代数学演習

– 代数的整数論 –

中川 仁

2012 年度後期

記号
$\mathbb{Z}$:有理整数環，$\mathbb{Q}$:有理数全体の集合，$\mathbb{R}$:実数全体の集合，$\mathbb{C}$:複素数全体の集合.

目 次

0 有理整数環 $\mathbb{Z}$ のイデアルと剰余環

定義 0.1. $\mathbb{Z}$ の部分集合 I が次の条件をみたすとき，I は $\mathbb{Z}$ の**イデアル**であるという:

$$a, b \in I \Longrightarrow a + b \in I;$$

$r \in \mathbb{Z}, a \in I \Longrightarrow ra \in I.$

命題 0.2. I を $\mathbb{Z}$ のイデアルとすると，$\exists m \in \mathbb{Z},\ m \geq 0,\ I = m\mathbb{Z}.$

[証明]　I を $\mathbb{Z}$ のイデアルとする．$I = \{0\}$ ならば，$m = 0$ とおけば，$I = m\mathbb{Z}$ である．$I \supsetneq \{0\}$ とする．このとき，$a \in I$ ならば，$-a \in I$ だから，I は必ず正の整数を含む．m を I に含まれる最小の正の整数とする．このとき，任意の $a \in I$ に対して，a を m で割算して，

$$a = mq + r,\ q \in \mathbb{Z},\ 0 \leq r < m$$

とかく．$r = a - mq \in I$ より，m の最小性から，$r = 0$ でなければならない．したがって，$a = mq \in m\mathbb{Z}$ となる．すなわち，$I \subset m\mathbb{Z}$ である．$I \supset m\mathbb{Z}$ は明かであるから，$I = m\mathbb{Z}$ が示された．　□

定義 0.3. I を $\mathbb{Z}$ のイデアルとする．各 $a \in \mathbb{Z}$ に対して，$\mathbb{Z}$ の部分集合

$$a + I = \{a + x \,|\, x \in I\}$$

を，a によって代表される I を法とする**剰余類**という．$a + I = b + I \Longleftrightarrow a - b \in I$ である．I を法とする剰余類全体からなる集合を $\mathbb{Z}/I$ で表す．すなわち，

$$\mathbb{Z}/I = \{a + I \,|\, a \in I\}.$$

命題 0.4. I を環 $\mathbb{Z}$ のイデアルとする．このとき，$\mathbb{Z}/I$ は自然に環になる．これを $\mathbb{Z}$ の I による**剰余環**という．

[証明]　$\mathbb{Z}/I$ に加法，乗法を次のように定義する．$a + I = [a]$ とかく．

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

これは代表元のとりかたによらず矛盾なく定義される．$[0]$ は $\mathbb{Z}/I$ の零元，$[1]$ は $\mathbb{Z}/I$ の単位元であり，$-[a] = [-a]$,

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c],$$
$$[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)].$$

□

$I = m\mathbb{Z}$ $(m \in \mathbb{Z},\ m > 0)$ として，剰余環 $\mathbb{Z}/m\mathbb{Z}$ を考察する．$a \in \mathbb{Z}$ によって代表される剰余類 $a + m\mathbb{Z}$ を $[a]$ とかくことにする．$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \cdots, [m-1]\}$ である．$[a] = [b]$ を $a \equiv b \pmod{m}$ とかく．

補題 0.5. 少なくとも一方は 0 でない整数 a, b に対して,

$$I = \{ax + by \,|\, x, y \in \mathbb{Z}\}$$

とおけば，I は $\mathbb{Z}$ のイデアルであり，m を $I = m\mathbb{Z}$ となる正の整数とすると (命題 0.2)，m は a, b の最大公約数である．

[証明]　I がイデアルであることは明か．$a, b \in I$ より，$a = ma_1$, $b = mb_1$, $a_1, b_1 \in \mathbb{Z}$ とかける．よって，m は a, b の公約数である．d を整数 a, b の公約数とすると，$a = da'$, $b = db'$, $a', b' \in \mathbb{Z}$ とかける．一方，$m = ax + by$ とかけるから，$m = d(a'x + b'y)$．すなわち，d は m の約数である．ゆえに，m は a, b の最大公約数である．　□

系 0.6. 少なくとも一方は 0 でない整数 a, b に対して，m を a, b の最大公約数とすれば,

$$ax + by = m$$

を満たす $x, y \in \mathbb{Z}$ が存在する．

系 0.7. p を素数とし，$a \in \mathbb{Z}$ を p で割り切れないとすれば,

$$ax + py = 1$$

を満たす $x, y \in \mathbb{Z}$ が存在する．

[証明]　p の正の約数は 1 と p だけである．a は p で割り切れないから，a と p の最大公約数は 1 である．系 0.6 より，$ax + py = 1$ を満たす $x, y \in \mathbb{Z}$ が存在する．　□

命題 0.8. $\mathbb{Z}/p\mathbb{Z}$ において，$[a] \neq [0]$ とすれば，$[x] \in \mathbb{Z}/p\mathbb{Z}$ で $[a][x] = [1]$ を満たすものが存在する．

上の命題 0.8 より，$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ は体である．体 $\mathbb{F}_p$ を p 個の元からなる**有限体**という．

次に，K を任意の体とする (例えば，$K = \mathbb{Q}$) とする．$K[X]$ によって 1 変数 X の K の元を係数とする多項式の全体を表す．$K[X]$ は多項式の加法，乗法によって環をなす．この環についても，$\mathbb{Z}$ と同様のことが定義され，同様の性質を持つことが示せる．

定義 0.9. $K[X]$ の部分集合 I が次の条件をみたすとき，I は $K[X]$ の**イデアル**であるという:

$$a, b \in I \Longrightarrow a + b \in I;$$

$$r \in K[X], a \in I \Longrightarrow ra \in I.$$

命題 0.10. I を $K[X]$ のイデアルとすると，$\exists m \in K[X],\ m \geq 0,\ I = mK[X]$.

[証明]　I を $K[X]$ のイデアルとする．$I = \{0\}$ ならば，$m = 0$ とおけば，$I = mK[X]$ である．$I \supsetneq \{0\}$ とする．このとき，m を I に含まれる最小の次数の多項式とする．このとき，任意の $a \in I$ に対して，a を m で割算して，

$$a = mq + r,\ q \in K[X],\ r = 0 \ \text{または}\ \deg r < \deg m$$

とかく．$r = a - mq \in I$ より，m の次数の最小性から，$r = 0$ でなければならない．したがって，$a = mq \in mK[X]$ となる．すなわち，$I \subset mK[X]$ である．$I \supset mK[X]$ は明かであるから，$I = mK[X]$ が示された．　□

定義 0.11. I を $K[X]$ のイデアルとする．各 $a \in K[X]$ に対して，$K[X]$ の部分集合

$$a + I = \{a + h \,|\, h \in I\}$$

を，a によって代表される I を法とする**剰余類**という．$a + I = b + I \Longleftrightarrow a - b \in I$ である．I を法とする剰余類全体からなる集合を $K[X]/I$ で表す．すなわち，

$$K[X]/I = \{a + I \,|\, a \in I\}.$$

命題 0.12. I を環 $K[X]$ のイデアルとする．このとき，$K[X]/I$ は自然に環になる．これを $K[X]$ の I による**剰余環**という．

[証明]　$K[X]/I$ に加法，乗法を次のように定義する．$a + I = [a]$ とかく．

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

これは代表元のとりかたによらず矛盾なく定義される．$[0]$ は $K[X]/I$ の零元，$[1]$ は $K[X]/I$ の単位元であり，$-[a] = [-a]$,

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c],$$
$$[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)].$$

□

$I = mK[X]$ $(m \in K[X],\ \deg m > 0)$ として，剰余環 $K[X]/mK[X]$ を考察する．$a \in K[X]$ によって代表される剰余類 $a + mK[X]$ を $[a]$ とかくことにする．

$$K[X]/mK[X] = \{[g] \,|\, g \in K[X],\ \deg g < \deg m\}$$

である．$[a] = [b]$ を $a \equiv b \pmod{m}$ とかく．

補題 0.13. 少なくとも一方は 0 でない $a, b \in K[X]$ に対して,

$$I = \{af + bg \,|\, f, g \in K[X]\}$$

とおけば，I は $K[X]$ のイデアルであり，m を $I = mK[X]$ となる多項式とすると (命題 0.2)，m は a, b の最大公約多項式である．

[証明]　I がイデアルであることは明か．$a, b \in I$ より，$a = ma_1$, $b = mb_1$, $a_1, b_1 \in K[X]$ とかける．よって，m は a, b の公約数である．d を整数 a, b の公約数とすると，$a = da'$, $b = db'$, $a', b' \in K[X]$ とかける．一方，$m = af + bg$ とかけるから，$m = d(a'f + b'g)$．すなわち，d は m の約数である．ゆえに，m は a, b の最大公約多項式である．　□

系 0.14. 少なくとも一方は 0 でない多項式 a, b に対して，m を a, b の最大公約多項式とすれば,

$$af + bg = m$$

を満たす $f, g \in K[X]$ が存在する．

系 0.15. $p \in K[X]$ を既約多項式とし，$a \in K[X]$ を p で割り切れない多項式とすれば,

$$af + pg = 1$$

を満たす $f, g \in K[X]$ が存在する．

[証明]　p を割り切る多項式は 0 でない定数と p の 0 でない定数倍だけである．a は p で割り切れないから，a と p の最大公約多項式は 1 である．系 0.6 より，$af+pg = 1$ を満たす $f, g \in K[X]$ が存在する．　□

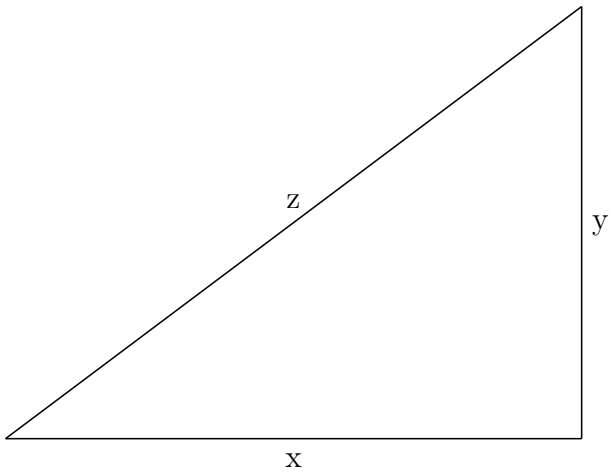
命題 0.16. $K[X]/pK[X]$ において，$[a] \neq [0]$ とすれば，$[x] \in K[X]/pK[X]$ で $[a][x] = [1]$ を満たすものが存在する．

1　ピタゴラス数とガウスの整数環

方程式

$$x^2 + y^2 = z^2 \tag{1.1}$$

を満たす自然数 x, y, z を**ピタゴラス数**という．



例 1.1. $3^2+4^2=5^2$, $5^2+12^2=13^2$, ... 等バビロニアの時代から知られていた.

一般解を 2 次体の整数論を用いて求めてみよう. $x=dx_1$ と $y=dy_1$ ならば, $z^2=d^2(x_1^2+y_1^2)$ より, $z=dz_1$ とかける. よって, はじめから x と y は公約数を持たないとする. 虚数単位 i を用いて, (1.1) の左辺を因数分解する.

$$(x+yi)(x-yi)=z^2. \tag{1.2}$$

そこで,

$$\mathcal{O}=\{a+bi \mid a,b\in\mathbb{Z}\} \quad (\subset\mathbb{C})$$

とおく.

命題 1.2. $\mathcal{O}$ は単位元 1 を持つ可換環である.

[証明] $\alpha=a+bi, \beta=c+di\in\mathcal{O}$ とすると,

$$\begin{aligned} \alpha\pm\beta &= (a+bi)\pm(c+di)=(a\pm c)+(b\pm d)i\in\mathcal{O}, \\ \alpha\beta &= (a+bi)(c+di)=(ac-bd)+(ad+bc)i\in\mathcal{O}. \end{aligned}$$

$1\in\mathcal{O}$, $\alpha\beta=\beta\alpha$ である. よって, $\mathcal{O}$ は単位元 1 を持つ可換環である. $2\in\mathcal{O}$ であるが, $2\alpha=1$ となる $\alpha\in\mathcal{O}$ は存在しないから, 体ではない. □

定義 1.3. $\alpha\in\mathcal{O}$ について, $\beta\in\mathcal{O}$ で $\alpha\beta=1$ となるものが存在するとき, α は $\mathcal{O}$ の**可逆元**であるという. $\mathcal{O}$ の可逆元全体の集合を $\mathcal{O}^\times$ で表す. $\mathcal{O}^\times$ は乗法に関して群になる.

命題 1.4. $\mathcal{O}^\times=\{1,-1,i,-i\}$ であり, これは i によって生成される位数 4 の巡回群である.

[証明]　$\alpha = a + bi, \beta = c + di \in \mathcal{O}$, $\alpha\beta = 1$ とすると，

$$1 = |\alpha\beta|^2 = (\alpha\beta)(\overline{\alpha\beta}) = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = |\alpha|^2|\beta|^2 = (a^2 + b^2)(c^2 + d^2).$$

$a^2 + b^2, c^2 + d^2 \in \mathbb{Z}$ は非負であり，その積が 1 であるから，$a^2 + b^2 = c^2 + d^2 = 1$. $a, b, c, d \in \mathbb{Z}$ より，$a = \pm 1, b = 0$ または $a = 0, b = \pm 1$ である．よって，$\alpha = \pm 1$ または $\alpha = \pm i$ である．そのとき，$\beta = \pm 1$ または $\beta = \mp i$ である．ゆえに，

$$\mathcal{O}^\times = \{1, -1, i, -i\} = \{i^m \mid m = 0, 1, 2, 3\}.$$

□

次のような $\mathbb{C}$ の部分集合 K を考える．

$$\mathcal{O} \subset K = \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}.$$

$0 \neq \alpha = a + bi \in K$ ならば，

$$\frac{1}{\alpha} = \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{(-b)}{a^2 + b^2} i \in K$$

であるから，K は体である．

定義 1.5. $\mathcal{O}$ の部分集合 $\mathfrak{a}$ が

$\forall \alpha, \beta \in \mathfrak{a}$ に対して，$\alpha + \beta \in \mathfrak{a}$,

$\forall \alpha \in \mathfrak{a}$, $\forall \gamma \in \mathcal{O}$ に対して，$\gamma\alpha \in \mathfrak{a}$

を満たすとき，$\mathfrak{a}$ は $\mathcal{O}$ の**イデアル**であるという．

環 $\mathcal{O}$ のイデアルについて調べよう．

定理 1.6. $\mathcal{O}$ の任意のイデアルは単項イデアルである．

[証明]　$\{0\} \subsetneq \mathfrak{a} \subset \mathcal{O}$ をイデアルとする．$0 \neq \alpha = a+bi \in \mathfrak{a}$ を $|\alpha|^2 = \alpha\bar{\alpha} = a^2+b^2$ が最小になるようにとる．$\alpha \in \mathfrak{a}$ より，任意の $\gamma \in \mathcal{O}$ に対して，$\gamma\alpha \in \mathfrak{a}$ である．よって，$(\alpha) = \alpha\mathcal{O} \subset \mathfrak{a}$ である．逆向きの包含関係を示そう．そのために，任意の $\beta \in \mathfrak{a}$ をとる．$\dfrac{\beta}{\alpha} \in K$ より，

$$\frac{\beta}{\alpha} = x + yi, \quad x, y \in \mathbb{Q}$$

とかける．x, y に一番近い整数をそれぞれ c, d とする．

$$c - \frac{1}{2} \leq x < c + \frac{1}{2}, \quad d - \frac{1}{2} \leq y < d + \frac{1}{2}$$

となるようにすれば，c, d は一意的に定まる．$u = x - c$, $v = y - d$ とおけば，$x = c + u$, $y = d + v$,

$$|u| \leq \frac{1}{2}, \quad |v| \leq \frac{1}{2}$$

である．よって，$\gamma = c + di \in \mathcal{O}$ とおいて，$\delta = \beta + (-\gamma)\alpha$ とおけば，$\delta \in \mathfrak{a}$ であり，

$$\delta = \alpha\left(\frac{\beta}{\alpha} - \gamma\right) = \alpha(u + vi)$$

であるから，

$$\begin{aligned} |\delta|^2 &= |\alpha(u+vi)|^2 = \alpha(u+vi)\bar{\alpha}(u-iv) = |\alpha|^2(u^2+v^2) \\ &\leq |\alpha|^2\left(\frac{1}{4}+\frac{1}{4}\right) = \frac{1}{2}|\alpha|^2 < |\alpha|^2. \end{aligned}$$

$|\alpha|^2$ の最小性から，$\delta = 0$ でなければならない．ゆえに，$\beta = \gamma\alpha \in (\alpha)$．これが任意の $\beta \in \mathfrak{a}$ について成り立つから，$\mathfrak{a} \subset (\alpha)$ である．$(\alpha) \subset \mathfrak{a}$ はすでに示されているから，$\mathfrak{a} = (\alpha)$ を得た．すなわち，$\mathfrak{a}$ は単項イデアルである． □

$\mathcal{O}$ における倍数，約数，素数 (既約元) の概念が $\mathbb{Z}$ のときと同様に定義できる．

定義 1.7. $\alpha, \beta \in \mathcal{O}$ について，$\gamma \in \mathcal{O}$ で，$\alpha = \beta\gamma$ となるものが存在するとき，α は β の**倍数**である，β は α の**約数**であるといい，$\beta|\alpha$ とかく．α が約数として，ε と $\varepsilon\alpha$, $\varepsilon \in \mathcal{O}^\times$ の形のものしか持たないとき，α は**既約元**であるという．

命題 1.8. $\alpha \in \mathcal{O}$ を既約元とすれば，単項イデアル $(\alpha) = \alpha\mathcal{O}$ は素イデアルである．

[証明] $\beta, \gamma \in \mathcal{O}$, $\beta\gamma \in (\alpha)$ とする．$\beta \notin (\alpha)$ とする．$\mathfrak{a} = \alpha\mathcal{O} + \beta\mathcal{O}$ とおけば，$\mathfrak{a} = (\delta)$ とすれば，$\alpha = \delta\alpha_1$, $\alpha_1 \in \mathcal{O}$ である．α は既約元であるから，$\delta \in \mathcal{O}^\times$ または $\alpha_1 \in \mathcal{O}^\times$ である．しかし，$\alpha_1 \in \mathcal{O}^\times$ とすると，$\beta \in (\delta) = (\alpha)$ となって矛盾する．ゆえに，$\delta \in \mathcal{O}^\times$ である．したがって，$\alpha\xi + \beta\eta = 1$ となる $\xi, \eta \in \mathcal{O}$ が存在する．$\gamma = \alpha\gamma\xi + \beta\gamma\eta \in (\alpha)$ である． □

$\mathbb{Z}$ における素因数分解の一意性の証明と同様にして，$\mathcal{O}$ において，次のことが証明される．

定理 1.9. 任意の $\alpha \in \mathcal{O}, \alpha \neq 0$ は

$$\alpha = \varepsilon\pi_1^{a_1} \cdots \pi_r^{a_r},$$

の形に表せる．ここで，$\varepsilon \in \mathcal{O}^\times$ であり，$\pi_1, \ldots, \pi_r$ は既約元で，$i \neq j$ のときは π_i は π_j の可逆元倍ではない．さらに，この表し方は積の順序と可逆元倍を除いて一意的である．すなわち，もし，

$$\alpha = \varepsilon'(\pi_1')^{b_1} \cdots (\pi_s')^{b_s},$$

が同様の表し方であるとすれば，$s = r$ であり，番号を付け替えれば，$\pi_1', \ldots, \pi_r'$ はそれぞれ $\pi_1, \ldots, \pi_r$ の可逆元倍であり，$b_1 = a_1, \ldots, b_r = a_r$ である．

x, y, z を $x^2 + y^2 = z^2$ を満たす自然数で，整数 x, y は互いに素であるとする．
そのとき，x, y がともに偶数であることはない．
さらに，x, y がともに奇数であることもない．
[証明]　もし，$x = 2x_1 + 1$, $y = 2y_1 + 1$, $x_1, y_1 \in \mathbb{Z}$ とすると，

$$z^2 = (2x_1 + 1)^2 + (2y_1 + 1)^2 = 4(x_1^2 + x_1 + y_1^2 + y_1) + 2.$$

よって，z^2 を 4 で割った余りは 2 である．しかし，$z = 2z_1$ ならば，$z^2 = 4z_1^2$, $z = 2z_1 + 1$ ならば，$z^2 = 4(z_1^2 + z_1) + 1$ だから，z^2 を 4 で割った余りは 0 か 1 で，2 になることはない．これは矛盾である．　□

以下，x は奇数, y は偶数であるとする．
そのとき，$x + yi$ と $x - yi$ は互いに素である．
[証明]　$x + yi = \alpha\beta$, $x - yi = \alpha\gamma$ とすると，

$$2x = \alpha(\beta + \gamma), \quad 2y = -i\alpha(\beta - \gamma), \quad \gcd(x, y) = 1$$

より，$u, v \in \mathbb{Z}$ で，$xu + yv = 1$ となるものが存在する．よって，

$$2 = 2xu + 2yv = \alpha\delta, \quad \delta = u(\beta + \gamma) - iv(\beta - \gamma)$$

とかける．$\alpha = a + bi$, $\delta = c + di$ とすると，

$$\alpha\delta = (a + bi)(c + di) = ac - bd + (ad + bc)i$$

より，$ac - bd = 2$, $ad + bc = 0$,

$$4 = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2).$$

これから，$a^2 + b^2 = 1, 2$ または 4 である．$a^2 + b^2 = 4$ ならば，$a = \pm 2$, $b = 0$ または $a = 0$, $b = \pm 2$ であり，$\alpha = \pm 2$ または $\pm 2i$ である．このとき，$x + yi = \pm 2\beta$ または $\pm 2i\beta$，したがって，x, y ともに偶数となって矛盾である．$a^2 + b^2 = 2$ ならば，$a = \pm 1$, $b = \pm 1$ であり，$\alpha = 1 \pm i$ としてよい．$\beta = s + ti$ とおけば，

$$x + yi = (1 \pm i)\beta = (1 \pm i)(s + ti) = s \mp t + (t \pm s)i.$$

よって，$x = s \mp t$, $y = t \pm s$, $x - y = (s - t) - (t + s) = -2t$ または $x - y = (s + t) - (t - s) = 2s$ となって，いずれも $x - y$ は偶数である．これは，x が奇数, y が偶数であることに矛盾する．　□

等式 (1.2) の両辺を既約元の積にかけば，定理 1.9 より，$\alpha = a + bi \in \mathcal{O}$ と $\varepsilon \in \mathcal{O}^\times$ で，

$$x + iy = \varepsilon\alpha^2 = \varepsilon((a^2 - b^2) + i(2ab)),$$

となるものが存在する．$\varepsilon = \pm 1, \pm i$ であり，x は奇数としたから，$\varepsilon = \pm 1$ であり，

$$\begin{cases} x &= a^2 - b^2, \\ y &= 2ab, \end{cases} \qquad \begin{cases} x &= b^2 - a^2, \\ y &= -2ab \end{cases}$$

となる．ここで，$x, y > 0$, $a, b > 0$ とすれば，

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

となり，$a > b$ であり，$x = a^2 - b^2 > 0$ が奇数であることから，a, b はどちらか一方だけが奇数である．

a	b	x	y	z
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41

2　フェルマー予想

350 年以上の間，未解決であったフェルマー予想は，1994 年にワイルズによって証明された．

定理 2.1. n を 3 以上の整数とするとき，

$$x^n + y^n = z^n \tag{2.1}$$

を満たす自然数 x, y, z は存在しない．

2.1　$n = 4$ の場合の証明

定理 2.2.

$$x^4 + y^4 = z^2$$

を満たす自然数 x, y, z は存在しない．したがって，

$$x^4 + y^4 = z^4$$

を満たす自然数 x, y, z は存在しない．

[証明]　もし，このような自然数の組 (x, y, z) が存在するとすれば，それらの中で，z が最小になるようなものがとれる．そのとき，x と y は互いに素である．実際，d を x, y の最大公約数として，$x = dx_1$, $y = dy_1$, x_1, y_1 は自然数，x_1 と y_1 は互いに素，とかけば，

$$z^2 = x^4 + y^4 = d_1^4(x_1^4 + y_1^4), \qquad \left(\frac{z}{d^2}\right)^2 = x_1^4 + y_1^4.$$

したがって，$\left(\frac{z}{d^2}\right)^2$ は自然数であり，$\frac{z}{d^2} = z_1$ も自然数である．そのとき，

$$x_1^4 + y_1^4 = z_1^2$$

であるから，$d > 1$ ならば，$z_1 < z = dz_1$ となって，z が最小であることに矛盾する．ゆえに，$d = 1$ である．

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

であり，x^2 と y^2 は互いに素である．前節の結果によって，x, y の一方は奇数で，もう一方は偶数であり，x を奇数とすれば，互いに素な自然数 a, b で，$a > b$, a, b の一方だけが奇数で，

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

となるものが存在する．このとき，

$$x^2 + b^2 = a^2$$

であり，a と b が互いに素であるから，x と b も互いに素である．したがって，上と同じ議論によって，x と b の一方だけが奇数であるが，x を奇数としているので，b は偶数である．よって，互いに素な自然数 s, t で，$s > t$, s, t の一方だけが奇数で，

$$x = s^2 - t^2, \quad b = 2st, \quad a = s^2 + t^2$$

となるものが存在する．$y^2 = 2ab$ より，

$$y^2 = 2ab = 4st(s^2 + t^2).$$

$y = 2y_0$ とかけば，

$$y_0^2 = st(s^2 + t^2)$$

である．ここで，s と t は互いに素であるから，s, t, $s^2 + t^2$ のどの 2 つも互いに素であることがわかる．それらの積が平方数であるから，素因数分解を考えれば，s, t, $s^2 + t^2$ はそれぞれ平方数でなければならない．よって，$s = x_1^2$, $t = y_1^2$, $s^2 + t^2 = z_1^2$ となる自然数 x_1, y_1, z_1 が存在する．そのとき，

$$x_1^4 + y_1^4 = z_1^2$$

であるが，

$$z_1 \leq z_1^2 = s^2 + t^2 = a < a^2 + b^2 = z$$

であるから，z が最小であることに矛盾する． □

2.2 $n = 3$ の場合の証明

$\omega = \dfrac{-1+\sqrt{-3}}{2}$ とおけば，$\omega^2 + \omega + 1 = 0$, $\omega^3 = 1$ である．このとき，

$$\mathcal{O} = \mathbb{Z}[\omega] = \{a + b\omega \,|\, a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

とおけば，命題 1.2 と同様に，次が成り立つ．

命題 2.3. $\mathcal{O}$ は単位元 1 を持つ可換環である．

[証明] $\alpha = a + b\omega, \beta = c + d\omega \in \mathcal{O}$ とすると，

$$\begin{aligned}
\alpha \pm \beta &= (a + b\omega) \pm (c + d\omega) = (a \pm c) + (b \pm d)\omega \in \mathcal{O}, \\
\alpha\beta &= (a + b\omega)(c + d\omega) = ac + (ad + bc)\omega + bd\omega^2 \\
&= ac + (ad + bc)\omega + bd(-\omega - 1) \\
&= ac - bd + (ad + bc - bd)\omega \in \mathcal{O}.
\end{aligned}$$

$1 \in \mathcal{O}$, $\alpha\beta = \beta\alpha$ である．よって，$\mathcal{O}$ は単位元 1 を持つ可換環である． □

命題 2.4. $\mathcal{O}^\times = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$ であり，これは $-\omega$ によって生成される位数 6 の巡回群である．

[証明] $\alpha = a + b\omega, \beta = c + d\omega \in \mathcal{O}$, $\alpha\beta = 1$ とすると，

$$1 = |\alpha\beta|^2 = (\alpha\beta)(\overline{\alpha\beta}) = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = |\alpha|^2|\beta|^2.$$

