岩澤理論セミナー ～ 理論から計算まで ～

目次

第 I 部

イデアル類群と単数群

1　代数的整数

$0 \neq f(X) \in \mathbb{Q}[X]$ の根 $\alpha \in \mathbb{C}$ を**代数的数**という．$\alpha \in \mathbb{C}$ を根にもつ多項式 $f(X) \in \mathbb{Q}[X]$ のうち, 次数が最小でモニックであるものが一意的に存在する．これを α の $\mathbb{Q}$ 上の**最小多項式**という．このとき $f(X)$ の多項式としての次数を α の次数という．$\mathbb{Q}$ 上の最小多項式は $\mathbb{Q}$ 上既約である．代数的数 α がモニック多項式 $g(X) \in \mathbb{Z}[X]$ の根であるとき**代数的整数**という．代数的数 α の $\mathbb{Q}$ 上の最小多項式を $f(X)$ とするとき, α が代数的整数 $\iff$ $f(X) \in \mathbb{Z}[X]$ が成り立つ．

Lemma 1.1. $\alpha \in \mathbb{C}$ を代数的数とする．このとき以下は同値である．

(1) α は代数的整数.
(2) $\mathbb{Z}[\alpha]$ は有限生成 $\mathbb{Z}$ 加群.
(3) $^{\exists}$ 有限生成 $\mathbb{Z}$ 加群 L s.t. $\alpha L \subset L$.

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1) という流れで示す．

[(1) $\Rightarrow$ (2)] α の次数を n とする, すなわち α は $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$ $(c_i \in \mathbb{Z})$ を満たすとする．このとき $\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$ であることを示せばよい．「$\supset$」は明らかなので逆の包含, すなわち $^{\forall} f \in \mathbb{Z}[\alpha]$ が, 高々 $n-1$ 次の α の多項式で表されることを示せばよい．しかしこれは初めに述べた α が満たす関係式より明らか.

[(2) $\Rightarrow$ (3)] $L = \mathbb{Z}[\alpha]$ と取ればよい．そうすれば仮定より $\mathbb{Z}[\alpha]$ は有限生成 $\mathbb{Z}$ 加群だし $\alpha\mathbb{Z}[\alpha] \subset \mathbb{Z}[\alpha]$ も自明.

[(3) $\Rightarrow$ (1)] L の生成元を $\{v_1, \ldots, v_n\}$ とする．このとき $\alpha v_i \in L$ であるから, $\alpha v_i = a_{i1}v_1 + \cdots + a_{in}v_n$ $(a_{ij} \in \mathbb{Z})$ と表せる．このとき $A = (a_{ij}), v = {}^t(v_1 v_2 \ldots v_n)$ とおけば $Av = \alpha v$ が成り立ち, $\det(\alpha E - A) = 0$ となる．つまりモニック多項式 $f(x) = \det(xE - A) \in \mathbb{Z}[x]$ は α の根である．(既約性は言わなくてもよい．それが代数的整数の定義．) □

Example 1.2. $\alpha = \sqrt[3]{2}$ とする．α の $\mathbb{Q}$ 上最小多項式は $x^3 - 2$ である．(既約であることは Eisenstein の判定法において $p = 2$ とすればよい．) これは整数係数モニック多項式の根であることから特に α は代数的整数である．
このとき $\mathbb{Z}[\sqrt[3]{2}] = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{2}^2$ となる．実際包含「$\supset$」は明らかで「$\subset$」は関係式 $(\sqrt[3]{2})^3 - 2 = 0$ を用いて次数下げを行えばよい.

Corollary 1.3. α, β が代数的整数ならば $\alpha + \beta$, $\alpha\beta$ も代数的整数である．

Proof. α と β の次数をそれぞれ m, n とする．このとき補題 1.1 より $\mathbb{Z}[\alpha]$ と $\mathbb{Z}[\beta]$ は有限生成 $\mathbb{Z}$ 加群である．主張を示すためには $(\alpha+\beta)L \subset L, (\alpha\beta)L \subset L$ なる有限生成 $\mathbb{Z}$ 加群 L の存在を言えばよいが,

$$L = \sum_{0 \leq i < m, 0 \leq j < n} \mathbb{Z}\alpha^i\beta^j = \mathbb{Z}[\alpha, \beta]$$

が条件を満たす. □

2　整数環

K を**代数体**, すなわち $K/\mathbb{Q}$ は体の代数拡大とする．$\dim_{\mathbb{Q}} K := [K : \mathbb{Q}] :=$ ($\mathbb{Q}$ 上のベクトル空間 K の次元) として定義する．$[K : \mathbb{Q}] < \infty$ のときは K は**有限次代数体**, $[K : \mathbb{Q}] = \infty$ のときは**無限次代数体**という．系 1.3 より K の代数的整数全体 $\mathcal{O}_K$ は環になり, **整数環**という．

Example 2.1. $K_1 = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega), K_2 = \mathbb{Q}(\sqrt{-5})$ としてそれぞれの整数環を求める. 以下で $\mathcal{O}_{K_1} = \mathbb{Z}[\omega], \mathcal{O}_{K_2} = \mathbb{Z}[\sqrt{-5}]$ を示す. どちらの場合も包含「$\supset$」は明らかなので, 「$\subset$」のみを示せばよい.
まず $a + b\sqrt{-3} \in \mathcal{O}_{K_1}$
$UTF00A0(a, b \in \mathbb{Q})$ と仮定する. このとき整数環の定義から $a + b\sqrt{-3}$ の $\mathbb{Q}$ 上最小多項式

$$(X - (a + b\sqrt{-3}))(X - (a - b\sqrt{-3})) = X^2 - 2aX + (a^2 + 3b^2)$$

は整数係数多項式とならなければならない. 従って $2a, a^2 + 3b^2 \in \mathbb{Z}$ である. また, $4(a^2 + 3b^2) = (2a)^2 + 12b^2 \in \mathbb{Z}$ より $12b^2 \in \mathbb{Z}$ となるが, 少し頑張れば $2b \in \mathbb{Z}$ が分かる. 以上より $a = c/2, b = d/2$ $(c, d \in \mathbb{Z})$ と表せる. よって

$$a + b\sqrt{-3} = \frac{c}{2} + \frac{d}{2}\sqrt{-3} = \frac{(c-d)+d}{2} + \frac{d}{2}\sqrt{-3} = \frac{c-d}{2} + d\frac{1+\sqrt{-3}}{2}$$

となるので, あとは $(c - d)/2 \in \mathbb{Z}$, すなわち $c - d \equiv 0 \bmod 2$, すなわち $(2a) - (2b) \equiv 0 \bmod 2$, すなわち $(2a)$ と $(2b)$ の偶奇が一致することを示せばよい. $0 \equiv 4(a^2 + 3b^2) = (2a)^2 + 3(2b)^2 \bmod 4$ であることから $((2a)^2, (2b)^2) \equiv (0, 0), (1, 1) \bmod 4$ を得るが, これは $(2a, 2b) = (even, even), (odd, odd)$ となることがすぐに分かる. よって ok. K_2 の場合も同様に示せる.
一般に $K = \mathbb{Q}(\sqrt{d})$ $(d : square - free)$ の整数環は

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & (d \equiv 2, 3 \bmod 4) \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & (d \equiv 1 \bmod 4) \end{cases}$$

となることが同様の議論で示せる.

Lemma 2.2. K を代数体とする. このとき以下が成り立つ.

(1) $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.
(2) $^\forall\alpha \in K$, $^\exists m \in \mathbb{N}$ s.t. $m\alpha \in \mathcal{O}_K$.

Proof. (1) $\mathcal{O}_K \cap \mathbb{Q} \subset \mathbb{Z}$ のみ示せば十分である. 任意の既約分数 $a/b \in \mathcal{O}_K \cap \mathbb{Q}$ を一つ取る. $(a, b \in \mathbb{Z})$ このとき $a/b \in \mathcal{O}_K$ より, ある $c_i \in \mathbb{Z}, n \in \mathbb{N}$ が存在して

$$\left(\frac{b}{a}\right)^n + c_1\left(\frac{b}{a}\right)^{n-1} + \cdots + c_n = 0$$

が成り立つ. 両辺 a^n をかけて移項して左辺を b で括ることで

$$b\left(b^{n-1} + c_1 a b^{n-2} + \cdots + c_{n-1}a^{n-1}\right) = -a^n$$

を得る. 従って b は a の約数となるが, a と b の取り方より $\gcd(a, b) = 1$ なので $b = \pm 1$ にしかならない. 従って $a/b = \pm a \in \mathbb{Z}$ を得る.
(2) $K/\mathbb{Q}$ は代数拡大であるから, $\alpha \in K$ に対して

$$c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0 \ (c_i \in \mathbb{Q})$$

が成り立つ. $c_i = a_i/b_i$ と既約分数表示し, 全ての b_i の最小公倍数を l とおき, 両辺 l をかけることで

$$l_n a_n \alpha^n + l_{n-1}a_{n-1}\alpha^{n-1} + l_{n-2}a_{n-2}\alpha^{n-2} + \cdots + l_0 a_0 = 0 \ (lc_i = la_i/b_i = l_i a_i, l_i \in \mathbb{Z})$$

が成り立つ. さらに両辺 $l_n^{n-1}a_n^{n-1}$ をかけることで

$$(l_n a_n \alpha)^n + l_{n-1}a_{n-1}(l_n a_n \alpha)^{n-1} + l_{n-2}a_{n-2}l_n a_n (l_n a_n \alpha)^{n-2} + \cdots + l_0 a_0 l_n^{n-1}a_n^{n-1} = 0$$

となり, $m\alpha = l_n a_n \alpha$ は整数係数モニック多項式の根となり, 確かに $m\alpha \in \mathcal{O}_K$ が得られた. □

単射準同型 $\sigma : K \to \mathbb{C}$ を, K から $\mathbb{C}$ への埋め込みと呼び, K から $\mathbb{C}$ への埋め込み全体を $\mathrm{Emb}(K,\mathbb{C})$ と書く. $[K:\mathbb{Q}] = n$ のとき K を n **次代数体**という. このとき n 個の異なる埋め込み $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ が存在する. $x \in K$ に対し $x^{\sigma_i} = x^{(i)} = \sigma_i(x)$ と表す. また, $x \in K$ のトレースとノルムを

$$\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_i x^{(i)}$$
$$\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_i x^{(i)}$$

と定義する. $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ と $\mathrm{N}_{K/\mathbb{Q}}(x)$ は x の $\mathbb{Q}$ 上の最小多項式 (の (大体) 定数項と 1 次の項の係数) なので, $\mathrm{Tr}(x), \mathrm{N}(x) \in \mathbb{Q}$ である. 特に $x \in \mathcal{O}_K$ ならば $\mathrm{Tr}(x), \mathrm{N}(x) \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ である.

Lemma 2.3. $[K:\mathbb{Q}] = n$ とする. このとき $v_1, v_2, \dots, v_n \in K$ が $\mathbb{Q}$ 上独立ならば $\det(v_j^{(i)}) \neq 0$ である.

Proof. $K/\mathbb{Q}$ は有限次分離拡大なので単拡大, すなわち $\alpha \in K$ が存在して $K = \mathbb{Q}(\alpha)$ と表せる. $[K:\mathbb{Q}] = n$ なので, K は $\mathbb{Q}$ 上のベクトル空間として基底 $\{v_1, \dots, v_n\}$ の他に $\{1, \dots, \alpha^{n-1}\}$ が取れる. このとき線形代数の基本的な結果から, ある $A \in GL_n(\mathbb{Q})$ が存在して $(v_1\ v_2\ \dots\ v_n) = (1\ \alpha\ \dots\ \alpha^{n-1})A$ が成り立つ. v_j に対するこの操作を $v_j^{(i)} = \sigma_i(v_j)$ で同様に行うことで $(v_1^{(i)}\ v_2^{(i)}\ \dots$
$UTF00A0v_n^{(i)}) = (1\ \alpha_i\ \alpha_i^2\ \dots\ \alpha_i^{n-1})A$ を得る. ただし $\alpha_i := \alpha^{(i)}$ である. 全ての i を動かしてこれらの関係式を繋げることで, 関係式

$$\begin{pmatrix} v_1^{(1)} & v_2^{(1)} & \dots & v_n^{(1)} \\ v_1^{(2)} & v_2^{(2)} & \dots & v_n^{(2)} \\ \dots & \dots & \dots & \dots \\ v_1^{(n)} & v_2^{(n)} & \dots & v_n^{(n)} \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & \alpha_n & \dots & \alpha_n^{n-1} \end{pmatrix} A =: XA$$

を得る. 両辺行列式を取れば $\det A \neq 0$ であること, $\det X = (\text{Vandermond の行列式}) = \prod_{i<j}(\alpha_i - \alpha_j) \neq 0$ であることから主張を得る. □

Theorem 2.4. $[K:\mathbb{Q}] = n$ のとき, $\mathcal{O}_K$ は $\mathrm{rank}\, n$ の自由 $\mathbb{Z}$ 加群, すなわち

$$\mathcal{O}_K \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}.$$

Proof. まず $[K:\mathbb{Q}] = n$ よりベクトル空間 K の $\mathbb{Q}$ 上の基底として $\{v_1, \dots, v_n\}$ を取れるが, 補題 2.2 より適切に v_i に $m_i \in \mathbb{Z}$ をかけることで初めから $v_i \in \mathcal{O}_K$ としてよい. このとき $\mathrm{rank}\, n$ の自由 $\mathbb{Z}$ 加群 $R := \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ を考える. このとき $^\exists m\mathcal{O}_K \subset R (\subset \mathcal{O}_K)$ を示す. これが示されれば

$$n \leq \mathrm{rank}\, \mathcal{O}_K \leq \mathrm{rank}\, m\mathcal{O}_K \leq n$$

より, $\mathrm{rank}\, \mathcal{O}_K = n$ が分かる.

行列 $V = (v_j^{(i)})$ を考えると補題 2.3 より $K \ni \det V =: |V| \neq 0$ である. 従って $(\det V)^{-1} \in K$ であり補題 2.2 より, ある $m \in \mathbb{N}$ が存在して $m|V|^{-1} \in \mathcal{O}_K$ とできる. $x \in K$ を取ると $\{v_i, \dots, v_n\}$ は基底なので $x = x_1v_1 + \cdots + x_nv_n$ なる $x_i \in \mathbb{Q}$ が存在する. このとき

$$^t(x_1\ x_2\ \dots\ x_n) = V^{-1}\ ^t(x^{(1)}\ x^{(2)}\ \dots\ x^{(n)}) = \frac{1}{|V|}\tilde{V}^t(x^{(1)}\ x^{(2)}\ \dots\ x^{(n)})$$

が成り立つ. ただし $\tilde{V}$ は V の余因子行列である. "$\tilde{V}$ の成分"$\in \mathcal{O}_K$ に気を付けると $m|V|^{-1} \in \mathcal{O}_K$ と合わせて, $^\forall x \in \mathcal{O}_K$ に対して $m(x_1, x_2, \dots, x_n) \in \mathcal{O}_K^n \cap \mathbb{Q}^n = \mathbb{Z}^n$ を得る., つまり $m\mathcal{O}_K \subset R \subset \mathcal{O}_K$ が成り立つ. □

上の証明における $\{v_1, \dots, v_n\}$ のような $v_i \in \mathcal{O}_K$ となる $\mathcal{O}_K$ の $\mathbb{Z}$ 基底を, **整数基**という. このとき

$$d(K) = \left(\det(v_j^{(i)})\right)^2$$

を K の**判別式**という.

