrak{a}}$ に対応している。命題 6.1.54 より

$$\mathfrak{N}_{A/\mathfrak{a}} = \bigcap_{\mathfrak{P} \in \mathrm{Spec}A/\mathfrak{a}} \mathfrak{P}$$

であるから、定理 6.1.30 および命題 6.1.45 より $A/\mathfrak{a}$ の素イデアルと $\mathfrak{a}$ を含む A の素イデアルとの間に 1 対 1 の対応が存在することに注意すれば

$$r(\mathfrak{a}) = \pi^{-1}\Big(\bigcap_{\mathfrak{P} \in \mathrm{Spec}A/\mathfrak{a}} \mathfrak{P}\Big) = \bigcap_{\mathfrak{P} \in \mathrm{Spec}A/\mathfrak{a}} \pi^{-1}(\mathfrak{P}) = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p} \in \mathrm{Spec}A} \mathfrak{p}$$

を得る。(ただし $\pi : A \longrightarrow A/\mathfrak{a}$ は自然な写像)　**証明終**

命題 6.1.58 $\mathfrak{p}$ が A の素イデアルならば $r(\mathfrak{p}) = \mathfrak{p}$ が成立する。

証明　根基の定義より明らかに $\mathfrak{p} \subseteq r(\mathfrak{p})$ が成り立つ。
一方、$x \in r(\mathfrak{p})$ をとると $x^n \in \mathfrak{p}$ を満たす $n \in \mathbb{N}$ が存在するが、$\mathfrak{p}$ が素イデアルなので

$$\begin{aligned} x^n \in \mathfrak{p} &\Longleftrightarrow x^{n-1} \in \mathfrak{p} \\ &\Longleftrightarrow x^{n-2} \in \mathfrak{p} \\ &\Longleftrightarrow \cdots \\ &\Longleftrightarrow x \in \mathfrak{p} \end{aligned}$$

より $r(\mathfrak{p}) \subseteq \mathfrak{p}$ を得る。　**証明終**

命題 6.1.59 イデアルの根基をとる操作と有限個の共通部分をとる操作は、可換である。すなわち、$\mathfrak{a}, \mathfrak{b}$ を環 A のイデアルとするとき

$$r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$$

が成り立つ。

証明

$$\begin{aligned} x \in r(\mathfrak{a} \cap \mathfrak{b}) &\iff \exists n \in \mathbb{N}\ s.t.\ x^n \in \mathfrak{a} \cap \mathfrak{b} \\ &\iff \exists n \in \mathbb{N}\ s.t.\ x^n \in \mathfrak{a} \text{ かつ } x^n \in \mathfrak{b} \\ &\iff x \in r(\mathfrak{a}) \text{ かつ } x \in r(\mathfrak{b}) \\ &\iff x \in r(\mathfrak{a}) \cap r(\mathfrak{b}) \end{aligned}$$

証明終

命題 6.1.60 $\mathfrak{a}, \mathfrak{b}$ を環 A のイデアルとするとき

$$\begin{aligned} r(\mathfrak{a}\mathfrak{b}) &= r(\mathfrak{a}) \cap r(\mathfrak{b}) \\ r(\mathfrak{a} + \mathfrak{b}) &= r(r(\mathfrak{a}) + r(\mathfrak{b})) \end{aligned}$$

が成り立つ。

証明

$$\begin{aligned} x \in r(\mathfrak{a}\mathfrak{b}) &\iff \exists n \in \mathbb{N}\ s.t.\ x^n \in \mathfrak{a}\mathfrak{b} \\ &\iff \exists n \in \mathbb{N}, \exists a_i \in \mathfrak{a}, \exists b_i \in \mathfrak{b}\ s.t.\ x^n = \Sigma a_i b_i \\ &\iff \exists n \in \mathbb{N}\ s.t.\ x^n \in \mathfrak{a} \cap \mathfrak{b} \\ &\iff x \in r(\mathfrak{a} \cap \mathfrak{b}) \\ &\iff x \in r(\mathfrak{a}) \cap r(\mathfrak{b}) \end{aligned}$$

$$\begin{aligned} x \in r(\mathfrak{a} + \mathfrak{b}) &\iff \exists n \in \mathbb{N}\ s.t.\ x^n \in \mathfrak{a} + \mathfrak{b} \\ &\iff \exists n \in \mathbb{N}, \exists a \in \mathfrak{a}, \exists b \in \mathfrak{b}\ s.t.\ x^n = a + b \\ &\iff \exists n \in \mathbb{N}\ s.t.\ x^n \in r(\mathfrak{a}) + r(\mathfrak{b}) \\ &\iff x \in r(r(\mathfrak{a}) + r(\mathfrak{b})) \end{aligned}$$

命題 6.1.61 $\mathfrak{a}, \mathfrak{b}$ を環 A のイデアルとするとき、

$$r(\mathfrak{a}) + r(\mathfrak{b}) = A \Longrightarrow \mathfrak{a} + \mathfrak{b} = A$$

が成立する。

証明 命題 6.1.60 より

$$r(\mathfrak{a}+\mathfrak{b}) = r(r(\mathfrak{a})+r(\mathfrak{b})) = r(A) = A$$

であるから、$1 \in \mathfrak{a}+\mathfrak{b}$ が成り立つ。すなわち $\mathfrak{a}+\mathfrak{b} = A$ である。 **証明終**

定義 6.1.62 環 A のイデアル $\mathfrak{a}, \mathfrak{b}$ について、$\mathfrak{a}+\mathfrak{b} = A$ が成り立つとき、$\mathfrak{a}$ と $\mathfrak{b}$ は**互いに素**であるという。

命題 6.1.63 環 A のイデアル $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ がどの二つのイデアルも互いに素であるとき、

$$\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

が成り立つ。

証明 n についての帰納法で証明する。

まず、$n = 2$ とする。$\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ は明らかに成り立つ。一方 $x \in \mathfrak{a} \cap \mathfrak{b}$ をとると、$a+b = 1$ となる $a \in \mathfrak{a}, b \in \mathfrak{b}$ が存在するので

$$x = x(a+b) = xa + xb \in \mathfrak{ab}$$

が成立する。

$n \geq 3$ とし、$\Pi_{i=1}^{n-1}\mathfrak{a}_1 = \cap_{i=1}^{n-1}\mathfrak{a}_1$ が成り立っているとする。このとき $\mathfrak{b} = \Pi_{i=1}^{n-1}\mathfrak{a}_1 = \cap_{i=1}^{n-1}\mathfrak{a}_1$ とおく。いま、任意の $1 \leq i \leq n-1$ に対して $\mathfrak{a}_i + \mathfrak{a}_n = A$ であるから、$x_i + y_i = 1$ となる $x_i \in \mathfrak{a}_i$ および $y_i \in \mathfrak{a}_n$ が存在する。すると

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1}(1-y_i)$$

より、$\Pi_{i=1}^{n-1}x_i + Y = 1$ となる $Y \in \mathfrak{a}_n$ が存在することがわかる。したがって $\Pi_{i=1}^{n-1}x_i \in \mathfrak{b}$ より $\mathfrak{b}+\mathfrak{a}_n = A$ が成り立ち、$n = 2$ の場合を用いて

$$\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

となる。 **証明終**

定義 6.1.64 環 A のイデアル $\mathfrak{a}, \mathfrak{b}$ に対し $\mathfrak{a}$ と $\mathfrak{b}$ の**イデアル商** $(\mathfrak{a} : \mathfrak{b})$ を

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$$

と定める。$\mathfrak{b}$ が単項イデアル (x) である場合、$(\mathfrak{a} : \mathfrak{b})$ を $(\mathfrak{a} : x)$ と表す。

注意 6.1.65 イデアル商 $(\mathfrak{a} : \mathfrak{b})$ は A のイデアルである。実際 $x, y \in (\mathfrak{a} : \mathfrak{b})$ をとると、$x\mathfrak{b}, y\mathfrak{b} \subseteq \mathfrak{a}$ が成り立つので、任意の $a \in A,\ b \in \mathfrak{b}$ に対して

$$(x-y)b = xb - yb \in \mathfrak{a}$$
$$axb \in \mathfrak{a}$$

が成り立つことより、$x - y, ax \in (\mathfrak{a} : \mathfrak{b})$ である。

定義 6.1.66 A-加群 M に対し、

$$\mathrm{Ann}(M) = \{a \in A \mid aM = 0\}$$

とおくと、$\mathrm{Ann}(M)$ は A のイデアルとなる。このイデアルを M の**零化イデアル**(もしくは、**annihilator**) という。
$\mathrm{Ann}(M) = 0$ となるとき、M は A-加群として**忠実**であるという。

定義 6.1.67 $f : A \to B$ を環準同型写像とする。A のイデアル $\mathfrak{a}$ に対し、$\mathfrak{a}$ の f による**拡大**$\mathfrak{a}^e$ を、$f(\mathfrak{a})$ によって生成された B のイデアル、すなわち

$$\mathfrak{a}^e = f(\mathfrak{a})B = \{\sum_{\text{有限和}} x_i y_i \mid x_i \in f(\mathfrak{a}),\ y_i \in B\}$$

と定める。また、B のイデアル $\mathfrak{b}$ に対して、$\mathfrak{b}$ の f による**縮約**(あるいは**引き戻し**)$\mathfrak{b}^c$ を

$$\mathfrak{b}^c = f^{-1}(\mathfrak{b})$$

と定める。(命題 6.1.45 より $\mathfrak{b}^c$ は A のイデアルである)

命題 6.1.68 $f : A \to B$ を環準同型写像、$\mathfrak{a}$ を A のイデアル、$\mathfrak{b}$ を B のイデアルとするとき、次が成り立つ。

(1) $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$

(2) $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$

(3) $r(\mathfrak{a})^e \subseteq r(\mathfrak{a}^e)$

証明 (1), (2) については定義から明らかである。
次に (3) を示す。 $x \in r(\mathfrak{a})^e$ をとると $x = \Sigma_{i=1}^m y_i b_i$ となる $b_i \in B,\ y_i \in f(r(\mathfrak{a}))$ が存在する。このとき、各 y_i はある $r(\mathfrak{a})$ の元 a_i を用いて $y_i = f(a_i)$ と書けるから、各 i に対して $a_i^{n_i} \in \mathfrak{a}$ となる $n_i \in \mathbb{N}$ が存在し、したがって $y_i^{n_i} = f(a_i^{n_i}) \in f(\mathfrak{a}) \subseteq \mathfrak{a}^e$ となる。したがって $N \in \mathbb{N}$ を十分大きくとれば $x^N \in \mathfrak{a}^e$ が成り立つ。(例えば、$n = \max\{n_1, n_2, \cdots, n_m\}$ に対し $N = mn$ とおけばよい) **証明終**

