整数論（雪江明彦）

目次

第 I 巻

初等整数論から p 進数へ（第 1 版第 4 刷）

第 8 章

代数的整数

追加定理 8.0.1. 代数体の整数環は整閉整域である

証明 A を整域，K を A の商体，L/K を有限次拡大とする．B を A の L における整閉包とする．この時，B の商体は L になる（命題 8.1.14）．C を L における B の整閉包とする．ここで，B/A が整拡大，C/B が整拡大なので，C/A も整拡大（命題 8.1.4）となり，$C \subset B$ となる．また，L が B の商体であることを考えれば，$B \subset L$ は明らかに B 上整なので，$B \subset C$ である．以上から，$B = C$ となり，B の商体 L における B の整閉包は B なので B は整閉整域．これを $A = \mathbb{Z}$，$K = \mathbb{Q}$，$L = K$，$B = \mathcal{O}_K$ とすれば代数体 K の整数環 $\mathcal{O}_K$ が整閉整域である． □

8.5 2 次体の整数環

■例 8.5.6

同型で素イデアルが対応する

証明 $\phi : A \to B$ によって $A \simeq B$，A の素イデアルを $\mathfrak{p}$ とする．$a, b \in A$ に対し，$ab \in \mathfrak{p} \Rightarrow a, b \in \mathfrak{p}$．従って，$\phi(ab) = \phi(a)\phi(b) \in \phi(\mathfrak{p}) \Rightarrow \mathfrak{a}, \mathfrak{b} \in \phi(\mathfrak{p})$．すなわち，$\phi(\mathfrak{p})$ は B における素イデアル． □

追加主張 8.5.2. 代数体の整数環 A のイデアル I の素イデアル分解の流れ

証明 素イデアル $\mathfrak{p}$ が素数 p の上にあるとすれば，系 II-1.10.16，命題 II-1.10.13 から，f を $\mathfrak{p}/p$ の相対次数として

$$\mathcal{N}(\mathfrak{p}) = \mathcal{N}_{\mathbb{Z}}(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})) = \mathcal{N}_{\mathbb{Z}}(p^f) = p^f.$$

I の素イデアル分解を $I = {\mathfrak{p}_1}^{a_1} \cdots {\mathfrak{p}_s}^{a_s}$ とする．中国式剰余定理から

$$A/({\mathfrak{p}_1}^{a_1} \cdots {\mathfrak{p}_s}^{a_s}) \simeq A/{\mathfrak{p}_1}^{a_1} \times \cdots \times A/{\mathfrak{p}_s}^{a_s}$$

なので，$\mathcal{N}(I) = \mathcal{N}(\mathfrak{p}_1)^{a_1} \cdots$．$\mathfrak{p}_1, \ldots$ の下にある素数を $q_1, \ldots$ とおく（$i \neq j$ であれば $q_i \neq q_j$ とする）．今までの話から，$\mathcal{N}_A(I) = {q_1}^{b_1} \cdots {q_t}^{b_t}$ と表すことができる．

さらに，$A/I \simeq B/J$ とする（B は必ずしも代数体でなくとも良い）．$\mathcal{N}_A(I) = \mathcal{N}_B(J)$ となる．$\mathcal{N}_B(J) = {q_1}^{b_1} \cdots {q_t}^{b_t}$ と素因数分解されれば，I について，$q_1, \ldots, q_t$ の上にある素イデアルで構成されることが分かる．

□

例 8.5.6 の素イデアル分解

証明 $A/I \simeq \mathbb{F}_3 \times \mathbb{F}_5 \simeq A/\mathfrak{p}_1 \times A/\mathfrak{p}_2$ となるので，$\mathfrak{p}_1$ は 3 の上に，$\mathfrak{p}_2$ は 5 の上にある．準同型：

$$\begin{array}{ccccccc} A & \twoheadrightarrow & A/\mathfrak{p}_1 \times A/\mathfrak{p}_2 & = & A/\mathfrak{p}_1 \times A/\mathfrak{p}_2 & \simeq & \mathbb{F}_3 \times \mathbb{F}_5 \\ \cup & & \cup & & \cup & & \cup \\ a + b\sqrt{-5} & \longmapsto & ([a + b\sqrt{-5}], [a + b\sqrt{-5}]) & = & ([\overline{a} + \overline{b}\sqrt{-5}], [\overline{a}' + \overline{b}'\sqrt{-5}]) & \longmapsto & (\overline{a} + \overline{b}, \overline{a}') \end{array}$$

を考える．$\overline{a}, \overline{b}$ は a, b を 3 で割った余り，$\overline{a}', \overline{b}'$ は a, b を 5 で割った余り．

$$a + b\sqrt{-5} \in \mathfrak{p}_1 \Leftrightarrow (0, \bullet) \in A/\mathfrak{p}_1 \times A/\mathfrak{p}_2 \Leftrightarrow (0, \bullet) \in \mathbb{F}_3 \times \mathbb{F}_5 \Leftrightarrow \overline{a} + \overline{b} = 0 \Leftrightarrow a + b\sqrt{-5} \in (3, \sqrt{-5} - 1)$$

なので $\mathfrak{p}_1 = (3, \sqrt{-5} - 1)$．同様に

$$a + b\sqrt{-5} \in \mathfrak{p}_1 \Leftrightarrow (\bullet, 0) \in A/\mathfrak{p}_1 \times A/\mathfrak{p}_2 \Leftrightarrow (\bullet, 0) \in \mathbb{F}_3 \times \mathbb{F}_5 \Leftrightarrow \overline{a}' = 0 \Leftrightarrow a + b\sqrt{-5} \in (\sqrt{-5})$$

なので $\mathfrak{p}_2 = (\sqrt{-5})$. □

8.7 不定方程式 $x^3 + y^3 = 1$

■定理 8.7.1

$(a + b)(a + b\omega)(a + b\omega^2) = \varepsilon c^3$ の分解（p.270 の最後と p.271 の上）

証明 $a + b = \varepsilon_1 \alpha \lambda^{\mathrm{ord}(c)-2}, a + b\omega = \varepsilon_2 \beta \lambda, a + b\omega^2 = \varepsilon_3 \gamma \lambda$ とする．ここで，$\varepsilon_1, \varepsilon_2, \varepsilon_3$ は単数とする．さらに，$\omega, \lambda \nmid \alpha, \beta, \gamma$ とする．また，$a + b, a + b\omega, a + b\omega^2$ の 2 つづつの最大公約元は λ なので，α, β, γ は互いに素であり，公約元は単元のうち ± 1 のみ．この時，$c = \lambda^{\mathrm{ord}(c)} k$ とすれば，$\varepsilon k^3 = \varepsilon_1 \varepsilon_2 \varepsilon_3 \alpha \beta \gamma$.

ε は単元なので，$k^3 = \varepsilon_1 \varepsilon_2 \varepsilon_3 \varepsilon^{-1} \alpha \beta \gamma$．ここで，$\varepsilon_1 \varepsilon_2 \varepsilon_3 \varepsilon^{-1}$ は単元 $\{ \pm 1, \pm\omega, \pm\omega^2 \}$ のいずれか．

さらに，$k = a + b\omega$ $(a, b \in \mathbb{Z})$ として $k^3 = (a + b\omega)^3$ が ω の倍数にならないことが初等的に証明できる．よって，k^3 は ω の倍数ではないので，$\varepsilon_1 \varepsilon_2 \varepsilon_3 \varepsilon^{-1} \alpha \beta \gamma$ も ω の倍数ではない．よって，単元 $\varepsilon_1 \varepsilon_2 \varepsilon_3 \varepsilon^{-1}$ は ± 1.

$\mathbb{Z}[\omega]$ が Euclid 環であることに注意し，k を素元分解し，$k = {p_1}^{t_1} \cdots {p_n}^{t_n}$ とする．ここで，α, β は互いに素なので，$p_i \mid \alpha, \beta$ となることはない．さらに $q_1 \mid \alpha, q_2 \mid \beta$ によって $q_1 q_2 = p_i$ となる場合 p_i が素元であるので，q_1 は単元，$q_2 = p_i$ となる（どうせ 3 乗するのでこれでいい）．よって，

$$\alpha = {p_1}^{3t_1} \cdots {p_u}^{3t_u}, \beta = {p_{u+1}}^{3t_{u+1}} \cdots {p_v}^{3t_v}, \gamma = {p_{v+1}}^{3t_{v+1}} \cdots {p_n}^{3t_n}.$$

改めてこれらを $\alpha^3, \beta^3, \gamma^3$ として，示すべき分解が得られる． □

8.11 円分体の整数環

合成体 $M \cdot N$ は M の元の N 上線形結合になる

証明 k を体，A を k 代数，$S = (s_1, \ldots, s_n) \subset A$ を乗法的部分集合とする．乗法的部分集合 S で生成された部分 k 代数 $k[S] = \{ f(s_1, \ldots, s_n) \mid f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n], s_i \in S \}$ で多項式 $f(x_1, \ldots, x_n)$ は各引数 $x_1, \ldots, x_n$ について 1 次で構わない．なぜなら，$x_i {x_j}^2$ の様な項があったらそれは部分 k 代数では $s_1 {s_j}^2 = s_c$ となり，x_c の 1 次式になるから．よって，乗法的部分集合 S で生成された部分 k 代数は $k[S] = \{ \sum_i k_i s_i \mid k_i \in k, s_i \in S \}$ と線形結合になる．

合成体 $M(N)$ は

$$M(N) = \{ f(s_1, \ldots, s_n)/g(s_1, \ldots, s_n) \mid f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in M[x_1, \ldots, x_n], s_i \in N \}$$

となるが，上と同様の考察をすれば $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n)$ は引数 $x_1, \ldots, x_n$ に対し 1 次で構わない．よって合成体は次の様になる：

$$\left\{ \sum_i m_i n_i / \sum_i m_i' n_i' \;\middle|\; m_i, m_i' \in M, n_i, n_i' \in N \right\}.$$

系 7.1.14 から，$M(N)/M$ が体の代数拡大，$N \in M(N)$ なので，$M[N]$ は体．合成体

$$M(N) = N(M) = \left\{ \sum_i m_i n_i / \sum_i m_i' n_i' \;\middle|\; m_i, m_i' \in M, n_i, n_i' \in N \right\}$$

は $M[N] = \{ \sum_i m_i n_i \mid m_i \in M, n_i \in N \}$ の商体である．$M[N]$ は体なので，その商体 $M(N)$ と一致する．よって，$M(N) = M[N] = \{ \sum_i m_i n_i \mid m_i \in M, n_i \in N \}$. □

（完全体の）Galois 拡大の合成体が Galois 拡大である

証明 K を完全体，M/K，N/K を Galois 拡大とする．命題 7.4.13 から $M = K(\alpha)$，$N = K(\beta)$ となり，上の話から $M \cdot N = K(\alpha, \beta)$．$M/K$ は正規拡大なので α の K 上共軛は M に含まれ，同様に β の K 上共軛は N に含まれる．よって α, β の共軛は $M \cdot N$ に含まれる．よって系 7.3.10 から $M \cdot N/K$ は正規拡大．K は完全体なので $M \cdot N/K$ は分離拡大．以上から $M \cdot N/K$ は Galois 拡大． □

■補題 8.11.19

$\mathbb{Q}(\zeta_p)$ が $\pm {\zeta_p}^r$ 以外の 1 の冪根をもてば，$\zeta_4, \zeta_{p^d}, \zeta_q$ のいずれかを含む（p.291 の真ん中ら辺）

証明 奇素数 $p \geq 5$ とする．4 以上の整数は，p^d $(d \in \mathbb{N})$ の倍数か 4 の倍数か p と互いに素な奇素数 q の倍数．なぜなら，もし q の倍数でなければ $2^k, p^l$ $(k, l \in \mathbb{N}, k \geq 2)$ の形であり，これらはそれぞれ 4 の倍数，p^d の倍数．よって，$\mathbb{Q}(\zeta_p)$ が $\pm {\zeta_p}^r$ 以外の 1 の冪根をもてば，$\zeta_4, \zeta_{p^d}, \zeta_q$ のいずれかを含む． □

第 9 章

p 進数

9.1 p 進数と Hensel の補題

■定理 9.1.26

p 進整数環 $\mathbb{Z}_p := \{ x \in \mathbb{Q}_p \mid |x|_p \leq 1 \}$ は Dedekind 環

証明 定理 6.1.6 から単項イデアル整域は一意分解環で，命題 8.1.8 から一意分解環は正規環なので，$\mathbb{Z}_p$ は正規環．例 6.8.35 から単項イデアル整域は Noether 環なので，$\mathbb{Z}_p$ は Noether 環．$\mathbb{Z}_p$ は単項イデアル整域なので命題 6.6.12 から，(0) でない任意の素イデアルが極大イデアルであることが言える．よって，$\mathbb{Z}_p$ は Dedekind 環となる． □

p 進整数の距離が 1 未満であれば $\mathbb{Z}_p$ の単数である

証明 $x \in \mathbb{Z}_p$ の p 進展開

$$x = a_0 + pa_1 + \cdots + p^n a_n + \cdots \ (a_i \in \{ 0, \ldots, p-1 \})$$

で $a_0 \neq 0$ ならば $z \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$. $\mathbb{Z}_p$ は $p\mathbb{Z}_p$ を極大イデアルとする離散付値環なので命題 6.5.8 から $x \in \mathbb{Z}_p^\times$． □

■命題 9.1.31

同型 $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ の存在

証明 $x \in \mathbb{Z}_p$ の p 進展開

$$x = a_0 + pa_1 + \cdots + p^n a_n + \cdots \ (a_i \in \{ 0, \ldots, p-1 \})$$

を考えると，$\mathbb{Z}_p/p\mathbb{Z}_p \ni a_0 + p\mathbb{Z}_p$ となる．自然な準同型 $\phi : \mathbb{Z}_p/p\mathbb{Z}_p \ni a_0 + p\mathbb{Z}_p \mapsto a_0 \in \mathbb{Z}/\mathbb{Z}_p$ によって同型が得られる．同様に考えれば，$x \in \mathbb{Q}_p$ の p 進展開

$$x = p^n(a_0 + pa_1 + \cdots + p^n a_n + \cdots) \ (a_i \in \{ 0, \ldots, p-1 \})$$

に対しても，

$$p^n\mathbb{Z}_p/p^m\mathbb{Z}_p \ni p^n(a_0+\cdots+p^{m-n-1}a_{m-n-1})+p^m\mathbb{Z}_p \mapsto p^n(a_0+\cdots+p^{m-n-1}a_{m-n-1}) \in p^n\mathbb{Z}/p^m\mathbb{Z}$$

が同型となる．□

9.2 2 次形式と Hilbert 記号

■定理 9.2.8

$(\mathbb{Q}_p^\times : \mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}) \leq 2$

証明 $c \in \mathbb{Z}_p^\times$ に対し，体拡大 $\mathbb{Q}_p(\sqrt{c})$ を考える．Hensel の補題から，任意の $e \in \mathbb{Q}_p^\times$ に対し，$x^2-cy^2=e$ を満たす $x,y \in \mathbb{Z}_p$ が存在する．よって $\mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}(x+\sqrt{c}y)=e \in \mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}$ なので，$\mathbb{Z}_p^\times \subset \mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}$．よって，

$$a_0+pa_1+\cdots+p^na_n+\cdots \in \mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}\ (a_0 \neq 0, a_i \in \{0,\ldots,p-1\}).$$

$\mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}(p)=p^2$ なので，$p^2 \in \mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}$．また，$\mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}$ は $\mathbb{Q}_p^\times$ の部分群となるので，$p^{2k}(a_0+pa_1+\cdots) \in \mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}$ $(a_0 \neq 0, k \in \mathbb{Z})$．よって，$\mathbb{Q}_p^\times / \mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}$ の完全代表系は $\{1,p\}$（もしくは $\{1\}$）．よって，$(\mathbb{Q}_p^\times : \mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}) \leq 2$. □

第 II 巻

代数的整数論の基礎（第 1 版第 3 刷）

第 1 章

分岐と完備化

1.2 Dedekind 環の完備化

■命題 1.2.13

自然な写像 $\phi\colon \mathfrak{p}^n/\mathfrak{p}^m \ni a+\mathfrak{p}^m \mapsto a+\mathfrak{p}^m A_\mathfrak{p} \in \mathfrak{p}^n A_\mathfrak{p}/\mathfrak{p}^m A_\mathfrak{p}$ は単射

証明 $\ker(\phi) = (\mathfrak{p}^m A_\mathfrak{p} \cap \mathfrak{p}^n) + \mathfrak{p}^m$ であるが，命題 I-6.5.9(4) から $\mathfrak{p}^m A_\mathfrak{p} \cap \mathfrak{p}^n \subset \mathfrak{p}^m A_\mathfrak{p} \cap A = \mathfrak{p}^m$ なので，$\ker(\phi) \subset 0+\mathfrak{p}^m$．$\ker(\phi) \supset 0+\mathfrak{p}^m$ は明らかなので，$\ker(\phi) = 0+\mathfrak{p}^m$． □

自然な写像 $\mathfrak{p}^n/\mathfrak{p}^m \to \mathfrak{p}^n A_\mathfrak{p}/\mathfrak{p}^m A_\mathfrak{p}$ は全射

証明 $s \in A \setminus \mathfrak{p}$ とすると，$b+cs=1$ となる $b \in \mathfrak{p}^{m-n}$，$c \in A$ が存在する．$a \in \mathfrak{p}^n$ とすれば，$a+\mathfrak{p}^m = (b+cs)(a+\mathfrak{p}^m) = (ab+acs)+\mathfrak{p}^m$ となるが，$ab \in \mathfrak{p}^m$ なので $a+\mathfrak{p}^m = acs+\mathfrak{p}^m$．つまり $a-acs \in \mathfrak{p}^m$．従って，$(a/s)-ca \in \mathfrak{p}^m A_\mathfrak{p}$．以上から，自然な写像は

$$\mathfrak{p}^n/\mathfrak{p}^m \ni ca+\mathfrak{p}^m \mapsto ca+\mathfrak{p}^m A_\mathfrak{p} = a/s+\mathfrak{p}^m A_\mathfrak{p} \in \mathfrak{p}^n A_\mathfrak{p}/\mathfrak{p}^m A_\mathfrak{p}.$$

と表すことができ，これは全射となる． □

準同型 $\phi\colon A/\mathfrak{p}^{m-n} \ni a+\mathfrak{p}^{m-n} \mapsto ax+\mathfrak{p}^m \in \mathfrak{p}^n/\mathfrak{p}^m$ $(x \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1})$ は単射

証明 $\ker(\phi) = \{\, b+\mathfrak{p}^{m-n} \in A/\mathfrak{p}^{m-n} \mid b \in A, bx \in \mathfrak{p}^m \,\}$ である．$\mathrm{ord}_\mathfrak{p}(bx) \geq m$，$\mathrm{ord}_\mathfrak{p}(x) = n$ なので，$\mathrm{ord}_\mathfrak{p}(b) \geq m-n$ であり，$b \in \mathfrak{p}^{m-n} A_\mathfrak{p}$．$b \in A$ でもあるので，命題 I-6.5.9(4) から $b \in A \cap \mathfrak{p}^{m-n} A_\mathfrak{p} = \mathfrak{p}^{m-n}$．従って，$\ker(\phi) = 0+\mathfrak{p}^{m-n}$． □

■命題 1.2.14

Dedekind 環 A の全ての素イデアル $\mathfrak{p}$ に対して $a \in A_\mathfrak{p}$ なら $a \in A$

証明 命題 I-8.3.12 で L の部分 A 加群として A を取れば $A = \bigcap_\mathfrak{p} A_\mathfrak{p} A \supset \bigcap_\mathfrak{p} aA = aA$．よって $a \in A$． □

1.3 分岐と完備化

■注 1.3.6(2)

$\mathfrak{p}$ が Dedekind 環 A の素イデアル，Dedekind 環 B が A の整閉包，$P_1,\dots,P_t \in B$ を $\mathfrak{p}$ の上にある全ての素イデアルとした場合，イデアル $\mathfrak{p}B$ の素イデアル分解が，$\mathfrak{p}B = {P_1}^{e_1}\cdots{P_t}^{e_t}$ $(e_i > 0)$ であり，これらが $\mathfrak{p}$ の上にある B の全ての素イデアルである

証明 $\mathfrak{p}B$ は B の零でないイデアルなので，命題 I-8.3.12 から B の適当な極大イデアル達 P_i' によって $\mathfrak{p}B = \bigcap_i \mathfrak{p}BB_{P_i'}$．Dedekind 環に関する仮定から，$b \in \mathfrak{p}B$ であれば $B/(b)$ が有限である．よって，(b を含み，(b) と異なるイデアルを作るには $B/(b)$ の完全代表系からいくつかの生成元を選ぶことになるので) b を含む素イデアルの数は有限である．従って，$\mathfrak{p}B$ を含む素イデアルの数も有限である．

$P_i' \subset B$ が素イデアルで $\mathfrak{p}B \nsubseteq P_i'$ なら $s \in \mathfrak{p}B \setminus P_i'$ とすると，s は $B_{P_i'}$ の単元．つまり，有限個の ($\mathfrak{p}B \subset P_i'$ を満たす) 素イデアル P_i' に対し，$\mathfrak{p}B_{P_i'} = B_{P_i'}$ が成立する．$P_1,\dots,P_t$ を $\mathfrak{p}B$ を含む全ての素イデアルとする．命題 I-8.3.15 により $\mathfrak{p}BB_{P_i} = {P_i}^{e_i}$ なる $e_i \in \mathbb{Z}$ が存在．$\mathfrak{p}B \in P_i$ なので命題 I-8.3.12 から

$$\mathfrak{p}B = \bigcap_i (\mathfrak{p}BB_{P_i} \cap B) = \bigcap_i ({P_i}^{e_i}B_{P_i} \cap B) = \bigcap_i {P_i}^{e_i} = {P_1}^{e_1}\cdots{P_t}^{e_t}$$

が命題 I-6.5.9(4) と中国剰余定理から成立．$\mathfrak{p}B \subset P_i$ ならば $1 \in B$ を考え $\mathfrak{p} \subset P_i$．逆に，$\mathfrak{p} \subset P_i$ ならば両辺に B をかけて (P_i は B のイデアルなので) $\mathfrak{p}B \subset P_i$．よって，$\mathfrak{p} \subset P_i$ なる全ての素イデアル $P_1,\dots,P_t$ によって $\mathfrak{p}B = {P_1}^{e_1}\cdots{P_t}^{e_t}$ $(e_i > 0)$．補題 1.3.3 から $P_1,\dots,P_t \in B$ は $\mathfrak{p}$ の上にある全ての素イデアルで，$\mathfrak{p}B = {P_1}^{e_1}\cdots{P_t}^{e_t}$ $(e_i > 0)$ である．

上の結果により，$\mathfrak{p}B$ の素イデアル分解に現れる素イデアルだけを分岐の考察対象にすれば良い事が分かる． □

■例 1.3.8

$\mathbb{F}_2[x]/((x+1)^2)$ の極大イデアルを求める

証明 $((x+1)^2) \subset (x+1) \subset \mathbb{F}_2[x]$ なので，定理 I-6.1.34 から

$$(\mathbb{F}[x]/((x+1)^2))/((x+1)/((x+1)^2)) \simeq \mathbb{F}_2[x]/(x+1) \simeq \mathbb{F}_2.$$

$\mathbb{F}_2$ は体なので，$(x+1)/((x+1)^2)$ は $\mathbb{F}[x]/((x+1)^2)$ における極大イデアル（命題 6.3.4)． □

■定理 1.3.23

$B_{\mathfrak{p}}$ が階数 n の自由 $A_{\mathfrak{p}}$ 加群なら，A 加群として $B \otimes_A \widehat{A}_{\mathfrak{p}} \simeq {\widehat{A}_{\mathfrak{p}}}^n$ である

証明 A 加群の同型を構成すればよい：

$$B \otimes_A \widehat{A}_{\mathfrak{p}} \ni b \otimes a \mapsto b \otimes 1 \otimes a \in B \otimes_A A_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}}$$

$$
\begin{aligned}
&\mapsto b \otimes a \in B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}} \\
&\mapsto \left(\sum b_i\right) \otimes a \in \left({A_{\mathfrak{p}}}^{\oplus n}\right) \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}} \\
&\mapsto \sum (b_i \otimes a) \in \left(A_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}}\right)^{\oplus n} \\
&\mapsto \sum (ab_i) \in {\widehat{A}_{\mathfrak{p}}}^{\oplus n} \\
&\mapsto (ab_1, \ldots, ab_n) \in {\widehat{A}_{\mathfrak{p}}}^{n}.
\end{aligned}
$$

□

A 加群として $(B \otimes_A \widehat{A}_{\mathfrak{p}})/\mathfrak{p}^m(B \otimes_A \widehat{A}_{\mathfrak{p}}) \simeq {\widehat{A}_{\mathfrak{p}}}^n/\mathfrak{p}^m{\widehat{A}_{\mathfrak{p}}}^n \simeq (\widehat{A}_{\mathfrak{p}}/\mathfrak{p}^m\widehat{A}_{\mathfrak{p}})^n$ である

証明 1 つめの同型は，上で示した同型によって自然に引き起こされる：

$$
B \otimes_A \widehat{A}_{\mathfrak{p}}/\mathfrak{p}^m(B \otimes_A \widehat{A}_{\mathfrak{p}}) \ni b \otimes a + \mathfrak{p}^m(B \otimes_A \widehat{A}_{\mathfrak{p}}) \mapsto (ab_1, \ldots, ab_n) + \mathfrak{p}^m{\widehat{A}_{\mathfrak{p}}}^n \in {\widehat{A}_{\mathfrak{p}}}^n/\mathfrak{p}^m{\widehat{A}_{\mathfrak{p}}}^n.
$$

準同型 $\phi\colon {\widehat{A}_{\mathfrak{p}}}^n \ni (a_1, \ldots, a_n) \mapsto (a_1 + \mathfrak{p}^m A_{\mathfrak{p}}, \ldots, a_n + \mathfrak{p}^m A_{\mathfrak{p}}) \in (\widehat{A}_{\mathfrak{p}}/\mathfrak{p}^m A_{\mathfrak{p}})^n$ の核は $\mathfrak{p}^m {A_{\mathfrak{p}}}^n$ なので，準同型定理から ${\widehat{A}_{\mathfrak{p}}}^n/\mathfrak{p}^m{\widehat{A}_{\mathfrak{p}}}^n \simeq (\widehat{A}_{\mathfrak{p}}/\mathfrak{p}^m\widehat{A}_{\mathfrak{p}})^n$. □

$K \otimes_A B \simeq L$（A 代数の環同型）

証明 $S = A \setminus \{0\}$ とする．命題 I-8.1.13 から $S^{-1}B$ は $S^{-1}A = K$ 上整で K は体なので，命題 I-8.1.12 から $K \otimes_A B = S^{-1}B$ も体．よって，$S^{-1}B$ の元 b/a $(b \in B, a \in A \setminus \{0\})$ に対し $c \in B, d \in A \setminus \{0\}$ が存在し $bc/ad = 1$，つまり $bc = ad \in A$ となる．b は任意に選ぶことができるので，$\forall b \in B$ に対し $bc \in A$ となる $c \in A$ が存在することが分かる．よって，L の元 b_0/b_1 $(b_0, b_1 \in B)$ として $b_1c_1 \in A$ となる $c_1 \in A$ を選べば，$b_0/b_1 = b_0c_1/b_1c_1 \in S^{-1}B$ なので $L \subset S^{-1}B$．$S^{-1}B \subset L$ は明らか．よって，$S^{-1}B = L$．全射準同型

$$
\phi\colon K \otimes_A B \ni a \otimes b \mapsto ab \in S^{-1}B = L
$$

を考える．$\ker\phi = \{0\}$ なので単射．よって $a \otimes b \mapsto ab$ によって $K \otimes_A B \simeq L$. □

追加補題 1.3.1. 体の直積は異なる数の体の直積と環同型にはなり得ない

証明 同型 $\phi\colon E_1 \times \cdots E_m \to F_1 \times \cdots \times F_n$ $(m > n)$ によって

$$
\begin{aligned}
\phi(1, 0, \ldots, 0) &= (a_1^{(1)}, \ldots, a_n^{(1)}) \\
\phi(0, 1, \ldots, 0) &= (a_1^{(2)}, \ldots, a_n^{(2)}) \\
&\vdots \\
\phi(0, \ldots, 0, 1) &= (a_1^{(m)}, \ldots, a_n^{(m)})
\end{aligned}
$$

に写るとする．右辺は 0 にならないので，$a_1^{(i)} = \cdots = a_n^{(i)} = 0$ となることはない．i 番目の式と j 番目の式をかけて $(0, \ldots, 0) = (a_1^{(i)}a_1^{(j)}, \ldots, a_n^{(i)}a_n^{(j)})$ となる．よって $a_1^{(i)}, a_1^{(j)}$ のうち少なくとも片方は 0.．このような式が $m(m-1)/2$ 個得られ，これらを全て満たすには $a_1^{(1)}, \ldots, a_1^{(m)}$ のうち $m-1$ 個が 0 である必要があ

る．a_2 などについても同様の議論を行えば，$1 \leq i \leq n$ に対し $a_i^{(1)}, \ldots, a_i^{(m)}$ のうち 0 でないものは高々 1 個しかない．$m > n$ なので $a_1^{(j)} = \cdots = a_n^{(j)} = 0$ となる $1 \leq j \leq m$ が必ず存在し，矛盾． □

追加補題 1.3.2. 体の直積が同型なら，構成する体の間で同型となるペアが存在する

証明 同型 $\phi\colon E_1 \times \cdots E_n \to F_1 \times \cdots \times F_n$ とする．先程と同様の議論から，必要ならば適当に F_i を並び替えることによって

$$\begin{aligned}\phi(1,0,\ldots,0) &= (c_1,0,\ldots,0)\\ \phi(0,1,\ldots,0) &= (0,c_2,\ldots,0)\\ &\vdots\\ \phi(0,\ldots,0,1) &= (0,\ldots,0,c_n)\end{aligned}$$

に写るとして良い．初めの式を 2 乗すれば

$$({c_1}^2,0,\ldots,0) = \phi(1,0,\ldots,0)^2 = \phi(1,0,\ldots,0) = (c_1,0,\ldots,0)$$

なので，${c_1}^2 = c_1$．E_1 は整域なので，$c_1 = 1$ である．他についても同様に，$c_1 = \ldots = c_n = 0$ となる．

$\phi(a_1,\ldots) = (b_1,\ldots)$ とする．上の式とかければ $\phi(a_1,0,\ldots,0) = (b_1,0,\ldots,0)$ となる．これは写像 $\varphi\colon E_1 \to F_1$ を引き起こす：

$$\varphi\colon E_1 \ni a_1 \mapsto \pi_1(\phi(a_1,0,\ldots,0)) \in F_1.$$

ただし，π_1 は $F_1 \times \cdots F_n$ の元の第 1 成分のみを取り出す射影．φ が同型になることは容易に分かる．他についても同様． □

追加補題 1.3.3. 体 E, F に対し $\phi\colon E \simeq F$ とすれば，$\phi(\mathcal{O}_E) = \mathcal{O}_F$.

証明 $x \in \mathcal{O}_E$ とする．x は $\mathbb{Z}$ 上整なので，$a_1,\ldots,a_n \in \mathbb{Z}$，$\psi\colon \mathbb{Z} \to E$ があり

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

これを ϕ でうつせば

$$\phi(x)^n + \phi\circ\psi(a_1)\phi(x)^{n-1} + \cdots + \phi\circ\psi(a_n) = 0$$

なので F 上整となり，$\phi(x) \in \mathcal{O}_F$.

$y \in \mathcal{O}_F$ とする．y は $\mathbb{Z}$ 上整なので，$a_1,\ldots,a_n \in \mathbb{Z}$，$\psi\colon \mathbb{Z} \to F$ があり

$$y^n + \psi(a_1)y^{n-1} + \cdots + \psi(a_n) = 0.$$

$y = \phi(x)$ とすれば

$$\begin{aligned}0 &= \phi(x^n) + \phi\circ\phi^{-1}\circ\psi(a_1)\phi(x^{n-1}) + \cdots + \phi\circ\phi^{-1}\circ\psi(a_n)\\ &= \phi\left(x^n + \phi^{-1}\circ\psi(a_1)x^{n-1} + \cdots + \phi^{-1}\circ\psi(a_n)\right)\end{aligned}$$

なので，$x^n + \phi^{-1}\circ\psi(a_1)x^{n-1} + \cdots + \phi^{-1}\circ\psi(a_n) = 0$ となり，$x \in \mathcal{O}_E$．従って，$y = \phi(x) \in \phi(\mathcal{O}_E)$． □

追加定理 1.3.4. 定理 1.3.23(2) の環同型について

p.24 の最後らへんに書かれているように $\phi_i\colon B \hookrightarrow \widehat{B}_i$ として，環同型

$$B \otimes_A \widehat{A}_{\mathfrak{p}} \ni x \otimes y \mapsto (\phi_1(x)y, \dots, \phi_g(x)y) \in \widehat{B}_1 \times \cdots \times \widehat{B}_g$$

によって $B \otimes_A \widehat{A}_{\mathfrak{p}} \simeq \widehat{B}_1 \times \cdots \times \widehat{B}_g$.