Example 2.5. $K=\mathbb{Q}(\sqrt{-1})$ のとき $d(K)$ を求める. $\mathcal{O}_K=\mathbb{Z}\oplus\mathbb{Z}i$ であることから整数基は $\{1,i\}$ である. また, 埋め込み $K\hookrightarrow\mathbb{C}$ は id と σ(共役) の二つのみであることが $[K:\mathbb{Q}]=2$ より分かる. 以上より判別式は

$$d(K)=\begin{vmatrix}1 & 1^\sigma\\ i & i^\sigma\end{vmatrix}^2=\begin{vmatrix}1 & 1\\ i & -i\end{vmatrix}^2=(-2i)^2=-4$$

となる. (なんか行列式のサイズ無駄に長くなっちゃってワロタ)

Lemma 2.6. $0\neq d(K)\in\mathbb{Z}$ であり, $d(K)$ は整数基の取り方に依らない.

Proof. 整数基を $\{v_1,\dots,v_n\}$ と $\{w_1,\dots,w_n\}$ という二通り用意する. このとき加群論から, ある $A\in GL_2(\mathbb{Z})$ が存在して $(w_1\ w_2\ \dots\ w_n)=(v_1\ v_2\ \dots\ v_n)A$ が成り立つ. 同様の操作を $\{v_1^{(i)},\dots,v_n^{(i)}\}$ と $\{w_1^{(i)},\dots,w_n^{(i)}\}$ で行い関係式を立て両辺の行列式を取ることで $\det(w_j^{(i)})=\det(v_j^{(i)})\det A=\pm\det(v_j^{(i)})$ が成り立つ. あとはさらに両辺二乗すれば整数基の取り方に依らないことが分かる.

次に $d(K)\in\mathbb{Z}$ を示す. $d(K)=\det(v_j^{(i)})^2=\det\left((v_i^{(j)})(v_j^{(i)})\right)$ であるから特に $(v_i^{(j)})(v_j^{(i)})$ の (i,j) 成分が $\mathbb{Z}$ に属すことを示せばよい. そしてその (i,j) 成分は以下のように計算できる.

$$\sum_{k=1}^{n}v_i^{(k)}v_j^{(k)}=\mathrm{Tr}_{K/\mathbb{Q}}(v_iv_j)\in\mathcal{O}_K\cap\mathbb{Q}=\mathbb{Z}$$

従って主張が得られた. □

$\alpha\in K$ に対しトレースとノルムを定義したが, これはある線形写像のトレースと行列式に関係している. 次の補題では $\alpha\in\mathcal{O}_K$ とするが, $\alpha\in K$ に対しても同様の議論が可能である.

Lemma 2.7. $0\neq\alpha\in\mathcal{O}_K$ は線形写像 $f_\alpha:\mathcal{O}_K\to\mathcal{O}_K;x\mapsto\alpha x$ を誘導する. このとき

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)=\mathrm{Tr}(f_\alpha),\ \mathrm{N}_{K/\mathbb{Q}}(\alpha)=\det(f_\alpha)$$

が成り立つ.

Proof. $\mathcal{O}_K$ の整数基を $\{v_1,\dots,v_n\}$ とする. このとき $f_\alpha(v_i)\in\mathcal{O}_K$ より $\alpha v_i=b_{i1}v_1+\cdots+b_{in}v_n$ $(b_{ij}\in\mathbb{Z})$ と表せる. よって $B=(b_{ij})\in M_n(\mathbb{Z})$ により $\alpha(v_1\ \dots\ v_n)=(v_1\ \dots\ v_n)B$ が成り立つ. 以上より

$$\begin{pmatrix}\alpha^{(1)} & & \\ & \cdots & \\ & & \alpha^{(n)}\end{pmatrix}\begin{pmatrix}v_1^{(1)} & \dots & v_n^{(1)}\\ \dots & & \dots\\ v_1^{(n)} & \dots & v_n^{(n)}\end{pmatrix}=\begin{pmatrix}v_1^{(1)} & \dots & v_n^{(1)}\\ \dots & & \dots\\ v_1^{(n)} & \dots & v_n^{(n)}\end{pmatrix}B$$

が成り立つ. めんどくさいので上の式を $AV=VB$ と表す. このとき

$$\mathrm{Tr}(f_\alpha)=\mathrm{Tr}(B)=\mathrm{Tr}(V^{-1}AV)=\mathrm{Tr}(A)=\sum_i\alpha^{(i)}=\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$$

$$\det(f_\alpha)=\det(B)=\det(V^{-1}AV)=\det(A)=\prod_i\alpha^{(i)}=\mathrm{N}_{K/\mathbb{Q}}(\alpha)$$

となって ok. □

Lemma 2.8. K を n 次代数体とする. このとき以下が成り立つ.

- $0\neq\alpha\in\mathcal{O}_K$ に対して $(\mathcal{O}_K:\alpha\mathcal{O}_K)=|\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$.
- $\mathcal{O}_K$ のイデアル $\mathfrak{a}\neq0$ に対して $(\mathcal{O}_K:\mathfrak{a})<\infty$, つまり $\mathfrak{a}$ は $\mathrm{rank}\,n$ の自由 $\mathbb{Z}$ 加群.

Proof. 前補題の記号をそのまま使うことにすると $(\mathcal{O}_K : \alpha\mathcal{O}_K) \overset{\text{非自明?}}{=} |\det(B)| = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$ で ok. 次に $0 \neq \alpha \in \mathfrak{a}$ を取る. このとき $(\alpha) \subset \mathfrak{a}$, すなわち $\alpha\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$ となる. 従って $(\mathcal{O}_K : \mathfrak{a}) \leq (\mathcal{O}_K : \alpha\mathcal{O}_K) < \infty$ となり ok. □

Theorem 2.9. 有限次代数体 K の整数環 $\mathcal{O}_K$ は**デデキント整域**, すなわち以下を満たす.

- $\mathcal{O}_K$ はネーター環である.
- $\mathcal{O}_K$ は整閉である.
- $\mathcal{O}_K$ の 0 でない素イデアルは極大イデアル.

Proof. (1) $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$ を $\mathcal{O}_K$ の 0 でないイデアルの昇鎖列とする. 背理法で示す. 任意の $N \in \mathbb{N}$ に対して $\mathfrak{a}_N \subsetneq \mathfrak{a}_{N+1} \subsetneq \dots$ と仮定すると補題 2.8 を用いて

$$\infty > |\mathcal{O}_K/\mathfrak{a}_N| > |\mathcal{O}_K/\mathfrak{a}_{N+1}| > \dots$$

が成り立つ. しかし $|\mathcal{O}_K/\mathfrak{a}_n|$ は有限なので無限に降下していくことはない. 矛盾.

(2) $x \in K$ が $\mathcal{O}_K$ 上整と仮定, すなわち

$$x^m = a_{m-1}x^{m-1} + \dots + a_1 x + a_0 \ (a_i \in \mathcal{O}_K)$$

が成り立つと仮定する. $x \in \mathcal{O}_K$ を示すためには補題 1.1 より $xL \subset L$ なる非自明な有限生成 $\mathbb{Z}$ 加群 L が存在すればよい. $L_0 := \mathbb{Z}[a_0, \dots, a_{m-1}]$ とおき, $L := L_0[x] = L_0 + L_0 x + \dots + L_0 x^{m-1}$ とおく. 明らかに $xL \subset L$ である. ok.

(3) $\mathfrak{p}$ を 0 でない素イデアルとする. このとき $\mathcal{O}_K/\mathfrak{p}$ は整域であり, さらに補題 2.8 より有限である. 一般に有限整域は体であるから $\mathfrak{p}$ は極大イデアルである. □

3 イデアル群

ここでは K のイデアル群 I_K を定義する. $\mathcal{O}_K$ のイデアルを K の**整イデアル**という. K の整イデアル $\mathfrak{a}$ と $c \in K$ に対し $c\mathfrak{a} \subset K$ は $\mathcal{O}_K$ 加群になる. これを K の**分数イデアル**という. ここで

$$\mathfrak{b} \text{ が } K \text{ の分数イデアル} \iff \begin{cases} \mathfrak{b} \text{ は } \mathcal{O}_K \text{加群} \\ 0 \neq {}^{\exists}c \in K \text{ s.t. } c\mathfrak{b} \subset \mathcal{O}_K \end{cases} \iff \begin{cases} \mathfrak{b} \text{ は } \mathcal{O}_K \text{加群} \\ 0 \neq {}^{\exists}c \in \mathcal{O}_K \text{ s.t. } c\mathfrak{b} \subset \mathcal{O}_K \end{cases}$$

であることに注意する. 実際二つ目の同値の「$\Rightarrow$」は明らかで, 「$\Leftarrow$」は補題 2.2 より $cm\mathfrak{b} \subset m\mathcal{O}_K \subset \mathcal{O}_K$ より従う. K の 0 でない分数イデアル全体を I_K と書き, K のイデアル群と呼ぶ. $\mathfrak{a}, \mathfrak{b} \in I_K$ に対し, 通常のイデアルの積 $\mathfrak{ab}$ として演算を定める. 単位元は $(1) = \mathcal{O}_K$ であり, $\mathfrak{a} \in I_K$ の逆元は

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset \mathcal{O}_K\}$$

である. I_K が実際に群となることを以下で証明していくが, 長くなるので適度に省略する.

Lemma 3.1.
- $\mathfrak{a} \in I_K$ ならば $\mathfrak{a}^{-1} \in I_K$.
- $\mathfrak{a}, \mathfrak{b} \in I_K$ かつ $\mathfrak{ab} = \mathcal{O}_K$ ならば $\mathfrak{b} = \mathfrak{a}^{-1}$.
- $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ をイデアル, $\mathfrak{p} \subset \mathcal{O}_K$ を素イデアルとする. このとき $\mathfrak{ab} \subset \mathfrak{p}$ ならば $\mathfrak{a} \subset \mathfrak{p}$ または $\mathfrak{b} \subset \mathfrak{a}$ である.

Theorem 3.2. I_K は群である.

Lemma 3.3. $\mathfrak{a}, \mathfrak{b}$ を整イデアル, $\mathfrak{p}$ を素イデアルとする. このとき以下が成り立つ.

- $\mathfrak{b}|\mathfrak{a} \iff \mathfrak{a} \subset \mathfrak{b}$.
- $\mathfrak{p}|\mathfrak{ab}$ ならば $\mathfrak{p}|\mathfrak{a}$ または $\mathfrak{p}|\mathfrak{b}$.

Theorem 3.4. $\mathcal{O}_K$ では素イデアル分解の一意性が成立する. すなわち任意の $(\mathcal{O}_K \neq)\mathfrak{a} \in I_K$ に対し

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r}$$

となる相異なる素イデアル $\mathfrak{p}_i$ と $(0 \neq)e_i \in \mathbb{Z}$ が (順序を除き) 一意的に存在する.

Example 3.5. $K = \mathbb{Q}(\sqrt{-5}), \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ としてイデアル $(2) = 2\mathbb{Z}[\sqrt{-5}]$ を素イデアル分解する.

$$\mathbb{Z}[\sqrt{-5}]/(2) \cong \mathbb{Z}[x]/(2, x^2+5) = \mathbb{Z}[x]/(2, (x+1)^2) = \mathbb{Z}[x]/(2, x+1)^2$$

という同型により $\mathbb{Z}[\sqrt{-5}]$ のイデアル (2) と $\mathbb{Z}[x]$ のイデアル $(2, x+1)^2$ が対応する. また,

$$\mathbb{Z}[x]/(2, x+1) = \mathbb{F}_2[x]/(x+1) \cong \mathbb{F}_2[-1] = \mathbb{F}_2$$

より $(2, x+1)$ は極大イデアルである. 従って対応するイデアル $(2, \sqrt{-5}+1)$ も極大イデアルであり素イデアルである. 以上より $(2) = (2, \sqrt{-5}+1)^2$ という素イデアル分解となる.

$0 \neq \mathfrak{a} \subset \mathcal{O}_K$ を整イデアルとすると補題 2.2 より $(\mathcal{O}_K : \mathfrak{a}) < \infty$ である. つまり $\mathcal{O}_K/\mathfrak{a}$ は有限アーベル群となる. 以下でこの構造を調べる. $N(\mathfrak{a}) := (\mathcal{O}_K : \mathfrak{a})$ を $\mathfrak{a}$ の**ノルム**という.

整イデアル $\mathfrak{a}, \mathfrak{b}$ に対し, **最大公約イデアル** $\gcd(\mathfrak{a}, \mathfrak{b})$ と**最小公倍イデアル** $\mathrm{lcm}(\mathfrak{a}, \mathfrak{b})$ を以下のように定義する. ただし $\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r}, \mathfrak{b} = \mathfrak{p}_1^{f_1}\mathfrak{p}_2^{f_2}\dots\mathfrak{p}_r^{f_r}$ とする. (e_i, f_i は 0 も含める.)

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \prod_i \mathfrak{p}_i^{\min(e_i, f_i)},\ \mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod_i \mathfrak{p}_i^{\max(e_i, f_i)}$$

$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathcal{O}_K$ のとき, $\mathfrak{a}$ と $\mathfrak{b}$ は互いに素であるといい, $(\mathfrak{a}, \mathfrak{b}) = 1$ と書く.

Lemma 3.6.
- $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b},\ \mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$.
- $(\mathfrak{a}, \mathfrak{b}) = 1$ ならば環の同型 $\mathcal{O}_K/\mathfrak{a}\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}$ が成り立つ.
- $^\forall n \in \mathbb{N}$ に対して $\mathcal{O}_K$ 加群の同型 $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}$ が成り立つ.