命題 6.1.68(1), (2) より次が成り立つ。

系 6.1.69 $f : A \to B$ を環準同型写像、$\mathfrak{a}$ を A のイデアル、$\mathfrak{b}$ を B のイデアルとするとき

$$\mathfrak{a}^{ece} = \mathfrak{a}^e,\ \mathfrak{b}^{cec} = \mathfrak{b}^c$$

が成り立つ。

定義 6.1.70 環 A のイデアル $\mathfrak{q}(\neq A)$ が A の**準素イデアル**であるとは、次の条件を満たすこととする。

$$xy \in \mathfrak{q} \Longrightarrow x \in \mathfrak{q} \text{ または } \exists n \in \mathbb{N}\ s.t.\ y^n \in \mathfrak{q}$$

注意 6.1.71 定義 6.1.70 の条件を言い換えると

$$\mathfrak{q} \text{ が準素イデアル} \Longleftrightarrow A/\mathfrak{q} \neq 0 \text{ かつ } A/\mathfrak{q} \text{ の零因子はベキ零元である}$$

命題 6.1.72 $\mathfrak{q}$ を環 A の準素イデアルとするとき、$r(\mathfrak{q})$ は $\mathfrak{q}$ を含むような最小の A の素イデアルである。

証明

$$\begin{aligned} xy \in r(\mathfrak{q}) &\Longleftrightarrow \exists m \in \mathbb{N}\ s.t.\ x^m y^m \in \mathfrak{q} \\ &\Longrightarrow \exists m \in \mathbb{N}\ s.t.\ 「x^m \in \mathfrak{q} \text{ または } \exists n \in \mathbb{N}\ s.t.\ y^{mn} \in \mathfrak{q}」 \\ &\Longleftrightarrow x \in r(\mathfrak{q}) \text{ または } y \in r(\mathfrak{q}) \end{aligned}$$

であるから、$r(\mathfrak{q})$ は A の素イデアルである。すると、命題 6.1.57 より $r(\mathfrak{q})$ は $\mathfrak{q}$ を含む最小の A の素イデアルであることがわかる。 **証明終**

命題 6.1.73 $f : A \to B$ を環準同型写像、$\mathfrak{q}$ を B の準素イデアルとするとき、$f^{-1}(\mathfrak{q})$ は A の準素イデアルである。

証明 f と自然な写像 $\pi : B \to B/\mathfrak{q}$ との合成 $\pi \circ f$ を考えると $f^{-1}(\mathfrak{q}) = f^{-1}(\operatorname{Ker}\pi)$ であるから定理 6.1.31 より $\pi \circ f = g \circ \phi$ となる単射な環準同型写像 $g : A/f^{-1}(\mathfrak{q}) \to B/\mathfrak{q}$ が誘導される (ただし $\phi : A \to A/f^{-1}(\mathfrak{q})$ は自然な写像)。したがって $A/f^{-1}(\mathfrak{q})$ は $B/\mathfrak{q}$ の部分環に同型であり、注意 6.1.71 の条件を満たす。 **証明終**

定義 6.1.74 $\mathfrak{q}$ を環 A の準素イデアルとするとき、素イデアル $\mathfrak{p}$ を $\mathfrak{p} = r(\mathfrak{q})$ とおき、$\mathfrak{q}$ は **$\mathfrak{p}$-準素イデアル**であるという。

定義 6.1.75 環 A のイデアル $\mathfrak{a}$ が有限個の準素イデアル $\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_n$ によって

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

と表されるとき、この表記 $\mathfrak{a} = \cap \mathfrak{q}_i$ を $\mathfrak{a}$ の**準素分解**と言い、$\mathfrak{a}$ は**分解可能**であるという。

定義 6.1.76 環 A のイデアル $\mathfrak{a}$ を分解可能なイデアルとする。$\mathfrak{a}$ の準素分解 $\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$ が以下の条件を満たすとき、準素分解 $\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$ は**最短**であるという。

(1) $i \neq j \Longrightarrow r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$

(2) 任意の $i = 1, 2, \cdots, n$ に対して $\displaystyle\bigcap_{j\neq i}\mathfrak{q}_j \not\subseteq \mathfrak{q}_i$

命題 6.1.77 準素分解可能なイデアルは最短な準素分解を持つ。

証明　まず、(1) が成り立つことを示すために、$\mathfrak{p}$-準素イデアルの共通部分が再び $\mathfrak{p}$-準素イデアルとなることを示す。$\mathfrak{q}_1, \mathfrak{q}_2$ を $\mathfrak{p}$-準素イデアルとする。このとき $r(\mathfrak{q}_1) = r(\mathfrak{q}_2) = \mathfrak{p}$ が成り立つ。まず、命題 6.1.59 より

$$r(\mathfrak{q}_1 \cap \mathfrak{q}_2) = r(\mathfrak{q}_1) \cap r(\mathfrak{q}_2) = \mathfrak{p} \cap \mathfrak{p} = \mathfrak{p}$$

が成り立つことに注意する。$xy \in \mathfrak{q}_1 \cap \mathfrak{q}_2$ とし、$y \notin \mathfrak{q}_1 \cap \mathfrak{q}_2$ とすると、ある i ($i = 1$ または $i = 2$) に対し $xy \in \mathfrak{q}_i$かつ $y \notin \mathfrak{q}_i$ であるから $x^n \in \mathfrak{q}_i$ を満たす $n \in \mathbb{N}$ が存在する。すなわち

$$x \in r(\mathfrak{q}_i) = \mathfrak{p} = r(\mathfrak{q}_1 \cap \mathfrak{q}_2)$$

であるから、$x^m \in \mathfrak{q}_1 \cap \mathfrak{q}_2$ を満たす $m \in \mathbb{N}$ が存在し、$\mathfrak{q}_1 \cap \mathfrak{q}_2$ は $\mathfrak{p}$-準素イデアルであることがわかる。したがって、根基をとったときに等しくなる準素イデアルをまとめることによって (1) が成り立つようにできる。

$\mathfrak{a}$ を環 A の分解可能なイデアルとし、$\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$ をその準素分解とする。このとき、集合の一般論から $A \cap B \subseteq C$ であれば $A \cap B \cap C = A \cap B$ である。よって、

$$\bigcap_{j\neq i}\mathfrak{q}_j \subseteq \mathfrak{q}_i$$

であれば、$\{\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_n\}$ から $\mathfrak{q}_i$ を取り除いても $\mathfrak{a}$ の準素分解

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \cdots \cap \mathfrak{q}_n$$

になる。このように、余分な準素イデアルを取り除くことによって定義 6.1.76(2) が成り立つようにできる。　**証明終**

補題 6.1.78 x を環 A の元、$\mathfrak{q}$ を A の $\mathfrak{p}$-準素イデアルとするとき、次が成り立つ。

(1) $x \in \mathfrak{q}$ のとき、$(\mathfrak{q} : x) = A$ である。

(2) $x \notin \mathfrak{q}$ のとき、$(\mathfrak{q} : x)$ は $\mathfrak{p}$-準素イデアルである。

(3) $x \notin \mathfrak{p}$ のとき、$(\mathfrak{q} : x) = \mathfrak{q}$ である。

証明 (1), (3) はイデアル商と準素イデアルの定義から直ちにわかる。
(2) を示す。 $y \in (\mathfrak{q} : x)$ をとると、$xy \in \mathfrak{q}$ より、$x \notin \mathfrak{q}$ であることから $y^n \in \mathfrak{q}$ となる $n \in \mathbb{N}$ が存在する。すなわち $y \in r(\mathfrak{q}) = \mathfrak{p}$ である。したがって $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$ が成り立つので、両辺の根基をとれば $r((\mathfrak{q} : x)) = \mathfrak{p}$ を得る。
$(\mathfrak{q} : x)$ が $\mathfrak{p}$-準素イデアルであることを示すために、$yz \in (\mathfrak{q} : x)$ かつ $y \notin r(\mathfrak{q}) = \mathfrak{p}$ とすると、$xyz \in \mathfrak{q}$ より $xz \in \mathfrak{q}$ となるから、$z \in (\mathfrak{q} : x)$ を得る。 **証明終**

命題 6.1.79 $\mathfrak{a}$ を環 A の分解可能なイデアルとし、$\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$ を $\mathfrak{a}$ の最短準素分解とする (各 $\mathfrak{q}_i$ は $\mathfrak{p}_i$-準素イデアルであるものとする)。このとき $\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n\}$ は、準素分解のとりかたに依らず一意的に定まる。

証明 $x \in A$ を任意にとると、

$$(\mathfrak{a} : x) = (\cap_{i=1}^n \mathfrak{q}_i : x) = \cap_{i=1}^n (\mathfrak{q}_i : x)$$

が成立する。したがって、補題 6.1.78(1),(2) より

$$r((\mathfrak{a} : x)) = \cap_{i=1}^n r((\mathfrak{q}_i : x)) = \cap_{x \notin \mathfrak{q}_j} \mathfrak{p}_i$$

である。このとき $r((\mathfrak{a} : x))$ が素イデアルであると仮定すると、命題 6.1.46 より $r((\mathfrak{a} : x)) = \mathfrak{p}_j$ となる j が存在する。したがって、$r((\mathfrak{a} : x))$ という形の素イデアルは、$\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ のいずれかとなる。
逆に、準素分解 $\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$ が最短であることから任意の i に対して $x_i \notin \mathfrak{q}_i$ かつ $x_i \in \cap_{j \neq i} \mathfrak{q}_i$ となるものが存在するので、補題 6.1.78(2) より $r((\mathfrak{a} : x_i)) = \mathfrak{p}_i$ が成り立つ。したがって、$\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n\}$ は $r((\mathfrak{a} : x))$ という形の素イデアル全体の集合と等しく、$\mathfrak{a}$ の準素分解の仕方に依らないことがわかる。 **証明終**

定義 6.1.80 命題 6.1.79 における素イデアル $\mathfrak{p}_i$ は、$\mathfrak{a}$ に**付随する素イデアル**という。特に、$\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n\}$ の包含関係に関する極小元のことを**極小素イデアル**といい、極小素イデアルに対応する準素イデアルのことを**孤立準素成分**という。

6.2 局所化

定義 6.2.1 A を環とするとき、次の性質を満たす部分集合 $S \subseteq A$ を A の**積閉集合**という。

(1) $1 \in S$

(2) $a, b \in S \Longrightarrow ab \in S$

命題 6.2.2 A を環、$\mathfrak{a}$ を A のイデアルとする。

(1) A が整域 $\Longleftrightarrow$ $A \setminus \{0\}$ が積閉集合

(2) $A \setminus \mathfrak{a}$ が積閉集合 $\Longleftrightarrow$ $\mathfrak{a}$ が A の素イデアル