もしくは，逆極限によっても構成できる[*1]．$\mathfrak{p}^n B = {P_1}^{e_1} \cdots {P_g}^{e_g}$ なので，中国式剰余定理から $B/\mathfrak{p}^n B \simeq \prod_{i=1}^g B/{P_i}^{ne_i}$ である．A は Noether 環で B を有限生成 A 加群なので，

$$B \otimes_A \varprojlim (A/\mathfrak{p}^n) \simeq \varprojlim (B/\mathfrak{p}^n B) \simeq \prod_{i=1}^g \varprojlim (B/{P_i}^{ne_i}).$$

K 代数としての環同型 $L \otimes_K \widehat{K}_{\mathfrak{p}} \simeq \widehat{K}_1 \times \cdots \times \widehat{K}_g$ は p.26 の最後らへんに書いてるように構成される：

$$\begin{aligned}
L \otimes_K \widehat{K}_{\mathfrak{p}} \ni a/b \otimes c &\mapsto a \otimes 1/b \otimes c \in B \otimes_A K \otimes_K \widehat{K}_{\mathfrak{p}} \\
&= a \otimes 1 \otimes c/b \in B \otimes_A K \otimes_K \widehat{K}_{\mathfrak{p}} \\
&\mapsto a \otimes c/b \in B \otimes_A \widehat{K}_{\mathfrak{p}} \\
&\mapsto a \otimes 1 \otimes c/b \in B \otimes_A \widehat{A}_{\mathfrak{p}} \otimes_{\widehat{A}_{\mathfrak{p}}} \widehat{K}_{\mathfrak{p}} \\
&\mapsto (\phi_1(a), \dots, \phi_g(a)) \otimes c/b \in \left(\widehat{B}_1 \times \cdots \times \widehat{B}_g\right) \otimes_{\widehat{A}_{\mathfrak{p}}} \widehat{K}_{\mathfrak{p}} \\
&\mapsto (\phi_1(a)c/b, \dots, \phi_g(a)c/b) \in \widehat{L}_1 \times \cdots \times \widehat{L}_g.
\end{aligned}$$

これは K 加群としての同型であるが，$\widehat{K}_{\mathfrak{p}}$ 代数としての環同型にもなる．

$L = K(\alpha)$，α の K 上最小多項式を $f(x)$，$f(x)$ の $\widehat{K}_{\mathfrak{p}}$ での因数分解を $f_1(x), \dots, f_g(x) \in \widehat{K}_{\mathfrak{p}}[x]$ とおく．$f_i(x)$ の根を α_i，$\phi_i(\alpha) = \alpha_i$ とする．K は PID で，$K_{\mathfrak{p}}$ は torsion-free なので，$\widehat{K}_{\mathfrak{p}}$ は K 上平坦である．従って，

$$\begin{aligned}
L \otimes_K \widehat{K}_{\mathfrak{p}} &\simeq (K[x]/(f(x))) \otimes_K \widehat{K}_{\mathfrak{p}} \simeq \left(K[x] \otimes_K \widehat{K}_{\mathfrak{p}}\right)/(f(x)) \simeq \widehat{K}_{\mathfrak{p}}[x]/(f(x)) \\
&\simeq \widehat{K}_{\mathfrak{p}}[x]/(f_1(x)) \times \cdots \times \widehat{K}_{\mathfrak{p}}[x]/(f_g(x)) \simeq \widehat{K}_{\mathfrak{p}}(\alpha_1) \times \cdots \times \widehat{K}_{\mathfrak{p}}(\alpha_g)
\end{aligned}$$

となる．$L \otimes_K \widehat{K}_{\mathfrak{p}} \simeq \widehat{L}_1 \times \cdots$ なので，$\widehat{K}_{\mathfrak{p}}$ 代数の同型

$$\widehat{L}_1 \simeq \widehat{K}_{\mathfrak{p}}(\alpha_1), \dots, \widehat{L}_g \simeq \widehat{K}_{\mathfrak{p}}(\alpha_g)$$

を得る．

$[L : K] = 1$ ならば $L = K$

証明 $L \supset K$ は明らか．L の K 基底として $\{v\}$ が取れる．L の任意の元は kv $(k \in K, v \in L)$ と表すことができる．特に，$1 = kv$ なので $v = k^{-1} \in K$．よって，L の任意の元は K の元の積となるので K の元：$L \subset K$. □

[*1] 参考：数論 I の命題 6.50，補題 6.69 など

$\widehat{B}_i$ は $\widehat{A}_{\mathfrak{p}}$ 上整

証明 $\widehat{B}_i$ は有限生成 $\widehat{A}_{\mathfrak{p}}$ 加群．$\forall x \in \widehat{B}_i$ に対し，$\widehat{A}_{\mathfrak{p}}[x]$ はやはり $\widehat{A}_{\mathfrak{p}}$ 加群 $\widehat{B}_i$ の元となる．つまり $\widehat{A}_{\mathfrak{p}}[x] \subset \widehat{B}_i$．命題 I-8.1.3 から x は $\widehat{A}_{\mathfrak{p}}$ 上整である．よって，$\widehat{B}_i$ は $\widehat{A}_{\mathfrak{p}}$ 上整． □

■定理 1.3.26

追加補題 1.3.5. L/K が Galois 拡大なら，$\forall \sigma \in \mathrm{Gal}(L/K)$ に対し $\sigma(B) = B$ である

証明 $b \in B \subset L$ とすれば b は A 上整なので，系 I-8.1.11 から，b の L における K 上の共軛は全て A 上整となる．つまり，B の元である．Gal は共軛の置換であることに注意して，$\forall \sigma \in \mathrm{Gal}(L/K)$ に対し $\sigma(B) \subset B$．両辺に σ をかけて $\sigma^2(B) \subset \sigma(B) \subset B$．これを繰り返せば，$B = \sigma^{[L:K]}(B) \subset \cdots \subset B$ となる．従って，$\sigma B = B$． □

1.4 Hilbert の理論と分岐・不分岐

■命題 1.4.4

$\mathrm{N}_{L_D/K}(x)$ を考えるときに $\sigma \in \mathrm{Hom}_K^{\mathrm{al}}(L_D, L)$ が出てくる理由

証明 $\mathrm{Hom}_K^{\mathrm{al}}(L_D, \overline{K})$ は $\mathrm{Hom}_K^{\mathrm{al}}(K, \overline{K})$ に延長できるが，$\mathrm{Hom}_K^{\mathrm{al}}(K, \overline{K}) = \mathrm{Aut}_K^{\mathrm{al}} L\colon L \to L$ なので，$\mathrm{Hom}_K^{\mathrm{al}}(L_D, \overline{K})$ は $L_D \to L$．従ってこれを $\mathrm{Hom}_K^{\mathrm{al}}(L_D, L)$ と書くことができる． □

包含写像 $\phi\colon \mathbb{F}_K \hookrightarrow \mathbb{F}_D$ によって $\mathbb{F}_K \simeq \mathbb{F}_D$ である

証明 ϕ は包含写像なので単射．証明の前半で示したように，$\forall x \in B_D$ に対し，$y \in A$ が存在し $x \equiv y \bmod P_D$ とできる．

$$\phi\colon \mathbb{F}_K = A/\mathfrak{p} \ni y + \mathfrak{p} \mapsto y + P_D = x + P_D \in B_D/P_D = \mathbb{F}_D$$

であるので，ϕ は全射となる．よって ϕ により $\mathbb{F}_K \simeq \mathbb{F}_D$． □

■定理 1.4.5

ϕ_L の構成

証明 $\sigma \in D_P \subset \mathrm{Gal}(L/K)$ に対し，自然な準同型 $\phi_L(\sigma)\colon \mathbb{F}_L = B/P \ni b + P \mapsto \sigma(b) + P \in \mathbb{F}_L$ が定まる．$a + \mathfrak{p} \in \mathbb{F}_K$ に対し，$\phi_L(\sigma)(a + \mathfrak{p}) = \sigma(a) + \mathfrak{p} = a + \mathfrak{p}$ なので，$\phi_L(\sigma)$ は $\mathbb{F}_K$ の元に対し恒等的．すなわち，$\phi_L(\sigma) \in \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$ であり，$\phi_L\colon \mathrm{Gal}(L/K) \supset D_P \to \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$ となる．$\ker(\phi_L)$ は $\phi_L(\sigma)$ が恒等的になるような σ，すなわち $\forall b \in B$ に対し $\sigma(b) + P = b + P$ となるような D_P の元である（I_P の定義）． □

Hilbert の理論

証明 $D_P/I_P \simeq \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$ である．この同型は

$$\overline{\phi}_L \colon D_P/I_P \ni \sigma \circ I_P \mapsto (b + P \mapsto \sigma(b) + P) \in \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$$

で与えられる． □

■例 1.4.9

$\mathcal{O}_K$ での素イデアル分解

証明

$$\begin{aligned}\mathcal{O}_K/(2) &\simeq \mathbb{F}_2[x,y]/(x^2-2, y^2-y-1)\\ &\simeq \mathbb{F}_2[x,y]/(x^2, y^2+y+1)\\ &\simeq \mathbb{F}_4[x]/(x^2)\end{aligned}$$

$\mathbb{F}_4$ は $\mathbb{F}_2[\omega] = \{0, 1, \omega, \omega+1\}$ である．$\mathbb{F}_4[x]/(x^2)$ において，$0, x, \omega x, (1+\omega)x$ 以外の元は可逆（6 乗すれば 1 になる）．すなわち，$(x)/(x^2)$ 以外の元が可逆であるので，命題 I-6.5.8 から $\mathbb{F}_4[x]/(x^2)$ は $(x)/(x^2)$ を極大イデアルとする局所環である．先程の同型による $(x)/(x^2) = \{0, x, \omega x, \omega x + x\} + (x^2)$ の逆像を求める：

$$\begin{aligned}\mathbb{F}_4[x]/(x^2) \supset \{0, x, \omega x, \omega x + x\} + (x^2) &\mapsto \{0, x, xy, xy + x\} + (x^2, y^2+y+1) \in \mathbb{F}_2[x,y]/(x^2, y^2+y+1)\\ &= (x) + (x^2, y^2+y+1) \in \mathbb{F}_2[x,y]/(x^2, y^2+y+1)\\ &\mapsto (\sqrt{2}) + (2) \subset \mathcal{O}_K/(2).\end{aligned}$$

従って，$\mathbb{F}_4[x]/(x^2)$ の極大イデアルは $(x)/(x^2)$ で，これに対応する $\mathcal{O}_K/(2)$ の極大イデアルは $(\sqrt{2})/(2)$ となる．よって，

$$\begin{aligned}\mathbb{F}_4 &\simeq \mathbb{F}_4[x]/(x)\\ &\simeq (\mathbb{F}_4[x]/(x^2))/((x)/(x^2))\\ &\simeq (\mathcal{O}_K/(2))/(\sqrt{2}/(2))\\ &\simeq \mathcal{O}_2/(\sqrt{2}).\end{aligned}$$

従って $(\sqrt{2})$ は $2\mathbb{Z}$ の上にある $\mathcal{O}_K$ の素イデアルで，$2\mathcal{O}_K = (\sqrt{2})^2$ であるので，分岐指数は $e((\sqrt{2})/2\mathbb{Z}) = 2$ である． □

$\mathbb{F}_{25}(y)/((y-3)^2)$ は $(y-3)/((y-3)^2)$ を極大イデアルとする局所環

証明 $\mathbb{F}_{25}(y)/((y-3)^2)$ から $(y-3)/((y-3)^2)$ を除いた集合の元 $a(y-3)+b$ $(a, b \in \mathbb{F}_5, b \neq 0)$ を考える．$(a(y-3)+b)^{120} \equiv b^{120} = (b^{24})^{10} = 1^{10} = 1$ なので，命題 I-6.5.8 から $\mathbb{F}_{25}[x]/((y-3)^2)$ は $(y-3)/((y-3)^2)$ を極大イデアルとする局所環である． □

K を体，$f(x)$ を K のモニック既約多項式，$f(x)$ の根を $\alpha \in \overline{K} \setminus K$ として，$K[x]/(f(x)) \simeq K[\alpha]$

証明 系 I-6.6.14 から $K(x)/(f(x))$ は体．準同型 $\phi\colon K[x]/(f(x)) \ni g(x) + (f(x)) \mapsto g(\alpha) \in K[\alpha]$ を考える．系 I-6.1.28 から ϕ は単射である．全射性は明らか．よって，$K[x]/(f(x)) \simeq K$．

例えば x^2-x-1 が既約となる $\mathbb{F}_p$ (実際には $p \equiv 1, 4 \bmod 5$) として，$\mathbb{F}_p[x]/(x^2-x-1) \simeq \mathbb{F}_p[\phi] \simeq \mathbb{F}_{p^2}$． □

K を体，$f(x)$ を K の 1 次モニック多項式として，$K[x]/(f(x)) \simeq K$

証明 $\alpha \in K$ を $f(x)$ の根として，$\phi\colon K[x]/(f(x)) \ni a + (f(x)) \mapsto a \in K$．明らかに全単射． □

K を体，$f(x)$ を K の 2 次モニック可約多項式として，$K[x]/(f(x)) \simeq K \times K$

証明 $\alpha, \beta \in K$ を $f(x)$ の異なる根として，準同型

$$\phi\colon K[x]/(f(x)) \ni ax + b + (f(x)) \mapsto (a\alpha + \beta, a\beta + b) \in K \times K$$

を考える．$a\alpha + b = a\beta + b = 0$ であれば $a = 0, b = 0$ となるので $\ker(\phi) = 0$ となり ϕ は単射である．$\forall c, d \in K \times K$ に対し，$a = (c-d)(\alpha-\beta)^{-1}, b = c - \alpha(c-d)(\alpha-\beta)^{-1}$ とすれば $\phi(a + bx + (f(x))) = (c, d)$ となるので ϕ は全射． □

■命題 1.4.11

不分岐性は Galois 群の作用で不変

証明 L/K を Galois 拡大，M を中間体とする．M/K が不分岐拡大であれば，任意の A の素イデアル $\mathfrak{p}$ と，$\mathfrak{p}$ の上にある $B \cap M$ の素イデアル $P_1, P_2, \ldots$ について，$\mathfrak{p}(B \cap M) = P_1 P_2 \cdots$ が成立する．これに $\sigma \in \mathrm{Gal}(L/K)$ を作用させれば $\sigma(\mathfrak{p})\sigma(B \cap M) = \sigma(P_1)\cdots$．$\mathfrak{p} \subset A \subset K$ なので $\sigma(\mathfrak{p}) = \mathfrak{p}$．追加補題 1.3.5(p.16) から，$\sigma(P_i \cap B) = \sigma(P_i) \cap \sigma(B) = \sigma(P_i) \cap B$．以上まとめて，$\mathfrak{p}B \cap \sigma(M) = \sigma(P_1)\cdots$．ところで，$P_i$ は $M \cap B$ の素イデアルなので $\sigma^{-1}(a), \sigma^{-1}(b) \in M \cap B$ に対し $\sigma^{-1}(a)\sigma^{-1}(b) \in P_i$ ならば $\sigma^{-1}(a) \in P_i$ もしくは $\sigma^{-1}(b) \in P_i$．これに σ を作用させて $a, b \in \sigma M \cap B$ に対し $\sigma(\sigma^{-1}(a)\sigma^{-1}(b)) = ab \in \sigma(P_i)$ ならば $a \in \sigma P_i$ もしくは $b \in \sigma P_i$．よって $\sigma(P_i)$ は $B \cap \sigma(M)$ の素イデアル．よって，$\sigma(P_1), \ldots$ は $\mathfrak{p}$ の上にある $B \cap \sigma(M)$ の全ての素イデアルで，分岐指数は $e(\sigma(P_i)/\mathfrak{p}) = 1$．よって $\sigma(M)$ は K の不分岐拡大．

上の話で $M = L$ $(B \cap M = B)$ とすれば $\mathfrak{p}$ の上にある B の素イデアル $P_1, P_2, \ldots$ は $\mathrm{Gal}(L/K)$ によって互いに写りあう（このうち $P_i \to P_i$ になるのが P_i の分解群）．定理 1.3.26 から $P_i = \sigma(P_j)$ なる $\sigma \in \mathrm{Gal}(L/K)$ は存在するので，$\forall \sigma \in \mathrm{Gal}(L/K)$ によって P_i は $P_1, P_2, \ldots$ に写る．つまり，$\mathrm{Gal}(L/K)$ は $\mathfrak{p}$ の上にある B の素イデアルに推移的に作用する． □

■命題 1.4.12

L/K が Galois 拡大なら $\widehat{L}_1/\widehat{K}_{\mathfrak{p}}$ も Galois 拡大である

証明 $\sigma \in D_1$ は P_1 進距離を変えないので，(x_n) が L の Cauchy 列であれば $(\sigma(x_n))$ も L の Cauchy 列．さらに $\sigma \in \mathrm{Gal}(L/K)$ は $\widehat{K}_\mathfrak{p}$ を不変にする．よって群準同型 $\phi\colon D_1 \to \mathrm{Aut}^{\mathrm{al}}_{\widehat{K}_\mathfrak{p}}(\widehat{L}_1)$ を考えることができる．ここで，σ が $\widehat{L}_1$ に自明に作用するなら，σ は L にも自明に作用するので，$\ker\phi = 1$，つまり ϕ は単射である．よって，$|D_1| \leq |\mathrm{Aut}^{\mathrm{al}}_{\widehat{K}_\mathfrak{p}}(\widehat{L}_1)|$．$L/K$ は Galois 拡大であるので，命題 1.4.7 から $|D_1| = ef$．命題 I-7.4.3(1) から $|\mathrm{Aut}^{\mathrm{al}}_{\widehat{K}_\mathfrak{p}}(\widehat{L}_1)| \leq [\widehat{L}_1 : \widehat{K}_\mathfrak{p}]$．さらに定理 1.3.23(4) から $[\widehat{L}_1 : \widehat{K}_\mathfrak{p}] = ef$．以上から $ef = |D_1| \leq |\mathrm{Aut}^{\mathrm{al}}_{\widehat{K}_\mathfrak{p}}(\widehat{L}_1)| \leq [\widehat{L}_1 : \widehat{K}_\mathfrak{p}] = ef$．よって ϕ は全単射で $|\mathrm{Aut}^{\mathrm{al}}_{\widehat{K}_\mathfrak{p}}(\widehat{L}_1)| = [\widehat{L}_1 : \widehat{K}_\mathfrak{p}]$．命題 I-7.4.3(2) から $\widehat{L}_1/\widehat{K}_\mathfrak{p}$ は Galois 拡大である．さらに，$\mathrm{Gal}(\widehat{L}_1/\widehat{K}_\mathfrak{p})$ の元を L に制限すれば $D_1 \simeq \mathrm{Gal}(\widehat{L}_1/\widehat{K}_\mathfrak{p})$． □

1.5 局所体

■定理 1.5.6

$\alpha \in \mathbb{F}_{q^n}$ に対し，$h(\alpha_0) \equiv 0 \bmod P$ となる $\alpha_0 \in \mathcal{O}_K$ が存在し，異なる α に対しては異なる α_0 が定まる
(Hensel の補題を使うにはこれを示す必要がある)

証明 同型を $\phi\colon \mathbb{F}_{q^n} \to \mathcal{O}_{K^n}/P$ と表す．$(\mathbb{F}^{q^n-1})^\times$ は位数 q^n-1 の群なので，$\{\phi(\alpha)\}^{q^n-1} = \phi(\alpha^{q^n-1}) = \phi(1) = 1$．従って，$\phi(\alpha) \in \mathcal{O}_{K^n}/P$ は $x^{q^n-1} - 1$ の根である．$\phi(\alpha)$ の代表元を α_0 とすれば，これは $(\alpha_0 + P)^{q^n-1} = {\alpha_0}^{q^n-1} + P = 1 + P$ を意味する．従って，$\alpha_0 \in \mathcal{O}_K$ は $h(\alpha_0) \equiv 0 \bmod P$ となる．ϕ は単射なので異なる α に対しては異なる $\phi(\alpha)$ が対応し，その代表元も当然異なる． □

1.7 絶対判別式

■系 1.7.5

代数体 K の整数環 $\mathcal{O}_K$ の $\mathbb{Z}$ 基底 $\boldsymbol{v} = \{v_1, \ldots, v_n\}, \boldsymbol{w} = \{w_1, \ldots, w_n\}$ について $\boldsymbol{w} = A\boldsymbol{b}$ となる $A \in \mathrm{GL}_n(\mathbb{Z})$ があり，$\det A = \pm 1$ である

証明 系 I-8.1.25 から $\mathcal{O}_K$ は $\mathbb{Z}$ 加群．$w_1, \ldots, w_n \in \mathcal{O}_K$ なので，$B \in M_n(\mathbb{Z})$ が存在し $\boldsymbol{w} = B\boldsymbol{v}$．同様に，$C \in M_n(\mathbb{Z})$ が存在し $\boldsymbol{v} = C\boldsymbol{w}$．よって B, C は互いの逆行列になっていて，主張の $A \in \mathrm{GL}_n(\mathbb{Z})$ が存在する．系 I-6.7.9(1) から $\det A \in \mathbb{Z}^\times = \{\pm 1\}$． □

代数体 K の $\mathbb{Q}$ 基底のうち K の整数環 $\mathcal{O}_K$ に含まれるものを $\boldsymbol{v} = \{v_1, \ldots, v_n\}$ として，V を $\boldsymbol{v}$ で生成される $\mathbb{Z}$ 加群とする．K の整数環 $\mathcal{O}_K$ の $\mathbb{Z}$ 基底を $\boldsymbol{w} = \{w_1, \ldots, w_n\}$ として $v_i = \sum_j a_{ij} w_j$, $A = (a_{ij})$ とすれば，$|\det A| = |\mathcal{O}_K/V|$ である

証明 $\mathcal{O}_K$ は $\boldsymbol{w}$ を基底とする $\mathbb{Z}$ 加群なので，命題 I-6.8.26 から，$\mathcal{O}_K \simeq \bigoplus_{\boldsymbol{w}} \mathbb{Z} \simeq \mathbb{Z}^n$（$\mathbb{Z}$ 加群としての同型）．また，

$$V = v_1\mathbb{Z} + \cdots + v_n\mathbb{Z} = \sum_i a_{1i} w_i \mathbb{Z} + \cdots + \sum_i a_{ni} w_i \mathbb{Z} = \left(\sum_i a_{i1}\mathbb{Z}\right) w_1 + \cdots + \left(\sum_i a_{in}\mathbb{Z}\right) w_n$$

であることに注意して，次の準同型を考える：

$$\phi\colon {}^tA\mathbb{Z}^n \ni \left(\sum_i a_{i1}t_i, \dots, \sum_i a_{in}t_i\right) \mapsto \left(\sum_i a_{i1}t_i\right)w_1 + \cdots + \left(\sum_i a_{in}t_i\right)w_n \in V.$$

ϕ は明らかに全射．$V \subset \mathcal{O}_K$ で，$\boldsymbol{w}$ は $\mathcal{O}_K$ の $\mathbb{Z}$ 基底なので $\mathbb{Z}$ 上 1 次独立．$v_i \in \mathcal{O}_K$ で $\boldsymbol{w}$ は $\mathcal{O}_K$ の $\mathbb{Z}$ 基底であるので，$a_{ij} \in \mathbb{Z}$．よって，$(\sum_i a_{i1}t_i)w_1 + \cdots + (\sum_i a_{in}t_i)w_n = 0$ ならば $\mathbb{Z} \ni \sum_i a_{i1}t_i = \cdots = \sum_i a_{in}t_n = 0$．つまり，$\ker\phi = 0$ なので ϕ は単射．以上から，$V \simeq {}^tA\mathbb{Z}^n$．よって系 1.6.3 で $A = \mathbb{Z}, P = {}^tA$ とすれば，$|\mathbb{Z}/(\det A)| = |\mathbb{Z}^n/{}^tA\mathbb{Z}^n|$．$\phi$ の延長によって $\mathbb{Z}^n \simeq \mathcal{O}_K$，$\phi\colon {}^tA\mathbb{Z}^n \simeq V$ なので，$|\mathbb{Z}^n/{}^tA\mathbb{Z}^n| = |\mathcal{O}_K/V|$．よって，$|\det A| = |\mathcal{O}_K/V|$． □

1.8 相対判別式

■補題 1.8.3

$\det P \in A_{\mathfrak{p}}^{\times}$

証明 $\mathrm{ord}_{\mathfrak{p}}(\Delta_{L/K}(v_1, \dots, v_n)) \leq 1$ なので，加法的付値の性質（命題 I-8.4.5(1)）から，

$$\mathrm{ord}_{\mathfrak{p}}((\det P)^2\Delta_{L/K}(w_1, \dots, w_n)) = 2\,\mathrm{ord}_{\mathfrak{p}}(\det P) + \mathrm{ord}_{\mathfrak{p}}(\Delta_{L/K}(w_1, \dots, w_n)) \leq 1.$$

よって，$\mathrm{ord}_{\mathfrak{p}}(\det P) = 0$ であり，$\det P \in A_{\mathfrak{p}}^{\times}$． □

■補題 1.8.7

$s \in \mathfrak{p}^n$ をかける写像 $I/J \to I/J$ が全単射ならば自然な写像 $\mathfrak{p}^nI/\mathfrak{p}^nJ \to I/J$ が全射

証明 自然な写像 $\mathfrak{p}^nI/\mathfrak{p}^nJ \ni a + \mathfrak{p}^nJ \mapsto a + J \in I/J$ は well-defined．s をかける写像 $I/J \to I/J$ が全単射であるので，$a + J \in I/J$ に対し $a's + J = a + J$ となる $a' \in J$ が存在する．従って，自然な写像は次のように書ける：

$$\mathfrak{p}^nI/\mathfrak{p}^nJ \ni a's + \mathfrak{p}^nJ \mapsto a's + J = a + J \in I/J.$$

従って自然な写像は全射． □

■命題 1.8.6

$I/J \simeq I/\mathfrak{a}_1I \oplus \cdots \oplus I/\mathfrak{a}_tI$

証明 $\mathfrak{a}_1 \cdots \mathfrak{a}_t(I/J) = \{0\}$ なので $I/J \simeq (I/J)/((\mathfrak{a}_1 \cdots \mathfrak{a}_t)(I/J))$．$\mathfrak{a}_i + \mathfrak{a}_j = A$ $(i \neq j)$ なので命題 I-6.8.27 から $\simeq (I/J)/(\mathfrak{a}_1I/J) \oplus \cdots \oplus (I/J)/(\mathfrak{a}_tI/J)$．命題 I-6.8.22 から $(I/J)/(\mathfrak{a}_iI/J) \simeq I/\mathfrak{a}_iI$． □

$|A/{\mathfrak{p}_1}^a| = |A/\mathfrak{p}_1|^a$

証明 $A \supset {\mathfrak{p}_1}^{a-1} \supset {\mathfrak{p}_1}^a$ なので命題 I-6.8.22 から，$(A/{\mathfrak{p}_1}^a)/({\mathfrak{p}_1}^{a-1}/{\mathfrak{p}_1}^a) \simeq A/{\mathfrak{p}_1}^{a-1}$．命題 1.2.13(1) から ${\mathfrak{p}_1}^{a-1}/{\mathfrak{p}_1}^a \simeq A/\mathfrak{p}_1$ なので，$(A/{\mathfrak{p}_1}^a)/(A/\mathfrak{p}_1) \simeq A/{\mathfrak{p}_1}^{a-1}$ となり，$((A/{\mathfrak{p}_1}^a) : (A/\mathfrak{p}_1)) = |A/{\mathfrak{p}_1}^{a-1}|$. Lagrange の定理から，

$$|A/{\mathfrak{p}_1}^a| = ((A/{\mathfrak{p}_1}^a) : (A/\mathfrak{p}_1))|A/\mathfrak{p}_1| = |A/{\mathfrak{p}_1}^{a-1}||A/\mathfrak{p}_1|.$$

これを繰り返して，$|A/{\mathfrak{p}_1}^a| = |A/\mathfrak{p}_1|^a$. □

■命題 1.8.9

$I(B_\mathfrak{p}/M \otimes_A A_\mathfrak{p}) = \{0\}$，$B_\mathfrak{p} = M \otimes_A A_\mathfrak{p}$

証明 1 つ目については，$IB_\mathfrak{p} \subset M \otimes_A A_\mathfrak{p}$ を示せばよい．$B \otimes_A A_\mathfrak{p} = B \otimes_A S^{-1}A \simeq S^{-1}B = B_\mathfrak{p}$ なので（補題 1.3.22），$IB_\mathfrak{p} \simeq I(B \otimes_A A_\mathfrak{p})$．ここで $I \subset A$ なので，A 上テンソル積の双線形性から右辺は $(IB) \otimes_A A_\mathfrak{p}$ に等しい．I の定義から $IB \subset M$ なので，$IB_\mathfrak{p} \simeq (IB) \otimes_A A_\mathfrak{p} \subset M \otimes_A A_\mathfrak{p}$ となる．さらに，I は $A_\mathfrak{p}$ の単元を含むので，$B_\mathfrak{p} = IB_\mathfrak{p} \subset M \otimes_A A_\mathfrak{p}$．$M \otimes_A A_\mathfrak{p} \subset B \otimes_A A_\mathfrak{p} \simeq B_\mathfrak{p}$ なので，$B_\mathfrak{p} = M \otimes_A A_\mathfrak{p}$ となる． □

$s\phi(\pi_1(c)) = \phi(s\pi_1(c)) = \phi(\pi_1(b)) = \pi_2(b/1) = s\pi_2(b/s)$

証明 自然な写像 $\psi\colon B \hookrightarrow B_\mathfrak{p}$, ψ が引き起こす準同型 $\phi\colon B/(\mathfrak{p}^aB + M) \to B_\mathfrak{p}/(\mathfrak{p}^aB_\mathfrak{p} + S^{-1}M)$，自然な写像 $\pi_1\colon B \to B/(\mathfrak{p}^aB + M)$，$\pi_2\colon B_\mathfrak{p} \to B_\mathfrak{p}/(\mathfrak{p}^aB_\mathfrak{p} + S^{-1}M)$ に対し，次のような図式：

$$\begin{array}{ccc} B \ni b & \xmapsto{\quad\psi\quad} & b/1 \in B_\mathfrak{p} \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ B/(\mathfrak{p}^aB + M) \ni [b] & \xmapsto{\quad\phi\quad} & [b/1] \in B_\mathfrak{p}/(\mathfrak{p}^aB_\mathfrak{p} + S^{-1}M) \end{array}$$

が得られる．$\pi_1(c) = b' + (\mathfrak{p}^aB + M)$ とすれば，

$$\begin{aligned} &s\phi(\pi_1(c)) = s\phi(b' + (\mathfrak{p}^aB + M)) = s[b'/1 + (\mathfrak{p}^aB_\mathfrak{p} + S^{-1}M)] = sb'/1 + (\mathfrak{p}^aB_\mathfrak{p} + S^{-1}M) \\ &= \phi(sb' + (\mathfrak{p}^aB + M)) = \phi(s(b' + (\mathfrak{p}^aB + M))) = \phi(s\pi_1(c)). \end{aligned}$$

$s\pi_1(c) = \pi_1(b)$ なので $\phi(s\pi_1(c)) = \phi(\pi_1(b)) = \pi_2(\psi(b)) = \pi_2(b/1)$．さらに，

$$\pi_2(b/1) = b/1 + (\mathfrak{p}^aB_\mathfrak{p} + S^{-1}M) = s[b/s + (\mathfrak{p}^aB_\mathfrak{p} + S^{-1}M)] = s\pi_2(b/s).$$

□

$\phi(\pi_1(b)) = 0$ であれば $c \in \mathfrak{p}^aB + M$ と $s \in S$ があり，$b/1 \in c/s$

証明 $\phi(\pi_1(b)) = b/1 + (\mathfrak{p}^aB_\mathfrak{p} + S^{-1}M)$ なので，$b/1 \in (\mathfrak{p}^aB_\mathfrak{p} + S^{-1}M)$ である．よって，$b/1 = c/s \in B_\mathfrak{p}$ となる c, s が存在する． □

N は有限生成・自由 $A_\mathfrak{p}$ 加群

証明 補題 I-8.3.3 から $A_\mathfrak{p}$ は Dedekind 環（つまり Noether 環でもある）．$A_\mathfrak{p}$ の商体は K で，命題 I-8.1.14 から $A_\mathfrak{p}$ の L における整閉包は $B_\mathfrak{p}$．よって命題 I-8.1.24 から $B_\mathfrak{p}$ は有限生成 $A_\mathfrak{p}$ 加群．$A_\mathfrak{p}$ は Noether 環なので，命題 I-6.8.36 から $N \subset B_\mathfrak{p}$ は有限生成 $A_\mathfrak{p}$ 加群．N は有限生成 $A_\mathfrak{p}$ 加群でねじれがないので，自由 $A_\mathfrak{p}$ 加群である（定理 I-6.8.38）． □