Proof. (1) 一般的な場合は同様に出来るので, ここでは分かりやすく $\mathfrak{a} = \mathfrak{p}_1^3\mathfrak{p}_2, \mathfrak{b} = \mathfrak{p}_1^2\mathfrak{p}_2^2$ と素イデアル分解されているとする. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^2\mathfrak{p}_2$ であるから, 前者は $\mathfrak{p}_1^2\mathfrak{p}_2 = \mathfrak{p}_1^3\mathfrak{p}_2 + \mathfrak{p}_1^2\mathfrak{p}_2^2$ を示せばよい. 包含「$\supset$」は明らかなので「$\subset$」を示せばよい. ($\mathfrak{p}_1^3\mathfrak{p}_2 + \mathfrak{p}_1^2\mathfrak{p}_2^2 = \mathfrak{p}_1^2\mathfrak{p}_2(\mathfrak{p}_1 + \mathfrak{p}_2) = \mathfrak{p}_1^2\mathfrak{p}_2$ を意識して示す. ただしこれは集合と元を混合していてよくない表記なので元を取って正確に示す.) 任意に $x = p_1^2p_2 \in \mathfrak{p}_1^2\mathfrak{p}_2$ を取る. $\gcd(\mathfrak{p}_1, \mathfrak{p}_2) = 1$, すなわち $\mathfrak{p}_1 + \mathfrak{p}_2 = \mathcal{O}_K$ であるから, ある $q_1 \in \mathfrak{p}_1, q_2 \in \mathfrak{p}_2$ が存在して $q_1 + q_2 = 1$ が成り立つ. 従って

$$x = p_1^2p_2 \cdot 1 = p_1^2p_2(q_1+q_2) = (p_1^2q_1)p_2 + p_1^2(p_2q_2) \in \mathfrak{p}_1^3\mathfrak{p}_2 + \mathfrak{p}_1^2\mathfrak{p}_2^2$$

となって ok. 後者は $\mathfrak{p}_1^3\mathfrak{p}_2^2 = \mathfrak{p}_1^3\mathfrak{p}_2 \cap \mathfrak{p}_1^2\mathfrak{p}_2^2$ を示せばよい. しかしこれは実際に元を取ることで容易に分かる.

(2) 中国剰余定理そのまま.

(3) $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$ を一つ取る. このとき

$$\varphi : \mathcal{O}_K \to \mathfrak{p}^n/\mathfrak{p}^{n+1}; x \mapsto \alpha^n x + \mathfrak{p}^{n+1}$$

は $\mathcal{O}_K$ 加群の準同型である. 全射であることを示す. 任意の $y \in \mathfrak{p}^n$ に対して, $\alpha^{-n}y \in \mathfrak{p}^{-n}\mathfrak{p}^n = \mathcal{O}_K$ である. このとき $\varphi(\alpha^{-n}y) = y + \mathfrak{p}^{n+1}$ より ok. あとは $\mathrm{Ker}\varphi = \mathfrak{p}$ を示せば準同型定理より主張が得られる. そしてそれは

$$x \in \mathrm{Ker}\varphi \iff \alpha^n x \in \mathfrak{p}^{n+1} \iff x \in \mathfrak{p}$$

より分かる. ただし最後の同値の $\Rightarrow$ は $x = \alpha^{-n}(\alpha^n x) \in \mathfrak{p}^{-n}\mathfrak{p}^{n+1} = \mathfrak{p}$ より従う. □

Theorem 3.7. 有限次代数体 K の整イデアル $\mathfrak{a}$ の素イデアル分解が $\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r}$ のとき, 以下が成り立つ.

$$\mathcal{O}_K/\mathfrak{a} \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \mathcal{O}_K/\mathfrak{p}_2^{e_2} \times \dots \mathcal{O}_K/\mathfrak{p}_r^{e_r}.$$
$$N(\mathfrak{a}) = N(\mathfrak{p}_1)^{e_1}N(\mathfrak{p}_2)^{e_2}\dots N(\mathfrak{p}_r)^{e_r}.$$

Proof. 前者は補題 3.6(2) より明らか. 後者は, 前者の結果を用いることで $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$ のみ示せば十分である.

$$(\mathcal{O}_K : \mathfrak{p}^e) = (\mathcal{O}_K : \mathfrak{p})(\mathfrak{p} : \mathfrak{p}^2) \dots (\mathfrak{p}^{e-1} : \mathfrak{p}^e)$$

であること, 補題 3.6(3) より $(\mathfrak{p}^i : \mathfrak{p}^{i+1}) = (\mathcal{O}_K : \mathfrak{p})$ であることより従う. □

分数イデアル $\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r}$ に対しては $(\mathcal{O}_K : \mathfrak{a})$ というものは考えられないので, 定理 3.7 の後者の式を用いてノルムを定義する.

Theorem 3.8.
- $\mathfrak{a}, \mathfrak{b} \in I_K$ に対し $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.
- $\alpha \in K^\times$ に対し $N(\alpha\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$.

Proof. (1) ノルムの準同型性を主張する定理である. これは定理 3.7 の後者の主張より従う.
(2) 補題 2.8(1) の主張を分数イデアルに拡張すればよい. □

K の**単項イデアル群**を $P_K = \{\alpha\mathcal{O}_K \mid \alpha \in K^\times\} \subset I_K$ と定義する. さらに $C_K = I_K/P_K$ を**イデアル類群**と呼び, その元のことをイデアル類という. イデアル類群 I_K の位数を $h(K)$ で表し**類数**といい, 次の定理より C_K は**有限群**であることが分かる. $\sigma(K) \subset \mathbb{R}$ となる埋め込み $\sigma \in \mathrm{Emb}(K, \mathbb{C})$ の数を r_1, $\sigma(K) \not\subset \mathbb{R}$ となる σ の数を $2r_2$ とするとき, (r_1, r_2) を K の符号という.

Theorem 3.9. K の次数が n, 符号が (r_1, r_2) であれば, C_K の任意のイデアル類は

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d(K)|}$$

を満たす整イデアル $\mathfrak{a}$ を含む. 右辺の定数を**ミンコフスキー定数**という.

Corollary 3.10. K が有限次代数体ならば C_K は有限アーベル群である.

4 単数群

本では $\mathcal{O}_K$ の単数群を E_K と表記しているが, 通常通りここでは $\mathcal{O}_K^\times$ と表記することにする. $\mathcal{O}_K^\times$ の捩れ部分群 $\mathrm{Tor}(\mathcal{O}_K^\times)$ は W_K, すなわち K に含まれる 1 のベキ根全体に一致する. 特に K が有限次代数体ならば W_K は巡回群である. K が n 次代数体のとき n 個の埋め込みを $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ として, いつも通り $x \in K$ に対し $x^{\sigma_i} = x^{(i)}$ と書く. 特に $x = x^{(1)}$ である.

Lemma 4.1. $[K : \mathbb{Q}] = n$ かつ $x \in \mathcal{O}_K$ とする. このとき以下が成り立つ.

- $x \in \mathcal{O}_K^\times \iff \mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1$.
- $|x^{(i)}| = 1$
  $UTF00A0(1 \leq i \leq n) \iff x \in W_K$.

Proof. (1) 定義に従って計算すれば

$$\begin{aligned} x \in \mathcal{O}_K^\times &\iff {}^\exists x^{-1} \in \mathcal{O}_K \text{ s.t. } xx^{-1} = 1 \\ &\Longrightarrow \mathrm{N}_{K/\mathbb{Q}}(x)\,\mathrm{N}_{K/\mathbb{Q}}(x^{-1}) = 1 \\ &\iff N_{K/\mathbb{Q}}(x) = \pm 1 \end{aligned}$$

となって「⇒」は ok. ただし $x \in \mathcal{O}_K$ に対し $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$ であったことに注意する. 逆に, $\mathrm{N}_{K/\mathbb{Q}}(x) = xx^{(2)}x^{(3)} \dots x^{(n)} = \pm 1$ ならば $x^{-1} = \pm x^{(2)} \dots x^{(n)} \in \mathcal{O}_K$ となって ok.

(2) 「⇒」を示す. 任意の $1 \leq i \leq n$ に対して $|x^{(i)}| = 1$ と仮定する. このとき任意の $m \in \mathbb{N}$ に対して $|(x^m)^{(i)}| = 1$ であり, x^m の $\mathbb{Q}$ 上最小多項式は

$$(X - x^m)(X - (x^m)^{(2)}) \dots (X - (x^m)^{(n)}) = X^n + (1 \text{ 次対称式})X^{n-1} + (2 \text{ 次対称式})X^{n-2} + \dots + (n \text{ 次対称式})$$

のようになる. しかし対称式の部分は全て $(x^m)^{(1)}, \dots, (x^m)^{(n)}$ の多項式で表せ, $|(x^m)^{(i)}| = 1$ より, この最小多項式は任意の $m \in \mathbb{N}$ に対して有限個の可能性しか取り得ない. 従って鳩の巣論法から, ある $N_1 \neq N_2 \in \mathbb{N}$ が存在して x^{N_1} と x^{N_2} の $\mathbb{Q}$ 上最小多項式は一致するとしてよい. すなわち x^{N_1} と x^{N_2} は $\mathbb{Q}$ 上共役である. さらに x^{N_1}(と x^{N_2}) の $\mathbb{Q}$ 上共役元も有限個しかないので, N_1, N_2 を上手く取ることで x^{N_1} と x^{N_2} は $\mathbb{Q}$ 上最小多項式が等しくさらに (共役というより) そのものが等しい, すなわち $x^{N_1} = x^{N_2}$ としてよい. 以上より $x^{N_1 - N_2} = 1$, つまり $x \in W_K$ である.

「$\Leftarrow$」を示す. $x \in W_K$, すなわちある $n \in \mathbb{N}$ が存在して $x^n = 1$ と仮定する. このとき任意の $1 \leq i \leq n$ に対して $(x^{(i)})^n = 1$ であるから特に $x^{(i)} = \pm 1$ である. □

次に付値の理論を簡単に復習しておく. 写像 $|\cdot| : K \to \mathbb{R}$ が付値であるとは, 以下を満たすことである.

- $|x| \geq 0$ かつ, $|x| = 0 \iff x = 0$.
- $|xy| = |x||y|$.
- $^{\exists}C \geq 1$ s.t. $|x| \leq 1 \Rightarrow |1 + x| \leq C$.

$C = 1$ と取れるときは**非アルキメデス付値**, そうでないときは**アルキメデス付値**という. $\gamma > 0$ に対して $|\cdot|' := |\cdot|^\gamma$ も付値になる. これを同値な付値という.

有限次代数体 K の素イデアルの一つを $\mathfrak{p}$, 定数 $0 < c < 1$ を固定する. $\alpha \in K^\times$ の素イデアル分解が $(\alpha) = \mathfrak{p}^e\mathfrak{a}$, $(\mathfrak{p}, \mathfrak{a}) = 1$ であるとき, $|\alpha| = c^e$ と定義するとこれは非アルキメデス付値となる. 逆に $|\cdot|$ を K の非アルキメデス付値とすれば $\mathfrak{p} := \{x \in \mathcal{O}_K \mid |x| < 1\}$ は K の素イデアルとなる. このようにして K の非アルキメデス付値の同値類と K の素イデアルが 1:1 に対応する. この対応を通して, 付値の同値類 (と素イデアル) を**有限素点**という.

埋め込み $\sigma : K \to \mathbb{C}$ に対して $|\cdot| : K \to \mathbb{R}; x \mapsto |x^\sigma|$ はアルキメデス付値となる. 複素共役を $\bar{z}$ で表すことにすると $|\bar{x}^\sigma| = \overline{|x^\sigma|} = |x^\sigma|$ であるから, σ と σ^- は同値な埋め込みであると考えることにする. そのようにして K のアルキメデス付値の同値類と埋め込み $\sigma : K \to \mathbb{C}$ の同値類が 1:1 に対応する. この対応を通して, それらの同値類を無限素点という. 特に $\sigma(K) \subset \mathbb{R}$ のときは実無限素点, $\sigma(K) \not\subset \mathbb{R}$ のときは虚無限素点という. $[K : \mathbb{Q}] = n$ で実無限素点の数を r_1, 虚無限素点の数を r_2 とすると $n = r_1 + 2r_2$ が成り立つのであった. そしてペア (r_1, r_2) を K の符号と呼んでいた.

Theorem 4.2 (ディリクレの単数定理)**.** 有限次代数体 K の符号を (r_1, r_2) とする. このとき $\mathcal{O}_K^\times / W_K$ は $\operatorname{rank} r_1 + r_2 - 1$ の自由 $\mathbb{Z}$ 加群, すなわち

$$\mathcal{O}_K^\times \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r_1 + r_2 - 1} \oplus W_K$$

が成り立つ.

Proof. ここでは証明の概略のみしか書かない. $r = r_1 + r_2 - 1$ とおき, $\sigma_1, \dots, \sigma_{r_1}$ を実無限素点, $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ を虚無限素点とする.

$$c_i = \begin{cases} 1 & (1 \leq i \leq r_1) \\ 2 & (r_1 + 1 \leq i \leq r_1 + r_2 = r + 1) \end{cases}$$

として準同型

$$\varphi : \mathcal{O}_K^\times \to \mathbb{R}^{r+1}; \varepsilon \mapsto \left(c_1 \log |\varepsilon^{(1)}|, \dots, c_{r+1} \log |\varepsilon^{(r+1)}| \right)$$

を考える. 補題 4.1 より $\operatorname{Ker} \varphi = W_K$ となり, 同じく補題 4.1 より

$$\operatorname{Im}\varphi \subset \left\{ (x_1, \dots, x_{r+1}) \in \mathbb{R}^{r+1} \mid x_1 + \cdots + x_{r+1} = 0 \right\}$$

となる. さらに証明は省略するが付値の独立性から, ある $\varepsilon_1, \dots, \varepsilon_r \in \mathcal{O}_K^\times$ が存在して

$$\begin{cases} \log |\varepsilon_i^{(i)}| > 1 & (1 \leq i \leq r) \\ \log |\varepsilon_i^{(j)}| < 1 & (i \neq j, j \leq r + 1) \end{cases}$$

が成り立つ. また, 任意の有界部分集合 $D \subset \mathbb{R}^{r+1}$ に対し $|D \cap \operatorname{Im}\varphi| < \infty$ となる (すなわち $\operatorname{Im}\varphi$ は $\mathbb{R}^{r+1}$ の離散部分群). 従って $\mathcal{O}_K^\times / W_K \cong \operatorname{Im}\varphi$ は $\operatorname{rank} r$ の自由 $\mathbb{Z}$ 加群となる. □

$\mathcal{O}_K^\times/W_K$ の代表系を K の**基本単数**または**基本単数系**という．K の基本単数系を $\varepsilon_1,\dots,\varepsilon_r$ とするとき, $(r+1)\times r$ 行列

$$A=\begin{pmatrix} c_1\log|\varepsilon_1^{(1)}| & \dots & c_1\log|\varepsilon_r^{(1)}| \\ \dots & \dots & \dots \\ c_{r+1}\log|\varepsilon_1^{(r+1)}| & \dots & c_{r+1}\log|\varepsilon_r^{(r+1)}| \end{pmatrix}$$

のランクは r である．A から任意に r 行を選んで作った r 次行列の行列式は, 行の取り方に依らず一定である．さらに基本単数系の選び方にも依らない．これを R_K で表し K の**単数基準 (レギュレーター)** という．

次に第 10 章で必要になる **S 単数**について述べる．K の無限素点全体からなる集合を S_∞ で表す．K の符号が (r_1,r_2) であれば $|S_\infty|=r_1+r_2$ である．K の素点 v に対応する付値を $|\cdot|_v$ で表す．S を S_∞ を含む K の素点の有限集合とする．S に含まれない任意の付値 v に対して $|\alpha|_v=1$ となるとき, α を S 単数といい

$$(\mathcal{O}_K^\times)^{(S)}:=\left\{\alpha\in K\mid {}^\forall v\notin S,\ |\alpha|_v=1\right\}$$

を **S 単数群**という．$(\mathcal{O}_K^\times)^{(S_\infty)}=\mathcal{O}_K^\times$ である．以下の定理もディリクレの単数定理と同様に証明される．

Theorem 4.3. $|S|=s$ ならば $(\mathcal{O}_K^\times)^{(S)}/W_K$ は $\operatorname{rank} s-1$ の自由 $\mathbb{Z}$ 加群である．

5　類数と単数の関係

Theorem 5.1. 有限次代数体 K の符号を (r_1,r_2) とし, W_K の位数を $w(K)$ で表すと以下が成り立つ．

$$h(K)R_K=\frac{w(K)\sqrt{|d(K)|}}{2^{r_1}(2\pi)^{r_2}}\prod_p\frac{1-p^{-1}}{\prod_{\mathfrak{p}|p}(1-N(\mathfrak{p})^{-1})}$$

第 II 部
無限次ガロア拡大

6　位相の導入

体の代数拡大 L/F がガロア拡大であるとは, 分離拡大かつ正規拡大であるときのことをいうのであった．すなわち

- ${}^\forall\alpha\in L$ の F 上最小多項式は重根を持たない．
- 任意の F の代数閉包への埋め込み $\sigma:F\to\bar{F}$ に対して $\sigma(L)\subset L$.