証明 (1) を示す。

$$\begin{aligned} A \text{ が整域} &\Longleftrightarrow \forall a, b \in A, 「ab = 0 \Longrightarrow a = 0 \text{ または } b = 0」 \\ &\Longleftrightarrow \forall a, b \in A \setminus \{0\},\ ab \neq 0 \\ &\Longleftrightarrow A \setminus \{0\} \text{ が積閉集合} \end{aligned}$$

(2) を示す。

$$\begin{aligned} A \setminus \mathfrak{a} \text{ が積閉集合} &\Longleftrightarrow \forall a, b \in A, 「a, b \notin \mathfrak{a} \Longrightarrow ab \notin \mathfrak{a}」 \\ &\Longleftrightarrow \forall a, b \in A, 「ab \in \mathfrak{a} \Longrightarrow a \in \mathfrak{a} \text{ または } b \in \mathfrak{a}」 \\ &\Longleftrightarrow \mathfrak{a} \text{ が } A \text{ の素イデアル} \end{aligned}$$

証明終

命題 6.2.3 A を環、S をその積閉集合とし、$A \times S$ 上に

$$(a, s) \sim (b, t) \overset{def}{\Longleftrightarrow} \text{ある } u \in S \text{ に対して } (at - bs)u = 0$$

により関係 $\sim$ を定めると、$\sim$ は $A \times S$ 上の同値関係である。

証明 $as - as = 0$ より $(a, s) \sim (a, s)$ となる。
$(a, s) \sim (b, t)$ と仮定すると $(at - bs)u = 0$ なる $u \in S$ が存在するが、$(bs - at)u = 0$ となるので $(b, t) \sim (a, s)$ となる。
$(a, s) \sim (b, t)$ かつ $(b, t) \sim (c, u)$ と仮定すると $(at - bs)v = (bu - ct)w = 0$ なる $v, w \in S$ が存在する。このとき

$$\begin{aligned} (at - bs)uvw = atuvw - bsuvw = 0 \\ (bu - ct)svw = bsuvw - cstvw = 0 \end{aligned}$$

が成り立つので、辺々を加えて $atuvw - cstvw = (au - cs)tvw = 0$ を得る。すなわち $(a, s) \sim (c, u)$ となる。 **証明終**

命題 6.2.4 命題 6.2.3 において定義された同値関係による商集合を $S^{-1}A$ によって表し、(a, s) によって代表される $S^{-1}A$ の元を a/s によって表すことにする。このとき、$S^{-1}A$ 上に加法および乗法を

$$\begin{aligned} (a/s) + (b/t) = (at + bs)/st \\ (a/s)(b/t) = ab/st \end{aligned}$$

によって定めると、これらの演算は well-defined であり、さらに $S^{-1}A$ はこの演算によって環をなす。

証明　命題 6.2.6(1) に注意する。well-defined であることのみを示し、環をなすことの証明は省略する。
$a/s = a'/s'$, $b/t = b'/t'$ とする。このとき $(as' - a's)u = 0$, $(bt' - b't)v = 0$ となる $u, v \in S$ が存在する。すなわち

$$as'u = a'su$$
$$bt'v = b'tv$$

が成立している。すると

$$\begin{aligned}(at + bs)s't'uv &= (as'u)tt'v + (bt'v)ss'u \\ &= (a'su)tt'v + (b'tv)ss'u \\ &= (a't' + b's')stuv\end{aligned}$$

となるので $(at + bs)/st = (a't' + b's')/s't'$ が成立する。
同様に

$$(as'u)(bt'v) = (a'su)(b'tv)$$

であるから $(abs't' - a'b'st)uv = 0$、すなわち $ab/st = a'b'/s't'$ が成立する。

証明終

定義 6.2.5　$S^{-1}A$ を A の S による**局所化**という。

命題 6.2.6　A の局所化 $S^{-1}A$ について次が成り立つ。$a \in A$, $s, s' \in S$ とする。

(1)　$s'a/ss' = a/s$

(2)　単位元は s/s

(3)　零元は $0/s$

証明　(1) は、 $s(s'a) - (ss')a = 0$ が成り立つことから明らか。
(2)、(3) は、 演算の定義から明らか。

証明終

注意 6.2.7　$a/s = 0$ であっても $a = 0$ とは限らない。実際、$at = 0$ をみたす $t \in S$ が存在するとき $a/s = 0$ が成り立つ。

命題 6.2.8　A を環、S を A の積閉集合とする。このとき、$f : A \to S^{-1}A$ を

$$f(a) = a/1$$

と定めると、f は環の準同型写像である。

証明 $a, b \in A$ を任意にとると

$$\begin{aligned} f(a+b) &= (a+b)/1 = a/1 + b/1 = f(a) + f(b) \\ f(ab) &= ab/1 = (a/1)(b/1) = f(a)f(b) \\ f(1) &= 1/1 = 1 \end{aligned}$$

が成立するので、f は準同型写像である。 **証明終**

注意 6.2.9 命題 6.2.8 の準同型写像 f を、**局所化の自然な写像**という。f は単射とは限らない。実際

$$\mathrm{Ker}(f) = \{a \in A \mid \exists s \in S \ s.t. \ sa = 0\}$$

が成り立つ。したがって、特に、A が整域ならば f は単射である。

証明

$$\begin{aligned} a \in \mathrm{Ker}(f) &\Longleftrightarrow a/1 = 0 \\ &\Longleftrightarrow \exists s \in S \ s.t. \ sa = 0 \end{aligned}$$

より成り立つ。 **証明終**

系 6.2.10 命題 6.2.2 と命題 6.2.6 より次が成り立つ。

(1) A が整域であるとき

$$S = A \setminus \{0\}$$

とおくと、$S^{-1}A$ は A を含む最小の体である。このとき $S^{-1}A$ を $\mathrm{Frac}A$ と書き、A の**商体**という。

(2) A の素イデアル $\mathfrak{p}$ に対して

$$S = A \setminus \mathfrak{p}$$

とおくと、S は A の積閉集合である。このとき、$S^{-1}A$ を $A_{\mathfrak{p}}$ と書き、A の $\mathfrak{p}$ による局所化という。

証明 (2) は明らかである。
(1) を示す。 $0 \neq a/s \in S^{-1}A$ を任意にとると、$a \neq 0$ なので $a \in S$ である。したがって $s/a \in S^{-1}A$ という元が存在するので a/s は $S^{-1}A$ の単元である。
また、注意 6.2.9 より局所化の自然な写像 $f : A \to S^{-1}A$ は単射なので $A \subseteq S^{-1}A$ と見做すことができる。このとき、a/s は as^{-1} と見做せるので、A を含む体 F に対し、$as^{-1} \in F$ であることから $S^{-1}A$ の最小性がわかる。 **証明終**

環の場合と同様に、A-加群 M に対しても、次のように A の積閉集合 S による局所化を定義することができる。

定義 6.2.11 A を環、S を A の積閉集合、M を A-加群とする。このとき、$M \times S$ 上に関係 $\sim$ を

$$(x,s) \sim (y,t) \overset{def}{\iff} \exists u \in S \ s.t. \ u(sy - tx) = 0$$

によって定めると、これは $M \times S$ 上の同値関係である。この同値関係による商集合を $S^{-1}M$ と表し、(x,s) で代表される $S^{-1}M$ の元を x/s と書くことにする。
さらに、任意の $x/s, y/t \in S^{-1}M$、任意の $a/u \in S^{-1}A$ に対し

$$x/s + y/t = (tx + sy)/st$$
$$(a/u)(x/s) = ax/su$$

と定めることによって、$S^{-1}M$ は $S^{-1}A$-加群の構造を持つ。

命題 6.2.12 $f : M \to N$ を A-線形写像とする。このとき、$S^{-1}f : S^{-1}M \to S^{-1}N$ を

$$S^{-1}f(x/s) = f(x)/s$$

と定めると、$S^{-1}f$ は $S^{-1}A$-線形写像である。

証明 まず、$S^{-1}f$ が写像として well-defined であることを示す。 $x/s = x'/s'$ とすると、$t(s'x - sx') = 0$ となる $t \in S$ が存在する。よって、$ts'x = tsx'$ であるから、$ts'f(x) = tsf(x')$ である。すると

$$S^{-1}f(x/s) = f(x)/s = ts'f(x)/tss' = tsf(x')/tss' = f(x')/s' = S^{-1}f(x'/s')$$

が成り立ち、$S^{-1}f$ は代表元の取り方によらないことがわかる。
次に、$S^{-1}f$ が $S^{-1}A$-線形であることを示す。 $x/s, y/t \in S^{-1}M$、$a/u \in S^{-1}A$ をそれぞれ任意にとると

$$\begin{aligned} S^{-1}f(x/s + y/t) = S^{-1}f(tx + sy/st) = f(tx + sy)/st &= f(x)/s + f(y)/t \\ &= S^{-1}f(x) + S^{-1}f(y) \end{aligned}$$

$$\begin{aligned} S^{-1}f((a/u)(x/s)) = S^{-1}f(ax/su) = af(x)/su &= (a/u)(f(x)/s) \\ &= (a/u)S^{-1}f(x/s) \end{aligned}$$

となるので $S^{-1}f$ は $S^{-1}A$-線形写像である。 **証明終**

命題 6.2.13 $f : M \to N$ を単射な A-線形写像とすると、$S^{-1}f : S^{-1}M \to S^{-1}N$ も単射である。

証明 $x/s \in \operatorname{Ker} S^{-1}f$ をとると、$f(x)/s = 0$ より $uf(x) = 0$ となる $u \in S$ が存在する。$ux \in \operatorname{Ker} f$ より $ux = 0$、すなわち $x/s = ux/us = 0$ である。 **証明終**

系 6.2.14 A を環、$\mathfrak{a}, \mathfrak{b}$ を A のイデアル、S を A の積閉集合とするとき、$\mathfrak{a} \subseteq \mathfrak{b}$ ならば $S^{-1}\mathfrak{a}$ は $S^{-1}\mathfrak{b}$ の部分 $S^{-1}A$-加群と見做すことができる。特に、$S^{-1}\mathfrak{a}, S^{-1}\mathfrak{b}$ は $S^{-1}A$ のイデアルと見做すことができる。

系 6.2.14 より、環 A のイデアル $\mathfrak{a}$ の局所化の自然な写像 $f : A \to S^{-1}A$ による拡大 $\mathfrak{a}^e = S^{-1}Af(\mathfrak{a})$ と $S^{-1}A$-加群 $S^{-1}\mathfrak{a}$ が同一視できることがわかる。

