

2015年度藏野研究室卒業論文
「初等整数論に関するいくつかの話題」

明治大学理工学部数学科

植草 充史

小沢 章一

川上 杏李

重信 一樹

富樫 智美

吉田 有希

2016年2月22日

目次

1	序	3
1.1	概要	3
1.2	Fermat 及び証明に関わった数学者たち	5
2	Fermat の最終定理	6
2.1	p -進付値	6
2.2	四次の Fermat 方程式	8
3	ABC 定理、abc 予想	9
3.1	ABC 定理	10
3.2	ABC 定理の応用	15
3.3	abc 予想	17
4	平方剰余の相互法則	21
4.1	準備	21
4.2	平方剰余の相互法則	29
4.3	平方剰余の相互法則の別証明	33
5	虚二次体	36
5.1	虚二次体とその部分環	36
5.2	素数の分解	38
5.3	イデアル類群	41
6	付録	48
6.1	準素イデアル分解	48
6.2	整拡大	52
6.3	Dedekind 整域	62

1 序

1.1 概要

定理 1.1 n を 3 以上の整数とする。このとき、

$$x^n + y^n = z^n$$

を満たす正整数の組 (x, y, z) は存在しない。

これが有名な「Fermat¹ の最終定理」である。今から約 400 年前、Fermat がこの予想を残した。Fermat 自身は $n = 4$ の場合のときにこの定理の証明に取り組んだのだが、これまで多くの名だたる数学者が挑戦してきたのにも関わらず、1995 年まで誰も解くことができなかったほどの難問である。完全に証明が公表されたのは、1995 年 5 月、Wiles² によってである。Wiles による証明には高度な数学が駆使されている。第 2 章では Fermat による $n = 4$ のときの証明を示す。

ところで、Fermat の最終定理の多項式における類似である次の定理も興味深いものである。

定理 1.2 n を 3 以上の整数とし F を標数 0 の体とする。このとき、

$$X(t)^n + Y(t)^n = Z(t)^n$$

を満たす F 上の多項式の組 (X, Y, Z) は、自明な解しか存在しない。

ただし、 F 上の多項式の組 (X, Y, Z) が上の方程式の自明な解であるとは、 $a^n + b^n = c^n$ を満たす定数 a, b, c と多項式 W により、 $(X, Y, Z) = (aW, bW, cW)$ と表せるときをいう。

この定理は 19 世紀後半頃には知られていたようだが、20 世紀末に簡明な証明が発見された。つまり、「ABC 定理 (Mason-Stothers の定理)」という 1980 年代に発見された定理により証明することができる。一方で

¹Pierre de Fermat (1601-1665) フランスの数学者。本業は法律家、政治家。同世代のフランス人の数学者で、Descartes や、Pascal などがある。Fermat の生前には一冊の本も論文も発表せず、Fermat の研究は、友人たちに送る書簡と蔵書に書かれていた。中でも Fermat が愛読していた Diophantus の『算術』の余白に「Fermat の最終定理」が書き込まれていた。Fermat の長男が収録した『Pierre de Fermat による所見を含む Diophantus の算術』の出版により現在、「Fermat の最終定理」が私たちの目にも触れるようになった。

²Andrew John Wiles (1953-) イギリスの数学者。Oxford 大学の教授。

「ABC 定理」の整数における類似であるものが予想されている。「abc 予想 (Oesterlé-Masser 予想)」は、1985 年に提起された数論の予想であるが、2012 年に望月 新一氏がその予想を解決したとする論文が公開され、現在検証段階にある。「abc 予想」を真だと仮定すると、多数くの系が得られる。その中には既に知られている結果もあれば（予想の提出後に予想とは独立に証明されたものもある）、部分的証明ができるものもある。そのうちの例の一つとして「Fermat の最終定理」さえも、ほとんどの場合の別証明を与えてしまう。「abc 予想」が成立した場合に解決される予想はいろいろあり、また数論の深い問題と結び付きがあるので、「abc 予想」は重要な問題である。第 3 章では、「ABC 定理」の証明を与え、さらにその応用として定理 1.2 よりも強い定理や、数論における Catalan 予想の類似のものを証明する。後半では「abc 予想」がどのようなものであるかを紹介し、「abc 予想」を仮定したときの、「Fermat の最終定理」の一部や Beal 予想を示してゆく。

Fermat が研究したのは、最終定理における方程式だけではない。

問題 1.3 素数 p についての方程式

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

は整数解 (x, y) を有するのであろうか？

問題 1.4 素数 p についての方程式

$$p = x^2 + 5y^2$$

は整数解 (x, y) を有するのであろうか？

Fermat 自身は問題 1.3 については完全に解決したが、問題 1.4 については証明までは至らなかった。この 2 つの違いを理解するためには、

$$x + y\sqrt{-d} \quad (x, y \in \mathbb{Z}, d \in \mathbb{Z}_{>0})$$

という数を研究することが不可欠である。Fermat は $d = 1$ のときと、 $d = 5$ のときの違いを見出すことができなかったのである。その違いを測る道具が、「イデアル類群」という整数論の中心的研究対象である。第 5 章では、 $x + y\sqrt{-d}$ という数の世界を定義し、イデアル類群がどのようなものかを紹介する。

さて、第5章で定められる数の世界における“素数”の対応物を研究する上では、「平方剰余の相互法則」という定理が非常に重要な役割を果たす。Gauss³ が生涯に渡り、この定理に全く異なる7つの証明を与えた。第4章では、V. A. Lebesgue による相互法則の証明と、その別証明を与える。

この卒業論文は、セミナーで輪読した [3], [4] の内容の一部をまとめたものである。

1.2 Fermat 及び証明に関わった数学者たち

「Fermat の最終定理」の歴史を紐解いていく。一見、それほど複雑な問題のようには見えない、この問題を証明するのに400年近くかかっているのは「存在しない」ことを証明しなければならなかったからである。「Fermat の最終定理」は、 $n = 4$ 又は奇素数の場合に証明すればよい。証明されるまで、何人もの数学者の挑戦があつて、はじめて証明が成し遂げられた。最終的に解いたのは、Wiles だが、決して Wiles だけの力で解かれたわけではない。最初は、 $n = 3$ の場合、 $n = 4$ の場合、 $n = 5$ の場合といったように、一つずつ解かれてきた。では、どのようにしてこの難問が解かれてきたのかを、順を追ってみていくことにしよう。

まず最初に $n = 4$ の場合を証明したのは、Fermat 自身である。無限降下法により証明された。これは Fermat 自身があみ出し、得意としていた方法である。ただし、これは不完全な証明であつたため、後に Euler⁴ によって完全に証明された。その Euler は、1770 年に $n = 3$ の場合を完全に証明した。Fermat が定理を書き残したのは1630年頃と言われているので、この時点で120年以上もの月日経っていることになる。

$n = 5$ の場合が証明されたのは1820年、Dirichlet⁵ によってである。Euler が $n = 3$ を証明してから、更に60年以上経っていた。Dirichlet は $n = 14$ の場合も証明している。

³Carolus Fridericus Gauss (1777-1855) ドイツの数学者、天文学者、物理学者。19世紀最大の数学者の一人。1795年頃、Gauss が18歳頃に独力で相互法則第1補充則を発見した。『Disquisitiones Arithmeticae』の序文にもあるように、Fermat、Euler、Lagrange らの先達の業績も知らず、独自で研究に没頭した。相互法則の証明の完成は、1796年頃と文献には残っている。7つの証明の中の6つは生前に公表され、最後の1つは死後に発表された。

⁴Leonhard Euler (1707-1783) スイス生まれの数学者、天文学者。数学史上最も大きな業績を残した数学者の一人であり、「Fermat の最終定理」に大きな関心を寄せていた。

⁵Peter Gustav Lejeune Dircchret (1805-1859) ドイツの数学者。Fermat や Euler に並ぶ、数論や解析学などの方面で重要な実績を残した数学者である。

Dirichlet はさらに $n = 7$ の場合にも挑戦したが、1839 年に Lamé⁶ がこれを証明した。このころ、数学者たちの間で「Fermat の最終定理」を巡る激しい競争が起こっていた。Lamé、Cauchy⁷、Kummer⁸ などが他の学者よりいち早く証明しようと必死になっていたのである。結局この競争は、Kummer の勝利で幕を閉じた。Kummer は、 n が正則素数の場合に証明したのである。これは既に 20 世紀に入った 1908 年のことであった。100 以下の素数で正則でないものは、37, 59, 67 の 3 つしかないことが知られている。また、素数全体の中で、約半分が正則素数であるという未解決な予想もある。

このあと、コンピュータの導入により、1992 年までに n が 400 万まで証明された。

1980 年代に入り、「Fermat の最終定理」の証明は最終局面を迎える。1984 年、「楕円曲線 (Frey 曲線)」という曲線の理論を使って「Fermat の最終定理」が解ける可能性のあることが発見され、また、「谷山・志村予想」で貢献した日本人の数学者も大きな役割を担い、ついに 1995 年に Wiles によって完全証明が果たされた。

2 Fermat の最終定理

この章では、素因数分解の一意性は既知のものとして議論を進める。つまり、2 以上の任意の自然数 a は、

$$a = p_1 p_2 \cdots p_n \quad (\text{各 } p_i \text{ は素数}) \quad (1)$$

と (積の順番を除いて) 一意的に分解される。

2.1 p -進付値

素因数分解の一意性で主張されていることは、次のように言い換えることができる。 a を整数、 p を素数とする。 $a > 0$ のとき、(1) を満たす素

⁶Gabriel Lamé (1795-1780) フランスの数学者。数理物理学、代数学、幾何学などで功績を残した。

⁷Augustin Louis Cauchy (1789-1857) フランスの数学者。解析学の分野において、数多くの貢献からフランスの Gauss と呼ばれることもある。

⁸Ernst Eduard Kummer (1810-1893) ドイツの数学者。Dirichlet の弟子である。Kummer らは虚数を含む数の素因数分解の一意性が必ずしもないことを指摘したが、そこに一意性を持たせる為に理想数を取り入れた。これは後のイデアルの概念へとつながっている。

数の列 $p_1, p_2, \dots, p_n$ は順序を入れ替えることによって一意である。よって、集合 $\{i | 1 \leq i \leq r, p_i = p\}$ の元の個数は一定である。この個数を a の p -進付値といい、 $\nu_p(a)$ と書く。 $a < 0$ の場合は $\nu_p(a) = \nu_p(-a)$ と定めると、0 でない任意の整数 a に対して $\nu_p(a) \in \mathbb{Z}_{\geq 0}$ が定まり、

$$a = \epsilon(a) \prod_{p:\text{素数}} p^{\nu_p(a)} \quad (2)$$

が成り立つことになる。ここで $\epsilon(a)$ は a の符号を表す。すなわち、

$$\epsilon(a) = \begin{cases} 1 & a > 0 \text{ のとき} \\ -1 & a < 0 \text{ のとき} \end{cases}$$

である。改めて、分解式 (2) を a の素因数分解といい、 $\nu_p(a) > 0$ となる素数 p を a の素因数という。なお、素数は無限に多く存在するが、 $p > |a|$ ならば $\nu_p(a) = 0$ なので分解式の右辺の積は実際には有限積である。また、 $\nu_p(a) = n$ とおくと、 a は p^n の倍数であって p^{n+1} の倍数ではないから

$$a \in (p^{\nu_p(a)}), \quad a \notin (p^{\nu_p(a)+1})$$

が成り立つ。すなわち $\nu_p(a)$ は $a \in (p^n)$ となる最大の整数 n に一致する。

補題 2.1 (1) x, y, z を 0 でない整数とする。 x, y が互いに素で $xy = z^3$ が成り立てば、 $x = a^3, y = b^3$ を満たす整数 $a, b \neq 0$ が存在する。

(2) x, y, z を正整数とする。 x, y が互いに素で $xy = z^2$ が成り立てば、 $x = a^2, y = b^2$ を満たす正整数 a, b が存在する。

(3) x, y, z, w を正整数とする。 x, y, z はどの二つも互いに素で $xyz = w^2$ が成り立てば、 $x = a^2, y = b^2, z = c^2$ を満たす正整数 a, b, c が存在する。

証明 どれも素因数分解の一意性からの単純な帰結である。ここでは (1) のみを証明する。 p を素数とする。 x, y は互いに素なので $\nu_p(x) = 0$ か $\nu_p(y) = 0$ が成り立つ。 $xy = z^3$ から $\nu_p(x) + \nu_p(y) = 3\nu_p(z)$ となる。よってすべての素数 p に対して $\nu_p(x), \nu_p(y)$ は 3 の倍数である。そこで $a = \epsilon(x) \prod_{p:\text{素数}} p^{\frac{\nu_p(x)}{3}}, b = \epsilon(y) \prod_{p:\text{素数}} p^{\frac{\nu_p(y)}{3}}$ とおけば結論が成り立つ。

証明終

2.2 四次の Fermat 方程式

ここでは無限降下法で、四次の Fermat 方程式が非自明な解を持たないことを証明することを目指す。

定理 2.2 正整数 x, y, z に対して、次の二条件は同値である。

- (1) x, y は互いに素、 x は奇数、 y は偶数、かつ次式が成り立つ。

$$x^2 + y^2 = z^2$$

- (2) 互いに素な整数 $a > b > 0$ で、 a, b のどちらかは偶数であり、かつ次式を満たすものが存在する。

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2$$

証明 (1) を仮定する。 x, z は奇数だから、 $z \pm x$ は偶数である。 $\frac{z+x}{2}, \frac{z-x}{2}$ が共通な素因数 p をもつとすると、 $x = \frac{z+x}{2} - \frac{z-x}{2}$ と $z = \frac{z+x}{2} + \frac{z-x}{2}$ は共通の素因数 p をもち、 x, y が互いに素という仮定に反する。よって $\frac{z+x}{2}, \frac{z-x}{2}$ は互いに素な整数である。 $x^2 + y^2 = z^2$ を書き換えると $(\frac{y}{z})^2 = \frac{z+x}{z} \cdot \frac{z-x}{z}$ となる。補題 2.1(1) より、 $z+x = 2a^2, z-x = 2b^2$ となる正整数 $a > b$ が存在する。すると $x = a^2 - b^2, y = 2ab, z = a^2 + b^2$ となる。 $a^2 = \frac{z+x}{2}$ と $b^2 = \frac{z-x}{2}$ が互いに素なので a, b も互いに素である。 $x = a^2 - b^2$ は奇数だから a, b のうち一方が奇数で他方は偶数である。よって (2) が示された。

次に (2) を仮定する。 $x^2 + y^2$ に $x = a^2 - b^2, y = 2ab$ を代入すると $x^2 + y^2 = (a^2 + b^2)^2 = z^2$ となる。 a, b の片方のみが偶数であるから x は奇数、 y は偶数である。 x, y が互いに素でないとすると、共通な素因数 p をもつ。 $y = 2ab$ より p は $2, a, b$ のいずれかを割りきる。 $p = 2$ とすると、 x が偶数となり矛盾する。 p が a を割り切るとすると $a^2 - x = b^2$ より p は b を割り切る。よって a, b は互いに素に矛盾する。 p が b を割り切るとしても同様に矛盾する。以上より x, y は互いに素である。よって (1) が示された。

よって (1) と (2) は同値である。

証明終

Fermat の最終定理の $n = 4$ のケースは、次の定理から直ちに従う。

定理 2.3 (四次の Fermat 方程式) $x^4 + y^4 = z^2$ を満たす正整数 x, y, z は存在しない。

証明 $x^4 + y^4 = z^2$ を満たす正整数 x, y, z があると仮定する。また、 z はこれを満たす最小のものとする。 x, y が互いに素でない、つまり x, y を割り切る共通な素因数 p が存在すると仮定すると $x^4 + y^4 = z^2$ より、 $(\frac{x}{p})^4 + (\frac{y}{p})^4 = (\frac{z}{p^2})^2$ とすることができる。ここで、 $\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2}$ は自然数であることに注意する。しかしこれは z の最小性に矛盾する。これより x, y は互いに素である。もし x, z に共通の素因数 p があれば、 $x^4 + y^4 = z^2$ より y も p の倍数となり、 x, y は互いに素であることに矛盾する。よって x と z, y と z も互いに素であることがわかる。ここで x, y の両方を奇数とすると、 $x^4 + y^4$ を 4 で割った余りは 2 になるが、このとき z は偶数だから z^2 は 4 の倍数となり矛盾が生じる。よって x を奇数、 y を偶数とする。

定理 2.2 より、互いに素な整数 $a > b > 0$ で、 a, b のどちらかは偶数であり、かつ次式を満たすものが存在する。

$$x^2 = a^2 - b^2, \quad y^2 = 2ab, \quad z = a^2 + b^2$$

$x^2 = a^2 - b^2$ を $x^2 + b^2 = a^2$ と書き換えると、4 で割って余りを考えれば、 x は奇数なので a は奇数、 b は偶数である。また、 a, b が互いに素より、 x, b は互いに素である。 $x^2 + b^2 = a^2$ に再び定理 2.2 を用いると、

$$x = k^2 - l^2, \quad b = 2kl, \quad a = k^2 + l^2$$

を満たす互いに素で、かつ、どちらかは偶数である k, l ($k > l > 0$) が得られる。 $y^2 = 2ab, b = 2kl, a = k^2 + l^2$ より $(\frac{y}{2})^2 = \frac{1}{2}ab = kl(k^2 + l^2)$ となる。 $k, l, k^2 + l^2$ はどの二つも互いに素なので、補題 2.1(3) より $k = s^2, l = t^2, k^2 + l^2 = u^2$ となる整数 s, t, u (> 0) が存在する。このとき、

$$s^4 + t^4 = u^2$$

である。一方 $u^4 = (k^2 + l^2)^2 = a^2 < a^2 + b^2 = z \leq z^4$ であるから、これは z の最小性に矛盾する。証明終

3 ABC 定理、abc 予想

この節では F は、標数 0 の体とする。

3.1 ABC 定理

定義 3.1 $n \in \mathbb{Z}_{\geq 0}$, $a_0, \dots, a_n \in F$ に対し

$$A(t) = a_n t^n + a_{n-1} t^{n-1} + \dots + a_0$$

の形に表されるものを F 上の多項式といい、 F 上の多項式全体の集合を

$$F[t] = \{a_n t^n + a_{n-1} t^{n-1} + \dots + a_0 \mid n \in \mathbb{Z}_{\geq 0}, a_0, \dots, a_n \in F\}$$

と書く。

上の $A(t) \in F[t]$ に対して、 $a_n \neq 0$ であるとき、 n を $A(t)$ の次数といい、 $n = \deg A(t)$ と表す。また、 a_n を $A(t)$ の最高次数係数といい $a_n = \epsilon(A(t))$ と表す。

定義 3.2 $I \subset F[t]$ で次の条件を満たすものを $F[t]$ のイデアルという。

- (1) $0 \in I$
- (2) $A, B \in I$ のとき、 $A + B \in I$
- (3) $A \in I$, $X \in F[t]$ のとき、 $AX \in I$

また、 $(A) = \{AX \mid X \in F[t]\}$ と書く。

上の (A) は、 $F[t]$ のイデアルである。実は $F[t]$ は単項イデアル整域であるので、 $F[t]$ のイデアルは必ず (A) の形をしている。

命題 3.3 定数でない多項式 $P \in F[t]$ に対し、次の条件は同値である。

- (1) $A, B \in F[t]$, $(AB) \in (P)$ ならば $A \in (P)$ または $B \in (P)$ である。
すなわち、 P が AB の約数ならば、 P は A または B の約数である。
- (2) $C \in F[t]$, $P \in (C)$ ならば、 $(C) = (P)$ または $(C) = (1)$ である。
すなわち、 P の約数は単数と P の単数倍だけである。

証明 まず (1) を仮定する。 $P \in (C)$ となる $C \in F[t]$ をとる。すると、 $P = CD$ となる $D \in F[t]$ が存在する。 $CD \in (P)$ なので、(1) より、 $C \in (P)$ または $D \in (P)$ である。 $C \in (P)$ のとき、 $P \in (C)$ より、 $(C) = (P)$ である。 $D \in (P)$ のとき、 $D = EP$ となるような $E \in F[t]$ が

存在し、 $P = CD = CEP$ となり、 $CE = 1$ となる。したがって $(C) = (1)$ となり、(2) が成り立った。

次に (2) を仮定する。 $A, B \in F[t]$ が $AB \in (P)$ かつ $A \notin (P)$ を満たすと仮定する。ここで、 $F[t]$ は単項イデアル整域⁹ だから、 $(P, A) = (C)$ となる $C \in F[t]$ が存在する。一方で $P \in (P, A) = (C)$ より、(2) を利用して $(C) = (P)$ または $(C) = (1)$ となる。 $(C) = (P)$ のとき、 $A \in (P, A) = (C) = (P)$ となり、仮定である $A \notin (P)$ に反する。したがって、 $(P, A) = (1)$ であり、 $PX + AY = 1$ となる $X, Y \in F[t]$ が存在する。仮定より、 $AB \in (P)$ なので $B = BPX + BAY \in (P)$ である。したがって、 $A, B \in F[t]$ が $AB \in (P)$ と $A \notin (P)$ を満たすとき、 $B \in (P)$ となったので (1) が成り立った。

よってこの二つの条件は同値である。

証明終

定義 3.4 $P \in F[t]$ を定数でない多項式とする。命題 3.3 の同値な条件が成り立つとき、 P を既約多項式という。また、モニックな既約多項式を素式と呼ぶ。