を満たすことをいう．ガロア拡大 L/F が有限次拡大であれば, ガロア群 $G(L/F)$ と L/F の中間体の間に 1:1 の対応があるのだった．しかし無限次ガロア拡大の場合は 1:1 の対応は存在しない．実際に反例を構成してみよう．

Proposition 6.1. $\mathrm{id}\neq\varphi\in G:=\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ に対して $\langle\varphi\rangle=\{\varphi^n\mid n\in\mathbb{Z}\}$ は G の部分群である．このとき $\langle\varphi\rangle$ も G も $\mathbb{F}_p$ の固定群であるが, $\langle\varphi\rangle\subsetneq G$ である．

Proof. 具体的に $\psi\in G\setminus\langle\varphi\rangle$ を構成する．まず数列 $\{a_n\}_n$ で

$$m|n\Longrightarrow a_n\equiv a_m \bmod m$$

という条件を満たすものを一つ取る．($\bar{\mathbb{Z}}=\varprojlim_n\mathbb{Z}/n\mathbb{Z}$ の元を一つ取ると言っている．例としては, $n=n'p^{v_p(n)}$ $((n',p)=1)$ と書き, $1=n'x_n+p^{v_p(n)}y_n$ なる $x_n,y_n\in\mathbb{Z}$ を取る．このとき $a_n=n'x_n$ が上の条件を満たす．本当に満たす？？) さて, $\psi_n:=\varphi^{a_n}|_{\mathbb{F}_{p^n}}$ とすると $m|n$, すなわち $\mathbb{F}_{p^m}\subset\mathbb{F}_{p^n}$ のとき

$$\psi_n|_{\mathbb{F}_{p^m}}=\varphi^{a_n}|_{\mathbb{F}_{p^m}}=\varphi^{a_m}|_{\mathbb{F}_{p^m}}=\psi_m$$

となることが分かる．従って ψ_n らを $\bar{\mathbb{F}}_p$ まで延長すれば $\psi \in Gal(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ が定まる．ここで ($\psi \notin \langle\varphi\rangle$ を示したいので)$\psi = \varphi^a$ と書けたと仮定する．このとき両辺を $\mathbb{F}_{p^n}$ まで制限すれば

$$\psi|_{\mathbb{F}_{p^n}} = \varphi^{a_n}|_{\mathbb{F}_{p^n}} = \varphi^a|_{\mathbb{F}_{p^n}}$$

が成り立つ．このことは, $^\forall n \in \mathbb{Z}$ について $a_n \equiv a \bmod n$ なる $a \in \mathbb{Z}$ が存在するということを意味する．しかしそのような $a \in \mathbb{Z}$ は明らかに存在しないので矛盾． □

上の反例より, $G(L/F)$ に Krull 位相という位相を入れ, $G(L/F)$ の閉部分群と L/F の中間体の間の対応が 1:1 であることを示す．以下では L/F を無限次ガロア拡大とする．

まず

$$\mathcal{F} = \{G(L/K) \mid K \text{ は } [K:F] < \infty \text{ なる中間体 }\} = \{G(L/F(\alpha)) \mid \alpha \in L\}$$

とする．このとき任意の $g \in G(L/F)$ の基本近傍系が $g\mathcal{F}$ となるような位相が $G(L/F)$ に定まる．基本近傍系から定まる位相の開集合は

$$\mathcal{O} = \left\{U \subset G(L/F) \mid {}^\forall g \in U, {}^\exists gG(L/K) \in g\mathcal{F} \text{ s.t. } gG(L/K) \subset U\right\}$$

となるのだった．

基本近傍系の公理を満たすことを示す．

[$g\mathcal{F} \neq \varnothing, gG(L/K) \in g\mathcal{F}$ ならば $g \in gG(L/K)$] $\mathrm{id} \in \mathcal{F}$ より $g\,\mathrm{id} \in g\mathcal{F}$ なので前者は ok. $gG(L/K) \in g\mathcal{F}$ に対して $g = g\,\mathrm{id} \in gG(L/K)$ より後者も ok.

[$gG(L/K_1), gG(L/K_2) \in g\mathcal{F}$ ならば, ある $gG(L/K_3) \in g\mathcal{F}$ が存在して $gG(L/K_3) \subset gG(L/K_1) \cap gG(L/K_2)$]
UTF00A0$K_3 = K_1 \cdot K_2$ とすればよい.

[$gG(L/K_1) \in g\mathcal{F}$ に対して, ある $gG(L/K_2) \in g\mathcal{F}$ が存在して, 任意の $g\sigma \in gG(L/K_2)$ に対して $g\sigma G(L/K_3) \in g\sigma\mathcal{F}$ で $g\sigma G(L/K_3) \subset gG(L/K_1)$ となるものがある]
UTF00A0 ややこしいのでゼミでは図を描いて説明したい．要するに, g の近傍 $G(L/K_1)$ の中にすっぽり収まるような g の近傍 $g(L/K_2)$ が取れるということを示せばよい．$\alpha \in L \setminus K_1$ を一つ取る．(L/F は無限次拡大なので取れる．) このとき $K_2 = K_1(\alpha)$ とすればよい．実際 $gG(L/K_2) \subset gG(L/K_1)$ となって, 任意の $g\sigma \in G(L/K_2)$ に対して $g\sigma G(L/K_2) \in g\sigma\mathcal{F}$ に対して $g\sigma G(L/K_2) \subset g(L/K_1)$ となる．

Lemma 6.2. $G(L/F)$ は上記の Krull 位相によりハウスドルフ位相群となる．

Proof. まずハウスドルフであることを示す．$\sigma \neq \tau \in G$ に対して σ の開近傍 σU と τ の開近傍 τV が存在して $\sigma U \cap \tau V = \varnothing$ であることを示せばよい．まず $\sigma \neq \tau$ より $(\sigma^{-1}\tau)(\alpha) \neq \alpha$ なる $\alpha \in L$ が存在する．このとき $U = V = G(L/F(\alpha)) \in \mathcal{F}$ とおく．$x = \sigma u_1 = \tau u_2 \in \sigma U \cap \tau U$ が取れると仮定する．このとき $\sigma^{-1}\tau = u_1 u_2^{-1} \in U$ より$\sigma^{-1}\tau$ は $F(\alpha)$ を固定する．しかしこれは $\sigma^{-1}\tau(\alpha) \neq \alpha$ に矛盾．よって $\sigma U \cap \tau U = \varnothing$ である．

位相群であることを示す．まず演算

$$\varphi : G(L/F) \times G(L/F) \to G(L/F); (g,h) \mapsto gh$$

が連続写像であることを示す．それは gh の基本近傍 $ghG(L/K)$ の引き戻しが (g,h) の基本近傍であればよい．ここで, $\varphi(gG(L/K), hG(L/K)) = gG(L/K) \cdot hG(L/K) = ghG(L/K)$ であることから確かに $ghG(L/K)$ の引き戻しが (g,h) の基本近傍 $(gG(L/K), hG(L/K))$ となっている．ただし, $gG(L/K) \cdot hG(L/K) = ghG(L/K)$ は $G(L/K) \lhd G(L/F)$ であることより従う．次に逆元を取る写像

$$\psi : G(L/F) \to G(L/F); g \mapsto g^{-1}$$

が連続写像であることを示す．g^{-1} の近傍 $g^{-1}G(L/K)$ の引き戻しは $gG(L/K)$ である．何故ならば, $\psi(gG(L/K)) = (gG(L/K))^{-1} = g^{-1}G(L/K)$ となるからである．これも, $G(L/K) \lhd G(L/F)$ より従う．以上より $G(L/F)$ は Krull 位相に関してハウスドルフ位相群である． □

Lemma 6.3. $H \leq G$ による L の固定体を $K := L^H$ とする．このとき $G(L/K) = \bar{H}$ である．

Proof. $[G(L/K) \supset \bar{H}]$ $^\forall\sigma \in \bar{H}$ を一つ取る．(σ は $^\forall\alpha \in K$ を固定すればよい．) σ の取り方と $\bar{H}$ の定義から，σ の開近傍と H の交わりは空でない．従って $U = G(L/F(\alpha)) \in \mathcal{F}$ とすれば $H \cap \sigma U \neq \varnothing$ である．よって $\tau \in H \cap \sigma U$ が取れる．このとき $\sigma \in \tau U^{-1} = \tau U$ であって，$\tau \in H$ より τ は α を固定，U の元も α を固定する．従って σ も α を固定する．で ok.

$[G(L/K) \subset \bar{H}]$ $^\forall\sigma \in G(L/K)$ を一つ取る．(任意の $U \in \mathcal{F}$ に対して $H \cap \sigma U \neq \varnothing$ であることを示せばよい．) $\alpha \in L$ を取り $U = G(L/F(\alpha))$ と書く．(本来は有限生成，すなわち $F(\alpha_1, \ldots, \alpha_n)$ とするべきだが，一元生成と仮定しても今後の議論に影響はない．)$K(\alpha)/K$ のガロア閉包を N とおく．$G(L/K) \twoheadrightarrow G(N/K)$ における H の像を H' とすると $K \subset N^{H'} \subset L^H = K$ より $K = N^{H'}$ が分かる．N/K は有限次ガロア拡大であるから $H' = G(N/K)$ となる．よって $G(L/K) \ni \sigma \mapsto \sigma' \in G(N/K) = H'$となる$\sigma' \in H'$ に対してその引き戻しを考えることで $\tau \in H$ で $\tau(\alpha) = \sigma(\alpha)$ なるものが存在する．従って $\sigma^{-1}\tau \in U$ となり $\tau \in \sigma U$，つまり $\tau \in H \cap \sigma U$ で ok. □

Lemma 6.4. K を L/F の中間体とし，$H = G(L/K)$ とおくと，H は $G = G(L/F)$ の閉部分群であり $L^H = K$．

Proof. $[K \subset L^H]$ $^\forall x \in K$ は H によって固定されるので $x \in L^H$ となり ok.

$[K \supset L^H]$ 示すことは「$^\forall\sigma \in H$ に対して $\sigma(\alpha) = \alpha$ ならば $\alpha \in K$」であるが，その対偶「($\alpha \in L$ が)$\alpha \notin K$ ならば $\sigma(\alpha) \neq \alpha$ なる $\sigma \in H$ が存在する」を示すことにする．$\alpha \notin K$ と仮定する．$f(X) \in K[X]$ を α の K 上最小多項式とすれば $\deg f \geq 2$ であり，α と異なる $f(X)$ の根 α' が存在する．$\sigma : K(\alpha) \hookrightarrow L; \alpha \mapsto \alpha'$ と定義し，定義域を L まで延長すれば $\sigma \in G(L/K) = H$ であり $\sigma(\alpha) \neq \alpha$ となり ok.

$[H \subset G$ は閉部分群]

UTF00A0H の G における補集合を H^c で表す．(H^c が開部分群であることを示せばよい．) $\sigma \in H^c$ を一つ取ると，ある $\alpha \in K$ が存在して $\sigma(\alpha) \neq \alpha$ となる．このとき $U = G(L/F(\alpha)) \in \mathcal{F}$ であり，$^\forall\tau \in U$ に対して当然 $\sigma\tau \in H^c$ である．従って $\sigma U \subset H^c$ となり H^c が開近傍を含むから開集合．ok. □

Theorem 6.5. L/F をガロア拡大とする．$\mathcal{G}$ を $G(L/F)$ の閉部分群全体，$\mathcal{K}$ を L/F の中間体全体とする．写像 Ψ と Φ を

$$\Phi : \mathcal{G} \to \mathcal{K}; H \mapsto L^H$$
$$\Psi : \mathcal{K} \to \mathcal{G}; K \mapsto G(L/K)$$

と定義するとこれらは互いに逆写像である． つまり，$G = G(L/F)$ の閉部分群 H と L/F の中間体 K は，$H = G(L/K), K = L^H$ の関係で 1:1 に対応する．

Proof. 補題 6.3 を用いることで $\Psi \circ \Phi(H) = \Psi(L^H) = G(L/L^H) = \bar{H} = H$ となって ok. ただし H は閉部分群として取っているので $\bar{H} = H$ に注意．同様に補題 6.4 を用いることで $\Phi \circ \Psi(K) = \Phi(G(L/K)) = L^{G(L/K)} = K$ となり ok. □

Lemma 6.6. 定理 6.5 において $H = G(L/K)$ と対応しているとき以下が成り立つ．

- $H \in \mathcal{G}$ のガロア群 $G(L/K)$ としての位相と，部分集合 $H \leq G$ としての相対位相は一致する．
- $H \triangleleft G \iff K/F$: ガロア拡大．このとき自然な位相同型 $G/H \cong G(K/F)$ が成り立つ．ただし G/H には商位相を入れる．

Proof. (1) 単位元の近傍が一致することだけ示す．$1 \in G(L/K)$ の基本近傍系を同様に $\{G(L/M) \mid [M : K] < \infty\}$ とする．このとき "$1 \in G(L/K)$ の近傍" = "$1 \in G(L/F)$ の近傍 $\cap\, G(L/K)$" を示せばよい．$G(L/K) \supset G(L/M) \in$ (左辺) に対して $[M : F] < \infty$ であるから $G(L/M) \in$ (右辺) である．逆も同様に示せる．

(2) 前者の主張は雪江代数 2 の (有限次) ガロア理論の基本定理の証明と同様．後者の主張は位相群の準同型定理より従う． □

Theorem 6.7. L/F がガロア拡大であれば, ガロア群 $G = G(L/F)$ はコンパクト位相群である.