次の命題は、$S^{-1}A$ のイデアルはこのような拡大イデアルのみであるということを主張している。

命題 6.2.15 $f : A \to S^{-1}A$ を局所化の自然な写像とする。このとき $S^{-1}A$ のイデアル I に対して、$I = S^{-1}\mathfrak{a}$ となる A のイデアル $\mathfrak{a}$ が存在する。

証明 $x/s \in I$ をとると $s/1 \in S^{-1}A$ より $x/1 \in I$。したがって $x \in I^c$ であるから、$x/s \in I^{ce}$ である。ゆえに $I \subseteq I^{ce}$ である。一方、$I^{ce} \subseteq I$ は一般に成り立つ (命題 6.1.68) ので、$I = I^{ce}$ である。したがって $\mathfrak{a}$ として I^c をとればよい。 **証明終**

一般に、イデアル $\mathfrak{a}$ に対して、$\mathfrak{a}^{ece} = \mathfrak{a}^e$、$\mathfrak{a}^{cec} = \mathfrak{a}^c$ が成り立つ (系 6.1.69) ことに注意すれば、命題 6.2.15 より次を得る。

系 6.2.16 A のイデアル $\mathfrak{a}$ で $\mathfrak{a} = \mathfrak{a}^{ec}$ となるものと、$S^{-1}A$ のイデアルの間には包含関係による順序を保つ 1 対 1 の対応

$$\mathfrak{a} \longleftrightarrow S^{-1}\mathfrak{a}$$

が存在する。

命題 6.2.17 局所化は、有限個の共通部分をとる操作と可換である。すなわち S を環 A の積閉集合、$\mathfrak{a}, \mathfrak{b}$ を A のイデアルとするとき、

$$S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b} = S^{-1}(\mathfrak{a} \cap \mathfrak{b})$$

が成り立つ。

証明 $\alpha \in S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}$ をとると、ある $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, $s, t \in S$ を用いて $\alpha = a/s = b/t$ と表せるので、ある $u \in S$ に対して $(ta - sb)u = 0$ と書ける。したがって $tua = sub \in \mathfrak{a} \cap \mathfrak{b}$ である。このとき

$$a/s = tua/tus \in S^{-1}(\mathfrak{a} \cap \mathfrak{b})$$

となるので $S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b} \subseteq S^{-1}(\mathfrak{a} \cap \mathfrak{b})$ である。

逆に、$a/s \in S^{-1}(\mathfrak{a} \cap \mathfrak{b})$ をとれば $a \in \mathfrak{a} \cap \mathfrak{b}$ ととれるので $a/s \in S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}$ が成り立つ。 **証明終**

命題 6.2.18 局所化は根基をとる操作と可換である。すなわち S を環 A の積閉集合、$\mathfrak{a}$ を A のイデアルとするとき

$$r(S^{-1}\mathfrak{a}) = S^{-1}r(\mathfrak{a})$$

が成り立つ。

証明 命題 6.1.68(3) より一般に $r(\mathfrak{a})^e \subseteq r(\mathfrak{a}^e)$ すなわち $S^{-1}r(\mathfrak{a}) \subseteq r(S^{-1}\mathfrak{a})$ が成り立つ。
一方で、$x/s \in r(S^{-1}\mathfrak{a})$ をとると、$(x/s)^n \in S^{-1}\mathfrak{a}$ をみたす自然数 n があるから

$$u(tx^n - s^n a) = 0$$

となる $t, u \in S$ および $a \in \mathfrak{a}$ が存在する。 すると

$$u^n t^n x^n = u^n t^{n-1} s^n a \in \mathfrak{a}$$

であるから、$utx \in r(\mathfrak{a})$ である。したがって

$$x/s = utx/uts \in S^{-1}r(\mathfrak{a})$$

が成り立つ。 **証明終**

命題 6.2.19 $f : A \to S^{-1}A$ を局所化の自然な写像、$\mathfrak{q}$ を A の $\mathfrak{p}$-準素イデアルとするとき、次が成り立つ。

(1) $S \cap \mathfrak{p} \neq \emptyset$ ならば $S^{-1}\mathfrak{q} = S^{-1}A$。

(2) $S \cap \mathfrak{p} = \emptyset$ ならば $S^{-1}\mathfrak{q}$ は $S^{-1}\mathfrak{p}$-準素イデアルであり $(S^{-1}\mathfrak{q})^c = \mathfrak{q}$。

証明

(1) $x \in S \cap \mathfrak{p}$ をとると、$x \in \mathfrak{p} = r(\mathfrak{q})$ より $x^n \in \mathfrak{q}$ をみたす n が存在する。すると S が積閉集合であることから $x^n \in S$ も成り立つので $x^n/1 \in S^{-1}\mathfrak{q}$ は $S^{-1}A$ の単元である。

(2) まず $\mathfrak{q}^{ec} = \mathfrak{q}$ を示す。
$\mathfrak{q} \subseteq \mathfrak{q}^{ec}$ は一般に成り立つ (命題 6.1.68)。一方 $x \in \mathfrak{q}^{ec}$ をとると

$$f(x) = x/1 \in \mathfrak{q}^e = S^{-1}\mathfrak{q}$$

より $x/1$ はある $S^{-1}\mathfrak{q}$ の元 a/s を用いて $x/1 = a/s$ と書ける。すなわち $(sx - a)t = 0$ となる $s, t \in S$ が存在する。すると $tsx = at \in \mathfrak{q}$ であるが、$S \cap \mathfrak{p} = \emptyset$ より $ts \notin \mathfrak{p}$ である。よって、$x \in \mathfrak{q}$ であり、$\mathfrak{q}^{ec} \subseteq \mathfrak{q}$ が成り立つ。したがって $(S^{-1}\mathfrak{q})^c = \mathfrak{q}$ が成り立つ。

次に $S^{-1}\mathfrak{q}$ が $S^{-1}\mathfrak{p}$-準素イデアルであることを示す。$(x/s)(y/t) \in S^{-1}\mathfrak{q}$ かつ $y/t \notin S^{-1}\mathfrak{q}$ と仮定すると

$$(uxy - sta)v = 0$$

となる $u, v \in S$ および $a \in \mathfrak{q}$ が存在する。すなわち $uvxy \in \mathfrak{q}$ となる $u, v \in S$ が存在する。ここで $uv \notin \mathfrak{p}$ に注意すれば、$xy \in \mathfrak{q}$ がわかる。いま、仮定より $y \notin \mathfrak{q}$ であるから、$\mathfrak{q}$ が準素イデアルであることより $x^n \in \mathfrak{q}$ となる $n \in \mathbb{N}$ が存在する。したがって

$$(x/s)^n = x^n/s^n \in S^{-1}\mathfrak{q}$$

が成り立つ。また、命題 6.2.18 より

$$r(S^{-1}\mathfrak{q}) = S^{-1}r(\mathfrak{q}) = S^{-1}\mathfrak{p}$$

が成り立つので、$S^{-1}\mathfrak{q}$ は $S^{-1}\mathfrak{p}$-準素イデアルである。

証明終

注意 6.2.20 命題 6.1.73 より、準素イデアルの引き戻しは準素イデアルであることに注意する。すると、命題 6.2.19 より系 6.2.16 の A のイデアルと $S^{-1}A$ のイデアルとの対応関係において、$S^{-1}A$ の準素イデアルと A の準素イデアルで根基が S と交わらないものが 1 対 1 に対応することがわかる。

命題 6.2.21 $f : A \to S^{-1}A$ を局所化の自然な写像、$\mathfrak{a}$ を A の分解可能なイデアルとし、$\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$ を $\mathfrak{a}$ の最短準素分解とする (各 $\mathfrak{q}_i$ は $\mathfrak{p}_i$-準素イデアルであるとする)。さらに、添字を付け替えて、S が $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_m$ と交わらず、$\mathfrak{p}_{m+1}, \mathfrak{p}_{m+2}, \cdots, \mathfrak{p}_n$ と交わっているものとする。このとき

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i,\ (S^{-1}\mathfrak{a})^c = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

が成立する。さらに、これらは $S^{-1}\mathfrak{a}$ および $(S^{-1}\mathfrak{a})^c$ の最短準素分解である。

証明 命題 6.2.17 より $S^{-1}\mathfrak{a} = S^{-1}(\cap_{i=1}^{n}\mathfrak{q}_i) = \cap_{i=1}^{n}S^{-1}\mathfrak{q}_i$ が成り立ち、また、命題 6.2.19 より $\cap_{i=1}^{n}S^{-1}\mathfrak{q}_i = \cap_{i=1}^{m}S^{-1}\mathfrak{q}_i$ が成り立つ。
いま $S^{-1}\mathfrak{q}_i$ は $S^{-1}\mathfrak{p}_i$-準素イデアルであり、$\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_m$ が互いに相異なることから $S^{-1}\mathfrak{p}_1, S^{-1}\mathfrak{p}_2, \cdots, S^{-1}\mathfrak{p}_m$ も互いに相異なる。(もし、ある $i \neq j$ に対して $S^{-1}\mathfrak{p}_i = S^{-1}\mathfrak{p}_j$ が成り立ったとすると、注意 6.2.20 に矛盾する。) このとき、$\cap_{j\neq i}S^{-1}\mathfrak{q}_j \subseteq S^{-1}\mathfrak{q}_i$(ただし、$1 \leq i, j \leq m$) となる i が存在したとすると、両辺を f で引き戻せば、$\cap_{j\neq i}\mathfrak{q}_j \subseteq \mathfrak{q}_i (1 \leq i, j \leq m)$ となり、$\cap_{j\neq i}\mathfrak{q}_j \not\subseteq \mathfrak{q}_i (1 \leq i, j \leq n)$ に矛盾する。したがって $S^{-1}\mathfrak{a} = \cap_{i=1}^{m}S^{-1}\mathfrak{q}_i$ は最短準素分解である。

また、これより

$$(S^{-1}\mathfrak{a})^c = \bigcap_{i=1}^{m}(S^{-1}\mathfrak{q}_i)^c = \bigcap_{i=1}^{m}\mathfrak{q}_i$$

を得る。これは、$\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$ が最短準素分解であることから、明らかに最短準素分解となっている。 **証明終**

命題 6.2.22 $\mathfrak{a}$ を環 A の分解可能なイデアルとするとき、$\mathfrak{a}$ の孤立準素成分は最短準素分解のとりかたに依らず、$\mathfrak{a}$ に依ってのみ定まる。