ここで，$\bar{\omega} = \dfrac{-1-\sqrt{-3}}{2} = -1 - \omega = \omega^2$ であるから，

$$|\alpha|^2 = (a + b\omega)(a + b\bar{\omega}) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2$$

である．同様に，$|\beta|^2 = c^2 - cd + d^2$ である．よって，

$$(a^2 - ab + b^2)(c^2 - cd + d^2) = 1.$$

$a^2 - ab + b^2, c^2 - cd + d^2 \in \mathbb{Z}$ は非負であり，その積が 1 であるから，$a^2 - ab + b^2 = c^2 - cd + d^2 = 1$.

$$a^2 - ab + b^2 = \left(a - \frac{1}{2}b\right)^2 + \frac{3}{4}b^2 = 1$$

$a, b \in \mathbb{Z}$ より，$|b| \leq 1$ である．$b = 0$ のとき，$a = \pm 1$ であり，$b = \pm 1$ のとき，

$$a^2 \mp a + 1 = 1, \qquad a(a \mp 1) = 0, \qquad a = 0, \pm 1.$$

$a = \pm 1, b = 0$ または $a = 0, b = \pm 1$ である．よって，$\alpha = \pm 1, = \pm\omega,$ または $\pm(1 + \omega) = \mp\omega^2$ である．そのとき，$\beta = \pm 1, \pm\omega^2$，または $\mp\omega$ である．ゆえに，

$$\mathcal{O}^\times = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\} = \{(-\omega)^k \,|\, 0 \leq k \leq 5\}.$$

□

次のような $\mathbb{C}$ の部分集合 K を考える．

$$\mathcal{O} \subset K = \{a + b\omega \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}.$$

$0 \neq \alpha = a + b\omega \in K$ ならば，

$$\frac{1}{\alpha} = \frac{1}{a + b\omega} = \frac{a + b\omega^2}{a^2 - ab + b^2} = \frac{a - b}{a^2 - ab + b^2} + \frac{(-b)}{a^2 - ab + b^2}\omega \in K$$

であるから，K は体である．

定理 2.5. $\mathcal{O}$ の任意のイデアルは単項イデアルである．

[証明] $\{0\} \subsetneq \mathfrak{a} \subset \mathcal{O}$ をイデアルとする．$0 \neq \alpha = a + b\omega \in \mathfrak{a}$ を $|\alpha|^2 = \alpha\bar{\alpha} = a^2 - ab + b^2$ が最小になるようにとる．$\alpha \in \mathfrak{a}$ より，任意の $\gamma \in \mathcal{O}$ に対して，$\gamma\alpha \in \mathfrak{a}$ である．よって，$(\alpha) = \alpha\mathcal{O} \subset \mathfrak{a}$ である．逆向きの包含関係を示そう．そのために，任意の $\beta \in \mathfrak{a}$ をとる．$\dfrac{\beta}{\alpha} \in K$ より，

$$\frac{\beta}{\alpha} = x + y\omega, \quad x, y \in \mathbb{Q}$$

とかける．x, y に一番近い整数をそれぞれ c, d とする．

$$c - \frac{1}{2} \leq x < c + \frac{1}{2}, \quad d - \frac{1}{2} \leq y < d + \frac{1}{2}$$

となるようにすれば，c, d は一意的に定まる．$u = x - c$, $v = y - d$ とおけば，$x = c + u$, $y = d + v$,

$$|u| \leq \frac{1}{2}, \quad |v| \leq \frac{1}{2}$$

である．よって，$\gamma = c + d\omega \in \mathcal{O}$ とおいて，$\delta = \beta + (-\gamma)\alpha$ とおけば，$\delta \in \mathfrak{a}$ であり，

$$\delta = \alpha\left(\frac{\beta}{\alpha} - \gamma\right) = \alpha(u + v\omega)$$

であるから，

$$\begin{aligned} |\delta|^2 = |\alpha(u + v\omega)|^2 &= \alpha(u + v\omega)\bar{\alpha}(u + v\omega^2) = |\alpha|^2(u^2 - uv + v^2) \\ &\leq |\alpha|^2\left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) = \frac{3}{4}|\alpha|^2 < |\alpha|^2. \end{aligned}$$

$|\alpha|^2$ の最小性から，$\delta = 0$ でなければならない．ゆえに，$\beta = \gamma\alpha \in (\alpha)$．これが任意の $\beta \in \mathfrak{a}$ について成り立つから，$\mathfrak{a} \subset (\alpha)$ である．$(\alpha) \subset \mathfrak{a}$ はすでに示されているから，$\mathfrak{a} = (\alpha)$ を得た．すなわち，$\mathfrak{a}$ は単項イデアルである． □

この環 $\mathcal{O}$ についても，定理 1.9 が成り立つ．

補題 2.6. $\mathfrak{p} = (1-\omega) = (1-\omega^2)$ は $\mathcal{O}$ は素イデアルであり，$\mathfrak{p}^2 = 3\mathcal{O}$ である．

[証明]

$$(1-\omega^2)\mathcal{O} = (1-\omega)(1+\omega)\mathcal{O} = (1-\omega)(-\omega^2)\mathcal{O} = (1-\omega)\mathcal{O}.$$

$\alpha, \beta \in \mathcal{O}$, $1-\omega = \alpha\beta$ とすれば,

$$3 = |1-\omega|^2 = |\alpha|^2|\beta|^2.$$

よって，正整数 $|\alpha|^2$, $|\beta|^2$ の一方は 3 で，他方は 1 である．$\alpha \in \mathcal{O}^\times$ または $\beta \in \mathcal{O}^\times$ である．すなわち，$1-\omega$ は既約元であり，命題 1.8 より，$\mathfrak{p} = (1-\omega)$ は素イデアルである．$\mathfrak{p}^2 = (1-\omega)(1-\omega)\mathcal{O} = (1-\omega)(1-\omega^2)\mathcal{O} = 3\mathcal{O}$ である． □

補題 2.7. $\alpha \in \mathcal{O}$, $\alpha \notin 2\mathcal{O}$ ならば，$\alpha^3 \equiv 1 \pmod{2\mathcal{O}}$ である．

[証明] $\alpha = a + b\omega$ とすると，$a \equiv 0, 1 \pmod 2$, $b \equiv 0, 1 \pmod 2$ より，$\alpha \notin 2\mathcal{O}$ は $\bmod 2\mathcal{O}$ で，$1, \omega, 1+\omega = -\omega^2$ と合同である．よって，α^3 は $\bmod 2\mathcal{O}$ で，$1^3 = 1$, $\omega^3 = 1$, $(-\omega)^3 = -1$ と合同である．$-1 \equiv 1 \pmod{2\mathcal{O}}$ であるから，補題が証明された． □

これらのことを使って，フェルマー予想の $n = 3$ の場合が証明される．

定理 2.8.

$$x^3 + y^3 = z^3, \quad xyz \neq 0$$

を満たす整数 x, y, z は存在しない．

[証明] $n = 3$ に対するフェルーマーの方程式

$$x^3 + y^3 = z^3$$

の整数解 x, y, z で，$xyz \neq 0$ となるものが存在したとする．$\max(|x|, |y|, |z|)$ が最小のものをとる．そのとき，x, y, z のどの 2 つも互いに素である．x, y, z すべて奇数となることはないから，x, y, z のうち偶数は 1 つで，奇数は 2 つである．x, y が奇数であり，z が偶数であるとしてよい．$\mathcal{O}$ において,

$$(x+y)(x+y\omega)(x+y\omega^2) = z^3 \tag{2.2}$$

と表せる．実際,

$$\begin{aligned}(x+y)(x+y\omega)(x+y\omega^2) &= (x+y)(x^2 + (\omega^2+\omega)xy + \omega^3 y^2) \\ &= (x+y)(x^2 - xy + y^2) = x^3 + y^3.\end{aligned}$$

z が 3 で割り切れないとき. $\mathcal{O}$ の元 $x+y$, $x+y\omega$, $x+y\omega^2$ は 2 つずつ互いに素である．実際，もし，既約元 α が $x+y$ と $x+y\omega$ を割り切ったとすると，差をとっ

て，$y(1-\omega)$ は α で割り切れる．よって，y または $1-\omega$ は α で割り切れる．y が α で割り切れるとき，$x=(x+y)-y$ も α で割り切れる．これは，x と y が互いに素であることに矛盾する．$1-\omega$ が α で割り切れるとすると，$1-\omega$ は既約元であるから，$\alpha=(1-\omega)\xi,\ \xi\in\mathcal{O}^\times$ である．そのとき，z^3 は $(\alpha)^2=3\mathcal{O}$ で割り切れる．これは z が 3 で割り切れないことに矛盾する．よって，$x+y$ と $x+y\omega$ は互いに素である．同様にして，$x+y$ と $x+y\omega^2$, $x+y\omega$ と $x+y\omega^2$ も互いに素であることがわかる．等式 (2.2) の両辺を既約元の積に分解して，定理 1.9 を適用すれば，$x+y=u\beta^3,\ u\in\mathcal{O}^\times,\ \beta\in\mathcal{O}$, $x+y\omega=v\alpha^3,\ v\in\mathcal{O}^\times,\ \alpha\in\mathcal{O}$ とかける．このとき，

$$(x+y)^2=|u\beta^3|^2=|u|^2(|\beta|^2)^3=(|\beta|^2)^3.$$

左辺は平方数であり，右辺は立方数であるから，これは 6 乗数であり，$x+y=c^3,\ c\in\mathbb{Z}$ とかける．また，x,y は奇数であるから，$x+y\omega\notin 2\mathcal{O}$ である．よって，$\alpha\notin 2\mathcal{O}$ であり，補題 2.7 より，$\alpha^3\equiv 1\pmod{2\mathcal{O}}$ である．

$$1+\omega\equiv x+y\omega\equiv v\pmod{2\mathcal{O}},$$

よって，$v=\pm\omega^2$ であり，$x+y\omega=\pm\omega^2\alpha^3$ である．必要なら，α をあらためて $-\alpha$ とかけば，$x+y\omega=-\omega^2\alpha^3$ である．この複素共役をとれば，$\bar{\omega}=\omega^2$ であるから，$x+y\omega^2=-\omega\bar{\alpha}^3$ である．$\pm\alpha=a+b\omega,\ a,b\in\mathbb{Z}$ とかけば，

$$\begin{aligned}\alpha^3=(a+b\omega)^3&=a^3+3a^2b\omega+3ab^2\omega^2+b^3=a^3+b^3-3ab^2+(3a^2b-3ab^2)\omega,\\ x+y\omega&=-(a^3+b^3-3ab^2)\omega^2-(3a^2b-3ab^2)\\ &=-(a^3+b^3-3ab^2)(-1-\omega)-(3a^2b-3ab^2)\\ &=a^3+b^3-3a^2b+(a^3+b^3-3ab^2)\omega.\end{aligned}$$

よって，$x=a^3+b^3-3a^2b,\ y=a^3+b^3-3ab^2$ である．したがって，

$$\begin{aligned}x+y&=2a^3+2b^3-3a^2b-3ab^2=2(a+b)(a^2-ab+b^2)-3ab(a+b)\\ &=(a+b)(2a^2-2ab+2b^2-3ab)=(a+b)(2a^2-5ab+2b^2)\\ &=(a+b)(2a-b)(a-2b).\end{aligned}$$

$x+y=c^3$ であったから，

$$(a+b)(2a-b)(a-2b)=c^3 \tag{2.3}$$

を得る．このとき，$a\neq 0,\ b\neq 0$ がわかる．a と b が公約数 $d>1$ を持てば，$x,\ y$ も d で割り切れてしまい，x と y が互いに素であることに矛盾する．よって，a と b は互いに素である．

$$(a+b)+(2a-b)=3a,\quad 2(a+b)-(2a-b)=3b$$

より，$a+b$ と $2a-b$ が公約数 $d>1$ を持てば，d は $3a$ と $3b$ を割り切る．よって，$d=3$ となるが，そのとき，$x+y=c^3$ が $d=3$ で割り切れ，$z^3=(x+y)(x^2-xy+y^2)$ も 3 で割り切れるが，z は 3 で割り切れないとしているので，矛盾である．ゆえに，$a+b$ と $2a-b$ は互いに素である．

$$2(a+b)+(a-2b)=3a,\quad (a+b)-(a-2b)=3b,$$

$$2(2a-b)-(a-2b)=3a,\quad (2a-b)-2(a-2b)=3b,$$

であるから，$a+b$ と $a-2b$ は互いに素であり，$2a-b$ と $a-2b$ も互いに素である．等式 (2.3) の両辺の素因数分解を考えれば，$a+b=x_1^3$, $2a-b=z_1^3$, $a-2b=y_1^3$, $x_1,y_1,z_1\in\mathbb{Z}$ が存在する．$c\neq 0$ より，$x_1y_1z_1\neq 0$ であり，

$$x_1^3+y_1^3=(a+b)+(a-2b)=2a-b=z_1^3$$

である．ここで，$\max(|x_1|,|y_1|,|z_1)<\max(|x|,|y|,|z|)$ であることを示せば，$\max(|x|,|y|,|z|)$ が最小であることに矛盾する．$x_1^3y_1^3z_1^3=c^3$,$x_1y_1z_1=c$ である．$\min(|x_1|,|y_1|,|z_1|)=1$ となることはない．実際，例えば，$z_1=1$ とすると，$x_1^3+y_1^3=1$ となるが，そのとき，$x_1+y\omega\in\mathcal{O}^\times$, $(x_1,y_1)=\pm(1,0),\pm(0,1),\pm(1,1)$ である．$x_1y_1\neq 0$ より，$(x_1,y_1)=\pm(1,1)$ であるが，これは $x_1^3+y_1^3=\pm 2$ となって矛盾である．他の場合も同様である．よって，$\min(|x_1|,|y_1|,|z_1|)\geq 2$ である．したがって，

$$|c|=|x_1||y_1||z_1|\geq\max(|x_1|,|y_1|,|z_1|)\min(|x_1|,|y_1|,|z_1|)^2\geq 4\max(|x_1|,|y_1|,|z_1|),$$

$$\begin{aligned}\max(|x_1|,|y_1|,|z_1|)&\leq\frac{1}{4}|c|<\frac{1}{4}|c|^3=\frac{1}{4}|x+y|\leq\frac{1}{4}(|x|+|y|)\\&\leq\frac{1}{2}\max(|x|,|y|,|z|)<\max(|x|,|y|,|z|).\end{aligned}$$

<u>z が 3 で割り切れるとき.</u> $\mathfrak{p}=(1-\omega)\mathcal{O}$ とおく．$\mathfrak{p}^2=3\mathcal{O}$ である．z は $\mathfrak{p}$ で割り切れるから，

$$(x+y)(x+y\omega)(x+y\omega^2)=z^3$$

と

$$x+y\omega\equiv x+y\omega^2\equiv x+y\pmod{\mathfrak{p}}$$

より，$x+y$, $x+y\omega$, $x+y\omega^2$ はすべて $\mathfrak{p}$ に属する．もし，$x+y\omega\in 3\mathcal{O}=\mathfrak{p}^2$ ならば，x,y ともに 3 で割り切れ，x と y が互いに素であることに矛盾する．よって，$x+y\omega\notin\mathfrak{p}^2$ である．同様に，$x+y\omega^2\notin\mathfrak{p}^2$ である．$z\in 3\mathcal{O}=\mathfrak{p}^2$ であるから，$x+y\in 3^n\mathbb{Z}$, $x+y\notin 3^{n+1}\mathbb{Z}$, $z\in 3^m\mathbb{Z}$, $z\notin 3^{m+1}\mathbb{Z}$ とすれば，

$$2n+1+1=6m\geq 6,$$

$n\geq 2$ である．よって，

$$x+y=9r,\quad x+y\omega=(1-\omega)\xi,\quad x+y\bar{\omega}=(1-\bar{\omega})\bar{\xi},$$

$r \in \mathbb{Z}, \xi \in \mathcal{O}$ とかける．$\bar{\omega} = \omega^2$ である．このとき，$27r|\xi|^2 = z^3$,

$$r\xi\bar{\xi} = \left(\frac{z}{3}\right)^3 \tag{2.4}$$

である．$r, \xi, \bar{\xi}$ のどの 2 つも互いに素であるから，等式 (2.4) の両辺を既約元の積に分解して，定理 1.9 を適用すれば，$r = c^3$, $c \in \mathbb{Z}$, $\xi = v\alpha^3$, $v \in \mathcal{O}^\times$, $\alpha \in \mathcal{O}$ とかける．$x+y = 9c^3$, $x+y\omega = (1-\omega)v\alpha^3$ である．x, y は奇数であるから，$x+y\omega \notin 2\mathcal{O}$ である．よって，$\alpha \notin 2\mathcal{O}$ であり，補題 2.7 より，$\alpha^3 \equiv 1 \pmod{2\mathcal{O}}$ である．したがって，

$$1 + \omega \equiv x + y\omega \equiv (1-\omega)v\alpha^3 \equiv (1-\omega)v \equiv (1+\omega)v \pmod{2\mathcal{O}}.$$

$1 + \omega = -\omega^2$ であるから，両辺に $-\omega$ をかければ，$1 \equiv v \pmod{2\mathcal{O}}$, $v = \pm 1$ である．$\pm\alpha = a + b\omega$, $a, b \in \mathbb{Z}$ とかけば，

$$x + y\omega = (1-\omega)(a+b\omega)^3 = (a^3 + b^3 + 3a^2b - 6ab^2) - (a^3 + b^3 - 6a^2b + 3ab^2)\omega,$$

$$x = a^3 + b^3 + 3a^2b - 6ab^2, \qquad y = -a^3 - b^3 + 6a^2b - 3ab^2.$$

したがって，

$$9c^3 = x + y = 9a^2b - 9ab^2 = 9ab(a-b),$$

$$ab(a-b) = c^3 \tag{2.5}$$

を得る．このとき，$z \neq 0$ より， $c \neq 0$, $a \neq 0$, $b \neq 0$, $a \neq b$ がわかる．a と b が公約数 $d > 1$ を持てば，x, y も d で割り切れてしまい，x と y が互いに素であることに矛盾する．よって，a と b は互いに素である．よって，a と $a-b$，b と $a-b$ も互いに素である．等式 (2.5) の両辺の素因数分解を考えれば，$a = z_1^3$, $b = x_1^3$, $a - b = y_1^3$, $x_1, y_1, z_1 \in \mathbb{Z}$ が存在する．$x_1y_1z_1 \neq 0$ であり，

$$x_1^3 + y_1^3 = b + a - b = a = z_1^3.$$

$x_1^3y_1^3z_1^3 = c^3$,$x_1y_1z_1 = c$ である．したがって，

$$|c| = |x_1||y_1||z_1| \geq \max(|x_1|, |y_1|, |z_1|) \min(|x_1|, |y_1|, |z_1|)^2 \geq \max(|x_1|, |y_1|, |z_1|),$$

$$\begin{aligned}\max(|x_1|, |y_1|, |z_1|) \leq |c| \leq |c|^3 = \frac{1}{9}|x+y| \leq \frac{1}{9}(|x| + |y|) \\ \leq \frac{2}{9}\max(|x|, |y|, |z|) < \max(|x|, |y|, |z|).\end{aligned}$$

以上によって，定理が証明された．

□

3　代数的整数

定義 3.1. 複素数 α が**代数的数**であるとは，ある多項式 $f(X) \in \mathbb{Q}[X]$，$\deg f \geq 1$ があって，$f(\alpha) = 0$ となることである．代数的数の全体を $\bar{\mathbb{Q}}$ とかく．

定義 3.2. 複素数 α が**代数的整数**であるとは，あるモニック多項式 (最高次の係数が 1 の多項式)

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X],\ n \geq 1$$

があって，$f(\alpha) = 0$ となることである．代数的整数の全体を $\bar{\mathbb{Z}}$ とかく．

命題 3.3. $\mathbb{Q} \cap \bar{\mathbb{Z}} = \mathbb{Z}$.

[証明]　$\mathbb{Z} \subset \mathbb{Q} \cap \bar{\mathbb{Z}}$ は明か．$\gamma \in \mathbb{Q} \cap \bar{\mathbb{Z}}$ とする．$\gamma = c/d$，$c, d \in \mathbb{Z}$，$d \geq 1$，$\gcd(c, d) = 1$ とする．$\gamma \in \bar{\mathbb{Z}}$ より，多項式

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X],\ n \geq 1$$

があって，$f(\gamma) = 0$ となる．すなわち，

$$\left(\frac{c}{d}\right)^n + a_1 \left(\frac{c}{d}\right)^{n-1} + \cdots + a_n = 0.$$

分母を払って，

$$c^n = -d(a_1 c^{n-1} + \cdots + a_n d^{n-1}).$$

これから，$d | c^n$．もし $d > 1$ ならば，$p | d$ なる素数 p をとれば，$p | c^n$，したがって，$p | c$ となり，$(c, d) = 1$ に矛盾する．ゆえに $d = 1$，すなわち，$\gamma \in \mathbb{Z}$ でなければならない．　□

命題 3.4. $\alpha \in \bar{\mathbb{Q}}$ に対して，ある自然数 a がとれて，$a\alpha \in \bar{\mathbb{Z}}$ になる．

[証明]　α は

$$\alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0 \quad (a_i \in \mathbb{Q}, n \geq 1)$$

をみたすとする．係数 a_i の分母の最小公倍数をかけて，

$$b_0 \alpha^n + b_1 \alpha^{n-1} + \cdots + b_n = 0 \quad (b_i \in \mathbb{Z},\ b_0 > 0).$$

さらに，b_0^{n-1} をかければ，

$$(b_0\alpha)^n + b_1 (b_0\alpha)^{n-1} + \cdots + b_0^{n-1} b_n = 0.$$

これは $b_0\alpha \in \bar{\mathbb{Z}}$ を示している．　□

補題 3.5. $\gamma_1, \ldots, \gamma_m$ を少なくとも一つは 0 でない複素数とし，

$$M = \left\{ \sum_{i=1}^{m} c_i \gamma_i \,\middle|\, c_i \in \mathbb{Z} \right\}$$

とおく．このとき，複素数 α が $\alpha M \subset M$ を満たせば，$\alpha \in \bar{\mathbb{Z}}$ である．

[証明]　仮定から

$$\alpha \gamma_i = \sum_{j=1}^{m} a_{ij} \gamma_j,\ a_{ij} \in \mathbb{Z}.$$

$A = (a_{ij})$ とおけば，

$$\alpha \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix} = A \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix}.$$

これは，α が整数成分の m 次行列 A の固有値であることを示している．したがって，α は A の固有多項式の根であり，固有多項式は m 次，整数係数，最高次の係数は 1 である． □

命題 3.6. $\bar{\mathbb{Z}}$ は $\mathbb{C}$ の部分環である．$\bar{\mathbb{Z}}$ を**代数的整数環**という．

[証明]　$\alpha, \beta \in \bar{\mathbb{Z}}$ とする．

$$\alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0,\ a_i \in \mathbb{Z},$$
$$\beta^m + b_1 \beta^{n-1} + \cdots + b_m = 0,\ b_j \in \mathbb{Z}$$

とする．

$$M = \left\{ \sum_{0 \le i \le n-1, 0 \le j \le m-1} c_{ij} \alpha^i \beta^j \,\middle|\, c_{ij} \in \mathbb{Z} \right\}$$

とおく．$\alpha M \subset M$，$\beta M \subset M$ が容易にわかる．これから，

$$(\alpha \pm \beta) M \subset \alpha M + \beta M \subset M + M \subset M,$$
$$\alpha\beta M = \alpha(\beta M) \subset \alpha M \subset M$$

となる．補題 3.5 によって，$\alpha \pm \beta, \alpha\beta \in \bar{\mathbb{Z}}$ を得る． □

補題 3.7. $\mathbb{Q}\bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}$.

[証明]　$\alpha \in \bar{\mathbb{Z}}$，$r \in \mathbb{Q}$，$r \neq 0$ とする．

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

とする．$\beta = r\alpha$ とおくと，$\alpha = \beta / r$ だから，

$$(\beta/r)^n + a_1 (\beta/r)^{n-1} + \cdots + a_n = 0,$$
$$(\beta)^n + a_1 r (\beta)^{n-1} + \cdots + a_n r^n = 0.$$

したがって，$\beta = r\alpha \in \bar{\mathbb{Q}}$ である． □

命題 3.8. $\bar{\mathbb{Q}}$ は $\mathbb{C}$ の部分体である．$\bar{\mathbb{Q}}$ を**代数的数体**という．

[証明] $\alpha, \beta \in \bar{\mathbb{Q}}$ をとる．命題 3.4 により，自然数 a, b で $a\alpha, b\beta \in \bar{\mathbb{Z}}$ となるものをとれる．$\mathbb{Z} \subset \bar{\mathbb{Z}}$ かつ，$\bar{\mathbb{Z}}$ は環だから $ab\alpha = b(a\alpha) \in \bar{\mathbb{Z}}$ である．同様に，$ab\beta = a(b\beta) \in \bar{\mathbb{Z}}$．したがって，

$$ab(\alpha \pm \beta) = ab\alpha \pm ab\beta \in \bar{\mathbb{Z}}.$$

補題 3.7 により

$$\alpha \pm \beta = \frac{1}{ab} ab(\alpha \pm \beta) \in \bar{\mathbb{Q}}.$$

また，$ab(\alpha\beta) = (a\alpha)(b\beta) \in \bar{\mathbb{Z}}$ だから，

$$\alpha\beta = \frac{1}{ab} ab(\alpha\beta) \in \bar{\mathbb{Q}}.$$

最後に，$\alpha \in \bar{\mathbb{Q}}$，$\alpha \neq 0$ ならば，α の満たす有理数係数の方程式

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \quad (a_0 \neq 0, a_n \neq 0)$$

の両辺に α^{-n} をかけて

$$a_0 + a_1(\alpha^{-1}) + \cdots + a_n(\alpha^{-1})^n = 0, \quad (a_0 \neq 0, a_n \neq 0)$$

を得るから，$\alpha^{-1} \in \bar{\mathbb{Q}}$ である． □

練習問題 3.1. α を 3 次方程式 $x^3 - x - 1 = 0$ の一つの根とする．このとき，$\gamma_1 = 1, \gamma_2 = \alpha, \gamma_3 = \alpha^2$,

$$M = \{c_1\gamma_1 + c_2\gamma_2 + c_3\gamma_3 \,|\, c_i \in \mathbb{Z}\}$$

とおけば，$\gamma_3 M \subset M$ であることを証明せよ．さらに，$\gamma_3 = \alpha^2$ の満たす整数係数の方程式を求めよ．

4 代数体

4.1 2 次体

定義 4.1. $\mathbb{Q} \subset k \subset \bar{\mathbb{Q}}$ を満たす体 k で，$\mathbb{Q}$ 上のベクトル空間として有限次元であるようなものを，**有限次代数体**という．以下，有限次代数体のことを単に代数体ということにする．$\dim_{\mathbb{Q}} k = [k : \mathbb{Q}]$ とかき，これを代数体 k の $\mathbb{Q}$ 上の**次数**という．$[k : \mathbb{Q}] = n$ のとき，k は n 次体であるという．

命題 4.2. $m \neq 0, 1$ を平方因数を持たない整数とする．このとき，

$$k = \mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \,|\, a, b \in \mathbb{Q}\}$$

とおけば，k は 2 次体である．逆に，すべての 2 次体はこのようにして得られる．

[証明]　$\mathbb{Q} \subset k$ は明らか．$\alpha = a + b\sqrt{m},\ a, b \in \mathbb{Q}$ とおけば，

$$(\alpha - a)^2 = b^2 m, \quad \alpha^2 - 2a\alpha + a^2 - b^2 m = 0.$$

したがって，$\alpha \in \bar{\mathbb{Q}},\ k \subset \bar{\mathbb{Q}}$ である．k が環であることはあきらか．$a + b\sqrt{m} = 0 \Longleftrightarrow a = b = 0$ だから，$\alpha = a + b\sqrt{m} \neq 0$ のとき，$\alpha' = a - b\sqrt{m} \neq 0$. したがって，$r = \alpha\alpha' = a^2 - mb^2 \neq 0$ である．ゆえに，

$$\frac{1}{\alpha} = \frac{\alpha'}{r} = \frac{a}{a^2 - mb^2} - \frac{b}{a^2 - mb^2}\sqrt{m} \in k.$$