Proof. 略. 後に G が有限次ガロア拡大 $G(K/F)$ の射影極限として表せることを用いれば, チコノフの定理 (とか) よりコンパクトであることがすぐに従う. □

Lemma 6.8. K をガロア拡大 L/F の中間体とし, $H = G(L/K)$ とおく. このとき, $H \leq G = G(L/F)$ が開部分群 $\iff$ $[K : F] < \infty$ が成り立つ.

Proof. $[\Rightarrow]$ $H \leq G$ を開部分群とする. このとき G の開被覆 $G = \cup_{\sigma\in G}\sigma H$ が取れる. 定理 6.7 より G はコンパクトなので有限開被覆 $G = H \cup \cdots \cup \sigma_n H$ が取れる. 従って $[K : F] = [G : H] = n < \infty$ より ok.

$[\Leftarrow]$ $[G : H] = [K : F] < \infty$ より G の (有限) 剰余分解 $G = H \cup \cdots \cup \sigma_n H$ が得られる. 従って $H^c = \sigma_2 H \cup \cdots \cup \sigma_n H$ であり $\sigma_i H$ は閉部分群であるから H^c も閉, つまり H は開. □

7 射影極限としてのガロア群

次に, 適切な体の拡大列から $\mathbb{Z}_p$ 拡大を構成できることを示す.

Proposition 7.1. 体の代数拡大の列

$$F = F_0 \subset F_1 \subset F_2 \subset F_3 \subset \dots$$

で F_n/F が p^n 次巡回拡大であるものが存在するとする. このとき $L := \cup_{i=0}^{\infty} F_i$ に対し L/F は無限次ガロア拡大であり位相群としての同型 $G(L/F) \cong \mathbb{Z}_p$ が得られる.

Proof. $[Step1]$ L/F の有限次ガロア中間体は F_i の形のみであることを示す. そのような中間体は, 有限次分離拡大は単拡大であることから $\alpha \in \bar{F}$ を用いて $F(\alpha)$ と表せる. さらにある $n \in \mathbb{N}$ が存在して $F(\alpha) \subset F_n$ であり, F_n/F が p^n 次巡回拡大であること, 位数が p^n の巡回群の部分群は位数が p べきの巡回群であることから $F(\alpha) = F_i$ という形をしていることが分かり ok.

$[Step2]$ ある $\sigma \in G(L/F)$ により $G = \overline{(\sigma)}$ であることを示す. まず $G(F_1/F)(\cong \mathbb{Z}/p\mathbb{Z})$ の生成元を σ とする. これを $G(L/F)$ まで延長したものもまた σ と書くことにする. $H := (\sigma)$ とおき, $G = \overline{H}, L^H = F$ を示す. 無限次ガロアの基本定理より $L^H = F$ のみ示せばよい. $L^H \supset F$ は自明なので, 「$\alpha \in L$ が $\sigma(\alpha) = \alpha$ を満たすならば $\alpha \in F$」を示せばよい. $\sigma(\alpha) = \alpha$ と仮定すると, σ は $F(\alpha) = F_i$ 上の恒等写像である. あとは $i = 0$ であることを示せばよい. 簡単のため $i = 2$ と仮定する. このとき $\sigma|_{F_2} = \mathrm{id} \in G(F_2/F)$ であり, さらに $\sigma|_{F_2}|_{F_1} = \mathrm{id} \in G(F_1/F)$ となるが, σ を F_1 に制限すると $G(F_1/F)$ の生成元であったはずなので矛盾. このように一般の $i \neq 0$ で矛盾が生じるので, $i = 0$ となり ok.

$[Step3]$ $\varphi : \mathbb{Z}_p \ni \alpha \mapsto \sigma^\alpha \in G(L/F)$ が位相群としての同型であることを示す. ただし $\alpha = \lim a_n \in \mathbb{Z}_p$に対し $\sigma^\alpha := \lim \sigma^{a_n} \in G$ である. この極限が存在することをまず確認する. $1 \in G$ の可算基本近傍系を, $U_n := G(L/F_n)$ に対し $U_0 \supset U_1 \supset U_2 \supset \dots$ と取れる. このとき容易に

$$\begin{aligned}
\lim_{n\to\infty} \sigma^{a_n}\text{が存在} &\iff {}^\forall n \in \mathbb{N}, {}^\exists N \in \mathbb{N} \text{ s.t. } \lambda, \mu \geq N \Longrightarrow \sigma^{a_\lambda - a_\mu} \in U_n \\
&\iff {}^\forall n \in \mathbb{N}, {}^\exists N \in \mathbb{N} \text{ s.t. } \lambda, \mu \geq N \Longrightarrow a_\lambda - a_\mu \equiv 0 \bmod p^n \\
&\iff \lim_{n\to\infty} a_n = \alpha\text{が } \mathbb{Z}_p\text{の中で存在}
\end{aligned}$$

が分かる. (ただし $G(L/F)/G(L/F_n) \cong G(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$ より, $\sigma^a \in U_n$ であることと $a \equiv 0 \bmod p^n$ が同値であることに注意する.)

φ が準同型であることは容易に分かる. まず全射であることを示す. G は第一可算公理を満たすので, ${}^\forall\tau \in G = \overline{(\sigma)}$ は $\tau = \lim \sigma^{a_n}$ と表現できる. このとき $\varphi(\lim a_n) = \tau$ となり ok.

単射を示す. $\alpha = \lim a_n$ に対し $\sigma^a = \lim \sigma^{a_n} = 1$ と仮定する. このとき

$${}^\exists N \in \mathbb{N} \text{ s.t. } n \geq N \Longrightarrow \sigma^{a_n} \in U_n$$

が成り立つが, $\sigma^{a_n} \in U_n \iff a_n \equiv 0 \bmod p^n$ より $\lim a_n = 0$ が分かる.

φ と φ^{-1} が連続を示す. 特に $G(L/F)$ と $\mathbb{Z}_p$ の基本近傍が移り合うこと, すなわち $U_m = \varphi(p^m\mathbb{Z}_p)$ を示す.

$$x \in \varphi(p^m\mathbb{Z}_p) \iff {}^{\exists}p^m a \in p^m\mathbb{Z}_p \text{ s.t. } x = \varphi(p^m a)$$

であるが, $x = \varphi(p^m a) = \varphi(p^m \lim a_n) = \varphi(\lim p^m a_n) = \lim \sigma^{p^m a_n} = (\sigma^a)^{p^m}$ あることより

$$\begin{aligned} x \in \varphi(p^m\mathbb{Z}_p) &\iff x = 0 \text{ in } G(F_m/F) \cong \mathbb{Z}/p^m\mathbb{Z} \\ &\iff x \in G(L/F_m) = U_m \end{aligned}$$

となり ok. □

以上のように構成した拡大 L/F は $\mathbb{Z}_p$ 拡大と呼ばれる. ($G = G(L/F) = \bar{H} = \overline{(\sigma)}$ であったから, $\mathbb{Z}_p$ 拡大のガロア群は一元生成の閉包 $\overline{\langle\gamma\rangle}$ で表せることが分かる. この γ を**位相的生成元**という.) これまでの議論の逆も成り立つ.

Proposition 7.2. L/F を無限次ガロア拡大で, 位相群としての同型 $G(L/F) \cong \mathbb{Z}_p$ が成り立つものとする. このとき体の拡大列

$$F = F_0 \supset F_1 \supset F_2 \supset \dots$$

で F_n/F が p^n 次巡回拡大となるものが存在する.

Proof. $\mathbb{Z}_p$ の非自明な閉部分群は $p^n\mathbb{Z}_p$ の形のみであるから, 対応する $G(L/F)$ の閉部分群を H_n とし, さらに H_n の固定体を F_n とおく. このとき $G(F_n/F) \cong G(L/F)/G(L/F_n) \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ より, F_n/F は p^n 次巡回拡大である. □

以下では, 無限次ガロア群が副有限群であること, すなわち有限群の射影極限として表されることを証明する. それが次の補題.

Lemma 7.3. L/F をガロア拡大, L/F の中間体の集合 $\mathcal{K}$ が以下の性質をもつとする.

- $K \in \mathcal{K}$ ならば K/F は L/F の有限次部分ガロア拡大.
- ${}^{\forall}K_1, K_2 \in \mathcal{K}, {}^{\exists}K \in \mathcal{K}$ such that $K_1K_2 \subset K$.

このとき

$$G(L/F) \cong \varprojlim_{K\in\mathcal{K}} G(K/F)$$

が成り立つ. 特に $\mathcal{K}$ として有限次ガロア部分拡大の集合を取ることができる.

Proof. 前半の主張は証明無し. 後者の主張は以下の定理を参考. しかし証明がよく分からん. 明らかに単射って明らかじゃねえ！定理 7.4 を認めると, 正規閉部分群の属 $\{N_\mu\}$ として

$$\mathcal{F}' = \{G(L/K) \mid F \subset K \subset L,\ K/F : \text{有限次ガロア拡大}\}$$

を取る. $\mathcal{F}'$ 自身が 1 の基本近傍系となることに気をつければ, $\{N_\mu\}$ が満たすべき性質を満たすことはすぐに分かる. 従って G は $\lim_{G(L/K)\in\mathcal{F}'} G(L/F)/G(L/K) \cong \lim_{K/F:fin.Gal.\in\mathcal{F}'} G(K/F)$ の稠密な部分群と位相同型となる. さらに定理 6.7 より G はコンパクトであったから, $G \cong \lim_{K/F:fin.Gal.\in\mathcal{F}'} G(K/F)$ を得る. ($A \subset B$ で A が稠密かつコンパクトなら $A = B$?) □

Theorem 7.4. 位相群 G の正規閉部分群の族 $\{N_\mu\}$ が以下を満たすとする.

- ${}^{\forall}N_\mu, N_\nu,\ {}^{\exists}N_\lambda$ s.t. $N_\lambda \subset N_\mu \cap N_\nu$.
- 任意の単位元の近傍 U に対し, ある N_μ が存在して $N_\mu \subset U$ となる.

このとき G は $\varprojlim_\mu G/N_\mu$ の稠密な部分群と位相同型である.

Proof. 分からなすぎて省略. どこが分からないかというと,

$$G \to \varprojlim_{\mu} G/N_\mu; x \mapsto (xN\mu)_\mu$$

が明らかに単射であるというところ. 準同型であることは明らかだから, $(xN\mu)_\mu = 0$, すなわち任意の μ に対して $x \in N_\mu$, すなわち $x \in \cap_\mu N_\mu$ と仮定する. このとき $x = 1$, すなわち $\cap_\mu N_\mu = \{1\}$ を示したい. $\{N_\mu\}$ の条件からこれが導けるか？ □

Example 7.5 ($\mathbb{Q}_1$ の円分 $\mathbb{Z}_p$ 拡大)**.** 以下では簡単のため p を奇素数とする. このとき $\mathbb{Q}_1 := \mathbb{Q}(\zeta_p), \mathbb{Q}_n := \mathbb{Q}(\zeta_{p^{n+1}})$ とおく. このとき $\mathbb{Q}_\infty := \cup_{i=1}^\infty \mathbb{Q}_n$ とすると $\mathbb{Q}_\infty/\mathbb{Q}_1$ は $\mathbb{Z}_p$ 拡大である. 実際,

$$G(\mathbb{Q}_n/\mathbb{Q}_1) \cong G(\mathbb{Q}_n/\mathbb{Q})/G(\mathbb{Q}_1/\mathbb{Q}) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times/(\mathbb{Z}/p\mathbb{Z})^\times \cong ((\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p^n\mathbb{Z})/(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/p^n\mathbb{Z}$$

となる. このように構成した $\mathbb{Z}_p$ 拡大 $\mathbb{Q}_\infty/\mathbb{Q}_1$ を, $\mathbb{Q}_1$ の**円分 $\mathbb{Z}_p$ 拡大**と呼ぶ.

Example 7.6 (岩澤の円分 $\mathbb{Z}_p$ 拡大)**.** 上と同様に p を奇素数とする. $\mathbb{Q}_n := \mathbb{Q}(\zeta_{p^n})$ とする. $\mathbb{Q}_\infty := \cup_{i=1}^\infty \mathbb{Q}_n$ とすると $\mathbb{Q}_\infty/\mathbb{Q}$ は $\mathbb{Z}_p$ 拡大にならない. 実際,

$$G(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p^{n-1}\mathbb{Z}$$

であるから

$$G(\mathbb{Q}_\infty/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times \times \varprojlim_n \mathbb{Z}/p^{n-1}\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p \neq \mathbb{Z}_p$$

となるためである. しかし改めて $\mathbb{Q}_n := (G(\mathbb{Q}_n/\mathbb{Q})$ の内, $(\mathbb{Z}/p\mathbb{Z})^\times$の作用で不変な部分$) \cong \mathbb{Z}/p^{n-1}\mathbb{Z}$ とすれば $G(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$ となり $\mathbb{Q}$ の $\mathbb{Z}_p$ 拡大 $\mathbb{Q}_\infty$ が得られる. これを**岩澤の円分 $\mathbb{Z}_p$ 拡大**という.

Example 7.7 (代数体 k の円分 $\mathbb{Z}_p$ 拡大)**.** ここでも p を奇素数とする. 一般の代数体 k に対して $k_\infty := k\mathbb{Q}_\infty$ とする. ただし $\mathbb{Q}_\infty/\mathbb{Q}$ は岩澤の円分 $\mathbb{Z}_p$ 拡大である. このとき k_∞/k は $\mathbb{Z}_p$ 拡大である. 実際, (無限次) ガロアの推進定理より

$$G(k_\infty/k) = G(k\mathbb{Q}_\infty/k) \cong G(\mathbb{Q}_\infty/k \cap \mathbb{Q}) = G(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$$

となる.

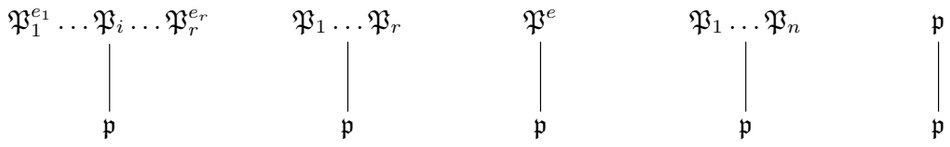
第 III 部
無限次拡大の分岐理論

8　有限次拡大の分岐理論

L/K を n 次拡大とすると, K の素イデアル $\mathfrak{p}$ は L において

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_r^{e_r}$$

と素イデアル分解される. $[\mathbb{F}_{\mathfrak{P}_i} : \mathbb{F}_{\mathfrak{p}}] =: f_i$, すなわち $\mathrm{N}_{L/K}(\mathfrak{P}_i) = \mathfrak{p}^{f_i}$ とすれば $n = \sum_{i=1}^{r} e_i f_i$ が成り立つことが知られている. $\mathfrak{P}_i$ を $\mathfrak{p}$ の上にある素イデアル, e_i を $\mathfrak{P}_i$ の**分岐指数**という.