証明 $\mathfrak{p}$ を $\mathfrak{a}$ の極小素イデアルとするとき ($\mathfrak{q}$ を対応する孤立準素成分とする)、

$$S = A \setminus \mathfrak{p}$$

とおくと S は A の積閉集合である。すると $\mathfrak{p}' \not\subseteq \mathfrak{p}$ であるような A の任意の素イデアル $\mathfrak{p}'$ に対して $\mathfrak{p}' \cap S \neq \emptyset$ であるから命題 6.2.21 より

$$(S^{-1}\mathfrak{a})^c = \mathfrak{q}$$

が成り立つ。S は $\mathfrak{p}$ から定まり、$\mathfrak{p}$ は $\mathfrak{a}$ から定まっていたので (命題 6.1.79)、$\mathfrak{q}$ も $\mathfrak{a}$ のみに依ることがわかる。 **証明終**

6.3 整従属

定義 6.3.1 A を環 B の部分環とする。このとき、$\alpha \in B$ が A 係数の monic 多項式の根となるとき、すなわち

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0$$

となる $n \in \mathbb{N}$ と $a_i \in A$ が存在するとき、x は ***A* 上整**であるという。

命題 6.3.2 A を環 B の部分環、$x \in B$ とするとき、次は同値である。

(1) $x \in B$ は A 上整。

(2) $A[x]$ は有限生成 A-加群。

(3) B の部分環かつ有限生成 A-加群でもある環 C が存在して、$A[x] \subseteq C$ となる。

(4) 有限生成 A-加群であり、かつ $A[x]$-加群として忠実な加群 M が存在する。

証明 (1)$\Longrightarrow$(2) を示す。$x^n+a_1x^{n-1}+\cdots+a_n=0$ をみたす $n\in\mathbb{N}$ と $a_1,a_2,\cdots,a_n\in A$ が存在するので、

$$x^n=-(a_1x^{n-1}+\cdots+a_n)$$

が成り立つ。よって x の n 次以上のベキは、$\{x^{n-1},x^{n-2},\cdots,x,1\}$ の A 上の線形結合で書けることがわかる。したがって

$$A[x]=Ax^{n-1}+Ax^{n-2}+\cdots+A$$

が成り立つ。

(2)$\Longrightarrow$(3) は、 $C=A[x]$ とおけば条件を満たす。

(3)$\Longrightarrow$(4) を示す。 $M=C$ とおく。C が環であることから、$y\in A[x]$ が $yC=0$ をみたせば $y\cdot 1=y=0$ となるので、M は忠実 $A[x]$-加群となる。

(4)$\Longrightarrow$(1) を示す。 $\phi:M\to M$ を $\phi(y)=xy$ とし $\mathfrak{a}=A$ とおくと M が $A[x]$-加群であることから、$\phi(M)=xM\subseteq M$ が成り立つので命題 6.1.53 の条件を満たす。したがって ϕ は

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

となる n および $a_i\in A$ が存在する。このとき、上式の左辺は、M の元に $x^n+a_1x^{n-1}+\cdots+a_n$ を掛ける写像であるが、M が忠実であることから、

$$x^n+a_1x^{n-1}+\cdots+a_n=0$$

が成り立つ。 **証明終**

系 6.3.3 $x_1,x_2,\cdots,x_n\in B$ を A 上整な元とすると、$A[x_1,x_2,\cdots,x_n]$ は有限生成 A-加群である。

証明 n についての帰納法で証明する。

$n=1$ のときは命題 6.3.2 より成り立つ。

$n-1$ まで命題が成立すると仮定すると $A_{n-1}=A[x_1,x_2,\cdots,x_{n-1}]$ は有限生成 A-加群である。すると x_n が A_{n-1} 上整であるので $A_n=A[x_1,x_2,\cdots,x_n]=A_{n-1}[x_n]$ は有限生成 A_{n-1}-加群である。このとき、$y_1,y_2,\cdots,y_m$ を A 上の A_{n-1} の生成元、$z_1,z_2,\cdots,z_l$ を A_{n-1} 上の A_n の生成元とすれば、A_n は $\{y_iz_j|1\leq i\leq m,\ 1\leq j\leq l\}$ によって A 上生成されるので有限生成 A-加群である。 **証明終**

定理 6.3.4 A 上整であるような B の元全体の集合 C は、A を含む B の部分環である。

証明 $x,y\in C$ をとると、$A[x,y]$ は系 6.3.3 より有限生成 A-加群である。したがって、$A[x-y],A[xy]\subseteq A[x,y]$ に注意すれば、命題 6.3.2(3) より $x-y,xy$ は A 上整、すなわち $x-y,xy\in C$ が成り立つ。 **証明終**

定義 6.3.5 $A \subseteq B$ を環とするとき、B の元で A 上整なもの全体の集合は、定理 6.3.4 より B の部分環となる。この環のことを A の B における**整閉包**という。A 自身が B における A の整閉包となっているとき、A は B で**整閉**であるという。特に自身の商体において整閉であるような整域のことを**整閉整域**という。一方 B における A の整閉包が B と一致するとき、B は A 上**整**であるという。

命題 6.3.6 A を環 B の部分環とし、C を B における A の整閉包とするとき、C は B において整閉である。

証明 $x \in B$ が C 上整であるとすると、

$$x^n + c_1 x^{n-1} + \cdots + c_n = 0$$

となる $n \in \mathbb{N}$ と $c_1, c_2, \cdots, c_n \in C$ が存在する。このとき、$C' = A[c_1, c_2, \cdots, c_n]$ とおくと、命題 6.3.2 より C' は有限生成 A-加群であり、また、x が C' 上整であることから $C'[x]$ は有限生成 C'-加群である。したがって $C'[x]$ は有限生成 A-加群であるので、再び命題 6.3.2 より x が A 上整であることがわかる。すなわち $x \in C$ である。 **証明終**

命題 6.3.7 A を環 B の部分環とし、B は A 上整であるとする。また、$\iota : A \to B$ を包含写像、$\mathfrak{q}$ を B の素イデアルとし、A の素イデアル $\mathfrak{p}$ を $\mathfrak{p} = \iota^{-1}(\mathfrak{q}) = \mathfrak{q} \cap A$ とおく。このとき、$\mathfrak{q}$ が B の極大イデアルであることと、$\mathfrak{p}$ が A の極大イデアルであることは同値である。

証明

$$A/\mathfrak{p} \text{ が体} \iff B/\mathfrak{q} \text{ が体}$$

を示せばよい。

$\pi : B \to B/\mathfrak{q}$ を自然な写像とすると、$\mathrm{Ker}\, \pi \circ \iota = \mathfrak{p}$ であるから、$A/\mathfrak{p}$ は $B/\mathfrak{q}$ の部分環と見做せる。すると、任意の $x \in B$ に対して、$x^n + a_1 x^{n-1} + \cdots + a_n = 0$ となる $n \in \mathbb{N},\ a_i \in A$ が存在することから、$B/\mathfrak{q}$ の元 $\overline{x}$ に対して

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

が成り立つので、$B/\mathfrak{q}$ は $A/\mathfrak{p}$ 上整であることに注意する。

まず、$A/\mathfrak{p}$ が体であると仮定し、$\overline{0} \neq \overline{x} \in B/\mathfrak{q}$ を任意にとる。このとき

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

となる $n \in \mathbb{N}$ および $\overline{a_i} \in A/\mathfrak{p}$ が存在する。このような n を最小にとると、

$$\begin{aligned} \overline{a_n} &= -(\overline{x}^n + \overline{a_1} \cdot \overline{x}^{n-1} + \cdots + \overline{a_{n-1}} \cdot \overline{x}) \\ &= -\overline{x}(\overline{x}^{n-1} + \overline{a_1} \cdot \overline{x}^{n-2} + \cdots + \overline{a_{n-1}}) \end{aligned}$$

となるが、$B/\mathfrak{q}$ が整域であることから $\overline{a}_n \neq \overline{0}$ である ($\overline{a}_n = 0$ とすると、$\overline{x}^{n-1} + \overline{a_1} \cdot \overline{x}^{n-2} + \cdots + \overline{a_{n-1}} = 0$ となって n の最小性に反する)。ゆえに、

$$\overline{x}^{-1} = -\overline{a_n}^{-1}(\overline{x}^{n-1} + \overline{a_1} \cdot \overline{x}^{n-2} + \cdots + \overline{a_{n-1}})$$

である。すると、仮定より $\overline{a_n}^{-1} \in A/\mathfrak{p} \subseteq B/\mathfrak{q}$ であったので $\overline{x}^{-1} \in B/\mathfrak{q}$ となる。したがって、$B/\mathfrak{q}$ は体である。

逆に、$B/\mathfrak{q}$ が体であるとし、$\overline{0} \neq \overline{y} \in A/\mathfrak{p}$ を任意にとる。このとき、$\overline{y}^{-1} \in B/\mathfrak{q}$ であるので、$\overline{y}^{-1}$ は $A/\mathfrak{p}$ 上整であるから、

$$\overline{y}^{-m} + \overline{a'_1} \cdot \overline{y}^{1-m} + \cdots + \overline{a'_m} = 0$$

となる $m \in \mathbb{N}$, $\overline{a'_i} \in A/\mathfrak{p}$ が存在する。両辺に $\overline{y}^{m-1}$ を掛けて

$$\overline{y}^{-1} = -(\overline{a'_1} + \overline{a'_2} \cdot \overline{y} \cdots + \overline{a'_m} \cdot \overline{y}^{m-1}) \in A/\mathfrak{p}$$

を得る。すなわち、$A/\mathfrak{p}$ は体である。 **証明終**

命題 6.3.8 A を環 B の部分環とし、B は A 上整であるとする。このとき、$\mathfrak{q} \subseteq \mathfrak{q}'$ をそれぞれ B の素イデアルとすると、

$$\mathfrak{q} \cap A = \mathfrak{q}' \cap A \Longrightarrow \mathfrak{q} = \mathfrak{q}'$$

が成り立つ。

証明 $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$ とおく。任意の $x \in B$ に対し、

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

となる $n \in \mathbb{N}$, $a_i \in A$ が存在するので、$x/s \in B_{\mathfrak{p}}$ に対し、

$$(x/s)^n + (a_1/s)(x/s)^{n-1} + (a_2/s^2)(x/s)^{n-2} + \cdots + (a_n/s^n) = 0$$

が成り立つ。すなわち x/s は $A_{\mathfrak{p}}$ 上整であり、したがって、$B_{\mathfrak{p}}$ は $A_{\mathfrak{p}}$ 上整であることに注意する。