すなわち，k は体である．$\dim_{\mathbb{Q}} k = 2$ も明らかであるから，k は 2 次体である．
逆に，k を 2 次体とする．$\alpha \in k,\ \alpha \notin \mathbb{Q}$ をとる．そのとき，$1, \alpha$ は $\mathbb{Q}$ 上 1 次独立である．また，$\dim_{\mathbb{Q}} k = 2$ であるから，$1, \alpha, \alpha^2$ は $\mathbb{Q}$ 上 1 次従属である．よって，$r, s \in \mathbb{Q}$ が存在して，$\alpha^2 + r\alpha + s = 0$ である．$\alpha \notin \mathbb{Q}$ より，$D = r^2 - 4s$ とけば，D は有理数の平方ではない．したがって，$D = t^2 m,\ m \in \mathbb{Z},\ m \neq 0, 1$ は平方因数を持たない，$t \in \mathbb{Q}^\times$ とかける．そのとき，$\alpha = (-a \pm t\sqrt{m})/2 \in \mathbb{Q}(\sqrt{m})$ であり，$k \subset \mathbb{Q}(\sqrt{m})$ である．$2 = \dim_{\mathbb{Q}} k \leq \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{m}) = 2$ より，$k = \mathbb{Q}(\sqrt{m})$. □

定義 4.3. $k = \mathbb{Q}(\sqrt{m})$ を 2 次体とする．$\alpha = a + b\sqrt{m} \in k$ に対して，$\alpha' = a - b\sqrt{m}$ を α の**共役**という．$\alpha, \beta \in k$ とすると，

$$(\alpha + \beta)' = \alpha' + \beta', \quad (\alpha\beta)' = \alpha'\beta' \tag{4.1}$$

が成り立つ．共役を用いて，

$$\begin{aligned} \mathrm{Tr}_{k/\mathbb{Q}}(\alpha) &= \alpha + \alpha' = 2a, \\ \mathrm{N}_{k/\mathbb{Q}}(\alpha) &= \alpha\alpha' = a^2 - b^2 m \end{aligned}$$

とおく．$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha),\ \mathrm{N}_{k/\mathbb{Q}}(\alpha)$ は有理数である．写像 $\mathrm{Tr}_{k/\mathbb{Q}} : k \longrightarrow \mathbb{Q},\ \mathrm{N}_{k/\mathbb{Q}} : k \longrightarrow \mathbb{Q}$ をそれぞれ k の**トレース**，**ノルム**という．明らかに，トレースは k から $\mathbb{Q}$ への $\mathbb{Q}$-線形写像であり，ノルムの $k^\times$ への制限は，乗法群 $k^\times$ から乗法群 $\mathbb{Q}^\times$ への準同型である．

定義 4.4. 代数体 k に対して，$\mathcal{O}_k = k \cap \bar{\mathbb{Z}}$ とおけば，$\mathbb{Z} \subset \mathcal{O}_k \subset \bar{\mathbb{Z}}$ であり，$\mathcal{O}_k$ は $\bar{\mathbb{Z}}$ の部分環である．$\mathcal{O}_k$ を k の**整数環**という．

補題 4.5. $k = \mathbb{Q}(\sqrt{m})$ を 2 次体とする．ここで，$m \neq 0, 1$ は平方因数を持たない整数とする．$\alpha \in k$ について，

$$\alpha \in \mathcal{O}_k \Longleftrightarrow \mathrm{Tr}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Z},\ \mathrm{N}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Z}$$

が成り立つ．

[証明]　$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, $\mathrm{N}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ とすると，α は

$$X^2 - \mathrm{Tr}_{k/\mathbb{Q}}(\alpha)X + \mathrm{N}_{k/\mathbb{Q}}(\alpha) = 0$$

の根であるから，$\alpha \in k \cap \bar{\mathbb{Z}} = \mathcal{O}_k$ である．逆に，$\alpha \in \mathcal{O}_k$ とし，

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0 \quad a_i \in \mathbb{Z}$$

とする．そのとき，等式 (4.1) より，

$$\begin{aligned} 0 &= (\alpha^n + a_1\alpha^{n-1} + \cdots + a_n)' \\ &= (\alpha^n)' + (a_1\alpha^{n-1})' + \cdots + (a_n)' \\ &= (\alpha')^n + a_1(\alpha')^{n-1} + \cdots + a_n \end{aligned}$$

したがって，$\alpha' \in \bar{\mathbb{Z}}$ である．命題 3.6 より，$\alpha + \alpha' \in \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$, $\alpha\alpha' \in \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ である．□

命題 4.6. $k = \mathbb{Q}(\sqrt{m})$ を 2 次体とする．ただし，$m \neq 0, 1$ は平方因数を持たない整数とする．そのとき，$\mathcal{O}_k = \{a + b\omega \,|\, a, b \in \mathbb{Z}\}$ である．ここで，

$$\omega = \begin{cases} \dfrac{1+\sqrt{m}}{2}, & m \equiv 1 \pmod 4, \\ \sqrt{m}, & m \equiv 2, 3 \pmod 4. \end{cases}$$

[証明]　$\sqrt{m}$ は $X^2 - m = 0$ の根であるから，$\sqrt{m} \in k \cap \bar{\mathbb{Z}} = \mathcal{O}_k$ である．また，$m \equiv 1 \pmod 4$ ならば，$\omega = (1 + \sqrt{m})/2$ は，$X^2 - X + (1 - m)/4 = 0$ の根であり，これは $\mathbb{Z}$-係数であるから，$\omega \in k \cap \bar{\mathbb{Z}} = \mathcal{O}_k$ である．したがって，いずれの場合も，$\omega \in \mathcal{O}_k$ であり，$\mathcal{O}_k$ は環であるから，$a + b\omega \in \mathcal{O}_k$, $a, b \in \mathbb{Z}$ である．

$\alpha = x + y\sqrt{m}$, $x, y \in \mathbb{Q}$ とおく．$\alpha \in \mathcal{O}_k$ とすると，補題 4.5 より，$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha) = 2x \in \mathbb{Z}$, $\mathrm{N}_{k/\mathbb{Q}}(\alpha) = x^2 - my^2 \in \mathbb{Z}$ である．$2x = x_1 \in \mathbb{Z}$ とおく．$4x^2 - 4my^2 \in 4\mathbb{Z}$ より，$x_1^2 - m(2y)^2 \in \mathbb{Z}$, したがって，$2y = y_1$ とおけば，$my_1^2 \in \mathbb{Z}$ である．m は平方因数を持たないから，$y_1 \in \mathbb{Z}$ を得る．よって，$\alpha = \dfrac{x_1 + y_1\sqrt{m}}{2}$, $x_1, y_1 \in \mathbb{Z}$ とかける．そのとき，$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha) = x_1 \in \mathbb{Z}$ であるから，$\mathrm{N}_{k/\mathbb{Q}}(\alpha) = \dfrac{x_1^2 - my_1^2}{4} \in \mathbb{Z}$, すなわち，

$$x_1^2 - my_1^2 \equiv 0 \pmod 4 \tag{4.2}$$

ならば，$\alpha \in \mathcal{O}_k$ である．$m \equiv 1 \pmod 4$ のとき，合同式 (4.2) は，$x_1^2 - y_1^2 \equiv 0 \pmod 4$ になり，これは，$x_1 \equiv y_1 \pmod 2$ と同値である．$y_1 = b$, $x_1 = b + 2a$, $a, b \in \mathbb{Z}$ とかけば，$\alpha = \dfrac{b + 2a + b\sqrt{m}}{2} = a + b\omega$ である．$m \equiv 2 \pmod 4$ のとき，合同式 (4.2) は，$x_1^2 - 2y_1^2 \equiv 0 \pmod 4$ になり，これから，x_1 は偶数，したがって，y_1 も偶数がわかる．$m \equiv 3 \pmod 4$ のとき，合同式 (4.2) は，$x_1^2 - 3y_1^2 \equiv 0 \pmod 4$, $x_1^2 + y_1^2 \equiv 0 \pmod 4$ になり，これから，x_1, y_1 ともに偶数がわかる．$x_1 = 2a$, $y_1 = 2b$, $a, b \in \mathbb{Z}$ とかけば，$\alpha = a + b\sqrt{m} = a + b\omega$ である．□

$\mathcal{O}_k$ の $\mathbb{Z}$ 上の基底 $1, \omega$ を k の**整数底**という．

4.2 原始元の存在

定義 4.7. $\alpha \in \bar{\mathbb{Q}}$ とするとき，α を含む最小の代数体を $\mathbb{Q}(\alpha)$ で表す．α を根とする $\mathbb{Q}$ 係数のモニック多項式で次数が最小のものを α の $\mathbb{Q}$ 上の**最小多項式**という．$\alpha_1, \ldots, \alpha_n \in \bar{\mathbb{Q}}$ とするとき，$\alpha_1, \ldots, \alpha_n$ を含む最小の代数体を $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ で表す．

命題 4.8. $\alpha \in \bar{\mathbb{Q}}$, $f(X)$ を α の $\mathbb{Q}$ 上の最小多項式とすると，$f(X)$ は $\mathbb{Q}$ 上既約であり，重根を持たない．

[証明] $n = \deg f(X)$ とする．$f(X) = g(X)h(X)$, $g(X), h(X) \in \mathbb{Q}[X]$ はモニックとすれば，

$$0 = f(\alpha) = g(\alpha)h(\alpha)$$

より，$g(\alpha) = 0$ または $h(\alpha) = 0$ である．$f(X)$ は $f(\alpha) = 0$ となる $\mathbb{Q}[X]$ の元で次数が最小のものであるから，$g(X) = f(X)$ または $h(X) = f(X)$ である．ゆえに，$f(X)$ は既約である．$f'(X)$ は $n-1$ 次多項式だから $\mathbb{Q}$ 上既約な n 次多項式 $f(X)$ で割り切れない．よって，系 0.15 より，

$$a(X)f(X) + b(X)f'(X) = 1$$

となる $a(X), b(X) \in \mathbb{Q}[X]$ が存在する．したがって，$f(X)$ と $f'(X)$ は共通の根を持たない．ゆえに，$f(X)$ は重根を持たない． □

命題 4.9. $\alpha \in \bar{\mathbb{Q}}$, $f(X)$ を α の $\mathbb{Q}$ 上の最小多項式，$n = \deg f(X)$ とすれば，$f(X)$ は $\mathbb{Q}$ 上既約であり，$\mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/f(X)\mathbb{Q}[X]$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ である．また，$1, \alpha, \ldots, \alpha^{n-1}$ は $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 上の基底である．

[証明] α と $\mathbb{Q}$ を含む $\bar{\mathbb{Q}}$ の最小の部分環を $\mathbb{Q}[\alpha]$ とする．写像 $\varphi : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[\alpha]$ を

$$\varphi(g(X)) = g(\alpha), \qquad g(X) \in \mathbb{Q}[X]$$

によって定義すれば，φ は環の全射準同型である．$\ker\varphi$ は $\mathbb{Q}[X]$ のイデアルである．命題 0.10 より，$f_0(X) \in \mathbb{Q}[X]$ が存在して，$\ker\varphi = f_0(X)\mathbb{Q}[X]$ であるが，この $f_0(X)$ はモニックとしてよく，そのとき，$f_0(X)$ は α の $\mathbb{Q}$ 上の最小多項式 $f(X)$ に等しい．準同型定理によって，

$$\mathbb{Q}[X]/f(X)\mathbb{Q}[X] \cong \mathbb{Q}[\alpha]$$

である．$\beta \in \mathbb{Q}[\alpha]$, $\beta \neq 0$ とすると，$\beta = g(\alpha)$, $g(X) \in \mathbb{Q}[X]$, $g(X) \notin \ker\varphi = f(X)\mathbb{Q}[X]$ とかける．系 0.15 より，

$$a(X)f(X) + b(X)g(X) = 1$$

となる $a(X), b(X) \in \mathbb{Q}[X]$ が存在する．これに，$x = \alpha$ を代入すれば，

$$b(\alpha)g(\alpha) = 1.$$

ゆえに，$\beta \in (\mathbb{Q}[\alpha])^\times$ であり，$\mathbb{Q}[\alpha]$ は体である．よって，$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ である．また，任意の $\beta = g(\alpha) \in \mathbb{Q}[\alpha]$ は，$g(X) = f(X)q(X) + r(X)$, $q(X), r(X) \in \mathbb{Q}[X]$,

$$r(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}, \quad c_0, c_1, \ldots, c_{n-1} \in \mathbb{Q}$$

とかけば，$\beta = r(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$ である．また，

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0$$

となるのは，$r(X) \in \ker\varphi = f(X)\mathbb{Q}[X]$ のときであるから，$\deg r(X) < n$ より，$r(X) = 0$, $c_0 = c_1 = \cdots = c_{n-1} = 0$ のときである．ゆえに，$1, \alpha, \ldots, \alpha^{n-1}$ は $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 上の基底であり，$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = n$ である． □

補題 4.10. $\alpha, \beta \in \bar{\mathbb{Q}}$ とすると，$\gamma \in \mathbb{Q}(\alpha, \beta)$ で $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$ となるものが存在する．

[証明] $f(X)$ を α の $\mathbb{Q}$ 上の最小多項式，$g(X)$ を β の $\mathbb{Q}$ 上の最小多項式とする．命題 4.8 より，$f(X)$, $g(X)$ は重根を持たない．$f(X)$ の根を $\alpha_1(= \alpha), \alpha_2, \ldots, \alpha_r$, $g(X)$ の根を $\beta_1(= \beta), \beta_2, \ldots, \beta_s$ とする．未知数 t の $(r-1)s$ 個の 1 次方程式

$$t\alpha_i + \beta_j = t\alpha + \beta \qquad (1 < i \leq r,\ 1 \leq j \leq s)$$

の根は高々 $(r-1)s$ 個であるから，$c \in \mathbb{Q}$ を

$$c\alpha_i + \beta_j \neq c\alpha + \beta \qquad (1 < i \leq r,\ 1 \leq j \leq s)$$

を満たすようにとれる．そのとき，$\gamma = c\alpha + \beta$ とおけば，$\mathbb{Q}(\gamma) \subset \mathbb{Q}(\alpha, \beta)$ である．逆向きの包含関係を示す．$h(X) = g(\gamma - cX)$ とおく．$c \neq 0$ であるから，$\deg h(X) = \deg g(X) = s$ である．$h(X) \in \mathbb{Q}(\gamma)[X]$ であり，

$$h(\alpha) = g(\gamma - c\alpha) = g(\beta) = 0$$

である．$f(X)$ と $h(X)$ は共通の根 α を持つ．もし，α_i, $i > 1$ が $h(X)$ の根であるとすると，

$$h(\alpha_i) = g(\gamma - c\alpha_i) = 0$$

より，ある $1 \leq j \leq s$ について $\gamma - c\alpha_i = \beta_j$ が成り立つ．しかし，これは $c\alpha + \beta = c\alpha_i + \beta_j$ となって，c のとり方に矛盾する．ゆえに，$f(X)$ と $h(X)$ は共通の根 α だけである．$f(X)$ と $h(X)$ の $\mathbb{Q}(\gamma)[X]$ における最大公約因子を $m(X)$, $m(X)$ はモニックとすれば，系 0.14 より，

$$a(X)f(X) + b(X)h(X) = m(X)$$

となる $a(X), b(X) \in \mathbb{Q}(\gamma)[X]$ が存在する．$m(X) \in \mathbb{Q}(\gamma)[X]$ は $f(X)$, $h(X)$ を割り切るから，$m(X)$ の根は $f(X)$ と $h(X)$ は共通の根 α だけである．ゆえに，$m(X)$ は1次であり，$m(X) = X - \alpha$ である．よって，$\alpha \in \mathbb{Q}(\gamma)$ である．$\beta = \gamma - c\alpha \in \mathbb{Q}(\gamma)$ であるから，$\mathbb{Q}(\alpha, \beta) \subset \mathbb{Q}(\gamma)$ である．したがって，$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$ である． □

定理 4.11. k を代数体とすれば，$\theta \in k$ が存在して，$k = \mathbb{Q}(\theta)$ である．

[証明] $n = [k : \mathbb{Q}]$ とおく．$\alpha_1, \ldots, \alpha_n$ を k の $\mathbb{Q}$ 上の基底とすると，

$$k = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$$

である．補題 4.10 より，$\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\gamma_2)$ となる $\gamma_2 \in k$ がとれ，

$$k = \mathbb{Q}(\gamma_2, \alpha_3, \ldots, \alpha_n)$$

となる．同様に，$\mathbb{Q}(\gamma_2, \alpha_3) = \mathbb{Q}(\gamma_3)$ となる $\gamma_3 \in k$ がとれ，

$$k = \mathbb{Q}(\gamma_3, \alpha_4, \ldots, \alpha_n)$$

となる．これを繰り返せば，$\gamma_n \in k$ がとれ，$k = \mathbb{Q}(\gamma_n)$ となる．$\gamma_n = \theta$ とすればよい． □

定理 4.11 の θ を k の**原始元**という．

4.3 共役写像

定義 4.12. $k = \mathbb{Q}(\theta)$ を n 次体とする．θ の $\mathbb{Q}$ 上の最小多項式を $f(X)$ とし，$f(X)$ の根を $\theta_1(= \theta), \theta_2, \ldots, \theta_n$ とする．$\alpha \in k$ を

$$\alpha = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}, \qquad c_j \in \mathbb{Q}$$

とかくとき，$1 \leq i \leq n$ に対して，写像 $\sigma_i : k \longrightarrow \bar{\mathbb{Q}}$ を

$$\sigma_i(\alpha) = c_0 + c_1\theta_i + \cdots + c_{n-1}\theta_i^{n-1}$$

によって定義する．σ_i を**共役写像**といい，$\alpha^{(i)} = \sigma_i(\alpha)$ とおくとき，$\alpha^{(1)}, \ldots, \alpha^{(n)}$ を α の $\mathbb{Q}$ 上の**共役**という．

命題 4.13. $k = \mathbb{Q}(\theta)$ を n 次体とする．共役写像 $\sigma_i : k \longrightarrow \bar{\mathbb{Q}}$ は単射準同型である．すなわち，$\alpha, \beta \in k$ に対して，

$$\sigma_i(\alpha + \beta) = \sigma_i(\alpha) + \sigma_i(\beta), \qquad \sigma_i(\alpha\beta) = \sigma_i(\alpha)\sigma_i(\beta)$$

が成り立つ．

[証明]　θ の $\mathbb{Q}$ 上の最小多項式を $f(X)$ とし，$f(X)$ の根を $\theta_1(=\theta), \theta_2, \ldots, \theta_n$ とする．命題 4.8 より，$f(X)$ は重根を持たないから，$\theta_1, \theta_2, \ldots, \theta_n$ は相異なる．$\{u_1, \ldots, u_n\}$ を k の $\mathbb{Q}$ 上の基底とする．各 $\alpha \in k$ に対して，αu_i を $u_1, \ldots, u_n$ の $\mathbb{Q}$ 係数 1 次結合として表すことによって，

$$\alpha \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = A_\alpha \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

となる $\mathbb{Q}$ を成分とする n 次行列 A_α が定まる．そのとき，$\alpha, \beta \in k$, $c \in \mathbb{Q}$ に対して，

$$A_{\alpha+\beta} = A_\alpha + A_\beta, \quad A_{c\alpha} = cA_\alpha, \quad A_{\alpha\beta} = A_\alpha A_\beta = A_\beta A_\alpha \tag{4.3}$$

が成り立つことが容易にわかる．一方，

$$\theta \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = A_\theta \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

より，θ は $\mathbb{Q}$ 係数の n 次行列 A_θ の固有値である．よって，θ は A_θ の固有多項式 $f_{A_\theta}(X)$ の根である．$f_{A_\theta}(X) \in \mathbb{Q}[X]$ は θ の $\mathbb{Q}$ 上の最小多項式で割り切れるが，$f_{A_\theta}(X)$, $f(X)$ はともに n 次モニックであるから，$f_{A_\theta}(X) = f(X)$ である．したがって，A_θ は $f(X)$ の根 $\theta_1, \ldots, \theta_n$ を相異なる固有値として持ち，対角化可能である．A_θ の固有値 θ_i の固有ベクトルを第 i 列の列ベクトルとする n 次行列を P とすれば，

$$P^{-1}A_\theta P = \begin{pmatrix} \theta_1 & & & \\ & \theta_2 & & \\ & & \ddots & \\ & & & \theta_n \end{pmatrix}.$$

$\alpha \in k$ を

$$\alpha = g(\theta), \quad g(X) = c_0 + c_1 X + \cdots + c_{n-1}X^{n-1}, \qquad c_j \in \mathbb{Q}$$

とかくとき，(4.3) より，

$$A_\alpha = \sum_{j=0}^{n-1} c_j A_\theta^j$$

である．よって，

$$P^{-1}A_\alpha P = \sum_{j=0}^{n-1} c_j P^{-1}A_\theta^j P = \sum_{j=0}^{n-1} c_j (P^{-1}A_\theta P)^j.$$

$$(P^{-1}A_\theta P)^j = \begin{pmatrix} \theta_1^j & & & \\ & \theta_2^j & & \\ & & \ddots & \\ & & & \theta_n^j \end{pmatrix},$$

であるから,

$$P^{-1}A_\alpha P = \begin{pmatrix} g(\theta_1) & & & \\ & g(\theta_2) & & \\ & & \ddots & \\ & & & g(\theta_n) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) & & & \\ & \sigma_2(\alpha) & & \\ & & \ddots & \\ & & & \sigma_n(\alpha) \end{pmatrix}.$$

$\beta \in k$ とすれば, 同様にして,

$$P^{-1}A_\beta P = \begin{pmatrix} \sigma_1(\beta) & & & \\ & \sigma_2(\beta) & & \\ & & \ddots & \\ & & & \sigma_n(\beta) \end{pmatrix},$$

$$P^{-1}A_{\alpha+\beta}P = \begin{pmatrix} \sigma_1(\alpha+\beta) & & & \\ & \sigma_2(\alpha+\beta) & & \\ & & \ddots & \\ & & & \sigma_n(\alpha+\beta) \end{pmatrix},$$

$$P^{-1}A_{\alpha\beta}P = \begin{pmatrix} \sigma_1(\alpha\beta) & & & \\ & \sigma_2(\alpha\beta) & & \\ & & \ddots & \\ & & & \sigma_n(\alpha\beta) \end{pmatrix}.$$

(4.3) より,

$$\begin{aligned} P^{-1}A_{\alpha+\beta}P &= P^{-1}(A_\alpha + A_\beta)P = P^{-1}A_\alpha P + P^{-1}A_\beta P \\ &= \begin{pmatrix} \sigma_1(\alpha)+\sigma_1(\beta) & & & \\ & \sigma_2(\alpha)+\sigma_2(\beta) & & \\ & & \ddots & \\ & & & \sigma_n(\alpha)+\sigma_n(\beta) \end{pmatrix} \end{aligned}$$

$$\begin{aligned} P^{-1}A_{\alpha\beta}P &= P^{-1}A_\alpha A_\beta P = (P^{-1}A_\alpha P)(P^{-1}A_\beta P) \\ &= \begin{pmatrix} \sigma_1(\alpha)\sigma_1(\beta) & & & \\ & \sigma_2(\alpha)\sigma_2(\beta) & & \\ & & \ddots & \\ & & & \sigma_n(\alpha)\sigma_n(\beta) \end{pmatrix}. \end{aligned}$$

これらの対角成分を比較すれば,

$$\sigma_i(\alpha+\beta)=\sigma_i(\alpha)+\sigma_i(\beta),\qquad \sigma_i(\alpha\beta)=\sigma_i(\alpha)\sigma_i(\beta).$$

$\sigma_i(1)=1$ であるから，$\alpha\neq 0$ ならば,

$$\sigma_i(\alpha)\sigma_i(\alpha^{-1})=\sigma_i(\alpha\alpha^{-1})=\sigma_i(1)=1.$$

よって，$\sigma_i(\alpha)\neq 0$ である．したがって，$\ker\sigma_i=\{0\}$ であり，σ_i は単射である． □

4.4 ノルムとトレース

定義 4.14. k を n 次代数体とする．$\sigma_i : k\longrightarrow\bar{\mathbb{Q}}$ を $(i=1,\ldots,n)$ を共役写像とする．$\alpha\in k$ に対して,

$$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha)=\sum_{i=1}^{n}\sigma_i(\alpha),$$
$$\mathrm{N}_{k/\mathbb{Q}}(\alpha)=\prod_{i=1}^{n}\sigma_i(\alpha)$$

とおく．$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha)$ を α の k から $\mathbb{Q}$ への**トレース**といい，$\mathrm{N}_{k/\mathbb{Q}}(\alpha)$ を α の k から $\mathbb{Q}$ への**ノルム**という.

定義 4.15. n 次行列 $A=(a_{ij})$ に対して，その対角成分の和

$$\sum_{i=1}^{n}a_{ii}$$

を行列 A の**トレース**といい，$\mathrm{Tr}(A)$ で表す.

補題 4.16. n 次行列 A,B に対して，$\mathrm{Tr}(AB)=\mathrm{Tr}(BA)$ である.