$(B_\mathfrak{p} : N) < \infty$ ならば N と $B_\mathfrak{p}$ の階数は等しい

証明 N は $B_\mathfrak{p}$ の部分加群なので，N の $A_\mathfrak{p}$ 基底として $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$, $B_\mathfrak{p}$ の $A_\mathfrak{p}$ 基底として $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\}$ を取ることができる．写像 $\phi\colon B_\mathfrak{p} \ni a_1\boldsymbol{x}_1 + \cdots + a_m\boldsymbol{x}_m \mapsto (a_1, \ldots, a_m) \in {A_\mathfrak{p}}^m$ によって $B_\mathfrak{p} \simeq {A_\mathfrak{p}}^m$ となる．N の元は $a_{n+1} = \cdots = a_m = 0$ となる $B_\mathfrak{p}$ の元と見做すことによって，ϕ を制限すれば $N \simeq {A_\mathfrak{p}}^n$ となる．よって ϕ は同型 $B_\mathfrak{p}/N \simeq {A_\mathfrak{p}}^m/{A_\mathfrak{p}}^n$ を引き起こす．右辺の代表元として $\{(0, \ldots, 0, a_{n+1}, \ldots, a_m) \mid a_i \in A_\mathfrak{p}\}$ を取ることができ，これが有限個となるのは $n = m$ の時だけ． □

$(B_\mathfrak{p} : N) = |A_\mathfrak{p}/(\det P)A_\mathfrak{p}|$

証明 $B_\mathfrak{p}$ は自由 $A_\mathfrak{p}$ 加群であるので，自由基底 $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ があり，$B_\mathfrak{p} = \boldsymbol{x}_1A_\mathfrak{p} + \cdots + \boldsymbol{x}_nA_\mathfrak{p}$．準同型

$$\phi\colon B_\mathfrak{p} \ni \boldsymbol{x}_1a_1 + \cdots + \boldsymbol{x}_na_n \mapsto (a_1, \ldots, a_n) \in {A_\mathfrak{p}}^n$$

は全単射なので，ϕ によって $B_\mathfrak{p} \simeq {A_\mathfrak{p}}^n$ となる．N が自由基底 $\{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n\}$ で生成されるとする．$\boldsymbol{y}_i = \sum_j \boldsymbol{x}_jp_{ji}$ とすれば，

$$\begin{aligned}\phi\colon N = \boldsymbol{y}_1A_\mathfrak{p} + \cdots + \boldsymbol{y}_nA_\mathfrak{p} \ni \boldsymbol{y}_1a_1 + \cdots + \boldsymbol{y}_na_n &= \sum_i p_{1i}a_i\boldsymbol{x}_1 + \cdots + \sum_i p_{ni}a_i\boldsymbol{x}_n \\ \mapsto \left(\sum_i p_{1i}a_i, \ldots, \sum_i p_{ni}a_i\right) &\in P{A_\mathfrak{p}}^n\end{aligned}$$

によって $N \simeq P{A_\mathfrak{p}}^n$．以上から，$\phi$ は写像

$$B_\mathfrak{p}/N \ni b + N \mapsto \phi(b) + P{A_\mathfrak{p}}^n \in {A_\mathfrak{p}}^n/P{A_\mathfrak{p}}^n$$

を引き起こし，これによって $B_\mathfrak{p}/N \simeq {A_\mathfrak{p}}^n/P{A_\mathfrak{p}}^n$．よって，系 1.6.3 から

$$(B_\mathfrak{p} : N) = ({A_\mathfrak{p}}^n : P{A_\mathfrak{p}}^n) = |A_\mathfrak{p}/(\det P)A_\mathfrak{p}|.$$

□

$(B_\mathfrak{p} \otimes_{A_\mathfrak{p}} \widehat{A}_\mathfrak{p} : N \otimes_{A_\mathfrak{p}} \widehat{A}_\mathfrak{p}) = |A_\mathfrak{p}/(\det P)A_\mathfrak{p}|$

証明 先に示した写像 $\phi\colon B_\mathfrak{p} \simeq {A_\mathfrak{p}}^n$，例 1.3.13，命題 1.3.15 を使えば，

$$\begin{array}{ccccc} B_\mathfrak{p} \otimes_{A_\mathfrak{p}} \widehat{A}_\mathfrak{p} & \xrightarrow{\phi\otimes\mathrm{id}} & {A_\mathfrak{p}}^n \otimes_{A_\mathfrak{p}} \widehat{A}_\mathfrak{p} & \xrightarrow{\simeq} & {\widehat{A}_\mathfrak{p}}^n \\ \cup & & \cup & & \cup \\ (\boldsymbol{x}_1a_1 + \cdots + \boldsymbol{x}_na_n) \otimes a & \longmapsto & (a_1, \ldots, a_n) \otimes a & \longmapsto & (a_1a, \ldots, a_na) \end{array}$$

によって同型 $B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}} \simeq \widehat{A}_{\mathfrak{p}}{}^n$ が得られる（$\widehat{A}_{\mathfrak{p}}$ は平坦 A 加群）．これを制限して，

$$\begin{array}{ccccc} N \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}} & \xrightarrow{\phi\otimes\mathrm{id}} & PA_{\mathfrak{p}}{}^n \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}} & \xrightarrow{\simeq} & P\widehat{A}_{\mathfrak{p}}{}^n \\ \cup & & \cup & & \cup \\ (\boldsymbol{y}_1 a_1 + \cdots + \boldsymbol{y}_n a_n) \otimes a & \longmapsto & (\textstyle\sum_i p_{1i} a_i, \ldots, \sum_i p_{ni} a_i) \otimes a & \longmapsto & (\textstyle\sum_i p_{1i} a_i a, \ldots, \sum_i p_{ni} a_i a) \end{array}$$

となる．よって，2 つの同型 $B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}} \simeq \widehat{A}_{\mathfrak{p}}{}^n$ 及び $N \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}} \simeq P\widehat{A}_{\mathfrak{p}}{}^n$ は同じ写像で構成される．さらに，この写像は同型 $B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}}/N \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}} \simeq \widehat{A}_{\mathfrak{p}}{}^n/P\widehat{A}_{\mathfrak{p}}{}^n$ を引き起こす．系 1.6.3 から $(B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}} : N \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\mathfrak{p}}) = |A_{\mathfrak{p}}/(\det P)A_{\mathfrak{p}}|$． □

■命題 1.8.11

$$W/V \simeq \bigoplus_{i=1}^{t} B_i{}^n/(\mathfrak{p}_i{}^{a_i} B_i{}^n + {}^t P B_i{}^n)$$

証明 準同型 $W/JW \ni w + JW \mapsto w + V \in W/V$ の ker は V/JW なので $(W/JW)/(V/JW) \simeq W/V$．準同型 $\phi\colon W = w_1A + \cdots + w_nA \ni w_1a_1 + \cdots + w_na_n \mapsto (a_1, \ldots, a_n) \in A^n$ によって $W/JW \simeq A^n/JA^n$．中国式剰余定理から準同型

$$\varphi\colon A^n/JA^n \ni (a_1, \ldots, a_n) + JA^n \mapsto ((a_1, \ldots, a_n) + \mathfrak{p}_i{}^{a_i} A^n)_{1\le i\le t} \in \bigoplus_{i=1}^{t} A^n/\mathfrak{p}_i{}^{a_i} A^n$$

によって $A^n/JA^n \simeq \bigoplus_{i=1}^t A^n/\mathfrak{p}_i{}^{a_i} A^n$．命題 1.2.13 から準同型

$$\psi_i\colon A^n/\mathfrak{p}_i{}^{a_i} A^n \ni (a_1, \ldots, a_n) + \mathfrak{p}_i{}^{a_i} A^n \mapsto (a_1/s, \ldots, a_n/s) + \mathfrak{p}_i{}^{a_i} A_{\mathfrak{p}_i}{}^n \in A_{\mathfrak{p}_i}{}^n/\mathfrak{p}_i{}^{a_i} A_{\mathfrak{p}_i}{}^n$$

によって $\bigoplus_{i=1}^t A^n/\mathfrak{p}_i{}^{a_i} A^n \simeq \bigoplus_{i=1}^t A_{\mathfrak{p}_i}{}^n/\mathfrak{p}_i{}^{a_i} A_{\mathfrak{p}_i}{}^n$．これらを制限して，

$$\begin{aligned} \phi\colon V = v_1A + \cdots + v_nA \ni v_1a_1 + \cdots + v_na_n &= \sum_j p_{1j} w_j a_1 + \cdots + \sum_j p_{nj} w_j a_n \\ &= \sum_i p_{i1} a_i w_1 + \cdots \sum_i p_{in} a_i w_n \mapsto \left(\sum_i p_{i1} a_i, \ldots, \sum_i p_{in} a_i \right) \in {}^t PA^n \end{aligned}$$

によって $V/JW \simeq {}^t PA^n/JA^n$．

$$\begin{aligned} \varphi\colon {}^t PA^n/JA^n &\ni \left(\sum_j p_{j1} a_i, \ldots, \sum_j p_{jn} a_i \right) + JA^n \\ &\mapsto \left(\left(\sum_j p_{j1} a_i, \ldots, \sum_j p_{jn} a_i \right) + \mathfrak{p}_i{}^{a_i} A^n \right)_{1\le i\le t} \in \bigoplus_{i=1}^{t} {}^t PA^n/\mathfrak{p}_i{}^{a_i} A^n \end{aligned}$$

によって ${}^t PA^n/JA^n \simeq \bigoplus_{i=1}^t {}^t PA^n/\mathfrak{p}_i{}^{a_i} A^n$．

$$\psi_i\colon {}^t PA^n/\mathfrak{p}_i{}^{a_i} A^n \ni \left(\sum_j p_{j1} a_i, \ldots, \sum_j p_{jn} a_i \right) + \mathfrak{p}_i{}^{a_i} A^n$$

$$\mapsto \left(\sum_j p_{j1}a_i/s, \ldots, \sum_j p_{jn}a_i/s \right) + {\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n \in {}^tP{A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n$$

によって $\bigoplus_{i=1}^t {}^tP{A^n}/{\mathfrak{p}_i}^{a_i}A^n \simeq \bigoplus_{i=1}^t {}^tP{A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n$．以上から，2 つの同型

$$W/JW \simeq \bigoplus_{i=1}^t {A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n, \quad V/JW \simeq \bigoplus_{i=1}^t {}^tP{A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n$$

は同じ写像によって構成される．よって，

$$W/V \simeq (W/JW)/(V/JW) \simeq \bigoplus_{i=1}^t ({A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n)/({}^tP{A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n).$$

ところで，自然な準同型

$${A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n \to {A_{\mathfrak{p}_i}}^n/({\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n + {}^tP{A_{\mathfrak{p}_i}}^n)$$

の ker は

$$({\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n + {}^tP{A_{\mathfrak{p}_i}}^n)/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n = {}^tP{A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n$$

なので，準同型定理から

$$({A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n)/({}^tP{A_{\mathfrak{p}_i}}^n/{\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n) \simeq {A_{\mathfrak{p}_i}}^n/({\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n + {}^tP{A_{\mathfrak{p}_i}}^n).$$

以上から，$W/V \simeq \bigoplus_{i=1}^t {A_{\mathfrak{p}_i}}^n/({\mathfrak{p}_i}^{a_i}{A_{\mathfrak{p}_i}}^n + {}^tP{A_{\mathfrak{p}_i}}^n)$. □

1.9 判別式と終結式

■定理 1.9.3

$(\alpha_i - \beta_j)$ は $L[a_0, \alpha_1, \ldots, \beta_m]$ の素イデアルである

証明 準同型

$$\begin{aligned}\phi\colon L[a_0, \alpha_1, \ldots, \beta_m]/(\alpha_i - \beta_j) \ni f(a_0, \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \beta_m) + (\alpha_i - \beta_j)\\ \mapsto f(a_0, \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \beta_m) \in L[a_0, \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \beta_m)]\end{aligned}$$

を考える．$ab \in (\alpha_i - \beta_j)$ とする．$0 = \phi(ab) = \phi(a)\phi(b)$ で $L[a_0, \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \beta_m)]$ は体上の多項式環なので一意分解環であり（命題 I-6.6.23），整域である．よって，$\phi(a) = 0$ もしくは $\phi(b) = 0$ である．よって，$a \in (\alpha_i - \beta_j)$ もしくは $b \in (\alpha_i - \beta_j)$ なので $(\alpha_i - \beta_j)$ は素イデアルである． □

1.10 イデアルの相対ノルム

■補題 1.10.6

$m(\alpha)$ が基底 $\{\alpha^i v_j\}$ に関して M_α が対角に n/l 個並んだブロック行列となる

証明 L の元に α $(\alpha^l + a_1\alpha^{l-1} + \cdots + a_l = 0)$ をかける写像は次のようになる：

$$m(\alpha)\colon l = \sum_{j=1}^{n/l}\sum_{i=0}^{l-1} b_{ji}\alpha^i v_j \mapsto \sum_{j=1}^{n/l}\sum_{i=0}^{l-1} b_{ji}\alpha^{i+1} v_j = \sum_{j=1}^{n/l}\left(\sum_{i=0}^{l-2} b_{ji}\alpha^{i+1}v_j + b_{j,l-1}\alpha^l v_j\right)$$
$$= \sum_{j=1}^{n/l}\left(\sum_{i=1}^{l-1} b_{j,i-1}\alpha^i v_j - b_{j,l-1}\sum_{i=0}^{l-1} a_{l-i}\alpha^i v_j\right).$$

ある j に対し，$m(\alpha)(l)$ の $\alpha^i v_j$ 成分は $i=0$ に対し $-b_{j,l-1}a_l$ であり，$i = 1, \ldots, l-i$ に対し $-b_{j,l-1}a_{l-i} + b_{j,i-1}$ となり，これを行列で表せば

$$\begin{pmatrix} & & & -a_l \\ 1 & & & -a_{l-1} \\ & \ddots & & \vdots \\ & & 1 & -a_1 \end{pmatrix} \begin{pmatrix} b_{j,0} \\ b_{j,1} \\ \vdots \\ b_{j,l-1} \end{pmatrix}$$

となる．よって，この行列をあらわに書けば

$$\left(\begin{array}{ccc|ccc|c|ccc} & & -a_l & & & & & & & \\ 1 & & -a_{l-1} & & & & & & & \\ & \ddots & \vdots & & & & & & & \\ & 1 & -a_1 & & & & & & & \\ \hline & & & & & -a_l & & & & \\ & & & 1 & & -a_{l-1} & & & & \\ & & & & \ddots & \vdots & & & & \\ & & & & 1 & -a_1 & & & & \\ \hline & & & & & & \ddots & & & \\ \hline & & & & & & & & & -a_l \\ & & & & & & & 1 & & -a_{l-1} \\ & & & & & & & & \ddots & \vdots \\ & & & & & & & & 1 & -a_1 \end{array}\right).$$

□

■命題 1.10.7

$\pi_B \in B$ が A 上整なら π_B の K 上最小多項式 $f(x) \in K[x]$ は $A[x]$ の元である

証明 π_B は A 上整なので，$h(\pi_B) = 0$ なるモニック $h(x) \in A[x]$ が存在し，さらに命題 I-7.1.11(2) から $h(x) = g(x)f(x)$ なる $g(x) \in K[x]$ が存在する．$\pi_B = \alpha_1, \alpha_2, \ldots, \alpha_n \in \overline{K}$ を $f(x)$ の根とすると，これらは $h(x)$ の根なので A 上整である．$f(x) = \sum_{i=1}^{n} a_i x^i$ とおくと，係数 a_i は α_i の基本対称式となるので，やはり A 上整である（$\overline{K}$ は A の拡大環なので命題 I-8.1.4(4) から従う）．$f(x) \in K[x]$ なので，$a_i \in K$．よって，$a_i \in K$ は A 上整となるが，A が整閉整域であることから，$a_i \in A$．よって $f(x) \in A[x]$. □

$\pi_B \in P$, $\sigma \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ に対し $\sigma(\pi_B) \in \mathcal{P}$

証明 $\tau \in \mathrm{Hom}_K^{\mathrm{al}}(\tilde{L}, \overline{K}) = \mathrm{Gal}(\tilde{L}/K)$ について，$\tau C = C$（追加補題 1.3.5, p.16）となる．$\mathcal{P}$ は C の素イデアルなので，$a, b \in \mathcal{P}$ ならば $a+b \in \mathcal{P}$ となる．$a \in \mathcal{P}, \tau^{-1}(c) \in C$ $(c \in C)$ に対し $a\tau^{-1}(c) \in \mathcal{P}$．よって，$\tau(a), \tau(b) \in \tau(\mathcal{P})$ に対し $\tau(a)+\tau(b) = \tau(a+b) \in \tau(\mathcal{P})$, $\tau(a) \in \tau(\mathcal{P}), c \in C$ に対し $\tau(a)c = \tau(a)\tau(\tau^{-1}(c)) = \tau(a\tau^{-1}(c)) \in \tau(\mathcal{P})$ となるので，$\tau(\mathcal{P})$ は C のイデアル．$\mathcal{P}$ は C の素イデアルなので $a, b \in C$ について，$\tau^{-1}(a)\tau^{-1}(b) \in \mathcal{P}$ ならば $\tau^{-1}(a) \in \mathcal{P}$ もしくは $\tau^{-1}(b) \in \mathcal{P}$．よって，$\tau(\tau^{-1}(a)\tau^{-1}(b)) = ab \in \tau(\mathcal{P})$ ならば $a \in \tau(\mathcal{P})$ もしくは $b \in \tau(\mathcal{P})$ となり，$\tau(\mathcal{P})$ は C の素イデアル．C の素イデアルは唯一なので，$\tau(\mathcal{P}) = \mathcal{P}$．命題 I-8.1.4(2) から C は B 上整．命題 I-8.1.15 から P の上にある C の素イデアルが存在し，これは $\mathcal{P}$．よって $\pi_B \in P \subset \mathcal{P}$．以上から，$\tau(\pi_B) \in \mathcal{P}$．$\tau$ を L に制限すれば $\sigma \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ になるので，$\sigma(\pi_B) \in \mathcal{P}$． □

A, B が離散付値環で P の $\mathfrak{p}$ 上の分岐指数を e とすれば．$a \in K^\times$ に対し，$\mathrm{ord}_P(a) = e\,\mathrm{ord}_{\mathfrak{p}}(a)$ である

証明 $\mathfrak{p} = \pi_A A$ とすれば，$c, d \in A$ によって $a = c/d = (\pi_A{}^i c')/(\pi_A{}^j d') = \pi_A{}^{i-j} c'/d'$ $(c', d' \notin A \setminus \mathfrak{p})$ なので $a = \pi_A{}^n s$ なる $s \in \{\, c/d \mid c, d \in A \setminus \mathfrak{p} \,\} = A_{\mathfrak{p}}^\times$ が存在する．$s^{-1} \in A_{\mathfrak{p}}$ なので，$aA_{\mathfrak{p}} = \pi_A{}^n s A_{\mathfrak{p}} = \pi_A{}^n A_{\mathfrak{p}}$ となり，$\mathrm{ord}_{\mathfrak{p}}(a) = n$．また，分岐指数が e なので，$\pi_A B_P = \pi_B{}^e B_P$，つまり $\mathrm{ord}_P(\pi_A) = e$．以上から $\mathrm{ord}_P(a) = \mathrm{ord}_P(\pi_A{}^n s) = n\,\mathrm{ord}(\pi_A) + \mathrm{ord}_P(s)$．ここで，$P$ が $\mathfrak{p}$ の上にあることに注意して $s \in \{\, c/d \mid c, d \in B \setminus P \,\}$ なので $\mathrm{ord}_P(s) = 0$．よって，$= n\,\mathrm{ord}(\pi_A) = en$．以上から，$\mathrm{ord}_P(a) = e\,\mathrm{ord}_{\mathfrak{p}}(a)$． □

■補題 1.10.10

$\mathrm{Tr}_{L/K}(x) = \sum_i \mathrm{Tr}_{\widehat{L}_i/\widehat{K}_{\mathfrak{p}}}(x)$

証明 L の K 基底を $\{y_1, \ldots, y_n\}$ とする．

$$L \otimes_K \widehat{K}_{\mathfrak{p}} \ni a \otimes t = \left(\sum_{i=1}^n a^{(i)} y_i\right) \otimes t \mapsto \sum_{i=1}^n a^{(i)} t y_i \in \widehat{K}_{\mathfrak{p}}{}^{\oplus n}$$

によって $L \otimes_K \widehat{K}_{\mathfrak{p}}$ は $\{y_1, \ldots, y_n\}$ を基底とする階数 n の自由 $\widehat{K}_{\mathfrak{p}}$ 加群とみなせる（以下，この同型を顕には書かない）．L の元に x をかける準同型

$$\phi\colon L \ni a = \sum_{i=1}^n a^{(i)} y_i \mapsto ax = \sum_{i=1}^n b^{(i)} y_i \in L \quad (a^{(i)}, b^{(i)} \in K)$$

を考える．ϕ は $L \otimes_K \widehat{K}_{\mathfrak{p}}$ の元に $x \otimes 1$ をかける準同型

$$\widehat{\phi}\colon L \otimes_K \widehat{K}_{\mathfrak{p}} \ni a \otimes t = \sum_{i=1}^n a^{(i)} t y_i \mapsto ax \otimes t = \sum_{i=1}^n b^{(i)} t y_i \in L \otimes_K \widehat{K}_{\mathfrak{p}}$$

を誘導する．ϕ を K 基底 $\{y_1, \ldots, y_n\}$ で表現した行列と $\widehat{\phi}$ を $\widehat{K}_{\mathfrak{p}}$ 基底 $\{y_1, \ldots, y_n\}$ で表した行列は同じなので，そのトレースは等しい：$\mathrm{Tr}_K(\phi) = \mathrm{Tr}_{\widehat{K}_{\mathfrak{p}}}(\widehat{\phi})$．補題 1.10.6 から $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_K(\phi)$ なので，

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_K(\phi) = \mathrm{Tr}_{\widehat{K}_{\mathfrak{p}}}(\widehat{\phi}).$$

定理 1.3.23(2) から同型 $\varphi\colon L \otimes_K \widehat{K}_{\mathfrak{p}} \to \widehat{L}_1 \times \cdots \times \widehat{L}_g$ が存在するので，$\widehat{K}_{\mathfrak{p}}$ 準同型

$$\phi_x = \varphi\widehat{\phi}\varphi^{-1}\colon \widehat{L}_1 \times \cdots \times \widehat{L}_g \to \widehat{L}_1 \times \cdots \times \widehat{L}_g$$

が存在し，$\mathrm{Tr}_{\widehat{K}_\mathfrak{p}}(\widehat{\phi}) = \mathrm{Tr}_{\widehat{K}_\mathfrak{p}}(\varphi\widehat{\phi}\varphi^{-1}) = \mathrm{Tr}_{\widehat{K}_\mathfrak{p}}(\phi_x)$.

$$\begin{array}{ccc} \widehat{L}_1 \times \cdots \times \widehat{L}_g & \xrightarrow{\phi_x} & \widehat{L}_1 \times \cdots \times \widehat{L}_g \\ {\scriptstyle\varphi}\uparrow & & {\scriptstyle\varphi}\uparrow \\ L \otimes_K \widehat{K}_\mathfrak{p} & \xrightarrow[\widehat{\phi}]{} & L \otimes_K \widehat{K}_\mathfrak{p} \\ \uparrow & & \uparrow \\ \widehat{K}_\mathfrak{p} & = & \widehat{K}_\mathfrak{p} \end{array}$$

$\varphi\widehat{\phi} = \phi_x\varphi$ を $a \otimes t \in L \otimes_K \widehat{K}_\mathfrak{p}$ に作用させて $\phi_x(\varphi(a \otimes t)) = \varphi(a \otimes t)\varphi(x \otimes 1)$ となる．$\varphi_i \colon B \hookrightarrow \widehat{B}_i$ として，$\varphi(x \otimes 1) = (\varphi_1(x), \ldots, \varphi_g(x))$ である（定理 1.3.23(3)）ので，ϕ_x は $L_1 \times \cdots \times L_g$ の元に $(\varphi_1(x), \ldots, \varphi_g(x))$ をかける写像である：

$$\phi_x \colon \widehat{L}_1 \times \cdots \times \widehat{L}_g \ni (c_1, \ldots, c_g) \mapsto (\varphi_1(x)c_1, \ldots, \varphi_g(x)c_g) \in \widehat{L}_1 \times \cdots \times \widehat{L}_g.$$

ϕ_x を $\widehat{L}_i$ に制限した $\widehat{K}_\mathfrak{p}$ 準同型

$$\psi_{x,i} \colon \widehat{L}_i \ni c_i \mapsto \varphi_i(x)c_i \in \widehat{L}_i$$

を考える．$[\widehat{L}_i : \widehat{K}_\mathfrak{p}] = n_i$ とすれば，定理 1.3.23(4)(5) から $n_1 + \cdots + n_g = n$．$\widehat{L}_i$ の $\widehat{K}_\mathfrak{p}$ 基底を $\{z_i^{(1)}, \ldots, z_i^{(n_i)}\}$ とすれば $\widehat{L}_1 \times \cdots \times \widehat{L}_g$ の $\widehat{K}_\mathfrak{p}$ 基底として

$$\left\{(z_1^{(1)}, \ldots, 0), \ldots, (z_1^{(n_1)}, \ldots, 0); (0, z_2^{(1)}, \ldots, 0), \ldots, (0, z_2^{(n_2)}, \ldots, 0); \ldots; (0, \ldots, z_g^{(1)}), \ldots, (0, \ldots, z_g^{(n_g)})\right\}$$

を取ることができる．

$\psi_{x,i}$ を $\{z_i^{(1)}, \ldots, z_i^{(n_i)}\}$ で表現した行列を M_i とすれば，ϕ_x を $\{(z_1^{(1)}, \ldots, 0), \ldots, (0, \ldots, z_g^{(n_g)})\}$ で表現した行列は

$$\begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_g \end{pmatrix}$$

となる．よって，$\mathrm{Tr}_{\widehat{K}_\mathfrak{p}}(\phi_x) = \sum_i \mathrm{Tr}_{\widehat{K}_\mathfrak{p}}(\psi_{x,i})$．補題 1.10.6 から $\mathrm{Tr}_{\widehat{K}_\mathfrak{p}}(\psi_{x,i}) = \mathrm{Tr}_{\widehat{L}_i/\widehat{K}_\mathfrak{p}}(x)$（包含写像 φ_i は省略した）．以上から，$\mathrm{Tr}_{L/K}(x) = \sum_i \mathrm{Tr}_{\widehat{L}_i/\widehat{K}_\mathfrak{p}}(x)$ となる． □

■補題 1.10.12

完備化と加法的付値

証明 $x \in K^\times$ に対し A での加法的付値は $xA_\mathfrak{p} = \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}A_\mathfrak{p}$ で定義される．また，$\mathfrak{p}$ 進付値は $|x|_\mathfrak{p} = |A/\mathfrak{p}|^{-\mathrm{ord}_\mathfrak{p}(x)}$ で定義される．更に，$\mathfrak{p}$ 距離 $d \colon K \times K \ni (x, y) \mapsto |x-y|_\mathfrak{p} \in |A/\mathfrak{p}|^a$ $(a \in \mathbb{Z})$ を定義する．距離空間 (K, d) を完備化して距離空間 $(\widehat{K}_\mathfrak{p}, \widehat{d})$ が得られる．補題 1.2.6(1) から $\widehat{d} \colon \widehat{K}_\mathfrak{p} \times \widehat{K}_\mathfrak{p} \ni (\widehat{x}, \widehat{y}) \mapsto |A/\mathfrak{p}|^a$ $(a \in \mathbb{Z})$．完備化の定義から $x \in K$ と $\vartheta \colon K \hookrightarrow \widehat{K}_\mathfrak{p}$ によって

$$\widehat{d}(\vartheta(x), \vartheta(0)) = d(x, 0) = |A/\mathfrak{p}|^{-\mathrm{ord}_\mathfrak{p}(x)} = |x|_\mathfrak{p}.$$

ところで，定理 1.2.8(7) から $\widehat{A}_\mathfrak{p}$ は $\widehat{\mathfrak{p}} = \mathfrak{p}\widehat{A}_\mathfrak{p}$ を極大イデアルとする離散付値環である．ここで，$\widehat{x} \in \widehat{K}_\mathfrak{p}$ に対し

$$\widehat{d}(\widehat{x}, \vartheta(0)) = |\widehat{x}|_{\widehat{\mathfrak{p}}} = |\widehat{A}_\mathfrak{p}/\widehat{\mathfrak{p}}|^{-\mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x})}$$

によって $|\bullet|_{\widehat{\mathfrak{p}}}$ と $\mathrm{ord}_{\widehat{\mathfrak{p}}}(\bullet)$ を定義する．命題 1.2.13(1) から $\widehat{A}_{\mathfrak{p}}/\widehat{\mathfrak{p}} \simeq A/\mathfrak{p}$ なので

$$\widehat{d}(\widehat{x}, \vartheta(0)) = |\widehat{x}|_{\widehat{\mathfrak{p}}} = |\widehat{A}_{\mathfrak{p}}/\widehat{\mathfrak{p}}|^{-\mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x})} = |A/\mathfrak{p}|^{-\mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x})}.$$

$\vartheta(x)$ に対しては，$|\vartheta(x)|_{\widehat{\mathfrak{p}}} = |x|_{\mathfrak{p}}$, $\mathrm{ord}_{\widehat{\mathfrak{p}}}(\vartheta(x)) = \mathrm{ord}_{\mathfrak{p}}(x)$．更に，定理 1.2.8(6) から $\widehat{x} \in \widehat{K}_{\mathfrak{p}}$ として，

$$|\widehat{A}_{\mathfrak{p}}/\widehat{\mathfrak{p}}|^{-\mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x})} \leq |\widehat{A}_{\mathfrak{p}}/\widehat{\mathfrak{p}}|^{-n} \Leftrightarrow n \leq \mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x}) \Leftrightarrow \widehat{x} \in \mathfrak{p}^n \widehat{A}_{\mathfrak{p}} = \widehat{\mathfrak{p}}^n \widehat{A}_{\mathfrak{p}}.$$

よって，$\widehat{x} \in \widehat{\mathfrak{p}}^{\mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x})} \widehat{A}_{\mathfrak{p}}$, $\widehat{x} \notin \widehat{\mathfrak{p}}^{\mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x})+1} \widehat{A}_{\mathfrak{p}}$ となるので，$\widehat{x}\widehat{A}_{\mathfrak{p}} = \widehat{\mathfrak{p}}^{\mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x})} \widehat{A}_{\mathfrak{p}}$．これは（離散付値環での）加法的付値の定義と一致している．

以上から，$\widehat{x} \in \widehat{K}_{\mathfrak{p}}$ の加法的付値 $\mathrm{ord}_{\widehat{\mathfrak{p}}}$ と $\widehat{\mathfrak{p}}$ 進付値 $|\bullet|_{\widehat{\mathfrak{p}}}$ は

$$\widehat{x}\widehat{A}_{\mathfrak{p}} = \widehat{\mathfrak{p}}^{\mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x})} \widehat{A}_{\mathfrak{p}}, \quad |\widehat{x}|_{\widehat{\mathfrak{p}}} = |\widehat{A}_{\mathfrak{p}}/\widehat{\mathfrak{p}}|^{-\mathrm{ord}_{\widehat{\mathfrak{p}}}(\widehat{x})}$$

で定まり，$x \in K$ に対しては（ほとんどの場合省略されるが）$\vartheta\colon K \hookrightarrow \widehat{K}_{\mathfrak{p}}$ によって

$$\mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\widehat{\mathfrak{p}}}(\vartheta(x)), \quad |x|_{\mathfrak{p}} = |\vartheta(x)|_{\widehat{\mathfrak{p}}}.$$

□

$\pi \in B$ に対し $\mathrm{ord}_{P_i}(\pi) = 0$ $(i = 2, \ldots, g)$ ならば，$\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{N}_{L/K}(\pi)\right) = \mathrm{ord}_{\widehat{\mathfrak{p}}}\left(\mathrm{N}_{\widehat{L}_1/\widehat{K}_{\mathfrak{p}}}(\pi)\right)$

証明 補題 1.10.10 から $\mathrm{N}_{L/K}(\pi) = \prod_i \mathrm{N}_{\widehat{L}_i/\widehat{K}_{\mathfrak{p}}}(\pi)$ となる．命題 1.1.13 を使えば，

$$\mathrm{ord}_{\widehat{\mathfrak{p}}}(\vartheta(\mathrm{N}_{L/K}(\pi))) = \mathrm{ord}_{\mathfrak{p}}(\mathrm{N}_{L/K}(\pi)) = \sum_i \mathrm{ord}_{\widehat{\mathfrak{p}}}\left(\mathrm{N}_{\widehat{L}_i/\widehat{K}_{\mathfrak{p}}}(\pi)\right).$$