定義 3.5 0 でない多項式 $A \in F[t]$ に対し、 A の素因数すべての積を $\text{rad } A$ と書く。すなわち、相異なる素式 $P_1, P_2, \dots, P_r$ と $e_1, e_2, \dots, e_r \in \mathbb{Z}_{>0}$ について、 $A = \epsilon(A)P_1^{e_1} \cdots P_r^{e_r}$ のとき $\text{rad } A = P_1 \cdots P_r$ である。

ABC 定理の証明に入る前に、微分の基本性質を振り返る。

補題 3.6 $A = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0 \in F[t]$ の微分 $A' \in F[t]$ を、 $A' = n a_n t^{n-1} + (n-1) a_{n-1} t^{n-2} + \cdots + 2 a_2 t + a_1$ と定義する。 $A, B \in F[t]$, $a, b \in F$, $e \in \mathbb{Z}_{>0}$ について次が成立する。

(1) $A' = 0$ であることと、 A が定数であることは同値である。

(2) $(aA + bB)' = aA' + bB'$

(3) A が定数でないとき、 $\deg A' = \deg A - 1$ である。

(4) $(AB)' = A'B + AB'$

⁹命題 3.3 の (1) は、 P が素元であると言っている。(2) は、 P が既約元であると言っている。素元であれば既約元であること、つまり (1) $\Rightarrow$ (2) は一般に成立する。(2) $\Rightarrow$ (1) は、考えている環が素元分解環であれば成立する。単項イデアル整域は素元分解環である。

(5) $B \in (A^e)$ のとき、 $B' \in (A^{e-1})$ である。

(6) $A \neq 0, B \neq 0$ とする。 $AB' = A'B$ であることと、 $A = cB$ となるような単数 c が存在することは同値である。

証明 (1), (2), (3) は、明らかである。

(4) について。

$$\begin{aligned} A(t) &= a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 \\ B(t) &= b_m t^m + b_{m-1} t^{m-1} + \cdots + b_0 \end{aligned}$$

とすると

$$\begin{aligned} AB &= a_n b_m t^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) t^{n+m-1} + \cdots \\ &\quad + (a_2 b_0 + a_1 b_1 + a_0 b_2) t^2 + (a_1 b_0 + a_0 b_1) t + a_0 b_0 \end{aligned}$$

となり、これを微分すると

$$\begin{aligned} (AB)' &= (m+n) a_n b_m t^{n+m-1} + (n+m-1) (a_n b_{m-1} + a_{n-1} b_m) t^{n+m-2} + \cdots \\ &\quad + 2(a_2 b_0 + a_1 b_1 + a_0 b_2) t + (a_1 b_0 + a_0 b_1) \end{aligned}$$

である。一方で

$$\begin{aligned} A'B &= n a_n b_m t^{n+m-1} + ((n-1) a_{n-1} b_m + n a_n b_{m-1}) t^{n+m-2} + \cdots \\ &\quad + (a_1 b_1 + 2a_2 b_0) t + a_1 b_0 \end{aligned}$$

$$\begin{aligned} AB' &= m a_n b_m t^{n+m-1} + ((m-1) a_n b_{m-1} + m a_{n-1} b_m) t^{n+m-2} + \cdots \\ &\quad + (a_1 b_1 + 2a_2 b_0) t + a_0 b_1 \end{aligned}$$

となり、

$$\begin{aligned} A'B + AB' &= (m+n) a_n b_m t^{n+m-1} + (n+m-1) (a_n b_{m-1} + a_{n-1} b_m) t^{n+m-2} + \cdots \\ &\quad + 2(a_2 b_0 + a_1 b_1 + a_0 b_2) t + (a_1 b_0 + a_0 b_1) \\ &= (AB)' \end{aligned}$$

となる。よって、 $(AB)' = A'B + AB'$ が成立する。

(5) について。 $B \in (A^e)$ より、 $B = A^e C$ となるような $C \in F[t]$ が存在する。 $(A^e)' = eA^{e-1}A'$ を利用して、

$$B' = eA^{e-1}A'C + A^e C' = A^{e-1}(eA'C + AC')$$

となる。したがって、 $B' \in (A^{e-1})$ である。

(6) について。 $A = cB$ なら、 $AB' = A'B$ は明らかである。逆を示そう。

$$A = \epsilon(A)P_1^{e_1} \cdots P_r^{e_r}$$

$$B = \epsilon(B)P_1^{f_1} \cdots P_r^{f_r}$$

とおく。但し、 $P_1 \cdots P_r$ は互いに異なる素式、 $e_1, \dots, e_r, f_1, \dots, f_r \in \mathbb{Z}_{\geq 0}$ である。このとき

$$AB' = \epsilon(A)\epsilon(B)P_1^{e_1+f_1} \cdots P_r^{e_r+f_r} \left(\sum_{i=1}^r \frac{f_i P'_i}{P_i} \right)$$

$$A'B = \epsilon(A)\epsilon(B)P_1^{e_1+f_1} \cdots P_r^{e_r+f_r} \left(\sum_{i=1}^r \frac{e_i P'_i}{P_i} \right)$$

である。仮定より、 $\epsilon(A) \neq 0, \epsilon(B) \neq 0$ であるので、

$$\sum_{i=1}^r \frac{(f_i - e_i) P'_i}{P_i} = 0$$

である。両辺に、 $P_1 P_2 \cdots P_r$ をかければ、 $i = 1, \dots, r$ に対して、

$$(f_i - e_i) P'_i \frac{P_1 \cdots P_r}{P_i} \in (P_i)$$

となる。 $P_1, \dots, P_r$ は互いに異なる素式なので、

$$(f_i - e_i) P'_i \in (P_i)$$

となる。このとき次数を考えれば $f_i - e_i = 0$ となる。よって $A = \frac{\epsilon(A)}{\epsilon(B)} B$ となる。
証明終

以上のことを利用して、ABC 定理を示す。

定理 3.7 (ABC 定理) $A, B, C \in F[t]$ を、どれも定数ではなく、どの二つも互いに素な多項式で、さらに $A + B = C$ を満たすものとする。このとき

$$\max(\deg A, \deg B, \deg C) < \deg \text{rad}(ABC)$$

が成立する。

証明 $D = AB' - BA'$ とする。 $A + B = C$ より、 $A' + B' = C'$ がいえる。
よって、

$$D = AB' - BA' = A(C' - A') - (C - A)A' = AC' - CA'$$

である。同様に、

$$D = AB' - BA' = (C - B)B' - B(C' - B') = CB' - BC'$$

となり、補題 3.6(6) より、

$$0 \neq D = AC' - CA' = CB' - BC'$$

となる。また、補題 3.6(3) より、

$$\deg D \leq \deg A + \deg B - 1$$

である。すなわち、

$$\deg C + \deg D < \deg(ABC)$$

である。この不等式と対称性より、 $\deg A + \deg D < \deg(ABC)$ 、 $\deg B + \deg D < \deg(ABC)$ がいえるので

$$\max(\deg A, \deg B, \deg C) + \deg D < \deg(ABC)$$

となる。ここで、

$$A_1 = \frac{A}{\text{rad } A}, B_1 = \frac{B}{\text{rad } B}, C_1 = \frac{C}{\text{rad } C} \in F[t]$$

とおく。相異なる素式 $P_1, P_2, \dots, P_r$ と $e_1, e_2, \dots, e_r \in \mathbb{Z}_{>0}$ を用いて A の素式分解を

$$A = \epsilon(A)P_1^{e_1} \cdots P_r^{e_r}$$

と表すと

$$A_1 = \epsilon(A)P_1^{e_1-1} \cdots P_r^{e_r-1}$$

である。 e_i の定義から、 $A \in (P_i^{e_i}) \subset (P_i^{e_i-1})$ であり、補題 3.6(5) から、 $A' \in (P_i^{e_i-1})$ である。 $D = AB' - BA'$ なので、各 $i = 1, \dots, r$ に対して、 $D \in (P_i^{e_i-1})$ がいえる。したがって、 $D \in (A_1)$ である。同様にして、 $D \in (B_1)$ 、 $D \in (C_1)$ もいえる。さらに、 A_1, B_1, C_1 はどの二つも素であ

ること、 $D \in (A_1)$, $D \in (B_1)$, $D \in (C_1)$ より、 $D \in (A_1 B_1 C_1)$ がいえる。
したがって、 $D \operatorname{rad}(ABC) \in (ABC)$ となり、

$$\deg D + \deg \operatorname{rad}(ABC) \geq \deg(ABC)$$

である。ゆえに、

$$\max(\deg A, \deg B, \deg C) + \deg D < \deg(ABC)$$

と

$$\deg D + \deg \operatorname{rad}(ABC) \geq \deg(ABC)$$

より

$$\max(\deg A, \deg B, \deg C) + \deg D < \deg(ABC) \leq \deg D + \deg \operatorname{rad}(ABC)$$

となるので、

$$\max(\deg A, \deg B, \deg C) < \deg \operatorname{rad}(ABC)$$

となる。

証明終

3.2 ABC 定理の応用

定理 3.8 $p, q, r \in \mathbb{Z}_{>0}$ が $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$ を満たすとき

$$X^p + Y^q = Z^r$$

を満たす多項式 X, Y, Z で、どれもが定数でなく、どの二つも互いに素なものは存在しない。

証明 定理にあるような X, Y, Z が存在すると仮定する。ABC 定理より、 $A = X^p$, $B = Y^q$, $C = Z^r$ として適用すると

$$\begin{aligned} \max(\deg(X^p), \deg(Y^q), \deg(Z^r)) &< \deg \operatorname{rad}(X^p Y^q Z^r) \\ &= \deg \operatorname{rad}(XYZ) \\ &\leq \deg(XYZ) \end{aligned}$$

と表せる。すなわち $p \deg X < \deg(XYZ)$, $q \deg Y < \deg(XYZ)$, $r \deg Z < \deg(XYZ)$ となる。それぞれを $\frac{1}{p}$, $\frac{1}{q}$, $\frac{1}{r}$ 倍して、さらにその和をとると

$$\deg X + \deg Y + \deg Z < \left(\frac{1}{p} + \frac{1}{q} + \frac{1}{r}\right) \deg(XYZ)$$

となるが、 $\deg X + \deg Y + \deg Z = \deg(XYZ) > 0$ なので、 $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$ に矛盾する。 証明終

定理 3.9 整数 $m, n \geq 2$ に対し、 $X^m - Y^n = 1$ を満たす定数でない多項式 X, Y は存在しない。

証明 定理にあるような X, Y が存在すると仮定する。このとき、 $X^m - Y^n = 1$ より、 $X^m, Y^n, 1$ はどの二つも互いに素である。 $A = X^m, B = Y^n, C = 1$ として、ABC 定理を適用すると

$$\begin{aligned} \max(\deg X^m, \deg Y^n, 0) &< \deg \text{rad}(X^m Y^n) \\ &= \deg \text{rad}(XY) \\ &\leq \deg(XY) \end{aligned}$$

となる。すなわち $m \deg X < \deg(XY)$, $n \deg Y < \deg(XY)$ が成立する。それぞれを n 倍、 m 倍して、さらにその和をとると

$$mn(\deg X + \deg Y) < (m + n) \deg(XY)$$

となるが、仮定より $\deg X + \deg Y = \deg(XY) > 0$ なので $mn < m + n$ となる。すなわち、 $(m - 1)(n - 1) < 1$ が得られる。これは、 $m, n \geq 2$ に矛盾する。 証明終

この定理の整数における類似として、次の定理が知られている。

定理 3.10 (Catalan 予想) $m, n, x, y \in \mathbb{Z}_{>0}$ に対し、 $x^m - y^n = 1$ で $m, n \geq 2$ を満たすものは

$$(m, n, x, y) = (2, 3, 3, 2)$$

すなわち、 $3^2 - 2^3 = 1$ のみである。

この定理は、Catalan により 1884 年に予想され、2002 年に Mihailescu により証明された。

3.3 abc 予想

0 でない整数 a に対し、 a の互いに異なる素因数全ての積を $\text{rad}(a)$ と書く。すなわち、

$$\text{rad}(a) = \prod_{p:a \text{ の素因数}} p$$

である。

言い換えると、相異なる素数 $p_1, p_2, \dots, p_r$ と $e_1, e_2, \dots, e_r \in \mathbb{Z}_{>0}$ について $a = \pm p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ のとき、 $\text{rad}(a) = p_1 p_2 \cdots p_r$ である。例えば、

$$\text{rad}(19800) = \text{rad}(2^3 \cdot 3^2 \cdot 5^2 \cdot 11) = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

である。ABC 定理の整数における単純な類似は、次のようになるであろう。

問題 3.11 (abc-1) 0 でない整数 a, b, c のどの 2 つも互いに素で $a + b = c$ を満たすとき、次の 2 つの不等式は成り立つだろうか？

$$\max(|a|, |b|, |c|) < \text{rad}(abc)$$

必要なら文字を入れ替えることで、 a, b, c は全て正としてもよい。すると $a + b = c$ から $\max(|a|, |b|, |c|) = c$ となる。

すると、次のように簡明に言い換えられる。

$$\mathbf{abc} = \left\{ (a, b, c) \in \mathbb{N}^3 \mid \begin{array}{l} (a, b) = (b, c) = (c, a) = (1), \\ 0 < a < b < c, \ a + b = c \end{array} \right\}$$

とすると、任意の $(a, b, c) \in \mathbf{abc}$ に対して $c < \text{rad}(abc)$ が成り立つのだろうか？

しかし反例が存在する。

例 3.12 (1) $(a, b, c) = (1, 8, 9)$ のとき、 $9 > \text{rad}(1 \cdot 8 \cdot 9) = 2 \cdot 3 = 6$ である。

(2) $(a, b, c) = (5, 27, 32)$ のとき、 $32 > \text{rad}(5 \cdot 27 \cdot 32) = 5 \cdot 3 \cdot 2 = 30$ である。

(3) r を正整数として、 $(a, b, c) = (1, 3^{2^r} - 1, 3^{2^r})$ とおく。このとき、

$$\begin{aligned} b &= 3^{2^r} - 1 = (3^{2^{r-1}})^2 - 1 = (3^{2^{r-1}} - 1)(3^{2^{r-1}} + 1) \\ &= \cdots = (3^{2^{r-1}} + 1)(3^{2^{r-2}} + 1) \cdots (3 + 1)(3 - 1) \end{aligned}$$

において、最後の積の各因子はすべて偶数であることと $3 + 1 = 4$ に注目すれば $3^{2^r} - 1$ は 2^{r+2} の倍数であることが分かる。したがって、

$$\text{rad}(abc) = \text{rad}((3^{2^r} - 1)3^{2^r}) \leq \frac{3^{2^r} - 1}{2^{r+1}} \cdot 3 < \frac{3}{2^{r+1}} \cdot c < c$$

となる。つまり、**abc-1** には、無限個の反例がある。

ところが問題 3.11 を弱めた次の予想には反例が知られていない。つまり未解決問題である。

予想 3.13 (abc-N) 次が成り立つような正整数 $N > 1$ が存在する。

$$\forall (a, b, c) \in \mathbf{abc} \text{ に対して } c < (\text{rad}(abc))^N$$

この予想が正しければ、「Fermat の最終定理」を (ほぼ) 直ちに証明することができる。つまり、

定理 3.14 $N > 1$ を整数とし、もし予想 3.13 が成り立てば、 $n \geq 3N$ に対する「Fermat の最終定理」が成り立つ。

証明 n を正整数とし、 $x^n + y^n = z^n$ と $x < y < z$ を満たし、どの 2 つも互いに素な正整数 x, y, z が存在すると仮定する。

$(a, b, c) = (x^n, y^n, z^n)$ は **abc** に属するので、予想 3.13 を使って、

$$z^n < (\text{rad}(x^n y^n z^n))^N = (\text{rad}(xyz))^N \leq (xyz)^N < z^{3N}$$

を得る。ここから $n < 3N$ が従う。

証明終

次に予想 3.13 をさらに詳しく見てみる。そのために、実数 $\kappa \geq 1$ に対し、

$$\mathbf{abc}[\kappa] = \{(a, b, c) \in \mathbf{abc} \mid c \geq (\text{rad}(abc))^\kappa\}$$

という集合を導入する。定義より、 $\kappa \leq \kappa'$ ならば $\mathbf{abc}[\kappa] \supset \mathbf{abc}[\kappa']$ が成り立つ。

例 3.12(3) によって $\mathbf{abc}[1]$ は無限集合である。予想 3.13 は $\mathbf{abc}[N]$ が空集合となる $N > 1$ が存在するだろうと考えている。つまり、 $\mathbf{abc}[\kappa]$ と

いう集合は $\kappa = 1$ のとき無限集合であるが、 κ が大きくなるごとに小さくなってゆき、いつかは空集合になると期待されているのである。実際には $\kappa = 2$ の場合 $\mathbf{abc}[2]$ に属する元は 1 つも知られていない。 $\kappa = 1.6$ については、次の例のように $\mathbf{abc}[1.6]$ の元が 2014 年の時点で 3 つだけ発見されている。

例 3.15

$$\begin{array}{ll} (2, 3^{10} \cdot 109, 23^5) & 1.62991\dots \\ (11^2, 3^2 \cdot 5^6 \cdot 7^3, 2^{21} \cdot 23) & 1.62599\dots \\ (19 \cdot 1307, 7 \cdot 29^2 \cdot 31^8, 2^8 \cdot 3^{22} \cdot 5^4) & 1.62349\dots \end{array}$$

左側が $\mathbf{abc}[1.6]$ の元であり、1 行目では $(a, b, c) = (2, 3^{10} \cdot 109, 23^5)$ のとき、 $c = (\text{rad}(abc))^{1.62991\dots}$ という意味である。 $\mathbf{abc}[1.5]$ の元は 13 個だけ知られている。

予想 3.16 (abc 予想) 任意の実数 $\kappa > 1$ に対して、 $\mathbf{abc}[\kappa]$ は有限集合であろう。

予想 3.16 は Oesterlé と Masser により、1985 年に提出された。なお、予想 3.16 は予想 3.13 を導く。より精密にすれば、例えば $\kappa = 1.6$ のときには $\mathbf{abc}[1.6]$ が上記の 3 つの元だけから成ると期待できる。今後研究が進み、探索の範囲が広がることで新たな元が発見されるとしても有限個しか出てこない、というのが abc 予想の述べていることだが、できればこの 3 つ以外に元は存在しないと言い切りたい。そこで、与えられた実数 $\kappa > 1$ に対し、 $\mathbf{abc}[\kappa]$ の元は有限個で、しかもその全てをリストアップできるという主張を『強い abc 予想』と呼ぶことにしよう。

abc 予想の例として、 $\kappa = \frac{12}{11}$ に対する強い abc 予想を仮定すれば、次の Beal 予想が解決できることを示してみよう。

予想 3.17 (Beal 予想) p, q, r が 3 以上の整数ならば、どの 2 つも互いに素な正整数 x, y, z で $x^p + y^q = z^r$ を満たすものは存在しない。

$\kappa = \frac{12}{11}$ に対する強い abc 予想を仮定すれば、Beal 予想は正しいかどうか判定できる。

はじめに、 $\mathbf{abc}[\frac{12}{11}]$ に $(a, b, c) = (x^p, y^q, z^r)$ (p, q, r は 3 以上の正整数) という形の元が入っているかどうか調べる。もし見つけた場合は予想 3.17 に反例が見つかったという意味で問題は解決される。以下、そのような元

は存在しないと仮定する。その上で、どの2つも互いに素な正整数 x, y, z と3以上の整数 p, q, r で $x^p + y^q = z^r$, $x^p < y^q < z^r$ を満たすものが存在したとしよう。 $(a, b, c) = (x^p, y^q, z^r)$ は $\mathbf{abc}[\frac{12}{11}]$ に属さない $\mathbf{abc}$ の元だから、不等式 $z^r < (xyz)^{\frac{12}{11}}$ が成り立つ。不等式 $x^p < z^r$, $y^q < z^r$ に注意すると、 $x^p < (xyz)^{\frac{12}{11}}$, $y^q < (xyz)^{\frac{12}{11}}$ であることがわかる。さらに書き直すと、 $x < (xyz)^{\frac{12}{11p}}$, $y < (xyz)^{\frac{12}{11q}}$, $z < (xyz)^{\frac{12}{11r}}$ となり、これらを掛け合わせた式から、

$$1 < \frac{12}{11} \left(\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \right)$$

を得る。 $(p, q, r) = (3, 3, 3)$ の場合に $x^3 + y^3 = z^3$ を満たす正整数 x, y, z が存在しないことは、Euler によって18世紀に示されている。それ以外の $p, q, r \geq 3$ に対しては、 $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{1}{3} + \frac{1}{3} + \frac{1}{4} = \frac{11}{12}$ が成り立ち、これは上式に反している。 証明終

$\mathbf{abc}$ 予想は次のように定式化されることが多い。

予想 3.18 任意の実数 $\kappa > 1$ 、任意の $(a, b, c) \in \mathbf{abc}$ に対し $c < M(\text{rad}(abc))^\kappa$ を満たす定数 M が存在する。

これは予想 3.16 と同値である。より正確には、

命題 3.19 任意の $1 < \kappa < \kappa'$ に対し次が成り立つ。

- (1) κ に対する予想 3.16 から κ に対する予想 3.18 が従う。
- (2) κ に対する予想 3.18 から κ' に対する予想 3.16 が従う。