$\mathfrak{P}_i$: 不分岐　　$\mathfrak{p}$: 不分岐　　$\mathfrak{p}$: 不分解　　$\mathfrak{p}$: 完全分解　　$\mathfrak{p}$: 惰性

以下で示すように, L/K がガロア拡大ならば $\mathfrak{p}\mathcal{O}_L$ の素イデアル分解は単純な形となる. 結果から言えば $e_1 = \cdots = e_r, f_1 = \cdots = f_r$ となる. 従って $[L : K] = efr$ $(e = e_i, f = f_i)$ を得る. (cf. Corollary 8.4)

Lemma 8.1. 環 A のイデアル $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ が $\mathfrak{a}_i + \mathfrak{a}_j = A$ $(i \neq j)$ を満たすとき, 任意の $x_1, \dots x_n \in A$ に対し, ある $x \in A$ が存在して $x \equiv x_i \bmod \mathfrak{a}_i$ $({}^\forall i)$ が成り立つ.

Proof. 中国剰余定理. □

Lemma 8.2. K の素イデアル $\mathfrak{p}$ の上にある L の素イデアルの一つを $\mathfrak{P}$ とする. このとき $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

Proof. 明らかに $\mathfrak{p} \subset \mathfrak{P} \cap \mathcal{O}_K \subset \mathcal{O}_K$ であり, $\mathcal{O}_K$ の素イデアルは全て極大イデアルであったから $\mathfrak{P} \cap \mathcal{O}_K$ は $\mathfrak{p}$ または $\mathcal{O}_K$ である. しかし $\mathfrak{P} \cap \mathcal{O}_K = \mathcal{O}_K$ とすると $1 \in \mathcal{O}_K$ より $1 \in \mathfrak{P}$, すなわち $\mathfrak{P} = \mathcal{O}_L$ となるが, $\mathfrak{P}$ が素イデアルであることに矛盾. □

Proposition 8.3. L/K を有限次代数体の有限次ガロア拡大とする. $\mathfrak{p}$ を K の素イデアル, $\mathfrak{P}, \mathfrak{P}'$ を $\mathfrak{p}$ の上にある L の素イデアルとすると, $\mathfrak{P}^\sigma = \mathfrak{P}'$ なる $\sigma \in G(L/K)$ が存在する.

Proof. 背理法で示す. ${}^\forall\sigma \in G(L/K)$ に対し $\mathfrak{P}^\sigma \neq \mathfrak{P}'$ と仮定して矛盾を導く. $\mathfrak{P}^\sigma$ と $\mathfrak{P}'$ は互いに素であるので補題 8.1 において $A = \mathcal{O}_L, \mathfrak{a}_i = \mathfrak{P}^\sigma, \mathfrak{a}_j = \mathfrak{P}'$ として適用すれば

$$x \equiv 0 \bmod \mathfrak{P}', \ x \equiv 1 \bmod \mathfrak{P}^\sigma \ ({}^\forall\sigma \in G(L/K))$$

となる $x \in \mathcal{O}_L$ が存在する. 後者の条件より $x \notin \mathfrak{P}^\sigma$ であるから $x^{\sigma^{-1}} \notin \mathfrak{P}$ となり, さらに σ は $G(L/K)$ 全体を動くから $x^\sigma \notin \mathfrak{P}$ としてよい. $({}^\forall\sigma \in G(L/K))$ 従って

$$N_{L/K}(x) = \prod_{\sigma \in G(L/K)} x^\sigma \notin \mathfrak{P}$$

が成り立つ. よって補題 8.2 より $N_{L/K}(x) \notin \mathfrak{p}$ となる. しかし $x \in \mathfrak{P}'$ であったから $N_{L/K}(x) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$ となって矛盾. □

Corollary 8.4. L/K が有限次代数体の n 次ガロア拡大のとき, K の素イデアル $\mathfrak{p}$ は L において

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \dots \mathfrak{P}_r)^e, \ N_{L/K}(\mathfrak{P}_i) = \mathfrak{p}^f$$

と素イデアル分解される. 特に $n = efr$ が成り立つ.

Proof. $\mathfrak{P}_1, \mathfrak{P}_2$ を $\mathfrak{p}$ の上にある素イデアルとして, $e_1 = e_2$ を示せばよい. 命題 8.3 より, ある $\sigma \in G(L/K)$ が存在して $\mathfrak{P}_1^\sigma = \mathfrak{P}_2$ が成り立つ. σ は K の元を固定するので $\mathfrak{p}^\sigma = \mathfrak{p}$, さらに $\sigma : \mathcal{O}_L \to \mathcal{O}_L$ は全単射より $(\mathfrak{p}\mathcal{O}_L)^\sigma = \mathfrak{p}\mathcal{O}_L$ であることを用いると

$$\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots = \mathfrak{p}\mathcal{O}_L = (\mathfrak{p}\mathcal{O}_L)^\sigma = \sigma(\mathfrak{P}_1)^{e_1}\sigma(\mathfrak{P}_2)^{e_2} \cdots = \mathfrak{P}_2^{e_1} \dots$$

より $e_1 = e_2$ が分かる.

次に $f_1 = f_2$ を示す.

$$\varphi : \mathcal{O}_L/\mathfrak{P}_1 \to \mathcal{O}_L/\mathfrak{P}_1^\sigma; x + \mathfrak{P}_1 \mapsto x^\sigma + \mathfrak{P}_1^\sigma$$
$$\psi : \mathcal{O}_L/\mathfrak{P}_1^\sigma \to \mathcal{O}_L/\mathfrak{P}_1; x + \mathfrak{P}_1^\sigma \mapsto x^{\sigma^{-1}} + \mathfrak{P}_1$$

が well-defined で互いに逆写像であればよい. 逆写像であることは容易に分かり, well-defined も

$$x - y \in \mathfrak{P}_1 \Longrightarrow x^\sigma - y^\sigma \in \mathfrak{P}_1^\sigma$$
$$x - y \in \mathfrak{P}_1^\sigma \Longrightarrow x^{\sigma^{-1}} - y^{\sigma^{-1}} \in \mathfrak{P}_1$$

より分かる. □

Corollary 8.5. L/K を有限次代数体の n 次ガロア拡大とする. L のイデアル $\mathfrak{a}$ の素因子全てが L/K で不分岐であり, $\mathfrak{a}$ が $G(L/K)$ の作用で不変ならば, $\mathfrak{a}$ は K のイデアルである.

Proof. 明らか. □

L/K をガロア拡大, $G = G(L/K)$ をガロア群とし, K の素イデアル $\mathfrak{p}$ が

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \dots \mathfrak{P}_r)^e,\ N_{L/K}(\mathfrak{P}_i) = \mathfrak{p}^f$$

と素イデアル分解されたとする. $\mathfrak{P}_i$ の一つを $\mathfrak{P}$ と書くことにすると

$$D_\mathfrak{P} = \{\sigma \in G \mid \mathfrak{P}^\sigma = \mathfrak{P}\}$$

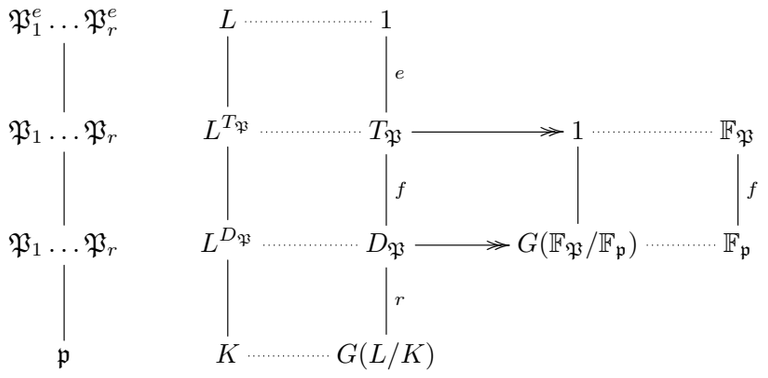
を $\mathfrak{P}$ の**分解群**という. このとき $\#G/D_\mathfrak{P} = r$ であることが示せる. $\mathbb{F}_\mathfrak{P} = \mathcal{O}_L/\mathfrak{P}, \mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ とおくと, $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ は f 次ガロア拡大であり, 自然な全射準同型 $\varphi : D_\mathfrak{P} \to G(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ が誘導される. $T_\mathfrak{P} = \mathrm{Ker}\varphi$, すなわち

$$T_\mathfrak{P} = \left\{\sigma \in D_\mathfrak{P} \mid {}^\forall x \in \mathcal{O}_L,\ x^\sigma \equiv x \bmod \mathfrak{P}\right\}$$

を $\mathfrak{P}$ の**惰性群**という. このとき $\#T_\mathfrak{P} = e$ であることが示せる. 特に

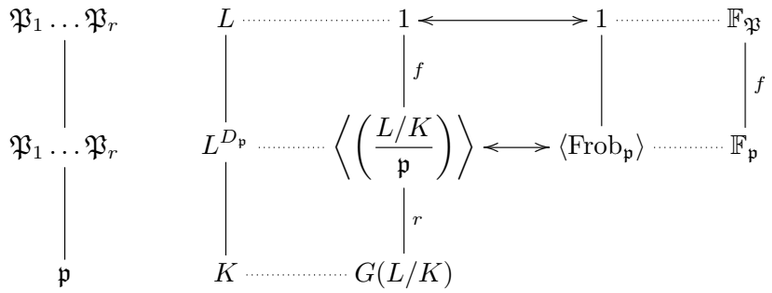
$$\mathfrak{P} \text{ が不分岐} \iff e = 1 \iff T_\mathfrak{P} = 1$$

という同値が成り立つ. これらの関係を図にしたのが以下である.



$\mathfrak{P}, \mathfrak{P}'$ を $\mathfrak{p}$ の上の異なる L の素イデアルとすると $\mathfrak{P}^\tau = \mathfrak{P}'$ なる $\tau \in G(L/K)$ が存在するのであった. このとき $D_{\mathfrak{P}'} = \tau D_{\mathfrak{P}} \tau^{-1}, T_{\mathfrak{P}'} = \tau T_{\mathfrak{P}} \tau^{-1}$ であることが分かる. 従って $\mathfrak{P}_i$ が不分岐であると言わずに $\mathfrak{p}$ が不分岐であると言っても差し支えない. 特に L/K がアーベル拡大のときは $D_{\mathfrak{P}'} = D_{\mathfrak{P}}, T_{\mathfrak{P}'} = T_{\mathfrak{P}}$ であるから, $\mathfrak{p}$ の分解群 $D_{\mathfrak{p}}$, 惰性群 $T_{\mathfrak{p}}$ といってもよい.

$\mathfrak{p}$ がアーベル拡大 L/K で不分岐のとき, $T_{\mathfrak{p}} = 1$ であるから $\varphi : D_{\mathfrak{p}} \to G(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ が全単射となり, さらに有限体のガロア群は (Frobenius と呼ばれる生成元 $\mathrm{Frob}_{\mathfrak{p}}$ により生成される) 巡回群であるので $D_{\mathfrak{p}}$ も巡回群となることが分かる. この $D_{\mathfrak{p}}$ の生成元を $\left(\frac{L/K}{\mathfrak{p}}\right)$ と書き, フロベニウス自己同型という. (アーベル拡大という仮定は, $\mathfrak{P}, \mathfrak{P}'$ の取り方に依らないことのために必要. アーベル拡大でなければ $\left(\frac{L/K}{\mathfrak{P}'}\right) = \tau \left(\frac{L/K}{\mathfrak{P}}\right) \tau^{-1}$ のようになる.) これらの状況, すなわち L/K がアーベル拡大で $\mathfrak{p}$ が不分岐である状況を図にしたのが以下である.



次に無限素点の分岐について考える. L/K を有限次拡大とする. K の埋め込み $\sigma : K \to \mathbb{C}$ は L の埋め込み $\tilde{\sigma} : L \to \mathbb{C}$ に延長できる. $\tilde{\sigma}$ が L/K で分岐するということを, $\sigma(K) \subset \mathbb{R}$ かつ $\tilde{\sigma}(L) \not\subset \mathbb{R}$ であることと定義する. L/K がガロア拡大であれば $\tilde{\sigma}$ の分解群と惰性群を

$$T_{\tilde{\sigma}} = D_{\tilde{\sigma}} = \{\tau \in G(L/K) \mid \tilde{\sigma}\tau = \tilde{\sigma} \text{または} \tilde{\sigma}\tau = \bar{\tilde{\sigma}}\}$$

と定義する.

Proposition 8.6. $T_{\tilde{\sigma}}$ の位数は 1 または 2 であり, $\tilde{\sigma}$ が不分岐 $\iff T_{\tilde{\sigma}} = 1$ が成り立つ.

Proof. $^\forall \tau \in T_{\tilde{\sigma}}$ を一つ取る. $\tilde{\sigma}(x) \in \mathbb{R}$ なる $x \in L$ に対しては

$$\tilde{\sigma}(\tau(x)) = \tilde{\sigma}(x) \text{ i.e. } \tau(x) = x$$
$$\tilde{\sigma}(\tau(x)) = \overline{\tilde{\sigma}(x)} = \sigma(x) \text{ i.e. } \tau(x) = x$$

となって τ の位数は 1 である. 次に $\tilde{\sigma}(x) \notin \mathbb{R}$ なる $x \in L$ に対しては

$$\tilde{\sigma}(\tau^2(x)) = \tilde{\sigma}(\tau(x)) = \tilde{\sigma}(x) \text{ i.e. } \tau^2(x) = x$$
$$\tilde{\sigma}(\tau^2(x)) = \overline{\tilde{\sigma}(\tau(x))} = \tilde{\sigma}(x) \text{ i.e. } \tau^2(x) = x$$

となることから従う. □

Example 8.7. $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2})$ とする. このとき K の無限素点は $\sigma = \mathrm{id}$ のみである. σ を L に延長する方法は二つあり, $\tilde{\sigma} = \mathrm{id}$ と $\tilde{\sigma}(a + b\sqrt{2}) = a - b\sqrt{2}$ である. いずれにしろ取る値は実数であるから σ は L/K で不分岐である.

Example 8.8. $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{-1})$ とする. K の唯一の無限素点 $\sigma = \mathrm{id}$ に対して, これを L に延長する方法は二つあり, $\tilde{\sigma} = \mathrm{id}$ と $\tilde{\sigma}(a + b\sqrt{-1}) = a - b\sqrt{-1}$ である. いずれにしろ $\tilde{\sigma}(L) \not\subset \mathbb{R}$ であるから分岐する.

9　無限次拡大の分岐理論

これまでの考察を無限次ガロア拡大または無限次代数体の場合に拡張したい．しかし無限次代数体においては素イデアル分解の一意性は成立しない．そこで惰性群を用いて分岐を定義する．以下, K を無限次代数体とする．K の素点は有限次と同じように定義する．(無限次代数体の整数環も同様に定義され, それは (Dedekind) 整域だから素イデアルも定義でき, 無限素点もただの $\mathbb{C}$ への埋め込み.)