[証明]　AB の (i,i)-成分は $\sum_{j=1}^{n}a_{ij}b_{ji}$ であるから,

$$\mathrm{Tr}(AB)=\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}b_{ji}.$$

同様に，BA の (j,j)-成分は $\sum_{i=1}^{n}b_{ji}a_{ij}$ であるから,

$$\mathrm{Tr}(BA)=\sum_{j=1}^{n}\sum_{i=1}^{n}b_{ji}a_{ij}=\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}b_{ji}=\mathrm{Tr}(AB).$$

□

命題 4.17. k を n 次代数体とし，$\{u_1, \ldots, u_n\}$ を k の $\mathbb{Q}$ 上の基底とする．$\alpha \in k$ に対して，

$$\alpha \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = A_\alpha \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

となる $\mathbb{Q}$ を成分とする n 次行列 A_α が定まる．そのとき，

$$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha) = \mathrm{Tr}(A_\alpha), \qquad \mathrm{N}_{k/\mathbb{Q}}(\alpha) = \det A_\alpha$$

が成り立つ．特に，$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Q}$, $\mathrm{N}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Q}$ である．

[証明]　$\sigma_i : k \longrightarrow \bar{\mathbb{Q}}$ $(i = 1, \ldots, n)$ を共役写像とする．命題 4.13 の証明でみたように，

$$P^{-1}A_\alpha P = \begin{pmatrix} \sigma_1(\alpha) & & & \\ & \sigma_2(\alpha) & & \\ & & \ddots & \\ & & & \sigma_n(\alpha) \end{pmatrix}.$$

したがって，補題 4.16 より，

$$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) = \mathrm{Tr}((P^{-1}A_\alpha)P) = \mathrm{Tr}(P(P^{-1}A_\alpha)) = \mathrm{Tr}(A_\alpha),$$
$$\mathrm{N}_{k/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \det(P^{-1}A_\alpha P) = (\det P^{-1})(\det A_\alpha)(\det P) = \det A_\alpha.$$

□

命題 4.18. トレースは k から $\mathbb{Q}$ への $\mathbb{Q}$-線形写像であり，ノルムの $k^\times$ への制限は，乗法群 $k^\times$ から乗法群 $\mathbb{Q}^\times$ への準同型である．

[証明]　$\alpha, \beta \in k$, $c \in \mathbb{Q}$ とすると，命題 4.13 より，

$$\begin{aligned}
\mathrm{Tr}_{k/\mathbb{Q}}(\alpha+\beta) &= \sum_{i=1}^{n} \sigma_i(\alpha+\beta) = \sum_{i=1}^{n} (\sigma_i(\alpha) + \sigma_i(\beta)) \\
&= \sum_{i=1}^{n} \sigma_i(\alpha) + \sum_{i=1}^{n} \sigma_i(\beta) = \mathrm{Tr}_{k/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{k/\mathbb{Q}}(\beta), \\
\mathrm{Tr}_{k/\mathbb{Q}}(c\alpha) &= \sum_{i=1}^{n} \sigma_i(c\alpha) = \sum_{i=1}^{n} c\sigma_i(\alpha) = c\sum_{i=1}^{n} \sigma_i(\alpha) = c\,\mathrm{Tr}_{k/\mathbb{Q}}(\alpha), \\
\mathrm{N}_{k/\mathbb{Q}}(\alpha\beta) &= \prod_{i=1}^{n} \sigma_i(\alpha\beta) = \prod_{i=1}^{n} \sigma_i(\alpha)\sigma_i(\beta) \\
&= \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)\left(\prod_{i=1}^{n} \sigma_i(\beta)\right) = \mathrm{N}_{k/\mathbb{Q}}(\alpha)\,\mathrm{N}_{k/\mathbb{Q}}(\beta).
\end{aligned}$$

□

代数体 k に対して，$k=\mathbb{Q}(\theta)$ となる θ をとって，$f_\theta(X)$ を θ の $\mathbb{Q}$ 上の最小多項式，$\theta_1(=\theta),\dots,\theta_n$ を $f_\theta(X)$ の根の全体とする．共役写像 $\sigma_i : k \longrightarrow \bar{\mathbb{Q}}$ $(i=1,\dots,n)$ を

$$\alpha = g(\theta), \quad g(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$$

に対して，

$$\sigma_i(\alpha) = g(\theta_i)$$

によって定義した．これは θ のとり方に依存するようにみえる．そこで，$k=\mathbb{Q}(\rho)$ となる ρ をとって，$f_\rho(X)$ を ρ の $\mathbb{Q}$ 上の最小多項式，$\rho_1(=\rho),\dots,\rho_n$ を $f_\rho(X)$ の根の全体とし，共役写像 $\tau_i : k \longrightarrow \bar{\mathbb{Q}}$ $(i=1,\dots,n)$ を

$$\alpha = h(\rho), \quad h(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$$

に対して，

$$\tau_i(\alpha) = h(\rho_i)$$

によって定義する．このとき，適当に番号をつけかえれば，$\tau_i=\sigma_i$ であることを示そう．そのために，$\{u_1,\dots,u_n\}$ を k の $\mathbb{Q}$ 上の基底として，各 $\alpha\in k$ に対して，

$$\alpha \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = A_\alpha \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

となる $\mathbb{Q}$ 係数の n 次行列 A_α をとる．これは θ,ρ と無関係に定まる．特に，$\alpha=\rho$ とすれば，命題 4.13 の証明でみたように，

$$P^{-1}A_\rho P = \begin{pmatrix} \sigma_1(\rho) & & & \\ & \sigma_2(\rho) & & \\ & & \ddots & \\ & & & \sigma_n(\rho) \end{pmatrix}.$$

一方，A_ρ の固有多項式は ρ の $\mathbb{Q}$ 上の最小多項式 $f_\rho(X)$ と一致するから，A_ρ の固有値は $\rho_1(=\rho),\rho_2,\dots,\rho_n$ である．したがって，$j_1,j_2,\dots,j_n$ を $1,2,\dots,n$ の適当な並べ替えとすれば，$\sigma_i(\rho)=\rho_{j_i}$ $(i=1,\dots,n)$ である．このとき，

$$\alpha = h(\rho), \quad h(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$$

に対して，

$$\begin{aligned} \tau_{j_i}(\alpha) &= h(\rho_{j_i}) = c_0 + c_1\rho_{j_i} + \cdots + c_{n-1}\rho_{j_i}^{n-1} \\ &= c_0 + c_1\sigma_i(\rho) + \cdots + c_{n-1}\sigma_i(\rho)^{n-1} \\ &= \sigma_i(c_0 + c_1\rho + \cdots + c_{n-1}\rho^{n-1}) = \sigma_i(h(\rho)) \\ &= \sigma_i(\alpha). \end{aligned}$$

ゆえに，$\sigma_i = \tau_{j_i}$ である．以上によって，共役写像の全体 $\{\sigma_1, \ldots, \sigma_n\}$ は $k = \mathbb{Q}(\theta)$ となる θ のとり方にはよらないことが示された．

命題 4.19. k を代数体，$\mathcal{O}_k$ を k の整数環，$\alpha \in \mathcal{O}_k$ とすれば，$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, $\mathrm{N}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ である．

[証明]　$\alpha \in \mathcal{O}_k$ とすれば，モニックな $h(X) \in \mathbb{Z}[X]$ で，$h(\alpha) = 0$ となるものがある．$n = [k : \mathbb{Q}]$ とし，$\sigma_i : k \longrightarrow \bar{\mathbb{Q}}$ $(i = 1, \ldots, n)$ を共役写像とする．

$$h(X) = X^m + a_1 X^{m-1} + \cdots + a_m, \qquad a_j \in \mathbb{Z}$$

とすれば，

$$h(\alpha) = \alpha^m + a_1 \alpha^{m-1} + \cdots + a_m = 0.$$

σ_i は準同型であるから，

$$0 = \sigma_i(0) = \sigma_i(\alpha^m + a_1 \alpha^{m-1} + \cdots + a_m) = \sigma_i(\alpha)^m + a_1 \sigma_i(\alpha)^{m-1} + \cdots + a_m.$$

すなわち，$h(\sigma_i(\alpha)) = 0$ であり，$\sigma_i(\alpha) \in \bar{\mathbb{Z}}$ である．これから，命題 3.6 と命題 3.3 より，

$$\mathrm{Tr}_{k/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \in \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}, \quad \mathrm{N}_{k/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

□

系 4.20. $\theta \in \bar{\mathbb{Z}}$, θ の $\mathbb{Q}$ 上の最小多項式を $f(X)$ とすれば，$f(X) \in \mathbb{Z}[X]$ である．

[証明]　$\theta_1 (= \theta), \theta_2, \ldots, \theta_n$ を $f(X)$ の根とすれば，θ_i の $\mathbb{Q}$ 上の最小多項式は $f(X)$ を割り切るが，$f(X)$ は既約であるから，θ_i の $\mathbb{Q}$ 上の最小多項式も $f(X)$ である．$\theta \in \bar{\mathbb{Z}}$ より，$h(X) \in \mathbb{Z}[X]$ をモニックで，$h(\theta) = 0$ となるものがとれる．このとき，$h(X) = f(X)g(X)$, $g(X) \in \mathbb{Q}[X]$ とかけるから，

$$h(\theta_i) = f(\theta_i)g(\theta_i) = 0, \quad i = 1, \ldots, n.$$

よって，$\theta_1, \ldots, \theta_n \in \bar{\mathbb{Z}}$ である．

$$f(X) = \prod_{i=1}^{n} (X - \theta_i)$$

より，$f(X)$ の各係数は $\theta_1, \ldots, \theta_n$ たちの $\mathbb{Z}$-係数の多項式であり，命題 3.6 と命題 3.3 より，それらは $\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ の元である．□

4.5 有限生成自由 $\mathbb{Z}$-加群

定義 4.21. L を加群とする．$u_1, \ldots, u_n \in L$ が存在して，L の任意の元が，

$$a_1u_1 + \cdots + a_nu_n, \qquad a_1, \ldots, a_n \in \mathbb{Z}$$

の形に一意的に表せるとき，L を**階数** n の**自由** $\mathbb{Z}$**-加群**という．また，$\{u_1, \ldots, u_r\}$ は L の**基底**であるという．

補題 4.22. L を階数 n の自由 $\mathbb{Z}$-加群とする．M を L の部分加群とすれば，M は階数 $r \leq n$ の自由 $\mathbb{Z}$-加群である．

[証明]　n に関する帰納法による．$n = 1$ のときは，$L = \{au \,|\, a \in \mathbb{Z}\}$ である．$M \subset L$ を部分加群とするとき，$I = \{a \in \mathbb{Z} \,|\, au \in M\}$ とおけば，I は $\mathbb{Z}$ のイデアルである．命題 0.2 より，$I = d\mathbb{Z}$, $d \geq 0$ とかける．$d = 0$ ならば，$M = \{0\}$ である (階数 0 の自由 $\mathbb{Z}$-加群)．$d > 0$ ならば，$u' = du$ とおくと，

$$M = \{au \,|\, a \in d\mathbb{Z}\} = \{bu' \,|\, b \in \mathbb{Z}\}$$

である．よって，M は階数 1 の自由 $\mathbb{Z}$-加群である．$n > 1$ として，$n-1$ までは主張が正しいとする．L を階数 n の自由 $\mathbb{Z}$-加群，M を L の部分加群とする．$\{u_1, \ldots, u_n\}$ を L の基底とし，

$$L' = \{a_2u_2 + \cdots + a_nu_n \,|\, a_2, \ldots, a_n \in \mathbb{Z}\}$$

とおく．$M' = M \cap L'$ とおくと，M' は階数 $n-1$ の自由 $\mathbb{Z}$-加群 L' の部分加群であるから，帰納法の仮定によって，階数 $r-1 \leq n-1$ の自由 $\mathbb{Z}$-加群である．

$$I = \{a \in \mathbb{Z} \,|\, au_1 + u' \in M \ (\exists u' \in L')\}$$

とおけば，I は $\mathbb{Z}$ のイデアルである．$I = d\mathbb{Z}$, $d \geq 0$ とかける．$d = 0$ ならば，$M \subset L'$, $M = M \cap L' = M'$ であるから，M は階数 $r-1$ の自由 $\mathbb{Z}$-加群である．$d > 0$ ならば，$v_1 = du_1 + u_0 \in M$ となる $u_0 \in L'$ が存在する．任意の $v \in M$ は $v = bdu_1 + u'$, $b \in \mathbb{Z}$, $u' \in L'$ とかける．そのとき，$w = v - bv_1$ とおけば，$w \in M$ であり，

$$w = bdu_1 + u' - b(du_1 + u_0) = u' - bu_0 \in L'$$

であるから，$w \in M \cap L' = M'$ である．$\{v_2, \ldots, v_r\}$ を M' の基底とすれば，

$$w = b_2v_2 + \cdots + b_rv_r, \qquad b_2, \ldots, b_r \in \mathbb{Z}$$

とかけるから，

$$v = bv_1 + w = bv_1 + b_2v_2 + \cdots + b_rv_r$$

である．よって，M は $\{v_1,\dots,v_r\}$ の $\mathbb{Z}$ 係数の 1 次結合全体と一致する．また，そのような 1 次結合について，

$$b_1v_1+\cdots+b_rv_r=0$$

となるのは，各 v_j を $u_1,\dots,u_n$ の 1 次結合としてかくとき，u_1 を含むものは v_1 だけであるから，$b_1=0$ のときであり，

$$b_2v_2+\cdots+b_rv_r=0$$

となるが，これは $b_2=\cdots=b_r=0$ のときに限る．ゆえに，M は階数 $r\leq n$ の自由 $\mathbb{Z}$-加群である． □

補題 4.23. L を階数 n の自由 $\mathbb{Z}$-加群とし，M を L の階数 $r\leq n$ の部分加群とすれば，L の基底 $\{u_1,\dots,u_n\}$ と自然数 $d_1,\dots,d_r$ で，$d_i|d_{i+1}$ $(i=1,\dots,r-1)$ かつ $\{d_1u_1,\dots,d_ru_r\}$ が M の基底となるものが存在する．

[証明] 補題の主張のような基底の存在を n に関する帰納法で証明する．$n=1$ のときは，明らかである．$n>1$ として，$n-1$ までは主張が正しいとする．L を階数 n の自由 $\mathbb{Z}$-加群，M を L の部分加群とする．$\{u_1,\dots,u_n\}$ を L の基底とする．$v\in M$, $v\neq 0$ を $v=a_1u_1+\cdots+a_nu_n$, $a_i\in\mathbb{Z}$ とかくとき，$a_1,\dots,a_n$ の最大公約数を $g(v)$ で表す．$g(v)\geq 1$ である．$d_1=\min\{g(v)\,|\,v\in M,\,v\neq 0\}$ とおく．$v_1\in M$ を $g(v_1)=d_1$ となるようにとる．

$$v_1=a_{11}u_1+\cdots+a_{1n}u_n,\qquad a_{1j}\in\mathbb{Z}$$

とかくと，$\gcd(a_{11},\dots,a_{1n})=d_1$ である．このとき，$b_1,\dots,b_n\in\mathbb{Z}$ で，

$$b_1a_{11}+\cdots+b_na_{1n}=d_1$$

となるものが存在する．準同型 $\varphi_1:L\longrightarrow\mathbb{Z}$ を

$$\varphi_1(a_1u_1+\cdots+a_nu_n)=a_1b_1+\cdots+a_nb_n$$

によって定義する．$\varphi_1(v_1)=d_1$ である．さらに，$\varphi_1(M)=d_1\mathbb{Z}$ である．実際，$v\in M$ とし，$\varphi_1(v)=d_1q+r$, $q,r\in\mathbb{Z}$, $0\leq r<d_1$ とかくと，$v'=v-qv_1\in M$ とおけば，$\varphi_1(v')=\varphi_1(v)-q\varphi_1(v_1)=r$ である．もし，$r>0$ であるとすると，$v'\neq 0$ であり，$v'=a_1u_1+\cdots+a_nu_n$ とかけば，

$$r=\varphi_1(v')=a_1b_1+\cdots+a_nb_n$$

である．$g(v)=\gcd(a_1,\dots,a_n)$ とおくと，$g(v)>0$, $g(v)|r$ であるから，$g(v)\leq r<d_1$ である．これは $d_1=\min\{g(v)\,|\,v\in M,\,v\neq 0\}$ に矛盾する．ゆえに，$r=0$, $\varphi_1(M)=d_1\mathbb{Z}$ である．$a_{1j}=d_1a'_{1j}$, $a'_{1j}\in\mathbb{Z}$ とかき，

$$u'_1=a'_{11}u_1+\cdots+a'_{1n}u_n$$

とおくと，$u_1' \in L, v_1 = d_1u_1', \varphi_1(u_1') = 1$である．$L' = \ker\varphi_1 = \{u \in L \,|\, \varphi_1(u) = 0\}$ とおく．このとき，任意の $u \in L$ は, $u = a_1u_1' + u'$, $a_1 \in \mathbb{Z}$, $u' \in L'$ の形に一意的に表せる (このことを，$L = \mathbb{Z}u_1' \oplus L'$ と表す)．実際，$\varphi_1(u) = a_1$, $u' = u - a_1u_1'$ とおけば,

$$\varphi_1(u') = \varphi_1(u - a_1u_1') = \varphi_1(u) - a_1\varphi_1(u_1') = a_1 - a_1 = 0,$$

よって，$u' \in \ker\varphi_1 = L'$ であり，$u = a_1u_1' + u'$ とかける．この表し方が一意的であることは，$a_1u_1' + u' = 0$, $a_1 \in \mathbb{Z}$, $u' \in L'$ とするとき，$a_1 = 0$, $u' = 0$ であることをみればよい．これは，次のようにわかる．

$$0 = \varphi_1(a_1u_1' + u') = a_1\varphi_1(u_1') + \varphi_1(u') = a_1,$$

$a_1 = 0$, $u' = 0$ である．

$M' = M \cap L'$ とおくと，$M = \mathbb{Z}v_1 \oplus M'$ である．実際, $v \in M$ とすれば, $v \in L$ であるから，$v = a_1u_1' + u'$, $a_1 \in \mathbb{Z}$, $u' \in L'$ とかける．このとき，$\varphi_1(v) = a_1\varphi_1(u_1') = a_1$ である．$\varphi_1(M) = d_1\mathbb{Z}$ であるから，$a_1 = c_1d_1$ とかける．よって，

$$v = c_1d_1u_1' + u' = c_1v_1 + u'.$$

$u' = v - c_1v_1 \in M \cap L' = M'$ である．$c_1v_1 + u' = 0$ とすれば,

$$0 = \varphi_1(c_1v_1 + u') = c_1d_1,$$

$c_1 = 0$, $u' = 0$ である．ゆえに，$M = \mathbb{Z}v_1 \oplus M'$ である．

補題 4.22 より，L' は階数 $n-1$ の自由 $\mathbb{Z}$-加群である．補題 4.22 より，M' は階数 $s-1 \leq n-1$ の自由 $\mathbb{Z}$-加群である．帰納法の仮定によって，L' の基底 $\{u_2', \ldots, u_n'\}$ と自然数 $d_2, \ldots, d_s$ で，$d_i | d_{i+1}$ $(i = 2, \ldots, s-1)$ かつ $\{d_2u_2', \ldots, d_su_s'\}$ は M' の基底となるものが存在する．そのとき，$L = \mathbb{Z}u_1' \oplus L'$ であるから，$\{u_1', u_2', \ldots, u_n'\}$ は L の基底である．また，$M = \mathbb{Z}v_1 \oplus M'$ かつ $v_1 = d_1u_1'$ であるから，$\{d_1u_1', d_2u_2', \ldots, d_su_s'\}$ は M の基底である．最後に，$s \geq 2$ のとき，$d_1 | d_2$ を示すことが残されている．$d_2 = d_1q + r$, $q, r \in \mathbb{Z}$, $0 \leq r < d_1$ とする．準同型 $\psi : L \longrightarrow \mathbb{Z}$ を

$$\psi(a_1'u_1' + \cdots + a_n'u_n') = -qa_1' + a_2'$$

によって定義する．$v = d_1u_1' + d_2u_2'$ とおけば，$v \in M$, $v \neq 0$ であり，$\psi(v) = \psi(d_1u_1' + d_2u_2') = -qd_1 + d_2 = r$ である．一方,

$$v = d_1u_1' + d_2u_2' = a_1u_1 + \cdots + a_nu_n, \qquad a_i \in \mathbb{Z}$$

とかくとき，$v \neq 0$ より，$a_1, \ldots, a_n$ のうちの少なくとも 1 つは 0 でなく,

$$\psi(v) = a_1\psi(u_1) + \cdots + a_n\psi(u_n)$$

であるから，$g(v) = \gcd(a_1, \ldots, a_n) > 0$ は $r = \psi(v)$ を割り切る．$r > 0$ ならば，$g(v) \leq r < d_1$ となって，d_1 の最小性に矛盾する．ゆえに，$r = 0$ であり，$d_2 = d_1q$ である． □

系 4.24. L を階数 n の自由 $\mathbb{Z}$-加群とし，M を L の部分加群で階数 n であるとする．L の基底 $\{u_1, \ldots, u_n\}$ と自然数 $d_1, \ldots, d_n$ を $\{d_1u_1, \ldots, d_nu_n\}$ が M の基底となるようにとれば，剰余加群 L/M は有限加群であり，その位数は $d_1 \cdots d_n$ である．

[証明]　準同型 $f : L \longrightarrow (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})$ を

$$f(a_1u_1 + \cdots + a_nu_n) = ([a_1]_{d_1}, \ldots, [a_n]_{d_n})$$

によって定義する．ここで，$[a]_d = a + d\mathbb{Z} \in \mathbb{Z}/d\mathbb{Z}$ とおいた．明らかに，f は全射である．$\ker f = M$ であるから，準同型定理によって，f は同型

$$L/M \cong (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})$$

を引き起こす．$|L/M| = d_1 \cdots d_n$ である．　□

4.6　代数体の整数環

一般の代数体の整数環の構造を調べる．k を代数体，$n = [k : \mathbb{Q}]$ とする．定理 4.11 より，$k = \mathbb{Q}(\theta)$ となる $\theta \in k$ がとれる．命題 3.4 より，θ を適当な自然数倍で置き換えて，$\theta \in \bar{\mathbb{Z}}$ としてよい．そのとき，$\theta \in k \cap \bar{\mathbb{Z}} = \mathcal{O}_k$ である．$f(X)$ を θ の $\mathbb{Q}$ 上の最小多項式とすると，系 4.20 より，$f(X) \in \mathbb{Z}[X]$ である．環 $\mathbb{Z}[\theta]$ は

$$\mathbb{Z}[\theta] = \left\{c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} \,|\, c_0, \ldots, c_{n-1} \in \mathbb{Z}\right\}$$

であるから，階数 n の自由 $\mathbb{Z}$-加群である．明らかに，$\mathbb{Z}[\theta] \subset \mathcal{O}_k$ である．ここで，

$$L = \{\lambda \in k \,|\, \mathrm{Tr}_{k/\mathbb{Q}}(\lambda\mathbb{Z}[\theta]) \subset \mathbb{Z}\}$$

とおく．$\lambda \in \mathcal{O}_k$ ならば，任意の $\beta \in \mathbb{Z}[\theta]$ に対して，$\lambda\beta \in \mathcal{O}_k$ であるから，命題 4.19 より，$\mathrm{Tr}_{k/\mathbb{Q}}(\lambda\beta) \in \mathbb{Z}$ である．よって，$\lambda \in L$, $\mathcal{O}_k \subset L$ である．L が階数 n の自由 $\mathbb{Z}$-加群であることを示せば，補題 4.22 より，L の部分加群である $\mathcal{O}_k$ も階数 $r \leq n$ の自由 $\mathbb{Z}$-加群である．しかし，$\mathbb{Z}[\theta] \subset \mathcal{O}_k$ かつ $\mathbb{Z}[\theta]$ は階数 n の自由 $\mathbb{Z}$-加群であるから，$r = n$ となる．

L が階数 n の自由 $\mathbb{Z}$-加群であることを示そう．これは次の補題からわかる．

補題 4.25. $L = f'(\theta)^{-1}\mathbb{Z}[\theta]$ である．特に，L は階数 n の自由 $\mathbb{Z}$-加群である．

[証明]　$f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ とする．$f(X)$ は，

$$f(X) = \prod_{j=1}^{n}(X - \theta_j)$$

と $\bar{\mathbb{Q}}$ 上分解される．各 $1 \leq i \leq n$ に対して，

$$f_i(X) = \frac{f(X)}{X - \theta_i} = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (X - \theta_j)$$

とおき，$1 \leq l \leq n$ について，

$$G_l(X) = \sum_{r=1}^{n} \frac{\theta_r^{l-1}}{f'(\theta_r)} f_r(X)$$

とおく．

$$f'(X) = \sum_{r=1}^{n} f_r(X)$$

であり，$r \neq i$ ならば，$f_r(\theta_i) = 0$ だから，$f'(\theta_i) = f_i(\theta_i)$ である．したがって，$G_l(\theta_i) = \theta_i^{l-1}$, $i = 1, \ldots, n$，である．$f_r(X)$ は $n-1$ 次多項式だから，$G_l(X)$ は高々 $n-1$ 次の多項式である．$G_l(X) - X^{l-1}$ は高々 $n-1$ 次の多項式であって，n 個の根 $\theta_1, \ldots, \theta_n$ を持つ．したがって，$G_l(X) - X^{l-1} = 0$, $G_l(X) = X^{l-1}$ でなければならない．

$$\frac{f(X)}{X - \theta} = \lambda_1 X^{n-1} + \lambda_2 X^{n-2} + \cdots + \lambda_n$$

とすれば，

$$\begin{aligned} & f(X) \\ &= \lambda_1 X^n + \lambda_2 X^{n-1} + \cdots + \lambda_n X - \theta(\lambda_1 X^{n-1} + \lambda_2 X^{n-2} + \cdots + \lambda_n) \\ &= \lambda_1 X^n + (\lambda_2 - \theta\lambda_1) X^{n-1} + (\lambda_3 - \theta\lambda_2) X^{n-2} + \cdots \\ &\quad + (\lambda_n - \theta\lambda_{n-1}) X - \theta\lambda_n. \end{aligned}$$

よって，$\lambda_1 = 1$, $\lambda_{i+1} - \theta\lambda_i = a_i$, $i = 1, \ldots, n-1$ を得る．したがって，

$$\left.\begin{aligned} \lambda_1 &= 1, \\ \lambda_2 &= \theta + a_1, \\ \lambda_3 &= \theta^2 + a_1\theta + a_2, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \lambda_n &= \theta^{n-1} + a_1\theta^{n-2} + \cdots + a_{n-1}. \end{aligned}\right\} \tag{4.4}$$

λ_j の θ を θ_i で置き換えたものを $\lambda_j^{(i)}$ とかけば，

$$f_i(X) = \sum_{j=1}^{n} \lambda_j^{(i)} X^{j-1}$$

である．よって，

$$G_l(X) = \sum_{i=1}^{n} \frac{\theta_i^{l-1}}{f'(\theta_i)} f_i(X) = \sum_{i=1}^{n} \frac{\theta_i^{l-1}}{f'(\theta_i)} \sum_{j=1}^{n} \lambda_j^{(i)} X^{j-1} = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \frac{\theta_i^{l-1}}{f'(\theta_i)} \lambda_j^{(i)} \right) X^{j-1}.$$

よって，$G_l(X)$ の X^{j-1} の係数は，トレースの定義と $G_l(X) = X^{l-1}$ から，

$$\mathrm{Tr}_{k/\mathbb{Q}}\left(\theta^{l-1}\frac{\lambda_j}{f'(\theta)}\right) = \sum_{i=1}^{n}\frac{\theta_i^{l-1}}{f'(\theta_i)}\lambda_j^{(i)} = \begin{cases} 1, & j = l, \\ 0, & j \neq l. \end{cases} \tag{4.5}$$

(4.4) より，$f'(\theta)^{-1}\lambda_j$, $j = 1, \ldots, n$ は k の $\mathbb{Q}$ 上の基底である．よって，$\lambda \in k$ を

$$\lambda = c_1\frac{\lambda_1}{f'(\theta)} + \cdots + c_n\frac{\lambda_n}{f'(\theta)}, \quad c_j \in \mathbb{Q}$$

とかくとき，

$$\mathrm{Tr}_{k/\mathbb{Q}}(\lambda\theta^{l-1}) = \sum_{j=1}^{n} c_j \,\mathrm{Tr}_{k/\mathbb{Q}}\left(\theta^{l-1}\frac{\lambda_j}{f'(\theta)}\right) = c_l$$

であるから，

$$\lambda \in L \Longleftrightarrow c_l \in \mathbb{Z}, \quad l = 1, \ldots, n$$

である．ゆえに，L は $\{f'(\theta)^{-1}\lambda_j \,|\, j = 1, \ldots, n\}$ を基底とする階数 n の自由 $\mathbb{Z}$-加群である．$\{\lambda_1, \ldots, \lambda_n\}$ は $\mathbb{Z}[\theta]$ の基底であるから，$L = f'(\theta)^{-1}\mathbb{Z}[\theta]$ である． □

以上によって代数体の整数環 $\mathcal{O}_k$ について，次の定理が証明された．

定理 4.26. k を代数体，$n = [k : \mathbb{Q}]$ とすれば，k の整数環 $\mathcal{O}_k$ は階数 n の自由 $\mathbb{Z}$-加群である．すなわち，$\omega_1, \ldots, \omega_n \in \mathcal{O}_k$ が存在して，

$$\mathcal{O}_k = \{c_1\omega_1 + \cdots + c_n\omega_n \,|\, c_1, \ldots, c_n \in \mathbb{Z}\}.$$

$\{\omega_1, \ldots, \omega_n\}$ を k の**整数底**という．

5 代数体のイデアル

k を代数体，$n = [k : \mathbb{Q}]$, $\mathcal{O}_k$ を k の整数環とする．$\{\omega_1, \ldots, \omega_n\}$ を k の整数底とする．$\mathcal{O}_k$ のイデアルについて調べよう．以後，イデアルは $\{0\}$ でないものだけ考える．

命題 5.1. $\mathfrak{a} \subset \mathcal{O}_k$ をイデアルとすると，$\mathfrak{a}$ は階数 n の自由 $\mathbb{Z}$-加群である．すなわち，$\alpha_1, \ldots, \alpha_n \in \mathcal{O}_k$ が存在して，

$$\mathfrak{a} = \{c_1\alpha_1 + \cdots + c_n\alpha_n \,|\, c_1, \ldots, c_n \in \mathbb{Z}\}.$$