$i = 2, \ldots, g$ に対し，$\mathrm{ord}_{P_i\widehat{B}_i}(\pi) = 0$ なので，$\pi \in \widehat{B}_i^{\times}$．よって命題 I-8.5.2 から $\mathrm{N}_{\widehat{L}_i/\widehat{K}_{\mathfrak{p}}}(\pi) \in \widehat{A}_{\mathfrak{p}}^{\times}$ となるので $i = 2, \ldots, g$ に対し $\mathrm{ord}_{\widehat{\mathfrak{p}}}\left(\mathrm{N}_{\widehat{L}_i/\widehat{K}_{\mathfrak{p}}}(\pi)\right) = 0$．以上から，$\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{N}_{L/K}(\pi)\right) = \mathrm{ord}_{\widehat{\mathfrak{p}}}\left(\mathrm{N}_{\widehat{L}_1/\widehat{K}_{\mathfrak{p}}}(\pi)\right)$． □

Dedekind 環と完備化

証明 A を Dedekind 環，K を A の商体，L を K の有限次拡大，B を L の A における整閉包，$\mathfrak{p}$ を A の素イデアルとする．この時，B は Dedekind 環で，L は B の商体となる（命題 1.3.2）．$\mathfrak{p}$ の上にある B の素イデアルを $P_1, \ldots, P_g$ とする．

$$\begin{array}{ccccc} P_1 & \xleftarrow{\text{PI}} & B & \xrightarrow{\text{QF}} & L \\ \uparrow{\scriptstyle \text{aPI}} & & \uparrow{\scriptstyle \text{IC}} & & \uparrow{\scriptstyle \text{FE}} \\ \mathfrak{p} & \xleftarrow{\text{PI}} & A & \xrightarrow{\text{QF}} & K \end{array}$$

(PI：素イデアル，QF：商体，aPI：上にある素イデアル，IC：整閉包，FE：有限次拡大)

A, K を $\mathfrak{p}$ 進距離で完備化すると位相環 $\widehat{A}_{\mathfrak{p}}$，位相体 $\widehat{K}_{\mathfrak{p}}$ が得られる（系 1.2.9）．$\widehat{K}_{\mathfrak{p}}$ は $\widehat{A}_{\mathfrak{p}}$ の商体であり，$\widehat{A}_{\mathfrak{p}}$ は $\mathfrak{p}\widehat{A}_{\mathfrak{p}}$ を極大イデアルとする離散付値環である（定理 1.2.8(7)）．更に，B, L を P_1 進距離で完備化すると位相環 $\widehat{B}_1$，位相体 $\widehat{L}_1$ が得られ，$\widehat{L}_1$ は $\widehat{B}_1$ の商体であり，$\widehat{B}_1$ は $P_1\widehat{B}_1$ を極大イデアルとする離散付値環で

ある．$P_1\widehat{B}_1$ は $\mathfrak{p}\widehat{A}_\mathfrak{p}$ の上にある素イデアルである（補題 1.3.3）．この時，$\widehat{L}_1$ は $\widehat{K}_\mathfrak{p}$ の有限次拡大で $\widehat{B}_1$ は $\widehat{L}_1$ における $\widehat{A}_\mathfrak{p}$ の整閉包である（定理 1.3.23(3)）．

$$\begin{array}{ccccc} P_1\widehat{B}_1 & \xleftarrow{\text{MI1}} & \widehat{B}_1 & \xrightarrow{\text{QF}} & \widehat{L}_1 \\ \uparrow{\scriptstyle \text{aPI}} & & \uparrow{\scriptstyle \text{IC}} & & \uparrow{\scriptstyle \text{FE}} \\ \mathfrak{p}\widehat{A}_\mathfrak{p} & \xleftarrow{\text{MI1}} & \widehat{A}_\mathfrak{p} & \xrightarrow{\text{QF}} & \widehat{K}_\mathfrak{p} \end{array}$$

(MI1：唯一の極大イデアル)

M を $\widehat{L}_1/\widehat{K}_\mathfrak{p}$ の中間体とする．M と $\widehat{B}_1$ は環なので $M\cap\widehat{B}_1$ は環であり，$M\cap\widehat{B}_1$ は M の $\widehat{A}_\mathfrak{p}$ における整閉包である（命題 I-8.1.4(3)）．$x\in\widehat{L}_1$ が $M\cap\widehat{B}_1$ 上整なら $\widehat{B}_1$ 上整となる．$\widehat{B}_1$ は整閉整域なので $x\in\widehat{B}_1$．$x\in\widehat{B}_1$ は $\widehat{A}_\mathfrak{p}$ 上整なので $M\cap\widehat{B}_1$ 上整である（命題 I-8.1.4(2)）．以上から，$\widehat{L}_1$ の $M\cap\widehat{B}_1$ における整閉包は $\widehat{B}_1$ である．$M\cap\widehat{B}_1$ は Dedekind 環で，$M\cap\widehat{B}_1$ の商体は M である（命題 1.3.2）．

$M\cap P_1\widehat{B}_1$ が $M\cap\widehat{B}_1$ の素イデアルであることは容易に示せる．

$M\supset\mathfrak{p}\widehat{A}_\mathfrak{p}$, $P_1\widehat{B}_1\supset\mathfrak{p}\widehat{A}_\mathfrak{p}$ なので $M\cap P_1\widehat{B}_1$ は $\mathfrak{p}A_\mathfrak{p}$ の上にある素イデアルである（補題 1.3.3）．$P_1\widehat{B}_1\supset M\cap P_1\widehat{B}_1$ なので $P_1\widehat{B}_1$ は $M\cap P_1\widehat{B}_1$ の上にある素イデアルである（補題 1.3.3）．$M\cap\widehat{B}_1$ は $M\cap P_1\widehat{B}_1$ を極大イデアルとする完備離散付値環である（命題 1.5.3）．

$$\begin{array}{ccccc} P_1\widehat{B}_1 & \xleftarrow{\text{MI}} & \widehat{B}_1 & \xrightarrow{\text{QF}} & \widehat{L}_1 \\ \uparrow{\scriptstyle \text{aPI}} & & \uparrow{\scriptstyle \text{IC}} & & \uparrow{\scriptstyle \text{FE}} \\ M\cap P_1\widehat{B}_1 & \xleftarrow{\text{MI}} & M\cap\widehat{B}_1 & \xrightarrow{\text{QF}} & M \\ \uparrow{\scriptstyle \text{aPI}} & & \uparrow{\scriptstyle \text{IC}} & & \uparrow{\scriptstyle \text{FE}} \\ \mathfrak{p}\widehat{A}_\mathfrak{p} & \xleftarrow{\text{MI}} & \widehat{A}_\mathfrak{p} & \xrightarrow{\text{QF}} & \widehat{K}_\mathfrak{p} \end{array}$$

A が仮定 1.1.2 を満たせば，$\widehat{A}_\mathfrak{p}$ も仮定 1.1.2 を満たす（命題 1.2.13(4)）．$M\cap\widehat{B}_1$ と $\widehat{B}_1$ も仮定 1.1.2 を満たす（命題 1.3.2）． □

追加定理 1.10.6. 上の状況で，剰余体 $k=\widehat{A}_\mathfrak{p}/\mathfrak{p}\widehat{A}_\mathfrak{p}$, $l=\widehat{B}_1/P_1\widehat{B}_1$ を考える．$a\in l$ に対し，$[k(a):k]=[\widehat{K}_\mathfrak{p}(\alpha):\widehat{K}_\mathfrak{p}]$ となる $\alpha\in\widehat{B}_1$ が存在し，$\widehat{K}_\mathfrak{p}(\alpha)/\widehat{K}_\mathfrak{p}$ は不分岐拡大である

$$\begin{array}{ccccccc} P_1\widehat{B}_1 & \xleftarrow{\text{MI}} & \widehat{B}_1 & \xrightarrow{\text{QF}} & \widehat{L}_1 & & l \\ \uparrow{\scriptstyle \text{aPI}} & & \uparrow{\scriptstyle \text{IC}} & & \uparrow{\scriptstyle \text{FE}} & & \uparrow{\scriptstyle \text{FE}} \\ \widehat{K}_\mathfrak{p}(\alpha)\cap P_1\widehat{B}_1 & \xleftarrow{\text{MI}} & \widehat{K}_\mathfrak{p}(\alpha)\cap\widehat{B}_1 & \xrightarrow{\text{QF}} & \widehat{K}_\mathfrak{p}(\alpha) & & k(a) \\ \uparrow{\scriptstyle \text{aPI}} & & \uparrow{\scriptstyle \text{IC}} & & \uparrow{\scriptstyle \text{FE},\Phi(x)} & & \uparrow{\scriptstyle \text{FE},\phi(x)} \\ \mathfrak{p}\widehat{A}_\mathfrak{p} & \xleftarrow{\text{MI}} & \widehat{A}_\mathfrak{p} & \xrightarrow{\text{QF}} & \widehat{K}_\mathfrak{p} & & k \end{array}$$

証明 $\widehat{A}_\mathfrak{p}$ は仮定 1.1.2 を満たすので，剰余体は有限体．a の k 上最小多項式を $\phi(x)\in k[x]$ とする．k は有限体なので完全体（系 I-7.3.6）となり，$k(a)/k$ は分離拡大である（定義 I-7.3.1(5)）．よって $\phi(x)$ は分離多項式で，$\phi(a)=0$, $\phi'(a)\neq 0$．$\Phi(x)\equiv\phi(x)\bmod\mathfrak{p}\widehat{A}_\mathfrak{p}$ となるモニック $\Phi(x)\in\widehat{A}_\mathfrak{p}[x]$ 及び $\alpha_0\equiv a\bmod P_1\widehat{B}_1$ となる $\alpha_0\in\widehat{B}_1$ を考える（α_0 は a の代表元）．$\Phi(\alpha_0)\equiv 0\bmod P_1\widehat{B}_1$, $\Phi'(\alpha_0)\not\equiv 0\bmod P_1\widehat{B}_1$ であるので，

Hensel の補題から $\Phi(\alpha)=0$ となる $\alpha\in\widehat{B}_1$ ($\alpha\equiv\alpha_0 \bmod P_1\widehat{B}_1$) が存在する．$\phi(x)$ は k（$\widehat{A}_\mathfrak{p}/\mathfrak{p}\widehat{A}_\mathfrak{p}$ の商体）上既約なので，命題 I-8.2.1 と p.I-233 の注から $\Phi(x)$ は $\widehat{K}_\mathfrak{p}$ 上既約．よって，$\Phi(x)$ は $\widehat{K}_\mathfrak{p}(\alpha)$ の $\widehat{K}_\mathfrak{p}$ 上最小多項式となり，$[k(\alpha):k]=\deg(\phi(x))=\deg(\Phi(x))=[\widehat{K}_\mathfrak{p}(\alpha):\widehat{K}_\mathfrak{p}]$.

$\widehat{K}_\mathfrak{p}(\alpha)\cap\widehat{B}_1$ の剰余体 $m=\widehat{K}_\mathfrak{p}(\alpha)\cap\widehat{B}_1/\widehat{K}_\mathfrak{p}(\alpha)\cap P_1\widehat{B}_1$ を考える．$\alpha\in\widehat{K}_\mathfrak{p}(\alpha)\cap\widehat{B}_1$ なので，$a\in m$ である（$\vartheta\colon m\hookrightarrow l$ について $a\in\operatorname{Im}\vartheta$）．$k(a)$ は a を含む最小の体なので $[m:k(a)]\geq 1$．先程の結果と定理 1.3.23(4) から

$$[k(a):k]=[\widehat{K}_\mathfrak{p}(\alpha):\widehat{K}_\mathfrak{p}]\geq f(\widehat{K}_\mathfrak{p}(\alpha)\cap P_1\widehat{B}_1:\mathfrak{p}\widehat{A}_\mathfrak{p})=[m:k]$$

となるので，$[k(a):m]\geq 1$．以上から $[k(a):m]=1$,

$$[\widehat{K}_\mathfrak{p}(\alpha):\widehat{K}_\mathfrak{p}]=f(\widehat{K}_\mathfrak{p}(\alpha)\cap P_1\widehat{B}_1:\mathfrak{p}\widehat{A}_\mathfrak{p})=[m:k]=[k(a):k]$$

となるので，再び定理 1.3.23(4) から分岐指数は $e(\widehat{K}_\mathfrak{p}(\alpha)\cap P_1\widehat{B}_1:\mathfrak{p}\widehat{A}_\mathfrak{p})=1$．つまり，$\widehat{K}_\mathfrak{p}(\alpha)/\widehat{K}_\mathfrak{p}$ は不分岐拡大． □

π の M 上最小多項式 $f(x)$ は $\widehat{B}_M=M\cap\widehat{B}_1$ 上の Eisenstein 多項式で，$\deg(f(x))=[\widehat{L}_1:M]$ である

証明 $\operatorname{ord}_{P_1}(\pi)=1$ より $\pi\widehat{B}_1=\widehat{P}_1\widehat{B}_1$ となるので，π は $\widehat{B}_1$ の素元．$\widehat{L}_1/M$ は完全分岐なので，命題 1.10.7 から π の M 上最小多項式は Eisenstein 多項式で，その次数は $[\widehat{L}_1:M]$ に等しい（命題の主張には書かれていないが，証明されている：p.62）．また，Eisenstein 多項式の定義から $f(x)\in\widehat{B}_M[x]$（M に対応する離散付値環は $\widehat{B}_M$）． □

■命題 1.10.13

$Q_1,\dots,Q_g$ が $P_1,\dots,P_t$ と互いに素

証明 $Q_i\cap A=\mathfrak{p}$, $P_j\cap A=\mathfrak{p}_j$ に注意すれば，$Q_i=P_j\Rightarrow\mathfrak{p}=\mathfrak{p}_j$．対偶をとって，$\mathfrak{p}\neq\mathfrak{p}_j\Rightarrow Q_i\neq P_j$．$\mathfrak{p}\neq\mathfrak{p}_j$ なので，Q_i と P_j は互いに素． □

I の相対イデアル $\mathrm{N}_{L/K}(I)$ も $\mathfrak{p}$ と互いに素

証明 相対イデアル $\mathrm{N}_{L/K}(I)$ は $\left\{\mathrm{N}_{L/K}(b)\,\middle|\,b\in I\right\}$ で生成される A のイデアル（定義 1.10.1）なので，A の適当なイデアル J によって，$\mathrm{N}_{L/K}(I)=\big(\mathrm{N}_{L/K}(x)\big)+J$ と書くことができる．$\big(\mathrm{N}_{L/K}(x)\big)$ は $\mathfrak{p}$ と互いに素なので，素イデアル分解には $\mathfrak{p}$ は現れない：$\big(\mathrm{N}_{L/K}(x)\big)=\mathfrak{p}^0\cdots$．よって，定理 I-8.3.17(3) から $\mathrm{N}_{L/K}(I)=\big(\mathrm{N}_{L/K}(x)\big)+J$ の素イデアル分解は $\mathfrak{p}^0\cdots$ となる，つまり $\mathrm{N}_{L/K}(I)$ は $\mathfrak{p}$ と互いに素． □

$\mathrm{N}_{L/K}(I)\supset{\mathfrak{p}_1}^{f_1}\cdots{\mathfrak{p}_t}^{f_t}$

証明 $\mathrm{N}_{L/K}(I)\supset{\mathfrak{p}_1}^{f_1}\cdots{\mathfrak{p}_t}^{f_t}J$ なので，定理 I-8.3.17(2) から A のイデアル J' があり，$J'\mathrm{N}_{L/K}(I)={\mathfrak{p}_1}^{f_1}\cdots{\mathfrak{p}_t}^{f_t}J$. J の素イデアル分解を ${\tilde{\mathfrak{p}}_1}^{a_1}\cdots{\tilde{\mathfrak{p}}_s}^{a_s}$ とすれば, $J'\mathrm{N}_{L/K}(I)={\mathfrak{p}_1}^{f_1}\cdots{\mathfrak{p}_t}^{f_t}{\tilde{\mathfrak{p}}_1}^{a_1}\cdots{\tilde{\mathfrak{p}}_s}^{a_s}$. $\mathrm{N}_{L/K}(I)$ が J と互いに素であることから，$\mathrm{N}_{L/K}(I)$ の素イデアル分解には $\tilde{\mathfrak{p}}_1,\dots,\tilde{\mathfrak{p}}_s$ は現れない．よって，$J'=$

$\tilde{\mathfrak{p}}_1{}^{a_1}\cdots\tilde{\mathfrak{p}}_s{}^{a_s}J''$ となるので，$\tilde{\mathfrak{p}}_1{}^{a_1}\cdots\tilde{\mathfrak{p}}_s{}^{a_s}J''\,\mathrm{N}_{L/K}(I)=\mathfrak{p}_1{}^{f_1}\cdots\mathfrak{p}_t{}^{f_t}\tilde{\mathfrak{p}}_1{}^{a_1}\cdots\tilde{\mathfrak{p}}_s{}^{a_s}$．よって，$J''\,\mathrm{N}_{L/K}(I)=\mathfrak{p}_1{}^{f_1}\cdots\mathfrak{p}_t{}^{f_t}$．定理 I-8.3.17(2) から $\mathrm{N}_{L/K}(I)\supset\mathfrak{p}_1{}^{f_1}\cdots\mathfrak{p}_t{}^{f_t}$． □

$I\widehat{B}_1=Q_{1,1}{}^{m_1}\widehat{B}_1=x\widehat{B}_1$

証明 $x_1,\dots,x_{m_1}$ の $Q_{1,1}=P_1=\cdots=P_{m_1}$ に関する加法的付値が 1，$x_{m_1+1},\dots,x_t$ の P_1 に関する加法的付値が 0 となる．よって，$\mathrm{ord}_{Q_{1,1}}(x_1)=1$ なので，$x_1\widehat{B}_1=Q_{1,1}\widehat{B}_1$．また，$\mathrm{ord}_{Q_{1,1}}(x_t)=0$ なので $x_t\widehat{B}_1=\widehat{B}_1$，つまり $x_t\in\widehat{B}_1^{\times}$．以上から，$x_1,\dots,x_{m_1}$ は $Q_{1,1}\widehat{B}_1$ を生成し，$x_{m_1+1},\dots,x_t$ は $\widehat{B}_1^{\times}$ の元である．$i\geq m_1+1$ に対し $x_i\in P_i$，$x_i\in\widehat{B}_1^{\times}$ なので $P_iP_1\widehat{B}_1=P_1\widehat{B}_1$．よって，$I=P_1\cdots P_t=Q_{1,1}{}^{m_1}P_{m_1+1}\cdots P_t$ なので $I\widehat{B}_1=Q_{1,1}{}^{m_1}\widehat{B}_1$．$x=x_1\cdots x_t$ で $x_1\widehat{B}_1=\cdots=x_{m_1}\widehat{B}_1=Q_{1,1}\widehat{B}_1$，$x_{m_1+1},\dots,x_t\in\widehat{B}_1^{\times}$ なので $x\widehat{B}_1=Q_{1,1}{}^{m_1}\widehat{B}_1$． □

$I\widehat{B}_1=x\widehat{B}_1$，$y\in I$ なら $z\in\widehat{B}_1$ が存在して $y=zx$ となる

証明 $x\widehat{B}_1=I\widehat{B}_1\supset y\widehat{B}_1$ なので，定理 I-8.3.17(2) から単項イデアル整域 $\widehat{B}_1$ のイデアル $z'\widehat{B}_1$ が存在し $xz'\widehat{B}_1=y\widehat{B}_1$ となる．$y\in y\widehat{B}_1$ なので $y\in xz'\widehat{B}_1$，つまり $b\in\widehat{B}_1$ があり $y=xz'b$．$z=z'b\in\widehat{B}_1$ とすれば主張が従う． □

■命題 1.10.19

$IA_{\mathfrak{p}}$ が $\Delta_{B/A,\mathfrak{p}}$ を割り切る

証明 I の定義から $s^{2n}\Delta_{L/K}(u_1,\dots,u_n)=\Delta_{L/K}(su_1,\dots,su_n)A=Ia$ となる $a\in A$ が存在する．よって，$aIA_{\mathfrak{p}}=s^{2n}\Delta_{L/K}(u_1,\dots,u_n)A_{\mathfrak{p}}$．$s^{2n}\in A_{\mathfrak{p}}^{\times}$ なので，$=\Delta_{L/K}(u_1,\dots,u_n)A_{\mathfrak{p}}=\Delta_{B/A,\mathfrak{p}}A_{\mathfrak{p}}$ となるので従う． □

1.11 完備化と Dedekind の判別定理

B の A 基底は $B_{\mathfrak{p}}$ の $A_{\mathfrak{p}}$ 基底であり，L の K 基底である

証明 B の A 基底を $\{w_1,\dots,w_n\}$ とする．$\forall b\in B$ は $\sum y_iw_i$ $(y_i\in A)$ と表すことができる．$B_{\mathfrak{p}}$ の任意の元は $b\in B$ と $s\in A\setminus\mathfrak{p}$ で b/s と表せる．上の式を代入して $b/s=\sum_{i=1}^n(y_i/s)w_i,\quad(y_i/s\in A_{\mathfrak{p}})$．$B_{\mathfrak{p}}$ の任意の元は $\{w_1,\dots,w_n\}$ の $A_{\mathfrak{p}}$ 係数の線形結合で表すことができる．$\sum(y_i/s_i)w_i=0$ $(y_i\in A,\quad s_i\in A\setminus\mathfrak{p})$ とする．$\sum_{i=1}^n(y_is_1\cdots s_n/s_i)w_i=0$ となり，w_i の係数は A の元．$\{w_1,\dots,w_n\}$ の A 基底としての一時独立性から，$y_i=0$．よって $A_{\mathfrak{p}}$ 基底として一次独立．

L/K も同様．$S=A\setminus\{0\}$ として $L=S^{-1}B$ と表せることを使う． □

■命題 1.11.1

$\Delta_{B/A,\mathfrak{p}} = \prod_{i=1}^{g} \Delta_{\widehat{B}_i/\widehat{A}_\mathfrak{p}}$

証明 $\{w_1,\dots,w_n\}$ を B の A 基底とする．$m(w_i)$ を B の元に $w_i \in B$ をかける写像とする：

$$m(w_i)\colon B \ni a = \sum_{i=1}^{n} a^{(i)} w_i \mapsto a w_i = \sum_{i=1}^{n} b^{(i)} w_i \in B.$$

これは $B \otimes_A \widehat{A}_\mathfrak{p}$ の元に $w_i \otimes 1 \in B \otimes_A \widehat{A}_\mathfrak{p}$ をかける写像 $\tilde{m}(w_i)$ を誘導する：

$$\tilde{m}(w_i)\colon B \otimes_A \widehat{A}_\mathfrak{p} \ni a \otimes t = \sum_{i=1}^{n} a^{(i)} w_i \otimes t \mapsto a w_i \otimes t = \sum_{i=1}^{n} b^{(i)} w_i \otimes t \in B \otimes_A \widehat{A}_\mathfrak{p}.$$

定理 1.3.23(2) から，$\phi_i\colon B \hookrightarrow \widehat{B}_i$ として同型

$$\phi\colon B \otimes_A \widehat{A}_\mathfrak{p} \ni a \otimes t \to (\phi_1(a)t,\dots,\phi_g(a)t) \in \widehat{B}_1 \times \cdots \times \widehat{B}_g$$

が得られる．ϕ によって $\{w_i\}_{1\le i\le n}$ は $\{(\phi_1(w_i),\dots,\phi_g(w_i))\}_{1\le i\le g}$ に写るので，$\{(\phi_1(w_i),\dots,\phi_g(w_i))\}_{1\le i\le g}$ は $\widehat{B}_1 \times \cdots \times \widehat{B}_g$ の $\widehat{A}_\mathfrak{p}$ 基底である．

$\widehat{m} = \phi\tilde{m}\phi^{-1}$ として，

$$\widehat{m}\colon \widehat{B}_1 \times \cdots \times \widehat{B}_g \ni \phi(a \otimes t) \mapsto \phi(a w_i \otimes t) \in \widehat{B}_1 \times \cdots \times \widehat{B}_g$$

を構成する．

$$\begin{array}{ccc} \widehat{B}_1 \times \cdots \times \widehat{B}_g & \xrightarrow{\widehat{m}} & \widehat{B}_1 \times \cdots \times \widehat{B}_g \\ {\scriptstyle\phi}\uparrow & & {\scriptstyle\phi}\uparrow \\ B_\mathfrak{p} \otimes_{A_\mathfrak{p}} \widehat{A}_\mathfrak{p} & \xrightarrow[\tilde{m}]{} & B_\mathfrak{p} \otimes_{A_\mathfrak{p}} \widehat{A}_\mathfrak{p} \end{array}$$

$\phi(a \otimes t) = (\phi_1(a)t,\dots,\phi_g(a)t)$，$\phi(aw_i \otimes t) = (\phi(w_i)\phi_1(a)t,\dots,\phi(w_i)\phi_g(a)t)$ であるので，$\widehat{m}(w_i)$ は $\widehat{B}_1 \times \cdots \times \widehat{B}_g$ の元に $(\phi_1(w_i),\dots,\phi_g(w_i))$ をかける写像である．構成から（適当な基底を取ることによって）$\mathrm{Tr}(m) = \mathrm{Tr}(\tilde{m}) = \mathrm{Tr}(\widehat{m})$ であることが分かる．

$\{v_{i,1},\dots,v_{i,N_i}\}$ を $\widehat{B}_i$ の $\widehat{A}_\mathfrak{p}$ 基底とする（$N_i = e_i f_i$：定理 1.3.23(4)）．

$$\begin{gathered} \overline{v}_1 = (v_{1,1},0,\dots,0),\dots,\overline{v}_{N_1} = (v_{1,N_1},0,\dots,0) \\ \overline{v}_{N_1+1} = (0,v_{2,1},0,\dots,0),\dots,\overline{v}_{N_1+N_2} = (0,v_{2,N_2},0,\dots,0) \\ \vdots \\ \overline{v}_{n-N_g+1} = (0,\dots,0,v_{g,1}),\dots,\overline{v}_n = (0,\dots,0,v_{g,N_g}) \end{gathered}$$

とすれば，$\{\overline{v}_1,\dots,\overline{v}_n\}$ は $\widehat{B}_1 \times \cdots \times \widehat{B}_g$ の $\widehat{A}_\mathfrak{p}$ 基底となる．$\{(\phi_1(w_i),\dots,\phi_g(w_i))\}_{1\le i\le g}$，$\{\overline{v}_1,\dots,\overline{v}_n\}$ は共に $\widehat{B}_1 \times \cdots \times \widehat{B}_g$ の $\widehat{A}_\mathfrak{p}$ 基底であるので，$A \in \mathrm{GL}_n(\widehat{A}_\mathfrak{p})$ が存在し，

$$(\phi_1(w_i),\dots,\phi_g(w_i)) = \sum_{j=1}^{n} A_{ij}\overline{v}_j.$$

補題 1.10.6 を使えば,

$$\begin{aligned}\mathrm{Tr}_{L/K}(w_iw_j) = \mathrm{Tr}(m(w_iw_j)) = \mathrm{Tr}(\widehat{m}(w_iw_j)) &= \mathrm{Tr}\left(\widehat{m}\left(\sum_{k=1}^{n}\sum_{l=1}^{n} A_{ik}A_{jl}\overline{v}_k\overline{v}_l\right)\right)\\ &= \sum_{k=1}^{n}\sum_{l=1}^{n} A_{ik}A_{jl}\,\mathrm{Tr}(\widehat{m}(\overline{v}_k\overline{v}_l)).\end{aligned}$$

$\mathrm{Tr}_{L/K}(w_iw_j)$ を (i,j) 成分とする $n\times n$ 行列を W，$\mathrm{Tr}(\widehat{m}(\overline{v}_i\overline{v}_j))$ を (i,j) 成分とする $n\times n$ 行列を M とすれば，これは $W = AM^tA$ と書ける.

M の $(N_1+\cdots+N_{l-1}+i, N_1+\cdots+N_{l-1}+j)$ $(1\le i,j\le N_l)$ 成分は $\widehat{B}_1\times\cdots\times\widehat{B}_g$ に対して，$\overline{v}_{N_1+\cdots+N_{l-1}+i}\overline{v}_{N_1+\cdots+N_{l-1}+j} = (0,\dots,0,v_{l,i}v_{l,j},0,\dots,0)$ をかける線形写像のトレースであり，これは $\widehat{B}_l$ の元に $v_{l,i}v_{l,j}$ をかける線形写像のトレース．よって補題 1.10.6 からこれは $\mathrm{Tr}_{\widehat{L}_l/\widehat{K}_\mathfrak{p}}(v_{l,i}v_{l,j})$ に等しい．$i\ne j$ であれば $v_{ik}v_{jl}=0$ なので，$\mathrm{Tr}_{\widehat{L}_i/\widehat{K}_\mathfrak{p}}(v_{ik}v_{il})$ を (k,l) 成分とする $N_i\times N_i$ 行列を M_i とすれば,

$$M = \begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_g\end{pmatrix},\quad \det M_i = \Delta_{\widehat{L}_i/\widehat{K}_\mathfrak{p}}(v_{i,1},\dots,v_{i,N_i}).$$

よって,

$$\Delta_{L/K}(w_1,\dots,w_n) = \det W = (\det A)^2\det M = (\det A)^2\prod_{i=1}^{g}\det M_i = (\det A)^2\prod_{i=1}^{g}\Delta_{\widehat{L}_i/\widehat{K}_\mathfrak{p}}(v_{i,1},\dots,v_{i,N_i})$$

となり，系 I-6.7.9(1) から $\det A\in\widehat{A}_\mathfrak{p}^\times$ なので

$$\begin{aligned}\mathrm{ord}_\mathfrak{p}(\Delta_{L/K}(w_1,\dots,w_n)) &= \mathrm{ord}_{\mathfrak{p}\widehat{A}_\mathfrak{p}}\left(\prod_{i=1}^{g}\Delta_{\widehat{L}_i/\widehat{K}_\mathfrak{p}}(v_{i,1},\dots,v_{i,N_i})\right)\\ &= \sum_{i=1}^{g}\mathrm{ord}_{\mathfrak{p}\widehat{A}_\mathfrak{p}}\left(\Delta_{\widehat{L}_i/\widehat{K}_\mathfrak{p}}(v_{i,1},\dots,v_{i,N_i})\right).\end{aligned}$$

$\widehat{A}_\mathfrak{p}$ は離散付値環で $\mathfrak{p}\widehat{A}_\mathfrak{p}$ が唯一の素イデアルなので

$$\Delta_{B/A,\mathfrak{p}} = \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\Delta_{L/K}(w_1,\dots,w_n))}\widehat{A}_\mathfrak{p} = \prod_{i=1}^{g}\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}\widehat{A}_\mathfrak{p}}\left(\Delta_{\widehat{L}_i/\widehat{K}_\mathfrak{p}}(v_{i,1},\dots,v_{i,N_i})\right)}\widehat{A}_\mathfrak{p} = \prod_{i=1}^{g}\Delta_{\widehat{B}_i/\widehat{A}_\mathfrak{p}}.$$

□

■命題 1.11.4

$y = s_1\cdots s_mx\in\delta(B/A)^{-1}$

証明 $a\in B$ として，$\mathrm{Tr}_{L/K}(as_1\cdots s_mx) = s_1\cdots s_m\,\mathrm{Tr}_{L/K}(ax)$．$a = b_1w_1+\cdots+b_mw_m$ $(b_i\in A)$ とすれば,

$$= s_1\cdots s_m\,\mathrm{Tr}_{L/K}\left(\sum_i b_iw_ix\right) = s_1\cdots s_m\sum_i b_i\,\mathrm{Tr}_{L/K}\,(w_ix) = s_1\cdots s_m\sum_i b_ia_i/s_i$$

なので $\mathrm{Tr}_{L/K}(as_1\cdots s_mx)\in A$．つまり，$s_1\cdots s_mx\in\delta(B/A)^{-1}$. □

■命題 1.11.6

$x \in \delta(B/B_M)^{-1}(\delta(B_M/A)B)^{-1}$

証明 $x\delta(B_M/A) \subset \delta(B/B_M)^{-1}$ は本文から容易に分かる. $b \in \delta(B/B_M)^{-1}$ であれば $\forall y \in B$ に対し, 定義から $by \in \delta(B/B_M)^{-1}$ となるので, $bB \subset \delta(B/B_M)^{-1}$. 以上から $x\delta(B_M/A)B \subset \delta(B/B_M)^{-1}$. $\delta(B_M/A)B$ は B のイデアルなので有限生成（命題 I-6.8.34）で, 分数イデアル（Dedekind 環のイデアルは分数イデアル. 命題 I-8.3.24 からも分かる）. よって, 命題 I-8.3.21 から

$$xB = x\delta(B_M/A)B(\delta(B_M/A)B)^{-1} \subset \delta(B/B_M)^{-1}(\delta(B_M/A)B)^{-1}.$$

よって, $x \in \delta(B/B_M)^{-1}(\delta(B_M/A)B)^{-1}$. □

■系 1.11.11

$\overline{g}(x)$ の根が $A/\mathfrak{p}$ 上 $M \cap B/M \cap P$ を生成し, $g(x)$ の根が K 上 M を生成する様な $g(x)$ が存在し, $g(x)$ は既約, $\overline{g}(x)$ が既約・分離である