$\mathfrak{m}$ を $\mathfrak{p}$ の $A_{\mathfrak{p}}$ への拡大とすると、$\mathfrak{m}$ は A の極大イデアルである。また、$\mathfrak{n}$, $\mathfrak{n}'$ をそれぞれ $\mathfrak{q}$, $\mathfrak{q}'$ の $B_{\mathfrak{p}}$ への拡大とすると、$\mathfrak{n} \subseteq \mathfrak{n}'$ であり、$\mathfrak{n} \cap A_{\mathfrak{p}} = \mathfrak{n}' \cap A_{\mathfrak{p}} = \mathfrak{m}$ が成り立つ ($\mathfrak{n} \cap A_{\mathfrak{p}} = \mathfrak{q}_{\mathfrak{p}} \cap A_{\mathfrak{p}} = (\mathfrak{q} \cap A)_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}} = \mathfrak{m}$ である。$\mathfrak{n}'$ も同様)。したがって、命題 6.3.7 より $\mathfrak{n}$, $\mathfrak{n}'$ は $B_{\mathfrak{p}}$ の極大イデアルとなるので、$\mathfrak{n} \subseteq \mathfrak{n}'$ より、$\mathfrak{n} = \mathfrak{n}'$ でなければならない。よって、系 6.2.16 より、$\mathfrak{q} = \mathfrak{q}'$ となる。 **証明終**

命題 6.3.9 A を環 B の部分環とし、C を B における A の整閉包とする。さらに S を A の積閉集合とすると、$S^{-1}C$ は $S^{-1}B$ における $S^{-1}A$ の整閉包である。

証明 $x/s \in S^{-1}C$ をとる。このとき、$x \in C,\ s \in S$ として良い。$x \in C$ が A 上整であることから、ある $n \in \mathbb{N}$ と $a_i \in A$ が存在して

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

が成り立つ。よって

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

が成り立つ。すなわち x/s は $S^{-1}A$ 上整である。したがって $S^{-1}C$ は $S^{-1}A$ 上整である。

逆に $y/t \in S^{-1}B$ を $S^{-1}A$ 上整な元とすれば

$$(y/t)^m + (b_1/t_1)(y/t)^{m-1} + \cdots + b_m/t_m = 0$$

となる $n \in \mathbb{N},\ b_i \in A,\ t_i \in S$ が存在する。そこで $u = t_1 t_2 \cdots t_m$ とおいて上式の両辺に $(tu)^m$ を掛ければ

$$((yu)^m + b_1 t_2 t_3 \cdots t_m t(yu)^{m-1} + \cdots + b_m t_1 t_2 \cdots t_{m-1} t^m u^{n-1})v = 0$$

となる $v \in S$ が存在することがわかる。このとき、yuv は A 上整であり $yuv \in C$ となる。したがって $y/t = yuv/tuv \in S^{-1}C$ となる。 **証明終**

定義 6.3.10 $A \subseteq B$ を環、$\mathfrak{a}$ を A のイデアルとする。このとき、B の元 x が **$\mathfrak{a}$ 上整**であるとは、x が最高次以下の係数が $\mathfrak{a}$ に属するような monic 多項式の根となることである。$\mathfrak{a}$ 上整であるような B の元全体の集合を B における $\mathfrak{a}$ の**整閉包**という。

命題 6.3.11 A を環 B の部分環とし、C を B における A の整閉包とする。$\mathfrak{a}^e$ を包含写像による A のイデアル $\mathfrak{a}$ の C への拡大とすると、B における $\mathfrak{a}$ の整閉包は $r(\mathfrak{a}^e)$ である。

証明 $x \in B$ が $\mathfrak{a}$ 上整であるとすると

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

となる $n \in \mathbb{N},\ a_1, a_2, \cdots, a_n \in \mathfrak{a}$ が存在する。したがって x は A 上整であるので $x \in C$ となり、また

$$x^n = -(a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n)$$

より $x^n \in \mathfrak{a}^e$ となるので、$x \in r(\mathfrak{a}^e)$ が成り立つ。

逆に、$x \in r(\mathfrak{a}^e)$ をとると、ある $n \in \mathbb{N}$ が存在して $x^n \in \mathfrak{a}^e$ となる。すなわち

$$x^n = \sum_{i=1}^{m} a_i x_i$$

となる $m \in \mathbb{N},\ a_i \in \mathfrak{a},\ x_i \in C$ が存在する。このとき、各 x_i は A 上整であるから、系 6.3.3 より

$$M = A[x_1, x_2, \cdots, x_m]$$

は有限生成 A-加群であり、また、

$$x^n M \subseteq \sum_{i=1}^{m} a_i x_i M \subseteq \mathfrak{a}M$$

が成り立つ。そこで M 上の自己準同型 ϕ を x^n を掛ける写像とすれば命題 6.1.53 が適用でき、x^n が $\mathfrak{a}$ 上整であることがわかる。したがって、x は $\mathfrak{a}$ 上整である。

証明終

命題 6.3.12 A を整域 B の部分環で整閉整域であるとする。また、$x \in B$ を A のイデアル $\mathfrak{a}$ 上整な元とする。このとき、x は $K = \mathrm{Frac}A$ 上代数的な元であり、K の x の最小多項式は最高次以外の係数が $r(\mathfrak{a})$ に属する。

証明　x は $\mathfrak{a}$ 上整なので、明らかに K 上代数的である。x のすべての共役元 x_1, x_2,..., x_n を含む K の拡大体 L をとる。
すると各 x_i が x と K 上共役であるので、x の整従属の関係式が $K[t]$ に属していることに注意すれば、x_i は x と同じ整従属の関係式を満たすことがわかる。すなわち、各 x_i は $\mathfrak{a}$ 上整である。K 上の x の最小多項式は $\Pi(t - x_i)$ で与えられるので、最小多項式の係数は $x_1, x_2, \cdots, x_n$ の多項式となる。すると命題 6.3.11 より $\mathfrak{a}$ 上整な元は和、差、積で閉じていたので、最小多項式の係数は $\mathfrak{a}$ 上整な K の元である。A が K 内で整閉であることから命題 6.3.11 において $r(\mathfrak{a}^e) = r(\mathfrak{a})$ なので、これらの係数は $r(\mathfrak{a})$ に属する。

証明終

命題 6.3.14 を示すためには、体論および線形代数学から次の補題が必要となる。

補題 6.3.13 L/K を体の拡大とするとき、任意の $\alpha \in L$ に対して $\phi_\alpha : L \to L$ を、$v \in L$ に対し $\phi_\alpha(v) = \alpha v$ と定めると ϕ_α は K-線形写像となる。このとき、L の適当な K 上の基底に対する ϕ_α の行列表示 A_α が得られるが、写像 $T : L \to K$ を $v \in L$ に対し $T(v) = \mathrm{Tr}A_\alpha$ とおくと、T は L の基底の取り方に依らない。そこで、この T を L/K の**トレース**といい、$\mathrm{Tr}_{L/K}$ によって表す。$\mathrm{Tr}_{L/K}(v)$ を $\boldsymbol{v}$ **のトレース**という。

また、写像 $\psi : L \times L \to K$ を $\psi(x, y) = \mathrm{Tr}_{L/K}(xy)$ とおくと、ψ は K-双線形写像となり、L/K が分離拡大であるとき、ψ は非退化である。すなわち

- 任意の $x \in L$ に対して $\psi(x, y) = 0$ ならば、$y = 0$ である。
- 任意の $y \in L$ に対して $\psi(x, y) = 0$ ならば、$x = 0$ である。

が成り立つ。

命題 6.3.14 A を整閉整域とし $K = \mathrm{Frac}A$、L を K の有限次分離拡大体、B を L における A の整閉包とすると、K 上の L の基底 $\{v_1, v_2, \cdots, v_n\}$ で

$$B \subseteq \sum_{i=1}^{n} Av_i$$

となるものが存在する。

証明 補題 6.3.13 の記号を用いる。

$v \in L$ を任意にとると、v は K 上代数的なので

$$a_0 v^r + a_1 v^{r-1} + \cdots + a_r = 0$$

となる $r \in \mathbb{N}$, $a_i \in K$ が存在する。このとき、A の適当な元を両辺に掛けることによって、$a_i \in A$ であるとしてよい。また、両辺に a_0^{r-1} を掛けることにより、$a_0 v$ は A 上整であることがわかる。したがって、L の K 上の基底が与えられたとき、それらに A の適当な元を掛けることによってすべてが B に属する L の K 上の基底を得ることができる。そこで、$u_1, u_2, \cdots, u_n$ を L の K 上の基底で $u_i \in B$ $(i = 1, 2, \cdots, n)$ であるものとする。

いま、L/K が分離的であることから ψ は非退化である。すなわち、任意の $0 \neq x \in L$ に対して、$\psi(x, \cdot) : L \to K$ は全射な K-線形写像である。したがって、$\psi(u_i, v_j) = \mathrm{Tr}_{L/K}(u_i v_j) = \delta_{ij}$ となる L の K 上の基底 $v_1, v_2, \cdots, v_n$ が存在する。$x \in B$ を任意にとり、x が

$$x = \sum_{i=1}^{n} x_i v_i \ (x_i \in K)$$

と表されているとすると、$u_i \in B$ より、$xu_i \in B$ である。このとき、任意の $y \in L$ に対して y の K 上の最小多項式を

$$t^m + a_1 t^{m-1} + \cdots + a_m$$

とすると、

$$\mathrm{Tr}_{L/K}(y) = -[L : K(y)]a_1$$

が成り立つことに注意すれば、命題 6.3.12 より ($\mathfrak{a} = A$ として)

$$\mathrm{Tr}_{L/K}(xu_i) \in A$$

となる。すると、このとき

$$\mathrm{Tr}_{L/K}(xu_i) = \mathrm{Tr}_{L/K}(\sum_{j=1}^{n} x_j u_i v_j) = \sum_{j=1}^{n} \mathrm{Tr}_{L/K}(x_j u_i v_j) = \sum_{j=1}^{n} x_j \mathrm{Tr}_{L/K}(u_i v_j) = \sum_{j=1}^{n} x_j \delta_{ij} = x_i$$

であるので、$x_i \in A$ となる。したがって $x \in \sum_{i=1}^{n} Av_i$、すなわち $B \subseteq \sum_{i=1}^{n} Av_i$ が成り立つ。 **証明終**

6.4 Noether 環、Dedekind 環

命題 6.4.1 A を環とするとき、次の三条件は同値である。

(1) 任意の空でない A のイデアルの集合 $\mathscr{I}$ は、包含関係に関する極大元を持つ。

(2) A の任意のイデアルは有限生成である。

(3) A の任意のイデアルの昇鎖 $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ に対し、自然数 n が存在し