証明 (1) を示す。 $\kappa > 1$ に対し、 $\mathbf{abc}[\kappa]$ は有限集合であるので、任意の $(a, b, c) \in \mathbf{abc}[\kappa]$ に対して、 $c < M(\text{rad}(abc))^\kappa$ を満たすように実数 M をとることができる。

(2) を示す。 $\kappa > 1$ とする。ある実数 $M > 0$ が存在し、任意の $(a, b, c) \in \mathbf{abc}$, $c < M(\text{rad}(abc))^\kappa$ と仮定する。

示したい事は、任意の $\kappa' > \kappa$ に対し、 $|\mathbf{abc}[\kappa']| < \infty$ である。

つまり、

$$\left| \left\{ (a, b, c) \in \mathbb{N}^3 \left| \begin{array}{l} (a, b) = (b, c) = (c, a) = (1), \\ 0 < a < b < c, \ a + b = c, \\ c \geq (\text{rad}(abc))^{\kappa'} \end{array} \right. \right\} \right| < \infty$$

である。

ここで、 $\kappa' > \kappa$ を固定し、 $(a, b, c) \in \mathbf{abc}[\kappa']$ とする。このとき、 $\text{rad}(abc)^{\kappa'} < c$ がいえる。 $\mathbf{abc}[\kappa] \supset \mathbf{abc}[\kappa']$ であるので、仮定より、 $c < M(\text{rad}(abc))^\kappa$ がいえる。よって、

$$\text{rad}(abc)^{\kappa'} < c < M(\text{rad}(abc))^\kappa$$

が成り立つ。

両辺を $\text{rad}(abc)^\kappa$ で割ると $\text{rad}(abc)^{\kappa'-\kappa} < M$ となり、 $\kappa' - \kappa > 0$ により $\text{rad}(abc) < M^{\frac{1}{\kappa'-\kappa}}$ である。両辺を κ 乗すると、 $\text{rad}(abc)^\kappa < M^{\frac{\kappa}{\kappa'-\kappa}}$ を得る。上式に実数 $M > 0$ を掛けると、 $M\text{rad}(abc)^\kappa < M \cdot M^{\frac{1}{\kappa'-\kappa}}$ であり、仮定から $c < M\text{rad}(abc)^\kappa$ なので、

$$c < M^{1+\frac{\kappa}{\kappa'-\kappa}}$$

が成り立つ。

よって、 $\mathbf{abc}[\kappa']$ は有限集合である。

証明終

4 平方剰余の相互法則

4.1 準備

整数 a が与えられたとき、方程式

$$x^2 \equiv a \pmod{p}$$

の解の個数が素数 p に対してどのように変化するかを示す法則を与える。この法則のことを平方剰余の相互法則と呼ぶ。

定義 4.1 p を奇素数、 a を p と互いに素な整数とする。

$$x^2 \equiv a \pmod{p}$$

を満たす $x \in \mathbb{Z}$ が存在するとき a は p を法とする平方剰余といい、そうでないとき平方非剰余という。これを用いて、Legendre 記号を次のように定義する。

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & (a \text{ が } p \text{ を法とする平方剰余のとき}) \\ -1 & (a \text{ が } p \text{ を法とする平方非剰余のとき}) \end{cases}$$

命題 4.2 p を奇素数、 a を p と互いに素な整数とする。このとき

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

が成立する。この式は **Euler の基準** と呼ばれる。

定義 4.3 素数 p を固定する。正整数 n と $a \in \mathbf{F}_p$ に対し、 $N_n(a)$ を次のように定義する。

$$N_n(a) = |\{x \in \mathbf{F}_p \mid x^n = a\}|$$

定義 4.4 体 F と正整数 m に対して $\mathbf{X}_m(F)$ を次のように定義する。

$$\mathbf{X}_m(F) = \{(x_1, \dots, x_m) \in F^m \mid x_1^2 + \dots + x_m^2 = 1\}$$

命題 4.5 p を素数、 n を正整数、 $a \in \mathbf{F}_p$ とする。 n と $p-1$ の最大公約数を d とおく。このとき次の式が成立する。

$$N_n(a) = \begin{cases} 1 & (a = 0 \text{ のとき}) \\ d & (a^{\frac{p-1}{d}} = 1 \text{ のとき}) \\ 0 & (a^{\frac{p-1}{d}} \neq 0, 1) \end{cases}$$

この命題は次の補題より成り立つ。またこの命題で $n = 2$, p を奇素数としたとき、Euler 基準 (命題 4.2) が従うことに注意する。

補題 4.6 C を位数 l の巡回群とする。 $a \in C$, n を正整数、 d を l と n の最大公約数とする。このとき、

$$N_n(a) = \begin{cases} d & (a^{\frac{l}{d}} = 1 \text{ のとき}) \\ 0 & (\text{それ以外の場合}) \end{cases}$$

が成立する。

証明 n, l は d を使って、 $n = n'd$, $l = l'd$ と表せる。ただし n' と l' は互いに素な自然数である。

C は巡回群より $C = \langle \alpha \rangle$ を満たす $\alpha \in C$ が存在する。すると、 $C = \{1, \alpha, \alpha^2, \dots, \alpha^{l-1}\}$ とかける。

次に写像 ϕ を次のように定める。

$$\begin{aligned}\phi: C &\rightarrow C \\ \beta &\mapsto \beta^n\end{aligned}$$

すると、 C は Abel 群より ϕ は準同型写像である。

$\text{Ker}\phi$ について考える。 $(l', n') = 1$ に注意すると、

$$\begin{aligned}\alpha^k \in \text{Ker}\phi = \{\beta \in C \mid \beta^n = 1\} &\iff \alpha^{kn} = 1 \\ &\iff l \mid kn \\ &\iff l' \mid kn' \\ &\iff l' \mid k\end{aligned}$$

が成立する。よって $\text{Ker}\phi = \{1, \alpha^{l'}, \alpha^{2l'}, \dots, \alpha^{(d-1)l'}\}$ となり、 $|\text{Ker}\phi| = d$ である。

同型定理より、

$$\text{Im}\phi \cong C/\text{Ker}\phi$$

となる。よって、

$$|\text{Im}\phi| = |C|/|\text{Ker}\phi| = l/d = l'$$

である。巡回群の部分群は巡回群より、 $\text{Im}\phi \subset C$ は位数 l' の巡回群である。

$a \in \text{Im}\phi$ のときは、 $\phi(c) = a$ ($c \in C$) と表せる。このとき、

$$\begin{aligned}\phi(c) = \phi(b) &\iff \phi(c)^{-1}\phi(b) = 1 \\ &\iff \phi(c^{-1})\phi(b) = 1 \\ &\iff \phi(c^{-1}b) = 1 \\ &\iff c^{-1}b \in \text{Ker}\phi \\ &\iff b \in c\text{Ker}\phi\end{aligned}$$

が成立する。よって、

$$|\{b \in C \mid \phi(b) = 1\}| = d$$

となる。故に、

$$N_n(a) = d$$

が成立する。

また $a \notin \text{Im}\phi$ のときは $\text{Im}\phi$ と $N_n(a)$ の定義より $N_n(a) = 0$ となる。

最後に、 $a \in \text{Im}\phi \Leftrightarrow a^{l'} = 1$ を示す。 $\mathbf{V} = \{\beta \in C \mid \beta^{l'} = 1\}$ とおく。 $\text{Im}\phi$ は位数 l' の巡回群であったので $\text{Im}\phi \subset \mathbf{V}$ である。

$\mathbf{V}$ は、位数 l' の巡回群であることを示す。巡回群の部分群は巡回群なので、 $\mathbf{V}$ も巡回群である。よって、 $\mathbf{V} = \langle \gamma \rangle$ と書ける。すると、 $|\mathbf{V}| = \text{ord}(\gamma)$ である。しかし、 $\gamma \in \mathbf{V}$ より $\gamma^{l'} = 1$ となる。よって、 $\text{ord}(\gamma) \mid l'$ となることがわかる。つまり $|\mathbf{V}|$ は l' の約数である。ところが、 $1, \alpha^d, \alpha^{2d}, \dots, \alpha^{(l'-1)d} \in \mathbf{V}$ であるので $|\mathbf{V}| \geq l'$ であることが分かる。以上より、 $|\mathbf{V}| = l'$ となり証明は完了した。 証明終

命題 4.7 p を素数とすると、次が成り立つ。

$$|\mathbf{X}_2(\mathbf{F}_p)| = \begin{cases} 2 & (p = 2 \text{ のとき}) \\ p - 1 & (p \equiv 1 \pmod{4} \text{ のとき}) \\ p + 1 & (p \equiv 3 \pmod{4} \text{ のとき}) \end{cases}$$

この命題を証明するために、次の補題を用意する。

補題 4.8 p を素数とすると、次が成り立つ。

$$|\{x \in \mathbf{F}_p \mid x^2 + 1 = 0\}| = \begin{cases} 1 & (p = 2 \text{ のとき}) \\ 2 & (p \equiv 1 \pmod{4} \text{ のとき}) \\ 0 & (p \equiv 3 \pmod{4} \text{ のとき}) \end{cases}$$

証明 $p = 2$ のときは、 $x = 1$ のみ $x^2 + 1 = 0$ を満たす。 $p \neq 2$ のときは、 $(-1)^{\frac{p-1}{2}} = 1$ が $p \equiv 1 \pmod{4}$ と同値であることを注意して、命題 4.5 を $n = 2$, $a = -1$ として適用すればよい。 証明終

補題 4.9 F を標数が 2 でない体とすれば、次の写像は全単射である。

$$f: \{t \in F \mid t^2 \neq -1\} \rightarrow \mathbf{X}_2(F) \setminus \{(-1, 0)\}, \quad f(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

証明 任意の $t \in F$ 、(ただし、 $t^2 \neq -1$) に対して、 $f(t) \neq (-1, 0)$ であり、

$$\left(\frac{1-t^2}{1+t^2} \right)^2 + \left(\frac{2t}{1+t^2} \right)^2 = \frac{(1+t^2)^2}{(1+t^2)^2} = 1$$

となるので、 $f(t) \in \mathbf{X}_2(F) \setminus \{(-1, 0)\}$ である。よって写像

$$f : \{t \in F | t^2 \neq -1\} \rightarrow \mathbf{X}_2(F) \setminus \{(-1, 0)\}$$

は定義された。次に g を

$$g : \mathbf{X}_2(F) \setminus \{(-1, 0)\} \rightarrow \{t \in F | t^2 \neq -1\}, \quad g(x, y) = \frac{y}{1+x}$$

と定めたい。 $(x, y) \in \mathbf{X}_2(F) \setminus \{(-1, 0)\}$ に対して、 $y^2 = 1 - x^2$ であることに注意すると

$$\left(\frac{y}{1+x}\right)^2 = \frac{y^2}{(1+x)^2} = \frac{(1+x)(1-x)}{(1+x)^2} = \frac{1-x}{1+x} \neq -1$$

であり、写像 g が定まった。

次に g が f の逆写像であることを示す。 $(x, y) \in \mathbf{X}_2(F) \setminus \{(-1, 0)\}$ に対して、 $x^2 + y^2 = 1$ であることに注意すると

$$\begin{aligned} f(g(x, y)) &= f\left(\frac{y}{1+x}\right) = \left(\frac{1 - \left(\frac{y}{1+x}\right)^2}{1 + \left(\frac{y}{1+x}\right)^2}, \frac{2\frac{y}{1+x}}{1 + \left(\frac{y}{1+x}\right)^2}\right) \\ &= \left(\frac{(1+x)^2 - y^2}{(1+x)^2 + y^2}, \frac{2y(1+x)}{(1+x)^2 + y^2}\right) \\ &= \left(\frac{2x + 2x^2}{2 + 2x}, \frac{2y(1+x)}{2 + 2x}\right) \\ &= (x, y) \end{aligned}$$

となる。また、 $t \in F$ 、(ただし $t^2 \neq -1$) のとき

$$g(f(t)) = g\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = \frac{\frac{2t}{1+t^2}}{1 + \frac{1-t^2}{1+t^2}} = \frac{2t}{2} = t$$

となる。よって f は全単射である。

証明終

命題 4.7 の証明 $p = 2$ のときは

$$\begin{aligned} |\mathbf{X}_2(\mathbf{F}_2)| &= |\{(x, y) \in \mathbf{F}_2 | x^2 + y^2 = 1\}| \\ &= |\{(0, 1), (1, 0)\}| \\ &= 2 \end{aligned}$$

である。以下、 $p \neq 2$ と仮定する。

補題 4.8 を用いると、

$$|\{t \in \mathbf{F}_p | t^2 \neq -1\}| = \begin{cases} p-2 & (p \equiv 1 \pmod{4}) \\ p & (p \equiv 3 \pmod{4}) \end{cases}$$

となる。補題 4.9 より

$$f : \{t \in \mathbf{F}_p \mid t^2 \neq -1\} \rightarrow \mathbf{X}_2(\mathbf{F}_p) \setminus \{(-1, 0)\}, f(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

は全単射である。よって、

$$\begin{aligned} |\mathbf{X}_2(\mathbf{F}_p) \setminus \{(-1, 0)\}| &= |\{t \in \mathbf{F}_p \mid t^2 \neq -1\}| \\ &= \begin{cases} p-2 & (p \equiv 1 \pmod{4}) \\ p & (p \equiv 3 \pmod{4}) \end{cases} \end{aligned}$$

となる。

証明終

定理 4.10 奇素数 p と正整数 m に対して次が成り立つ。

$$|\mathbf{X}_m(\mathbf{F}_p)| = \begin{cases} p^{m-1} + p^{\frac{m-1}{2}} & (p \equiv 1 \pmod{4}, m : \text{奇数}) \\ p^{m-1} - p^{\frac{m}{2}-1} & (p \equiv 1 \pmod{4}, m : \text{偶数}) \\ p^{m-1} + (-1)^{\frac{m-1}{2}} p^{\frac{m-1}{2}} & (p \equiv 3 \pmod{4}, m : \text{奇数}) \\ p^{m-1} - (-1)^{\frac{m}{2}} p^{\frac{m}{2}-1} & (p \equiv 3 \pmod{4}, m : \text{偶数}) \end{cases}$$

この定理の証明ために、次の補題を用意する。

補題 4.11 p を奇素数、 $a \in \mathbf{F}_p$ とする。集合 $\mathbf{S}_a$ を次のように定める。

$$\mathbf{S}_a = \{(u, v) \in \mathbf{F}_p^2 \mid u^2 + v^2 = a\}$$

(1) $a = 0$ ならば次が成り立つ。

$$|\mathbf{S}_0| = \begin{cases} 2p-1 & (p \equiv 1 \pmod{4} \text{ のとき}) \\ 1 & (p \equiv 3 \pmod{4} \text{ のとき}) \end{cases}$$

(2) $a \neq 0$ ならば次が成り立つ。

$$|\mathbf{S}_a| = \begin{cases} p-1 & (p \equiv 1 \pmod{4} \text{ のとき}) \\ p+1 & (p \equiv 3 \pmod{4} \text{ のとき}) \end{cases}$$

証明 (1) を示す。 $\mathbf{S}_0 = \{(u, v) \in \mathbf{F}_p^2 \mid u^2 + v^2 = 0\}$ である。 $p \equiv 3 \pmod{4}$ のとき補題 4.8 より $\mathbf{S}_0 = \{(0, 0)\}$ となる。よってこのとき $|\mathbf{S}_0| = 1$ となる。

$p \equiv 1 \pmod{4}$ のとき補題 4.8 を用いて $j^2 = -1$ となる $j \in \mathbf{F}_p$ をとると、

$$\mathbf{S}_0 = \{(0, 0), (1, \pm j), (2, \pm 2j), \dots, (p-1, \pm(p-1)j)\}$$

となる。よって $\mathbf{S}_0 = 2p-1$ となる。

(2) を示す。 $a = 1$ のとき $\mathbf{S}_1 = \mathbf{X}_2(\mathbf{F}_p)$ より命題 4.7 から定理が成立する。よって、 $a \in \mathbf{F}_p$ に対して、 $|\mathbf{S}_a| = |\mathbf{S}_1|$ を示せばよい。

g を $\mathbf{F}_p$ の原始元とする。 $\mathbf{F}_p = \{0, 1, g, g^2, \dots, g^{p-2}\}$ であるので

$$\{s^2 | s \in \mathbf{F}_p\} = \{0, 1, g^2, g^4, \dots, g^{p-3}\}$$

となる。 s が $\mathbf{F}_p$ の元を走るとき、 s^2 は $\frac{1}{2}(p+1)$ 個の値をとる。よって、 t が $\mathbf{F}_p$ の元を走るとき、 $a-t^2$ は $\frac{1}{2}(p+1)$ 個の値をとることも分かる。 $\mathbf{F}_p$ の元の個数は p 個であり、 $\frac{1}{2}(p+1) + \frac{1}{2}(p+1) = p+1$ より真に小さいので、両者は共通の値をとる。つまり、 $s^2 = a-t^2$ を満たす $s, t \in \mathbf{F}_p$ が存在し、 $(s, t) \in \mathbf{S}_a$ となる。 $x^2 + y^2 = 1$ ならば $(sx - ty)^2 + (sy + tx)^2 = (s^2 + t^2)(x^2 + y^2) = a$ となるので

$$\begin{aligned} f : \mathbf{S}_1 &\rightarrow \mathbf{S}_a \\ (x, y) &\mapsto (sx - ty, sy + tx) \end{aligned}$$

写像 f は well-defined である。 $(u, v) \in \mathbf{S}_a$ として

$$\frac{1}{a^2}(su + tv)^2 + \frac{1}{a^2}(sv - tu)^2 = \frac{1}{a^2}(s^2 + t^2)(u^2 + v^2) = 1$$

が成り立つので、

$$\begin{aligned} h : \mathbf{S}_a &\rightarrow \mathbf{S}_1 \\ (u, v) &\mapsto \left(\frac{1}{a}(su + tv), \frac{1}{a}(sv - tu)\right) \end{aligned}$$

より写像 h は well-defined。

次に $h(f(x, y)) = (x, y)$, $f(h(u, v)) = (u, v)$ を確かめる。

$$\begin{aligned} h(f(x, y)) &= \left(\frac{1}{a}(s(sx - ty) + t(sy + tx)), \frac{1}{a}(s(sy + tx) - t(sx - ty))\right) \\ &= \left(\frac{s^2 + t^2}{a}x, \frac{s^2 + t^2}{a}y\right) \\ &= (x, y) \\ f(h(u, v)) &= \left(s\frac{su + tv}{a} - t\frac{sv - tu}{a}, s\frac{sv - tu}{a} + t\frac{su + tv}{a}\right) \\ &= \left(\frac{s^2 + t^2}{a}u, \frac{s^2 + t^2}{a}v\right) \\ &= (u, v) \end{aligned}$$

これにより f と h 互いに逆写像であることが確認できた。

よって $|S_a| = |S_1|$ である。

証明終

定理 4.10 の証明 $m = 1$ のときは $\mathbf{X}_1(\mathbf{F}_p) = \{\pm 1\}$ より成立する。

$m = 2$ のときは命題 4.7 で示した。

$m \geq 3$ として $(x_1, \dots, x_{m-2}) \in \mathbf{F}_p^{m-2}$ を任意にとる。集合

$$\{(x_{m-1}, x_m) \in \mathbf{F}_p^2 \mid (x_1, \dots, x_{m-2}, x_{m-1}, x_m) \in \mathbf{X}_m(\mathbf{F}_p)\}$$

の元の個数は、次のように場合分けして求めることが出来る。

- (1) $(x_1, \dots, x_{m-2}) \in \mathbf{X}_{m-2}(\mathbf{F}_p)$ のときは $|\mathbf{S}_0|$ 通り。
- (2) そうでないときは補題 4.11 を用いて、 $|\mathbf{S}_1|$ 通りある。

$$\begin{aligned} |\mathbf{X}_m(\mathbf{F}_p)| &= \begin{cases} (2p-1)|\mathbf{X}_{m-2}(\mathbf{F}_p)| + (p-1)(p^{m-2} - |\mathbf{X}_{m-2}(\mathbf{F}_p)|) & (p \equiv 1 \pmod{4}) \\ |\mathbf{X}_{p-2}(\mathbf{F}_p)| + (p+1)(p^{m-2} - |\mathbf{X}_{p-2}(\mathbf{F}_p)|) & (p \equiv 3 \pmod{4}) \end{cases} \\ &= \begin{cases} p^{m-1} - p^{m-2} + p|\mathbf{X}_{m-2}(\mathbf{F}_p)| & (p \equiv 1 \pmod{4}) \\ p^{m-1} + p^{m-2} - p|\mathbf{X}_{m-2}(\mathbf{F}_p)| & (p \equiv 3 \pmod{4}) \end{cases} \end{aligned}$$

がわかる。以下、定理 4.10 を m に関する帰納法を用いて示す。 $m = 1, 2$ のときは示した。 $m \geq 3$ として $m-1$ まで仮定する。

- (1) m が奇数のとき、 $m-2$ のときに正しいので、

$$\begin{aligned} |\mathbf{X}_m(\mathbf{F}_p)| &= \begin{cases} p^{m-1} - p^{m-2} + p|\mathbf{X}_{m-2}(\mathbf{F}_p)| & (p \equiv 1 \pmod{4}) \\ p^{m-1} + p^{m-2} - p|\mathbf{X}_{m-2}(\mathbf{F}_p)| & (p \equiv 3 \pmod{4}) \end{cases} \\ &= \begin{cases} p^{m-1} - p^{m-2} + p(p^{m-3} + p^{\frac{m-3}{2}}) & (p \equiv 1 \pmod{4}) \\ p^{m-1} + p^{m-2} - p(p^{m-3} + (-1)^{\frac{m-3}{2}} p^{m-3}) & (p \equiv 3 \pmod{4}) \end{cases} \\ &= \begin{cases} p^{m-1} + p^{\frac{m-1}{2}} & (p \equiv 1 \pmod{4}) \\ p^{m-1} + (-1)^{\frac{m-1}{2}} p^{\frac{m-1}{2}} & (p \equiv 3 \pmod{4}) \end{cases} \end{aligned}$$