[証明] 定理 4.26 と補題 4.22 より，$\mathfrak{a}$ は階数 $r \leq n$ の自由 $\mathbb{Z}$-加群である．$\gamma \in \mathfrak{a}$, $\gamma \neq 0$ をとると，$\gamma\mathcal{O}_k \subset \mathfrak{a}$ であり，$\{\omega_1, \ldots, \omega_n\}$ を k の整数底とすれば，$\gamma\mathcal{O}_k$ は $\{\gamma\omega_1, \ldots, \gamma\omega_n\}$ を基底とする階数 n の自由 $\mathbb{Z}$-加群であるから，$r = n$ である． □

命題 5.2. 剰余環 $\mathcal{O}_k/\mathfrak{a}$ は有限環である．

[証明]　命題5.1より，$\mathfrak{a}$は階数nの自由$\mathbb{Z}$-加群である．補題4.23より，$\mathcal{O}_k$の基底$\{\omega_1,\dots,\omega_n\}$と自然数$d_1,\dots,d_n$で，$d_i|d_{i+1}$ $(i=1,\dots,n-1)$かつ$\{d_1\omega_1,\dots,d_n\omega_n\}$が$\mathfrak{a}$の基底となるものが存在する．そのとき，系4.24より，$\mathcal{O}_k/\mathfrak{a}$は有限加群であり，位数は$d_1\cdots d_n$である．　□

定義 5.3. 自然数$|\mathcal{O}_k/\mathfrak{a}|$をイデアル$\mathfrak{a}$の**ノルム**といい，$\mathrm{N}(\mathfrak{a})$で表す．$\{\alpha_1,\dots,\alpha_n\}$がイデアル$\mathfrak{a}$の基底であるとき，$\mathfrak{a}=[\alpha_1,\dots,\alpha_n]$とかく．

命題 5.4. $\mathfrak{a}\subset\mathcal{O}_k$をイデアルとする．$\mathcal{O}_k=[\omega_1,\dots,\omega_n]$，$\mathfrak{a}=[\alpha_1,\dots,\alpha_n]$とする．

$$(\alpha_1,\dots,\alpha_n)=(\omega_1,\dots,\omega_n)A,\qquad A\in M_n(\mathbb{Z})$$

とかく．そのとき，

$$\mathrm{N}(\mathfrak{a})=|\mathcal{O}_k/\mathfrak{a}|=|\det A|$$

が成り立つ．

[証明]　補題4.23より，$\mathcal{O}_k$の基底$\{\eta_1,\dots,\eta_n\}$と自然数$d_1,\dots,d_n$で，$d_i|d_{i+1}$ $(i=1,\dots,n-1)$かつ$\{d_1\eta_1,\dots,d_n\eta_n\}$が$\mathfrak{a}$の基底となるものが存在する．そのとき，

$$(\eta_1,\dots,\eta_n)=(\omega_1,\dots,\omega_n)T,$$

Tは$\mathbb{Z}$の元を成分とする行列式±1のn次行列である．同様に，

$$(\alpha_1,\dots,\alpha_n)=(d_1\eta_1,\dots,d_n\eta_n)S,$$

Sも$\mathbb{Z}$の元を成分とする行列式±1のn次行列である．よって，

$$(\alpha_1,\dots,\alpha_n)=(d_1\eta_1,\dots,d_n\eta_n)S=(\eta_1,\dots,\eta_n)\begin{pmatrix}d_1&&&\\&d_2&&\\&&\ddots&\\&&&d_n\end{pmatrix}S$$

$$=(\omega_1,\dots,\omega_n)T\begin{pmatrix}d_1&&&\\&d_2&&\\&&\ddots&\\&&&d_n\end{pmatrix}S,$$

$$A=T\begin{pmatrix}d_1&&&\\&d_2&&\\&&\ddots&\\&&&d_n\end{pmatrix}S.$$

この行列式をとれば，

$$\det A=(\det T)d_1\cdots d_n(\det S)=(\pm1)(d_1\cdots d_n)(\pm1),$$

$|\det A|=d_1\cdots d_n=\mathrm{N}(\mathfrak{a})$である．　□

定義 5.5. n 次体 k の整数環のイデアル $\mathfrak{a} = [\alpha_1, \ldots, \alpha_n]$ に対して,

$$D(\mathfrak{a}) = \det((\mathrm{Tr}_{k/\mathbb{Q}}(\alpha_i\alpha_j)) = \begin{vmatrix} \mathrm{Tr}_{k/\mathbb{Q}}(\alpha_1^2) & \mathrm{Tr}_{k/\mathbb{Q}}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}_{k/\mathbb{Q}}(\alpha_1\alpha_n) \\ \mathrm{Tr}_{k/\mathbb{Q}}(\alpha_2\alpha_1) & \mathrm{Tr}_{k/\mathbb{Q}}(\alpha_2^2) & \cdots & \mathrm{Tr}_{k/\mathbb{Q}}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{k/\mathbb{Q}}(\alpha_n\alpha_1) & \mathrm{Tr}_{k/\mathbb{Q}}(\alpha_n\alpha_2) & \cdots & \mathrm{Tr}_{k/\mathbb{Q}}(\alpha_n^2) \end{vmatrix}$$

を $\mathfrak{a}$ の**判別式**という．特に，$\mathfrak{a} = \mathcal{O}_k$ のとき，$D_k = D(\mathcal{O}_k)$ を k の**判別式**という．

命題 5.6. $\mathcal{O}_k$ のイデアル $\mathfrak{a}$ について，$\mathfrak{a}$ の判別式 $D(\mathfrak{a})$ は 0 でない整数であり，$\mathfrak{a}$ の基底のとり方によらない．また,

$$D(\mathfrak{a}) = D_k\,\mathrm{N}(\mathfrak{a})^2$$

が成り立つ.

[証明] $\{\alpha_1, \ldots, \alpha_n\}$ を $\mathfrak{a}$ の基底とする．$\sigma_i : k \longrightarrow \bar{\mathbb{Q}}$ $(i = 1, \ldots, n)$ を共役写像とすると,

$$B = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$$

とおけば,

$${}^tBB = \left(\sum_{r=1}^{n} \sigma_r(\alpha_i)\sigma_r(\alpha_j)\right) = \left(\sum_{r=1}^{n} \sigma_r(\alpha_i\alpha_j)\right) = \left(\mathrm{Tr}_{k/\mathbb{Q}}(\alpha_i\alpha_j)\right)$$

であるから，行列式をとれば,

$$D(\mathfrak{a}) = \det({}^tBB) = (\det {}^tB)(\det B) = (\det B)^2.$$

一方，$(\alpha_1, \ldots, \alpha_n) = (\omega_1, \ldots, \omega_n)A$ となる $\mathbb{Z}$-係数の n 次行列 A をとれば，命題 5.4 より，$\mathrm{N}(\mathfrak{a}) = |\det A|$ である．また，$(\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n)) = (\sigma_i(\omega_1), \ldots, \sigma_i(\omega_n))A$ であるから,

$$B = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_n) \end{pmatrix} A.$$

よって，$(\det B)^2 = (\det(\sigma_i(\omega_j)))^2(\det A)^2 = D(\mathcal{O}_k)\,\mathrm{N}(A)^2$ である．$D(\mathfrak{a})$ は整数であることは $\mathrm{Tr}_{k/\mathbb{Q}}(\alpha_i\alpha_j) \in \mathbb{Z}$ からわかる．これが 0 でないことは次のようにわかる．$k = \mathbb{Q}(\theta)$ となる $\theta \in \mathcal{O}_k$ をとる．$f(X)$ を θ の最小多項式とすると，$f(X)$

は重根を持たない．θ の共役を $\sigma_i(\theta) = \theta_i$ $(i = 1, \dots, n)$ とする．$\mathbb{Z}[\theta] \subset \mathcal{O}_k$ より，$(1, \theta, \dots, \theta^{n-1}) = (\omega_1, \dots, \omega_n)C$ となる $\mathbb{Z}$-係数の n 次行列 C をとれば，

$$\begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{pmatrix} = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_n) \end{pmatrix} C.$$

この両辺の行列式の 2 乗をとれば，

$$\begin{vmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{vmatrix}^2 = D(\mathfrak{a})(\det C)^2.$$

この左辺は

$$\prod_{1 \le i < j \le n} (\theta_j - \theta_i)^2 \neq 0$$

である．よって，$D(\mathcal{O}_k) \neq 0$, $D(\mathfrak{a}) \neq 0$ である． □

例 5.7. $\mathbb{Q}(\sqrt{3})$ の判別式は

$$\begin{vmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{vmatrix}^2 = (-2\sqrt{3})^2 = 12.$$

$\mathbb{Q}(\sqrt{5})$ の判別式は

$$\begin{vmatrix} 1 & (1+\sqrt{5})/2 \\ 1 & (1-\sqrt{5})/2 \end{vmatrix}^2 = (\sqrt{5})^2 = 5.$$

一般に，$k = \mathbb{Q}(\sqrt{m})$, $m \neq 0, 1$ は平方因数を持たない整数，とするとき，

$$D_k = \begin{cases} m, & m \equiv 1 \pmod 4, \\ 4m, & m \equiv 2, 3 \pmod 4. \end{cases}$$

命題 5.8. $\alpha \in \mathcal{O}_k$, $\alpha \neq 0$ とすれば，単項イデアル $(\alpha) = \alpha\mathcal{O}_k$ について，

$$\mathrm{N}((\alpha)) = |\,\mathrm{N}_{k/\mathbb{Q}}(\alpha)|.$$

[証明] $\mathcal{O}_k = [\omega_1, \dots, \omega_k]$ とすれば，$(\alpha) = [\alpha\omega_1, \dots, \alpha\omega_n]$ であるから，

$$\begin{aligned} D((\alpha)) &= \begin{vmatrix} \sigma_1(\alpha\omega_1) & \sigma_1(\alpha\omega_2) & \cdots & \sigma_1(\alpha\omega_n) \\ \sigma_2(\alpha\omega_1) & \sigma_2(\alpha\omega_2) & \cdots & \sigma_2(\alpha\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha\omega_1) & \sigma_n(\alpha\omega_2) & \cdots & \sigma_n(\alpha\omega_n) \end{vmatrix}^2 \\ &= (\sigma_1(\alpha) \cdots \sigma_n(\alpha))^2 D(\mathcal{O}_k) = \mathrm{N}_{k/\mathbb{Q}}(\alpha)^2 D_k. \end{aligned}$$

命題 5.6 より，$D((\alpha)) = D_k\,\mathrm{N}((\alpha))^2$ であるから，$\mathrm{N}((\alpha)) = |\,\mathrm{N}_{k/\mathbb{Q}}(\alpha)|$ を得る． □

6　類数の有限性

k を代数体とする．$\mathcal{O}_k$ のイデアル $\mathfrak{p}$ について

$$\begin{aligned}\mathfrak{p} \text{ が}\textbf{素イデアル} &\iff \mathcal{O}_k/\mathfrak{p} \text{ が整域} \\ &\iff \alpha\beta \in \mathfrak{p} \text{ ならば } \alpha \in \mathfrak{p} \text{ または } \beta \in \mathfrak{p}.\end{aligned}$$

命題 6.1. $\mathcal{O}_k$ のイデアルの列

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \cdots$$

があれば，ある番号から先は一定である．すなわち，ある番号 N が存在して，任意の $m \geq N$ について，$\mathfrak{a}_m = \mathfrak{a}_N$ が成立する ($\mathcal{O}_k$ は**ネーター環**である).

[証明]　命題 5.2 によって，$\mathcal{O}_k/\mathfrak{a}_1$ は有限環である．したがって，等式

$$(\mathcal{O}_k : \mathfrak{a}_1) = (\mathcal{O}_k : \mathfrak{a}_m)(\mathfrak{a}_{m-1} : \mathfrak{a}_{m-2}) \cdots (\mathfrak{a}_2 : \mathfrak{a}_1)$$

によって，ある番号から先は一定でなければならない．　□

命題 6.2. $\mathfrak{p}$ を $\mathcal{O}_k$ の素イデアルとすると，$\mathcal{O}_k/\mathfrak{p}$ は体である．

[証明]　$\gamma \in \mathcal{O}_k$ の属する $\bmod \mathfrak{p}$ の剰余類を $[\gamma]$ とかく．$[\alpha] \in \mathcal{O}_k/\mathfrak{p}$，$[\alpha] \neq 0$ をとる．写像 $f : \mathcal{O}_k/\mathfrak{p} \longrightarrow \mathcal{O}_k/\mathfrak{p}$ を

$$f([\gamma]) = [\alpha][\gamma]$$

によって定義すると，f は加法について群の準同型である．$\mathfrak{p}$ が素イデアルであることから，f は単射であることがわかる．f は有限集合 $\mathcal{O}_k/\mathfrak{p}$ から自分自身への単射だから，全単射である．したがって特に，$f([\gamma]) = [1]$ となる $[\gamma]$ が存在する．よって，$(\mathcal{O}_k/\mathfrak{p})^\times = (\mathcal{O}_k/\mathfrak{p}) - \{0\}$ である．すなわち，$\mathcal{O}_k/\mathfrak{p}$ は体である．　□

定義 6.3. $\mathcal{O}_k$ の 2 つのイデアル $\mathfrak{a}$，$\mathfrak{b}$ に対して，

$$\mathfrak{a} \sim \mathfrak{b} \Longleftrightarrow \exists \alpha, \beta \in \mathcal{O}_k, \alpha, \beta \neq 0,\ (\beta)\mathfrak{a} = (\alpha)\mathfrak{b}$$

と定義する．これは $\mathcal{O}_k$ の 0 でないイデアル全体の集合に同値関係を定義する．この同値類を**イデアル類**という.

補題 6.4 (フルヴィッツの補題). 代数体 k のみによって定まる自然数 M で次の性質を持つものが存在する*:* 任意の $\alpha, \beta \in \mathcal{O}_k$，$\beta \neq 0$ に対して，$1 \leq t \leq M$ なる $t \in \mathbb{Z}$ と $\theta \in \mathcal{O}_k$ で,

$$|\,\mathrm{N}_{k/\mathbb{Q}}(t\alpha - \theta\beta)| < |\,\mathrm{N}_{k/\mathbb{Q}}(\beta)|$$

となるものが存在する.

[証明]　$\mathcal{O}_k = [\omega_1, \ldots, \omega_n]$ とする．写像 $\varphi : k \longrightarrow \mathbb{R}^n$ を k の元を $\gamma = \sum_{j=1}^n a_j\omega_j$, $a_j \in \mathbb{Q}$ とかくとき，$\varphi(\gamma) = (a_1, \ldots, a_n) \in \mathbb{R}^n$ によって定義する．また，

$$\|\gamma\| = \max(|a_1|, \ldots, |a_n|)$$

とおく．$\sigma_i : k \longrightarrow \bar{\mathbb{Q}}$ $(i = 1, \ldots, n)$ を共役写像とする．このとき，

$$\begin{aligned} |\,\mathrm{N}_{k/\mathbb{Q}}(\gamma)| &= \prod_{i=1}^n |\sigma_i(\gamma)| \le \prod_{i=1}^n \sum_{j=1}^n |a_j||\sigma_i(\omega_j)| \\ &\le \|\gamma\|^n \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(\omega_j)| = C\|\gamma\|^n. \end{aligned} \tag{6.1}$$

ここで，$C = \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(\omega_j)|$ とおいた．$m \in \mathbb{Z}$ を $m > C^{1/n}$ にとって，$M = m^n$ とおく．$\gamma = a_1\omega_1 + \cdots + a_n\omega_n \in k$，$a_1, \ldots, a_n \in \mathbb{Q}$ に対して，

$$a_j = b_j + c_j, \quad b_j \in \mathbb{Z},\ 0 \le c_j < 1 \qquad (1 \le j \le n)$$

と整数部分と小数部分に分けてかく．さらに，

$$[\gamma] = \sum_{j=1}^n b_j\omega_j, \qquad \{\gamma\} = \sum_{j=1}^n c_j\omega_j$$

とおくと，

$$\gamma = [\gamma] + \{\gamma\}, \quad [\gamma] \in \mathcal{O}_k,\ \{\gamma\} \in k$$

である．

$$U = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \,|\, 0 \le x_j < 1\ (j = 1, \ldots, n)\}$$

とおいて，$\{\gamma\} \in k$ を φ でうつせば，

$$\varphi(\{\gamma\}) \in U$$

である．このことを，$\gamma_j = j\dfrac{\alpha}{\beta}$，$j = 1, \ldots, M+1$ について適用すれば，$M+1$ 個の U の点 $\varphi(\{\gamma_j\})$，$j = 1, \ldots, M+1$ を得る．U を一辺の長さが $1/m$ の $M = m^n$ 個の小立方体に分割すれば，これらの $M+1$ 個の U の点のうち，どれか 2 つは必ず同じ小立方体に属する．それを $\varphi(\{\gamma_j\})$，$\varphi(\{\gamma_l\})$，$j < l$ とすると，

$$(l-j)\frac{\alpha}{\beta} = \gamma_l - \gamma_j = [\gamma_l] - [\gamma_j] + \{\gamma_l\} - \{\gamma_j\}.$$

よって，$t = l - j$，$\theta = [\gamma_l] - [\gamma_j]$ とおけば，$t \in \mathbb{Z}$，$1 \le t \le M$，$\theta \in \mathcal{O}_k$ であり，

$$t\frac{\alpha}{\beta} - \theta = \{\gamma_l\} - \{\gamma_j\}.$$

(6.1) と $\varphi(\{\gamma_j\})$，$\varphi(\{\gamma_l\})$ が同じ小正方形に属することから，

$$\left|\mathrm{N}_{k/\mathbb{Q}}\left(t\frac{\alpha}{\beta}-\theta\right)\right| \leq C\|\{\gamma_l\}-\{\gamma_j\}\|^n \leq C\left(\frac{1}{m}\right)^n < m^n\frac{1}{m^n} = 1.$$

この両辺に $|\mathrm{N}_{k/\mathbb{Q}}(\beta)|$ をかければ，

$$|\mathrm{N}_{k/\mathbb{Q}}(t\alpha-\theta\beta)| < |\mathrm{N}_{k/\mathbb{Q}}(\beta)|$$

を得る．□

定理 6.5. $\mathcal{O}_k$ のイデアル類の数は有限である．

[証明] $\mathfrak{a}$ を $\mathcal{O}_k$ の任意のイデアルとする．$\beta \in \mathfrak{a}$，$\beta \neq 0$ を $|\mathrm{N}_{k/\mathbb{Q}}(\beta)|$ が最小になるようにとる．このとき，任意の $\alpha \in \mathfrak{a}$ に対して，フルヴィッツの補題を用いれば，$1 \leq t \leq M$ なる $t \in \mathbb{Z}$ と $\theta \in \mathcal{O}_k$ があって

$$|\mathrm{N}_{k/\mathbb{Q}}(t\alpha-\theta\beta)| < |\mathrm{N}_{k/\mathbb{Q}}(\beta)|$$

が成り立つ．ここで，$t\alpha-\theta\beta \in \mathfrak{a}$ だから β のノルムの最小性によって，$t\alpha-\theta\beta = 0$ でなければならない．よって，$t\alpha \in (\beta)$．$1 \leq t \leq M$ だから，$t|M!$ である．したがって，$M!\alpha \in (\beta)$．これが任意の $\alpha \in \mathfrak{a}$ について成り立つから，$M!\mathfrak{a} \subset (\beta) = \beta\mathcal{O}_k$ を得る．よって，

$$\mathfrak{b} = \left(\frac{1}{\beta}\right)M!\mathfrak{a} \subset \mathcal{O}_k.$$

$(M!)\mathfrak{a} = (\beta)\mathfrak{b}$ だから $\mathfrak{a} \sim \mathfrak{b}$ である．また，

$$M!\beta \in M!\mathfrak{a} = (\beta)\mathfrak{b}$$

だから，$(M!) \subset \mathfrak{b}$ である．命題 5.2 によって，$\mathcal{O}_k/(M!)$ は有限環だから，このような $\mathfrak{b}$ は有限個しかない．任意のイデアル $\mathfrak{a}$ がある有限個のイデアル $\mathfrak{b}$ と必ず同値になるのだから，イデアル類の数は有限である．□

定義 6.6. $\mathcal{O}_k$ のイデアル類の数を k の**類数**といい，h_k で表す．

注意 6.7. $\mathfrak{a} \sim \mathcal{O}_k = (1)$ のことを $\mathfrak{a} \sim 1$ と略記する．

$$\mathfrak{a} \sim 1 \Longleftrightarrow \exists\alpha,\ \mathfrak{a} = (\alpha)$$

である．したがって，

$$h_k = 1 \Longleftrightarrow \text{すべてのイデアルが単項イデアル.}$$

例 6.8. 定理 1.6 より，$\mathbb{Q}(\sqrt{-1})$ の類数は 1 である．定理 2.5 より，$\mathbb{Q}(\sqrt{-3})$ の類数も 1 である．

例 6.9. $k=\mathbb{Q}(\sqrt{-5})$ の類数は 1 ではない.

[証明] $\omega=\sqrt{-5}$ とおけば，$\mathcal{O}_k=[1,\omega]$ である．$\mathfrak{a}=[2,\omega+1]$ とおけば，$\mathfrak{a}$ はイデアルであり，$\mathrm{N}(\mathfrak{a})=2$ である．実際,

$$\begin{aligned}\omega\mathfrak{a}=\omega[2,\omega+1]&=[2\omega,\omega^2+\omega]=[2\omega,-5+\omega],\\ 2\omega&=(-1)2+2(\omega+1)\in[2,\omega+1]=\mathfrak{a},\\ -5+\omega&=(-3)2+\omega+1\in[2,\omega+1]=\mathfrak{a}.,\\ (2,\omega+1)=(1,\omega)&\begin{pmatrix}2&1\\0&1\end{pmatrix},\quad \begin{vmatrix}2&1\\0&1\end{vmatrix}=2.\end{aligned}$$

もし，$\mathfrak{a}=(\alpha)$ とすると，命題 5.8 より，$|\mathrm{N}_{k/\mathbb{Q}}(\alpha)|=\mathrm{N}(\mathfrak{a})=2$ である．$x,y\in\mathbb{Z}$ とすると,

$$\mathrm{N}_{k/\mathbb{Q}}(x+y\omega)=x^2+5y^2.$$

$x^2+5y^2=2$ は整数解を持たない．ゆえに，$\mathfrak{a}$ は単項イデアルではない． □

練習問題 6.1. $k=\mathbb{Q}(\sqrt{-23})$ とすると，$\mathcal{O}_k=[1,\omega]$，$\omega=\dfrac{1+\sqrt{-23}}{2}$ である．このとき，$\mathfrak{a}=[3,\omega-1]$ はイデアルであるが，$\mathfrak{a}$ は単項イデアルではないことを証明せよ.

7　イデアル論の基本定理

k を代数体，$[k:\mathbb{Q}]=n$ とする.

補題 7.1. $\mathfrak{a}$，$\mathfrak{b}$ を $\mathcal{O}_k$ のイデアル，$\mathfrak{a}=\mathfrak{a}\mathfrak{b}$ とすると，$\mathfrak{b}=\mathcal{O}_k$ である.

[証明] $\mathfrak{a}=[\alpha_1,\dots,\alpha_n]$ とする．$\mathfrak{a}=\mathfrak{a}\mathfrak{b}$ から,

$$\alpha_i=\sum_{j=1}^{n}\beta_{ij}\alpha_j,\quad i=1,\dots,n$$

となる $\beta_{ij}\in\mathfrak{b}$ が存在する．これは，1 が n 次行列 $B=(\beta_{ij})$ の固有値であることを意味する．したがって,

$$\begin{vmatrix}1-\beta_{11}&-\beta_{12}&\cdots&-\beta_{1n}\\-\beta_{21}&1-\beta_{22}&\cdots&-\beta_{2n}\\\vdots&\vdots&\cdots&\vdots\\-\beta_{n1}&-\beta_{n2}&\cdots&1-\beta_{nn}\end{vmatrix}=0.$$

これを展開すれば，$\beta_{ij}\in\mathfrak{b}$ から，$1\in\mathfrak{b}$，したがって，$\mathfrak{b}=\mathcal{O}_k$ を得る． □

補題 7.2. $\mathfrak{a}$，$\mathfrak{b}$ を $\mathcal{O}_k$ のイデアル，$\beta \in \mathcal{O}_k$，$\mathfrak{a}(\beta) = \mathfrak{a}\mathfrak{b}$ とすると，$\mathfrak{b} = (\beta)$.