証明 $k = A/\mathfrak{p}$, $l = B/P$, $m = C/P_M$ とする. M/K は不分岐拡大なので $[m : k] = [M : K] = f$. k は有限体なので完全体（系 I-7.3.6）となり m/k は分離拡大（よって, g の存在を示せば $\overline{g}(x)$ は分離多項式と分かる）で, $m = k(a)$ となる $a \in l$ が存在する. これに対して追加定理 1.10.6(p.29) の証明を適用すれば, f 次の不分岐拡大 $K(\alpha)/K$ $(\alpha \in B)$ が存在する. g は Φ, $\overline{g}$ は ϕ に対応するので, $g(x), \overline{g}(x)$ は既約多項式. M/K は f 次の最大不分岐拡大であったので $M = K(\alpha)$ となる. □

$R(g, g') \in A^\times$, $\Delta_{C/A} = A$

証明 $R(g, g')$ を $\bmod \mathfrak{p}$ で考えた $R(\overline{g}, \overline{g}')$ は $\overline{g}(x)$ の判別式になる（系 1.9.7）. $\overline{g}(x)$ は分離多項式なので $\overline{g}$ と $\overline{g}'$ は共通根を持たない. よって系 1.9.6 から $R(\overline{g}, \overline{g}') \neq 0$. 従って $R(g, g') \in A\backslash\mathfrak{p}$ で, 命題 I-6.5.8 から $A\backslash\mathfrak{p} = A^\times$. 上で示したように, $g(x) \in A[x]$ は $\alpha \in C$ の K 上最小多項式で, $\Delta_{M/K}(1, \alpha, \cdots, \alpha^{f-1}) = R(g, g')$（命題 1.9.9）なので $\Delta_{M/K}(1, \alpha, \cdots, \alpha^{f-1}) \in A^\times$. すなわち $\mathrm{ord}_\mathfrak{p}(\Delta_{M/K}(1, \alpha, \cdots, \alpha^{f-1})) = 0$. よって補題 1.8.3 から $\{1, \alpha, \ldots, \alpha^{f-1}\}$ は C の A 基底となる（補題の主張はアレ；p.49 の上の方参照）ので, 相対判別式の計算に $\{1, \alpha, \ldots, \alpha^{f-1}\}$ を使用できる：

$$\Delta_{C/A} = \Delta_{C/A,\mathfrak{p}} = \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\Delta_{M/K}(1,\alpha,\ldots,\alpha^{f-1}))} = \mathfrak{p}^0 = A.$$

□

■命題 1.11.14

A を離散付値環, $\{x_1, \ldots, x_l\}$ $(l = [N : K])$ を B_N の A 基底, $\Delta_{N/K}(x_1, \ldots, x_l) \in A^\times$ とすれば, $\{x_1, \ldots, x_l\}$ は L の M 基底となる

証明 命題 I-8.1.24 から B_N は階数 l の自由 A 加群（だから基底が l 個）．$\Delta_{N/K}(x_1,\dots,x_l)\neq 0$ なので命題 1.7.3(2) から $\{x_1,\dots,x_l\}\subset N$ は K 上一次独立．よって定理 I-8.11.9(3) から M 上一次独立．命題 I-8.11.9(2) から $[L:M]=l$ なので $\{x_1,\dots,x_l\}$ は L の M 基底となる． □

■定理 1.11.16

A が離散付値環なら，B_M の A 基底を $\{v_1,\dots,v_m\}$，B_N の A 基底を $\{w_1,\dots,w_n\}$ とすれば，$\{v_1,\dots,v_m\}$ は N 上一次独立で，$\{w_1,\dots,w_n\}$ は K 上一次独立である

証明 I-p.241 のはじめの話から，$\{v_1,\dots,v_m\}$ と $\{w_1,\dots,w_n\}$ は K 上一次独立．さらに，定理 I-8.11.9 から $\{v_1,\dots,v_m\}$ は N 上一次独立となる． □

上の状況で，$\mathrm{Tr}_{L/K}(v_iw_kv_jw_l)=\mathrm{Tr}_{M/K}(v_iv_j)\,\mathrm{Tr}_{N/K}(w_kw_l)$

証明 まず，

$$\mathrm{Tr}_{L/K}(v_iw_kv_jw_l)=\mathrm{Tr}_{L/K}(v_iv_jw_kw_l).$$

命題 I-8.1.18(5) から

$$=\mathrm{Tr}_{M/K}\left(\mathrm{Tr}_{L/M}(v_iv_jw_kw_l)\right).$$

$v_iv_j\in M$ なので，

$$=\mathrm{Tr}_{M/K}\left(v_iv_j\,\mathrm{Tr}_{L/M}(w_kw_l)\right).$$

(1.11.15) と同様の考察から $\mathrm{Tr}_{L/M}(w_kw_l)=\mathrm{Tr}_{N/K}(w_kw_l)$ なので

$$=\mathrm{Tr}_{M/K}\left(v_iv_j\,\mathrm{Tr}_{N/K}(w_kw_l)\right).$$

補題 I-8.1.17 から $\mathrm{Tr}_{N/K}(w_kw_l)\in K$ なので，

$$=\mathrm{Tr}_{M/K}(v_iv_j)\,\mathrm{Tr}_{N/K}(w_kw_l).$$

□

上の状況で $\Delta_L=\Delta_M{}^n\Delta_N{}^m$

証明 B の A 基底として

$$\{v_1w_1,\dots,v_1w_n;v_2w_1,\dots,v_2w_n;\cdots;v_mw_1,\dots,v_mw_n\}$$

をとれる（p.81 の上の方）．G を (i,j) 成分を $g_{ij}=\mathrm{Tr}_{L/K}(v_iv_j)$ とする m 次行列，H を (k,l) 成分を $\mathrm{Tr}_{L/K}(w_kw_l)$ とする n 次行列とする．$((i-1)n+k,(j-1)n+l)$ 成分が $\mathrm{Tr}_{L/K}(v_iw_kv_jw_l)$ の行列を X とする．$\mathrm{Tr}_{L/K}(v_iw_kv_jw_l)=\mathrm{Tr}_{L/K}(v_iv_j)\,\mathrm{Tr}_{L/K}(w_kw_l)$ なので，

$$X=\begin{pmatrix} g_{11}H & \cdots & g_{1m}H\\ g_{21}H & \cdots & g_{2m}H\\ & \vdots & \\ g_{m1}H & \cdots & g_{mm}H\end{pmatrix}=G\otimes H$$

(行列の Kronecker 積) となる．線形代数で知られているように，$\det(G \otimes H) = (\det G)^n (\det H)^m$ なので，

$$\Delta_{L/K}(v_1 w_1, \ldots) = \det X = \det(G \otimes H) = (\det G)^n (\det H)^m = \Delta_{M/K}(v_1, \ldots, v_m)^n \Delta_{N/K}(w_1, \ldots, w_n)^m.$$

$A = \mathbb{Z}$, $K = \mathbb{Q}$ とすれば，主張が従う． □

1.12 積公式

■補題 1.12.1 $\mathrm{Tr}_{L/K}$ じゃなくて $\mathrm{Tr}_{K/\mathbb{Q}}$ じゃね？

■定理 1.12.2

$x \in \mathcal{O}_K$ に対し積公式 $\prod_{v \in \mathfrak{M}} |x|_v = 1$ が成立すれば $x \in K^\times$ に対しても成立する

証明 まず $v \in \mathfrak{p}$ については $|x|_\mathfrak{p}|1/x|_\mathfrak{p} = 1$．$v \in \mathfrak{M}_\mathbb{R}$ に対しては $\sigma_v \in \mathrm{Hom}_\mathbb{Q}^{\mathrm{al}}(K, \mathbb{C})$ について $|\sigma_v(x)||\sigma_v(1/x)| = |\sigma_v(1)| = 1$．$v \in \mathfrak{M}_\mathbb{C}$ に対しても同様に $|\sigma_v(x)|^2 |\sigma_v(1/x)|^2 = |\sigma_v(1)|^2 = 1$．以上から，$x \in \mathcal{O}_K$ に対し，$|x|_v = |1/x|_v$ なので，$1/x \in K$ $(x \in \mathcal{O}_K)$ に対しても積公式が成立．K は $\mathcal{O}_K$ の商体なので，$\forall x \in K$ は a/b $(a, b \in \mathcal{O}_K)$ と表すことができる．a, $1/b$ に対し積公式が成立するので，上の議論と同様にして $x = a/b$ に対しても成立． □

1.13 Krasner の補題

■定理 1.13.1

A, B を完備離散付値環，L/K を Galois 拡大，$\tau \in \mathrm{Gal}(L/K(\beta))$ $(\beta \in L)$ として，$|\tau(x)| = |x|$

証明 B の極大イデアルを P とする．$\mathrm{ord}_P(x) = n$ とすれば，$xB = P^n B$ となり，$\tau(x)\tau(B) = \tau(P)^n$．$\tau(B) = B$（追加補題 1.3.5, p.16），$\tau(P) = P$ なので $\tau(x)B = P^n$．つまり，$\mathrm{ord}_P(\tau(x)) = n$． □

■系 1.13.3

局所体（$\mathbb{Q}_p$ の有限次拡大）が代数体（$\mathbb{Q}$ の有限次拡大）の完備化に同型である

証明 本文の証明の前半から，局所体 $L = \mathbb{Q}_p(\beta)$，代数体 $K = \mathbb{Q}(\beta)$ と表すことができる．$\mathcal{O}_L$ を L の整数環，P を $\mathcal{O}_L$ の素イデアルとする．この時，$\mathfrak{p} = P \cap \mathcal{O}_K$ とする．$\mathbb{Z} \subset \mathbb{Z}_p$，$K \subset L$ なので $\mathcal{O}_K \subset \mathcal{O}_L$ である．$a, b \in \mathfrak{p}$，$x \in \mathcal{O}_K$ とする．$a, b \in \mathcal{O}_K, P$ なので $a + b \in \mathcal{O}_K, P$，つまり $a + b \in \mathfrak{p}$．$a, x \in \mathcal{O}_K$ なので $ax \in \mathcal{O}_K$．$a \in P$，$x \in \mathcal{O}_L$ なので $ax \in P$．よって，$ax \in \mathfrak{p}$．以上から，$\mathfrak{p}$ は $\mathcal{O}_K$ のイデアル．$a, b \in \mathcal{O}_K$ で $ab \in \mathfrak{p}$ とする．$ab \in P$ で P は $\mathcal{O}_L$ の素イデアルなので $a \in P$（若しくは $b \in P$）となり，$a \in \mathfrak{p}$．よって，$\mathfrak{p}$ は $\mathcal{O}_K$ の素イデアル．$\mathcal{O}_L$ は完備離散付値環（命題 I-9.1.31(4)，命題 1.5.3(2)）なので $\mathfrak{p}\mathcal{O}_L = P^e \mathcal{O}_L$ となる e が存在する（命題 I-8.3.15）．$\mathcal{O}_L/P$ は $\mathcal{O}_K/\mathfrak{p}$ の有限次拡大．$\mathcal{O}_L$ は単項イデアル整域なので P は単項イデアル．$\mathcal{O}_L$ は仮定 1.1.2 を満たす（命題 I-1.5.3）ので，$\mathcal{O}_L/P$ は有限体．よって $\mathcal{O}_K/\mathfrak{p}$ も有限体．よって，定

理 1.3.23(1) の証明と同様にして K（を L への包含）上では P 進距離は $\mathfrak{p}$ 進距離の冪乗となる．$P \supset p\mathbb{Z}_p$, $\mathcal{O}_K \supset \mathbb{Z}$ なので $\mathfrak{p} \supset p\mathbb{Z}$．よって補題 1.3.3 より $\mathfrak{p}$ は $p\mathbb{Z}$ の上にある素イデアル（$p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$）．

$$\begin{array}{ccccc} \mathfrak{p} & \longleftarrow & \mathcal{O}_K & \longrightarrow & K \\ \uparrow & & \uparrow & & \uparrow \\ p\mathbb{Z} & \longleftarrow & \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

完備化して

$$\begin{array}{ccccc} \mathfrak{p}\mathcal{O}_{\widehat{K}} & \longleftarrow & \mathcal{O}_{\widehat{K}} & \longrightarrow & \widehat{K} \\ \uparrow & & \uparrow & & \uparrow \\ p\mathbb{Z}_p & \longleftarrow & \mathbb{Z}_p & \longrightarrow & \mathbb{Q}_p \end{array}$$

$\beta \in K$ なので $\beta \in \widehat{K}$．よって，$\widehat{K} \supset \mathbb{Q}_p(\beta) = L$．$f, g$ 共に $\mathbb{Q}_p$ 上既約なので $[L : \mathbb{Q}_p] = \deg f = \deg g = [K : \mathbb{Q}]$．定理 1.3.23(3)(4) から $[\widehat{K} : \mathbb{Q}_p] \leq [K : \mathbb{Q}]$ なので $[L : \mathbb{Q}_p] \geq [\widehat{K} : \mathbb{Q}_p]$．以上から $\widehat{K} = L$． □

■命題 1.13.5

L/K を $\mathbb{Q}_p$ の有限次拡大，$\mathfrak{p}$ を $\mathcal{O}_K$ の素イデアル，P を $\mathfrak{p}$ の上にある $\mathcal{O}_L$ の素イデアルとする．$\mathcal{O}_L/P \simeq \mathcal{O}_K/\mathfrak{p}$ ならば $u \in \mathcal{O}_L$ に対し $u_0 \equiv u \bmod P$ となる $u_0 \in \mathcal{O}_K$ が存在する

証明 $\mathcal{O}_K/\mathfrak{p}$ の完全代表系を $\{a_1, a_2, \ldots\}$ とする．a_1 と a_2 は別の同値類に属するので $a_1 - a_2 \notin \mathfrak{p}$，つまり $a_1 - a_2 \in \mathcal{O}_K \setminus \mathfrak{p}$．よって $a_1 - a_2 \notin P$．a_1, a_2 は $\mathcal{O}_L$ の元としても異なる同値類に属する．$\mathcal{O}_L/P$ と $\mathcal{O}_K/\mathfrak{p}$ の位数は等しいので，他の元についても同様にして $\mathcal{O}_L/P$ の完全代表系として $\{a_1, a_2, \ldots\}$ が取れる．よって，$u \in \mathcal{O}_L$ が含まれる同値類の代表元を u_0 とすればよい． □

上の状況で，L/K が完全分岐で馴分岐，F/L の整数環 $\mathcal{O}_F$ の極大イデアルを $\mathcal{P}$，$\mathcal{P}$ 進距離を $|\bullet|$ とする．この時，L/K の分岐指数 e について $|e| = 1$

証明 F は $\mathbb{Q}_p$ の有限次拡大でもあるので，$|\mathcal{O}_F/\mathcal{P}|$ は $|\mathbb{Z}_p/p\mathbb{Z}_p|$ の倍数．命題 I-9.1.31(1) から $|\mathbb{Z}_p/p\mathbb{Z}_p| = |\mathbb{Z}/p\mathbb{Z}| = p$ なので，$|\mathcal{O}_F/\mathcal{P}|$ は p の倍数．従って，$\mathcal{O}_F/\mathcal{P}$ の標数は p（p.I-216 とか参照）．L/K が馴分岐なので $p \nmid e$ となり，$\mathcal{O}_F$ の元として e と 0 は異なる同値類に属する．よって $e \notin \mathcal{P}$ であり，$|e| = 1$． □

1.14 2 次の暴分岐

■命題 1.14.1

追加補題 1.14.7. K を $\mathbb{Q}_2$ の有限次拡大，$\mathfrak{p}$ を $\mathcal{O}_K$ の素イデアル，$F = K(\sqrt{\pi})$ とする．π が $\mathcal{O}_K$ の素元であれば $\mathcal{O}_F$ の $\mathcal{O}_K$ 上基底が $\{1, \sqrt{\pi}\}$ である（命題 1.7.3 使った方が楽）

証明 $2 = \pi^m d$ $(\mathrm{ord}_{\mathfrak{p}}(d) = 0)$ とする．$\mathrm{ord}_{\mathfrak{p}}(\pi) = 1$ である．$\alpha = a + b\sqrt{\pi} \in F$ $(a, b \in K)$ が $\mathcal{O}_K$ 上整であるとする．

$$A = \mathrm{Tr}_{F/K}(\alpha) = (a + b\sqrt{\pi}) + (a - b\sqrt{\pi}) = 2a, \quad B = \mathrm{N}_{F/K}(\alpha) = (a + b\sqrt{\pi})(a - b\sqrt{\pi}) = a^2 - \pi b^2.$$

命題 I-8.1.19 から $A, B \in \mathcal{O}_K$．$4B = A^2 - 4\pi b^2 \in 4\mathcal{O}_K$ なので $4\pi b^2 \in \mathcal{O}_K$，つまり $\mathrm{ord}_{\mathfrak{p}}(4\pi b^2) \geq 0$．よって $2m + 1 + 2\,\mathrm{ord}_{\mathfrak{p}}(b) \geq 0$（命題 1.1.3(1)）なので $\mathrm{ord}_{\mathfrak{p}}(b) \geq -m$．よって $b = c\pi^{-m}$ $(c \in \mathcal{O}_K)$ と表すことができる．$\mathrm{ord}_{\mathfrak{p}}(b) < 0$ とする．つまり $0 \leq \mathrm{ord}_{\mathfrak{p}}(c) \leq m - 1$．$A^2 - 4\pi b^2 = A^2 - \pi c^2 d^2 \in 4\mathcal{O}_K$ なので $A^2 - \pi c^2 d^2 \equiv 0 \bmod \mathfrak{p}^{2m}$．$A = \pi^k t$ $(\mathrm{ord}_{\mathfrak{p}}(t) = 0)$，$c = \pi^{s-1} u$ $(\mathrm{ord}_{\mathfrak{p}}(u) = 0, s \leq m)$ とおけば，この式は $\pi^{2k} t^2 - \pi^{2s-1} u^2 d^2 = \pi^{2m} w$ $(\mathrm{ord}_{\mathfrak{p}}(w) \geq 0)$ となる．

$2k > 2s-1$ であれば $\pi^{2s-1}(\pi^{2k-2s+1} t^2 - u^2 d^2) = \pi^{2m} w$．命題 1.1.3(3) から $\mathrm{ord}_{\mathfrak{p}}(\pi^{2k-2s+1} t^2 - u^2 d^2) = 0$ なので $2s - 1 \geq 2m$．これは $s \leq m$ に矛盾．

$2k < 2s-1$ であれば $\pi^{2k}(t^2 - \pi^{2s-2k-1} u^2 d^2) = \pi^{2m} w$．命題 1.1.3(3) から $\mathrm{ord}_{\mathfrak{p}}(t^2 - \pi^{2s-2k-1} u^2 d^2) = 0$ なので $k \geq m$ となり，$2s - 1 > 2k \geq 2m$ となり $s \leq m$ に矛盾．以上から $\mathrm{ord}_{\mathfrak{p}}(b) \geq 0$，つまり $b \in \mathcal{O}_K$．$a^2 - \pi b^2 \in \mathcal{O}_K$ なので $a^2 \in \mathcal{O}_K$，よって $a \in \mathcal{O}_K$．以上から $\mathcal{O}_F$ は $\mathcal{O}_K + \mathcal{O}_K\sqrt{\pi}$．

逆に $a + b\sqrt{\pi}$ $(a, b \in \mathcal{O}_K)$ は $x^2 - 2ax + a^2 - \pi b^2$ の根なので $\mathcal{O}_K$ 上整． □

K を $\mathbb{Q}_2$ の有限次拡大，$F = K(\sqrt{\pi'})$（π' は $\mathcal{O}_K$ の素元），$\mathfrak{p}$ を $\mathcal{O}_K$ の素イデアルとするとき，$\Delta_{F/K} = 4\mathfrak{p}$

証明 $\sqrt{\pi'}$ の K 上最小多項式は $x^2 - \pi'$ で，その判　別式は $4\pi'$．命題 1.9.9 から $\Delta_{F/K}(1, \sqrt{\pi'}) = 4\pi'$．$\{1, \sqrt{\pi'}\}$ が $\mathcal{O}_F$ の $\mathcal{O}_K$ 基底（上で示した）．K は局所体なので命題 1.5.3 から $\mathcal{O}_K$ は完備離散付値環．$\Delta_{F/K} = \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(4\pi')} = 4\pi'\mathcal{O}_K = 4\mathfrak{p}$． □

K を $\mathbb{Q}_2$ の有限次拡大，$F = K(\sqrt{\mu})$ $(\mu \in \mathcal{O}_K^{\times})$，$\mathcal{O}_K/\mathfrak{p} = \mathbb{F}$ とする．$n = |\mathbb{F}|$ が偶数であれば $\mathbb{F}^{\times} \ni x \mapsto x^2 \in \mathbb{F}^{\times}$ が全単射である

証明 定理 I-7.4.10 から $\mathbb{F}^{\times}$ は位数 $n-1$ の巡回群：$\mathbb{F}^{\times} = \{\, g^i \mid 0 \leq i \leq n-2 \,\}$．$g^{n-1} = 1$ である．$g^i \neq g^j$ とする．$1 \leq |i - j| \leq n - 2$ なので $2 \leq |2i - 2j| \leq 2n - 4$．$n - 1$ は奇数なので $2i - 2j \neq n - 1$．よって $g^{2i} \neq g^{2j}$ となり，単射．$g^1, g^2, \ldots, g^{n/2-1}$ は $g^2, g^4, \ldots, g^{n-2}$ に写る．$g^{n/2}, g^{n/2+1}, \ldots, g^{n-2}$ は $g^{n-1+1}, g^{n-1+3}, \ldots, g^{n-1+n-3}$，つまり $g^1, g^3, \ldots, g^{n-3}$ に写るので全射． □

$\mathrm{mod}\,\mathfrak{p}^l \to \mathrm{mod}\,\mathfrak{p}^{l+1}, \mathrm{mod}\,\mathfrak{p}^{l+2}, \ldots$ の議論が成立していることの検証（p.91 の真ん中らへん）

証明 本文から，$\mathrm{ord}_{\mathfrak{p}}(\mu - 1) = l$ $(\mu \in \mathcal{O}_K^{\times} \setminus (\mathcal{O}_K^{\times})^2)$ に対し l が $2m$ で以下の偶数であれば $\mu' = (1 + \pi^{l_1} c)^{-2}\mu$ があり，$(1 + \pi^{l_1} c)^{-2} \equiv 1 + \pi^l u \bmod \mathfrak{p}^{l+1}$，$\mu' \equiv 1 \bmod \mathfrak{p}^{l+1}$．$(1 + \pi^{l_1} c)^{-2} \in (\mathcal{O}_K^{\times})^2$ となる（背理法で容易に示せる）ので $\mu' \in \mathcal{O}_K^{\times} \setminus (\mathcal{O}_K^{\times})^2$（対偶を考えれば明らか）．$\mathrm{ord}_{\mathfrak{p}}(\mu' - 1) \geq l + 1$ となり，これによって $l = 2m$ となるか l が奇数になるまで l を大きくすることができる． □

K を $\mathbb{Q}_2$ の有限次拡大，$\mathfrak{p}$ を $\mathcal{O}_K$ の素イデアル，$F = K(\sqrt{\mu})$ とする．$\mu \in \mathcal{O}_K^{\times} \setminus (\mathcal{O}_K^{\times})^2$，$\mu = 1 + 4u$ $(u \in \mathcal{O}_K^{\times})$ であれば F/K が不分岐であることの証明．（上の検証で l が $2m$ になった場合．l が奇数になった場合も同様）

証明 $\alpha = (1 + \sqrt{\mu})/2 \in F$ とすれば，α は $g(x) = x^2 - x + (1 - \mu)/4$ の根．$(1 - \mu)/4 \in \mathcal{O}_K$ なので $g(x) \in \mathcal{O}_K[x]$ であることから，α は $\mathcal{O}_K$ 上モニックの根となる．つまり，$\alpha \in \mathcal{O}_F$．また，命題 1.9.9 から

$\Delta_{F/K}(1,\alpha)=\mu\neq 0$. よって, 命題 1.7.3(2) から, $\{1,\alpha\}$ は F の K 基底となり $\mathcal{O}_K$ 上一次独立. $\{1,\alpha\}\in\mathcal{O}_F$ なので, これは $\mathcal{O}_F$ の $\mathcal{O}_K$ 基底になる. よって, $\mathcal{O}_F=\mathcal{O}_K[\alpha]$ で, $\Delta_{F/K}$ の計算に $\Delta_{F/K}(1,\alpha)=\mu$ を使える. K は局所体なので命題 1.5.3 から $\mathcal{O}_K$ は完備離散付値環. $\Delta_{F/K}=\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mu)}=\mu\mathcal{O}_K$. $\mu\in\mathcal{O}_K^{\times}=\mathcal{O}_K\setminus\mathfrak{p}$ (命題 I-6.5.8) なので, $\Delta_{F/K}$ は $\mathfrak{p}$ で割り切れない. よって Dedekind の判別定理 (定理 1.11.12) から F/K は不分岐. □

F を局所体, π を $\mathcal{O}_F$ の素元, $F=K(\sqrt{\pi})$ とすれば, $\sqrt{\pi}$ が $\mathcal{O}_F$ の素元である

証明 追加補題 1.14.7(p.37) から $\mathcal{O}_F=\mathcal{O}_K[\sqrt{\pi}]$, つまり $\mathcal{O}_F=\{\,a+b\sqrt{\pi}\mid a,b\in\mathcal{O}_K\,\}$ なので, $\sqrt{\pi}\mathcal{O}_F=\{\pi b+a\sqrt{\pi}\mid a,b\in\mathcal{O}_K\}$. $c,d\in\mathcal{O}_F\setminus\sqrt{\pi}\mathcal{O}_F$ とする. $c=c_1+c_2\sqrt{\pi}$, $d=d_1+d_2\sqrt{\pi}$ とすれば, $c_1,d_1\notin\pi\mathcal{O}_K$, つまり $\mathrm{ord}_{\mathfrak{p}}(c_1)=\mathrm{ord}_{\mathfrak{p}}(d_1)=0$. $cd=(c_1d_1+c_2d_2\pi)+(c_1d_2+c_2d_1)\sqrt{\pi}$ で, 命題 1.1.3(3) から $\mathrm{ord}_{\mathfrak{p}}(c_1d_1+c_2d_2\pi)=0$ なので $cd\in\mathcal{O}_F\setminus\sqrt{\pi}\mathcal{O}_F$. つまり, $\sqrt{\pi}\mathcal{O}_F$ は素イデアル. □

F を局所体, π を $\mathcal{O}_F$ の素元, $\mu=1+\pi^{2k+1}u$ $(u\in\mathcal{O}_K^{\times})$, $F=K(\sqrt{\mu})$ とすれば $q=(1+\sqrt{\mu})/\pi^k$ が $\mathcal{O}_F$ の素元である

証明 $F=K(\sqrt{\mu})=K(q)$. q は Eisenstein 多項式 $g(x)=x^2-\pi^{m-k}x-\pi u$ の根なので, $\mathcal{O}_K$ 上整となり $q\in\mathcal{O}_F$. $g(x)$ の判別式は $\pi^{2(m-k)}+4\pi u\neq 0$ なので命題 1.9.9, 命題 1.7.3 から $\{1,q\}$ は F の K 基底で $\mathcal{O}_F$ の $\mathcal{O}_K$ 基底:$\mathcal{O}_F=\mathcal{O}_K[q]$, つまり $\mathcal{O}_F=\{\,a+bq\mid a,b\in\mathcal{O}_K\,\}$. $g(q)=0$ なので $aq+bq^2=bu\pi+(a+b\pi^{m-k})q$. よって $q\mathcal{O}_F=\{\,bu\pi+(a+b\pi^{m-k})q\mid a,b\in\mathcal{O}_K\,\}$. $c,d\in\mathcal{O}_F\setminus q\mathcal{O}_F$ とする. $c=c_1+c_2q$, $d=d_1+d_2q$ とすれば $c_1,c_2\notin\pi\mathcal{O}_K$, つまり $\mathrm{ord}_{\mathfrak{p}}(c_1)=\mathrm{ord}_{\mathfrak{p}}(d_1)=0$.

$$cd=c_1d_1+c_2d_2q^2+(c_1d_2+c_2d_1)q=(c_1d_1+c_2d_2\pi u)+(c_1d_2+c_2d_1+c_2d_2\pi^{m-k})q$$

で $\mathrm{ord}_{\mathfrak{p}}(c_1d_1+c_2d_2\pi u)=0$ なので, $cd\in\mathcal{O}_F\setminus q\mathcal{O}_F$. よって $q\mathcal{O}_F$ は $\mathcal{O}_F$ の素イデアル. □

第 2 章

整数環と判別式の例

2.2 Kummer 理論

■命題 2.2.5

G, H の間の perfect pairing を ϕ，$\sigma_g \colon H \ni h \mapsto \Phi(g,h) \in \mathbb{C}^1$ とすれば，写像 $\chi \colon G \ni g \mapsto \sigma_g \in H^*$ は準同型

証明 G は加群，$\mathbb{C}^1$ は乗法群．$\forall h \in H$ に対し，

$$[\chi(g_1)\chi(g_2)]\,(h) = \sigma_{g_1}(h)\sigma_{g_2}(h) = \Phi(g_1,h)\Phi(g_2,h) = \Phi(g_1+g_2,h) = \sigma_{g_1+g_2}(h) = \chi(g_1+g_2)(h).$$

よって，$\chi(g_1)\chi(g_2) = \chi(g_1+g_2)$ となり χ は準同型． □

■定理 2.2.8

$R/(K^\times)^n$ の完全代表系を $\{a_1, \ldots, a_t\}$ とすれば，$K(\sqrt[n]{R}) = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t})$

証明 $\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t} \in \sqrt[n]{R}$ なので $K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t}) \subset K(\sqrt[n]{R})$．$\forall a \in R$ は $b \in K^\times$ によって $a = a_i b^n$ となるので $\sqrt[n]{a} = \sqrt[n]{a_i}b$，つまり $\sqrt[n]{R} = \{\, \sqrt[n]{a_i}b \mid b \in K^\times \,\}$．よって，$\sqrt[n]{R}$ の有限部分集合が生成する体は $K(\sqrt[n]{a_i}, \sqrt[n]{a_j}, \ldots)$ という形になるので，$K(\sqrt[n]{R}) \subset K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t})$．以上から $K(\sqrt[n]{R}) = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t})$． □

■例 2.2.9　$a, b, c, d \in \mathbb{Z}$ に対して $R = 2^a 3^b 5^c 7^d (\mathbb{Q}^\times)^2$ とすれば，$\mathbb{Q}^\times \supset R \supset (\mathbb{Q}^\times)^2$ が成立する．$K = \mathbb{Q}(\sqrt{R}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ とする．$R/(\mathbb{Q}^\times)^2$ の完全代表系として $2^i 3^j 5^k 7^l$ $(i,j,k,l = 0,1)$ が取れる．準同型

$$\begin{aligned}\phi \colon \mathbb{Z}^4 \ni (a,b,c,d) &\mapsto 2^a 3^b 5^c 7^d \in \mathbb{Q}^\times \\ &\mapsto 2^i 3^j 5^k 7^l \in R/(\mathbb{Q}^\times)^2\end{aligned}$$

を考える．明らかに ϕ は全射なので $\operatorname{Im}\phi = R/(\mathbb{Q}^\times)^2$．$R/(\mathbb{Q}^\times)^2$ の単位元は $2^0 3^0 5^0 7^0 = 1$．$\phi(a,b,c,d) = 1$ となるのは a, b, c, d が偶数の時なので，$\ker\phi = (2\mathbb{Z})^4$．よって準同型定理から $R/(\mathbb{Q}^\times)^2 \simeq \mathbb{Z}^4/(2\mathbb{Z})^4 \simeq (\mathbb{Z}/2\mathbb{Z})^4$．命題 2.2.3，定理 2.2.8 から $\operatorname{Gal}(K/\mathbb{Q}) \simeq (R/(\mathbb{Q}^\times)^2)^* \simeq R/(\mathbb{Q}^\times)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^4$．

■例 2.2.10　$\mu \in \mathbb{Z}$，l を素数，ζ を 1 の原始 l 乗根，$F = \mathbb{Q}(\zeta)$ とする．定理 I-8.11.7 から $\mathrm{Gal}(F/\mathbb{Q}) \simeq (\mathbb{Z}/l\mathbb{Z})^\times$．命題 I-7.4.3(2) から $|\mathrm{Gal}(F/\mathbb{Q})| = l-1 = [F:\mathbb{Q}]$．よって，$\mathrm{Hom}^{\mathrm{al}}_{\mathbb{Q}}(F, \overline{\mathbb{Q}}) = \{\sigma_1, \dots, \sigma_{l-1}\}$．

$\mu = a^l$ $(a \in F^\times)$ と仮定する．命題 I-8.1.18(2) から

$$\mathrm{N}_{F/\mathbb{Q}}(\mu) = \mathrm{N}_{F/\mathbb{Q}}(a^l) = [\mathrm{N}_{F/\mathbb{Q}}(a)]^l = \prod_{i=1}^{l-1} \sigma_i(\mu) = \prod_{i=1}^{l-1} \mu = \mu^{l-1} = a^{l(l-1)}.$$