Definition 9.1. L/K を (有限次とは限らない) ガロア拡大とする．K の素点 v とその上にある L の素点 w に対し, 惰性群 T_w を有限次の場合と同様に以下のように定義する．

$$T_w = \left\{\sigma \in G(L/K) \mid {}^\forall x \in \mathcal{O}_L,\ x^\sigma \equiv x \bmod w\right\}$$

L の素点 w の分岐指数を $\#T_w$ で定義し, w が不分岐であることを $T_w = 1$ で定義する．

次に L/K がガロア拡大でない場合を考える．体の拡大列 $\mathbb{Q} \subset K \subset L \subset \bar{\mathbb{Q}}$ に対して $\bar{\mathbb{Q}}/L, \bar{\mathbb{Q}}/K$ はガロア拡大であるから, $\bar{\mathbb{Q}}$ の素点 w に対する惰性群を考えることができる．

Definition 9.2. L/K をガロアとは限らない体の拡大, v を K の素点とする．v の $\bar{\mathbb{Q}}$ への任意の延長 w を取り, $T = T_w \subset G(\bar{\mathbb{Q}}/\mathbb{Q})$ を w の $\bar{\mathbb{Q}}/\mathbb{Q}$ に対する惰性群とする．このとき一般に以下が成り立つ．

$$T \cap G(\bar{\mathbb{Q}}/L) \subset T \cap G(\bar{\mathbb{Q}}/K).$$

v が L/K で不分岐であることを, 上の等号が成り立つとき, すなわち $T \cap G(\bar{\mathbb{Q}}/L) = T \cap G(\bar{\mathbb{Q}}/K)$ が成り立つことと定義する．逆に v が L/K で分岐することを, 不分岐でないこととして定義する．

以下で, $T \cap G(\bar{\mathbb{Q}}/L) \subset T \cap G(\bar{\mathbb{Q}}/K)$ が成り立つこと, この定義が有限次の場合と矛盾しないことを見る． まず ${}^\forall\sigma \in T \cap G(\bar{\mathbb{Q}}/L)$ を一つ取る．$\sigma \in T$ は明らかなので $\sigma \in G(\bar{\mathbb{Q}}/K)$, すなわち σ は K を固定することを見ればよい．しかし $K \subset L$ であること, σ は L を固定することから明らか.

K を有限次代数体, L/K を有限次ガロア拡大, $\mathfrak{p}$ を K の素イデアル, $\mathfrak{P}$ を $\mathfrak{p}$ の上にある L の素イデアル, e を分岐指数とする．このとき

$$T_\mathfrak{P} \cap G(\bar{\mathbb{Q}}/L) = T_\mathfrak{P} \cap G(\bar{\mathbb{Q}}/K) = T_\mathfrak{P} \iff e = 1$$

を示せばよい．「⇒」を示す．任意に $\sigma \in T_\mathfrak{P}$ を一つ取ると, $x \in \mathcal{O}_L$ に対して $\sigma(x) \equiv x \bmod \mathfrak{P}$ となる．仮定 $(\sigma \in G(\bar{\mathbb{Q}}/L))$ より σ は L を固定するので $\sigma(x) = x$, すなわち $\sigma = \mathrm{id}$, すなわち $T_\mathfrak{P} = 1$ となって $e = 1$ が示された．逆に $e = 1$ とすると, 任意の $\sigma \in T_\mathfrak{P}$ は $\sigma = \mathrm{id}$ となるので当然 L の元も固定する．よって $\sigma \in T_\mathfrak{P} \cap G(\bar{\mathbb{Q}}/L)$ となって ok.

Lemma 9.3. $K \subset F \subset L, K \subset E$ とする．

- L/K が不分岐ならば, K 上の任意の埋め込み $\sigma : L \to \bar{\mathbb{Q}}$ に対し L^σ/K も不分岐.
- L/K が不分岐 $\iff$ L/F および F/K が不分岐.
- L/K が不分岐ならば LE/E も不分岐.

Proof. $L/F/K, E/K$ が無限次代数体の拡大の場合のみ示せば十分である．あとめんどくさいので有限素点についてのみ言及することにする．

[一つ目] K の任意の有限素点 v を一つ取り, $\bar{\mathbb{Q}}$ まで延長する．このとき仮定より

$$T_v \cap G(\bar{\mathbb{Q}}/L) = T_v \cap G(\bar{\mathbb{Q}}/K)$$

が成り立っている．示したいものは $T_v \cap G(\bar{\mathbb{Q}}/L^\sigma) = T_v \cap G(\bar{\mathbb{Q}}/K)$ である．しかし L を固定する元は L^σ も固定するので明らか.

[二つ目] K の任意の有限素点 v を一つ取り, $\bar{\mathbb{Q}}$ まで延長する．示したいことは

$$T_v \cap G(\bar{\mathbb{Q}}/L) = T_v \cap G(\bar{\mathbb{Q}}/K) \Longleftrightarrow T_v \cap G(\bar{\mathbb{Q}}/L) = T_v \cap G(\bar{\mathbb{Q}}/F) \text{ かつ } T_v \cap G(\bar{\mathbb{Q}}/F) = T_v \cap G(\bar{\mathbb{Q}}/K)$$

である. しかしこれは見れば明らかである.

[三つ目] K の任意の有限素点 v を一つ取り, $\bar{\mathbb{Q}}$ まで延長する. このとき仮定より

$$T_v \cap G(\bar{\mathbb{Q}}/L) = T_v \cap G(\bar{\mathbb{Q}}/K)$$

が成り立っている. 示したいものは $T_v \cap G(\bar{\mathbb{Q}}/LE) = T_v \cap G(\bar{\mathbb{Q}}/E)$ である. $\sigma \in T_v \cap G(\bar{\mathbb{Q}}/E)$ は, K を固定し仮定より L も固定するので $\sigma \in T_v \cap G(\bar{\mathbb{Q}}/LE)$ となり ok.

□

10 フロベニウス写像と類体論

K/k を有限次アーベル拡大とし, $\mathfrak{p}$ を k の素点で K/k で不分岐なものであるとする. このときフロベニウス自己同型

$$\sigma = \left(\frac{K/k}{\mathfrak{p}}\right) \in G(K/k)$$

が定まるのだった. 具体的にフロベニウス自己同型の作用は以下のようになっていた. $\mathfrak{p}$ の上にある K の素点を $\mathfrak{P}$ として, $N_{K/k}(\mathfrak{P}) = \mathfrak{p}^f$ とする. このとき $(\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_k/\mathfrak{p})$ は f 次巡回拡大であり, σ は

$$^\forall x \in \mathcal{O}_K,\ x^\sigma \equiv x^{N\mathfrak{p}} \bmod \mathfrak{P}$$

という条件で特徴付けられた. このフロベニウス自己同型は以下の性質をもつ.

- $^\forall \tau \in \mathrm{Emb}(K, \mathbb{C})$ に対し
$$\left(\frac{K^\tau/k^\tau}{\mathfrak{p}^\tau}\right) = \tau \left(\frac{K/k}{\mathfrak{p}}\right) \tau^{-1}.$$
- K'/k が K/k を含むアーベル拡大で, $\mathfrak{p}$ が K'/k で不分岐ならば
$$\mathrm{Res}_K \left(\frac{K'/k}{\mathfrak{p}}\right) = \left(\frac{K/k}{\mathfrak{p}}\right).$$
- E/k が有限次ガロア拡大のとき, $\mathfrak{p}$ の上にある E の素点を $\mathfrak{q}$ とすれば, $\mathfrak{q}$ は KE/E で不分岐であり,
$$\mathrm{Res}_K \left(\frac{KE/E}{\mathfrak{q}}\right) = \left(\frac{K/k}{\mathrm{N}_{E/k}(\mathfrak{p})}\right).$$
- 特に $k \subset E \subset K$ のときは
$$\left(\frac{E/k}{\mathfrak{q}}\right) = \left(\frac{K/k}{\mathrm{N}_{E/k}(\mathfrak{p})}\right).$$
- k の最大不分岐アーベル拡大を L, k のイデアル類群を C_k とすると
$$C_k \ni [\mathfrak{p}] \mapsto \left(\frac{L/k}{\mathfrak{p}}\right) \in G(L/k)$$
は同型写像である.

第 IV 部
Λ 加群の構造定理

11 Λ の定義と性質

岩澤理論においては, $\mathbb{Z}_p$ 上の一変数冪級数環 $\Lambda = \mathbb{Z}_p[[T]]$ が重要である. まずここでは Λ の性質をまとめることにする. 有名な事実として $f(T) \in \Lambda^\times \iff f(0) \in \mathbb{Z}_p^\times$ であることに注意. (cf. アティマク演習問題)

Lemma 11.1. (1) Λ は $\mathfrak{m} = (p, T)$ を唯一の極大イデアルとする局所環.
(2) $\cap_n \mathfrak{m}^n = \{0\}$.

Proof. [(1)] まず $\mathfrak{m}$ が極大イデアルであることを示す. 割って体ならよい. 実際

$$\Lambda/\mathfrak{m} = \mathbb{Z}_p[[T]]/(p,T) \cong (\mathbb{Z}_p/p\mathbb{Z}_p[[T]])/(T) \cong \mathbb{F}_p$$

となり ok. 次に $\mathfrak{a} \subsetneq \Lambda$ を $\mathfrak{m}$ と異なる極大イデアルとして, $(p,T) = \mathfrak{m} \subset \mathfrak{a} (\subset \Lambda)$ を示せばよい. 従って $p, T \in \mathfrak{a}$ を示せば十分である. まず $p \notin \mathfrak{a}$ と仮定して矛盾を導く. このとき $(p) = p\Lambda$ は $\mathfrak{a}$ よりも真に大きいイデアルなので $p\Lambda + \mathfrak{a} = \Lambda$ とならなければならない. 従って $pf + a = 1$ となる $f \in \Lambda, a \in \mathfrak{a}$ が存在する. よって $a = 1 - pf \in \Lambda^\times$ となるが, これは $\mathfrak{a} = \Lambda$ を意味するので矛盾. よって $p \in \mathfrak{a}$ が示された. 全く同様の議論で $T \in \mathfrak{a}$ が示される.

[(2)]

UTF00A0$^\forall n \in \mathbb{N}$ について $f \in \mathfrak{m}^n$ ならば $f = 0$ を示せばよい. 特に対偶の「$0 \neq f \in \Lambda$ に対して, ある $n \in \mathbb{N}$ が存在して $f \notin \mathfrak{m}^n$」を示すことにする. まず

$$\mathfrak{m}^n = \left(p^n, p^{n-1}T, p^{n-2}T^2, \dots, p^2T^{n-2}, pT^{n-1}, T^n\right)$$

である. 従って $\mathfrak{m}^{m+n} \subset (p^m, T^n) \subset \mathfrak{m}^k$ $(k = \min\{m,n\})$ が分かる. さて, まず $n, m \in \mathbb{N}$ を任意に動かし $f = a_{n,m}p^mT^n + a_{n+1}T^{n+1} + \dots$ $((a_{n,m}, p) = 1)$ と表す. しかし $f/a_{n,m} \in \Lambda$ を考えることで初めから $f = p^mT^n + a_{n+1}T^{n+1} + \dots$ という形をしているとしてよい. このとき $f \notin (p^{m+1}, T^{n+1})$ であることを示せばよい. (そうすれば $\mathfrak{m}^{(m+1)+(n+1)} \subset (p^{m+1}, T^{n+1})$ より $f \notin \mathfrak{m}^{(m+1)+(n+1)}$ が分かる.) $f \in (p^{m+1}, T^{n+1})$ と仮定して矛盾を導く. 簡単な計算で

$$p^mT^n \in (p^{m+1}, T^{n+1}) \Longrightarrow p^m \in (p^m, T) \Longrightarrow 1 \in (p,T) \Longleftrightarrow \mathfrak{m} = (p,T) = \Lambda$$

が分かる. 実際, $p^mT^n = p^{m+1}f_1 + T^{n+1}f_2$ と表せたとする. $T^n(p^m - Tf_2) = p^{m+1}f_1$ であるから, $f_1 = T^nf_1'$ という形をしていなければならない. 従って $p^mT^n = p^{m+1}T^nf_1' + T^{n+1}f_2$, すなわち $p^m = p^{m+1}f_1' + Tf_2$ となり, 最初の「$\Rightarrow$」が分かる. 同様にして, $p^m(1 - pf_1') = Tf_2$ であるから, $f_2 = p^mf_2'$ という形をしてなければならない. 従って $p^m = p^{m+1}f_1' + Tp^mf_2'$, すなわち $1 = pf_1' + Tf_2'$ となり, 2 番目の「$\Rightarrow$」が分かる. 以上より, $f \notin \mathfrak{m}^{\min\{m+1,n+1\}}$ である. □

$0 \in \Lambda$ の基本近傍系を $\{\mathfrak{m}^n\}_{n\in\mathbb{N}}$ とすることで Λ に位相を入れる. 補題 11.1 よりこれはハウスドルフ位相となる. また, Λ の加法と乗法は連続になるので位相環となることも分かる.

位相空間 X に対し, X がハウスドルフ $\Longleftrightarrow$ $^\forall x \in X$ の閉近傍全体の共通部分は $\{x\}$ という同値が成り立つ. ここから従う.

Lemma 11.2. Λ はコンパクト位相環である.

Proof.「コンパクトの連続像はコンパクト」を用いて示す. まず

$$\psi : \Lambda \ni \sum_{i=0}^{\infty} a_iT^i \mapsto (a_i)_i \in \mathbb{Z}_p^\infty$$

は環同型である. (全単射と準同型はすぐ分かるので略.) 従って ψ が位相環として同型であれば ψ^{-1} の像として Λ が得られるので, 主張を得る. 以下で ψ が位相同型であることを示す.

次に ψ が連続であることを示す. $\mathbb{Z}_p^\infty$ の 0 の開近傍の一つ $V_0 := \prod_{\text{有限個の } i} p^i\mathbb{Z}_p \times \prod_{\text{無限個の } i} \mathbb{Z}_p$ の引き戻しが Λ の開近傍, すなわち $\mathfrak{m}^{\text{なんか}}$ に含まれればよい. $\mathbb{Z}_p^\infty$ は位相環であるから, 「$(-p^i\mathbb{Z}_p, 0, 0, \dots)$ ずらす写像」は同相写像である. 従って初めから $V_0 = \{0\} \times \prod_{\text{有限個の } i} p^i\mathbb{Z}_p \times \prod_{\text{無限個の } i} \mathbb{Z}_p$ という形をしていると思ってよい. このとき $\psi^{-1}(V_0)$ は初項が 0 となる冪級数全体なので, $\psi^{-1}(V_0) \subset (T) \subset \mathfrak{m}$ が分かる. よって ψ は連続.