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots$$

が成立する。

証明 (1)$\Longrightarrow$(2) を示す。A のイデアル $\mathfrak{a}$ を任意にとり、$\mathscr{I}$ を $\mathfrak{a}$ に含まれる A の有限生成イデアル全体の集合とすると、$\{0\} \in \mathscr{I}$ より $\mathscr{I} \neq \emptyset$ であるから、$\mathscr{I}$ は極大元 $\mathfrak{a}_0$ をもつ。このとき、$\mathfrak{a} \neq \mathfrak{a}_0$ ならば $x \in \mathfrak{a} \setminus \mathfrak{a}_0$ が存在する。しかし、$\mathfrak{a}_1 = \mathfrak{a}_0 + (x)$ とおくと $\mathfrak{a}_1$ は有限生成かつ $\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1$ であるから $\mathfrak{a}_0$ のとり方に反する。したがって $\mathfrak{a} = \mathfrak{a}_0$ であり $\mathfrak{a}$ は有限生成である。

(2)$\Longrightarrow$(3) を示す。A のイデアルの昇鎖 $(\mathfrak{a}_i)_{i\in\mathbb{N}}$ を任意にとる。すると、定理 6.1.42 の証明と同様に

$$\mathfrak{a} = \bigcup_{i\in\mathbb{N}} \mathfrak{a}_i$$

は A のイデアルとなる。したがって、仮定より $\mathfrak{a}$ は有限生成である。そこで、$\mathfrak{a} = (x_1, x_2, \cdots, x_r)$ とする。このとき、$x_1, x_2, \cdots, x_r \in \mathfrak{a}_n$ となる $n \in \mathbb{N}$ が存在するので、$\mathfrak{a} = \mathfrak{a}_n$ である。したがって $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$ が成り立つ。

(3)$\Longrightarrow$(1) を示す。対偶を示す。空でない A のイデアルの集合 $\mathscr{I}$ が極大元を持たないと仮定すると、任意の $\mathfrak{a} \in \mathscr{I}$ に対し、$\mathfrak{a} \subsetneqq \mathfrak{b}$ となる $\mathfrak{b} \in \mathscr{I}$ が存在するので、$\mathscr{I}$ の元から無限に続く真増大列を構成することができる。 **証明終**

定義 6.4.2 命題 6.4.1 の同値な三条件を満たす環を **Noether 環**という。

注意 6.4.3 定義 6.4.1(1) の条件を**極大条件**、(3) の条件を**昇鎖条件**という。

命題 6.4.4 A を Noether 環とする。このとき、A の積閉集合 S での局所化 $S^{-1}A$ は Noether 環である。また、A のイデアル $\mathfrak{a}$ による剰余環 $A/\mathfrak{a}$ も Noether 環である。

証明 系 6.2.16 より $S^{-1}A$ のイデアルの集合と A のイデアル $\mathfrak{a}$ で $\mathfrak{a}^{ec} = \mathfrak{a}$ となるものの集合の間には、順序を保つ 1 対 1 の対応が存在するので、$S^{-1}A$ は極大条件を満たす。
同様に定理 6.1.30 より $A/\mathfrak{a}$ のイデアルの集合と A のイデアルで $\mathfrak{a}$ を含むものの集合の間には、順序を保つ 1 対 1 の対応が存在するので、$A/\mathfrak{a}$ は極大条件を満たす。 **証明終**

特に命題 6.4.4 より直ちに次が成り立つ。

系 6.4.5 A を Noether 環とする。このとき、A の素イデアル $\mathfrak{p}$ での局所化 $A_{\mathfrak{p}}$ は Noether 環である。また、環 B に対して全射な環準同型 $\phi : A \to B$ が存在するとき、B も Noether 環である。

証明 $A_{\mathfrak{p}}$ については明らか。B については、ϕ が全射であることから B は A のある剰余環 $A/\mathfrak{a}$ と同型になることからしたがう。 **証明終**

命題 6.4.6 A は Noether 環で、環 B の部分環とする。このとき、B が有限生成 A-加群であれば、B も Noether 環である。

証明 A-加群 M に対して、M の任意の部分 A-加群の族が極大条件を満たすとき、M は Noether A-加群であるということにする。

A, B は、条件を満たす環とする。環 B のイデアルは、B の A-部分加群になる。よって、B が Noether A-加群になれば、B は Noether 環になる。

故に、一般に、Notether 環 A 上の有限生成加群 M は、Noether 加群であることを証明すればよい。命題 6.1.52 より、M は A の適当な直和 A^n の剰余加群と同型になるので、A^n が Noether A-加群であることを示せば十分である。次のことが証明できれば、n に関する帰納法で A^n が Noether A-加群であることが証明できる。

A が環、$\pi : M \to N$ は A-加群の全射準同型で、N と $\ker \pi$ は共に Noether A-加群であるとする。このとき、M も、Noether A-加群である。

上のことを証明する。M の部分 A-加群の増大列

$$M_1 \subset M_2 \subset \cdots$$

をとる。このとき、増大列

$$\pi(M_1) \subset \pi(M_2) \subset \cdots$$

と

$$(M_1 \cap \ker \pi) \subset (M_2 \cap \ker \pi) \subset \cdots$$

は無限真増大列にはならないので、

$$\pi(M_n) = \pi(M_{n+1}) = \cdots$$

かつ

$$(M_n \cap \ker \pi) = (M_{n+1} \cap \ker \pi) = \cdots$$

を満たす n が存在する。すると、簡単に

$$M_n = M_{n+1} = \cdots$$

であることがわかる。以上で、M が Noether A-加群であることがわかった。

証明終

定義 6.4.7 $\mathfrak{a}$,$\mathfrak{b}$,$\mathfrak{c}$ をイデアルとする

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Longrightarrow \mathfrak{a} = \mathfrak{b} \text{ または } \mathfrak{a} = \mathfrak{c}$$

が成り立つとき、イデアル $\mathfrak{a}$ は**既約**であるといい、そうでないとき**可約**であるという。

補題 6.4.8 Noether 環 A の任意のイデアルは、有限個の既約イデアルの共通部分として表すことができる。

証明 題意が成り立たないと仮定すると

$\Sigma = \{\mathfrak{a} \mid \mathfrak{a}$ は A のイデアルであって有限個の既約イデアルの共通部分としては表されない $\}$

とおく。$\Sigma \neq \emptyset$ であるから、極大条件より Σ には極大元 $\mathfrak{a}$ が少なくともひとつ存在する。すると $\mathfrak{a}$ は可約であるので $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ となる A のイデアル $\mathfrak{b}, \mathfrak{c} (\neq \mathfrak{a})$ が存在する。 $\mathfrak{a}$ の極大性から $\mathfrak{b}, \mathfrak{c}$ は有限個の既約イデアルの共通部分として表されるが、これは $\mathfrak{a}$ がそうではないことに反する。

証明終

補題 6.4.9 Noether 環 A の任意の既約イデアルは、準素イデアルである。

証明 $\mathfrak{a}$ を A の既約イデアルとし、$xy \in \mathfrak{a}$ かつ $x \notin \mathfrak{a}$ であるとする。任意の $n \in \mathbb{N}$ に対して $y^n \notin \mathfrak{a}$ と仮定する。このとき、昇鎖

$$(\mathfrak{a} : (y)) \subseteq (\mathfrak{a} : (y^2)) \subseteq (\mathfrak{a} : (y^3)) \subseteq \cdots$$

を考えると、昇鎖条件より $(\mathfrak{a} : (y^n)) = (\mathfrak{a} : (y^{n+1}))$ となる $n \in \mathbb{N}$ が存在する。$a \in (\mathfrak{a} + (x)) \cap (\mathfrak{a} + (y^n))$ をとると $a = \alpha + sx = \beta + ty^n$ となる $\alpha, \beta \in \mathfrak{a},\ s, t \in A$ が存在する。すると $ay = y\alpha + sxy \in \mathfrak{a}$ であるから、$ay = y\beta + ty^{n+1}$ より $ty^{n+1} =$

$ay - y\beta \in \mathfrak{a}$ が成り立ち、$t \in (\mathfrak{a} : (y^{n+1})) = (\mathfrak{a} : (y^n))$ となる。ゆえに $ty^n \in \mathfrak{a}$ であるから $a = \beta + ty^n \in \mathfrak{a}$ となり $(\mathfrak{a} + (x)) \cap (\mathfrak{a} + (y^n)) \subseteq \mathfrak{a}$ が成り立つ。

逆に $\mathfrak{a} \subseteq (\mathfrak{a} + (x)) \cap (\mathfrak{a} + (y^n))$ は明らかに成り立つので

$$\mathfrak{a} = (\mathfrak{a} + (x)) \cap (\mathfrak{a} + (y^n))$$

である。ところが $x, y^n \notin \mathfrak{a}$ より $\mathfrak{a} + (x),\ \mathfrak{a} + (y^n)$ は $\mathfrak{a}$ を真に含むので、これは $\mathfrak{a}$ が既約イデアルであることに反する。したがって、ある $n \in \mathbb{N}$ に対して $y^n \in \mathfrak{a}$ とならなければならず、$\mathfrak{a}$ は A の準素イデアルである。 **証明終**

命題 6.4.10 Noether 環の任意のイデアル $\neq (1)$ は準素分解を持つ。

証明 補題 6.4.8 および補題 6.4.9 よりしたがう。 **証明終**

命題 6.4.11 A を Noether 環、$\mathfrak{a}$ を A のイデアルとするとき、$r(\mathfrak{a})^n \subseteq \mathfrak{a}$ となる $n \in \mathbb{N}$ が存在する。

証明 A は Noether 環なので $r(\mathfrak{a})$ は有限生成であるから $r(\mathfrak{a}) = (x_1, x_2, \cdots, x_m)$ とおくことができる。このとき $x_i \in r(\mathfrak{a})$ であるので、各 i に対して $x_i^{k_i} \in \mathfrak{a}$ となる $k_i \in \mathbb{N}$ が存在する。$n \in \mathbb{N}$ を十分大きくとれば (例えば、$n = \Sigma_{i=1}^m (k_i - 1) + 1$ とすればよい)、$\Sigma l_i = n$ となる任意の $l_1, l_2, \cdots, l_m \in \mathbb{N}$ に対して $x_1^{l_1} x_2^{l_2} \cdots x_m^{l_m} \in \mathfrak{a}$ となるから、$r(\mathfrak{a})^n = A\{x_1^{l_1} x_2^{l_2} \cdots x_m^{l_m} | \Sigma l_i = n\} \subseteq \mathfrak{a}$ が成り立つ。 **証明終**

定義 6.4.12 環 A のイデアルの真増大列

$$\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \cdots \subsetneqq \mathfrak{a}_n$$