となり、 m のときも成立する。

(2) m が偶数のとき、 $m-2$ のときに正しいので、

$$\begin{aligned}
|\mathbf{X}_m(\mathbf{F}_p)| &= \begin{cases} p^{m-1} - p^{m-2} + p|\mathbf{X}_{m-2}(\mathbf{F}_p)| & (p \equiv 1 \pmod{4}) \\ p^{m-1} + p^{m-2} - p|\mathbf{X}_{m-2}(\mathbf{F}_p)| & (p \equiv 3 \pmod{4}) \end{cases} \\
&= \begin{cases} p^{m-1} - p^{m-2} + p(p^{m-3} - p^{\frac{m-2}{2}-1}) & (p \equiv 1 \pmod{4}) \\ p^{m-1} + p^{m-2} - p(p^{m-3} - (-1)^{\frac{m-2}{2}} p^{\frac{m-2}{2}-1}) & (p \equiv 3 \pmod{4}) \end{cases} \\
&= \begin{cases} p^{m-1} - p^{\frac{m}{2}-1} & (p \equiv 1 \pmod{4}) \\ p^{m-1} + (-1)^{\frac{m}{2}} p^{\frac{m}{2}-1} & (p \equiv 3 \pmod{4}) \end{cases}
\end{aligned}$$

となり m のときも成立する。

証明終

4.2 平方剰余の相互法則

定理 4.12 (1) (第一補充法則) p を奇素数とすると、次が成り立つ。

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

(2) (第二補充法則) p を奇素数とすると、次が成り立つ。

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & (p \equiv 1, 7 \pmod{8} \text{ のとき}) \\ -1 & (p \equiv 3, 5 \pmod{8} \text{ のとき}) \end{cases}$$

(3) (平方剰余の相互法則) p, q を相異なる奇素数とすると、次が成り立つ。

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = \begin{cases} 1 & (p \equiv 1 \pmod{4} \text{ または } q \equiv 1 \pmod{4}) \\ -1 & (p \equiv 3 \pmod{4} \text{ かつ } q \equiv 3 \pmod{4}) \end{cases}$$

証明 (1) は補題 4.8 の言い換えである。

(2) は p を奇素数、 F を体とする。 $\mathbf{X}_2(\mathbf{F}_p)$ の元の個数を求める。 $(x, y) \in \mathbf{X}_2(\mathbf{F}_p)$ とする。

(a) $x, y \neq 0$ かつ $x \neq \pm y$ と仮定する。このとき、 $(\pm x, \pm y), (\pm y, \pm x)$ の形の 8 個の元は $\mathbf{X}_2(\mathbf{F}_p)$ の元である。

- (b) $(x, y) \in \mathbf{X}_2(\mathbf{F}_p)$ のうち $x = 0$ となるものは $(0, \pm 1)$ の 2 個、 $y = 0$ となるものは $(\pm 1, 0)$ の 2 個である。
- (c) $x = \pm y$ となるものについて考える。 $2t^2 = 1$ を満たす t の個数は、 $1 + \left(\frac{2^{-1}}{p}\right) = 1 + \left(\frac{2}{p}\right)$ 個になることに注意すると $x = \pm y$ となる $(x, y) \in \mathbf{X}_2(\mathbf{F}_p)$ は $2 + 2\left(\frac{2}{p}\right)$ 個ある。

以上より $\mathbf{X}_2(\mathbf{F}_p) = (\text{a}) \amalg (\text{b}) \amalg (\text{c})$ であることから、

$$|\mathbf{X}_2(\mathbf{F}_p)| \equiv 6 + 2\left(\frac{2}{p}\right) \pmod{8} \quad (*)$$

が成立する。命題 4.7 と比較すると、

- (A) $p \equiv 1 \pmod{4}$ つまり、 $p \equiv 1, 5 \pmod{8}$ とする。 $(*)$ は $p - 1 \equiv 6 + 2\left(\frac{2}{p}\right) \pmod{8}$ となる。

$p \equiv 1 \pmod{8}$ のときは、 $0 \equiv 6 + 2\left(\frac{2}{p}\right) \pmod{8}$ により、 $\left(\frac{2}{p}\right) = 1$ となる。

次に $p \equiv 5 \pmod{8}$ のときは、 $4 \equiv 6 + 2\left(\frac{2}{p}\right) \pmod{8}$ により、 $\left(\frac{2}{p}\right) = -1$ となる。

- (B) $p \equiv 3 \pmod{4}$ つまり、 $p \equiv 3, 7 \pmod{8}$ とする。 $(*)$ は $p + 1 \equiv 6 + 2\left(\frac{2}{p}\right) \pmod{8}$ となる。

$p \equiv 3 \pmod{8}$ のときは、 $4 \equiv 6 + 2\left(\frac{2}{p}\right) \pmod{8}$ により、 $\left(\frac{2}{p}\right) = -1$ となる。

次に、 $p \equiv 7 \pmod{8}$ のときは、 $8 \equiv 6 + 2\left(\frac{2}{p}\right) \pmod{8}$ により、 $\left(\frac{2}{p}\right) = 1$ となる。

以上により

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & (p \equiv 1, 7 \pmod{8} \text{ のとき}) \\ -1 & (p \equiv 3, 5 \pmod{8} \text{ のとき}) \end{cases}$$

が示された。

- (3) p, q を異なる奇素数とする。 $\mathbf{X}_q(\mathbf{F}_p)$ の元の個数を調べる。

$(x_1, \dots, x_p) \in \mathbf{X}_p(\mathbf{F}_p)$ に対して $x_1 = x_2 = \dots = x_q$ を満たさない限り、

$$\begin{aligned} & (x_1, x_2, x_3, \dots, x_q), \\ & (x_q, x_1, x_2, \dots, x_{q-1}), \\ & (x_{q-1}, x_q, x_1, \dots, x_{q-2}), \\ & \vdots \\ & (x_2, x_3, \dots, x_{q-1}, x_q, x_1) \end{aligned}$$

は q 個の異なる $\mathbf{X}_q(\mathbf{F}_p)$ の元を与える。(このことは後で補題 4.14 で示す。)

$qt^2 = 1$ を満たす $t \in \mathbf{F}_p$ の個数は $1 + \left(\frac{q}{p}\right)$ であることに注意すると、
 $x_1 = x_2 = \dots = x_q$ を満たすような $\mathbf{X}_q(\mathbf{F}_p)$ の元は $1 + \left(\frac{q}{p}\right)$ 個あることがわかる。よって、

$$|\mathbf{X}_q(\mathbf{F}_p)| \equiv 1 + \left(\frac{q}{p}\right) \pmod{q}$$

となる。 $p^{q-1} \equiv 1 \pmod{q}$ (Fermat の小定理), $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod{q}$ (Euler 基準) に注意して定理 4.10 と比較する。

(1) $p \equiv 1 \pmod{4}$ のときは、 $|\mathbf{X}_q(\mathbf{F}_p)| = p^{q-1} + p^{\frac{q-1}{2}}$ なので、

$$\begin{aligned} p^{q-1} + p^{\frac{q-1}{2}} &\equiv 1 + \left(\frac{q}{p}\right) \pmod{q} \\ 1 + \left(\frac{p}{q}\right) &\equiv 1 + \left(\frac{q}{p}\right) \pmod{q} \\ \left(\frac{p}{q}\right) &\equiv \left(\frac{q}{p}\right) \pmod{q} \end{aligned}$$

となる。ここで $\left(\frac{p}{q}\right), \left(\frac{q}{p}\right)$ は 1 か -1 のどちらかなので、

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

である。よって

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = 1$$

となる。

(2) $p \equiv 3 \pmod{4}$ かつ $q \equiv 3 \pmod{4}$ のときは、 $|\mathbf{X}_q(\mathbf{F}_p)| = p^{q-1} + (-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}}$ なので、

$$\begin{aligned} 1 + \left(\frac{q}{p}\right) &\equiv p^{q-1} + (-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} \pmod{q} \\ 1 + \left(\frac{q}{p}\right) &\equiv 1 + (-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} \pmod{q} \\ \left(\frac{q}{p}\right) &\equiv (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod{q} \end{aligned}$$

となる。ここで、 $\left(\frac{p}{q}\right), \left(\frac{q}{p}\right)$ は 1 か -1 のどちらかなので、

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

となる。 $q \equiv 3 \pmod{4}$ より $\frac{q-1}{2}$ は奇数であるので、

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

となる。(1), (2) より

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = \begin{cases} 1 & (p \equiv 1 \pmod{4} \text{ または } q \equiv 1 \pmod{4}) \\ -1 & (p \equiv 3 \pmod{4} \text{ かつ } q \equiv 3 \pmod{4}) \end{cases}$$

が示された。

証明終

注意 4.13 p を奇数とするとき、

$$\begin{aligned} \frac{p-1}{2} &\equiv \begin{cases} 0 \pmod{2} & (p \equiv 1 \pmod{4} \text{ のとき}) \\ 1 \pmod{2} & (p \equiv 3 \pmod{4} \text{ のとき}) \end{cases} \\ \frac{p^2-1}{8} &\equiv \begin{cases} 0 & (p \equiv 1, 7 \pmod{8} \text{ のとき}) \\ 1 & (p \equiv 3, 5 \pmod{8} \text{ のとき}) \end{cases} \end{aligned}$$

が成り立つ。これを用いると、定理 4.12 は奇素数 p, q に対して、

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \quad \left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

と表せる。この表現はよく使われる。

補題 4.14 p, q を奇素数とする。

$$\left. \begin{array}{l} (x_0, x_1, \dots, x_{q-1}) \\ (x_1, x_2, \dots, x_0) \\ (x_2, x_3, \dots, x_1) \\ \vdots \\ (x_{q-1}, x_1, \dots, x_{q-2}) \end{array} \right\} \in (\mathbf{F}_p)^q$$

の中に少なくとも一組同じ元があることの必要十分条件は、 $x_0 = x_1 = \dots = x_{q-1}$ となることである。

証明 $j = mq + l$ ($0 \leq l < q$) に対して $x_j := x_l$ と定める。

ある 2 元が等しいなら、

$$\begin{aligned} x_0 &= x_i \\ x_1 &= x_{i+1} \\ &\vdots \\ x_{q-1} &= x_{i+q-1} \end{aligned}$$

を満たす i がある。ただし i は $0 \leq i \leq q-1$ を満たす。つまり、任意の $j \geq 0$ に対して $x_{j+i} = x_j$ である。よって、 $x_0 = x_i = x_{2i} = \dots$ が分かる。
(i, q) = 1 より任意の $0 \leq j < q$ に対して、

$$ni + mq = j$$

を満たす $n \in \mathbf{N}, m \in \mathbf{Z}$ が存在する。

以上により、 $x_0 = x_{ni} = x_{j-mq} = x_j$ である。よって、任意の $0 \leq j < q$ に対して $x_0 = x_j$ が示された。 証明終

4.3 平方剰余の相互法則の別証明

定理 4.12(3) の別証明として、Gauss の第五証明を元に Schmidt の改良を経て Rousseau が簡易化した証明を与える。

証明 p, q を奇素数とする。 $(\mathbb{Z}/(p))^\times \times (\mathbb{Z}/(q))^\times$ の二つの部分集合を、次のように定義する。

$$\begin{aligned} S &= \left\{ (i + (p), j + (q)) \mid 1 \leq i \leq p-1, 1 \leq j \leq \frac{q-1}{2} \right\}, \\ T &= \left\{ (k + (p), k + (q)) \mid 1 \leq k \leq \frac{pq-1}{2}, (k, pq) = (1) \right\}. \end{aligned}$$

ここで、次の三つの主張を証明する。

- (a) S の元すべての積を $\prod_S \in (\mathbb{Z}/(p))^\times \times (\mathbb{Z}/(q))^\times$ とおくと次が成り立つ。

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

- (b) T の元すべての積を $\prod_T \in (\mathbb{Z}/(p))^\times \times (\mathbb{Z}/(q))^\times$ とおくと次が成り立つ。

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

- (c) 任意の $(s_1, s_2) \in (\mathbb{Z}/(p))^\times \times (\mathbb{Z}/(q))^\times$ に対して、 (s_1, s_2) と $(-s_1, -s_2)$ の片方のみが S に属する。同様に、 (s_1, s_2) と $(-s_1, -s_2)$ の片方のみが T に属する。特に、 $|S| = |T|$ である。

- (a) を証明する。定義により、

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

である。ここで、

$$\begin{aligned} (q-1)! &= \left(1 \cdot 2 \cdots \frac{q-1}{2} \right) \cdot \left(\frac{q+1}{2} \cdots (q-2) \cdot (q-1) \right) \\ &\equiv \left(1 \cdot 2 \cdots \frac{q-1}{2} \right) \cdot \left(-\frac{q-1}{2} \cdots (-2) \cdot (-1) \right) \\ &= (-1)^{\frac{q-1}{2}} \left(\frac{q-1}{2}! \right)^2 \pmod{q} \end{aligned}$$

となることに注意して第二成分を書き直せば

$$\begin{aligned} \left(\frac{q-1}{2}! \right)^{p-1} &= \left(\left(\frac{q-1}{2}! \right) \right)^{2 \cdot \frac{p-1}{2}} \\ &\equiv \left((q-1)! \right)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \pmod{q} \end{aligned}$$

となる。よって、(a) は示せた。

- (b) を証明する。第一成分を考える。まず、

$$\frac{pq-1}{2} = \frac{p(q-1) + p-1}{2} = p \frac{q-1}{2} + \frac{p-1}{2}$$

に注意する。よって、 k が $1 \leq k \leq \frac{pq-1}{2}$ の範囲の p と互いに素であるような全ての整数を走るとき、それらの積は、

$$\begin{aligned} & \left(\prod_{i=1}^{p-1} i \right) \left(\prod_{i=1}^{p-1} (p+i) \right) \cdots \left(\prod_{i=1}^{p-1} \left(\frac{q-3}{2}p + i \right) \right) \left(\prod_{i=1}^{(p-1)/2} \left(\frac{q-1}{2}p + i \right) \right) \\ & \equiv ((p-1)!)^{\frac{q-1}{2}} \cdot \frac{p-1}{2}! \pmod{p} \end{aligned}$$

となる。

$$\frac{p-1}{2}q < \frac{pq-1}{2} < \frac{p+1}{2}q$$

であるので、この中で q の倍数となるような k の積は、

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

で与えられる。これと Euler の基準 $\left(\left(\frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p} \right)$ を用いると

$$\prod_{(a,b) \in T} a \equiv \frac{((p-1)!)^{\frac{q-1}{2}} \cdot \frac{p-1}{2}!}{q^{\frac{p-1}{2}} \cdot \frac{p-1}{2}!} \equiv ((p-1)!)^{\frac{q-1}{2}} \left(\frac{q}{p} \right) \pmod{p}$$

を得る。第二成分についても同様である。よって (b) は示せた。

(c) を証明する。

定義により、 $(\bar{a}, \bar{b}) \in (\mathbb{Z}/(p))^{\times} \times (\mathbb{Z}/(q))^{\times}$ に対して、 $(\bar{a}, \bar{b})$ 又は、 $(-\bar{a}, -\bar{b})$ のどちらか片方のみが S に入ることは明らかである。

自然な写像

$$\begin{aligned} G : (\mathbb{Z}/(pq))^{\times} &\longrightarrow (\mathbb{Z}/(p))^{\times} \times (\mathbb{Z}/(q))^{\times} \\ u + (pq) &\longmapsto (u + (p), u + (q)) \end{aligned}$$

について考える。この写像は中国剰余定理によって、全単射である。ここで、

$$T' = \left\{ \bar{c} \in (\mathbb{Z}/(pq))^{\times} \mid 1 \leq c \leq \frac{pq}{2} \right\}$$

と定義する。このとき、 $T = G(T')$ である。 $\bar{c} \in (\mathbb{Z}/(pq))^{\times}$ に対して、 $\bar{c}$ と、 $-\bar{c}$ の片方のみが T' に入る。つまり、 $(\bar{a}, \bar{b}) \in (\mathbb{Z}/(p))^{\times} \times (\mathbb{Z}/(q))^{\times}$ に対して、 $(\bar{a}, \bar{b}), (-\bar{a}, -\bar{b})$ の片方のみが T に属する。

$(\bar{a}, \bar{b}) \in (\mathbb{Z}/(p))^{\times} \times (\mathbb{Z}/(q))^{\times}$ のとき、 $(\bar{a}, \bar{b}) \neq (-\bar{a}, -\bar{b})$ である。このことから、 $|S| = |T|$ がわかる。これより (c) が従う。

定理 4.12 (3) は次のように、(a), (b), (c) から従う。

(c) において、 $(s_1, s_2) \in S$ かつ $(-s_1, -s_2) \in T$ を満たす (s_1, s_2) の個数を u とおく。(a), (b) を比較すると、

$$\begin{aligned} ((p-1)!)^{\frac{q-1}{2}} &\equiv (-1)^u ((p-1)!)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p} \\ (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} ((q-1)!)^{\frac{p-1}{2}} &\equiv (-1)^u ((q-1)!)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q} \end{aligned}$$

を得るとなる。これより、

$$\begin{aligned} 1 &\equiv (-1)^u \left(\frac{q}{p}\right) \pmod{p} \\ (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} &\equiv (-1)^u \left(\frac{q}{p}\right) \pmod{q} \end{aligned}$$

となるが、各項全て ± 1 なので、合同式は等式で置き換えられる。よって、

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

となる。

証明終

5 虚二次体

5.1 虚二次体とその部分環

定義 5.1 $\alpha \in \mathbb{C}$ に対して、 $\alpha = a + b\sqrt{-1}$ ($a, b \in \mathbb{R}$) と表したとき、 $\bar{\alpha} = a - b\sqrt{-1}$ と定める。これを α の共役という。また、

$$N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 \in \mathbb{R}_{\geq 0}, \quad \text{Tr}(\alpha) = \alpha + \bar{\alpha} = 2a \in \mathbb{R}$$

をそれぞれ α のノルム、 α のトレースと言う。

ノルムとトレースは、 $N(\alpha\beta) = N(\alpha)N(\beta)$, $\text{Tr}(\alpha + \beta) = \text{Tr}(\alpha) + \text{Tr}(\beta)$ を満たす。

以下、 $d \in \mathbb{Z}_{>0}$ とする。 $\sqrt{-d} = \sqrt{d}\sqrt{-1}$ として、

$$\mathbb{Q}(\sqrt{-d}) = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$$

を虚二次体という。

$\mathbb{Q}(\sqrt{-d})$ が $\mathbb{C}$ の部分体であることは、四則演算について閉じていることをみれば分かる。

$d, d_1, n \in \mathbb{Z}_{>0}$ に対して、 $d = d_1 n^2$ ならば $\sqrt{-d} = n\sqrt{-d_1}$ により $\mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(\sqrt{-d_1})$ なので以降、次を仮定する; $1 < n \in \mathbb{Z}$ で、 $n^2 \mid d$ となるものは存在しない。 $(d \text{ が square free であるという。})$

命題 5.2 (1) $\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$ は、 $\mathbb{Q}(\sqrt{-d})$ の部分環である。

(2) $d \in \mathbb{Z}_{>0}$ は square free で $d \equiv 1, 2 \pmod{4}$ とする。このとき、 $\alpha \in \mathbb{Q}(\sqrt{-d})$ について、次は同値である。

- (a) $\alpha \in \mathbb{Z}[\sqrt{-d}]$
- (b) $N(\alpha), \text{Tr}(\alpha) \in \mathbb{Z}$
- (c) ある $a, b \in \mathbb{Z}$ があって、 $\alpha^2 + a\alpha + b = 0$ を満たす。

証明 (1) は、和と差と積で閉じていて $1 \in \mathbb{Z}[\sqrt{-d}]$ なのでよい。

(2) を示す。(a) $\Rightarrow$ (b) は、定義から明らかである。

(b) $\Rightarrow$ (c) については $a = -\text{Tr}(\alpha), b = N(\alpha)$ とおけばよい。

(c) $\Rightarrow$ (a) を示す。 $\mathbb{Z}$ の素因数分解の一意性により、 $\alpha \in \mathbb{Q}$ ならば $\alpha \in \mathbb{Z}$ である。

$\alpha \notin \mathbb{Q}$ とすると、 $\alpha = x + y\sqrt{-d}$ ($x, y \in \mathbb{Q}, y \neq 0$) と書ける。 $\alpha, \bar{\alpha}$ は $T^2 + aT + b = 0$ の解なので、解と係数の関係により $2x = -a \in \mathbb{Z}$, $x^2 + y^2 d = b \in \mathbb{Z}$ となる。この2式より $d(2y)^2 = 4b - a^2 \in \mathbb{Z}$ を得る。このとき $2y \in \mathbb{Z}$ である。もしそうでないとすると、 $2y = t/s$ ($0 \neq s, t \in \mathbb{Z}, s$ と t は互いに素) と表せるが、 $dt^2 = s^2(4b - a^2)$ となる。ここで、 s, t は互いに素なので、 s^2, t^2 もそうである。したがって、 $s^2 \mid d$ であり、 d が square free なので $s = 1$ である。故に、 $y = y'/2$ ($y' \in \mathbb{Z}$) とすれば、 $b = x^2 + dy^2 = (a^2 + dy'^2)/4 \in \mathbb{Z}$ により、 $4 \mid a^2 + dy'^2$ となり、 $d \equiv 1, 2 \pmod{4}$ であることによって、 a, y' は共に偶数となる。よって、 $x = -a/2 \in \mathbb{Z}$, $y = y'/2 \in \mathbb{Z}$ なので、 $\alpha \in \mathbb{Z}[\sqrt{-d}]$ を得る。 証明終