補題 I-8.1.17 から $\mathrm{N}_{F/\mathbb{Q}}(a) \in \mathbb{Q}$ なので互いに素な $b, c \in \mathbb{Z}$ によって $\mathrm{N}_{F/\mathbb{Q}}(a) = c/b$．上の式に代入して $c^l = (ba^{l-1})^l$，よって $c = ba^{l-1}$ となり矛盾．以上から $\mu \notin (F^\times)^l$．

μ が属する $F^\times/(F^\times)^l$ の代表元を g とする．$\mu^l \in (F^\times)^l$ であり，l は素数なので g の位数は l．$1 \le i < j \le l$ に対し $g^i = g^j$ とする．$g^{j-i} = 1$ となるが $1 \le j-i \le l-1$ なので矛盾．よって $\{1, g, \dots, g^{l-1}\}$ は位数 l の $F^\times/(F^\times)^l$ 部分群．$F^\times \supset R = \{\, \mu^i (F^\times)^l \mid 1 \le i \le l \,\} \supset (F^\times)^l$ とすれば $F(\sqrt[n]{R}) = F(\sqrt[n]{\mu})$．命題 2.2.3 と定理 2.2.8 から

$$\mathrm{Gal}(F(\sqrt[n]{\mu})/F) \simeq (R/(F^\times)^l)^* \simeq (R/(F^\times)^l) \simeq \{1, \mu, \dots, \mu^{l-1}\}$$

なので $[F(\sqrt[n]{\mu}) : F] = l$．

■命題 2.2.11

> A を仮定 1.1.2 を満たす Dedekind 環，$\mathfrak{p}$ を A の素イデアル，$f(x) = x^e - \mu$，e は $A/\mathfrak{p}$ の標数 p で割り切れない，$\mu \in A \setminus \mathfrak{p}$ とすれば，$f(x)$ の判別式 $\Delta(f)$ は $\mathfrak{p}$ に含まれない

証明 系 1.9.7 から $\Delta(f) = \pm\mu^{e-1}e^e$．仮定 1.1.2 から A の商体 K の標数は 0 なので $\mathbb{Q}$ を含み，$a/1$ $(a \in \mathbb{Z})$ という形の元を含む．よって $\mathbb{Z} \subset A$．$\mathfrak{p}$ は $p\mathbb{Z}$ の上にあり，$e \notin p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ なので $e \notin \mathfrak{p}$ である．よって，$\mu^{e-1}e^e \notin \mathfrak{p}$ となる．　□

> $L = K(\sqrt[e]{\mu})$，$g(x) \in A[x]$ を $\sqrt[e]{\mu}$ の K 上最小多項式，$\Delta(g) \in A \setminus \mathfrak{p}$ とすれば $\mathfrak{p}$ は L で不分岐

証明 $g(x) \in A[x]$ なので $\sqrt[e]{\mu} \in L$ は A 上整，すなわち B の元となり $\Delta_{L/K}(1, \sqrt[e]{\mu}, \dots, \sqrt[e]{\mu}^{n-1}) = \Delta(g) \in A \setminus \mathfrak{p} \subset A_{\mathfrak{p}}^\times$（命題 1.9.9）．補題 1.7.3(2) から $\{1, \sqrt[e]{\mu}, \dots, \sqrt[e]{\mu}^{n-1}\}$ は B に含まれる L の K 基底となり，補題 1.8.3 から $\Delta_{L/K,\mathfrak{p}} = A$．$\Delta_{L/K}$ は $\mathfrak{p}$ で割り切れないので Dedekind の判別定理から $\mathfrak{p}$ は L で不分岐．　□

> $B \otimes_A A_{\mathfrak{p}}$ の $A_{\mathfrak{p}}$ 基底が取れる

証明 命題 I-6.5.9，補題 I-8.3.3，補題 I-8.3.13 から $A_{\mathfrak{p}}$ は単項イデアル整域．命題 I-8.1.14 から L における $A_{\mathfrak{p}}$ の整閉包は $B_{\mathfrak{p}}$．命題 I-8.1.24 から $B_{\mathfrak{p}}$ は階数 $[L:K] = n$ の自由 $A_{\mathfrak{p}}$ 加群なので n 個の $A_{\mathfrak{p}}$ 基底を取れる．補題 1.3.22 から $B_{\mathfrak{p}} \simeq A_{\mathfrak{p}} \otimes_A B \simeq B \otimes_A A_{\mathfrak{p}}$ よって，$B_{\mathfrak{p}}$ の $A_{\mathfrak{p}}$ を上の同型によって写せば，$B \otimes_A A_{\mathfrak{p}}$ の $A_{\mathfrak{p}}$ 基底となる．　□

2.3 3 次体

よく使う命題を列挙しておく．

- 系 I-8.1.25．$\mathcal{O}_K$ は階数 $[K:\mathbb{Q}]$ の自由 $\mathbb{Z}$ 加群
- 命題 1.2.14．$\forall \mathfrak{p} \in \operatorname{Spec} A$ に対し $a \in \widehat{A}_{\mathfrak{p}}$ なら $a \in A$
- 系 1.7.5．$\Delta_K(v_1,\dots,v_n) = (\mathcal{O}_K : V)^2 \Delta_K$
- 命題 1.8.9．$(B:M) = \displaystyle\prod_{\mathfrak{p}\in\operatorname{Spec} A} (B \otimes_A \widehat{A}_{\mathfrak{p}} : M \otimes_A \widehat{A}_{\mathfrak{p}})$
- 命題 1.9.9．$\Delta(f) = \Delta_{L/K}(1,\alpha,\dots)$
- 命題 1.10.7．CDVR での Eisenstein と完全分岐
- 命題 1.11.1．$\Delta_{B/A,\mathfrak{p}} = \displaystyle\prod_{i=1}^{g} \Delta_{\widehat{B}_i/\widehat{A}_{\mathfrak{p}}}$

■例 2.3.3

t の $\mathbb{Q}$ 上最小多項式 $f(x)$ の判別式が 49 ならば $(\mathcal{O}_K : \mathbb{Z}[t]) = 1, 7$

証明 命題 1.9.9 から $\Delta_{K/\mathbb{Q}}(1,t,t^2) = \Delta(f) = 49$．$\{1,t,t^2\}$ は $K = \mathbb{Q}(t)$ の $\mathbb{Q}$ 基底で，$\mathcal{O}_K$ に含まれる．よって系 1.7.5(2) から $\Delta_{K/\mathbb{Q}}(1,t,t^2) = (\mathcal{O}_K : \mathbb{Z}[t])^2 \Delta_K$ となり従う． □

$(B_{\mathfrak{p}} : M \otimes_A A_{\mathfrak{p}}) = 1$，$\mathcal{O}_K = \mathbb{Z}[t]$，$\Delta_K = 49$

証明 $f(x+2) = g(x)$ とする．$g(x)$ は Eisenstein 多項式で，$\mathbb{Q}_7$ 上既約である．$\mathbb{Q}_7$ は平坦 $\mathbb{Q}$ 加群なので

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_7 \simeq \left(\frac{\mathbb{Q}[x]}{(g(x))}\right) \otimes_{\mathbb{Q}} \mathbb{Q}_7 \simeq \frac{\mathbb{Q}[x] \otimes_{\mathbb{Q}} \mathbb{Q}_7}{(g(x)) \otimes_{\mathbb{Q}} \mathbb{Q}_7} \simeq \frac{\mathbb{Q}_7[x]}{(g(x))} \simeq \mathbb{Q}_7(t).$$

従って，定理 1.3.23 から，$7\mathbb{Z}$ の上にある $\mathcal{O}_K$ の素イデアルは 1 個で，K の完備化は $\mathbb{Q}_7(t)$．$\mathbb{Q}_7[t]$ の整数環は $\mathbb{Z}_7[t]$ なので，再び定理 1.3.23 から $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_7 \simeq \mathbb{Z}_7[t]$．さらに，$\mathbb{Z}[t] \otimes_{\mathbb{Z}} \mathbb{Z}_7 \simeq \mathbb{Z}_7[t]$ で，これらの同型は同じ写像である（$a \otimes b \mapsto ab$）．従って，命題 1.8.9(3) から $(B_{\mathfrak{p}} : M \otimes_A A_{\mathfrak{p}}) = (B \otimes_A \widehat{A}_{\mathfrak{p}} : M \otimes_A \widehat{A}_{\mathfrak{p}}) = (\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_7 : \mathbb{Z}[t] \otimes_{\mathbb{Z}} \mathbb{Z}_7) = 1$.

$\mathfrak{p} = p\mathbb{Z} \neq 7\mathbb{Z}$ に対しては $(B_{\mathfrak{p}} : M \otimes_A A_{\mathfrak{p}})$ は命題 1.8.9(2) から p の冪なので 7 の倍数では無い．よって命題 1.8.9(1) から $(B:M) = (\mathcal{O}_K : \mathbb{Z}[t]) = 1$．上の話と合わせて $\Delta_K = \Delta_{K/\mathbb{Q}}(1,t,t^2) = 49$． □

$t = 2\cos 2\pi/7$ として $\mathbb{Q}(t)/\mathbb{Q}$ は Galois 拡大である

証明 例 I-8.11.8 から t の $\mathbb{Q}$ 上最小多項式は $x^3 + x^2 - 2x + 1$ で，t の共軛は $2\cos 4\pi/7$ と $2\cos 6\pi/7$．$2\cos 4\pi/7 = 4t^2 - 2$，$2\cos 6\pi/7 = -4t^2 - t + 1$ なので t の共軛は全て $\mathbb{Q}(t)$ に含まれる．よって系 I-7.3.10 から $\mathbb{Q}(t)/\mathbb{Q}$ は正規拡大．$\mathbb{Q}$ は完全体（系 I-7.3.6）なので $\mathbb{Q}(t)/\mathbb{Q}$ は分離拡大． □

■命題 2.3.4

同型 ϕ: $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \to {\mathbb{Z}_p}^n$ が存在すれば，$\mathcal{O}_K$ の $\mathbb{Z}$ 基底を $\{1, \alpha, \ldots, \alpha^{n-1}\}$，$\beta = \phi(\alpha)$ として $\{1, \beta, \ldots, \beta^{n-1}\}$ が ${\mathbb{Z}_p}^n$ の $\mathbb{Z}_p$ 基底となる

証明 $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ の $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ 基底として，$\{1 \otimes 1, \alpha \otimes 1, \ldots, \alpha^{n-1} \otimes 1\}$ が取れることを示す．

先ず，$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ の任意の元は

$$\xi = (a_0 \otimes b_0)(1 \otimes 1) + (a_1 \otimes b_1)(\alpha \otimes 1) + \cdots + (a_{n-1} \otimes b_{n-1})(\alpha^{n-1} \otimes 1)$$

と表すことができるので，$\{1 \otimes 1, \alpha \otimes 1, \ldots, \alpha^{n-1} \otimes 1\}$ は $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ 上 $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ を生成する．

$\{1, \alpha, \ldots, \alpha^{n-1}\}$ は $\mathcal{O}_K$ の $\mathbb{Z}$ 基底なので

$$\mathbb{Z}^n \ni (a_0, \ldots, a_{n-1}) \mapsto a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in \mathcal{O}_K$$

は全単射．$\mathbb{Z}_p$ は平坦 $\mathbb{Z}$ 加群なので，$(\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^n \simeq \mathbb{Z}^n \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ も全単射である．従って，同型

$$(\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^n \ni \begin{pmatrix} a_0 \otimes b_0 \\ a_1 \otimes b_1 \\ \vdots \\ a_{n-1} \otimes b_{n-1} \end{pmatrix} \mapsto a_0 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \otimes b_0 + a_1 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \otimes b_1 + \cdots + a_{n-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \otimes b_{n-1} \in \mathbb{Z}^n \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

$$\mapsto a_0 \otimes b_0 + \cdots + a_{n-1}\alpha^{n-1} \otimes b_{n-1} \in \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

が得られる．よって，$\xi = 0$ なら $a_i \otimes b_i = 0$ となるので，$\{1 \otimes 1, \alpha \otimes 1, \ldots, \alpha^{n-1} \otimes 1\}$ は一次独立．

$$\begin{aligned}
\phi(\xi) &= \phi((a_0 \otimes b_0)(1 \otimes 1) + (a_1 \otimes b_1)(\alpha \otimes 1) + \cdots + (a_{n-1} \otimes b_{n-1})(\alpha^{n-1} \otimes 1)) \\
&= \phi((a_0 \otimes b_0)(1 \otimes 1)) + \phi((a_1 \otimes b_1)(\alpha \otimes 1)) + \cdots + \phi((a_{n-1} \otimes b_{n-1})(\alpha^{n-1} \otimes 1)) \\
&= \phi(a_0 \otimes b_0)\phi(1 \otimes 1) + \phi(a_1 \otimes b_1)\phi(\alpha \otimes 1) + \cdots + \phi(a_{n-1} \otimes b_{n-1})\phi(\alpha^{n-1} \otimes 1) \\
&= \phi(a_0 \otimes b_0)\phi(1 \otimes 1) + \phi(a_1 \otimes b_1)\phi(\alpha \otimes 1) + \cdots + \phi(a_{n-1} \otimes b_{n-1})\phi(\alpha \otimes 1)^{n-1}.
\end{aligned}$$

なので，

$$\phi(\xi) = 0 \Leftrightarrow \xi = 0 \Leftrightarrow a_i \otimes b_i = 0 \Leftrightarrow \phi(a_i \otimes b_i) = 0$$

となるので，$\beta = \phi(\alpha \otimes 1)$ として $\{1, \beta, \ldots, \beta^{n-1}\}$ が ${\mathbb{Z}_p}^n$ の $\mathbb{Z}_p$ 基底となる． □

$\beta = (\beta_1, \ldots, \beta_n) \in {\mathbb{Z}_p}^n$ として，${\mathbb{Z}_p}^n$ の $\mathbb{Z}_p$ 基底が $\{1, \beta, \ldots, \beta^{n-1}\}$ であれば $\det(1, \beta, \ldots, \beta^{n-1}) \in \mathbb{Z}_p^{\times}$

証明 $\{1, \beta, \ldots, \beta^{n-1}\}$ は ${\mathbb{Z}_p}^n$ の $\mathbb{Z}_p$ 基底なので

$$(1, 0, \ldots, 0) = (a_0^{(1)}, \ldots, a_{n-1}^{(1)}) \begin{pmatrix} 1 & \cdots & 1 \\ \beta_1 & \cdots & \beta_n \\ & \vdots & \\ {\beta_1}^{n-1} & \cdots & {\beta_n}^{n-1} \end{pmatrix}$$

となる $a_0^{(1)},\dots,a_{n-1}^{(1)}\in\mathbb{Z}_p$ が存在する．同様にして

$$\begin{pmatrix}1&&&\\&1&&\\&&\ddots&\\&&&1\end{pmatrix}=\begin{pmatrix}a_0^{(1)}&\cdots&a_{n-1}^{(1)}\\&\vdots&\\a_0^{(n)}&\cdots&a_{n-1}^{(n)}\end{pmatrix}\begin{pmatrix}1&\cdots&1\\\beta_1&\cdots&\beta_n\\&\vdots&\\{\beta_1}^{n-1}&\cdots&{\beta_n}^{n-1}\end{pmatrix}=:AX$$

となるので，行列式をとって $1=\det A\det X$．よって $\det X\in\mathbb{Z}_p^\times$． □

$\beta_1,\dots,\beta_n\in\mathbb{Z}_p$ $(p<n)$ とすれば $i\neq j$ で $\beta_i\equiv\beta_j \bmod p\mathbb{Z}_p$

証明 命題 I-9.1.31(1) から $|\mathbb{Z}_p/p\mathbb{Z}_p|=p$．$\beta_1-\beta_2,\dots,\beta_1-\beta_n$ のうち少なくとも 1 つが $\equiv 0$，もしくは 1 組が $\equiv$ である．後者の場合はその二つの差が $\equiv 0$ となり主張を満たす． □

$\alpha\in\mathcal{O}_K$，$K=\mathbb{Q}(\alpha)$ で，$\mathcal{O}_K$ が冪基底を持たなければ，$(\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p:\mathbb{Z}_p[\alpha])\neq 1$ で，これは p の冪であり，$(\mathcal{O}_K:\mathbb{Z}[\alpha])$ の約数になる

証明 $(\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p:\mathbb{Z}[\alpha]\otimes_{\mathbb{Z}}\mathbb{Z}_p)=1$ とする．完全系列

$$0\longrightarrow\mathbb{Z}[\alpha]\longrightarrow\mathcal{O}_K\longrightarrow\mathcal{O}_K/\mathbb{Z}[\alpha]\longrightarrow 0$$

に対し，$\mathbb{Z}_p$ は平坦 $\mathbb{Z}$ 加群なので，

$$0\longrightarrow\mathbb{Z}[\alpha]\otimes_{\mathbb{Z}}\mathbb{Z}_p\longrightarrow\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p\longrightarrow(\mathcal{O}_K/\mathbb{Z}[\alpha])\otimes_{\mathbb{Z}}\mathbb{Z}_p\longrightarrow 0$$

も完全．従って，

$$\begin{aligned}0=\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p/\mathbb{Z}[\alpha]\otimes_{\mathbb{Z}}\mathbb{Z}_p&\simeq(\mathcal{O}_K/\mathbb{Z}[\alpha])\otimes_{\mathbb{Z}}\mathbb{Z}_p\\&\simeq(\mathcal{O}_K/\mathbb{Z}[\alpha])\otimes_{\mathbb{Z}_{(p)}}\mathbb{Z}_{(p)}\otimes_{\mathbb{Z}}\mathbb{Z}_p\simeq(\mathcal{O}_K/\mathbb{Z}[\alpha])\otimes_{\mathbb{Z}_{(p)}}\mathbb{Z}_p\end{aligned}$$

となる．$\mathbb{Z}_p\simeq\varprojlim(\mathbb{Z}/p^n\mathbb{Z})\simeq\varprojlim(\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)})$ なので，$\mathbb{Z}_p$ は局所 Noether 環 $\mathbb{Z}_{(p)}$ の完備化であり，$\mathbb{Z}_{(p)}$ 上忠実平坦．従って，$\mathcal{O}_K/\mathbb{Z}[\alpha]=0$，すなわち $\mathcal{O}_K=\mathbb{Z}[\alpha]$ となり矛盾．

例 2.3.3 と同様に，$A=\mathbb{Z}$，$B=\mathcal{O}_K$，$M=\mathbb{Z}[\alpha]$，$\mathfrak{p}=p\mathbb{Z}$ とすれば $(B_{\mathfrak{p}}:M\otimes_A A_{\mathfrak{p}})=(\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p:\mathbb{Z}_p[\alpha])$．命題 1.8.9(2) からこれは $\mathcal{N}(\mathfrak{p})=p$ の冪．主張の後半は命題 1.8.9(1) から従う． □

■例 2.3.5

$K=\mathbb{Q}(\alpha)$，α の $\mathbb{Q}$ 上最小多項式を $f(x)\in\mathbb{Z}[x]$，$\mathbb{Q}_2$ での $f(x)$ の根を $\beta_1,\beta_2,\beta_3\in\mathbb{Z}_2$ とする．この時，$K\otimes_{\mathbb{Q}}\mathbb{Q}_2\simeq{\mathbb{Q}_2}^3$，$\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_2\simeq{\mathbb{Z}_2}^3$ で，$\alpha\mapsto\beta_1,\beta_2,\beta_3$ と対応する

証明 $\mathbb{Q}_2$ は平坦 $\mathbb{Q}$ 加群なので，

$$\begin{aligned}K\otimes_{\mathbb{Q}}\mathbb{Q}_2=\mathbb{Q}(\alpha)\otimes_{\mathbb{Q}}\mathbb{Q}_2&\simeq\left(\frac{\mathbb{Q}[x]}{(f(x))}\right)\otimes_{\mathbb{Q}}\mathbb{Q}_2\simeq\frac{\mathbb{Q}[x]\otimes_{\mathbb{Q}}\mathbb{Q}_2}{(f(x))\otimes_{\mathbb{Q}}\mathbb{Q}_2}\simeq\mathbb{Q}_2[x]/(f(x))\\&=\mathbb{Q}_2[x]/((x-\beta_1)(x-\beta_2)(x-\beta_3))\simeq\mathbb{Q}_2[x]/(x-\beta_1)\times\mathbb{Q}_2[x]/(x-\beta_2)\times\mathbb{Q}_2[x]/(x-\beta_3)\end{aligned}$$

$$\simeq \mathbb{Q}_2 \times \mathbb{Q}_2 \times \mathbb{Q}_2$$

である．この同型によって，$\alpha \otimes 1 \mapsto [x] \otimes 1 \mapsto [x] \mapsto ([x],[x],[x]) \mapsto (\beta_1, \beta_2, \beta_3)$ となる．

定理 1.3.23 から $2\mathbb{Z}$ の上にある $\mathcal{O}_K$ の素イデアルは 3 つであり，それらによる K の完備化を $\widehat{K}_1$，その整数環を $\widehat{\mathcal{O}}_1$ などと表す．この時，

$$\begin{array}{ccccc} K \otimes_{\mathbb{Q}} \mathbb{Q}_2 & \xrightarrow{\simeq} & \widehat{K}_1 \times \widehat{K}_2 \times \widehat{K}_3 & \xrightarrow{\simeq} & {\mathbb{Q}_2}^3 \\ \cup & & \cup & & \cup \\ \alpha \otimes 1 & \longmapsto & (\phi_1(\alpha), \phi_2(\alpha), \phi_3(\alpha)) & \longmapsto & (\beta_1, \beta_2, \beta_3) \end{array}$$

が得られる．追加定理 1.3.4(p.15) から，これを整数環に制限して

$$\begin{array}{ccccc} \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_2 & \xrightarrow{\simeq} & \widehat{\mathcal{O}}_1 \times \widehat{\mathcal{O}}_2 \times \widehat{\mathcal{O}}_3 & \xrightarrow{\simeq} & {\mathbb{Z}_2}^3 \\ \cup & & \cup & & \cup \\ \alpha \otimes 1 & \longmapsto & (\phi_1(\alpha), \phi_2(\alpha), \phi_3(\alpha)) & \longmapsto & (\beta_1, \beta_2, \beta_3) \end{array}$$

となる． □

$\mathcal{O}_K \supset \mathbb{Z}[\alpha]$ なら，奇素数 p に対して $(\alpha^2 - \alpha)/2 \in \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$

証明 $\alpha^2 - \alpha \in \mathcal{O}_K$ である．$\mathrm{ord}_p(1/2) = 0$ なので $|1/2| = 1$，すなわち $1/2 \in \mathbb{Z}_p$（定理 I-9.1.26(5)）．よって $(\alpha^2 - \alpha) \otimes 1/2 \in \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$. □

全ての素数 p に対し $\gamma \otimes 1 \in \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ であれば $\gamma \in \mathcal{O}_K$

証明 $p\mathbb{Z}$ の上にある $\mathcal{O}_K$ の素イデアルを $P_1, \ldots$，P_i 進距離による $\mathcal{O}_K$ の完備化を $\widehat{\mathcal{O}}_i$ とする．定理 1.3.23(2) から $\phi_i \colon \mathcal{O}_K \hookrightarrow \widehat{\mathcal{O}}_i$ として $\phi \colon \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \ni x \otimes y \mapsto (\phi_1(x)y, \ldots) \in \widehat{\mathcal{O}}_1 \times \cdots$ なので，$\phi_i(\gamma) \in \widehat{\mathcal{O}}_i$．よって全ての p を考えれば，$\mathcal{O}_K$ の全ての素イデアル P に対し，P 進距離による完備化を $\widehat{\mathcal{O}}$ とすれば $\gamma \in \widehat{\mathcal{O}}$．よって命題 1.2.14 から $\gamma \in \mathcal{O}_K$. □

$K = \mathbb{Q}(\alpha)$, $\Delta_K = -503$, $\alpha^3 + 6\alpha^2 - \alpha + 2 = 0$, $\mathcal{O}_K$ の $\mathbb{Z}$ 基底を $\{1, \alpha, (\alpha^2 - \alpha)/2\}$ とすれば，$x \in \mathcal{O}_K$，$K = \mathbb{Q}(x)$ として $(\mathcal{O}_K : \mathbb{Z}[x])$ が 2 の倍数である

証明 p.106 の真ん中の方法と同様に，x の最小多項式を求める．

```
? m = [a, b − c / 2, c / 2; −c, a + c / 2, b − 7 ∗ c / 2; 7 ∗ c − 2 ∗ b, b − 9 ∗ c / 2, a − 6 ∗ b + 43 ∗ c /
    2]
? charpoly(m)
? poldisc(%2)
```

特性多項式 $g(x)$ は

$$x^3 + (-3a + (6b - 22c))x^2 + (3a^2 + (-12b + 44c)a + (-b^2 + 7cb - 9c^2))x$$

$$+(-a^3+(6b-22c)a^2+(b^2-7cb+9c^2)a+(2b^3-9cb^2+7c^2b-2c^3))$$

で，判別式は

$$\Delta(g)=-2012b^6+30180cb^5-175547c^2b^4+487910c^3b^3-634283c^4b^2+311860c^5b-50300c^6.$$

系 1.7.5(2)，命題 1.9.9 から

$$\begin{aligned}(\mathcal{O}_K:\mathbb{Z}[x])^2=\frac{\Delta(c)}{\Delta_K}&=4b^6+60cb^5+349c^2b^4-970c^3b^3+1261c^4b^2-620c^5b+100c^6\\&\equiv c^2b^2(349b^2+1261c^2)\equiv 0 \bmod 4\end{aligned}$$

となる．□

$f(x)=x^3+6x^2-x+2$，α を $f(x)$ の根，$K=\mathbb{Q}(\alpha)$，$A=\mathbb{Z}[x]/(f(x))\simeq\mathbb{Z}[\alpha]$ とした時，$A/503A\simeq\mathbb{F}_{503}[x]/((x-39)^2)\times\mathbb{F}_{503}[x]/(x+84)$

証明 $f(x)\equiv(x-39)^2(x+84) \bmod 503$ なので，$g(x)\in\mathbb{Z}[x]$ $(\deg g\leq 2)$ として自然な全射準同型

$$A=\mathbb{Z}[x]/(f(x))\ni g(x)+(f(x))\mapsto\overline{g}(x)+((x-39)^2(x+84))\in\mathbb{F}_{503}[x]/((x-39)^2(x+84))$$

の ker は $g(x)$ のうち係数が 503 の倍数の物で代表される：$503A$．よって準同型定理から $A/503A\simeq\mathbb{F}_{503}[x]/((x-39)^2(x+84))$. $-116(x-39)^2+116(x-6)(x+84)=-234900\equiv 1$ なので, $((x-39)^2)+(x+84)=\mathbb{F}_{503}[x]$．よって中国式剰余定理から

$$A/503A\simeq\mathbb{F}_{503}[x]/((x-39)^2(x+84))\simeq\mathbb{F}_{503}[x]/((x-39)^2)\times\mathbb{F}_{503}[x]/(x+84).$$

(503 は $(\mathcal{O}_K:\mathbb{Z}[\alpha])$ を割らないので，素イデアル分解に関する定理を使った方が早い) □

■例 2.3.6

$n=4$ の場合

$g(x+1)\in\mathbb{Z}_2[x]$ がモニックな Eisenstein 多項式であれば $g(x)=x^2+cx+d$ $(c\equiv 4,\ d\equiv 1 \bmod 8)$ の根を γ，$F=\mathbb{Q}_2(\gamma)$ とすれば $\mathcal{O}_F=\mathbb{Z}_2[\gamma]$

証明 $h(x)=g(x+1)$ とすれば $h(x)$ は Eisenstein 多項式で，その根は $\gamma-1$．$\mathbb{Q}_2(\gamma)=\mathbb{Q}_2(\gamma-1)$ は容易に分かる．$\mathbb{Z}_2$, $\mathcal{O}_F$ はともに完備離散付値環である．従って命題 1.10.7 から $F/\mathbb{Q}_2$ は完全分岐で，分岐指数は 2．$\mathcal{O}_F$ の素イデアルを P とする．$\mathrm{ord}_P(c+2)=2\,\mathrm{ord}_{2\mathbb{Z}_2}(c+2)=2$，同様に $\mathrm{ord}_P(c+d+1)=2$ となる．命題 1.1.3 と $h(\gamma-1)=0$ から

$$2=\mathrm{ord}_P((\gamma-1)^2+(c+2)(\gamma-1))\geq\min\{2\,\mathrm{ord}_P(\gamma-1),\mathrm{ord}_P(c+2)+\mathrm{ord}_P(\gamma-1)=2+\mathrm{ord}_P(\gamma-1)\},$$

ただし $2\,\mathrm{ord}_P(\gamma-1)\neq 2+\mathrm{ord}_P(\gamma-1)$ すなわち $\mathrm{ord}_P(\gamma-1)\neq 2$ なら等号が成立．$\gamma-1$ は $\mathbb{Z}_2$ 上整（実際 $h(x)$ が存在する）なので，$\mathrm{ord}_P(\gamma-1)\geq 0$．$\mathrm{ord}_P(\gamma-1)=0$ なら $2=0$ で矛盾．$\mathrm{ord}_P(\gamma-1)=1$ は式を満たす．$\mathrm{ord}_P(\gamma-1)\geq 2$ では右辺が 4 以上なので不適．よって $\mathrm{ord}_P(\gamma-1)=1$，つまり $\gamma-1$ は $\mathcal{O}_F$ の素元となり，再び命題 1.10.7 から $\mathcal{O}_F=\mathbb{Z}_2[\gamma-1]=\mathbb{Z}_2[\gamma]$ となる．□

上の状況で $\Delta_{F/\mathbb{Q}_2} = (4)$

証明 $h(x) = g(x+1)$ は $\mathbb{Q}_2$ 上既約なので $g(x)$ も $\mathbb{Q}_2$ 上既約である（対偶取る）．よって，$F = \mathbb{Q}_2(\gamma)$ で γ の $\mathbb{Q}_2$ 上最小多項式は $g(x) \in \mathbb{Z}_2[x]$ で，$\mathcal{O}_F = \mathbb{Z}_2[\gamma]$．$\Delta(g) \equiv 4 \bmod 8$，命題 1.9.9 から $\Delta_{F/\mathbb{Q}_2}(1,\gamma) = \Delta(g)$．よって $\mathrm{ord}_P(\Delta_{F/\mathbb{Q}_2}(1,\gamma)) = 2\,\mathrm{ord}_{2\mathbb{Z}_2}(\Delta_{F/\mathbb{Q}_2}(1,\gamma)) = 4$．$(2) = P^2$（分岐指数が 2）なので，$\Delta_{F/\mathbb{Q}_2} = \Delta_{F/\mathbb{Z}_Q,P} = P^4 = (2^2) = (4)$． □

$K = \mathbb{Q}(\alpha)$，α の $\mathbb{Q}$ 上最小多項式を $f(x) \in \mathbb{Z}[x]$ とする．$f(x)$ が $\mathbb{Q}_2$ 上 $(x-\beta)(x^2+cx+d)$（$\beta \in \mathbb{Z}_2$，x^2+cx+d は $\mathbb{Q}_2$ 上既約）となり，x^2+cx+d の根を γ，$F = \mathbb{Q}_2(\gamma)$ とすれば，$\mathbb{Q}_2$ 同型として $K \otimes_{\mathbb{Q}} \mathbb{Q}_2 \simeq \mathbb{Q}_2 \times F$ で，$\Delta_{\widehat{K}_1/\mathbb{Q}_2} = \Delta_{\mathbb{Q}_2/\mathbb{Q}_2}$, $\Delta_{\widehat{K}_2/\mathbb{Q}_2} = \Delta_{F/\mathbb{Q}_2}$

証明 例 2.3.5 と同様に．$\mathbb{Q}_2$ 同型

$$\mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{Q}_2 \simeq \mathbb{Q}[x]/(x-\beta) \times \mathbb{Q}[x]/(x^2+cx+d) \simeq \mathbb{Q}_2 \times F$$

を得る．従って，$2\mathbb{Z}$ の上にある $\mathcal{O}_K$ の素イデアルは 2 つ（$\mathfrak{p}_1$, $\mathfrak{p}_2$ とする）で，それらによる K の完備化を $\widehat{K}_1, \widehat{K}_2$ とする．$\mathbb{Q}_2$ 同型 $\widehat{K}_1 \times \widehat{K}_2 \simeq \mathbb{Q}_2 \times F$ から，$\mathbb{Q}_2$ 同型 $\widehat{K}_1 \simeq \mathbb{Q}_2$，$\widehat{K}_2 \simeq F$ が得られる．

以下の補題を使えば $\Delta_{\widehat{K}_1/\mathbb{Q}_2} = \Delta_{\mathbb{Q}_2/\mathbb{Q}_2}$, $\Delta_{\widehat{K}_2/\mathbb{Q}_2} = \Delta_{F/\mathbb{Q}_2}$ が分かる． □

追加補題 2.3.1. L/K, M/K を局所体とする．K 同型 $\phi\colon L \simeq M$ があれば，$\Delta_{L/K} = \Delta_{M/K}$．

証明 L, M における $\mathcal{O}_K =: A$ の整閉包を B, C とする．命題 1.5.3(2) から A, B, C は完備離散付値環で，$\phi(B) = C$ となる（追加補題 1.3.3, p.14）．それぞれの素イデアルを $\mathfrak{p}, P, \mathcal{P}$ とすると，$\phi(P) = \mathcal{P}$ となることは容易に分かる．命題 I-6.5.8(2) から $S = A \setminus \mathfrak{p}$ は $A^\times$ に含まれ，$S \subset (B \setminus P) \subset B^\times$，$S \subset C^\times$ が成立する．よって $A_{\mathfrak{p}} = S^{-1}A = A$，$B_{\mathfrak{p}} = B$，$C_{\mathfrak{p}} = C$ である．

$\{v_1, \ldots, v_n\}$ を B の A 基底とする（命題 I-8.1.24(3)）．ϕ は K の元を不変にするので A の元も変えない．$a_1v_1 + \cdots + a_nv_n = 0$ ならば $a_1 = \cdots = a_n = 0$．よって，$a_1\phi(v_1) + \cdots + a_n\phi(v_n) = 0$ ならば $a_1 = \cdots = a_n = 0$ なので $\{\phi(v_1), \ldots, \phi(v_n)\}$ は A 上一次独立．$\forall c \in C$ に対し $\phi^{-1}(c) = a_1v_1 + \cdots + a_nv_n$ となる $a_1, \ldots \in A$ が存在する．これを ϕ で写せば $c = a_1\phi(v_1) + \cdots + a_n\phi(v_n)$ となるので，$\{\phi(v_1), \ldots, \phi(v_n)\}$ は C の A 基底となる．

$\mathrm{Hom}_K^{\mathrm{al}}(M, \overline{K})$ と $\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ は ϕ の合成によって 1 対 1 に対応する．$\sigma_i \in \mathrm{Hom}_K^{\mathrm{al}}(M, \overline{K})$ とすれば，

$$\mathrm{Tr}_{M/K}(\phi(v_i)\phi(v_j)) = \sum_i \sigma_i(\phi(v_i)\phi(v_j)) = \sum_i \sigma_i \circ \phi(v_i)\sigma_i \circ \phi(v_j) = \mathrm{Tr}_{L/K}(v_iv_j).$$

よって $\Delta_{L/K}(v_1, \ldots, v_n) = \Delta_{M/K}(\phi(v_1), \ldots, \phi(v_n))$ となり，$\Delta_{L/K,\mathfrak{p}} = \Delta_{M/K,\mathfrak{p}}$．以上から，相対判別式は等しい：$\Delta_{L/K} = \Delta_{M/K}$． □

$\Delta_{K/\mathbb{Q},2} = (4)$ なら $\Delta_K = \Delta(f) = -436$ で $\mathcal{O}_K = \mathbb{Z}[\alpha]$

証明 命題 1.9.9 から $\Delta_{K/\mathbb{Q}}(1,\alpha,\alpha^2)=\Delta(f)=-436$. 系 1.7.5(2) から $\Delta_{K/\mathbb{Q}}(1,\alpha,\alpha^2)=(\mathcal{O}_K:\mathbb{Z}[\alpha])^2\Delta_K$. 命題 1.8.5 から Δ_K は 4 で割り切れるので，$\Delta_K=-436$. $(\mathcal{O}_K:\mathbb{Z}[\alpha])=1$ となるので，$\mathcal{O}_K=\mathbb{Z}[\alpha]$. □

$n=6$ の場合 前半は $n=4$ の場合と同様. $g(2y+1)$ の根を γ と置いたので，$f(x)=(x-\beta)g(x)$ の根は $\beta, 2\gamma+1$.