[証明]　$\gamma \in \mathfrak{b}$ をとる．$\gamma\mathfrak{a} \subset \mathfrak{a}\mathfrak{b} = (\beta)\mathfrak{a}$ だから，$\dfrac{\gamma}{\beta}\mathfrak{a} \subset \mathfrak{a}$. 補題3.5により，$\dfrac{\gamma}{\beta} \in \mathcal{O}_k$ である．

$$\gamma = \beta\frac{\gamma}{\beta} \in \beta\mathcal{O}_k = (\beta).$$

ゆえに，$\mathfrak{b} \subset (\beta)$，$\beta^{-1}\mathfrak{b} \subset \mathcal{O}_k$．$\mathfrak{a} = \beta^{-1}\mathfrak{a}\mathfrak{b} = \mathfrak{a}(\beta^{-1}\mathfrak{b})$ だから，補題 7.1 によって，$\beta^{-1}\mathfrak{b} = \mathcal{O}_k$，$\mathfrak{b} = (\beta)$. □

補題 7.3. $\mathfrak{a}$ を $\mathcal{O}_k$ のイデアルとすると，ある自然数 $1 \leq \nu \leq h_k$ が存在して，$\mathfrak{a}^\nu \sim 1$ となる．

[証明]　$h_k + 1$ 個のイデアル $\mathfrak{a}^i$，$i = 0, 1, \ldots, h_k$ のうちのどれか 2 つは同じイデアル類に属するから，$0 \leq i < j \leq h_k$ で，$\mathfrak{a}^i \sim \mathfrak{a}^j$ となるものがある．よって，

$$(\beta)\mathfrak{a}^i = (\alpha)\mathfrak{a}^j, \quad \alpha, \beta \in \mathcal{O}_k, \alpha, \beta \neq 0.$$

$\nu = j - i$ とおけば，$1 \leq \nu \leq h_k$,

$$\mathfrak{a}^i(\beta) = \mathfrak{a}^i(\alpha)\mathfrak{a}^\nu.$$

補題 7.2 より，$(\beta) = (\alpha)\mathfrak{a}^\nu$，すなわち，$\mathfrak{a}^\nu \sim 1$. □

定理 7.4. $\mathcal{O}_k$ のイデアル類全体の集合は，位数 h_k のアーベル群をなす．この群を k の**イデアル類群**といい，Cl_k とかく．

[証明]　イデアル $\mathfrak{a}$ のイデアル類を $[\mathfrak{a}]$ とかく．$\mathfrak{a} \sim \mathfrak{a}_1$，$\mathfrak{b} \sim \mathfrak{b}_1$ ならば,

$$(\alpha_1)\mathfrak{a} = (\alpha)\mathfrak{a}_1, \quad (\beta_1)\mathfrak{b} = (\beta)\mathfrak{b}$$

となる $\alpha, \alpha_1, \beta, \beta_1 \in \mathcal{O}_k - \{0\}$ がある．そのとき，$(\alpha_1\beta_1)\mathfrak{a}\mathfrak{b} = (\alpha\beta)\mathfrak{a}_1\mathfrak{b}_1$，すなわち，$\mathfrak{a}\mathfrak{b} \sim \mathfrak{a}_1\mathfrak{b}_1$ である．したがって,

$$[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$$

と定義すれば，これは代表のとりかたによらずに定まる．結合律 $([\mathfrak{a}][\mathfrak{b}])[\mathfrak{c}] = [\mathfrak{a}]([\mathfrak{b}][\mathfrak{c}])$ は明らかに成り立つ．$[1] = [\mathcal{O}_k]$ が単位元であり，$\mathfrak{a}^\nu \sim 1$ とすれば，$[\mathfrak{a}][\mathfrak{a}^{\nu-1}] = [\mathfrak{a}^\nu] = [1]$．ゆえに，$[\mathfrak{a}^{\nu-1}]$ は $[\mathfrak{a}]$ の逆元である． □

系 7.5. $\mathcal{O}_k$ の任意のイデアル $\mathfrak{a}$ に対して，$\mathfrak{a}^{h_k} \sim 1$ である．

補題 7.6. $\mathfrak{a}$，$\mathfrak{b}$，$\mathfrak{c}$ を $\mathcal{O}_k$ のイデアル，$\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ とすると，$\mathfrak{b} = \mathfrak{c}$ である．

[証明]　$\mathfrak{a}^\nu = (\alpha)$ とすると，$\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ に $\mathfrak{a}^{\nu-1}$ をかけて，$\mathfrak{a}^\nu\mathfrak{b} = \mathfrak{a}^\nu\mathfrak{c}$, $(\alpha)\mathfrak{b} = (\alpha)\mathfrak{c}$. よって，$\mathfrak{b} = \mathfrak{c}$ を得る． □

補題 7.7. $\mathfrak{a}$，$\mathfrak{b}$ を $\mathcal{O}_k$ のイデアル，$\mathfrak{a} \subset \mathfrak{b}$ とすると，$\mathcal{O}_k$ のイデアル $\mathfrak{c}$ で $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ となるものが存在する．

[証明]　$\mathfrak{b}^\nu = (\beta)$ とすると，$\mathfrak{a}\mathfrak{b}^{\nu-1} \subset \mathfrak{b}^\nu = (\beta)$．よって，

$$\mathfrak{c} = \beta^{-1}\mathfrak{a}\mathfrak{b}^{\nu-1} \subset \mathcal{O}_k$$

とおけば，$\mathfrak{b}\mathfrak{c} = \beta^{-1}\mathfrak{a}\mathfrak{b}^\nu = \beta^{-1}\beta\mathfrak{a} = \mathfrak{a}$. □

補題 7.8. 一般に環 R において，$\mathfrak{a}$，$\mathfrak{b}$ をイデアル，$\mathfrak{p}$ を素イデアルとすると，

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{p} \Longrightarrow \mathfrak{a} \subset \mathfrak{p} \text{ または } \mathfrak{b} \subset \mathfrak{p}.$$

[証明]　$\mathfrak{a} \not\subset \mathfrak{p}$ とする．そのとき，$a \in \mathfrak{a}$，$a \notin \mathfrak{p}$ がとれる．$\mathfrak{p}$ は素イデアルだから，$R/\mathfrak{p}$ は整域である．任意の $b \in \mathfrak{b}$ に対して，$ab \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ であり，整域 $R/\mathfrak{p}$ において，$[a][b] = [ab] = 0$，$[a] \neq 0$ だから，$[b] = 0$，すなわち，$b \in \mathfrak{p}$ を得る．よって，$\mathfrak{b} \subset \mathfrak{p}$. □

定理 7.9 (イデアル論の基本定理)**.** $\mathcal{O}_k$ の任意のイデアルは，順序を除いて一意的に素イデアルの積に分解される．

[証明]　$\mathfrak{a}_0 \neq \mathcal{O}_k$ をイデアルとする．命題 5.2 によって，$\mathcal{O}_k/\mathfrak{a}_0$ は有限環だから，

$$\mathfrak{a}_0 \subset \mathfrak{p}_1 \subsetneq \mathcal{O}_k$$

なる極大イデアル $\mathfrak{p}_1$ が存在する．$\mathfrak{p}_1$ は素イデアルである．補題 7.7 によって，

$$\mathfrak{a}_0 = \mathfrak{p}_1\mathfrak{a}_1, \quad \mathfrak{a}_1 \subset \mathcal{O}_k,\ \mathfrak{a}_1 \text{ はイデアル}$$

とかける．このとき，補題 7.1 によって，$\mathfrak{a}_0 \subsetneq \mathfrak{a}_1$ である．$\mathfrak{a}_1 \subsetneq \mathcal{O}_k$ ならば，同様に続ける．こうして，イデアルの列

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots$$

を得るが，命題 6.1 によって，有限回の後に，$\mathfrak{a}_m = \mathcal{O}_k$ となり，

$$\mathfrak{a}_0 = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m, \quad \mathfrak{p}_i \text{ は素イデアル}$$

とかける．

$$\mathfrak{a}_0 = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_l, \quad \mathfrak{q}_j \text{ は素イデアル}$$

ともかけたとする．

$$\mathfrak{p}_1(\mathfrak{p}_2\cdots\mathfrak{p}_m) = \mathfrak{a}_0 = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_l \subset \mathfrak{q}_1$$

だから，補題 7.8 によって，$\mathfrak{p}_1 \subset \mathfrak{q}_1$ または，$\mathfrak{p}_2\cdots\mathfrak{p}_m \subset \mathfrak{q}_1$．後者ならばこれを繰り返せば，結局ある番号 i があって，$\mathfrak{p}_i \subset \mathfrak{q}_1$ である．命題 6.2 によって，$\mathfrak{p}_i$ は極大イデアルであるから，$\mathfrak{p}_i = \mathfrak{q}_1$．番号を付け替えて，$i = 1$ としてよい．このとき，補題 7.6 によって，

$$\mathfrak{p}_2\cdots\mathfrak{p}_m = \mathfrak{q}_2\cdots\mathfrak{q}_l.$$

上の議論を繰り返せば，$l = m$，適当に番号を付け替えれば，$\mathfrak{p}_j = \mathfrak{q}_j$，$j = 1, 2, \ldots, m$ を得る． □

8　イデアルのノルム

k を代数体，$n=[k:\mathbb{Q}]$ とする．この節では，$\mathcal{O}_k$ のイデアルに対して，ノルムの乗法性が成り立つことを示す．

$\mathfrak{p}$ を $\mathcal{O}_k$ の素イデアルとする．命題 6.2 によって，$\mathcal{O}_k/\mathfrak{p}$ は体である．$\mathbb{Z}\cap\mathfrak{p}$ は $\mathbb{Z}$ のイデアルである．自然な準同型

$$\mathbb{Z}\longrightarrow\mathcal{O}_k\longrightarrow\mathcal{O}_k/\mathfrak{p}$$

を考えれば，この核は $\mathbb{Z}\cap\mathfrak{p}$ であり，準同型定理より，

$$\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{p})\longrightarrow\mathcal{O}_k/\mathfrak{p}$$

は体 $\mathcal{O}_k/\mathfrak{p}$ への単射準同型である．したがって，$\mathbb{Z}\cap\mathfrak{p}$ は $\mathbb{Z}$ の素イデアルであり，$\mathbb{Z}\cap\mathfrak{p}=p\mathbb{Z}$，$p$ は素数とかける．これによって，$\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ は体 $\mathcal{O}_k/\mathfrak{p}$ の部分体とみなせる．$\mathcal{O}_k/\mathfrak{p}$ は $\mathbb{F}_p$ 上のベクトル空間になるから，その次元を f とすると，

$$\mathrm{N}(\mathfrak{p})=|\mathcal{O}_k/\mathfrak{p}|=p^f$$

である．

補題 8.1. $\mathfrak{p}$ を $\mathcal{O}_k$ の素イデアル，$\mathbb{Z}\cap\mathfrak{p}=p\mathbb{Z}$ とする．$\pi\in\mathcal{O}_k$ を $\pi\in\mathfrak{p},\ \pi\notin\mathfrak{p}^2$ にとる．$\Gamma\subset\mathcal{O}_k$ を $\mathcal{O}_k/\mathfrak{p}$ の代表元の集合とする．このとき，$\mathcal{O}_k/\mathfrak{p}^m$ の代表元の集合として，

$$\left\{\gamma_0+\gamma_1\pi+\cdots+\gamma_{m-1}\pi^{m-1}\,|\,\gamma_0,\ldots,\gamma_{m-1}\in\Gamma\right\}$$

がとれる．特に，$\mathrm{N}(\mathfrak{p}^m)=\mathrm{N}(\mathfrak{p})^m$ である．

[証明]　$\alpha\in\mathcal{O}_k$ に対して，$\alpha\equiv\gamma_0\pmod{\mathfrak{p}}$ なる $\gamma_0\in\Gamma$ をとる．$\mathfrak{p}^2\subsetneq(\pi)+\mathfrak{p}^2\subset\mathfrak{p}$ だから，$(\pi)+\mathfrak{p}^2$ は，$\mathfrak{p}$ の倍数イデアルかつ $\mathfrak{p}^2$ の真の約数イデアルである．したがって，$(\pi)+\mathfrak{p}^2=\mathfrak{p}$ である．$\alpha-\gamma_0\in\mathfrak{p}$ より，

$$\alpha-\gamma_0=\alpha_1\pi+\beta_1,\quad\alpha_1\in\mathcal{O}_k,\beta_1\in\mathfrak{p}^2$$

とかける．すなわち，

$$\alpha\equiv\gamma_0+\alpha_1\pi\pmod{\mathfrak{p}^2}.$$

$\alpha_1\equiv\gamma_1\pmod{\mathfrak{p}}$ なる $\gamma_1\in\Gamma$ をとると，

$$\alpha-\gamma_0-\gamma_1\pi\in\mathfrak{p}^2.$$

$\mathfrak{p}^3\subsetneq(\pi^2)+\mathfrak{p}^3\subset\mathfrak{p}^2$ だから，$(\pi^2)+\mathfrak{p}^3$ は，$\mathfrak{p}^2$ の倍数イデアルかつ $\mathfrak{p}^3$ の真の約数イデアルである．したがって，$(\pi^2)+\mathfrak{p}^3=\mathfrak{p}^2$ である．$\alpha-\gamma_0-\gamma_1\pi\in\mathfrak{p}^2$ より，

$$\alpha-\gamma_0-\gamma_1\pi=\alpha_2\pi^2+\beta_2,\alpha_2\in\mathcal{O}_k,\beta_2\in\mathfrak{p}^3$$

とかける．すなわち，

$$\alpha \equiv \gamma_0 + \gamma_1\pi + \alpha_2\pi^2 \pmod{\mathfrak{p}^3}.$$

$\alpha_2 \equiv \gamma_2 \pmod{\mathfrak{p}}$ なる $\gamma_2 \in \Gamma$ をとると，

$$\alpha \equiv \gamma_0 + \gamma_1\pi + \gamma_2\pi^2 \pmod{\mathfrak{p}^3}.$$

これを繰り返せば，$\gamma_i \in \Gamma$, $i = 0, \ldots, m-1$ で，

$$\alpha \equiv \gamma_0 + \gamma_1\pi + \gamma_2\pi^2 + \cdots + \gamma_{m-1}\pi^{m-1} \pmod{\mathfrak{p}^m}$$

となるものがとれる．$\gamma_i, \gamma_i' \in \Gamma$ として，

$$\sum_{i=0}^{m-1} \gamma_i\pi^i \equiv \sum_{i=0}^{m-1} \gamma_i'\pi^i \pmod{\mathfrak{p}^m} \tag{8.1}$$

とすると，これを mod $\mathfrak{p}$ でみれば，$\gamma_0 \equiv \gamma_0' \pmod{\mathfrak{p}}$, $\gamma_0, \gamma_0' \in \Gamma$ より，$\gamma_0 = \gamma_0'$ である．(8.1) を mod $\mathfrak{p}^2$ でみれば，$\gamma_1\pi \equiv \gamma_1'\pi \pmod{\mathfrak{p}^2}$．もし，$\gamma_1 \not\equiv \gamma_1' \pmod{\mathfrak{p}}$ ならば，$\mathcal{O}_k/\mathfrak{p}$ は体だから，$\alpha \in \mathcal{O}_k$ で，

$$\alpha(\gamma_1 - \gamma_1') \equiv 1 \pmod{\mathfrak{p}}$$

となるものがとれる．よって，$(\gamma_1 - \gamma_1')\alpha + \beta = 1$, $\beta \in \mathfrak{p}$ とかける．これに π をかけて，

$$\pi = (\gamma_1\pi - \gamma_1'\pi)\alpha + \pi\beta \in \mathfrak{p}^2$$

となり矛盾である．よって，$\gamma_1 \equiv \gamma_1' \pmod{\mathfrak{p}}$, $\gamma_1 = \gamma_1'$ である．これを繰り返せば，$\gamma_i = \gamma_i'$, $i = 0, \ldots, m-1$ を得る． □

命題 8.2. $\mathfrak{a}$, $\mathfrak{b}$ を $\mathcal{O}_k$ のイデアルとすると，$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ が成り立つ．

[証明] $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{a_i}$ とすると，中国剰余定理によって，

$$\mathcal{O}_k/\mathfrak{a} \cong (\mathcal{O}_k/\mathfrak{p}_1^{a_1}) \times \cdots \times (\mathcal{O}_k/\mathfrak{p}_r^{a_r}).$$

したがって，

$$N(\mathfrak{a}) = \prod_{i=1}^r N(\mathfrak{p}_i^{a_i}) = \prod_{i=1}^r N(\mathfrak{p}_i)^{a_i}.$$

$\mathfrak{b}$, $\mathfrak{ab}$ についても同様だから，$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ を得る． □

9 単数

k を代数体，$n = [k : \mathbb{Q}]$ とする．この節では，k の整数環 $\mathcal{O}_k$ の可逆元の群 $E_k = \mathcal{O}_k^\times$ の構造について述べる．E_k を k の**単数群**という．$\varepsilon \in E_k$ とすると，$\varepsilon' \in \mathcal{O}_k$ で $\varepsilon\varepsilon' = 1$ となるものが存在する．したがって，このノルムをとれば，

$$\mathrm{N}_{k/\mathbb{Q}}(\varepsilon)\ \mathrm{N}_{k/\mathbb{Q}}(\varepsilon') = \mathrm{N}_{k/\mathbb{Q}}(\varepsilon\varepsilon') = \mathrm{N}_{k/\mathbb{Q}}(1) = 1$$

を得る．$\mathrm{N}_{k/\mathbb{Q}}(\varepsilon),\ \mathrm{N}_{k/\mathbb{Q}}(\varepsilon')$ は $\mathbb{Z}$ の元であるから，$\mathrm{N}_{k/\mathbb{Q}}(\varepsilon) = \pm 1$ である．逆に，$\varepsilon \in \mathcal{O}_k$ が $\mathrm{N}_{k/\mathbb{Q}}(\varepsilon) = \pm 1$ を満たせば，ε 以外の ε の共役たちの積を ε' とすれば，それらはすべて $\bar{\mathbb{Z}}$ の元だから，$\varepsilon' \in \bar{\mathbb{Z}}$ であり，$\varepsilon\varepsilon' = \mathrm{N}_{k/\mathbb{Q}}(\varepsilon) = \pm 1$ より，$\varepsilon' = \pm\dfrac{1}{\varepsilon} \in k \cap \bar{\mathbb{Z}} = \mathcal{O}_k$ である．$\varepsilon(\pm\varepsilon') = 1$ より，$\varepsilon \in E_k$ である．以上によって，次の命題を得た．

命題 9.1. $E_k = \{\varepsilon \in \mathcal{O}_k \mid \mathrm{N}_{k/\mathbb{Q}}(\varepsilon) = \pm 1\}$.

$k = \mathbb{Q}(\theta)$ とし，$\theta^{(i)},\ i = 1, \ldots, n$ を θ の共役とする．必要ならば，共役の番号をつけかえて，

$$\begin{aligned}
&\theta^{(i)} \in \mathbb{R},\ i = 1, \ldots, r_1,\\
&\theta^{(r_1+j)} \in \mathbb{C} - \mathbb{R},\ j = 1, \ldots, r_2,\\
&\theta^{(r_1+r_2+j)} = \overline{\theta^{(r_1+j)}},\ j = 1, \ldots, r_2
\end{aligned}$$

としてよい．$r_1, r_2 \geq 0,\ r_1 + 2r_2 = n$ である．以下，共役はこのようにとることにする．$\alpha \in k$ の i 番目の共役を $\alpha^{(i)}$ とかくことにする．$r = r_1 + r_2 - 1$ とおく．写像 $\ell : k^\times \longrightarrow \mathbb{R}^{r+1}$ を

$$\ell(\alpha) = (\log|\alpha^{(1)}|, \ldots, \log|\alpha^{(r+1)}|)$$

によって定義する．ℓ は乗法群 $k^\times$ から加法群 $\mathbb{R}^{r+1}$ への準同型である．

補題 9.2. $\ell(E_k)$ は $\mathbb{R}^{r+1}$ の離散部分群である．

[証明]　$\ell(E_k)$ の各点 v に対して，その点の開近傍 U で，$\ell(E_k) \cap U = \{v\}$ となるものが存在することを示さなければならない．平行移動によって，$v = 0$ としてよい．$t > 0$ に対して，

$$U_t = \{(x_1, \ldots, x_{r+1}) \in \mathbb{R}^{r+1} \mid |x_i| < t,\ i = 1, \ldots, r+1\}$$

とおけば，U_t は 0 の開近傍である．$\varepsilon \in E_k,\ \ell(\varepsilon) \in \ell(E_k) \cap U_1$ とする．そのとき，$|\varepsilon^{(i)}| < e,\ i = 1, \ldots, n$ であるから，$\varepsilon^{(i)}$ たちの基本対称式の絶対値は有界である．$\varepsilon \in \mathcal{O}_k$ だから，$\varepsilon^{(i)}$ たちの基本対称式の値は $\mathbb{Z}$ の元である．したがって，このような ε は有限個の整数係数の根であるから，有限個しかない．$\ell(E_k) \cap U_1$ は有限集合だから，$0 < t < 1$ を十分小さくとれば，$\ell(E_k) \cap U_t = \{0\}$ にできる．　□

補題 9.3. V を $\mathbb{R}$ 上の s 次元ベクトル空間とし，L をその離散部分群とする．そのとき，L は階数 $m \leq s$ の自由 $\mathbb{Z}$-加群である．

[証明]　L によって生成される V の部分空間を V' とする．$m = \dim V'$ とおけば，$m \leq s$ である．L の元からなる V' の基底がとれる．実際，V' の任意の基底 $v_1, \ldots, v_m$ をとれば，各 v_i は L の元の有限個の 1 次結合だから，それらに現れる L の元のなす有限集合を $\{u_1, \ldots, u_N\}$ とする．V' は $\{u_1, \ldots, u_N\}$ によって生成される V の部分空間だから，この中から V' の基底をとることができる．あらためて，$v_1, \ldots, v_m$ を L の元からなる V' の基底とする．$v_1, \ldots, v_m$ によって $\mathbb{Z}$ 上生成される L の部分群を L' とする．L/L' の代表系として $L \cap F$ がとれる．ここで，

$$F = \left\{ \sum_{i=1}^{m} x_i v_i \;\middle|\; 0 \leq x_i < 1,\ i = 1, \ldots, m \right\}.$$

$v_{m+1}, \ldots, v_s \in V$ を $v_1, \ldots, v_m, v_{m+1}, \ldots, v_s$ が V の基底となるようにとる．

$$C = \left\{ \sum_{i=1}^{s} x_i v_i \;\middle|\; 0 \leq x_i \leq 1,\ i = 1, \ldots, s \right\}.$$

とおけば，C は V のコンパクト部分集合であり，$F \subset C$ である．L は V の離散部分群であるから，$L \cap C$ は有限集合である．実際，L は離散部分群だから，各 $a \in L \cap C$ の開近傍 U_a で，$L \cap U_a = \{a\}$ となるものがとれる．また，L は V の閉部分群である．

$$L \cap C \subset \bigcup_{a \in L \cap C} U_a$$

であり，$(V - L) \cap C \subset (V - L)$ だから，

$$C = ((V - L) \cap C) \cup (L \cap C) \subset (V - L) \cup \cup_{a \in L \cap C} U_a.$$

C はコンパクトだから，有限個の $a_1, \ldots, a_t \in L \cap C$ がとれて，

$$C \subset (V - L) \cup \cup_{i=1}^{t} U_{a_i}.$$

よって，

$$L \cap C \subset \cup_{i=1}^{t} L \cap U_{a_i} = \{a_1, \ldots, a_t\}.$$

したがって，$L \cap F$ も有限集合である．ゆえに，L/L' は有限である．$d = |L/L'|$ とおけば，$dL \subset L'$ である．L' は階数 m の自由 $\mathbb{Z}$-加群であるから，補題 4.22 によって，その部分群 dL も階数 $\leq m$ の自由 $\mathbb{Z}$-加群である．したがって，L も同様である．$L' \subset L$ より，L の階数は m である．　□

$\alpha \in E_k$ とすると，

$$1 = |\,\mathrm{N}_{k/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{r_1} |\alpha^{(i)}| \prod_{i=r_1+1}^{r+1} |\alpha^{(i)}|^2$$

であるから，対数をとって，

$$0 = \sum_{i=1}^{r_1} \log|\alpha^{(i)}| + \sum_{i=r_1+1}^{r+1} 2\log|\alpha^{(i)}|.$$

したがって，$\mathbb{R}^{r+1}$ の r 次元部分空間 V_0 を

$$V_0 = \left\{ (x_1, \ldots, x_{r+1}) \in \mathbb{R}^{r+1} \;\middle|\; \sum_{i=1}^{r_1} x_i + \sum_{i=r_1+1}^{r+1} 2x_i = 0 \right\}$$

によって定義すれば，$\ell(E_k) \subset V_0$ である．補題 9.2 と補題 9.3 より，$\ell(E_k)$ は階数 $\leq r$ の自由 $\mathbb{Z}$-加群である．$\ell(E_k)$ は階数 r の自由 $\mathbb{Z}$-加群であることを示そう．そのためにいくつかの補題を準備する．$r = 0$ ならば，明らかである．よって，$r > 0$ とする．明らかに，$r < n$ である．

補題 9.4. m, n を $m < n$ を満たす自然数とする．n 変数 $x_1, \ldots, x_n$ の m 個の実数係数の 1 次形式

$$f_i(x_1, \ldots, x_n) = a_{i1}x_1 + \cdots + a_{in}x_n, \quad i = 1, \ldots, m$$

に対して，$a = \max_{1 \leq i \leq m} \sum_{j=1}^{n} |a_{ij}|$ とおく．整数 $t > 1$ が任意に与えられたとき，連立不等式

$$|f_i(x_1, \ldots, x_n)| \leq 2at^{1-\frac{n}{m}}, \quad i = 1, \ldots, m$$

の整数解 $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ で，$|x_j| \leq t,\ j = 1, \ldots, n$ を満たすものが存在する．

[証明]　a の定義から，$(x_1, \ldots, x_n) \in \mathbb{R}^n$ に対して，$|x_j| \leq t,\ j = 1, \ldots, n$ ならば，$|f_i(x_1, \ldots, x_n)| \leq at,\ i = 1, \ldots, m$ である．$t > 1,\ n/m > 1$ だから，

$$(t+1)^{n/m} > t^{n/m} + 1.$$

実際，$g(t) = (t+1)^{n/m} - t^{n/m} - 1$ とおけば，

$$g'(t) = (n/m)\{(t+1)^{n/m-1} - t^{n/m-1}\} > 0.$$

$g(0) = 0$ より，$g(t) > 0,\ t > 0$. したがって，自然数 h で，$t^{n/m} < h < (t+1)^{n/m}$ を満たすものが存在する．このとき，$t^n < h^m < (t+1)^n$ である．$\mathbb{R}^m$ の立方体

$$M = \{(y_1, \ldots, y_m) \in \mathbb{R}^m \mid |y_i| \leq at,\ i = 1, \ldots, m\}$$

を考え，M を一辺の長さが $2at/h$ の h^m 個の小立方体に分割する．$x_1, \ldots, x_n$ が $0, 1, \ldots, t$ を独立に動くとき，$(t+1)^n > h^m$ 個の M の点 $(f_1(x), \ldots, f_m(x))$ が得ら

れる．したがって，これらのうちの 2 点で同一の小立方体に属するものが存在する．それを

$$(f_1(x'),\dots,f_m(x')),\ (f_1(x''),\dots,f_m(x''))$$

とする．$x'=(x'_1,\dots,x'_n)$, $x''=(x''_1,\dots,x''_n)$ とすれば，$0\le x'_j,x''_j\le t$, $j=1,\dots,n$ であるから，$x_j=x'_j-x''_j$，$j=1,\dots,n$ とおいて，$x=(x_1,\dots,x_n)$ とおけば，$0\ne x\in\mathbb{Z}^n$, $|x_j|\le t$, $j=1,\dots,n$ であり，$i=1,\dots,m$ について，

$$|f_i(x)|=|f_i(x')-f_i(x'')|\le\frac{2at}{h}<2at^{1-\frac{n}{m}}.$$

□

補題 9.5. 代数体 k によって定まる定数 $c_1>0$ が存在して，各 $1\le i\le r+1$ と任意の整数 $t>1$ に対して，$\alpha\in\mathcal{O}_k$ で，不等式

$$\begin{aligned} c_1^{-n+1}t^{1-n/m}\le|\alpha^{(l)}|\le c_1t^{1-n/m}\qquad & (1\le l\le r+1,\ l\ne i),\\ c_1^{-n+1}t\le|\alpha^{(i)}|\le c_1t & \end{aligned}$$

を満たすものが存在する．ここで，

$$m=\begin{cases} r_1+2r_2-1=n-1, & i\le r_1\\ r_1+2(r_2-1)=n-2, & i>r_1.\end{cases}$$

[証明]　$\omega_1,\dots,\omega_n$ を k の整数底とする．各 $1\le l\le r+1$, $l\ne i$ に対して，

$$\begin{aligned} a_{lj}&=\omega_j^{(l)}, && l\le r_1,\\ a_{lj}&=\Re\omega_j^{(l)}, && l>r_1,\\ b_{lj}&=\Im\omega_j^{(l)}, && l>r_1 \end{aligned}$$

とおく．m 個の実数係数の 1 次形式

$$\begin{aligned} f_l(x_1,\dots,x_n)&=\sum_{j=1}^n a_{lj}x_j,\quad 1\le l\le r+1,\ l\ne i,\\ g_l(x_1,\dots,x_n)&=\sum_{j=1}^n b_{lj}x_j,\quad r_1+1\le l\le r+1,\ l\ne i \end{aligned}$$

を考える．補題 9.4 を適用すれば，$x=(x_1,\dots,x_n)\in\mathbb{Z}^n$, $x\ne0$ で，

$$\begin{aligned} |x_j|&\le t, && j=1,\dots,n,\\ |f_l(x)|&\le 2at^{1-n/m}, && 1\le l\le r+1,\ l\ne i,\\ |g_l(x)|&\le 2at^{1-n/m}, && r_1+1\le l\le r+1,\ l\ne i \end{aligned}$$

を満たすものが存在する．ここで，$a = \max\left(\sum_{j=1}^{n} |a_{lj}|, \sum_{j=1}^{n} |b_{lj}|\right)$ である．そのとき，$\alpha = \sum_{j=1}^{n} x_j\omega_j$ とおけば，$0 \neq \alpha \in \mathcal{O}_k$ であり，

$$\begin{aligned} |\alpha^{(l)}| &= |f_l(x)| \leq 2at^{1-n/m}, && l \leq r_1,\ l \neq i, \\ |\alpha^{(l)}| &\leq |f_l(x)| + |g_l(x)| \leq 4at^{1-n/m}, && r_1 + 1 \leq l \leq r,\ l \neq i. \end{aligned}$$

ここで，

$$c_1 = \max\left(4a, \max_{1 \leq l \leq r+1} \sum_{j=1}^{n} |\omega_j^{(l)}|\right)$$