注意 5.3 (1) $d \in \mathbb{Z}_{>0}$ は square free で、 $d \equiv 1, 2 \pmod{4}$ のとき、 $\mathbb{Z}[\sqrt{-d}]$ を $\mathbb{Q}(\sqrt{-d})$ の整数環という。

(2) $d \equiv 3 \pmod{4}$ のときは、命題 5.2(2) の (a) $\Leftrightarrow$ (c) は成立しない。実際、 $d = 3$, $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-d})$ について、 $\omega^2 + \omega + 1 = 0$ を満たすが、 $\omega \notin \mathbb{Z}[\sqrt{-d}]$ である。

補題 5.4 d は square free で $d \equiv 1, 2 \pmod{4}$ とすると、次が成り立つ。

(1) $\alpha \in \mathbb{Z}[\sqrt{-d}]$ に対して、 $\alpha \in \mathbb{Z}[\sqrt{-d}]^\times$ と $N(\alpha) = 1$ は同値である。

$$(2) \mathbb{Z}[\sqrt{-d}]^\times = \begin{cases} \{\pm 1, \pm\sqrt{-1}\} & (d = 1) \\ \{\pm 1\} & (d > 1) \end{cases}$$

証明 (1) を示そう。ある $\beta \in \mathbb{Z}[\sqrt{-d}]$ があって $\alpha\beta = 1$ を満たすならば、両辺ノルムをとって $N(\alpha)N(\beta) = 1$ より $N(\alpha) = 1$ を得る。逆に、 $N(\alpha) = 1$ ならば $\alpha\bar{\alpha} = N(\alpha) = 1$ より成立する。

(2) を示そう。 $\alpha \in \mathbb{Z}[\sqrt{-d}]^\times$ に対して、 $\alpha = a + b\sqrt{-d}$ ($a, b \in \mathbb{Z}$) と表すと、(1) より $a^2 + db^2 = N(\alpha) = 1$ となる。よって、

$$(a, b) = \begin{cases} (\pm 1, 0), (0, \pm 1) & (d = 1) \\ (\pm 1, 0) & (d > 1) \end{cases}$$

となる。

証明終

5.2 素数の分解

$d = 1, 2$ のとき、 $\mathbb{Z}[\sqrt{-d}]$ はノルム $N(\alpha)$ により Euclid 整域であるから PID であり素元分解ができてその一意性が成り立つ。これらの素元はどのようなものであるか。素数が $\mathbb{Z}[\sqrt{-d}]$ で素元であるとは限らない。実際 $\mathbb{Z}[\sqrt{-1}]$ において、

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

のようになり、一方、3 は $\mathbb{Z}[\sqrt{-1}]$ の素元であることが示される。まず $d = 1, 2$ のとき、どの素数が分解できて、 $\mathbb{Z}[\sqrt{-d}]$ の素元がどのようなものであるかを見てゆく。

補題 5.5 $d = 1, 2$ 、 $R = \mathbb{Z}[\sqrt{-d}]$ とする。

(1) $\pi \in R$ 、 $p = N(\pi)$ が素数ならば、 π は R の素元である。

(2) π が R の素元ならば、 $N(\pi) = p$ 又は p^2 (ただし、 $p \in \mathbb{Z}$ は素数) である。

証明 (1)を示そう。 $\alpha, \beta \in R$ 、 $\alpha\beta = \pi$ とすると、 $N(\alpha)N(\beta) = N(\pi) = p$ なので、 $N(\alpha) = 1$ または $N(\beta) = 1$ である。故に $\alpha \in R^\times$ または $\beta \in R^\times$ から従う。

(2)を示そう。 $I = (\pi) \cap \mathbb{Z}$ は(0)でない $\mathbb{Z}$ のイデアルより、 $I = p\mathbb{Z}$ ($p \in \mathbb{Z}_{>0}$)と表せる。もし $p = 1$ ならば、 $1 \in I \subseteq (\pi)$ より $\pi \in R^\times$ となり、素元であることに反する。よって、 $p > 1$ である。また $a, b \in \mathbb{Z}$ に対して $p = ab$ とすると、 $ab \in I \subset (\pi)$ で (π) が素イデアルなので $a \in (\pi)$ または $b \in (\pi)$ が言える。したがって、 $I = p\mathbb{Z}$ が $\mathbb{Z}$ の素イデアル、つまり p は素数である。 $p \in I \subseteq (\pi)$ により $p = \pi\alpha$ ($\alpha \in R$)と書けば、 $p^2 = N(\pi)N(\alpha)$ 、 $N(\pi) > 1$ より $N(\pi) = p, p^2$ を得る。 証明終

定理 5.6 $d = 1, 2$ 、 $R = \mathbb{Z}[\sqrt{-d}]$ とする。

(1) $p \in \mathbb{Z}$ を素数とする。 p の R における分解は次のように与えられる。

- (a) $p \neq 2$ 、 $\left(\frac{-d}{p}\right) = 1$ ならば、ある R の素元 π が存在して $p = \pi\bar{\pi}$ を満たし、この π と $\bar{\pi}$ は同伴でない。
- (b) $p \neq 2$ 、 $\left(\frac{-d}{p}\right) = -1$ ならば、 p は R の素元である。
- (c) $p = 2$ のとき

$$\pi_0 = \begin{cases} 1 + \sqrt{-1} & (d = 1) \\ \sqrt{-2} & (d = 2) \end{cases}$$

とおくと、 π_0 は $\bar{\pi}_0$ と同伴な R の素元で $2 = \pi_0\bar{\pi}_0$ を満たす。

(2) π を R の素元とすると、次のうちいずれかが成立する。

- (a) π は $\left(\frac{-d}{p}\right) = 1$ を満たす奇素数 p の素因子である。
- (b) π は $\left(\frac{-d}{p}\right) = -1$ を満たす奇素数 p と同伴である。
- (c) π は上の(1)の(c)で定めた π_0 と同伴である。

証明 (1)(a)を示す。仮定より、ある $x \in \mathbb{Z}$ があり $x^2 \equiv -d \pmod{p}$ を満たす。 $\rho = x - \sqrt{-d} \in R$ とおく。 R はPIDなので R のイデアル (ρ, p) は単項であり、 $(\rho, p) = (\pi)$ ($\pi \in R$)と表せる。このとき、 $\pi\bar{\pi} = p$ となる。何故ならば、 $\pi \in (\rho, p)$ より $\pi = \alpha\rho + \beta p$ ($\alpha, \beta \in R$)と書いて、両辺ノルムをとって整理すると $N(\pi) = N(\alpha)N(\rho) + p\text{Tr}(\alpha\rho\bar{\beta}) + p^2N(\beta)$ となる。ここで $N(\rho) = x^2 + d \equiv 0 \pmod{p}$ なので、先の式から $p \mid N(\pi)$

を得る。故に $N(\pi) > 1$ により π は R の単元でない。もし $\rho \in (p)$ ならば、 $p \in \mathbb{Z}$ より $p \mid x$ 、 $p \mid -1$ となり矛盾するので $\rho \notin (p)$ である。したがって、 $(p) \subsetneq (\pi) \subsetneq (1)$ により $p = \alpha\pi$ ($\alpha \in R$ は単元でない) と表せる。ノルムをとれば $p^2 = N(\alpha)N(\pi)$ となり、 $N(\alpha), N(\pi) > 1$ であるので $p = N(\pi) = \pi\bar{\pi}$ となる。このとき、補題 5.5(1) より π は R の素元である。

もしこの π が $\bar{\pi}$ と同伴であったとする。 $\pi = a + b\sqrt{-d}$ ($a, b \in \mathbb{Z}$) と表して、ノルムをとると $p = N(\pi) = a^2 + b^2d$ により、 $d = 1, 2$ どちらのときでも $a \neq 0$ かつ $b \neq 0$ である。一方、 π と $\bar{\pi}$ は同伴であるので、 $\pi = \epsilon\bar{\pi}$ ($\epsilon \in R^\times$) とできて、補題 5.4(2) より $d = 1, 2$ のどちらのときでも $a = 0, b = 0$ または $a = \pm b$ となってしまう、矛盾が生じる。 $(\pi$ は素元なので、 $a = \pm b$ なら $a = \pm b = \pm 1$ となるが、 $d = 1$ のとき $p = 2$ となり矛盾する。) ゆえに π と $\bar{\pi}$ は同伴でない。

(1)(b) を示す。 p が R の素元でない、つまり $p = \pi\alpha$ ($\pi, \alpha \in R \setminus R^\times$) と書けたとする。このとき、 $p^2 = N(\pi)N(\alpha)$ 、 $N(\pi), N(\alpha) > 1$ なので、 $p = N(\pi)$ を得る。 $\pi = a + b\sqrt{-d}$ ($a, b \in \mathbb{Z}$) とすれば $p = a^2 + b^2d$ となる。ここでもし $p \mid b$ とすると、 $p \mid a$ で、先の式から両辺の素因数 p の個数が異なることより矛盾する。故に、 p と b は互いに素であるので、 $bx' + py = 1$ となる $x', y \in \mathbb{Z}$ がとれる。両辺に a かけて整理すると $b(ax') \equiv a \pmod{p}$ を得て、 $b^2(ax')^2 \equiv a^2 \equiv p - b^2d \equiv b^2(-d) \pmod{p}$ となる。従って b^2 と p が互いに素であることにより、 $(ax')^2 \equiv -d \pmod{p}$ なので、 $-d$ が p を法とする平方剰余となり仮定に反する。以上より p は R の素元である。

(1)(c) を示す。 $d = 1$ のとき、 $\pi_0\bar{\pi}_0 = (1 + \sqrt{-1})(1 - \sqrt{-1}) = 2$ 、 $\bar{\pi}_0 = -\sqrt{-1}\pi_0$ により成立する。 $d = 2$ のとき、 $\pi_0\bar{\pi}_0 = \sqrt{-2}(-\sqrt{-2}) = 2$ 、 $\bar{\pi}_0 = (-1)\pi_0$ により成立する。また、補題 5.5(2) より、 π_0 は R の素元である。

(2) を示そう。 π が R の素元とすると、 $\bar{\pi}$ も R の素元であり、補題 5.5(2) より $\pi\bar{\pi} = p$ 又は p^2 (p は素数) と表せる。どちらの場合でも $p \in (\pi)$ 、 $p \in (\bar{\pi})$ から π と $\bar{\pi}$ は p の素因子である。

$p = 2$ で、 π は 2 の素因子とする。素元分解の一意性が成立するので、 $(\pi) = (\pi_0)$ で π は (1)(c) で定めた π_0 と同伴となり (2)(c) を満たす。

$N(\pi) = p$ で $p \neq 2$ のとき、 $p = \pi\bar{\pi}$ により p は R の素元でない。故に (1)(b) の対偶により (2)(a) を満たす。

$N(\pi) = p^2$ で $p \neq 2$ のとき、 $\pi\bar{\pi} = p^2$ において素元分解の一意性より $\pi, \bar{\pi}$ は p と同伴であり、つまり p は R の素元である。故に (1)(a) の対偶より (2)(b) を満たす。

証明終

前章で示した平方剰余の相互法則を用いて、定理 5.6 は次のように述べることができる。

系 5.7 $p \in \mathbb{Z}$ を素数とする。

(1) $p \equiv 1 \pmod{4}$ ならば、 $p = a^2 + b^2$ となる $a, b \in \mathbb{Z}$ が存在する。

$p \equiv 3 \pmod{4}$ ならば、そのような整数 a, b は存在しない。

(2) $p \equiv 1, 3 \pmod{8}$ ならば、 $p = a^2 + 2b^2$ となる $a, b \in \mathbb{Z}$ が存在する。

$p \equiv 5, 7 \pmod{8}$ ならば、そのような整数 a, b は存在しない。

証明 (1) を示す。 $p \equiv 1 \pmod{4}$ とすると、 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$ であるから、定理 5.16(1)(a) より $p = \pi\bar{\pi}$ となる $\mathbb{Z}[\sqrt{-1}]$ の素元 π が存在する。
 $\pi = a + b\sqrt{-1}$ ($a, b \in \mathbb{Z}$) と表せば成立する。

また、整数 a, b が奇数、偶数どちらの場合であっても $a^2 + b^2 \equiv 3 \pmod{4}$ とはならない。

(2) を示す。平方剰余の相互法則を用いて、

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p^2-1}{8}}$$

により、

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & p \equiv 1, 3 \pmod{8} \\ -1 & p \equiv 5, 7 \pmod{8} \end{cases}$$

が言えるので (1) と同様にして成立する。

証明終

5.3 イデアル類群

以下、 $R = \mathbb{Z}[\sqrt{-d}]$ とおき、 d は square free で $d \equiv 1, 2 \pmod{4}$ とする。
 $\alpha_1, \dots, \alpha_n \in R$ に対して、 R の部分集合

$$[\alpha_1, \dots, \alpha_n] := \{\alpha_1 x_1 + \dots + \alpha_n x_n \mid x_1, \dots, x_n \in \mathbb{Z}\}$$

について考えよう。これは R のイデアルになるとは限らない。

命題 5.8 $a, b, c \in \mathbb{Z}$, $c \neq 0$ に対し、次は同値である。

(a) $[a, b + c\sqrt{-d}]$ は R のイデアルである。

(b) c は a, b を割り切り、 a は $\frac{b^2}{c} + cd$ を割り切る。

証明 (a) $\Rightarrow$ (b) を示す。 $[a, b+c\sqrt{-d}]$ を I と書く。 $a\sqrt{-d} \in I$ 、 $(b+c\sqrt{-d})\sqrt{-d} \in I$ であるので、

$$\begin{cases} a\sqrt{-d} = ax + (b+c\sqrt{-d})y \\ (b+c\sqrt{-d})\sqrt{-d} = az + (b+c\sqrt{-d})w \end{cases}$$

$(x, y, z, w \in \mathbb{Z})$ と書ける。第一式より $a = cy$ を得て、 c は a を割り切る。
第二式より

$$\begin{cases} -cd = az + bw \\ b = cw \end{cases}$$

を得て、 c は b を割り切る。また $-az = \frac{b^2}{c} + cd \in \mathbb{Z}$ なので a は $\frac{b^2}{c} + cd$ を割り切る。

(b) $\Rightarrow$ (a) を示す。任意の $\alpha, \beta \in I$ 、任意の $x \in R$ に対して $\alpha + \beta, \alpha x \in I$ を示したい。 $a\sqrt{-d}, (b+c\sqrt{-d})\sqrt{-d} \in I$ を示すことができれば十分である。

$$\begin{aligned} a\sqrt{-d} &= \frac{-b}{c}a + \frac{a}{c}(b+c\sqrt{-d}) \in I \\ (b+c\sqrt{-d})\sqrt{-d} &= -(\frac{b^2}{c} + cd) + \frac{b}{c}(b+c\sqrt{-d}) \in I \end{aligned}$$

により (a) が成立する。

証明終

命題 5.9 $(0) \neq I$ が R のイデアルならば、次を満たす整数の組 (a, b, c) が唯一つ存在する。

(a) $I = [a, b+c\sqrt{-d}] = (a, b+c\sqrt{-d})$

(b) $I \cap \mathbb{Z} = [a]$

(c) $c \mid a, b$ かつ $a \mid \frac{b^2}{c} + cd$

(d) $0 \leq b < a, 0 < c$

証明 $0 \neq \alpha \in I$ に対して $0 \neq N(\alpha) \in I \cap \mathbb{Z}$ なので、 $I \cap \mathbb{Z}$ は 0 でない $\mathbb{Z}$ のイデアルである。それは、ある正の整数 a により $[a]$ と表せる。 a は条件 (b) と (d) により唯一つ決まる。ここで、

$$J = \{y \in \mathbb{Z} \mid x + y\sqrt{-d} \in I \ (\exists x \in \mathbb{Z})\}$$

とおくと、 J は (0) でない $\mathbb{Z}$ のイデアルである。

なぜならば $a\sqrt{-d} \in I$ により J は (0) でない。 $y_1, y_2 \in I$ に対して、ある $x_i \in \mathbb{Z}$ ($i = 1, 2$) があり $x_i + y_i\sqrt{-d} \in I$ を満たす。 $(x_1 + x_2) + (y_1 + y_2)\sqrt{-d}, zx_1 + zy_1\sqrt{-d} \in I$ ($z \in \mathbb{Z}$) なので $y_1 + y_2, zy_1 \in J$ となり、よって J は $\mathbb{Z}$ のイデアルである。故に $J = [c]$ ($c \in \mathbb{Z}_{>0}$) と表せる。

$$b = \min\{x \in \mathbb{Z}_{>0} \mid x + c\sqrt{-d} \in I\}$$

と定める。もし、 $b > a$ とすると、 $0 < b - a < b$ であり、 $b - a + c\sqrt{-d} \in I$ なので b の最小性に矛盾する。故に (d) が成立する。また、 $a, b + c\sqrt{-d} \in I$ より $[a, b + c\sqrt{-d}] \subset (a, b + c\sqrt{-d}) \subset I$ が言える。 $\alpha \in I$ に対して、 $\alpha = x + y\sqrt{-d}$ ($x, y \in \mathbb{Z}$) と書くと、 $y \in J$ より $y = cq$ ($q \in \mathbb{Z}$) と表せ、 $x - qb = \alpha - q(b + c\sqrt{-d}) \in I \cap \mathbb{Z}$ となる。故に $x - qb = ar$ ($r \in \mathbb{Z}$) と書けば、 $\alpha = ar + q(b + c\sqrt{-d}) \in [a, b + c\sqrt{-d}]$ により (a) が成立する。さらに命題 5.8 より (c) が成立する。

一意性を示す。(a)~(d) をみたす異なる整数の組 (a', b', c') があったとすると、 $[a] = [a']$, $0 < a, a'$ より $a = a'$ が成立する。また、(a) より $b' + c'\sqrt{-d} \in I$ が言えて、 $c' \in J$ なので $[c'] \subset J$ である。逆に $y \in J$ に対して、 $x + y\sqrt{-d} \in I$ となる整数 x があり $x + y\sqrt{-d} \in [a', b' + c'\sqrt{-d}]$ より c' は y を割り切るので $y \in [c']$ である。故に $J \subset [c']$ より等号が成り立ち、 $c = c'$ を得る。また今示したことにより $b' + c\sqrt{-d} \in I$ が言えて、 b の最小性により $b \leq b'$ である。ここでもし $b < b'$ とすると、 $b' - b = b' + c\sqrt{-d} - (b + \sqrt{-d}) \in I$ により $b' - b \in I \cap \mathbb{Z}$ なので $b' - b = ak$ のようにある整数 k で表せる。一方 (d) より $0 < b' - b < a$ であるので、代入して $0 < ak < a$ で k が整数であることに矛盾する。従って $b = b'$ を得る。

証明終

命題 5.10 I, I' を R のイデアルとすると次が成立する。

- (1) $\bar{I} = \{\bar{\alpha} \mid \alpha \in I\}$ は R のイデアル。
- (2) $I\bar{I} = (n)$ を満たす $n \in \mathbb{Z}_{\geq 0}$ が唯一つ存在する。(この n を $N(I)$ と書き I のノルムという。)
- (3) $N(I)N(I') = N(II')$
- (4) $I = (\alpha)$ ($\alpha \in R$) のとき、 $N(I) = N(\alpha)$ である。また $I = (0)$ と $N(I) = 0$ は同値であり、同様に $I = (1)$ と $N(I) = 1$ も同値である。

証明 (1) を示す。 I は空でないから $\bar{I}$ も空でない。 $\bar{\alpha}, \bar{\beta} \in \bar{I}$ 、 $\xi \in R$ に対し、 $\alpha + \beta, \bar{\xi}\alpha \in I$ より $\bar{\alpha} + \bar{\beta}, \bar{\xi}\bar{\alpha} \in \bar{I}$ であるのでよい。

(2) を示す。 $I = (0)$ なら $n = 0$ でよい。

$I \neq (0)$ ならば、命題 5.9 より $I = (\alpha, \beta)$ ($\alpha, \beta \in R$) という形をしていて、 $I\bar{I} = (\alpha\bar{\alpha}, \alpha\bar{\beta}, \bar{\alpha}\beta, \beta\bar{\beta})$ である。 $a = N(\alpha)$, $b = \text{Tr}(\alpha\bar{\beta})$, $c = N(\beta)$ とおくと $[a, b, c]$ は $\mathbb{Z}$ のイデアルとなる。故にそれを $[n]$ (n は正の整数) と表すと、 $n \in I\bar{I}$ より $(n) \subset I\bar{I}$ が言える。一方、 $\gamma = \frac{\alpha\bar{\beta}}{n}$ とおくと、 $\text{Tr}(\gamma) = \gamma + \bar{\gamma} = b/n \in \mathbb{Z}$, $N(\gamma) = ac/n^2 \in \mathbb{Z}$ であるので、補題 5.4 より、 $\gamma \in R$ である。従って $I\bar{I} = (a, n\gamma, n\bar{\gamma}, c) \subset (n)$ となり、 $I\bar{I} = (n)$ が言えた。またもし別の正の整数 n' があつたとすると $(n) = (n')$, $0 < n, n'$ から $n = n'$ となり一意性が言えた。