写像 ϕ は $K\hookrightarrow K\otimes_{\mathbb{Q}}\mathbb{Q}_2\simeq\mathbb{Q}_2\times F$. この話から，これを整数環に制限すれば $\mathcal{O}_K\hookrightarrow\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_2\simeq\mathbb{Z}_2\times\mathcal{O}_F$. したがって，$a\in K$ を ϕ で写した物が $\mathbb{Z}_2\times\mathcal{O}_F$ の元ならば $a\in\mathcal{O}_K$ と言える.

$n=14$ の場合 $g(4y+1)/16=y^2+(c+2)/4y+(c+d+1)/16$ を $2\mathbb{Z}_2$（係数の ord_2 は 0）を法として考えれば x^2+x+1 となり，±1 は根にならないので，命題 I-8.1.10 から $\mathbb{Z}_2/2\mathbb{Z}_2$ 上既約. 命題 I-8.2.1 からこれは $\mathbb{Z}_2$ 上既約.

$\mathcal{O}_F$ を求める. $\alpha=a+b\gamma\in F$ $(a,b\in\mathbb{Q}_2)$ が $\mathbb{Z}_2$ 上整，すなわち $\alpha\in\mathcal{O}_F$ とする. γ の $\mathbb{Q}_2$ 上共軛を $\overline{\gamma}$ とすれば

$$\mathrm{Tr}_{F/\mathbb{Q}_2}(\gamma)=\gamma+\overline{\gamma}=-(c+2)/4,\quad \mathrm{N}_{F/\mathbb{Q}_2}(\gamma)=\gamma\overline{\gamma}=(c+d+1)/16$$

で $\mathrm{ord}_2(\mathrm{Tr}_{F/\mathbb{Q}_2})=0$，$\mathrm{ord}_2(\mathrm{N}_{F/\mathbb{Q}_2})=0$. また，

$$\begin{aligned}A&:=\mathrm{Tr}_{F/\mathbb{Q}_2}(\alpha)=(a+b\gamma)+(a+b\overline{\gamma})=2a+b\,\mathrm{Tr}_{F/\mathbb{Q}_2}(\gamma),\\ B&:=\mathrm{N}_{F/\mathbb{Q}_2}(\alpha)=(a+b\gamma)(a+b\overline{\gamma})=a^2+ab\,\mathrm{Tr}_{F/\mathbb{Q}_2}(\gamma)+b^2\,\mathrm{N}_{F/\mathbb{Q}_2}(\gamma)\end{aligned}$$

とする. 命題 I-8.1.19 から $A,B\in\mathbb{Z}_2$. $4B=A^2+b^2[4\,\mathrm{N}_{F/\mathbb{Q}_2}(\alpha)-\mathrm{Tr}_{F/\mathbb{Q}_2}(\alpha)^2]\in4\mathbb{Z}_2$ なので $b^2[4\,\mathrm{N}_{F/\mathbb{Q}_2}(\alpha)-\mathrm{Tr}_{F/\mathbb{Q}_2}(\alpha)^2]\in\mathbb{Z}_2$. $\mathrm{ord}_2(4\,\mathrm{N}_{F/\mathbb{Q}_2}(\alpha)-\mathrm{Tr}_{F/\mathbb{Q}_2}(\alpha)^2)=0$ なので $\mathrm{ord}_2(b)\geq0$，つまり $b\in\mathbb{Z}_2$（命題 1.1.3，定理 I-9.1.26(5)）. B の定義式で ord_2 を考えて $a\in\mathbb{Z}_2$. 従って，$\mathcal{O}_F\subset\mathbb{Z}_2[\gamma]$ であり，$\mathcal{O}_F=\mathbb{Z}_2[\gamma]$.

$y^2+(c+2)/4y+(c+d+1)/16$ の判別式は $\equiv1 \bmod 4$. よって命題 1.9.9 から $\Delta_{F/\mathbb{Q}_2}(1,\gamma)$ は 2 で割り切れないので，補題 1.8.3 から $\Delta_{F/\mathbb{Q}_2,2}$ は $2\mathbb{Z}_2$ で割り切れず，$\Delta_{F/\mathbb{Q}_2}$ も $2\mathbb{Z}_2$ で割り切れない. よって，Dedekind の判別定理から $2\mathbb{Z}_2$ は $F/\mathbb{Q}_2$ で不分岐. 定理 I-9.1.26(7) から $2\mathbb{Z}_2$ は $\mathbb{Z}_2$ の唯一の素イデアルなので $F/\mathbb{Q}_2$ は不分岐拡大.

$\Delta_{K/\mathbb{Q},2}=\Delta_{\mathbb{Q}_2/\mathbb{Q}_2}\Delta_{F/\mathbb{Q}_2}$ は 2 で割り切れないので，Δ_K は 2 で割り切れない（命題 1.8.5）. 命題 1.9.9 から系 1.7.5(2) から $\Delta(f)=-5296=(\mathcal{O}_K:\mathbb{Z}[\alpha])^2\Delta_K$ なので $\Delta_K=-331$，$(\mathcal{O}_K:\mathbb{Z}[\alpha])=4$.

■命題 2.3.9 まず，$p\mid a$ もしくは $p\mid b$ について $\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p=V\otimes_{\mathbb{Z}}\mathbb{Z}_p$ を証明し，$(\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p:V\otimes_{\mathbb{Z}}\mathbb{Z}_p)=1$. 次に，$p\nmid3,a,b$ に対しても同じことが証明できる.

- a が 3 の倍数なら素数 p は上のいずれかに属する. よって命題 1.8.9(1)(3) から $(\mathcal{O}_K:V)=1$
- a,b が 3 の倍数でなければ，命題 1.8.9(3) から，$p\neq3$ については，命題 1.8.9(1) の右辺の因子は 1. よって命題 1.8.9(1) から $(\mathcal{O}_K:V)=(\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_3:V\otimes_{\mathbb{Z}}\mathbb{Z}_3)$
  - $a^2b^4\not\equiv1 \bmod 9$ なら $(\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_3:V\otimes_{\mathbb{Z}}\mathbb{Z}_3)=1$ なので $(\mathcal{O}_K:V)=1$
  - $a^2b^4\equiv1 \bmod 9$ なら，命題 1.8.9(2) から $(\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_3:V\otimes_{\mathbb{Z}}\mathbb{Z}_3)$ は 3 の冪. $\Delta_{K/\mathbb{Q},3}=(3)$ なので Δ_K の ord_3 は 1. よって，$(\mathcal{O}_K:V)=3$

a,b を平方因子を持たない互いに素な整数，$\beta_1=\sqrt[3]{ab^2}$，$\beta_2=\sqrt[3]{a^2b}$，$K=\mathbb{Q}(\beta_1)$，$V=\mathbb{Z}+\mathbb{Z}\beta_1+\mathbb{Z}\beta_2$ として素数 p が a を割り切れば，p は $K/\mathbb{Q}$ で完全分岐で $\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p=V\otimes_{\mathbb{Z}}\mathbb{Z}_p$

証明 x^3-ab^2 は Eisenstein 多項式なので $\mathbb{Q}$ 上既約であり，β_1 の $\mathbb{Q}$ 上最小多項式となる．これは $\mathbb{Q}_p$ 上でも Eisenstein 多項式なので既約であり，$[\mathbb{Q}_p(\beta_1):\mathbb{Q}_p]=3$．$p$ の上にある $\mathcal{O}_K$ の素イデアルによる K の完備化を $\widehat{K}_1,\dots,\widehat{K}_g$ とする．$\beta_1\in K\subset\widehat{K}_i$ なので $\mathbb{Q}_p(\beta_1)\subset\widehat{K}_i$ となり $[\widehat{K}_i:\mathbb{Q}_p(\beta_1)]\geq 1$．よって $[\widehat{K}_i:\mathbb{Q}_p]\geq 3$．定理 1.3.23(4)(5) から $[\widehat{K}_1:\mathbb{Q}_p]+\cdots+[\widehat{K}_g:\mathbb{Q}_p]=3$ なので $g=1$．すなわち，$p\mathbb{Z}$ の上にある $\mathcal{O}_K$ の素イデアルは 1 つ．$\widehat{K}_1$ を $\widehat{K}$ と書けば，$[\widehat{K}:\mathbb{Q}_p]=3$ で $[\widehat{K}:\mathbb{Q}_p(\beta_1)]=1$．従って，$\widehat{K}=\mathbb{Q}_p(\beta_1)$．$\widehat{K}$ の整数環を $\widehat{\mathcal{O}_K}$ とする．$\widehat{\mathcal{O}_K}$ の極大イデアルを P とすると命題 1.10.7 から $\widehat{K}/\mathbb{Q}_p$ は完全分岐で分岐指数は $e(P/p\mathbb{Z}_p)=3$．

よって $\mathrm{ord}_p(a)=1$，$\mathrm{ord}_p(b)=0$ に注意して

$$3\,\mathrm{ord}_P(\beta_1)=\mathrm{ord}_P({\beta_1}^3)=\mathrm{ord}_P(ab^2)=3\,\mathrm{ord}_p(ab^2)=3.$$

よって $\mathrm{ord}_P(\beta_1)=1$ となり β_1 は $\widehat{\mathcal{O}_K}$ の素元．再び命題 1.10.7 から $\widehat{\mathcal{O}_K}=\mathbb{Z}_p[\beta_1]$．定理 1.3.23(6) から $p\mathbb{Z}$ の分岐指数は 3 なので，$K/\mathbb{Q}$ で完全分岐．

$V\subset\mathcal{O}_K$ なので，$V\otimes_{\mathbb{Z}}\mathbb{Z}_p\subset\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p$．$b\in\mathbb{Z}_p^{\times}$，$\beta_2={\beta_1}^2/b$ に注意して，テンソル積の普遍性から加群準同型 $\phi\colon V\otimes_{\mathbb{Z}}\mathbb{Z}_p\to\mathbb{Z}_p[\beta_1]$ を得る（$\sigma\colon\mathcal{O}_K\hookrightarrow\widehat{\mathcal{O}_K}$）．

$$\begin{array}{ccc} V\times\mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p[\beta_1] \\ \downarrow & \nearrow_{\phi} & \\ V\otimes_{\mathbb{Z}}\mathbb{Z}_p & & \end{array} \qquad \begin{array}{ccc} (v,c) & \longmapsto & \sigma(v)c \\ \downarrow & \nearrow & \\ v\otimes c & & \end{array}$$

ϕ が $\mathbb{Z}_p$ 代数の同型であることは容易に分かる．定理 1.3.23(2) から同型

$$\mathcal{O}_k\otimes_{\mathbb{Z}}\mathbb{Z}_p\ni v\otimes c\mapsto\sigma(v)c\in\widehat{\mathcal{O}_K}=\mathbb{Z}_p[\beta_1]$$

の存在が分かるので，$\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p=V\otimes_{\mathbb{Z}}\mathbb{Z}_p$． □

a,b を平方因子を持たない互いに素な整数，$\beta_1=\sqrt[3]{ab^2}$，$\beta_2=\sqrt[3]{a^2b}$，$K=\mathbb{Q}(\beta_1)$，$V=\mathbb{Z}+\mathbb{Z}\beta_1+\mathbb{Z}\beta_2$，$p\nmid 3,a,b$ なら p は K で不分岐で $\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p=V\otimes_{\mathbb{Z}}\mathbb{Z}_p$

証明 命題 2.2.11 から $\mathbb{Z}_{(p)}[\beta_1]=\mathcal{O}_{K_{(p)}}\simeq\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_{(p)}$．よって，

$$\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p\simeq\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_{(p)}\otimes_{\mathbb{Z}_{(p)}}\mathbb{Z}_p\simeq\mathbb{Z}_{(p)}[\beta_1]\otimes_{\mathbb{Z}_{(p)}}\mathbb{Z}_p\simeq\mathbb{Z}_p[\beta_1].$$

これは $v\otimes c\mapsto\sigma(v)c$ で与えられるので，先程と同様に $\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p=V\otimes_{\mathbb{Z}}\mathbb{Z}_p$． □

${\alpha_1}^2\equiv 1 \bmod 9$ の場合．λ の行き先

証明 $f(x)=(x-\gamma)(x+\gamma x+\gamma^2)$ である．例 2.3.5 と同様にすれば，次の写像が得られる．

$$\begin{array}{ccccc} K & \hookrightarrow & K\otimes_{\mathbb{Q}}\mathbb{Q}_3 & \xrightarrow{\simeq} & \mathbb{Q}_3\times\mathbb{Q}_3(\omega\gamma) \\ \cup & & \cup & & \cup \\ a_0+a_1\beta_1+a_2{\beta_1}^2 & \longmapsto & (a_0+a_1\beta_1+a_2{\beta_1}^2)\otimes 1 & \longmapsto & (a_0+a_1\gamma+a_2\gamma^2,a_0+a_1\omega\gamma+a_2\omega^2\gamma^2) \end{array}$$

これを整数環に制限すれば，$\phi\colon\mathcal{O}_K\hookrightarrow\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_3\simeq\mathbb{Z}_3\times\mathbb{Z}_3[\omega\gamma]$ である． □

2.4 $\mathbb{Q}_p$ の 2 次拡大

■命題 2.4.2

$K = \mathbb{Q}_2(\sqrt{3})$，$\alpha = \sqrt{3} - 1$ として，$\mathcal{O}_K = \mathbb{Z}_2[\alpha]$

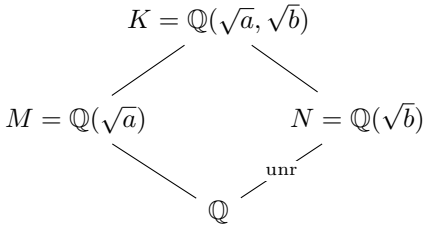
証明 $\mathcal{O}_K$ の素イデアルを P とする．α の $\mathbb{Q}_2$ 上最小多項式は Eisenstein 多項式なので，α が $\mathcal{O}_K$ の素元であることを証明すれば良い（命題 1.10.7）．$K/\mathbb{Q}_2$ は完全分岐で $e(P/2\mathbb{Z}_2) = 2$（命題 1.10.7）なので $\mathrm{ord}_P(2) = 2\,\mathrm{ord}_2(2) = 2$. $\mathrm{ord}_P(\alpha) = 0$ とする．命題 1.1.3 から $\mathrm{ord}_P(\alpha+2) = 0$ なので $\mathrm{ord}_P(\alpha(\alpha+2)) = 0$. しかし，$\alpha(\alpha+2) = 2$ なので，$\mathrm{ord}_P(\alpha(\alpha+2)) = 2$．よって矛盾．$\mathrm{ord}_P(\alpha) \geq 2$ とする．$\mathrm{ord}_P(\alpha+2) \geq 2$ なので $\mathrm{ord}_P(\alpha(\alpha+2)) \geq 4$．先程と同様に矛盾．よって，$\mathrm{ord}_P(\alpha) = 1$ となり示された． □

2.5 $\mathbb{Q}$ の双 2 次拡大

■命題 2.5.2

$K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ を双 2 次拡大，$M = \mathbb{Q}(\sqrt{a})$，$N = \mathbb{Q}(\sqrt{b})$，p が $N/\mathbb{Q}$ で不分岐とする．$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ は $\mathbb{Z}_p$ 上 $Q(\sqrt{a}), Q(\sqrt{b})$ の整数環で生成され，$\Delta_{K/\mathbb{Q},p} = {\Delta_{\mathbb{Q}(\sqrt{a})/\mathbb{Q},p}}^2 {\Delta_{\mathbb{Q}(\sqrt{b})/\mathbb{Q},p}}^2$

証明 $S = \mathbb{Z} \setminus p\mathbb{Z} \subset \mathbb{Z}_p^\times$ とする．命題 1.3.7 から p は $S^{-1}\mathcal{O}_N/S^{-1}\mathbb{Z}$ でも不分岐．



$\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z}$ に対して命題 1.11.14 の適用を考えよう．命題 1.11.14(2) から $S^{-1}\mathcal{O}_K$ は $S^{-1}\mathcal{O}_N, S^{-1}\mathcal{O}_M$ で生成される．定理 1.11.16(2) の証明と同様に，$S^{-1}\mathcal{O}_N$ の $S^{-1}\mathbb{Z}$ 基底を $\{v_1, v_2\}$，$S^{-1}\mathcal{O}_M$ の $S^{-1}\mathbb{Z}$ 基底を $\{w_1, w_2\}$ とすれば，$S^{-1}\mathcal{O}_K$ の $S^{-1}\mathbb{Z}$ 基底は $\{v_1w_1, \ldots, v_2w_2\}$．同定理 (4) の証明と同様に $\Delta_{K/\mathbb{Q},p} = {\Delta_{N/\mathbb{Q},p}}^2 {\Delta_{M/\mathbb{Q},p}}^2$ となる．

$\forall x \in S^{-1}\mathcal{O}_K$ に対し，$x_{ij} \in S^{-1}\mathbb{Z}$ が存在し，$x = \sum_{ij} x_{ij} v_i w_j$ と表すことができる．$y \in \mathbb{Z}_p$ として，

$$S^{-1}\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \ni x \otimes y = \sum_{ij} (x_{ij} \otimes y)(v_i w_j \otimes 1)$$

と表すことができる．$x = a/s$ $(a \in \mathcal{O}_K, s \in S)$, $v_i = \tilde{v}_i/s_i$ $(\tilde{v}_i \in \mathcal{O}_M, s_i \in S)$, $w_j = \tilde{w}_j/t_j$ $(\tilde{w}_j \in \mathcal{O}_N, t_j \in S)$ として，

$$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \ni a \otimes y/s = \sum_{ij} (1 \otimes x_{ij}y)(\tilde{v}_i\tilde{w}_j \otimes 1/s_it_j)$$

となる．これは，$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ の $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ 基底である．同様に，$\mathcal{O}_M \otimes_{\mathbb{Z}} \mathbb{Z}_p$ の $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ 基底として $\{\tilde{v}_i \otimes 1/s_i\}$，$\mathcal{O}_N \otimes_{\mathbb{Z}} \mathbb{Z}_p$ の $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ 基底として $\{\tilde{w}_j \otimes 1/t_j\}$ が取れる．

$\Delta_{M/\mathbb{Q}}(1, \sqrt{a}) = 4a$ なので，$\{1, \sqrt{a}\}$ は $S^{-1}\mathcal{O}_M$ の $S^{-1}\mathbb{Z}$ 基底（補題 1.8.3）．$S^{-1}\mathcal{O}_N$ の $S^{-1}\mathbb{Z}$ 基底は $\{1, \sqrt{b}\}$ となる．この場合は，上での s_i, t_j は 1 として良い．

命題 2.5.4(1) なら $\{1, (1+\sqrt{a})/2\}$ が $S^{-1}\mathcal{O}_M$ の $S^{-1}\mathbb{Z}$ 基底になる． □

2.6 4 次巡回体

■命題 2.6.4 $\{1, \alpha, \sqrt{d}, \beta\}$ で生成される $\mathbb{Z}$ 加群を V とする．$\Delta_{K/\mathbb{Q}}(1, \alpha, \sqrt{d}, \beta) = (\mathcal{O}_K : V)^2 \Delta_K = 2^8 d^3$ が成立する（系 1.7.5(2)）．$\forall p \mid d$ に対し，$\Delta K/\mathbb{Q}, p = (p^3)$ なので $p^3 \mid \Delta_K$．よって $(\mathcal{O}_K : V)^2$ は 2 の冪乗．命題 1.8.9 から $(\mathcal{O}_K : V) = \prod_p (\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p : V \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ となるが，これが 2 の冪乗なので奇素数 p に対しては $(\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p : V \otimes_{\mathbb{Z}} \mathbb{Z}_p) = 1$.

第 3 章

Minkowski の定理とその応用

3.2 判別式の評価と類数の有限性

■例 3.2.13 素数 p が $p\mathcal{O}_K = P_1 \cdots P_g$ と素イデアル分解できたとする．命題 1.10.15 から $\mathcal{N}((p)) = \mathcal{N}(P_1 \cdots P_g) = \mathcal{N}(P_1) \cdots \mathcal{N}(P_g)$．命題 1.10.17(2) から $\mathcal{N}((p)) = \mathrm{N}_{K/\mathbb{Q}}(p) = p^4$ なので，$\mathcal{N}(P_i)$ は p の冪乗．$\mathcal{O}_K$ の素イデアル P の下にある素数 p は一意的に定まるので，今の議論から，$\mathcal{N}(P)$ は素数 p の冪乗であり，p の上にある．よって，$\mathcal{O}_K$ の素イデアル P が $\mathcal{N}(P) = 2$ を満たすならば $2\mathbb{Z}$ の上にある．

■例 3.2.14 素数 p について，命題 1.10.17(2) から $\mathcal{N}((p)) = |\mathrm{N}_{K/\mathbb{Q}}(p)| = p^2$．$(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_\mathfrak{t}$ と素イデアル分解されるとする．命題 1.10.15 から $\mathcal{N}((p)) = \mathcal{N}(\mathfrak{p}_1) \cdots \mathcal{N}(\mathfrak{p}_t)$．よって，$t = 2$ で $\mathcal{N}(\mathfrak{p}_1) = \mathcal{N}(\mathfrak{p}_2) = p$. よって，ノルム 2 の素イデアルは (2) の素イデアル分解に現れる物だけ．

$\mathcal{O}_K = \mathbb{Z}[\alpha]$ のイデアル (2) を素イデアル分解する．準同型

$$\mathcal{O}_K \ni a + b\alpha \mapsto \overline{a} + \overline{b}\alpha + (2) \in \mathcal{O}_K/(2)$$

は全射．$\overline{a}, \overline{b}$ を a, b を 2 で割った余りとする．準同型

$$\begin{aligned}\mathcal{O}_K/(2) \ni \overline{a} + \overline{b}\alpha + (2) &\mapsto \overline{a} + \overline{b}x + (x(x+1)) \in \mathbb{F}_2[x]/(x(x+1)) \\ &\mapsto (\overline{a} + \overline{b}x + (x), \overline{a} + \overline{b}x + (x+1)) \in \mathbb{F}_2[x]/(x) \times \mathbb{F}_2[x]/(x+1) \\ &\mapsto (\overline{a}, \overline{a} - \overline{b}) \in \mathbb{F}_2 \times \mathbb{F}_2\end{aligned}$$

は同型．従って，$(2) = \mathfrak{p}_1\mathfrak{p}_2$ となる．特に，$\mathfrak{p}_1, \mathfrak{p}_2$ は 2 の上にある．中国式剰余定理から，

$$\mathcal{O}_K/(2) \ni \overline{a} + \overline{b}\alpha + (2) \mapsto (\overline{a} + \overline{b}\alpha + \mathfrak{p}_1, \overline{a} + \overline{b}\alpha + \mathfrak{p}_2) \in \mathcal{O}_K/\mathfrak{p}_1 \times \mathcal{O}_K/\mathfrak{p}_2$$

は同型．以上をまとめて，

$$\begin{array}{ccccccc}\mathcal{O}_K & \twoheadrightarrow & \mathcal{O}_K/\mathfrak{p}_1 \times \mathcal{O}_K/\mathfrak{p}_2 & = & \mathcal{O}_K/\mathfrak{p}_1 \times \mathcal{O}_K/\mathfrak{p}_2 & \xrightarrow{\simeq} & \mathbb{F}_2 \times \mathbb{F}_2 \\ \cup & & \cup & & \cup & & \cup \\ a + b\alpha & \longmapsto & (a + b\alpha + \mathfrak{p}_1, a + b\alpha + \mathfrak{p}_2) & = & (\overline{a} + \overline{b}\alpha + \mathfrak{p}_1, \overline{a} + \overline{b}\alpha + \mathfrak{p}_2) & \longmapsto & (\overline{a}, \overline{a} - \overline{b})\end{array}$$

となる．最後の同型を $\phi\colon \mathcal{O}_K/\mathfrak{p}_1 \times \mathcal{O}_K/\mathfrak{p}_2 \to \mathbb{F}_2 \times \mathbb{F}_2$ とする．ϕ が同型なことに注意して，

$$a + b\alpha \in \mathfrak{p}_1 \Leftrightarrow (0, \bullet) \in \mathcal{O}_K/\mathfrak{p}_1 \times \mathcal{O}_K/\mathfrak{p}_2 \Leftrightarrow (0, \bullet) \in \mathbb{F}_2 \times \mathbb{F}_2 \Leftrightarrow \overline{a} = 0 \Leftrightarrow a + b\alpha \in (2, \alpha)$$

なので $\mathfrak{p}_1 = (2, \alpha)$. 同様に,

$$a + b\alpha \in \mathfrak{p}_2 \Leftrightarrow (\bullet, 0) \in \mathcal{O}_K/\mathfrak{p}_1 \times \mathcal{O}_K/\mathfrak{p}_2 \Leftrightarrow (\bullet, 0) \in \mathbb{F}_2 \times \mathbb{F}_2 \Leftrightarrow \overline{a} - \overline{b} = 0 \Leftrightarrow a + b\alpha \in (2, 1 + \alpha)$$

なので $\mathfrak{p}_2 = (2, 1 + \alpha)$.

■例 3.2.22 $f(\mathfrak{p}_2/p\mathbb{Z}) = 1$ なので, $[\mathcal{O}_K/\mathfrak{p}_2 : \mathbb{F}_p] = 1$. つまり, $\mathcal{O}_K/\mathfrak{p}_2$ の完全代表系として $\{0, \dots, p-1\}$ が取れる. $\alpha \equiv k \bmod \mathfrak{p}_2$ ($k \in \{0, \dots, p-1\}$) とする. α が $\mathfrak{p}_2$ を法として平方非剰余なので $\alpha \not\equiv l^2 \bmod \mathfrak{p}_2$ ($\forall l \in \{0, \dots, p-1\}$). よって $k - l^2 \notin \mathfrak{p}_2$. $\mathfrak{p}_2$ は $p\mathbb{Z}$ の上にあり, $k, l \in \mathbb{Z}$ なので $k - l^2 \notin p\mathbb{Z}$. つまり p を法として k は平方非剰余. $-\alpha$ が $\mathfrak{p}_2$ を法として平方非剰余なので, 同様にして, p を法として $-k$ は平方非剰余. 系 I-1.11.5 から -1 は p を法として -1 は平方剰余.

離散部分群

Dirichlet の単数定理の証明に使う.[*1]

追加定義 3.2.1. $m \in \mathbb{Z}_{>0}$ とする. $\mathbb{R}^m$ の部分集合 S が離散的とは, 任意の $C \in \mathbb{R}_{>0}$ に対し

$$\#\left\{ (x_1, \dots, x_m) \in S \mid \max_{1 \le j \le m} |x_j| \le C \right\} < \infty$$

が成立することである. 定義から明らかに, 離散的集合の有界部分集合は有限集合となる.

追加補題 3.2.2. $\mathbb{R}$ の任意の離散的部分群 Γ は $\exists \gamma \in \Gamma$ によって $\Gamma = \mathbb{Z}\gamma$ となる.

証明 $\Gamma = \{\mathbf{0}\}$ なら $\gamma = \not\vdash$ とすればよい. $\Gamma \neq \{\mathbf{0}\}$ とする. $|\gamma_1| > 0$ となる $\gamma_1 \in \Gamma$ を取る. Γ は離散的なので, $|x| \le C$ となる $x \in \Gamma$ は有限個しかない. $\gamma = \min\{\, |x| \mid x \in \Gamma, \quad 0 < |x| \le C \,\}$ とおく. $\mathbb{Z}\gamma$ が Γ の部分群であることは明らかなので $\mathbb{Z}\gamma \subset \Gamma$.

$\forall x \in \Gamma$ に対し, $q_0 = \min\{\, q \in \mathbb{Z} \mid q > 0, \quad |x| \le q|\gamma| \}$ が存在する. $0 \le q_0|\gamma| - |x| < |\gamma|$ は明らか. $x, \gamma \in \Gamma$ で $-x, -\gamma \in \Gamma$ なので $|x|, |\gamma| \in \Gamma$. よって $q_0|\gamma| - |x| \in \Gamma$. γ の最小性から, $q_0|\gamma| - |x| = 0$. よって, $|x| \in \mathbb{Z}\gamma$ なので $x = \pm|x| \in \mathbb{Z}\gamma$ となり $\Gamma \subset \mathbb{Z}\gamma$. 以上から $\Gamma = \mathbb{Z}\gamma$. □

追加補題 3.2.3. $\Gamma \neq \{\mathbf{0}\}$ を $\mathbb{R}^m$ の離散的部分群とすれば, $\exists \gamma \in \Gamma \setminus \{\mathbf{0}\}$ によって $\mathbb{R}\gamma \cap \Gamma = \mathbb{Z}\gamma$ となる.

証明 $\gamma_0 \in \Gamma \setminus \{\mathbf{0}\}$ として, $M = \{u\gamma_0 \in \mathbb{R}^m \mid 0 < u \le 1\}$ とおくと, M は有界集合. $\gamma_0 \in \Gamma \cap M$ なので, $\Gamma \cap M \neq \varnothing$. よって, $\{\, u \in \mathbb{R} \mid u\gamma_0 \in \Gamma, \quad 0 < u \le 1 \,\}$ も空でない有限集合となり, 最小元 u_0 が存在する. $\gamma = u_0\gamma_0$ とおく.