とおけば，

$$|\alpha^{(\nu)}| \leq c_1 t, \quad 1 \leq \nu \leq n$$

かつ

$$|\alpha^{(l)}| \leq c_1 t^{1-n/m}, \quad 1 \leq l \leq r+1,\ l \neq i.$$

したがって，

$$1 \leq |\,\mathrm{N}_{k/\mathbb{Q}}(\alpha)| \leq |\alpha^{(i)}|(c_1 t^{1-n/m})^m (c_1 t)^{n-m-1} = |\alpha^{(i)}| c_1^{n-1} t^{-1},$$

$$c_1^{-n+1} t \leq |\alpha^{(i)}|.$$

また，$1 \leq l \leq r+1$, $l \neq i$ に対して，

$$1 \leq |\,\mathrm{N}_{k/\mathbb{Q}}(\alpha)| \leq |\alpha^{(l)}|(c_1 t^{1-n/m})^{m-1} (c_1 t)^{n-m} = |\alpha^{(l)}| c_1^{n-1} (t^{1-n/m})^{-1},$$

$$c_1^{-n+1} t^{1-n/m} \leq |\alpha^{(l)}|.$$

□

補題 9.6. $1 \leq i \leq r+1$ とする．m, c_1 を補題 9.5 の通りとする．そのとき，$\mathcal{O}_k$ の元の列 $\alpha_\nu \neq 0$, $\nu = 1, 2, \ldots$ で次の性質を持つものが存在する．

$$\begin{aligned} &|\alpha_\nu^{(l)}| > |\alpha_{\nu+1}^{(l)}|, \quad 1 \leq l \leq r+1,\ l \neq i, \\ &|\alpha_\nu^{(i)}| < |\alpha_{\nu+1}^{(i)}|, \\ &|\,\mathrm{N}_{k/\mathbb{Q}}(\alpha_\nu)| \leq c_1^n. \end{aligned}$$

[証明]　整数 M を $M > c_1^n$ かつ $M^{n/m-1} > c_1^n$ を満たすようにとり，整数 $t > 1$ を任意にとる．$t_{\nu+1} = Mt_\nu$, $\nu = 1, 2, \ldots$ とおく．各 t_ν に対して，補題 9.5 より，$\alpha_\nu \in \mathcal{O}_k$ で，

$$\begin{aligned} c_1^{-n+1} t_\nu^{1-n/m} \leq |\alpha_\nu^{(l)}| \leq c_1 t_\nu^{1-n/m} \qquad (1 \leq l \leq r+1,\ l \neq i), \\ c_1^{-n+1} t_\nu \leq |\alpha_\nu^{(i)}| \leq c_1 t_\nu \end{aligned}$$

を満たすものが存在する．M のとりかたから，

$$\begin{aligned} c_1 t_{\nu+1}^{1-n/m} &= c_1 M^{1-n/m} t_\nu^{1-n/m} < c_1^{-n+1} t_\nu^{1-n/m}, \\ c_1^{-n+1} t_{\nu+1} &= c_1^{-n+1} M t_\nu > c_1 t_\nu. \end{aligned}$$

これから，$1 \le l \le r+1$, $l \ne i$ に対して，

$$|\alpha_{\nu+1}^{(l)}| \le c_1 t_{\nu+1}^{1-n/m} < c_1^{-n+1} t_\nu^{1-n/m} \le |\alpha_\nu^{(l)}|,$$

$$|\alpha_{\nu+1}^{(i)}| \ge c_1^{-n+1} t_{\nu+1} > c_1 t_\nu \ge |\alpha_\nu^{(i)}|$$

を得る．また，

$$|\,\mathrm{N}_{k/\mathbb{Q}}(\alpha_\nu)| \le (c_1 t_\nu^{1-n/m})^m (c_1 t_\nu)^{n-m} = c_1^n.$$

□

補題 9.7. $1 \le i \le r+1$ とする．そのとき，単数 $\eta_i \in E_k$ で，$|\eta_i^{(i)}| > 1$, $|\eta_i^{(l)}| < 1$, $1 \le l \le r+1$, $l \ne i$ を満たすものが存在する．

[証明]　補題 9.6 より，$\mathcal{O}_k$ の元の列 $\alpha_\nu \ne 0$, $\nu = 1, 2, \ldots$ で

$$\begin{aligned} &|\alpha_\nu^{(l)}| > |\alpha_{\nu+1}^{(l)}|, \quad 1 \le l \le r+1,\ l \ne i, \\ &|\alpha_\nu^{(i)}| < |\alpha_{\nu+1}^{(i)}|, \\ &|\,\mathrm{N}_{k/\mathbb{Q}}(\alpha_\nu)| \le c_1^n. \end{aligned}$$

を満たすものが存在する．単項イデアル $\mathfrak{a}_\nu = (\alpha_\nu)$ を考えると，そのノルムは $|\,\mathrm{N}_{k/\mathbb{Q}}(\alpha_\nu)| \le c_1^n$ である．ノルムが c_1^n 以下の $\mathcal{O}_k$ のイデアルは有限個しかない．よって，ある番号 $\nu < \mu$ で，$\mathfrak{a}_\nu = \mathfrak{a}_\mu$ となるものが存在する．これは，$\alpha_\mu = \eta_i \alpha_\nu$, $\eta_i \in E_k$ とかけることを意味する．そのとき，

$$\begin{aligned} |\eta_i^{(i)}| &= \frac{|\alpha_\mu^{(i)}|}{|\alpha_\nu^{(i)}|} > 1, \\ |\eta_i^{(l)}| &= \frac{|\alpha_\mu^{(l)}|}{|\alpha_\nu^{(l)}|} < 1, \quad 1 \le l \le r+1,\ l \ne i. \end{aligned}$$

□

補題 9.8. 実数係数の r 次行列 $A = (a_{ij})$ において，

$$a_{ii} > 0, \quad a_{ij} \le 0 \ \ (j \ne i), \quad \sum_{j=1}^{r} a_{ij} > 0 \ \ (1 \le i \le r)$$

ならば，$\det A \ne 0$ である．

[証明] $\det A = 0$ とすると，$0 \neq x = {}^t(x_1, \ldots, x_r) \in \mathbb{R}^r$ で，$Ax = 0$ となるものがとれる．よって，

$$\sum_{j=1}^{r} a_{ij} x_j = 0, \quad 1 \leq i \leq r.$$

$\max\{|x_1|, \ldots, |x_r|\} = |x_p| > 0$ とする．$\sum_{j=1}^{r} a_{pj} x_j = 0$ より，

$$a_{pp} x_p = - \sum_{\substack{1 \leq j \leq r \\ j \neq p}} a_{pj} x_j, \quad a_{pp} = - \sum_{\substack{1 \leq j \leq r \\ j \neq p}} a_{pj} \frac{x_j}{x_p},$$

$$a_{pp} = |a_{pp}| = \left| \sum_{\substack{1 \leq j \leq r \\ j \neq p}} a_{pj} \frac{x_j}{x_p} \right| \leq \sum_{\substack{1 \leq j \leq r \\ j \neq p}} |a_{pj}| = - \sum_{\substack{1 \leq j \leq r \\ j \neq p}} a_{pj}.$$

したがって，$\sum_{j=1}^{r} a_{pj} \leq 0$ となる．しかし，$\sum_{j=1}^{r} a_{pj} > 0$ としたからこれは矛盾である． □

注意 9.9. 補題 9.8 の行列 A について，$\det A > 0$ である．これは，この不等式を満たす行列の全体が単位行列を含む弧状連結領域であり，$\det$ が連続関数であることからわかる．

補題 9.7 より，各 $1 \leq i \leq r+1$ に対して，単数 η_i で，

$$\begin{aligned} &|\eta_i^{(i)}| > 1, \\ &|\eta_i^{(j)}| < 1, \quad j \neq i,\ 1 \leq j \leq r+1 \end{aligned}$$

を満たすものが存在する．このとき，r 個の単数 $\eta_1, \ldots, \eta_r$ の写像 ℓ による像 $\ell(\eta_1), \ldots, \ell(\eta_r) \in V_0$ は $\mathbb{R}$ 上 1 次独立であることを証明しよう．これは，$r \times (r+1)$ 行列

$$\begin{pmatrix} \log|\eta_1^{(1)}| & \cdots & \log|\eta_1^{(r)}| & \log|\eta_1^{(r+1)}| \\ \vdots & \ddots & \vdots & \vdots \\ \log|\eta_r^{(1)}| & \cdots & \log|\eta_r^{(r)}| & \log|\eta_r^{(r+1)}| \end{pmatrix}$$

の階数が r であることである．よって，

$$R_0 = \begin{vmatrix} \log|\eta_1^{(1)}| & \cdots & \log|\eta_1^{(r)}| \\ \vdots & \ddots & \vdots \\ \log|\eta_r^{(1)}| & \cdots & \log|\eta_r^{(r)}| \end{vmatrix} \neq 0$$

を示せばよい．

$$R = \begin{vmatrix} \log|\eta_1^{(1)}| & \cdots & \log|\eta_1^{(r_1)}| & 2\log|\eta_1^{(r_1+1)}| & \cdots & 2\log|\eta_1^{(r)}| \\ \vdots & & \cdots\cdots\cdots\cdots\cdots\cdots & & & \vdots \\ \log|\eta_r^{(1)}| & \cdots & \log|\eta_r^{(r_1)}| & 2\log|\eta_r^{(r_1+1)}| & \cdots & 2\log|\eta_r^{(r)}| \end{vmatrix}$$

とおけば，$R = 2^{r_2-1}R_0$ であるから，$R \neq 0$ を示せばよい．

$$a_{ij} = \begin{cases} \log|\eta_i^{(j)}|, & 1 \leq j \leq r_1, \\ 2\log|\eta_i^{(j)}|, & r_1+1 \leq j \leq r \end{cases}$$

とおけば，実数 a_{ij} は

$$a_{ii} > 0, \qquad a_{ij} < 0 \ \ (1 \leq j \leq r+1,\ j \neq i)$$

を満たす．$|\mathrm{N}_{k/\mathbb{Q}}(\eta_i)| = 1$ より，

$$\sum_{j=1}^{r+1} a_{ij} = 0, \quad 1 \leq i \leq r.$$

よって，

$$\sum_{j=1}^{r} a_{ij} = -a_{i\,r+1} > 0, \quad 1 \leq i \leq r.$$

補題 9.8 より，$R = \det(a_{ij}) \neq 0$ である．したがって，$\ell(E_k)$ は r 個の 1 次独立な元を含む．すでに，$\ell(E_k)$ は r 以下の階数の自由 $\mathbb{Z}$-加群であることを示してあるから，これで $\ell(E_k)$ は丁度階数 r の自由 $\mathbb{Z}$-加群であることが証明された．今，$\zeta \in \ker\ell$ とすれば，$|\zeta^{(i)}| = 1,\ 1 \leq i \leq n$ である．よって，これらは係数が有界である整数係数の n 次モニック多項式の根である．そのよう多項式は有限個しかないから，$W = \ker\ell$ は有限群である．体の乗法群の有限部分群は巡回群であるから，W は有限巡回群である．W は k に含まれる 1 のべき根全体のなす群である．単数 $\varepsilon_1, \ldots, \varepsilon_r$ を $\ell(\varepsilon_1), \ldots, \ell(\varepsilon_r)$ が $\ell(E_k)$ の基底となるようにとる．そのとき，任意の $\eta \in E_k$ に対して，

$$\ell(\eta) = \sum_{i=1}^{r} a_i \ell(\varepsilon_i), \quad a_i \in \mathbb{Z}$$

とかけるから，$\zeta = \eta \prod_{i=1}^{r} \varepsilon_i^{-a_i}$ とおけば，$\zeta \in \ker\ell = W$ である．よって，

$$\eta = \zeta \prod_{i=1}^{r} \varepsilon_i^{a_i}$$

とかける．以上によって，次の定理が得られた．

定理 9.10 (Dirichlet の単数定理)．n 次代数体 k の実共役の個数を r_1, 虚共役の個数を $2r_2$ として，$r = r_1 + r_2 - 1$ とおく．そのとき，k の単数群 E_k は k に含まれる 1 のべき根のなす有限巡回群 W と階数 r の自由アーベル群の直積である．すなわち，$\varepsilon_1, \ldots, \varepsilon_r \in E_k$ が存在して，任意の $\eta \in E_k$ は，

$$\eta = \zeta \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}, \quad \zeta \in W,\ a_1, \ldots, a_r \in \mathbb{Z}$$

の形に一意的にかける．

定義 9.11. $r > 0$ のとき，定理 9.10 のような単数 $\varepsilon_1, \dots, \varepsilon_r$ を k の**基本単数**という．そのとき，行列式

$$R = \begin{vmatrix} \log|\varepsilon_1^{(1)}| & \cdots & \log|\varepsilon_1^{(r_1)}| & 2\log|\varepsilon_1^{(r_1+1)}| & \cdots & 2\log|\varepsilon_1^{(r)}| \\ \vdots & & \cdots\cdots\cdots & & & \vdots \\ \log|\varepsilon_r^{(1)}| & \cdots & \log|\varepsilon_r^{(r_1)}| & 2\log|\varepsilon_r^{(r_1+1)}| & \cdots & 2\log|\varepsilon_r^{(r)}| \end{vmatrix}$$

は基本単数のとりかたによらない．この R を k の**単数規準**という．$r = 0$ のとき，すなわち，$k = \mathbb{Q}$ または $k = \mathbb{Q}(\sqrt{-m})$, $m \in \mathbb{Z}$, $m > 0$ のときは，$R = 1$ とする．

10 素数の分解

k を代数体，$n = [k : \mathbb{Q}]$ とする．p を素数とする．定理 7.9 より，単項イデアル $(p) = p\mathcal{O}_k$ は素イデアルの積に順序を除いて一意的に分解される．

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}. \tag{10.1}$$

両辺のノルムをとれば，命題 5.8 と命題 8.2 より，

$$p^n = \mathrm{N}(\mathfrak{p}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{p}_g)^{e_g}$$

である．よって，$\mathrm{N}(\mathfrak{p}_i) = p^{f_i}$, $i = 1, \dots, g$ の形であり，

$$n = e_1 f_1 + \cdots + e_g f_g \tag{10.2}$$

が成り立つ．自然な準同型 $\mathbb{Z} \longrightarrow \mathcal{O}_k/\mathfrak{p}_i$ の核は $\mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z}$ であり，これは，体の単射準同型 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{O}_k/\mathfrak{p}_i$ を引き起こす．

定義 10.1. (10.1) における e_i, f_i をそれぞれ，素イデアル $\mathfrak{p}_i$ の $k/\mathbb{Q}$ における**分岐指数**，**剰余次数**という．$e_i > 1$ のとき，素イデアル $\mathfrak{p}_i$ は $k/\mathbb{Q}$ で**分岐する**という．また，$e_i > 1$ となる i が存在するとき，素数 p は $k/\mathbb{Q}$ で**分岐する**という．$e_i = 1$, $i = 1, \dots, g$ のとき，p は**不分岐**であるという．$g = n$, $e_i = f_i = 1$, $i = 1, \dots, n$ のとき，p は $k/\mathbb{Q}$ で**完全分解する**という．

以下，p が k で分岐するための条件を調べる．

$$\widehat{\mathcal{O}}_k = \{\alpha \in k \mid \mathrm{Tr}_{k/\mathbb{Q}}(\alpha\mathcal{O}_k) \subset \mathbb{Z}\}$$

とおく．$k = \mathbb{Q}(\theta)$, $\theta \in \mathcal{O}_k$ とする．$\mathbb{Z}[\theta] \subset \mathcal{O}_k$ より，明らかに，$\widehat{\mathcal{O}}_k \subset \widehat{\mathbb{Z}[\theta]}$ である．また，$\mathcal{O}_k \subset \widehat{\mathcal{O}}_k$ かつ $\widehat{\mathcal{O}}_k$ は $\mathcal{O}_k$-加群であることも明らかである．補題 4.25 より，

$$\mathcal{O}_k \subset \widehat{\mathbb{Z}[\theta]} = \delta^{-1}\mathbb{Z}[\theta] \subset \delta^{-1}\mathcal{O}_k$$

であった．ここで，$\delta = f'(\theta)$, $f(X)$ は θ の $\mathbb{Q}$ 上の最小多項式である．したがって，

$$\mathcal{O}_k \subset \widehat{\mathcal{O}}_k \subset \delta^{-1}\mathcal{O}_k$$

である．したがって，

$$\mathfrak{D}_k = (\widehat{\mathcal{O}}_k)^{-1} = \{\lambda \in k \mid \lambda\widehat{\mathcal{O}}_k \subset \mathcal{O}_k\}$$

とおけば，$\widehat{\mathcal{O}}_k$ が $\mathcal{O}_k$ 加群であることから，$\mathfrak{D}_k$ もそうであり，

$$(\delta) = \delta\mathcal{O}_k \subset \mathfrak{D}_k \subset \mathcal{O}_k$$

である．ゆえに，$\mathfrak{D}_k$ は $\mathcal{O}_k$ のイデアルである．$\mathfrak{D}_k$ を $k/\mathbb{Q}$ の**共役差積**という．また，$\delta = \delta_\theta$ を θ の**共役差積**という．$\mathfrak{D}_k|(\delta)$ である．

命題 10.2. $\mathrm{N}(\mathfrak{D}_k) = D_k$.

[証明]　$\lambda_1, \ldots, \lambda_n$ を (4.4) によって定める．そのとき，(4.5) より，

$$\delta^{-1}\lambda_1, \ldots, \delta^{-1}\lambda_n$$

はトレースに関する $1, \theta, \ldots, \theta^{n-1}$ の双対基底である．$\omega_1, \ldots, \omega_n$ を k の整数底とする．

$$\theta^{j-1} = \sum_{i=1}^{n} a_{ij}\omega_i, \quad .$$

$A = (a_{ij})$, $A^{-1} = (b_{ij})$ とする．そのとき，

$$\omega_j = \sum_{s=1}^{n} b_{sj}\theta^{s-1}, \quad j = 1, \ldots, n$$

である．ここで，

$$\omega_i^* = \sum_{t=1}^{n} a_{it}\delta^{-1}\lambda_t, \quad i = 1, \ldots, n$$

とおけば，

$$\begin{aligned}
\mathrm{Tr}_{k/\mathbb{Q}}(\omega_i\omega_j^*) &= \sum_{t=1}^{n}\sum_{s=1}^{n} a_{it}b_{sj}\,\mathrm{Tr}_{k/\mathbb{Q}}(\theta^{s-1}\delta^{-1}\lambda_t) \\
&= \sum_{t=1}^{n}\sum_{s=1}^{n} a_{it}b_{sj}\delta_{st} \\
&= \sum_{t=1}^{n} a_{it}b_{tj} = \delta_{ij}.
\end{aligned}$$

よって，$\omega_1^*, \ldots, \omega_n^*$ は $\widehat{\mathcal{O}}_k$ の基底である．

$$D_k = D(\mathcal{O}_k) = D(\widehat{\mathcal{O}}_k)(\widehat{\mathcal{O}}_k : \mathcal{O}_k)^2$$

と，$D_k = \det(\omega_i^{(l)})^2$, $D(\widehat{\mathcal{O}}_k) = \det((\omega_j^*)^{(l)})^2$,

$$(\omega_i^{(l)})^t((\omega_j^*)^{(l)}) = (\mathrm{Tr}_{k/\mathbb{Q}}(\omega_i\omega_j^*)) = I$$

より，$D_k D(\widehat{\mathcal{O}}_k) = 1$, したがって，$(\widehat{\mathcal{O}}_k : \mathcal{O}_k) = D_k$ を得る．$\delta\mathcal{O}_k \subset \delta\widehat{\mathcal{O}}_k \subset \mathcal{O}_k$ より，$(\delta) = (\delta\widehat{\mathcal{O}}_k)\mathfrak{c}$, $\mathfrak{c}$ は $\mathcal{O}_k$ のイデアルとかける．ここで，$\lambda \in k$ に対して，$\lambda \in \mathfrak{D}_k$ ならば，$\lambda\widehat{\mathcal{O}}_k \subset \mathcal{O}_k$，$\lambda(\delta\widehat{\mathcal{O}}_k)\mathfrak{c} \subset (\delta)\mathfrak{c}$，$\lambda(\delta) \subset (\delta)\mathfrak{c}$, $\lambda \in \mathfrak{c}$ である．逆に，$\lambda \in \mathfrak{c}$ ならば，$\lambda(\delta\widehat{\mathcal{O}}_k) \subset (\delta\widehat{\mathcal{O}}_k)\mathfrak{c} = (\delta)$, $\lambda\widehat{\mathcal{O}}_k \subset \mathcal{O}_k$, $\lambda \in \mathfrak{D}_k$．よって，$\mathfrak{c} = \mathfrak{D}_k$, $(\delta) = (\delta\widehat{\mathcal{O}}_k)\mathfrak{D}_k$ である．ノルムをとって，

$$|\,\mathrm{N}_{k/\mathbb{Q}}(\delta)| = \mathrm{N}(\delta\widehat{\mathcal{O}}_k)\,\mathrm{N}(\mathfrak{D}_k).$$

一方，$\mathcal{O}_k \subset \widehat{\mathcal{O}}_k \subset \delta^{-1}\mathcal{O}_k$ と $\delta^{-1}\mathcal{O}_k/\mathcal{O}_k \cong \mathcal{O}_k/\delta\mathcal{O}_k$ より，

$$\begin{aligned} |\,\mathrm{N}_{k/\mathbb{Q}}(\delta)| &= (\mathcal{O}_k : \delta\mathcal{O}_k) = (\delta^{-1}\mathcal{O}_k : \mathcal{O}_k) \\ &= (\delta^{-1}\mathcal{O}_k : \widehat{\mathcal{O}}_k)(\widehat{\mathcal{O}}_k : \mathcal{O}_k) \\ &= (\mathcal{O}_k : \delta\widehat{\mathcal{O}}_k)(\widehat{\mathcal{O}}_k : \mathcal{O}_k). = \mathrm{N}(\delta\widehat{\mathcal{O}}_k)(\widehat{\mathcal{O}}_k : \mathcal{O}_k). \end{aligned}$$

したがって，$\mathrm{N}(\mathfrak{D}_k) = (\widehat{\mathcal{O}}_k : \mathcal{O}_k) = D_k$ を得る． □

定義 10.3. R を k の整環とする．R に含まれる $\mathfrak{O}_k$ のイデアルで包含関係で最大のものを R の**導手**という．

命題 10.4. $\theta \in \mathcal{O}_k$, $k = \mathbb{Q}(\theta)$ に対して，$\delta = \delta_\theta$ を θ の共役差積とする．$\mathfrak{f} = \mathfrak{f}_\theta$ を整環 $\mathbb{Z}[\theta]$ の導手とする．そのとき，$(\delta) = \mathfrak{D}_k\mathfrak{f}$ である．

[証明]　命題 10.2 の証明から，$(\delta) = (\delta\widehat{\mathcal{O}}_k)\mathfrak{D}_k$ である．よって，$\mathfrak{f} = \delta\widehat{\mathcal{O}}_k$ を示せばよい．$\delta\widehat{\mathcal{O}}_k \subset \mathcal{O}_k$ かつ $\delta\widehat{\mathcal{O}}_k$ は $\mathcal{O}_k$ のイデアルだから，$\delta\widehat{\mathcal{O}}_k \subset \mathfrak{f}$ である．また，$\delta^{-1}\mathfrak{f} \subset \delta^{-1}\mathbb{Z}[\theta] = \widehat{\mathbb{Z}[\theta]}$ より，

$$\mathrm{Tr}_{k/\mathbb{Q}}(\delta^{-1}\mathfrak{f}\mathcal{O}_k) = \mathrm{Tr}_{k/\mathbb{Q}}(\delta^{-1}\mathfrak{f}) \subset \mathrm{Tr}_{k/\mathbb{Q}}(\widehat{\mathbb{Z}[\theta]}) \subset \mathbb{Z}.$$

よって，$\delta^{-1}\mathfrak{f} \subset \widehat{\mathcal{O}}_k$, $\mathfrak{f} \subset \delta\widehat{\mathcal{O}}_k$．ゆえに，$\mathfrak{f} = \delta\widehat{\mathcal{O}}_k$. □

補題 10.5. $\mathfrak{p}$ を $\mathcal{O}_k$ の素イデアルとする．$p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ とする．$(p) = \mathfrak{p}^e\mathfrak{a}$, $\mathfrak{a}$ は $\mathfrak{p}$ と素な $\mathcal{O}_k$ のイデアルとかく．さらに，$\theta \in \mathfrak{a}$ を $k = \mathbb{Q}(\theta)$, $\theta \notin \mathfrak{p}$ として，$R = \mathbb{Z}[\theta]$ とおく．そのとき，もし，すべての $m = 1, 2, \ldots$ に対して，自然な単射準同型

$$R/(R \cap \mathfrak{p}^m) \longrightarrow \mathcal{O}_k/\mathfrak{p}^m$$

が同型ならば，$\mathfrak{p} \nmid \mathfrak{f}_\theta$ である．

[証明]　$\delta = \delta_\theta$ とおく．$d = \mathrm{N}_{k/\mathbb{Q}}(\delta)$ とおく．$d = p^r a$, $p \nmid a$ とかく．仮定から，任意の $\beta \in \mathcal{O}_k$ に対して，$\rho \in R$ で，$\gamma = \beta - \rho \in \mathfrak{p}^{er}$ となるものが存在する．そのとき，

$$\begin{aligned} R &= \delta\hat{R} \supset \delta\mathcal{O}_k \supset \mathrm{N}_{k/\mathbb{Q}}(\delta)\mathcal{O}_k \\ &= p^r a\mathcal{O}_k = a\mathfrak{p}^{er}\mathfrak{a}^r \supset a\gamma\theta^r\mathcal{O}_k. \end{aligned}$$

よって，$a\gamma\theta^r \in R$．したがって，

$$a\beta\theta^r = a\gamma\theta^r + a\rho\theta^r \in R.$$

これが任意の $\beta \in \mathcal{O}_k$ について成り立つから，$a\theta^r\mathcal{O}_k \subset R$．したがって，$a\theta^r\mathcal{O}_k \subset \mathfrak{f}_\theta$, $\mathfrak{f}_\theta \mid a\theta^r\mathcal{O}_k$ である．$\mathfrak{p} \nmid a\theta^r\mathcal{O}_k$ より，$\mathfrak{p} \nmid \mathfrak{f}_\theta$ である．　□

補題 10.6. $\mathfrak{p}$ を $\mathcal{O}_k$ の素イデアルとし，$\mathfrak{a}$ を $\mathcal{O}_k$ のイデアルで，$\mathfrak{p} \nmid \mathfrak{a}$ であるものとする．そのとき，$\theta \in \mathfrak{a}$, $\theta \notin \mathfrak{p}$ で，次の性質を持つものが存在する：$k = \mathbb{Q}(\theta)$，任意の $m = 1, 2, \ldots$ に対して，$\mathbb{Z}[\theta]$ は $\mathcal{O}_k/\mathfrak{p}^m$ の完全剰余系を含む．

[証明]　$p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ とする．$\mathcal{O}_k/\mathfrak{p}$ は $\mathbb{F}_p$ の f 次拡大体である．$\mathcal{O}_k/\mathfrak{p} = \mathbb{F}_p(\bar{\zeta})$, $\bar{\zeta} = \zeta \pmod{\mathfrak{p}}$, $\zeta \in \mathcal{O}_k$ である．$\bar{\varphi}(X) \in \mathbb{F}_p[X]$ を $\bar{\zeta}$ の $\mathbb{F}_p$ 上の最小多項式とする．$\varphi(X) \in \mathbb{Z}[X]$ を $\bar{\varphi}(X) = \varphi(X) \pmod{p}$ となるものとする．もし，$\varphi(\zeta) \in \mathfrak{p}^2$ ならば，$\pi \in \mathfrak{p} - \mathfrak{p}^2$ をとると，

$$\varphi(\zeta + \pi) \equiv \varphi(\zeta) + \varphi'(\zeta)\pi \pmod{\mathfrak{p}^2}, \quad \varphi'(\zeta) \notin \mathfrak{p}$$