(3) については $(N(I\bar{I}')) = I\bar{I}'\bar{I}' = I\bar{I}'\bar{I}' = (N(I))(N(I')) = (N(I)N(I'))$ よりよい。

(4) を示す。 $(N(I)) = I\bar{I} = (\alpha\bar{\alpha}) = (N(\alpha))$ より $N(I), N(\alpha) \geq 0$ であるので $N(I) = N(\alpha)$ を得る。また、 $I = (0)$ ならば $N(I) = N(0) = 0$ でよい。逆に $N(I) = 0$ とする。 $\alpha \in I$ とすると、 $\alpha\bar{\alpha} \in I\bar{I} = (0)$ より、 $\alpha\bar{\alpha} = 0$ なので $\alpha = 0$ となる。従って $I = (0)$ となる。 $I = (1)$ についても同様に同値性が言える。

証明終

命題 5.11 I を (0) でない R のイデアルとし、命題 5.9 より $I = [a, b + c\sqrt{-d}]$ と表す。このとき、 $N(I) = ac$ である。

証明 $c = 1$ とする。 $n = N(I)$, $x = \frac{b^2+d}{a}$ とおき、 $J = (a, b + \sqrt{-d}, b - \sqrt{-d}, x)$ とおく。このとき $(n) = I\bar{I} = (a^2, a(b + \sqrt{-d}), a(b - \sqrt{-d}), b^2 + d) = aJ$ であるので、 $J = (1)$ を示せばよい。 $m = n/a$ とすると、 $J = (m)$ であるが、 $b + \sqrt{-d} \in J = (m)$ より $b + \sqrt{-d} = m(y + z\sqrt{-d})$ と表せば、 $mz = 1$ を得る。故に m は R の単元なので $J = (1)$ となる。

一般の場合は、命題 5.9(c) より $a = ca'$, $b = cb'$ と書いて、 $N(I) = N((c)[a', b' + \sqrt{-d}]) = N(c)N([a', b' + \sqrt{-d}]) = c^2a' = ca$ により示される。

証明終

命題 5.12 I, J, I_1, I_2 は (0) でない R のイデアルとする。

(1) $I_1J = I_2J$ ならば、 $I_1 = I_2$ である。

(2) 次は同値である。

(a) $J \subset I$

(b) ある R のイデアル I' が存在して、 $II' = J$ を満たす。

証明 (1) を示す。 $J = (\alpha)$ ($0 \neq \alpha \in R$) のときは、 $\alpha I_1 = \alpha I_2$ であるので、 α^{-1} をかければよい。一般の場合については、両辺に $\bar{J}$ をかけて $(N(J))I_1 = (N(J))I_2$ なので、前に示したことから成立する。

(2) を示す。(b) ならば (a) は自明である。(a) を仮定する。すると、 $J\bar{I} \subset I\bar{I} = (N(I))$ なので、 $I' = \{\frac{\alpha}{N(I)} \mid \alpha \in J\bar{I}\}$ とおくと、これは R のイデアルである。このとき $I\bar{I}I' = (N(I))I' = J\bar{I}$ であるので、(1) により $II' = J$ が成立する。 証明終

定義 5.13 $d \in \mathbb{Z}_{>0}$ は square free で $d \equiv 1, 2 \pmod{4}$ 、 $R = \mathbb{Z}[\sqrt{-d}]$ とする。このとき、

$$F(R) = \{I \mid 0 \neq I \text{ は } R \text{ のイデアル}\}$$

と定める。

また $I, I' \in F(R)$ に対して、関係 $\sim$ を

$$I \sim I' \iff \alpha I = \alpha' I' \text{ となる } 0 \text{ でない } \alpha, \alpha' \in R \text{ が存在する。}$$

と定める。

補題 5.14 (1) $I \in F(R)$ に対して、

$$I \sim (1) \iff I \text{ は単項イデアル}$$

が成立する。

(2) 任意の $I \in F(R)$ に対して、 $I\bar{I} \sim (1)$ である。

(3) 関係 $\sim$ は $F(R)$ において同値関係である。

(4) $I, I', J, J' \in F(R)$ について、 $I \sim I'$ 、 $J \sim J'$ ならば $IJ \sim I'J'$ が成立する。

(5) $I, J \in F(R)$ に対して、

$$I \sim J \iff I \text{ と } J \text{ は } R\text{-加群として同型}$$

が成立する。

証明 (1) について、 $(\Rightarrow)$ を示す。0 でない $\alpha, \alpha' \in R$ があって、 $\alpha I = \alpha'(1) = (\alpha')$ を満たす。 $\alpha' \in \alpha I$ より、ある $\beta \in I$ があって $\alpha' = \alpha\beta$ と表せる。このとき、 $\alpha I = \alpha(\beta)$ となる。よって、 $I = (\beta)$ である。

$(\Leftarrow)$ は $I = (\alpha)$ と表したとき、 $1 \cdot I = \alpha \cdot (1)$ により $I \sim (1)$ である。

(2) は命題 5.10(2) より成り立つ。

(3) を示す。 $I, J, K \in F(R)$ とする。 $I \sim I$ はよい。 $I \sim J$ ならば $J \sim I$ もよい。 $I \sim J$ かつ $J \sim K$ ならば、0 でない $\alpha, \alpha', \beta, \beta' \in R$ があって、 $\alpha I = \alpha' J$ 、 $\beta J = \beta' K$ と書ける。よって $\alpha\beta I = \alpha'\beta J = \alpha'\beta' K$ であるので、 $I \sim K$ が成立する。以上から、関係 $\sim$ は $F(R)$ 上の同値関係である。

(4) を示す。仮定より $\alpha I = \alpha' I'$ 、 $\beta J = \beta' J'$ と書いて、 $\alpha\beta IJ = \alpha'\beta' I'J'$ により $IJ \sim I'J'$ を得る。

(5) について、 $(\Rightarrow)$ を示す。ある 0 でない $\alpha, \beta \in R$ が存在して、 $\alpha I = \beta J$ を満たす。ここで、 R -加群準同型 $\phi: I \rightarrow \alpha I$ を $\phi(x) = \alpha x$ ($x \in I$) と定める。このとき、 ϕ は同型である。何故ならば、全射であることは明らかである。 $\phi(x) = 0$ とすると、 $\alpha x = 0$ であり、 R が整域なので、 $x = 0$ である。故に ϕ は単射である。同様に $\psi: J \rightarrow \beta J$ も同型なので、 I と J は R -加群として同型である。

$(\Leftarrow)$ を示す。 $\phi: I \rightarrow J$ を R -加群の同型写像とする。0 $\neq \beta \in I$ をとる。また $\phi(\beta) = \alpha$ とする。このとき任意の $x \in I$ に対して、 $\beta\phi(x) = \phi(\beta x) = x\alpha$ により、 $\phi(x) = \alpha\beta^{-1}x$ が成立する。故に $J = \alpha\beta^{-1}I$ より、 $\alpha I = \beta J$ であることが分かった。

証明終

定義 5.15 $I \in F(R)$ に対して、

$$[I] = \{J \in F(R) \mid J \sim I\}$$

と定める。さらに、

$$\text{Cl}(R) = \{[I] \mid I \in F(R)\}$$

と定め、これを R のイデアル類群と言う。 $\text{Cl}(R)$ における演算を

$$[I] \cdot [J] = [IJ]$$

と定めると、補題 5.14(4) から、これは well-defined な演算である。従って $[(1)]$ を単位元とし、補題 5.14(2) より $[I]$ の逆元を $[\bar{I}]$ として、アーベル群になる。

$\text{Cl}(R)$ の位数を R の類数といい、 $h(R)$ で表す。

定理 5.16 任意の $\mathcal{C} \in \text{Cl}(R)$ に対して、

$$\begin{cases} 0 < a < 2\sqrt{d/3} \\ -a/2 < b \leq a/2 \\ (a, b + \sqrt{-d}) \in \mathcal{C} \end{cases}$$

を満たす整数の組 (a, b) が存在する。

証明 $\mathcal{C} = [I]$ と表し、 $N(I)$ が最小となるように、0 でない R のイデアル I をとる。命題 5.9 より整数の組 (a, b, c) により $I = [a, b + c\sqrt{-d}]$ と表せる。この時、 $c = 1$ である。なぜならば、命題 5.9 より c は a と b を割り切れる。 $I_1 = (a/c, b/c + \sqrt{-d})$ とおく。 $I = cI_1$ より $I \sim I_1$ なので $\mathcal{C} = [I] = [I_1]$ である。一方、 $N(I) = c^2 N(I_1) \geq N(I_1)$ なので、 $c = 1$ である。また命題 5.9 より $0 < b \leq a$ を満たして、 $b > a/2$ のとき b を $b - a$ に置き換えることにより、 $-a/2 < b \leq a/2$ としてよい。この不等式から $a^2/4 \geq b^2$ を得る。また命題 5.11 より $N(I) = a$ である。さらに $(b + \sqrt{-d}) \in I$ なので、命題 5.12(2) より、 $IJ = (b + \sqrt{-d})$ となる 0 でない R のイデアル J が存在する。両辺のノルムをとると、 $aN(J) = N(I)N(J) = N(b + \sqrt{-d}) = b^2 + d$ である。さらに IJ は単項なので $[I][J] = [IJ] = [(1)]$ である。故に $\mathcal{C} = [I] = [\bar{J}]$ であって $N(I)$ の最小性により $N(J) = N(\bar{J}) \geq N(I) = a$ を得る。以上より $a^2/4 + d \geq b^2 + d = aN(J) \geq a^2$ であるので、 $0 < a \leq 2\sqrt{d/3}$ を満たす。今 $d \equiv 1, 2 \pmod{4}$ から $\sqrt{d/3}$ は整数でない。もしも $\sqrt{d/3}$ が有理数だとすると、互いに素な 0 でない自然数 p, q により $\sqrt{d/3} = p/q$ と表せて、 $dq^2 = 3p^2$ を得る。このとき $p^2 \mid d$ である。 $p = 1$ のとき、 $d = 3$, $q = 1$ となるが、これは $d \equiv 1, 2 \pmod{4}$ に反する。よって $p > 1$ である。これは d が square free であることに反するので、 $\sqrt{d/3}$ は有理数ではない。従って、 $0 < a < 2\sqrt{d/3}$ である。 証明終

系 5.17 $\text{Cl}(R)$ は有限 Abel 群である。

証明 集合 $X = \{(a, b) \in \mathbb{Z}^2 \mid 0 < a < 2\sqrt{d/3}, -a/2 < b \leq a/2\}$ の元の個数は $4d/3$ 未満なので、 $|\text{Cl}(R)| < |X| < 4d/3$ により $\text{Cl}(R)$ は有限である。 証明終

命題 5.18 (1) 次は同値である。

(a) $h(R) = 1$ である。

(b) $\text{Cl}(R)$ は単位元のみからなる群である。

(c) R は単項イデアル整域である。

(d) R は一意分解整域である。

(2) すべてのイデアル I に対して、 $I^{h(R)}$ は単項イデアルである。

証明 (1) を示す。 (a) $\Leftrightarrow$ (b) は明らかである。

(b) $\Rightarrow$ (c) を示す。 I を 0 でない R のイデアルとすると、 $[I] \in \text{Cl}(R)$ なので、仮定より $[I] = [(1)]$ である。故に $I \sim (1)$ なので、補題 5.14(1) より I は単項イデアルである。

(c) $\Rightarrow$ (b) を示す。 $C \in \text{Cl}(R)$ に対して、仮定より単項イデアル I により $C = [I]$ と表すことができる。補題 5.14(1) より $I \sim (1)$ なので $[I] = [(1)]$ である。よって (b) が成り立つ。

一般に (c) $\Rightarrow$ (d) は成立しているので、(d) $\Rightarrow$ (c) を示す。定理 6.36 より、 R は Dedekind 整域である。故に定理 6.34 より、0 でないイデアル I は有限個の極大イデアル $\mathfrak{m}_i$ ($1 \leq i \leq n$) により、 $I = \prod_{i=1}^n \mathfrak{m}_i$ と表せる。よって R の極大イデアル $\mathfrak{m}$ が単項イデアルであることを示せば十分である。 $0 \neq x \in \mathfrak{m}$ に対して、 x は単元でないので、 $x = \prod_{i=1}^l \pi_i$ (π_i は素元) と書ける。このとき $\prod_{i=1}^l \pi_i \in \mathfrak{m}$ なので、ある i があって $\pi_i \in \mathfrak{m}$ を満たす。故に $(0) \neq (\pi_i) \subseteq \mathfrak{m}$ だが、 R の次元は 1 なので $\mathfrak{m} = (\pi_i)$ である。従って R は単項イデアル整域である。

(2) については、Cauchy-Lagrange の定理より $[(1)] = [I]^{h(R)} = [I^{h(R)}]$ なので、補題 5.14 により $I^{h(R)}$ は単項イデアルである。 証明終

6 付録

単位元 1 をもつ可換環 A を単に環と呼ぶことにする。

6.1 準素イデアル分解

定義 6.1 (1) イデアル $\mathfrak{q}$ が環 A の準素イデアルとは、 $\mathfrak{q} \neq A$ であり「 $xy \in \mathfrak{q}$ ならば、 $x \in \mathfrak{q}$ またはある $n > 0$ があって $y^n \in \mathfrak{q}$ 」を満たすときを言う。また素イデアル $\mathfrak{p}$ について $\mathfrak{p} = \sqrt{\mathfrak{q}}$ を満たすとき $\mathfrak{q}$ を $\mathfrak{p}$ -準素イデアルと言う。

(2) A のイデアル $\mathfrak{a}$ について、準素イデアル $\mathfrak{q}_i$ により $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ と表せたとき、 $\mathfrak{a}$ を準素分解可能なイデアルといい、これを $\mathfrak{a}$ の準素分解という。さらに、この分解が、

(a) $\sqrt{\mathfrak{q}_i} \ (i = 1, \dots, n)$ のどの二つも異なっている。

(b) $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$

を満たすとき、無駄のない準素分解という。

補題 6.2 $\mathfrak{q}$ を $\mathfrak{p}$ -準素イデアルとし、 $x \in A$ とする。

(1) $x \in \mathfrak{q}$ ならば $(\mathfrak{q} : x) = (1)$ である。

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

(3) $x \notin \mathfrak{p}$ ならば $(\mathfrak{q} : x) = \mathfrak{q}$ である。

証明 (1) について。 $1 \cdot x \in \mathfrak{q}$ より、 $1 \in (\mathfrak{q} : x)$ となる。

(2) について。もし $1 \in (\mathfrak{q} : x)$ なら $x = x \cdot 1 \in \mathfrak{q}$ より矛盾するので $(\mathfrak{q} : x) \neq (1)$ である。また $y \in (\mathfrak{q} : x)$ ならば $xy \in \mathfrak{q}$ であるが、仮定より $y \in \mathfrak{p}$ なので $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$ が成り立つ。根基をとると $\mathfrak{p} = \sqrt{\mathfrak{q}} \subseteq \sqrt{(\mathfrak{q} : x)} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$ なので $\mathfrak{p} = \sqrt{(\mathfrak{q} : x)}$ である。ここで $z, w \in A$ について $zw \in (\mathfrak{q} : x)$ 、 $w \notin \mathfrak{p}$ とすると $xzw \in \mathfrak{q}$ で、仮定より $xz \in \mathfrak{q}$ となり $z \in (\mathfrak{q} : x)$ である。以上から $(\mathfrak{q} : x)$ は $\mathfrak{p}$ -準素イデアルである。

(3) について。 $\supseteq$ は明らかである。 $y \in (\mathfrak{q} : x)$ をとる。 $xy \in \mathfrak{q}$ で、仮定により $y \in \mathfrak{q}$ となるので $\subseteq$ が成立する。 証明終

定理 6.3 $\mathfrak{a}$ を A の準素分解可能なイデアル、 $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ を無駄のない準素分解とし、 $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \ (i = 1, \dots, n)$ とする。このとき、

$$\{\mathfrak{p}_i \mid 0 \leq i \leq n\} = \{\sqrt{(\mathfrak{a} : x)} \in \text{Spec}(A) \mid x \in A\}$$

である。すなわち、 $\{\mathfrak{p}_i \mid 0 \leq i \leq n\}$ は分解の仕方によらず、 $\mathfrak{a}$ のみにより定まる。

証明 任意の $x \in A$ に対して $(\mathfrak{a} : x) = (\bigcap_{i=1}^n \mathfrak{q}_i : x) = \bigcap_{i=1}^n (\mathfrak{q}_i : x)$ なので補題 6.2(1)(2) を用いて $\sqrt{(\mathfrak{a} : x)} = \bigcap_{i=1}^n \sqrt{(\mathfrak{q}_i : x)} = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$ となる。 $\sqrt{(\mathfrak{a} : x)}$ を素イデアルとすると、ある j があって $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}_j$ を満たす。よって $\supseteq$ は示せた。

一方、無駄のない準素分解ということより、任意の i に対して $x_i \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$ がとれる。故に $\sqrt{(\mathfrak{a} : x_i)} = \sqrt{(\bigcap \mathfrak{q}_i : x_i)} = \sqrt{(\mathfrak{q}_i : x_i)} = \mathfrak{p}_i$ により、 $\subseteq$ が示せた。 証明終

定義 6.4 (1) 定理 6.3 の $\mathfrak{p}_i$ ($i = 1, \dots, n$) を $\mathfrak{a}$ に属する素イデアルという。

(2) $\{\mathfrak{p}_i \mid 0 \leq i \leq n\}$ の極小元を $\mathfrak{a}$ に属する極小素イデアルという。

命題 6.5 S を A の積閉集合とし $\mathfrak{q}$ を $\mathfrak{p}$ -準素イデアルとする。

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

(2) $S \cap \mathfrak{p} = \emptyset$ とする。このとき、 $S^{-1}\mathfrak{q}$ は $S^{-1}\mathfrak{p}$ -準素イデアルであり、 $S^{-1}\mathfrak{q} \cap A = \mathfrak{q}$ を満たす。さらに $\{\mathfrak{q}$ は $\mathfrak{p}$ -準素イデアル $\}$ と $\{\mathfrak{Q}$ は $S^{-1}\mathfrak{p}$ -準素イデアル $\}$ は自然な写像 $A \rightarrow S^{-1}A$ におけるそれぞれのイデアルの制限と拡大により、一対一対応にある。

証明 (1) について。 $s \in S \cap \mathfrak{p}$ とする。 $s \in \sqrt{\mathfrak{q}}$ であるので、ある正の整数 n が存在して $s^n \in \mathfrak{q}$ を満たす。よって $s^n/1 \in S^{-1}\mathfrak{q}$ に注意して、 $1/1 = (s^n/1)(1/s^n) \in S^{-1}\mathfrak{q}$ なので $S^{-1}A = S^{-1}\mathfrak{q}$ となる。

(2) について。まず $S^{-1}\mathfrak{q} \cap A = \mathfrak{q}$ を示す。 $\mathfrak{q} \subseteq S^{-1}\mathfrak{q} \cap A$ はよい。 $x \in S^{-1}\mathfrak{q} \cap A$ をとる。 $x/1 \in S^{-1}\mathfrak{q}$ より $x/1 = q/s$ ($q \in \mathfrak{q}, s \in S$) と表せる。さらにある $t \in S$ があって $stx = qt$ を満たすので、 $stx \in \mathfrak{q}$ を得る。 $x \in \mathfrak{q}$ または $st \in \mathfrak{p}$ だが、 $S \cap \mathfrak{p} = \emptyset$ であるので $x \in \mathfrak{q}$ である。よって $S^{-1}\mathfrak{q} \cap A \subseteq \mathfrak{q}$ が言えたから等号は示せた。

次に $S^{-1}\mathfrak{q}$ は $S^{-1}\mathfrak{p}$ -準素イデアルを示す。 $S^{-1}\mathfrak{q} \cap A = \mathfrak{q}$ より、 $S^{-1}\mathfrak{q} \neq S^{-1}A$ である。また $x/s, y/t \in S^{-1}A$ に対し $(x/s)(y/t) \in S^{-1}\mathfrak{q}$ とすると、ある $u, v \in S$ と $q \in \mathfrak{q}$ により $xyuv = qstv$ を得る。これは $\mathfrak{q}$ の元であり、 $uv \in S$ なので $uv \notin \mathfrak{p}$ となり、 $xy \in \mathfrak{q}$ である。従って $x/s \in S^{-1}\mathfrak{q}$ または $y/t \in S^{-1}\mathfrak{p}$ なので、 $S^{-1}\mathfrak{q}$ は準素イデアルである。また $\sqrt{S^{-1}\mathfrak{q}} = S^{-1}\sqrt{\mathfrak{q}} = S^{-1}\mathfrak{p}$ であるので、 $S^{-1}\mathfrak{q}$ は $S^{-1}\mathfrak{p}$ -準素イデアルである。

局所化による素イデアルの一対一対応

$$\{\mathfrak{p} \in \text{Spec}(A) \mid S \cap \mathfrak{p} = \emptyset\} \leftrightarrow \text{Spec}(S^{-1}A)$$