$\alpha \in \Gamma \cap \mathbb{R}\gamma$ とおくと, $\alpha = u\gamma$ ($u \in \mathbb{R}$) と表される. $\alpha - \lfloor u \rfloor \gamma \in \Gamma$ は $(u - \lfloor u \rfloor)u_0\gamma_0$ となるが, $0 \le u - \lfloor u \rfloor < 1$ なので $0 \le (u - \lfloor u \rfloor)u_0\gamma_0 < u_0$. u_0 の最小性から, $u - \lfloor u \rfloor = 0$ なので, $\alpha = \lfloor u \rfloor \gamma \in \mathbb{Z}\gamma$ となり, $\Gamma \cap \mathbb{R}\gamma \subset \mathbb{Z}\gamma$. $\Gamma \cap \mathbb{R}\gamma \supset \mathbb{Z}\gamma$ は明らかなので, $\Gamma \cap \mathbb{R}\gamma = \mathbb{Z}\gamma$. □

[*1] https://mathematics-pdf.com/pdf/dirichlet_unit_theorem.pdf から必要な部分を取ってきた

Γ を $\mathbb{R}^m$ の離散的部分群で $\gamma \in \Gamma \setminus \{\mathbf{0}\}$ とする．$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{R}^m$ を，$\{\gamma, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_m\}$ が $\mathbb{R}^m$ の $\mathbb{R}$ 基底になるように取る．$m \geq 2$ に対し，$\mathbb{R}$ 線形写像 L_γ を

$$L_\gamma \colon \mathbb{R}^m \ni x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m \mapsto (x_2, \ldots, x_m) \in \mathbb{R}^{m-1}$$

とおく．

追加補題 3.2.4. $\gamma \in \Gamma \setminus \{\mathbf{0}\}$ に対し，$\ker L_\gamma = \mathbb{R}\gamma$.

証明 $\alpha \in \ker L_\gamma$ とし，$x_1, \ldots, x_m \in \mathbb{R}$ によって $\alpha = x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m$ とすれば，$(x_2, \ldots, x_m) = \mathbf{0}$. つまり，$\alpha = x_1\gamma \in \mathbb{R}\gamma$ なので，$\ker L_\gamma \subset \mathbb{R}\gamma$．$\ker L_\gamma \supset \mathbb{R}\gamma$ は明らかなので，$\ker L_\gamma = \mathbb{R}\gamma$. □

追加補題 3.2.5. $\forall \gamma \in \Gamma \setminus \{\mathbf{0}\}$ に対し，$\Gamma' = L_\gamma(\Gamma)$ は $\mathbb{R}^{m-1}$ の離散的部分群.

証明 L_γ は線形写像なので，$\mathbb{R}^m$ から $\mathbb{R}^{m-1}$ への（加群の）準同型．よって Γ' は $\mathbb{R}^{m-1}$ の部分群．$C \in \mathbb{R}_{>0}$ とする．$(x_2, \ldots, x_m) \in \Gamma'$ とし，

$$\max_{2 \leq j \leq m} |x_j| \leq C \tag{3.2.6}$$

であるとする．$\Gamma' = L_\gamma(\Gamma)$ なので，$\exists x_1 \in \mathbb{R}$ によって $x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m \in \Gamma$ となる．$\gamma \in \Gamma$ なので

$$(x_1 - \lfloor x_1 \rfloor)\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m = (x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m) - \lfloor x_1 \rfloor\gamma \in \Gamma.$$

$0 \leq x_1 - \lfloor x_1 \rfloor < 1$ で，$(x_1 - \lfloor x_1 \rfloor)\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m$ の L_γ による像は $(x_2, \ldots, x_m)$．よって，[3.2.6] を満たす $(x_2, \ldots, x_m)$ の個数は，

$$x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m \ (0 \leq x_1 < 1) \tag{3.2.7}$$

となる Γ の元の個数以下.

一方，$\gamma, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_m \in \mathbb{R}^m$ の各成分の絶対値の最大値を C' とすれば，[3.2.7] の形の元を $(y_1, \ldots, y_m)$ で表すとき，$|y_j|$ $(1 \leq j \leq m)$ の最大値は $C' + (m-1)CC'$ 以下．Γ は離散的なので，[3.2.7] の形の元は有限個しかない．したがって，[3.2.6] を満たす $(x_2, \ldots, x_m) \in \Gamma'$ も有限個，つまり Γ' は離散的. □

追加定理 3.2.8. $\mathbb{R}^m$ の任意の離散的部分群 Γ に対し，$\Gamma \simeq \mathbb{Z}^{\oplus s}$ $(s \leq m)$.

証明 $\Gamma = \{\mathbf{0}\}$ なら明らかなので，$\Gamma \neq \{\mathbf{0}\}$ の場合について，Γ の $\mathbb{Z}$ 基底 $\{\gamma_1, \ldots, \gamma_s\}$ の存在を m に関する数学的帰納法によって証明する.

$m = 1$ の時は追加補題 3.2.2 から従う.

$m \geq 2$ とし，$\mathbb{R}^{m-1}$ の任意の離散的部分群に対し，定理の主張が成立すると仮定する．追加補題 3.2.3 から，$\mathbb{R}\gamma_1 \cap \Gamma = \mathbb{Z}\gamma_1$ を満たす $\gamma_1 \in \Gamma \setminus \{\mathbf{0}\}$ が存在する．$L = L_{\gamma_1}$，$\Gamma' = L(\Gamma)$ とおく．追加補題 3.2.5 から，Γ' は $\mathbb{R}^{m-1}$ の離散的部分群．よって，仮定から，Γ' の $\mathbb{Z}$ 基底 $\{\gamma'_2, \ldots, \gamma'_s\}$ $(s \leq m)$ が存在する．$\Gamma' = L(\Gamma)$ なので $L(\gamma_j) = \gamma'_j$ となる $\gamma_1, \ldots, \gamma_s \in \Gamma$ が存在する．$n_1, \ldots, n_s \in \mathbb{Z}$ とし，$n_1\gamma_1 + \cdots + n_s\gamma_s = \mathbf{0}$ と仮定する．この時，$n_2\gamma'_2 + \cdots + n_s\gamma'_s = L(n_1\gamma_1 + \cdots + n_s\gamma_s) = \mathbf{0}$. $\{\gamma'_2, \ldots, \gamma'_s\}$ は Γ' の $\mathbb{Z}$ 基底なので，$n_2 = \cdots = n_s = 0$. さらに，$\gamma_1 \neq \mathbf{0}$ なので，$n_1 = 0$. よって，$\{\gamma_1, \ldots, \gamma_s\}$ は $\mathbb{Z}$ 上一次独立.

$\alpha \in \Gamma$ とすると，$L(\alpha) \in \Gamma'$ なので $\exists n_2, \ldots, n_s \in \mathbb{Z}$ によって $L = n_2\gamma_2' + \cdots + n_s\gamma_s' = L(n_2\gamma_2 + \cdots + n_s\gamma_s)$. よって，$L(\alpha - (n_2\gamma_2 + \cdots + n_s\gamma_s)) = \mathbf{0}$，つまり $\alpha - (n_2\gamma_2 + \cdots + n_s\gamma_s) \in \ker L \cap \Gamma$. 追加補題 3.2.4 から，$\ker L = \mathbb{R}\gamma_1$ なので，$\ker L \cap \Gamma = \mathbb{R}\gamma_1 \cap \Gamma = \mathbb{Z}\gamma_1$（追加補題 3.2.4）. よって，$\exists n_1 \in \mathbb{Z}$ によって $\alpha - (n_2\gamma_2 + \cdots + n_s\gamma_s) = n_1\gamma_1$，つまり $\alpha = n_1\gamma_1 + \cdots + n_s\gamma_s$. よって，$\{\gamma_1, \ldots, \gamma_s\}$ は Γ の $\mathbb{Z}$ 基底. □

追加補題 3.2.9. $\forall i = 1, \ldots, n$ に対し $|\sigma_i(\alpha)| < C$ となるような $\alpha \in \mathcal{O}_K$ は有限個しかない

証明 $\{w_1, \ldots, w_n\}$ を $\mathcal{O}_K$ の整基底とする. $\forall \alpha \in \mathcal{O}_K$ は $x_1, \ldots, x_n \in \mathbb{Z}$ によって $\alpha = x_1w_1 + \cdots + x_nw_n$ と表すことができる.

$$P = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_1(w_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(w_1) & \cdots & \sigma_n(w_n) \end{pmatrix}, \quad \boldsymbol{\alpha} = \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_1(\alpha) \end{pmatrix}, \quad \boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

とすれば，$\boldsymbol{\alpha} = P\boldsymbol{x}$. P は正則なので，$\boldsymbol{x} = P^{-1}\boldsymbol{\alpha}$. $P^{-1} = (p_{ij})$ とおき，C_1 を p_{ij} のうち最大のものとする. $i = 1, \ldots, n$ に対して

$$|x_i| = |p_{i1}\sigma_1(\alpha) + \cdots + p_{in}\sigma_n(\alpha)| \leq |p_{i1}||\sigma_1(\alpha)| + \cdots + |p_{in}||\sigma_n(\alpha)| \leq nc_1C$$

なので，このような x_i は有限個しか存在しない. □

3.3 Dirichlet の単数定理

■定理 3.3.1 ϕ の構成. $\phi\colon \mathcal{O}_K^\times \to H$ は積を和にする：$\phi(\varepsilon_1\varepsilon_2) = \phi(\varepsilon_1) + \phi(\varepsilon_2)$. $\mathcal{O}_K^\times$ は乗法群で H は $\mathbb{R}$ 加群.

p.163 の真ん中らへんの段落から. $r = r_1 + r_2 - 1 \leq 1$ とする. $\phi(\varepsilon_1), \ldots, \phi(\varepsilon_r)$ が一次独立な条件の元で $\phi(\mathcal{O}_K^\times)$ が $\mathbb{R}^r$ の離散的部分群であることを証明する. $\phi(\mathcal{O}_K^\times)$ が $\mathbb{R}^r$ の部分加群なのは明らか. $C \in \mathbb{R}_{>0}$ を考える. $\varepsilon \in \mathcal{O}_K$ を $|\log \sigma_i(\varepsilon)|$ $(1 \leq j \leq r)$ の最大値が C 以下になるように取る. この条件は $i = 1, \ldots, r$ に対し $e^{-C} \leq |\sigma_i(\varepsilon) \leq e^C$ が成立することと同値. $r_2 > 0$ の時，$j = 1, \ldots, r_2$ に対し $|\sigma_{r_1+r_2+j}(\varepsilon)| = |\sigma_{r_1+j}(\varepsilon)|$ なので，$i \neq r_1 + r_2, n$ に対し $e^{-C} \leq |\sigma_i(\varepsilon) \leq e^C$ が成立する. $1 = \left|\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)\right| = \prod_{i=1}^n |\sigma_i(\varepsilon)|$ なので，

$$|\sigma_{r_1+r_2}(\varepsilon)||\sigma_n(\varepsilon)| = \prod_{\substack{1 \leq j \leq n \\ i \neq r_1+r_2, n}} \frac{1}{|\sigma_i(\varepsilon)|} < e^{(n-2)C}.$$

よって，$|\sigma_{r_1+r_2}(\varepsilon)| = |\sigma_n(\varepsilon)| < e^{(n-2)C/2}$. したがって，$r_2 > 0$ なら $i = 1, \ldots, r$ に対して $|\sigma_i(\varepsilon)| < e^C$ が成立.

$r_2 = 0$ なら $r = r_1 - 1 = n - 1$ なので $i = 1, \ldots, n-1$ に対して $e^{-C} \leq |\sigma_i(\varepsilon) \leq e^C$. $1 = \left|\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)\right| = \prod_{i=1}^n |\sigma_i(\varepsilon)|$ なので，

$$|\sigma_n(\varepsilon)| = \prod_{i=1}^{n-1} \frac{1}{|\sigma_i(\varepsilon)|} < e^{(n-1)C}.$$

よって $r_2 = 0$ でも $i = 1, \ldots, r$ に対して $|\sigma_i(\varepsilon)| < e^C$ が成立.

$\forall i = 1, \ldots, n$ に対し $|\sigma_i(\alpha)| < e^C$ を満たす $\mathcal{O}_K$ の元は有限個しかない（追加補題 3.2.9）．よって，$\phi(\mathcal{O}_K^\times)$ は離散的．よって，離散部分群の追加定理 3.2.8 から，$\phi(\mathcal{O}_K^\times) \simeq \mathbb{Z}^{\oplus s}$ $(s \leq r)$．また，$\{\phi(\varepsilon_1), \ldots, \phi(\varepsilon_r)\}$ は $\mathbb{R}$ 上一次独立なので，$\mathbb{Z}$ 上一次独立．よって，$s = r$ となり，$\phi(\mathcal{O}_K^\times) \simeq \mathbb{Z}^{\oplus r}$．

また，K に含まれる 1 の冪根を R_K とすれば，$\ker \phi = R_K$ なので，$\mathcal{O}_K^\times = \mathbb{Z}^{\oplus r} \oplus R_K$．つまり，$\mathcal{O}_K^\times$ の元は 1 の冪根と基本単数 $\varepsilon_1, \ldots, \varepsilon_r$ の冪乗の積の形になる．

第 4 章

円分体

4.1 円分体の整数環 II

追加補題 4.1.1. 判別式について

証明 $f(x)$ の根を $\alpha_1, \ldots, \alpha_n$ とする．$f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ となる．

$$f'(\alpha_i) = (\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)$$

なので，

$$\Delta(f) = \prod_{i<j}(\alpha_i-\alpha_j)^2 = \prod_{i\neq j}(-1)^{n(n-1)/2}(\alpha_i-\alpha_j) = \prod_{i=1}^{n} f'(\alpha_i).$$

□

■命題 4.1.1

$f_k(x)$ の判別式は 単数 $\times \prod({\zeta_{p^k}}^{i-j}-1)$（ただし，$0<i\neq j<p^k$, $p\nmid i,j$）

証明

$$S = \left\{\, i \;\middle|\; 0<i<p^k, \gcd(i,p)=1 \,\right\} = \left\{\, i+jp \;\middle|\; 1\le i\le p-1; 0\le j\le p^{k-1}-1 \,\right\}$$

とおく．$\#S = (p-1)p^{k-1}$．$f_k(x)$ の判別式は

$$\begin{aligned}\prod_{i<j\in S}\left({\zeta_{p^k}}^{i}-{\zeta_{p^k}}^{j}\right)^2 &= (-1)^{\#S(\#S-1)/2}\prod_{i\neq j\in S}{\zeta_{p^k}}^{j}\left({\zeta_{p^k}}^{i-j}-1\right)\\ &= (-1)^{\#S(\#S-1)/2}\prod_{i\neq j\in S}{\zeta_{p^k}}^{j}\prod_{i\neq j\in S}\left({\zeta_{p^k}}^{i-j}-1\right).\end{aligned}$$

まず，1 つ目の積から考える．${\zeta_{p^k}}^{j}$ $(j\in S)$ は $f_k(x)$ の異なる根なので，これらの積は $f_k(x)$ の定数項と（符号を除いて）等しい．よって，

$$\zeta := \prod_{j\in S}{\zeta_{p^k}}^{j} = (-1)^{\#S}.$$

また，$\prod_{i\neq j\in S}{\zeta_{p^k}}^j$ を計算する際は，$i,j\in S$ の条件で積を求めてから，$i=j\in S$ の項で割れば良い：

$$\prod_{i\neq j\in S}{\zeta_{p^k}}^j=\left(\prod_{i=j\in S}{\zeta_{p^k}}^j\right)^{-1}\prod_{i,j\in S}{\zeta_{p^k}}^j=\zeta^{-1}\prod_{i\in S}\prod_{j\in S}{\zeta_{p^k}}^j=\zeta^{-1}\prod_{i\in S}\zeta=\zeta^{\#S-1}=(-1)^{\#S(\#S-1)}=1.$$

よって，

$$\Delta(f_k)=(-1)^{\#S(\#S-1)/2}\prod_{i\neq j\in S}\left({\zeta_{p^k}}^{i-j}-1\right).$$

□

f_k の判別式は p の冪

証明

$$f_k(x)=x^{(p-1)p^{k-1}}+x^{(p-2)p^{k-1}}+\cdots+x^{p^{k-1}}+1=\frac{x^{p^k}-1}{x^{p^{k-1}}-1}$$

なので，

$$t_i:=f_k'({\zeta_{p^k}}^i)=p^k\frac{{\zeta_{p^k}}^{i(p^k-1)}}{{\zeta_{p^k}}^{ip^{k-1}}-1}=p^k\frac{{\zeta_{p^k}}^{i(p^k-1)}}{{\zeta_p}^i-1}.$$

$f_k(x)$ の判別式は $(-1)^{\#S(\#S-1)/2}\prod_{i\in S}t_i$ に等しい（追加補題 4.1.1）．まず，$\prod_{i\in S}p^k=p^{k(p-1)p^{k-1}}$．$\prod_{i\in S}{\zeta_{p^k}}^{i(p^k-1)}={\zeta}^{p^k-1}=(-1)^{(p^k-1)\#S}=1$．${\zeta_p}^i-1$ $(i=1,\dots,p-1)$ は $x^{p-1}+px^{p-2}+\cdots+p$ の異なる根なので，$\prod_{i=1}^{p-1}({\zeta_p}^i-1)=(-1)^{p-1}p=p$．よって，$\prod_{i\in S}{\zeta_p}^i-1=\prod_{i=1}^{p-1}({\zeta_p}^i-1)^{p^{k-1}}=p^{p^{k-1}}$．

以上から，

$$\Delta(f_k)=(-1)^{\#S(\#S-1)/2}p^{(kp-k-1)p^{k-1}}.$$

$\Delta(f_k)>0$ となるのは，$\#S=(p-1)p^{k-1}$ が 4 の倍数のとき．これは，奇素数 p に対しては，$p\equiv 1 \bmod 4$ のとき．$p=2$ に対しては $2^k=8,16,\dots$．□

4.4 Kronecker-Weber の定理

■補題 4.4.3

$\mathbb{Q}(\zeta_{p^n})$ の p の上にある素イデアル $\mathfrak{p}$ による完備化は $\mathbb{Q}_p(\zeta_{p^n})$

証明 円分多項式 $\Phi_p(x)$ の x^{p-1} 係数は 1，定数項は p．$1\leq s\leq p-2$ に対し，x^s の係数は

$$\begin{aligned}\sum_{k=0}^{p-1-s}\binom{s+k}{s}&=\sum_{k=0}^{p-1-s}\binom{s+k-1}{s-1}+\sum_{k=0}^{p-1-s}\binom{s+k-1}{s}\\&=-\binom{p-1}{s-1}+\sum_{k=0}^{p-1-(s-1)}\binom{(s-1)+k}{s-1}+\sum_{k=0}^{p-2-s}\binom{s+k}{s}\end{aligned}$$

であるので，

$$\sum_{k=0}^{p-1-(s-1)}\binom{(s-1)+k}{s-1}=\binom{p-1}{s-1}+\binom{p-1}{s}=\binom{p}{s}.$$

この式の左辺が x^{s-1} の係数であることに注意すれば，x^s の係数は $\binom{p}{s+1}$ と分かる．また，$s=0, p-1$ でもこの式は成立するので，

$$\Phi_p(x+1) = \sum_{k=0}^{p-1} \binom{p}{s+1} x^s.$$

特に，$\Phi_p(x+1)$ は Eisenstein 多項式．I-p.282 から

$$\Phi_{p^n}(x) = \frac{x^{p^n}-1}{\Phi_1 \cdots \Phi_{p^{n-1}}} = \frac{x^{p^{n-1}}-1}{\Phi_1(x)\cdots\Phi_{p^{n-2}}} \frac{x^{p^n}-1}{(x^{p^{n-1}}-1)\Phi_{p^{n-1}}} = \Phi_{p^{n-1}} \frac{\Phi_p(x^{p^{n-1}})}{\Phi_{p^{n-1}}(x)} = \Phi_p(x^{p^{n-1}}).$$

上の結果と合わせて，$\Phi_{p^n}(x+1)$ は p についての Eisenstein 多項式．したがって，$\mathbb{Q}_p$ 上でも既約であり，$[\mathbb{Q}_p(\zeta_{p^n}) : \mathbb{Q}_p] = p^n - p^{n-1}$.

p.172 の議論と同様に進める．$N = p^n - p^{n-1} = [\mathbb{Q}(\zeta_{p^n}) : \mathbb{Q}]$，$\mathfrak{p} = (\zeta_{p^n} - 1)$ とおく．$p\mathcal{O} = \mathfrak{p}^N$ なので，$\mathfrak{p}$ は p の上にある素イデアルで，$e(\mathfrak{p}/p) = N$ で $f(\mathfrak{p}/p) = 1$．また，$\mathfrak{p}$ は p の上にある唯一の素イデアル（定理 1.3.23）．$\mathbb{Q}(\zeta_{p^n})$ の $\mathfrak{p}$ による完備化を $\widehat{\mathbb{Q}}(\zeta_{p^n})$ とおく．先程の議論から，

$$[\widehat{\mathbb{Q}}(\zeta_{p^n}) : \mathbb{Q}_p] = N, \quad f(\widehat{\mathbb{Q}}(\zeta_{p^n})/\mathbb{Q}_p) = 1, \quad e(\widehat{\mathbb{Q}}(\zeta_{p^n})/\mathbb{Q}_p) = N.$$

$\widehat{\mathbb{Q}}(\zeta_{p^n})/\mathbb{Q}_p$ は $\mathbb{Q}_p$ の上にあり，ζ_{p^n} を含むので，$[\widehat{\mathbb{Q}}(\zeta_{p^n}) : \mathbb{Q}_p(\zeta_{p^n})] \geq 1$．上の結果と併せて，$[\widehat{\mathbb{Q}}(\zeta_{p^n}) : \mathbb{Q}_p(\zeta_{p^n})] = 1$．よって示せた．

これを使えば，$\mathbb{Q}_p(\zeta_{p^{e_p}})$ における $\mathbb{Q}_p$ の最大不分岐拡大は $\mathbb{Q}_p$（p.181，2 段落目）なので，$\mathbb{Q}(\zeta_{p^{e_p}})$ における $\mathbb{Q}$ の最大不分岐拡大は $\mathbb{Q}$ となる． □

$\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ で $p \nmid n$ は不分岐

証明 定理 4.1.2(2) から $\mathbb{Q}(\zeta_n)$ の判別式は p で割り切れない．よって，Dedekind の判別定理から p は $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ で不分岐．p の上にある $\mathbb{Z}[\zeta_n]$ の素イデアルで $\mathbb{Q}(\zeta_n)$ を完備化した体を $\widehat{K}$ をとすれば，$\widehat{K}/\mathbb{Q}_p$ で p は不分岐（定理 1.3.23(6)）．$\mathbb{Q}_p(\zeta_n) \subset \widehat{K}$ なので，$\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ でも p は不分岐（命題 1.3.5(1)）． □

■定理 4.4.2

有限次 Abel 拡大は次数が素数冪の巡回拡大の合成である

証明 L/K を有限次 Abel 拡大，有限 Abel 群の基本定理から位数が素数冪の巡回群 $C_1, \ldots, C_r$ があり，$\mathrm{Gal}(L/K) \simeq C_1 \times \cdots \times C_r$．$G_i = C_1 \times \cdots C_{i-1} \times \{1\} \times C_{i+1} \times \cdots \times C_r$，$G_i$ の不変体を L_i とする．$L_1 \cdots L_r$ は $L_1, \ldots, L_r$ を含む最小の L の部分体．Galois の基本定理から，これに対応する $\mathrm{Gal}(L/K)$ の部分群は $G_1, \ldots, G_r$ に含まれる最大のもの．これは $G_1 \cap \cdots \cap G_r = \{1_G\}$．従って，$L_1 \cdots L_r = L$ となる．$[L : L_1] = \#G_i = \#C_1 \cdots \#C_{i-1} \#C_{i+1} \cdots \#C_r$ なので，$[L_1 : K] = \#C_1$．従って L_i は K の素数冪次の巡回拡大． □

$\mathrm{Gal}(N/\mathbb{Q}_2) \simeq (\mathbb{Z}/2\mathbb{Z})^4$ となる N は存在しない

証明 $[N:\mathbb{Q}_2]=16$ なので，$[N:M]=8$ となる中間体 M が存在する．$\mathrm{Gal}(N/M)$ と同型な $(\mathbb{Z}/2\mathbb{Z})^4$ の部分群は位数が 8 であり，このような部分群は次の 15 個存在する[*1]．したがって，$\mathbb{Q}_2$ の 2 次拡大が 15 個存在することになり矛盾（命題 2.4.2）．□

H と H_1 の構成（Galois 群が $(\mathbb{Z}/4\mathbb{Z})^3$ と同型になる $\mathbb{Q}_2$ の有限次拡大 N が存在しないことを証明する部分）

証明 Galois 群 $\mathrm{Gal}(N/\mathbb{Q}_2(\sqrt{-1}))$ を同型で写した，$(\mathbb{Z}/4\mathbb{Z})^3$ の部分群を H とする．$[N:\mathbb{Q}_2(\sqrt{-1})]=32$ なので $|H|=32$．H は位数 4 の元 2 つと位数 2 の元 1 つで生成されることが容易に分かる．α，β，γ を位数 4 の元として，H の生成系は $\{\alpha,\beta,2\gamma\}$ と表すことができる．H の任意の元は自然数 a,b,c によって $a\alpha+b\beta+2c\gamma$ と書ける．

$a\alpha+b\beta+2c\gamma=0$，$A=(\alpha,\beta,2\gamma)\in \mathrm{M}_3(\mathbb{Z})$ とする．$\det A=0$ なら $\{\alpha,\beta,2\gamma\}$ は線形従属となり，$\langle\alpha,\beta,2\gamma\rangle$ は位数が 32 未満となるので矛盾．従って $\det A\neq 0$ であり，$(a,b,c)=(0,0,0)$．つまり，$\{\alpha,\beta,2\gamma\}$ は線形独立．従って $\forall h\in H$ に対し，$h=a\alpha+b\beta+2c\gamma$ となる (a,b,c) が一意に定まる．これを $(a,b,2c)$ と表すことにする．$(a,b,4c)$ で表される元は $a\alpha+b\beta+4c\gamma=a\alpha+b\beta$ なので，$\langle\alpha,\beta\rangle\simeq(\mathbb{Z}/4\mathbb{Z})^2$．これを H_1 と書けば，$(\mathbb{Z}/4\mathbb{Z})^4/H_1\simeq\mathbb{Z}/4\mathbb{Z}$．□

[*1] `./src/4_4_2.py`

第 5 章

Gauss 和・Jacobi 和と有限体上の方程式

5.2 Gauss 和の応用

■補題 5.2.6

$N(x^n = a) = |G/G_1|$

証明 定理 I-7.4.10 から $\mathbb{F}_p^\times$ 巡回群であるので，g で生成されるとする．$n \nmid p-1$ なら $\mathbb{F}_p^\times = (\mathbb{F}_p^\times)^n$．実際，$i = g^\alpha$，$j = g^\beta$，$1 \le \alpha < \beta \le p-1$，$i^n = j^n$ とすれば，$g^{n\beta} - g^{n\alpha} = g^{n\alpha}(g^{n(\beta-\alpha)} - 1) = 0$ となるが，$p-1 \nmid n(\beta-\alpha)$ なので，$i = j$ となる．従って，$N(x^n = 1) = 1$.

他方，$n \mid p-1$，$p-1 = nk$ とする．$(\mathbb{F}_p^\times)^k = \{1, g^k, \dots, g^{(n-1)k}\}$ である．i, j を $x^n = a$ の解，さらに，$i = g^\alpha$，$j = g^\beta$，$0 \le \alpha < \beta \le p-1$ とする．$a = i^n = j^n$ なので，$g^{n(\beta-\alpha)} = 1$，従って $(p-1)l = n(\beta-\alpha)$ となる l が存在する．$kl = \beta - \alpha$ なので，$j = i^{\beta/\alpha} = i^{1+kl/\alpha} = i \times g^{kl} \in i(\mathbb{F}_p^\times)^k$．従って，$x^n = a$ の解は全て $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^k$ の同値類に属する．

逆に，$i^n = a$ ならば，$i(\mathbb{F}_p^\times)^k$ の全ての元は $x^n = a$ を満たす．従って，$N(x^n = a) = |(\mathbb{F}_p^\times)^k| = n$. □

5.5 不定方程式 $3x^3 + 4y^3 + 5z^3 = 0$

■定理 5.5.1

$P \mid I_1, I_2$ ならば $P = P_2$ もしくは $P = P_3$

証明 $\mathcal{O}_K$ の類数は 1 なので，$P = (\beta)$ となる $\beta \in \mathcal{O}_K$ があり，$\beta \mid 3\alpha^2x^2, 12y^2$ となる．x^2, y^2 は互いに素なので，$ax^2 + by^2 = 1$ となる整数 a, b が存在するので，$\beta \mid 12\alpha^2$ であることが分かる．従って，$\beta = 2-\alpha$，$\beta = 3 + 2\alpha + \alpha^2$ もしくは $\beta = \alpha$ である．$(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ と素イデアル分解されたとする．$p_i\mathbb{Z} = \mathfrak{p}_i \cap \mathbb{Z}$ とおく．命題 1.10.13, 命題 1.0.14 から $\mathrm{N}_{K/\mathbb{Q}}((\alpha)) = {p_1}^{f_1} \cdots {p_t}^{f_t} = (\mathrm{N}_{K/\mathbb{Q}}(\alpha)) = (6)$. したがって, $p_1 = 2, p_2 = 3$ となり，2 の上にある唯一の素イデアル，P_3 は 3 の上にある唯一の素イデアルなので，$(\alpha) = P_2P_3$. □

第 6 章

2 次体の整数論

6.1 2 次体の基本単数

■定理 6.1.4 $D > 1$（ただし $\equiv 0, 1 \bmod 4$）を与えると，Pell 方程式 $x^2 - Dy^2 = \pm 4$ 及び θ が決まる．b, c を $\theta^2 + b\theta + c = 0$ となるように定める．θ は簡約な 2 次実無理数なので（命題 6.1.33），連分数展開が可能（命題 6.1.29）：$\theta = [k_0, k_1, \ldots, k_{n-1}, \theta]$．これによって最小整数解 $\varepsilon = (x_1 + y_1\sqrt{D})/2$ を定める（命題 6.1.33）．ε^l は Pell 方程式の解であり（命題 6.1.35），Pell 方程式の解は ε^l の形である（系 6.1.39）．

■系 6.1.39

$t = u$ の場合

証明 (x, y) が Pell 方程式の解で

$$\begin{pmatrix} \frac{x-by}{2} & -cy \\ y & \frac{x+by}{2} \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} s+1 & s \\ 1 & 1 \end{pmatrix}$$

であるとする．$x = s + 2$，$y = 1$，$b = -s$ なので $\theta = (-b + \sqrt{D})/2 = (s + \sqrt{D})/2$ となる．$\theta = [s, 1, \theta]$ なので，$q_0 = 0$，$q_1 = 1$，$q_2 = 1$ である，従って，

$$\frac{x_1 + y_1\sqrt{D}}{2} = q_2\theta + q_1 = \theta + 1 = \frac{s + 2 + \sqrt{D}}{2} = \frac{x + y\sqrt{D}}{2}$$

となり，主張が従う． □

6.2 2 次体の類数

■定理 6.2.1 虚 2 次体では狭義のイデアル類とイデアル類が一致するので，イデアル類と $\mathrm{Sym}^2_{\mathrm{prim},D}(\mathbb{Z}^2)$ の正の同値類は

$$\alpha = (\alpha_1, \alpha_2) \mapsto f_\alpha, \quad ax^2 + bxy + cy^2 \mapsto \left\langle a, \frac{-b + \sqrt{D}}{2} \right\rangle$$

によって 1 対 1 に対応する（定理 6.2.14）．系 6.2.29 から $\mathrm{Sym}^2_{\mathrm{prim},D}(\mathbb{Z}^2)$ の異なる簡約 2 次形式は対等にならない．また，証明から $\mathrm{Sym}^2_{\mathrm{prim},D}(\mathbb{Z}^2)$ の任意の元は簡約 2 次形式と正に対等であることが分かる．従って，

$\mathrm{Sym}^2_{\mathrm{prim},D}(\mathbb{Z}^2)$ の正の同値類の完全代表系として簡約 2 次形式を取ることができる．よって，K の類数は簡約 2 次形式の係数の組み合わせの数に等しい．

■定理 6.2.2　イデアル類群と判別式 D の 2 次実無理数の対等による同値類 Y_D と 1 対 1 に対応する（定理 6.2.19）．判別式 D の 2 次実無理数は $(-b+\sqrt{D})/2a$ の形である．全ての判別式 D の 2 次実無理数は判別式 D の簡約な 2 次実無理数と対等である（系）ので，Y_D の完全代表系を判別式 D の簡約な 2 次実無理数から選ぶことができる．あとは，判別式 D の簡約な 2 次実無理数のうち，対等である（すなわち連分数展開に於いて循環節が一致する：命題 6.2.31）ものを同一視すれば，Y_D の完全代表系が得られる．また，判別式 D の 2 次実無理数 $(-b+\sqrt{D})/2a$ が簡約であることは，これを第 1 根に持つ 2 次形式 $ax^2+bxy+cy^2$ が簡約形式であることと同値（命題 6.2.21）．従って，類数を求める際は，判別式 D の簡約 2 次形式の係数のみを考えれば良い．