を長さ n のイデアルの**鎖**という。

A の素イデアルの鎖の長さの上限を A の**次元**といい、$\boldsymbol{\dim A}$ と書く。

補題 6.4.13 1 次元の Noether 局所整閉整域 A において、0 でも A でもない任意のイデアルは極大イデアルのベキである。すなわち、$0 \neq \mathfrak{a} \subsetneqq A$ を A のイデアル、$\mathfrak{m}$ を A の極大イデアルとするとき

$$\mathfrak{a} = \mathfrak{m}^n$$

となる $n \in \mathbb{N}$ が存在する。

証明 A は次元 1 の局所整域なので $\mathfrak{m}$ は A の唯一つの 0 でない素イデアルである。したがって命題 6.1.57 より $\mathfrak{a}$ が $\mathfrak{m}$-準素イデアルであることがわかる。すると、A が Noether 環であることから、命題 6.4.11 より $r(\mathfrak{a})^n = \mathfrak{m}^n \subseteq \mathfrak{a}$ となる $n \in \mathbb{N}$ が存在する。この n を最小にとる。すなわち、$\mathfrak{m}^n \subseteq \mathfrak{a}$ かつ $\mathfrak{m}^{n-1} \not\subseteq \mathfrak{a}$ が成り立っているとする。

まず$\mathfrak{m}$が単項イデアルであることを示す。$0 \neq a \in \mathfrak{m}$をとると、$r((a)) = \mathfrak{m}$であるので、$\mathfrak{m}^n \subseteq (a)$かつ$\mathfrak{m}^{n-1} \not\subseteq (a)$となる$n \in \mathbb{N}$が存在する。このとき$\mathfrak{m}^{n-1} \setminus (a) \neq \emptyset$であるから$b \in \mathfrak{m}^{n-1} \setminus (a)$をとることができるので、$x = a/b \in \mathrm{Frac}A$とおく。このとき$x^{-1} \in A$とすると

$$x^{-1} = b/a \in A \Longrightarrow b = b/1 = (b/a)(a/1) = x^{-1}a \in (a)$$

となるのでbの取り方に反する。したがって$x^{-1} \notin A$であり、Aが整閉であることからx^{-1}はA上整ではない。よって命題 6.3.2 より$x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$が成り立つ。($x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$とすると、$\mathfrak{m}$は$A[x^{-1}]$-加群の構造を持ち、また、Frac$A$が体であることから$\mathfrak{m}$は忠実な$A[x^{-1}]$-加群となる。さらに、$A$がNoether環であるので$\mathfrak{m}$は有限生成$A$-加群である。故に$x^{-1}$は$A$上整となる。)
一方で、$x^{-1} = b/a$より任意の$y \in \mathfrak{m}$に対して$by \in \mathfrak{m}^n \subseteq (a)$であるので、$by = az$となる$z \in A$が存在するから

$$x^{-1}y = by/a = az/a = z \in A$$

すなわち$x^{-1}\mathfrak{m} \subseteq A$が成り立つ。したがって$x^{-1}\mathfrak{m}$は$A$のイデアルであり、$\mathfrak{m}$の極大性から$x^{-1}\mathfrak{m} = A$が成り立つ。ゆえに$\mathfrak{m} = Ax = (x)$となる。($x^{-1}\mathfrak{m} = A$より$x \in \mathfrak{m}$が成り立つことに注意)

いま、$\mathfrak{m}^n \subseteq \mathfrak{a}$であったので、$x^n \in \mathfrak{a}$である。$A$が局所環であることから、系 6.1.44 より、$\mathfrak{m} = (x)$の任意の元はある$c \in A^\times$と$k \in \mathbb{N}$が存在して$cx^k$と書けることに注意する。$\mathfrak{a} \setminus \mathfrak{m}^n \neq \emptyset$と仮定する(すなわち、$\mathfrak{a}$の元で$x^n$で割れないものが存在するとする)と、$\mathfrak{a} \setminus \mathfrak{m}^n$の元は$dx^l$(ただし、$d \in A^\times$, $l < n$)と書けることがわかる。すると$x^l \in \mathfrak{a}$であることから$(x^{n-1}) = \mathfrak{m}^{n-1} \subseteq \mathfrak{a}$となり、$n$の取り方に反する。したがって$\mathfrak{a} \setminus \mathfrak{m}^n = \emptyset$である。すなわち、

$$\mathfrak{a} = (x^n) = \mathfrak{m}^n$$

が成り立つ。 **証明終**

定義 6.4.14 次元 1 の Noether 整閉整域を **Dedekind 環**という。

補題 6.4.15 Dedekind 環において、0 でない準素イデアルは極大イデアルのベキである。すなわち、$0 \neq \mathfrak{q}$を Dedekind 環Aの準素イデアルとするとき

$$\mathfrak{q} = \mathfrak{m}^n$$

となる極大イデアル$\mathfrak{m}$と$n \in \mathbb{N}$が存在する。

証明 Dedekind 環は 1 次元の整域なので、任意の 0 でない素イデアルは極大イデアルであるから、任意の準素イデアル$\mathfrak{q}(\neq 0)$に対して$r(\mathfrak{q})$は極大イデアルとなる

ことに注意する。そこで、$\mathfrak{q}$ を $\mathfrak{m}$-準素イデアルとすると、$\mathfrak{m} \neq 0$ なので命題 6.3.9 より A の $\mathfrak{m}$ による局所化 $A_{\mathfrak{m}}$ は再び Dedekind 環となり、また局所環でもある。すると注意 6.2.20 より $\mathfrak{q}$ は $S^{-1}\mathfrak{q}$ と対応しており、補題 6.4.13 より、$S^{-1}\mathfrak{q}$ は $A_{\mathfrak{m}}$ の極大イデアル $S^{-1}\mathfrak{m}$ を用いて

$$S^{-1}\mathfrak{q} = (S^{-1}\mathfrak{m})^n = S^{-1}\mathfrak{m}^n$$

と書ける。$\mathfrak{m}^n$ を含む素イデアルは $\mathfrak{m}$ のみであるので、$\mathfrak{m}^n$ は $\mathfrak{m}$-準素イデアルであり、$\mathfrak{q} = \mathfrak{m}^n$ が成り立つ。 **証明終**

定理 6.4.16 A を Dedekind 環、$0 \neq \mathfrak{a} \subseteq A$ を任意のイデアルとするとき、$\mathfrak{a}$ は A の極大イデアル $\mathfrak{m}_1$, $\mathfrak{m}_2$,. . . ,$\mathfrak{m}_s$ (重複はありうる) を用いて

$$\mathfrak{a} = \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_s$$

という形に (積の順序を除いて) 一意的に表すことができる。

証明 補題 6.4.15 より $\mathfrak{a}$ が互いに根基が相異なる準素イデアルの積として一意的に表されることを示せば良い。

A が Noether 環であることから命題 6.4.10 より $\mathfrak{a}$ は準素分解を持つ。$\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$ を $\mathfrak{a}$ の最短準素分解とする (ただし $\mathfrak{q}_i$ は $\mathfrak{n}_i$-準素イデアルとする)。A は次元が 1 の整域であるから、A の 0 でない素イデアルは極大イデアルである。したがって $\mathfrak{n}_1$, $\mathfrak{n}_2$,. . . , $\mathfrak{n}_n$ は互いに相異なる極大イデアルであり、命題 6.1.61 より $\mathfrak{q}_1$, $\mathfrak{q}_2$,. . . ,$\mathfrak{q}_n$ は互いに素である。すると命題 6.1.63 より $\cap_{i=1}^n \mathfrak{q}_i = \Pi_{i=1}^n \mathfrak{q}_i$ が成り立つので、$\mathfrak{a} = \Pi_{i=1}^n \mathfrak{q}_i$ を得る。

逆に $\mathfrak{a}$ が根基が互いに相異なる準素イデアル $\mathfrak{q}_i$ の積 $\Pi_{i=1}^n \mathfrak{q}_i$ として表されたとすると、上記と同様に各 $\mathfrak{q}_i$ は互いに素なので $\cap_{i=1}^n \mathfrak{q}_i = \Pi_{i=1}^n \mathfrak{q}_i$ が成り立つ。また、各 $\mathfrak{n}_i = r(\mathfrak{q}_i)$ が互いに相異なる極大イデアルであるので、各 $\mathfrak{n}_i$ は $\mathfrak{a}$ の極小素イデアルであり、したがって各 $\mathfrak{q}_i$ は $\mathfrak{a}$ の孤立準素成分であるから命題 6.2.22 より $\mathfrak{q}_i$ は $\mathfrak{a}$ に対して一意的に定まる。このとき $\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i = \Pi_{i=1}^n \mathfrak{q}_i$ は $\mathfrak{a}$ の最短準素分解となっている。 **証明終**

定理 6.4.17 代数体 K の整数環 O_K は Dedekind 環である。

証明 K を n 次代数体とする。$\mathbb{Q}$ は完全体なので $K/\mathbb{Q}$ は分離拡大である。したがって、命題 6.3.14 より、

$$O_K \subseteq \sum_{i=1}^{n} \mathbb{Z}v_i$$

となる K の $\mathbb{Q}$ 上の基底 $\{v_1, v_2, \cdots, v_n\}$ が存在する。ゆえに、O_K は有限生成 $\mathbb{Z}$-加群の部分加群となる。$\mathbb{Z}$ は PID であるので Noether 環であるから、命題 6.4.6 より

O_K は Noether 環である。さらに命題 6.3.6 より O_K は整閉である。したがって、O_K の次元が 1 であることを示せばよい。

O_K の 0 でない素イデアル $\mathfrak{p}$ を任意にとる。このとき、O_K は整域であるので、(0) は O_K の素イデアルであることに注意すると、$(0) \cap \mathbb{Z} = (0)$ であることから、命題 6.3.8 より、$\mathfrak{p} \cap \mathbb{Z} \neq (0)$ であることがわかる。したがって、$\mathfrak{p} \cap \mathbb{Z}$ は $\mathbb{Z}$ の極大イデアルであり、命題 6.3.7 より $\mathfrak{p}$ は O_K の極大イデアルとなる。 **証明終**

参考文献

[1] 加藤和也, 黒川信重, 斎藤毅, 数論 I(岩波書店,2005)

[2] M.F.Atiyah,I.G.MacDonald, Introduction to Commutative Algebra (Westview Press,1969)

[3] 後藤四郎, 渡辺敬一, 可換環論 (日本評論社,2011)

[4] Paulo Ribenboim 著, 吾郷博顕 訳, フェルマーの最終定理 (共立出版,1983)

[5] 足立恒雄, フェルマーを読む (日本評論社,1986)

[6] 雪江明彦, 代数学 2 環と体とガロア理論 (日本評論社,2010)