より，$\varphi(\zeta + \pi) \notin \mathfrak{p}^2$ である．よって，最初から，$\varphi(\zeta) \notin \mathfrak{p}^2$ としてよい．中国剰余定理によって，$\theta \in \mathcal{O}_k$ で，$\theta \equiv 0 \pmod{\mathfrak{a}}$, $\theta \equiv \zeta \pmod{\mathfrak{p}^2}$ を満たすものが存在する．さらに，θ は $k = \mathbb{Q}(\theta)$ となるようにとれる．そうでないとして，$\beta \in \mathcal{O}_k$ を $k = \mathbb{Q}(\beta)$ にとり，$0 \neq u \in \mathfrak{a}\mathfrak{p}^2 \cap \mathbb{Z}$ をとる．そのとき，補題**??**の証明から，$v \in \mathbb{Z}$ で，$\theta' = \theta + uv\beta$ が $k = \mathbb{Q}(\theta')$ となるものが存在する．この θ' は，$\theta' \equiv 0 \pmod{\mathfrak{a}}$, $\theta' \equiv \zeta \pmod{\mathfrak{p}^2}$ を満たす．よって，はじめから $k = \mathbb{Q}(\theta)$ であるとしてよい．任意の $\xi \in \mathcal{O}_k$ をとる．そのとき，$\psi(X) \in \mathbb{Z}[X]$ で，$\xi \equiv \psi(\zeta) \pmod{\mathfrak{p}}$ となるものが存在する．したがって，$\xi \equiv \psi(\theta) \pmod{\mathfrak{p}}$．したがって，補題の主張の $m = 1$ の場合が証明された．$m > 1$ とする．$\varphi(\zeta) \in \mathfrak{p} - \mathfrak{p}^2$ かつ $\varphi(\theta) \equiv \varphi(\zeta) \pmod{\mathfrak{p}^2}$ より，$\varphi(\theta) \in \mathfrak{p} - \mathfrak{p}^2$ である．したがって，補題 8.1 より，$\xi_0, \ldots, \xi_{m-1}$ を $\mathcal{O}_k/\mathfrak{p}$ の完全代表系からとって，

$$\xi \equiv \xi_0 + \xi_1\varphi(\theta) + \cdots + \xi_{m-1}\varphi(\theta)^{m-1} \pmod{\mathfrak{p}^m}$$

となるようにとれる．$m = 1$ の場合によって，$\mathcal{O}_k/\mathfrak{p}$ の完全代表系は $\mathbb{Z}[\theta]$ からとれたので，$\mathcal{O}_k/\mathfrak{p}^m$ の完全代表系は $\mathbb{Z}[\theta]$ からとれる．　□

定理 10.7. 共役差積 $\mathfrak{D}_k$ はすべての $\theta \in \mathcal{O}_k$ の共役差積 δ_θ たちの最大公約イデアルである．

[証明]　命題10.4より，$\mathfrak{D}_k$ はすべての $\theta \in \mathcal{O}_k$ の共役差積 δ_θ たちの公約イデアルである．補題10.5，10.6より，任意の素イデアル $\mathfrak{p}$ に対して，$\theta \in \mathcal{O}_k$ で，$\mathfrak{p} \nmid \mathfrak{f}_\theta$ となるものが存在する．命題10.4より，$(\delta_\theta) = \mathfrak{D}_k \mathfrak{f}_\theta$ だから，$\mathfrak{D}_k$ はすべての $\theta \in \mathcal{O}_k$ の共役差積 δ_θ たちの最大公約イデアルである．　□

定理 10.8. $\mathfrak{p}$ を $\mathcal{O}_k$ の素イデアルとし，$p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ とする．e を $\mathfrak{p}$ の $k/\mathbb{Q}$ における分岐指数とする．$\mathfrak{p}^\nu \| \mathfrak{D}_k$ とする．そのとき，

$$\begin{aligned} \nu &= e-1, \quad p \nmid e, \\ \nu &> e-1, \quad p | e. \end{aligned}$$

[証明]　$\varphi(X)$, $\theta \in \mathcal{O}_k$ を補題10.6の証明のようにとる．そのとき，$k = \mathbb{Q}(\theta)$, $\mathfrak{p} \nmid \mathfrak{f}_\theta$ であり，$\mathfrak{p} \| \varphi(\theta)$ である．命題10.4より，$\mathfrak{p}^\nu \| \delta = \delta_\theta$ である．$\mathfrak{p} \nmid \mathfrak{f}_\theta$ より，$\gamma \in \mathfrak{f}_\theta$ で，$\gamma \notin \mathfrak{p}$ となるものがとれる．$f(X)$ を θ の $\mathbb{Q}$ 上の最小多項式とし，$\bar{f}(X) = f(X) \pmod p$ の $\mathbb{F}_p[X]$ における分解を

$$\bar{f}(X) = \bar{g}(X)\bar{\varphi}(X)^m$$

とする．ここで，$g(X) \in \mathbb{Z}[X]$ はモニックで，$\bar{g}(X)$ は $\bar{\varphi}(X)$ と互いに素である．そのとき，$g(\theta) \not\equiv 0 \pmod{\mathfrak{p}}$ である．実際，もし，$g(\theta) \equiv 0 \pmod{\mathfrak{p}}$ ならば，$\bar{\varphi}(X)$ が $\theta \pmod{\mathfrak{p}}$ の $\mathbb{F}_p$ 上の最小多項式だから，$\bar{g}(X)$ は $\bar{\varphi}(X)$ で割り切れる．これは矛盾である．$\mathfrak{p} \nmid g(\theta)$, $\mathfrak{p} \| \varphi(\theta)$ より，$\mathfrak{p}^m \| g(\theta)\varphi(\theta)^m$ である．$f(X) = g(X)\varphi(X)^m + ph(X)$, $h(X) \in \mathbb{Z}[X]$ とかける．$X = \theta$ を代入すれば，$f(\theta) = 0$, $\mathfrak{p}^e \| (p)$ より，

$$g(\theta)\varphi(\theta)^m = -ph(\theta) \equiv 0 \pmod{\mathfrak{p}^e}.$$

ゆえに，$m \geq e$ である．$(p) = \mathfrak{p}^e\mathfrak{a}$, $\mathfrak{p} \nmid \mathfrak{a}$ とかく．$\alpha \in \mathcal{O}_k$ を $\alpha \equiv 0 \pmod{\mathfrak{a}}$, $\alpha \equiv 1 \pmod{\mathfrak{p}}$ にとれば，$p | \alpha\varphi(\theta)^e$ である．よって，$\alpha\varphi(\theta)^e = p\omega$, $\omega \in \mathcal{O}_k$ とかける．$\gamma\omega, \gamma\alpha \in \mathfrak{f}_\theta \subset \mathbb{Z}[\theta]$ より，$\psi(X), \xi(X) \in \mathbb{Z}[X]$ が存在して，$\gamma\omega = \psi(\theta)$, $\gamma\alpha = \xi(\theta)$ とかける．$\gamma\alpha\varphi(\theta)^e = p\gamma\omega$ より，$\xi(\theta)\varphi(\theta)^e = p\psi(\theta)$．したがって，

$$\xi(X)\varphi(X)^e - p\psi(X) = f(X)\eta(X), \quad \eta(X) \in \mathbb{Z}[X].$$

これを $\pmod p$ でみれば，

$$\bar{\xi}(X)\bar{\varphi}(X)^e = \bar{f}(X)\bar{\eta}(X) = \bar{g}(X)\bar{\varphi}(X)^m\bar{\eta}(X).$$

ここで，$\gamma\alpha = \xi(\theta)$ は $\mathfrak{p}$ と素だから，$\bar{\xi}(X)$ は $\varphi(\bar{X})$ と素である．よって，$e \geq m$ である．ゆえに，$m = e$ であり，

$$f(X) \equiv g(X)\varphi(X)^e \pmod p.$$

これを微分して，

$$f'(X) \equiv g'(X)\varphi(X)^e + eg(X)\varphi(X)^{e-1}\varphi'(X) \pmod p,$$

$$f'(\theta) \equiv g'(\theta)\varphi(\theta)^e + eg(\theta)\varphi(\theta)^{e-1}\varphi'(\theta) \pmod{p}.$$

したがって，

$$\delta_\theta \equiv eg(\theta)\varphi(\theta)^{e-1}\varphi'(\theta) \pmod{\mathfrak{p}^e}$$

を得る．これと，$\mathfrak{p}\|\varphi(\theta)$, $g(\theta)\varphi'(\theta) \notin \mathfrak{p}$ から，$p \nmid e$ ならば，$\nu = e-1$, $p|e$ ならば，$\nu \geq e$ がわかる． □

定理 10.9 (Dedekind の判別定理)**.** 素数 p が n 次代数体 k において，

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \quad \mathrm{N}(\mathfrak{p}_i) = p^{f_i},\ i = 1, \ldots, g$$

と分解したとする．また，$p^\nu \| D_k$ とする．そのとき， $p \nmid e_i$, $i = 1, \ldots, g$ ならば，

$$\nu = \sum_{i=1}^{g} (e_i - 1) f_i$$

であり，ある i について，$p|e_i$ ならば，

$$\nu > \sum_{i=1}^{g} (e_i - 1) f_i$$

である．特に，p が $k/\mathbb{Q}$ で分岐するための必要十分条件は，p が判別式 D_k を割り切ることである．

定理 10.10. k を n 次代数体，θ を $k = \mathbb{Q}(\theta)$ となる $\mathcal{O}_k$ の元とする．$f(X)$ を θ の $\mathbb{Q}$ 上の最小多項式とし，p を指数 $(\mathcal{O}_k : \mathbb{Z}[\theta])$ と素な素数とする．そのとき，多項式 $f(X) \bmod p$ の $\mathbb{F}_p[X]$ におけるモニック既約多項式への分解を

$$f(X) \equiv \varphi_1(X)^{e_1} \cdots \varphi_g(X)^{e_g} \pmod{p}$$

とすれば，p の k における素イデアル分解は

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

で与えられる．ここで，$\mathfrak{p}_i = (p, \varphi_i(\theta))$ であり，$\mathfrak{p}_i$ の剰余次数は $f_i = \deg \varphi_i(X)$ に等しい．

[証明] $g(X) \in \mathbb{Z}[X]$ に対して，$\bar{g}(X) = g(X) \bmod p \in \mathbb{F}_p[X]$ とかく．$p \nmid (\mathcal{O}_k : \mathbb{Z}[\theta])$ であるから，任意の $\alpha \in \mathcal{O}_k$ に対して，多項式 $g(X) \in \mathbb{Z}[X]$ が存在して，$\alpha \equiv g(\theta) \pmod{p\mathcal{O}_k}$ となる．よって，自然な準同型 $\mathbb{Z}[\theta] \longrightarrow \mathcal{O}_k/p\mathcal{O}_k$ は全射である．その核は $p\mathcal{O}_k \cap \mathbb{Z}[\theta] = p\mathbb{Z}[\theta]$ である．実際，$p\alpha = g(\theta)$, $\alpha \in \mathcal{O}_k$, $g(X) \in \mathbb{Z}[X]$ とすれば，$m = (\mathcal{O}_k : \mathbb{Z}[\theta])$ とおくとき，$ms + pt = 1$, $s, t \in \mathbb{Z}$, $m\alpha = h(\theta)$ とかけるから，$\alpha = sm\alpha + tp\alpha = sh(\theta) + tg(\theta) \in \mathbb{Z}[\theta]$ である．したがって，

$$\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong \mathcal{O}_k/p\mathcal{O}_k$$

を得る．各 $i=1,\dots,g$ に対して，$\bar{\varphi}_i(X)|\bar{f}(X)$ より，準同型

$$\lambda_i : \mathbb{Z}[\theta] \longrightarrow \mathbb{F}_p[X]/(\bar{\varphi}_i(X))$$

を $\lambda_i(g(\theta)) = \bar{g}(X) \bmod (\bar{\varphi}_i(X))$ によって定義できる．これは全射であり，体の同型

$$\mathbb{Z}[\theta]/\ker\lambda_i \cong \mathbb{F}_p[X]/(\bar{\varphi}_i(X))$$

を得る．$p\mathbb{Z}[\theta] \subset \ker\lambda_i$ であるから，自然な全射準同型

$$\mathcal{O}_k/p\mathcal{O}_k \cong \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \longrightarrow \mathbb{Z}[\theta]/\ker\lambda_i \cong \mathbb{F}_p[X]/(\bar{\varphi}_i(X))$$

がある．したがって，素イデアル $\mathfrak{p}_i \supset p\mathcal{O}_k$ が存在して，

$$\tilde{\lambda}_i : \mathcal{O}_k/\mathfrak{p}_i \cong \mathbb{F}_p[X]/(\bar{\varphi}_i(X))$$

となる．$\lambda_i(\varphi_i(\theta)) = 0$ より，$\varphi_i(\theta) \in \mathfrak{p}_i$，したがって，$(p, \varphi_i(\theta)) \subset \mathfrak{p}_i$ である．任意の $\alpha \in \mathfrak{p}_i$ に対して，$g(X) \in \mathbb{Z}[X]$ を，$\alpha \equiv g(\theta) \pmod{p\mathcal{O}_k}$ にとれば，$0 = \tilde{\lambda}_i(\alpha \bmod \mathfrak{p}_i) = \bar{g}(X) \bmod \bar{\varphi}_i(X)$ より，

$$g(X) = \varphi_i(X)h(X) + p\ell(X), \quad h(X), \ell(X) \in \mathbb{Z}[X]$$

とかける．よって，$g(\theta) \in (p, \varphi_i(\theta))$, $\alpha \in (p, \varphi_i(\theta))$ である．ゆえに，$\mathfrak{p}_i = (p, \varphi_i(\theta))$ である．さらに，p を割る素イデアル $\mathfrak{p}$ は，上のような $\mathfrak{p}_i$ しかないことが次のようにわかる．準同型 $\psi : \mathbb{F}_p[X] \longrightarrow \mathcal{O}_k/\mathfrak{p}$ を $\psi(\bar{g}(X)) = g(\theta) \bmod \mathfrak{p}$ によって定義すれば，これは全射であり，体の同型

$$\mathbb{F}_p[X]/\ker\psi \cong \mathcal{O}_k/\mathfrak{p}$$

を得る．$\bar{f}(X) \in \ker\psi$ であり，$\ker\psi$ はモニック既約多項式で生成される単項イデアルであるから，ある i について，$\ker\psi = (\bar{\varphi}_i(X))$ である．そのとき，$0 = \psi(\bar{\varphi}_i(X)) = \varphi_i(\theta) \bmod \mathfrak{p}$ より，$\mathfrak{p}_i = (p, \varphi_i(\theta)) \subset \mathfrak{p}$ がわかる．$\mathfrak{p}_i$, $\mathfrak{p}$ ともに $\mathcal{O}_k$ の極大イデアルであるから，$\mathfrak{p} = \mathfrak{p}_i$ である．$i \neq j$ ならば，$\bar{\varphi}_i(X)$ と $\bar{\varphi}_j(X)$ は互いに素であるから，$a(X), b(X), c(X) \in \mathbb{Z}[X]$ が存在して，

$$a(X)\varphi_i(X) + b(X)\varphi_j(X) = 1 + pc(X)$$

とかける．これから，$1 \in (p, \varphi_i(\theta), \varphi_j(\theta)) = \mathfrak{p}_i + \mathfrak{p}_j$ を得る．よって，$\mathfrak{p}_i \neq \mathfrak{p}_j$ である．$f_i = \deg\varphi_i(X)$ とすれば，同型 $\mathcal{O}_k/\mathfrak{p}_i \cong \mathbb{F}_p[X]/(\bar{\varphi}_i(X))$ より，$\mathrm{N}(\mathfrak{p}_i) = p^{f_i}$ を得る．

$$f(X) = \varphi_1(X)^{e_1} \cdots \varphi_g(X)^{e_g} + pd(X), \quad d(X) \in \mathbb{Z}$$

とかけるから，$X = \theta$ を代入すれば，$f(\theta) = 0$ より，

$$\varphi_1(\theta)^{e_1} \cdots \varphi_g(\theta)^{e_g} \in p\mathcal{O}_k$$

である．$\mathfrak{p}_i = (p, \varphi_i(\theta))$ より，$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \subset p\mathcal{O}_k$ を得る．一方，p の k における素イデアル分解を

$$(p) = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_g^{e_g'}$$

とすれば，$e_i \geq e_i'$, $i = 1, \ldots, g$ を得る．これと

$$\sum_{i=1}^{g} e_i f_i = \deg f(X) = [k : \mathbb{Q}] = \sum_{i=1}^{g} e_i' f_i$$

より，$e_i = e_i'$, $i = 1, \ldots, g$ を得る． □

系 10.11. 各 $i = 1, \ldots, g$ に対して，$\mathcal{O}_k/\mathfrak{p}_i^{e_i} \cong \mathbb{F}_p[X]/(\varphi_i(X)^{e_i})$ が成り立つ．また，$\mathfrak{p}_i^{e_i} = (p, \varphi_i(\theta)^{e_i})$ である．

[証明]　$e_i = 1$ の場合は既に示した．$e_i \geq 2$ とする．$\mathfrak{p}_i = (p, \varphi_i(\theta))$ より，もし，$\mathfrak{p}_i^2 | \varphi_i(\theta)$ ならば，$\mathfrak{p}_i^2 | p$ より，$\mathfrak{p}_i = (p, \varphi_i(\theta)) \subset \mathfrak{p}_i^2$ となって矛盾である．したがって，$\mathfrak{p}_i \| \varphi_i(\theta)$ である．$\mathcal{O}_k/\mathfrak{p}_i \cong \mathbb{F}_p[X]/(\varphi_i(X))$ より，$1, \theta, \ldots, \theta^{f_i - 1}$ は $\mathcal{O}_k/\mathfrak{p}_i$ の $\mathbb{F}_p$ 上の基底である．したがって，補題 8.1 より，$\theta^a \varphi_i(\theta)^b$, $0 \leq a \leq f_i - 1$, $0 \leq b \leq e_i - 1$ が $\mathcal{O}_k/\mathfrak{p}_i^{e_i}$ の $\mathbb{F}_p$ 上の基底としてとれる．$g(X) \longmapsto g(\theta) \bmod \mathfrak{p}_i^{e_i}$ によって定義される準同型 $\mathbb{F}_p[X] \longrightarrow \mathcal{O}_k/\mathfrak{p}_i^{e_i}$ は，明らかに全射である．任意の $g(X) \in \mathbb{F}_p[X]$ は割り算によって，

$$g(X) = r_0(X) + r_1(X)\varphi_i(X) + \cdots + r_{e_i-1}(X)\varphi_i(X)^{e_i-1} + q(X)\varphi_i(X)^{e_i},$$

$r_j(X) \in \mathbb{F}_p[X]$ は $f_i - 1$ 次以下の多項式，とかけるから，この核は $(\varphi_i(X)^{e_i})$ であることがわかる．$\mathfrak{p}_i = (p, \varphi_i(\theta))$, $p \in \mathfrak{p}_i^{e_i}$ より，

$$(p, \varphi_i(\theta)^{e_i}) \subset \mathfrak{p}_i^{e_i} = (p^{e_i}, p^{e_i-1}\varphi_i(\theta), \ \ldots \ , p\varphi_i(\theta)^{e_i-1}, \varphi_i(\theta)^{e_i}) \subset (p, \varphi_i(\theta)^{e_i}).$$

すなわち，$\mathfrak{p}_i^{e_i} = (p, \varphi_i(\theta)^{e_i})$ である． □

命題 10.12. $\mathcal{O}_k$ の $\mathfrak{p}_i$ に関する完備化を $\mathcal{O}_{k,\mathfrak{p}_i}$ とかく．そのとき，$\mathcal{O}_{k,\mathfrak{p}_i}$ は $\theta^\mu \varphi_i(\theta)^\nu$, $0 \leq \mu \leq f_i - 1$, $0 \leq \nu \leq e_i - 1$ を基底とする階数 $e_i f_i$ の自由 $\mathbb{Z}_p$-加群である．

[証明]　i を固定して，$\mathfrak{p}_i = \mathfrak{p}$, $e_i = e$, $f_i = f$, $\varphi_i(\theta) = \pi$ とかく．$(p) = \mathfrak{p}^e\mathfrak{a}$, $(\pi^e) = \mathfrak{p}^e\mathfrak{b}$, $\mathfrak{a}$, $\mathfrak{b}$ は $\mathfrak{p}$ と素な整イデアル，とかける．よって，$(p)\mathfrak{b} = (\pi^e)\mathfrak{a}$ である．$\mathfrak{b}$ のイデアル類の逆の類から $\mathfrak{p}$ と素な整イデアル $\mathfrak{c}$ をとれば，$\mathfrak{b}\mathfrak{c} = (\gamma)$, $\gamma \in \mathcal{O}_k$ は $\mathfrak{p}$ と素である．そのとき，$(p)(\gamma) = (\pi^e)\mathfrak{a}\mathfrak{c}$ より，$\delta = p\gamma/\pi^e$ とおけば，$(\delta) = \mathfrak{a}\mathfrak{c}$ であるから，$\delta \in \mathcal{O}_k$, δ は $\mathfrak{p}$ と素である．$p\gamma = \pi^e\delta$ である．任意の $\alpha \in \mathcal{O}_k$ をとる．任意の $n \geq 1$ に対して，

$$\alpha \equiv \sum_{t=0}^{n-1} p^t \beta_t \pmod{\mathfrak{p}^{ne}},$$

$$\beta_t = \sum_{\mu=0}^{f-1} \sum_{\nu=0}^{e-1} c_{\mu\nu}^{(t)} \theta^\mu \pi^\nu, \quad c_{\mu\nu}^{(t)} \in \{0, 1, \ \ldots \ , p-1\}$$

を満たす $c_{\mu\nu}^{(t)}$ がとれることを示そう．$\delta' \in \mathcal{O}_k$ を $\delta'\delta \equiv 1 \pmod{\mathfrak{p}^{ne}}$ にとる．そのとき，$\pi^e \equiv p\gamma\delta' \pmod{\mathfrak{p}^{(n+1)e}}$ である．$\lambda_0 = \alpha$ とおく．$\lambda_0 \equiv \beta_0 \pmod{\mathfrak{p}^e}$,

$$\beta_0 = \sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} c_{\mu\nu}^{(0)}\theta^\mu\pi^\nu, \quad \exists c_{\mu\nu}^{(0)} \in \{0,1,\dots,p-1\}$$

となる．$\lambda_0 - \beta_0 \in \mathfrak{p}^e = (p,\pi^e)$ であるから，$\lambda_0 - \beta_0 = p\xi_1 + \pi^e\eta_1,\ \xi_1,\eta_1 \in \mathcal{O}_k$ とかける．よって，$\lambda_1 = \xi_1 + \gamma\delta'\eta_1 \in \mathcal{O}_k$ とおけば,

$$\lambda_0 - \beta_0 \equiv p\lambda_1 \pmod{\mathfrak{p}^{(n+1)e}}.$$

$\lambda_1 \equiv \beta_1 \pmod{\mathfrak{p}^e}$,

$$\beta_1 = \sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} c_{\mu\nu}^{(1)}\theta^\mu\pi^\nu, \quad \exists c_{\mu\nu}^{(1)} \in \{0,1,\dots,p-1\}$$

である．$\lambda_1 - \beta_1 = p\xi_2 + \pi^e\eta_2,\ \xi_2,\eta_2 \in \mathcal{O}_k$ とかける．よって，$\lambda_2 = \xi_2 + \gamma\delta'\eta_2 \in \mathcal{O}_k$ とおけば,

$$\lambda_1 - \beta_1 \equiv p\lambda_2 \pmod{\mathfrak{p}^{(n+1)e}}.$$

これを繰り返して，$t = 0,1,2,\dots,n-1$ に対して，$\beta_t, \lambda_t \in \mathcal{O}_k$ で,

$$\beta_t = \sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} c_{\mu\nu}^{(t)}\theta^\mu\pi^\nu, \quad \exists c_{\mu\nu}^{(t)} \in \{0,1,\dots,p-1\},$$

$$\lambda_t - \beta_t \equiv p\lambda_{t+1} \pmod{\mathfrak{p}^{(n+1)e}}$$

となるものをとれる．

$$\lambda_t - p\lambda_{t+1} \equiv \beta_t \pmod{\mathfrak{p}^{(n+1)e}}$$

の両辺に p^t をかけて，$t = 0,1,\dots,n-1$ について加えれば,

$$\alpha - p^n\lambda_n \equiv \sum_{t=0}^{n-1} p^t\,\beta_t \pmod{\mathfrak{p}^{(n+1)e}},$$

$$\alpha \equiv \sum_{t=0}^{n-1} p^t\,\beta_t \pmod{\mathfrak{p}^{ne}}$$

を得る．$c_{\mu\nu} = \sum_{t=0}^{n-1} c_{\mu\nu}^{(t)}p^t \in \mathbb{Z}$ とおけば,

$$\alpha \equiv \sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} c_{\mu\nu}\theta^\mu\pi^\nu \pmod{\mathfrak{p}^{ne}}$$

を得る．次に，任意の$\alpha \in \mathcal{O}_{k,\mathfrak{p}}$をとる．$n = 1, 2, \ldots$について，$\alpha \equiv \alpha_n \pmod{\mathfrak{p}^{ne}\mathcal{O}_{k,\mathfrak{p}}}$となる$\alpha_n \in \mathcal{O}_k$をとる．上で示したことから，$c_{\mu\nu}(n) \in \mathbb{Z}$を

$$\alpha_n \equiv \sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} c_{\mu\nu}(n)\theta^\mu\pi^\nu \pmod{\mathfrak{p}^{ne}}$$

となるようにとれる．

$$\alpha_{n+1} \equiv \sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} c_{\mu\nu}(n+1)\theta^\mu\pi^\nu \pmod{\mathfrak{p}^{(n+1)e}}$$

と$\alpha_{n+1} \equiv \alpha_n \pmod{\mathfrak{p}^{ne}}$より，

$$\sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1}(c_{\mu\nu}(n+1) - c_{\mu\nu}(n))\theta^\mu\pi^\nu \equiv 0 \pmod{\mathfrak{p}^{ne}}.$$

これを$\bmod \mathfrak{p}^e$でみれば，$c_{\mu\nu}(n+1) - c_{\mu\nu}(n) \equiv 0 \pmod{p}, \forall\mu,\nu$を得る．$c_{\mu\nu}(n+1) - c_{\mu\nu}(n) = pd_{\mu\nu}^{(1)}$, $d_{\mu\nu}^{(1)} \in \mathbb{Z}$とかけば，

$$\sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} pd_{\mu\nu}^{(1)}\theta^\mu\pi^\nu \equiv 0 \pmod{\mathfrak{p}^{ne}},$$

したがって，

$$\sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} d_{\mu\nu}^{(1)}\theta^\mu\pi^\nu \equiv 0 \pmod{\mathfrak{p}^{(n-1)e}}.$$

これを$\bmod \mathfrak{p}^e$でみれば，$d_{\mu\nu}^{(1)} \equiv 0 \pmod{p}, \forall\mu,\nu$を得る．この議論を繰り返せば，結局，$c_{\mu\nu}(n+1) - c_{\mu\nu}(n) \equiv 0 \pmod{p^n}, \forall\mu,\nu$を得る．これから，$c_{\mu\nu} = \lim_{n\to\infty} c_{\mu\nu}(n) \in \mathbb{Z}_p$が定まり，

$$\alpha = \lim_{n\to\infty} \alpha_n = \sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} c_{\mu\nu}\theta^\mu\pi^\nu$$

を得る．$\{\theta^\mu\pi^\nu \mid 0 \le \mu \le f-1, 0 \le \nu \le e-1\}$は$\mathbb{Z}_p$上1次独立である．実際，$c_{\mu\nu} \in \mathbb{Z}_p$として，

$$\sum_{\nu=0}^{e-1}\sum_{\mu=0}^{f-1} c_{\mu\nu}\theta^\mu\pi^\nu = 0$$

とする．ここで，もし，ある係数は0でないとすれば，適当なpのべきで割ることによって，ある係数は$\mathbb{Z}_p$の単数であるとしてよい．そのとき，この等式を$\bmod \mathfrak{p}^e$で見ることによって，$c_{\mu\nu} \equiv 0 \pmod{p}, \forall\mu,\nu$を得るが，これはある係数が$\mathbb{Z}_p$の単数であることに矛盾する．したがって，$\{\theta^\mu\pi^\nu \mid 0 \le \mu \le f-1, 0 \le \nu \le e-1\}$は$\mathbb{Z}_p$上1次独立である． □