と同様にして、準素イデアルの一対一対応

$$\{\mathfrak{q} \text{ は } \mathfrak{p}\text{-準素イデアル}\} \leftrightarrow \{\mathfrak{Q} \text{ は } S^{-1}\mathfrak{p}\text{-準素イデアル}\}$$

があることがわかる。

証明終

命題 6.6 S を A の積閉集合、 $\mathfrak{a}$ を A の準素分解可能なイデアル、 $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ を無駄のない準素分解とし、 $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ ($i = 1, \dots, n$) とする。 $\mathfrak{p}_i$ について、 $S \cap \mathfrak{p}_i = \emptyset$ ($0 \leq i \leq m$)、 $S \cap \mathfrak{p}_i \neq \emptyset$ ($m+1 \leq i \leq n$) を満たすならば、

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^m S^{-1}\mathfrak{q}_i, \quad A \cap S^{-1}\mathfrak{a} = \bigcap_{i=1}^m \mathfrak{q}_i$$

であり、これらは無駄のない準素分解となっている。

証明 $S^{-1}\mathfrak{a} = S^{-1}(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap_{i=1}^n S^{-1}\mathfrak{q}_i$ であり、仮定と命題 6.5 から $S^{-1}\mathfrak{a} = \bigcap_{i=1}^m S^{-1}\mathfrak{q}_i$ となる。 $1 \leq i \leq m$ について、 $S^{-1}\mathfrak{q}_i$ は $S^{-1}\mathfrak{p}_i$ -準素イデアルである。 $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ は互いに異なるので、 $S^{-1}\mathfrak{p}_i$ ($i = 1, \dots, m$) も互いに異なっている。

また $A \cap S^{-1}\mathfrak{a} = A \cap (\bigcap_{i=1}^m S^{-1}\mathfrak{q}_i) = \bigcap_{i=1}^m (A \cap S^{-1}\mathfrak{q}_i) = \bigcap_{i=1}^m \mathfrak{q}_i$ である。 $\mathfrak{q}_1, \dots, \mathfrak{q}_m$ の根基は互いに異なり、 $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ は無駄のない準素分解なので、 $A \cap S^{-1}\mathfrak{a} = \bigcap_{i=1}^m \mathfrak{q}_i$ も無駄のない準素分解である。このことから、 $S^{-1}\mathfrak{a} = \bigcap_{i=1}^m S^{-1}\mathfrak{q}_i$ も無駄のない準素分解である。 証明終

定理 6.7 $\mathfrak{a}$ を A の準素分解可能なイデアル、 $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ を無駄のない準素分解とし、 $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ ($i = 1, \dots, n$) とする。 $\mathfrak{p}$ を $\mathfrak{a}$ に属する極小素イデアルとする。このとき、 $\mathfrak{p}$ -準素イデアル $\mathfrak{q}$ は分解の仕方によらず、 $\mathfrak{a}$ により定まる。

証明 $S = A \setminus \mathfrak{p}$ とおくと $S \cap \mathfrak{p} = \emptyset$ である。 $\mathfrak{a}$ に属する素イデアル $\mathfrak{p}'$ について、 $\mathfrak{p}' \neq \mathfrak{p}$ であれば $S \cap \mathfrak{p}' \neq \emptyset$ となる。故に命題 6.6 により $A \cap S^{-1}\mathfrak{a} = \mathfrak{q}$ を得る。 S は $\mathfrak{p}$ により定まるので、 $\mathfrak{q}$ は $\mathfrak{a}$ により定まる。 証明終

定義 6.8 $\mathfrak{a}$ は環 A のイデアルとする。 $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ (ただし、 $\mathfrak{b}, \mathfrak{c}$ は A のイデアルで $\mathfrak{a} \neq \mathfrak{b}$ かつ $\mathfrak{a} \neq \mathfrak{c}$) と書けるときの、イデアル $\mathfrak{a}$ は可約という。可約でないとき、既約という。

命題 6.9 A を Noether 環とする。

- (1) A のイデアルは、有限個の既約イデアルの共通部分になる。
 - (2) A の既約イデアルは準素イデアルである。
- (1), (2) より Noether 環のイデアルは、準素分解可能なイデアルと分かる。

証明 (1) について、もしそうでないと仮定する。

$\Sigma = \{\mathfrak{a} \mid \mathfrak{a} \text{ は有限個の既約イデアルの共通部分で表せない } A \text{ のイデアル} \}$

とおくと、これは空でない。 A は Noether 環なので、極大条件よりある Σ の極大元 $\mathfrak{a}$ が存在し、それは既約ではない。故にイデアル $\mathfrak{b}, \mathfrak{c} \supsetneq \mathfrak{a}$ により $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ と表せる。 $\mathfrak{a}$ の極大性から $\mathfrak{b}, \mathfrak{c} \notin \Sigma$ なので、それぞれ有限個の既約イデアルの共通部分で表せる。このとき $\mathfrak{a}$ もそうになってしまい、 $\mathfrak{a} \in \Sigma$ に反する。故に (1) は成立する。

(2) について。剰余環を通して、 (0) が既約イデアルならば、準素イデアルであることを示せばよい。 $xy \in (0)$ かつ $y \notin (0)$ とする。

$$\text{Ann}(x) \subseteq \text{Ann}(x^2) \subseteq \cdots$$

を考える。Noether 環の昇鎖条件より、ある正の整数 n があって

$$\text{Ann}(x^n) = \text{Ann}(x^{n+1}) = \cdots$$

を満たす。このとき $(x^n) \cap (y) = (0)$ である。なぜならば $a \in (x^n) \cap (y)$ をとると、 $a = bx^n = cy$ ($b, c \in A$) と表せる。 $bx^{n+1} = cxy = 0$ より $b \in \text{Ann}(x^{n+1}) = \text{Ann}(x^n)$ である。よって $bx^n = 0$ より $a = 0$ を得る。故に $(x^n) \cap (y) = (0)$ である。今、 (0) は既約イデアルなので、 $(x^n) = (0)$ または $(y) = (0)$ である。従って $x^n = 0$ であり、 (0) が準素イデアルであると示された。 証明終

6.2 整拡大

補題 6.10 M を有限生成 A -加群、 $\mathfrak{a}$ を A のイデアル、 ϕ を M の A -加群自己準同形で $\phi(M) \subseteq \mathfrak{a}M$ を満たすものとする。このときある $a_1, \dots, a_n \in \mathfrak{a}$ が存在して、 A -加群自己準同形として、

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

を満たす。

証明 $a \in A$ に対して、 $\lambda_a : M \rightarrow M$ は a 倍写像とする。 $a \mapsto \lambda_a$ によって、環準同型 $A \rightarrow \text{End}_A(M)$ が定まる。 $A \rightarrow A[t]$ を自然な準同型として、代入の原理より $\Phi(t) = \phi$ を満たす環準同型 $\Phi : A[t] \rightarrow \text{End}_A(M)$ が一意

的に存在する。これにより $f \in A[t]$ 、 $m \in M$ に対して、 $f \cdot m = \Phi(f)(m)$ と定めることにより、 M を $A[t]$ -加群と見なすことができる。

$x_1, \dots, x_n$ を M の生成元とする。仮定により各 $\phi(x_i) \in \mathfrak{a}M$ なので、

$$\phi(x_i) = \sum_{j=1}^n a_{ij}x_j \quad (a_{ij} \in \mathfrak{a})$$

と表せる。故に

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

を得る。 n 次正方行列 $(\delta_{ij}t - a_{ij})$ を P 、 $x = {}^t(x_1, \dots, x_n)$ とおくと、 $Px = 0$ となり、両辺の左から余因子行列 $P^{(c)}$ をかけて、 $(\det P)I_n x = 0$ (I_n は n 次単位行列) となる。よって各 i について $\det P \cdot x_i = 0$ を得る。故に任意の $m \in M$ に対して、 $\Phi(\det(P))(m) = 0$ である。また行列式を展開して

$$\det(P) = t^n + a_1 t^{n-1} + \dots + a_n = 0 \quad (a_i \in \mathfrak{a})$$

と表せば、 $\text{End}_A(M)$ において、

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

を満たす。

証明終

定義 6.11 B を環、 A をその部分環とし $\mathfrak{a}$ を A のイデアルとする。

- (1) $b \in B$ が A 上整とは、ある A 係数のモニック多項式が存在し、 b がその多項式の根になるときを言う。
- (2) $C = \{b \in B \mid b \text{ は } A \text{ 上整}\}$ と定める。これを B における A の整閉包と言う。
- (3) C を B における A の整閉包とする。 $A = C$ のとき A は B で整閉といい、 $C = B$ のとき B は A 上整（または、 B は A の整拡大）という。
- (4) A が整域であり、 A が商体内で整閉であるとき、単に A は整閉という。

命題 6.12 B を環、 A をその部分環とし、 $b \in B$ とする。このとき、次は同値である。

- (1) b は A 上整である。
- (2) B の部分環 $A[b]$ は、有限生成 A -加群である。
- (3) B の部分環 C で、 $A[b] \subseteq C$ であり C は A -加群として有限生成であるものが存在する。
- (4) 忠実な $A[b]$ -加群 M で、 A -加群として有限生成なものが存在する。

証明 (1) $\Rightarrow$ (2) を示す。仮定により、

$$b^n + a_1b^{n-1} + \cdots + a_n = 0$$

を満たす $a_1, \dots, a_n \in A$ がある。これより任意の $r \geq 0$ に対して b^{n+r} は $1, b, \dots, b^{n-1}$ で表せるので、 $A[b] = \sum_{i=1}^{n-1} Ab_i$ が示され、(2) が成立する。

(2) $\Rightarrow$ (3) については、 $C = A[b]$ とおけばよい。

(3) $\Rightarrow$ (4) を示す。 $M = C$ とおけば、 M は $A[b]$ -加群であり、 A -加群として有限生成である。また $f \in \text{Ann}_{A[b]}(M)$ をとると、 $fM = 0$ だが、 $1_B \in M$ であることより、 $f = f \cdot 1_B = 0$ となる。従って M は忠実な $A[b]$ -加群である。

(4) $\Rightarrow$ (1) を示す。 $b \in B$ に対して、(4) を満たす M が存在すると仮定する。ここで A -加群準同型 $\phi: M \rightarrow M$ を $\phi(m) = bm$ と定めると、 M が $A[b]$ -加群であることに注意して、 $\phi(M) = bM \subseteq M \subseteq AM$ が言えるので、補題 6.10 により、ある $a_1, \dots, a_n \in A$ が存在して、

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

を満たしている。つまり、

$$(b^n + a_1b^{n-1} + \cdots + a_n)m = 0$$

が言えて、 M は忠実な $A[b]$ -加群だから、

$$b^n + a_1b^{n-1} + \cdots + a_n = 0$$

を得る。従って (1) が成り立つ。

証明終

系 6.13 $b_1, \dots, b_n \in B$ を A 上整とする。このとき、 B の部分環 $A[b_1, \dots, b_n]$ は有限生成 A -加群である。

証明 n についての帰納法により示す。 $n = 1$ のときは命題 6.12(1) $\Rightarrow$ (2) で既に証明した。 $n > 1$ として、 $n - 1$ まで成立すると仮定する。 $A_r = A[b_1, \dots, b_r]$ ($r = 1, \dots, n$) とおくと、帰納法の仮定により A_{n-1} は有限生成 A -加群である。また $b_n \in B$ は A_{n-1} 上整であることより、再び命題 6.12(1) $\Rightarrow$ (2) により $A_{n-1}[b_n] = A[b_1, \dots, b_n]$ は有限生成 A_{n-1} -加群であることがわかる。故に $A[b_1, \dots, b_n]$ は有限生成 A -加群となり、 n のときも成立する。 証明終

系 6.14 $A \subseteq B$ は環の拡大とし、 C は B における A の整閉包とする。このとき C は B の部分環である。

証明 $c, c' \in C$ に対して、系 6.13 より $A[c, c']$ は有限生成 A -加群である。また $A[c \pm c'], A[cc'] \subseteq A[c, c']$ であるので、命題 6.12(3) により $c \pm c', cc' \in C$ である。故に、 C は B の部分環である。 証明終

系 6.15 $A \subseteq B \subseteq C$ を環とし、 B を A 上整、 C を B 上整とする。このとき C は A 上整である。

証明 $c \in C$ とおくと、 c は B 上整なので、

$$c^n + b_1 c^{n-1} + \dots + b_n = 0$$

を満たす $b_1, \dots, b_n$ が存在する。 $B' = A[b_1, \dots, b_n]$ とおくと、系 6.13 より B' は有限生成 A -加群である。 c は B' 上整でもあるので、 $B'[c]$ は有限生成 B' -加群である。故に $B'[c]$ は A 加群として有限生成であることより、命題 6.12(3) により c は A 上整である。 証明終

系 6.16 $A \subseteq B$ を環の拡大とし、 C を B における A の整閉包とする。このとき、 C は B で整閉である。

証明 $b \in B$ を C 上整とする。系 6.14 により C は B の部分環で、系 6.15 により b は A 上整である。故に $b \in C$ より、 C は B で整閉である。 証明終

命題 6.17 $A \subseteq B$ を環の整拡大とする。

- (1) $\mathfrak{b}$ を B のイデアル、 $\mathfrak{a} = A \cap \mathfrak{b}$ とすると、 $B/\mathfrak{b}$ は $A/\mathfrak{a}$ 上整である。
- (2) S を A の積閉集合とすると、 $S^{-1}B$ は $S^{-1}A$ 上整である。

証明 (1) を示す。 $\beta \in B/\mathfrak{b}$ に対して $\beta = \bar{b}$ ($b \in B$) と表すと、 B は A 上整より、

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

($a_i \in A$) と書ける。 $\bar{a}_i \in A/\mathfrak{a}$ であることに注意して、

$$\bar{b}^n + \bar{a}_1 \bar{b}^{n-1} + \cdots + \bar{a}_n = \bar{0}$$

を得る。よって $B/\mathfrak{b}$ は $A/\mathfrak{a}$ 上整である。

(2) を示す。 $b/s \in S^{-1}B$ ($b \in B, s \in S$) に対して、 B は A 上整であるので、

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

($a_i \in A$) と書ける。故に

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

により、 $S^{-1}B$ は $S^{-1}A$ 上整である。

証明終

命題 6.18 $A \subseteq B$ を整域の整拡大とする。このとき、

$$B \text{ が体} \iff A \text{ が体}$$

が成立する。

証明 ($\Leftarrow$) を示す。 $0 \neq b \in B$ に対して、 B は A 上整なので、

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0 \quad (a_i \in A)$$

の形に表せる。この n を最小にとると、 $a_n \neq 0$ である。(もしそうでないとすると、

$$b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) = 0$$

とできて、 B は整域なので、

$$b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1} = 0$$

を得る。これは、 n の最小性に矛盾する。) $a_n \neq 0$ であり、 A は体なので、

$$b(-a_n^{-1}b^{n-1} - a_1 a_n^{-1}b^{n-2} - \cdots - a_{n-1} a_n^{-1}) = 1$$

となり、 B は体となる。

($\Rightarrow$)を示す。 $0 \neq a \in A$ に対して、 B は体なので $a^{-1} \in B$ であり、 a^{-1} は A 上整である。よって、

$$a^{-m} + a'_1 a^{-m-1} + \cdots + a'_m = 0 \quad (a'_i \in A)$$

と書ける。故に

$$a^{-1} = a^{m-1} a^{-m} = -(a'_1 + \cdots + a'_m a^{m-1}) \in A$$

により、 A は体となる。

証明終

系 6.19 $A \subseteq B$ を環の整拡大とし、 $\mathfrak{q}$ を B の素イデアル、 $\mathfrak{p} = A \cap \mathfrak{q}$ とする。このとき、

$$\mathfrak{q} \text{ が極大イデアル} \iff \mathfrak{p} \text{ が極大イデアル}$$

が成立する。

証明 $\mathfrak{q}$ が B の素イデアルであるので、 $B/\mathfrak{q}$ は整域で、命題 6.17(1) より $A/\mathfrak{p} \subseteq B/\mathfrak{q}$ は整域の整拡大となる。一般に環 R と、そのイデアル $\mathfrak{m}$ に対して、 $\mathfrak{m}$ が極大イデアルであることと $R/\mathfrak{m}$ が体であることは同値なので、命題 6.18 と合わせてこの系は成立する。

証明終

系 6.20 $A \subseteq B$ を環の整拡大とし、 B の素イデアル $\mathfrak{q}, \mathfrak{q}'$ は $\mathfrak{q} \subseteq \mathfrak{q}'$ かつ $A \cap \mathfrak{q} = A \cap \mathfrak{q}'$ を満たすとする。このとき $\mathfrak{q} = \mathfrak{q}'$ である。

証明 $\mathfrak{p} = A \cap \mathfrak{q} = A \cap \mathfrak{q}'$ とおき、 $S = A \setminus \mathfrak{p}$ とおく。命題 6.17(2) より、 $B_{\mathfrak{p}}$ は $A_{\mathfrak{p}}$ 上整である。 $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$ 、 $\mathfrak{n} = \mathfrak{q}B_{\mathfrak{p}}$ 、 $\mathfrak{n}' = \mathfrak{q}'B_{\mathfrak{p}}$ とおくと、 A と $A_{\mathfrak{p}}$ の素イデアルの一対一対応

$$\{\mathfrak{p}' \in \text{Spec}(A) \mid \mathfrak{p}' \subseteq \mathfrak{p}\} \longleftrightarrow \text{Spec}(A_{\mathfrak{p}})$$

により $\mathfrak{m}$ は $A_{\mathfrak{p}}$ の極大イデアルである。また $A_{\mathfrak{p}} \cap \mathfrak{n} = (A \cap \mathfrak{q})_{\mathfrak{p}} = \mathfrak{m}$ 、同様にして $A_{\mathfrak{p}} \cap \mathfrak{n}' = \mathfrak{m}$ であるので、命題 6.19 により $\mathfrak{n}, \mathfrak{n}'$ は $B_{\mathfrak{p}}$ の極大イデアルである。 $\mathfrak{n} \subseteq \mathfrak{n}'$ より $\mathfrak{n} = \mathfrak{n}'$ となるので、上のような B と $B_{\mathfrak{p}}$ の素イデアルの一対一対応により $\mathfrak{q} = \mathfrak{q}'$ を得る。

証明終

命題 6.21 $A \subseteq B$ を環、 C を B における A の整閉包とし、 S を A の積閉集合とする。このとき $S^{-1}C$ は $S^{-1}B$ における $S^{-1}A$ の整閉包である。

証明 命題 6.17(2) より $S^{-1}C$ は $S^{-1}A$ 上整である。 $b/s \in S^{-1}B$ が $S^{-1}A$ 上整とすると、 $a_i \in A, s_i \in S$ ($i = 1, \dots, n$) により、

$$(b/s)^n + (a_1/s_1)(b/s)^{n-1} + \dots + a_n/s_n = 0/1$$

と書ける。 $t = s_1 \cdots s_n, t_i = s_1 \cdots s_{i-1}s_{i+1} \cdots s_n$ ($i = 1, \dots, n$) とおき、整理すると

$$(tb^n + a_1st_1b^{n-1} + \dots + a_ns^nt_n)/s^nt = 0/1$$

を得る。よって、

$$u(tb^n + a_1st_1b^{n-1} + \dots + a_ns^nt_n) = 0$$

となる $u \in S$ がとれる。この両辺に $t^{n-1}u^{n-1}$ をかけると、

$$(btu)^n + a_1st_1u(bt u)^{n-1} + \dots + a_ns^nt_nt^{n-1}u^n = 0$$

を得るので $btu \in C$ となる。故に、 $b/s = btu/stu \in S^{-1}C$ である。

証明終

命題 6.22 A を整域とすると、次は互いに同値である。

- (1) A は整閉である。
- (2) 任意の素イデアル $\mathfrak{p}$ に対して $A_{\mathfrak{p}}$ は整閉である。
- (3) 任意の極大イデアル $\mathfrak{m}$ に対して $A_{\mathfrak{m}}$ は整閉である。

証明 K を A の商体、 C を K における A の整閉包とする。 $\phi: A \rightarrow C$ を包含写像とする。このとき、 A が整閉であることと、 ϕ が全射であることと同値である。また命題 6.21 より、 $A_{\mathfrak{p}}$ (または、 $A_{\mathfrak{m}}$) が整閉であることと、 $\phi_{\mathfrak{p}}: A_{\mathfrak{p}} \rightarrow C_{\mathfrak{p}}$ (または、 $\phi_{\mathfrak{m}}: A_{\mathfrak{m}} \rightarrow C_{\mathfrak{m}}$) が全射であることと同値である。写像 ϕ が全射であることは local property であるので、(1)~(3) の同値性が示せた。

定義 6.23 $A \subseteq B$ を環、 $\mathfrak{a}$ を A のイデアルとする。

- (1) $b \in B$ が $\mathfrak{a}$ 上整とは、

$$b^n + a_1b^{n-1} + \dots + a_n = 0$$

を満たす $a_1, \dots, a_n \in \mathfrak{a}$ が存在するときを言う。また任意の B の元が $\mathfrak{a}$ 上整のとき B が $\mathfrak{a}$ 上整であるという。

(2) $\Gamma = \{b \in B \mid b \text{ は } \mathfrak{a} \text{ 上整}\}$ を B における $\mathfrak{a}$ の整閉包と言う。

補題 6.24 $A \subseteq B$ を環、 $\mathfrak{a}$ を A のイデアル、 C を B における A の整閉包とする。このとき、 B における $\mathfrak{a}$ の整閉包は $\sqrt{\mathfrak{a}C}$ となる。またそれは和と積で閉じている。

証明 Γ を B における $\mathfrak{a}$ の整閉包とする。 $b \in \Gamma$ をとると、

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0 \quad (a_i \in \mathfrak{a})$$

と表せる。特に $a_i \in A$ なので $b \in C$ である。さらに

$$b^n = -(a_1 b^{n-1} + \cdots + a_n) \in \mathfrak{a}C$$

より $b \in \sqrt{\mathfrak{a}C}$ が言える。逆に $b \in \sqrt{\mathfrak{a}C}$ をとると、ある正の整数 n があって $b^n \in \mathfrak{a}C$ を満たす。よって

$$b^n = \sum_{i=1}^m a_i c_i \quad (a_i \in \mathfrak{a}, c_i \in C)$$

と表せる。 c_i ($i = 1, \dots, m$) は A 上整より、系 6.13 により $A[c_1, \dots, c_m]$ は有限生成 A -加群である。これを M とおき、 A -加群準同型 $\phi: M \rightarrow M$ を $\phi(\alpha) = b^n \alpha$ により定める。このとき、 $\phi(M) = b^n M \subseteq \mathfrak{a}M$ を満たしている。故に補題 6.10 により、 $\text{End}_A(M)$ 内で

$$\phi^l + a'_1 \phi^{l-1} + \cdots + a'_l = 0$$

を満たすような正の整数 l と $a'_1, \dots, a'_l \in \mathfrak{a}$ が存在する。この写像による 1 の像を考えれば、

$$b^{nl} + a'_1 b^{n(l-1)} + \cdots + a'_l = 0$$

なので、 $b \in \Gamma$ である。以上により、 B における $\mathfrak{a}$ の整閉包は $\sqrt{\mathfrak{a}C}$ であることが分かった。またこれは B のイデアルであるので、和と積について閉じている。証明終

命題 6.25 $A \subseteq B$ を整域、 A は整閉、 $x \in B$ は A のイデアル $\mathfrak{a}$ 上整とする。このとき、 x は A の商体 K 上代数的であり、またその K 上最小多項式の係数は $\sqrt{\mathfrak{a}}$ に属している。

証明 仮定より K 上代数的である。 x の K 上最小多項式を

$$p(t) = t^n + a_1 t^{n-1} + \cdots + a_n$$

とし、 L を $p(t)$ の分解体とし、 $x_1, \dots, x_n \in L$ を $p(t)$ の根とする。 x は $\mathfrak{a}$ 上整なので、 $f(x) = 0$ を満たすような $f(t) = t^m + b_1 t^{m-1} + \cdots + b_m$ ($b_1, \dots, b_m \in \mathfrak{a}$) が存在する。特に $f(t) \in K[t]$ と見れて、 $p(t)$ が x の K 上最小多項式であるので $p \mid f$ が成立して、 $f(x_i) = 0$ ($i = 1, \dots, n$) を満たす。故に $x_1, \dots, x_n$ も $\mathfrak{a}$ 上整である。さらに $p(t)$ における根と係数の関係により、 $a_1, \dots, a_n$ は $x_1, \dots, x_n$ の和と積で表せる。従って補題 6.24 より、 $a_1, \dots, a_n$ は $\mathfrak{a}$ 上整な A の元であるので、 $a_1, \dots, a_n \in \sqrt{\mathfrak{a}}$ である。 証明終

定義 6.26 $K \subset L$ を有限次代数拡大とし、 n を拡大次数とする。(このとき、 L は K^n と K -ベクトル空間として同型である。) $\alpha \in L$ に対し K -線形変換 $M_\alpha : L \rightarrow L$ を $M_\alpha(x) = \alpha x$ と定める。(M_α は、 K 上の n 次正方行列として表せる。) このとき $\text{Tr}_{L/K}(\alpha) = \text{Tr}(M_\alpha)$ とおき、これを K 上の α のトレースという。

命題 6.28 を示すために、次の補題が必要となる。証明は、省略する。

補題 6.27 L/K を体の有限次拡大とする。

- (1) K 上の α のトレースは、 L の K 上の基底の取り方に依らない。
- (2) B を L/K の中間体とし L/B の拡大次数 d とする。このとき $\alpha \in B$ に対し、

$$d \text{Tr}_{B/K}(\alpha) = \text{Tr}_{L/K}(\alpha)$$

が成立する。

- (3) L/K が分離拡大 $\iff \text{Tr}_{L/K}(\alpha) \neq 0$ を満たす $\alpha \in L$ が存在する。

命題 6.28 A を整閉整域、 K を A の商体、 L を K 上有限次分離拡大、 B を L における A の整閉包とする。このとき $B \subseteq \sum_{j=1}^n A v_j$ を満たす K -ベクトル空間 L の基底 $v_1, \dots, v_n$ が存在する。

更に、 A が Noether 環であれば、 B は有限生成 A -加群である。

証明 任意の $v \in L$ に対し、 v は K 上代数的なので、

$$a_0 v^n + a_1 v^{n-1} + \cdots + a_n = 0 \quad (a_i \in A)$$

と表せる。両辺に a_0^{n-1} をかけて $u = a_0 v$ とおけば、 $u \in L$ は A 上整なので $u \in B$ である。故に、 $u_i \in B$ ($i = 1, \dots, n$) を満たす K -ベクトル空間 L の基底 $u_1, \dots, u_n$ がとれる。ここで K -双線形写像 $\phi : L \times L \rightarrow K$ を $\phi(x, y) = \text{Tr}_{L/K}(xy)$ と定める。このとき、 K -ベクトル空間 L の基底 $v_1, \dots, v_n$ で、 $\phi(u_i, v_j) = \delta_{ij}$ を満たすものが存在することを示す。

任意の i に対して、補題 6.27(3) より K -線形写像 $f_i(y) = \phi(u_i, y)$ は 0 射ではない。 K -線形写像 $\phi_1 : L \rightarrow K^{n-1}$ を $\phi_1(y) = (f_2(y), \dots, f_n(y))$ と定める。 $\text{Ker}(\phi_1) = \bigcap_{i=2}^n \text{Ker}(f_i)$ かつ $\dim \text{Ker}(\phi_1) + \dim \text{Im}(\phi_1) = n$ より、ある $0 \neq v \in \text{Ker} \phi_1$ があって、任意の $i \geq 2$ に対して $\phi(u_i, v) = f_i(v) = 0$ を満たす。ここで $\phi(u_1, v) = 0$ と仮定する。任意の $u \in L$ に対して、 $u = \sum_{i=1}^n c_i u_i$ と表すと、 $\text{Tr}_{L/K}(uv) = \phi(u, v) = \sum c_i \phi(u_i, v) = 0$ となり、 L/K が分離的であることに反する。 $s = \phi(u_1, v) \neq 0$ とおき、 $v_1 = v/s$ とおけば、 $\phi(u_i, v_1) = \delta_{i1}$ を得る。 $v_2, \dots, v_n$ も同様にすれば $\phi(u_i, v_j) = \delta_{ij}$ を得る。このようにしてとった $v_1, \dots, v_n$ は一次独立になることは容易に分かる。よって、 $v_1, \dots, v_n$ は K -ベクトル空間 L の基底になる。

以上をふまえて、任意の $x \in B$ に対して $x = \sum_{j=1}^n x_j v_j$ ($x_j \in K$) と表せて、 $xu_i \in B$ である。

このとき $\phi(u_i, x) \in A$ である。なぜならば、 $y = u_i x$ とおき $K(y)/K$ の拡大次数を d とすると、 $L/K(y)$ の拡大次数は n/d なので、補題 6.27(2) により $(n/d)\text{Tr}_{K(y)/K}(y) = \text{Tr}_{L/K}(y) = \phi(u_i, x)$ である。また $K(y)/K$ の基底 $1, y, \dots, y^{d-1}$ をとる。 y の K 上の最小多項式を $Y^d + t_1 Y^{d-1} + \cdots + t_d$ とする。 y 倍する K -線形写像 $L \rightarrow L$ を考えれば、 $1 \mapsto y, \dots, y^{d-1} \mapsto y^n = -t_1 y^{d-1} - \cdots - t_d$ なので、この写像の基底 $1, y, \dots, y^{d-1}$ に関する表現行列は、

$$M_y = \left(\begin{array}{c|cccc} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ \hline -t_d & -t_{d-1} & \cdots & \cdots & -t_1 \end{array} \right)$$

である。故に $\text{Tr}_{K(y)/K}(y) = \text{Tr}(M_y) = -t_1$ である。また命題 6.25 より $-t_1 \in A$ である。従って $\phi(u_i, x) \in A$ である。

以上から $\phi(u_i, x) = \phi(u_i, \sum_j x_j v_j) = \sum_j x_j \phi(u_i, v_j) = \sum_j x_j \delta_{ij} = x_i \in A$ なので、 $x = \sum x_j v_j \in \sum Av_j$ より $B \subseteq \sum Av_j$ を満たす。 証明終

6.3 Dedekind 整域

定義 6.29 A を環とする。

$$\dim A = \sup\{n \mid \exists \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n (\mathfrak{p}_i \in \operatorname{Spec} A)\}$$

と定め、これを A の次元という。

命題 6.30 A を 1 次元 Noether 整域とする。このとき、 (0) でない A のイデアル $\mathfrak{a}$ は、根基が異なるような準素イデアルの積で一意的に表せる。

証明 命題 6.9 により、 $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ ($\mathfrak{q}_i$ ($i = 1, \dots, n$) は $\mathfrak{p}_i$ -準素イデアル) のように無駄のない準素分解ができる。 A の次元が 1 で整域であることから、 (0) でない素イデアルは極大イデアルである。故に $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ は互いに素なので、 $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ も互いに素である。従って $\mathfrak{a} = \bigcap \mathfrak{q}_i = \prod \mathfrak{q}_i$ となり、 $\mathfrak{a}$ は準素イデアルの積で表せる。

一意性を示そう。 $\mathfrak{a} = \prod \mathfrak{q}_i$ のように、根基をとると互いに異なる準素イデアルの積で書けたとする。上の議論の逆をたどって $\mathfrak{a} = \bigcap \mathfrak{q}_i$ と書ける。 $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$ とすると、これらは互いに異なっていて、 A の次元が 1 であるので、 $\mathfrak{p}_i$ は $\mathfrak{a}$ に属する極小素イデアルである。故に定理 6.7 より各 $\mathfrak{q}_i$ は $\mathfrak{a}$ によって一意的に定まる。 証明終

定義 6.31 (1) 1 次元 Noether 整閉整域を Dedekind 整域という。

(2) 1 次元 Noether 局所整閉整域を離散付値環 (DVR) という。

命題 6.32 $(A, \mathfrak{m})$ を 1 次元 Noether 局所整域とすると、次は互いに同値である。

- (1) A は整閉である。
- (2) $\mathfrak{m}$ は単項イデアルである。
- (3) 任意の (0) でないイデアルは $\mathfrak{m}$ のべきで表せる。

(4) ある $x \in A$ があって、任意の (0) でないイデアルは非負整数 k により (x^k) と表せる。

証明 (1)~(4) の同値性を示すために、その準備として次の (I), (II) を示す。

(I) 「 (0) でない A のイデアル $\mathfrak{a}$ は $\mathfrak{m}$ -準素イデアルである。つまり、正の整数 n があって $\mathfrak{m}^n \subseteq \mathfrak{a}$ を満たす。」を示す。今、次元は 1 なので $\sqrt{\mathfrak{a}} = \mathfrak{m}$ である。 A は Noether 環より、 $\sqrt{\mathfrak{a}}$ の生成元を $x_1, \dots, x_k$ とする。 $x_i^{n_i} \in \mathfrak{a}$ を満たす $n_i \in \mathbb{N}$ をとる。 $n = 1 + \sum_{i=1}^k (n_i - 1)$ とおくと、 $(\sqrt{\mathfrak{a}})^n$ は $\sum r_i = n$ を満たす $x_1^{r_1} \cdots x_k^{r_k}$ により生成されるが、ここで少なくとも一つの r_i は $r_i \geq n_i$ を満たしている。故に $(\sqrt{\mathfrak{a}})^n$ の生成元はすべて $\mathfrak{a}$ に含まれるので、 $\mathfrak{m}^n = (\sqrt{\mathfrak{a}})^n \subseteq \mathfrak{a}$ を満たす。

(II) 「任意の正の整数 n に対して $\mathfrak{m}^{n+1} \neq \mathfrak{m}^n$ 」を示す。もしそうでないとすると、中山の補題より $\mathfrak{m}^n = (0)$ となる。任意の素イデアル $\mathfrak{p}$ に対して $\mathfrak{m}^n \subseteq \mathfrak{p}$ であり、両辺根基をとると $\mathfrak{m} = \mathfrak{p}$ となり、次元が 1 であることに矛盾する。

(1) $\Rightarrow$ (2) を示す。 $0 \neq a \in \mathfrak{m}$ に対して、(I) により (a) は $\mathfrak{m}$ -準素イデアルであり、ある正の整数 n があって $\mathfrak{m}^n \subseteq (a)$ を満たす。この n を最小にとれば $\mathfrak{m}^{n-1} \not\subseteq (a)$ がいえるので、ある $b \in \mathfrak{m}^{n-1}$ が存在して $b \notin (a)$ を満たす。ここで $x = ab^{-1}$ とおき、もし $x^{-1} \in A$ ならば $b = x^{-1}a \in (a)$ より矛盾が生じるので、 $x^{-1} \notin A$ である。よって A は整閉なので x^{-1} は A 上整でない。またもし $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$ と仮定すると、 $\mathfrak{m}$ は忠実な $A[x^{-1}]$ -加群となり、命題 6.12 より x^{-1} が A 上整となる。故に $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$ を得る。ここで $y \in x^{-1}\mathfrak{m}$ に対して、 $y = x^{-1}m$ ($m \in \mathfrak{m}$) と書く。 $y = ba^{-1}m$ であり、 $bm \in \mathfrak{m}^n \subseteq (a)$ なので、 $bm = az$ ($z \in A$) と表せる。故に、 $y = z \in A$ により、 $x^{-1}\mathfrak{m} \subseteq A$ が言える。従って $\mathfrak{m}$ の極大性により $x^{-1}\mathfrak{m} = A$ なので $\mathfrak{m} = (x)$ が言えた。

(2) $\Rightarrow$ (3) を示す。 $\mathfrak{a}$ を (0) でも A でもない A のイデアルとする。(I) により $\mathfrak{m}^n \subseteq \mathfrak{a} \subseteq \mathfrak{m}$ を満たすので、この n を最小にとる。仮定により $\mathfrak{m} = (x)$ と表せて、また A は局所環であるので、任意の $\mathfrak{m}$ の元は cx^k ($c \in A^\times$, k は正の整数) と書けることに注意する。ここでもし $\mathfrak{a} \setminus \mathfrak{m}^n \neq \emptyset$ とすると、 $\mathfrak{a} \setminus \mathfrak{m}^n$ の元は dx^l ($d \in A^\times$, $l < n$) と表せるので、 $\mathfrak{m}^l = (x^l) \subseteq \mathfrak{a}$ となり n の最小性に矛盾する。従って $\mathfrak{a} \setminus \mathfrak{m}^n = \emptyset$ なので、 $\mathfrak{a} = (x^n) = \mathfrak{m}^n$ と書ける。

(3) $\Rightarrow$ (4) を示す。(II) により、 $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ が存在し、仮定により $(x) = \mathfrak{m}^r$ と表せる。もし $r \geq 2$ とすると $x \in \mathfrak{m}^2$ となり矛盾するので、 $r = 1$ となり $\mathfrak{m} = (x)$ を得る。これにより (4) が成立する。

(4) $\Rightarrow$ (1)を示す。仮定より A は PID であるから、 $\mathbb{Z}$ が $\mathbb{Q}$ で整閉であることを示す時と同様にして A は整閉と言える。 証明終

命題 6.33 A を 1 次元 Noether 整域とすると次は互いに同値である。

- (1) A は整閉である。
- (2) 任意の A の極大イデアル $\mathfrak{m}$ に対して、 $A_{\mathfrak{m}}$ は DVR である。
- (3) 任意の準素イデアルは極大イデアルのベキである。

証明 (1) $\Rightarrow$ (2)を示す。 A の極大イデアル $\mathfrak{m}$ に対して、命題 6.22 より $A_{\mathfrak{m}}$ は整閉である。故に $A_{\mathfrak{m}}$ は 1 次元の局所整閉整域である。

(2) $\Rightarrow$ (1)を示す。 $\mathfrak{m}$ を A の極大イデアルとする。このとき、 $A_{\mathfrak{m}}$ は整閉なので、命題 6.22 より A も整閉である。

(2) $\Rightarrow$ (3)を示す。(0) でない A の準素イデアル $\mathfrak{q}$ に対して、命題 6.32(1) $\Rightarrow$ (3) により、 $\mathfrak{q}A_{\mathfrak{m}} = (\mathfrak{m}A_{\mathfrak{m}})^n$ ($\mathfrak{m}$ は A の極大イデアル、 n は整の整数) と表せる。故に $\mathfrak{q}A_{\mathfrak{m}} = \mathfrak{m}^n A_{\mathfrak{m}}$ より、 $\mathfrak{q} = \mathfrak{m}^n$ を得る。

(3) $\Rightarrow$ (2)を示す。 A の極大イデアル $\mathfrak{m}$ をとる。(0) でない $A_{\mathfrak{m}}$ のイデアルは、 $\mathfrak{a}A_{\mathfrak{m}}$ ($\mathfrak{a}$ は (0) でない A のイデアル) と表せる。 $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ ($\mathfrak{q}_i$ は $\mathfrak{p}_i$ -準素イデアル) のように準素分解する。(3) より $\mathfrak{q}_i = \mathfrak{p}_i^{n_i}$ (n_i は正の整数) と書ける。 $\mathfrak{a}A_{\mathfrak{m}} \subseteq \mathfrak{m}A_{\mathfrak{m}}$ ならば、 $\mathfrak{a} \subseteq \mathfrak{m}$ なので、番号を付け替えて $\mathfrak{m} = \mathfrak{p}_1$ としてよい。すると、 $\mathfrak{a}A_{\mathfrak{m}} = \bigcap_{i=1}^n \mathfrak{q}_i A_{\mathfrak{m}} = (\mathfrak{m}A_{\mathfrak{m}})^{n_1}$ となる。故に、命題 6.32(3) $\Rightarrow$ (1) により、 $A_{\mathfrak{m}}$ は DVR である。 証明終

定理 6.34 Dedekind 整域において (0) でないイデアルは極大イデアルの積で一意的に表せる。

証明 命題 6.30 より、(0) でないイデアル $\mathfrak{a}$ は $\mathfrak{a} = \prod_{i=1}^n \mathfrak{q}_i$ のように、互いに根基の異なる準素イデアル $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ の積で一意的に表せる。さらに命題 6.33 より、準素イデアルは極大イデアルのベキで表せるので、 $\mathfrak{a} = \prod_{i=1}^n \mathfrak{m}_i^{n_i}$ と極大イデアル $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ の積で表せる。

一意性を示す。 $\mathfrak{a} = \prod_{i=1}^n \mathfrak{m}_i^{n_i} = \prod_{i=1}^n \mathfrak{m}_i^{n'_i}$ と二通りに書けたとする。両辺 $\mathfrak{m}_i$ で局所化すると、 $(\mathfrak{m}_i A_{\mathfrak{m}_i})^{n_i} = (\mathfrak{m}_i A_{\mathfrak{m}_i})^{n'_i}$ より、 $n_i = n'_i$ ($i = 1, \dots, n$) と言える。故に、 $\mathfrak{a}$ は極大イデアルの積で一意的に表せる。 証明終

定義 6.35 $\mathbb{Q}$ 上有限次代数拡大体を代数体という。また代数体 K における $\mathbb{Z}$ の整閉包を K の整数環という。

定理 6.36 代数体 K の整数環は Dedekind 整域である。

証明 $\mathfrak{o}_K$ を K の整数環とする。 $K/\mathbb{Q}$ は分離拡大なので命題 6.28 より、ある $\mathbb{Q}$ 上 K の基底 $v_1, \dots, v_n$ が存在して、 $\mathfrak{o}_K \subseteq \sum_{j=1}^n \mathbb{Z}v_j$ を満たす。故に $\mathfrak{o}_K$ は $\mathbb{Z}$ -加群として有限生成だから、Noether 環である。また系 6.16 により $\mathfrak{o}_K$ は整閉である。最後に次元が 1 であることを示す。 $\mathfrak{p}$ を (0) でない $\mathfrak{o}_K$ の素イデアルとする。系 6.20 より $\mathbb{Z} \cap \mathfrak{p}$ も (0) でない $\mathbb{Z}$ の極大イデアルなので、系 6.19 より $\mathfrak{p}$ は $\mathfrak{o}_K$ の極大イデアルである。従って $\mathfrak{o}_K$ は Dedekind 整域である。 証明終

参考文献

- [1] 久我勝利, 図解雑学「数論とフェルマーの最終定理」(ナツメ社, 2005)
- [2] 倉田令二郎, 平方剰余の相互法則—ガウスの全証明 (日本評論社, 1992)
- [3] 山崎隆雄, 初等整数論 数論幾何への誘い (共立出版, 2015)
- [4] M.F.Atiyah, I.G.MacDonald, Introduction to Commutative Algebra (Westview Press, 1969)
- [5] Wikipedia(<https://ja.m.wikipedia.org>)