最後に ψ が開写像であることを示す. $\psi(\mathfrak{m}^k)$ が V_0 のようなものに含まれればよい. $\mathfrak{m}^k = (p^k, p^{k-1}T, p^{k-2}T^2, \dots, T^k)$ であるから,

$$\psi(\mathfrak{m}^k) \subset p^k\mathbb{Z}_p \times p^{k-1}\mathbb{Z}_p \times \times p^{k-2}\mathbb{Z}_p \times \dots \times p\mathbb{Z}_p \times \prod_{\text{無限個}} \mathbb{Z}_p$$

が分かる. 以上より ψ は位相同型である. □

次に, Λ における点列 $\{f_n\}$ の収束について考える. $\Lambda \cong \varprojlim_n \mathbb{Z}_p[T]/(T^n)$ として表せるので, Λ は完備であることに注意する.

$$\begin{aligned}
\lim_{n\to\infty} f_n\text{が存在} &\iff {}^\forall k \in \mathbb{N},\ {}^\exists N \in \mathbb{N} \text{ s.t. } n, m \geq N \Longrightarrow f_n - f_m \in \mathfrak{m}^k \\
\sum_{n=1}^{\infty} f_n\text{が収束} &\iff {}^\forall k \in \mathbb{N},\ {}^\exists N \in \mathbb{N} \text{ s.t. } n \geq m \geq N \Longrightarrow f_{n+1} + \cdots + f_m \in \mathfrak{m}^k \\
&\iff {}^\forall k \in \mathbb{N},\ {}^\exists N \in \mathbb{N} \text{ s.t. } n \geq N \Longrightarrow f_n \in \mathfrak{m}^k \\
&\iff \lim_{n\to\infty} f_n = 0
\end{aligned}$$

Λ においては以下の意味で除算が可能である.

Lemma 11.3 (ワイエルシュトラスの準備定理)**.** $g(T) = \sum_{i=0}^{\infty} a_i T^i \in \Lambda$ が

$$a_0 \equiv a_1 \equiv \cdots \equiv a_{n-1} \equiv 0 \bmod p,\ a_n \not\equiv 0 \bmod p$$

を満たすとする. このとき任意の $f(T) \in \Lambda$ に対し

$$f(T) = q(T)g(T) + r(T),\ \deg r < n$$

を満たす多項式 $q(T) \in \Lambda, r(T) \in \mathbb{Z}_p[T]$ が一意的に存在する.

Proof. まず先に一意性を証明する. $f = qg + r = q'g + r'$ と二通りに表されているとする. このとき $q = q'$ かつ $r = r'$ を示したい. ここで $q - q'$ を初めから q, $r - r'$ を初めから r とおくことで, $f = qg + r = 0$ と表されるときに $q = r = 0$ を示せばよい. 背理法により示す. 以下, $q \neq 0, r \neq 0$ と仮定する. ($qg + r = 0$ より一方を仮定すれば一方が成り立つ.) $qg + r = 0$ において両辺 p で割れるだけ割ることで $p \nmid q, p \nmid r$ と仮定してよい. (これも $qg + r = 0$ より一方を仮定すればもう一方が成り立つ.) $-r = qg$ を具体的に計算してみると

$$\begin{aligned}
qg &= \left(\sum_{i=0}^{\infty} q_i T^i\right)\left(\sum_{i=0}^{\infty} a_i T^i\right) \\
&= (a_0 q_0) + (a_0 q_1 + a_1 q_0)T + (a_0 q_2 + a_1 q_1 + a_2 q_0)T^2 + \cdots + (a_0 q_{n-1} + \cdots + a_{n-1} q_0)T^{n-1} \ (\because \deg r < n)
\end{aligned}$$

となる. 仮定より $a_0 \equiv a_{n-1} \equiv 0 \bmod p$ なので $qg = -r$ も p で割れることになる. しかしこれは $p \nmid r$ に矛盾. よって $q = r = 0$.

次に存在性を示す. まず準備をする. $h(T) = h_0 + h_1 T + \cdots + h_{n-1}T^{n-1} + T^n(h_n + h_{n+1}T + \dots) \in \Lambda$ に対して

$$\begin{aligned}
&\alpha : \Lambda \to \Lambda; h(T) \mapsto h_0 + h_1 T + \cdots + h_{n-1}T^{n-1} \\
&\tau : \Lambda \to \Lambda; h(T) \mapsto h_n + h_{n+1}T + \dots
\end{aligned}$$

は $\mathbb{Z}_p$ 線形写像であることがすぐに分かり, また $h(T) = \alpha(h(T)) + T^n \tau(h(T))$ である. これらの線形写像は以下の性質をもつことは明らかである.

- $\tau(h(T)) = 0 \iff h \in \mathbb{Z}_p[T],\ \deg h < n.$
- ${}^\forall h(T) \in \Lambda,\ \tau(T^n h(T)) = h(T).$

これで準備は終わりである. $g(T) = pP(T) + T^n U(T)$ $U(T) = \tau(g(T))$ と表しておく. ($p \nmid P(T)$) ここで $a_n \not\equiv 0 \bmod p$ と仮定しているので $U(0) \in \mathbb{Z}_p^\times$ であるから $U(T) \in \Lambda^\times$ であることに注意しておく. ここで

$$\begin{aligned}
q(T) &= \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j p^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(f(T)) \\
&= \frac{1}{U(T)} \left\{ \tau(f(T)) - p\tau\left(\frac{P}{U}\tau(f(T))\right) + p^2 \tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau(f(T))\right)\right) - \dots \right\} \in \Lambda \\
q(T)U(T) - \tau(f(T)) &= p\tau\left(\frac{P}{U}\tau(f(T))\right) - p^2\tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau(f(T))\right)\right) + p^3\tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau(f(T))\right)\right)\right) - \dots
\end{aligned}$$

とおく. このとき $f-qg$ が $n-1$ 次以下の多項式であることを示せばよい. 特に先ほど述べた τ の性質より $\tau(f-qg)=\tau(f)-\tau(qg)=0$ を示せばよい.

$$\begin{aligned}p\tau(q(T)P(T)) &= p\tau\left(\frac{P}{U}\tau(f(T))\right)-p^2\tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau(f(T))\right)\right)+p^3\tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau(f(T))\right)\right)\right)-\dots\\ &= \tau(f(T))-q(T)U(T)\end{aligned}$$

であり, $\tau(q(T)g(T))=\tau(q(T)(pP(T)+T^nU(T)))=\tau(pq(T)P(T)+T^nq(T)U(T))=p\tau(q(T)P(T))+q(T)U(T)=\tau(f(T))$ を得る. 以上により $\tau(f)-\tau(qg)=0$ が示された. □

Λ 加群の理論では

$$f(T)=a_0+a_1T+\dots+a_{n-1}T^{n-1}+T^n\ (a_0\equiv\dots\equiv a_{n-1}\equiv 0 \bmod p)$$

なる多項式が重要な役割をもつ. このような多項式を**有徴多項式 (distinguished polynomial)** と呼ぶことにする. $a_0\not\equiv 0 \bmod p^2$ ならばアイゼンシュタイン多項式となって既約となるが, 一般に有徴多項式は既約とは限らない. (例えば $p=2$ のとき $f(T)=T^2+4T+4=(T+2)^2$ がそうである.) 以下の系により, Λ の元は本質的に有徴多項式である.

Corollary 11.4. $g(T)=\sum_{i=0}^{\infty}a_iT^i\in\Lambda$ が

$$a_0\equiv\dots\equiv a_{n-1}\equiv 0 \bmod p,\ a_n\not\equiv 0 \bmod p$$

を満たすとする. このとき

$$g(T)=u(T)g_0(T)$$

となる $u(T)\in\Lambda^\times$ と n 次有徴多項式 $g_0(T)\in\mathbb{Z}_p[T]$ が一意的に存在する. さらに,

$$\begin{aligned}P(T)&=\frac{a_0+a_1T+\dots+a_{n-1}T^{n-1}}{p}\\ U(T)&=a_n+a_{n+1}T+\dots\end{aligned}$$

とすれば, $g_0(T)$ は具体的に

$$g_0(T)=\frac{g(T)}{U(T)}\sum_{j=0}^{\infty}(-1)^jp^j\left(\tau\circ\frac{P}{U}\right)^j\circ 1$$

で与えられる. 特に Λ は一意分解整域 (UFD) である.

Proof. まず一意性から示す. $g(T)=u(T)g_0(T)=u(T)(T^n+pr(T))$ $(u\in\Lambda^\times, r(T)\in\mathbb{Z}_p[T], \deg r\le n-1)$ と表しておく. このとき $T^n=u(T)^{-1}g(T)-pr(T)$ であるから, これはまさに T^n を $g(T)$ で割った式を表しているので, 補題 11.3 の一意性から, $u(T)$ と $r(T)$, つまり $u(T)$ と $g_0(T)$ は一意に定まる.

存在性を示す. 補題 11.3 において $f(T)=T^n$ とする. このとき $\tau(f(T))=1$ なので

$$q(T)=\frac{1}{U(T)}\left\{\tau(f(T))-p\tau\left(\frac{P}{U}\tau(f(T))\right)+p^2\tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau(f(T))\right)\right)-\dots\right\}\in\Lambda$$

という式があったのを思い出すと $q(T)=U(T)^{-1}T-\dots$ と始まるので $q(T)\in\Lambda^\times$ が分かる. さらに $\tau(q(T)g(T))=\tau(f(T))$ という式があったので $\tau(q(T)g(T))=1$ も分かる. 従って qg は n 次モニックで, g の形から有徴多項式である. $g_0=qg$ が求めるものである.

Λ が一意分解整域であることは, 任意の $g(T)\in\Lambda$ が単元と多項式 $g_0(T)\in\mathbb{Z}_p[T]$ の積で表せること, そして $\mathbb{Z}_p[T]$ が一意分解整域であることから従う. □

12　Λ 加群

位相群として $\mathbb{Z}_p$(加法群)$\cong \Gamma$ (乗法群) となる Γ が作用するような加群 X の性質を調べるとき, Γ の作用ではなく Λ の作用に置き換えると考えやすい (らしい). $\mathbb{Z}_p$ 加群 X に Γ が連続に作用しているとき, X は

$$\mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n]$$

上の加群と考えられる. ($\mathbb{Z}_p[[\Gamma]] \cong \Lambda$ はすぐ後で示す.) ただし $\Gamma = \overline{\langle\gamma\rangle}$ のとき $\Gamma_n = \overline{\langle\gamma^{p^n}\rangle}$ であり $\Gamma/\Gamma_n \cong \mathbb{Z}/p^n\mathbb{Z}$ である.

Theorem 12.1. $m \geq n \geq 0$ に対して $\omega_n = \omega_n(T)$ と $\nu_{n,m} = \nu_{n,m}(T) \in \Lambda$ を

$$\omega_n = (1+T)^{p^n} - 1,\ \nu_{n,m} = \omega_m/\omega_n$$

と定義する. このとき位相環としての同型 $\Lambda \cong \mathbb{Z}_p[[\Gamma]]; 1+T \mapsto \gamma$ が成り立つ.

Proof. まず環同型

$$\varphi : \mathbb{Z}_p[\Gamma/\Gamma_n] \xrightarrow{\cong} \mathbb{Z}_p[T]/(\omega_n); \sum_{i=0}^{p^n-1} a_i(\gamma\Gamma_n)^i \mapsto (\sum_{i=0}^{p^n-1} a_i(1+T)^i) + (\omega_n)$$

を示す. ここで $\mathbb{Z}_p[T] = \mathbb{Z}_p[1+T]$ であること, γ は位数が p^n であることに注意をする. まず準同型であること, 全射であることは明らかであるので, 単射を示す. $\sum_{i=0}^{p^n-1} a_i(1+T)^i \in (\omega_n)$ と仮定する. このとき $\sum_{i=0}^{p^n-1} a_i(1+T)^i = \omega_n f(T)$ と書けるが, 両辺の次数を比べて $f(T) = 0$ が分かる. 従って全ての i について $a_i = 0$ となり ok.

次に,

$$\Lambda \cong \varprojlim \mathbb{Z}_p[T]/(\omega_n); f \mapsto (f_n)_n$$

が位相同型であることを示す. ここで, f_n とは $f = q_n\omega_n + f_n$ ($q_n \in \Lambda, f_n \in \mathbb{Z}_p[T], \deg f_n < p^n$) を満たす多項式であり, 射影系は $n < m$ に対し

$$\mathbb{Z}_p[T]/(\omega_m) \to \mathbb{Z}_p[T]/(\omega_n); f_m \mapsto f_m \bmod \omega_n$$

とする. これが射影系になるためには $f_m \bmod \omega_n = f_n \bmod \omega_n$ を示せばよいが, $f = q_m\omega_m + f_m = q_m\omega_m + q'_m\omega_n +$ (余り) $= (q_m\nu_{n,m} + q'_m)\omega_n +$ (余り) であること, Weierstrass の準備定理の余りの一意性からわかる. さて, 以降はめんどくさいので右辺の環を $Y = \varprojlim Y_n$ とおく.

[単射] 全ての n について $f_n \in (\omega_n)$ であると仮定する. このとき $f = 0$ を示せばよい. 補題 11.1 より特に, 全ての m について $f \in \mathfrak{m}^m$ を示せばよい. まず $\omega_0 = T \in \mathfrak{m}$ であり, さらに

$$\frac{\omega_{n+1}}{\omega_n} = 1 + (1+T)^{p^n} + \cdots + (1+T)^{(p-1)p^n} \in \mathfrak{m}$$

であることから

$$\omega_n = \omega_0 \times \frac{\omega_1}{\omega_0} \times \frac{\omega_2}{\omega_0} \times \cdots \times \frac{\omega_{n+1}}{\omega_n} \in \mathfrak{m}^{n+1}$$

が分かる. 今, 全ての n について $f_n \equiv 0 \bmod \omega_n$ であるから, もちろん全ての n について $f \equiv 0 \bmod \omega_n$ である. 従って $f \in (\omega_n) \subset \mathfrak{m}^{n+1}$ より単射が示された.

[全射] 任意の $(g_n) \in Y_n$ を一つ取る. このとき $g_m - g_n \in (\omega_n) \subset \mathfrak{m}^{n+1}$ であるから $\{g_n\}_n$ はコーシー列である. 従って収束値 $f = \lim_n g_n \in \Lambda$ が存在する. そして $m \to \infty$ とすれば $f - g_n \in (\omega_n)$ が得られる. また, $f - f_n \in (\omega_n)$ であるから, $f_n - g_n = (f - g_n) - (f - f_n) \in (\omega_n)$ となり, まさにこれは $(f_n)_n = (g_n)_n$ を意味しているので全射が示された.

[位相同型] どういう位相が入ってるか問題で詰まってるなう. Washington の「Introduction to cyclotomic fields」では位相の議論はしていなかった. なので一旦ここは無視. □

以下では位相群と言えばハウスドルフを仮定する.

Lemma 12.2. 位相 Λ 加群 X はコンパクトであると仮定する. このとき以下が成り立つ.

- $\cap_n \mathfrak{m}^n X = \{0\}$.
- X は有限生成 Λ 加群 $\iff \#X/\mathfrak{m}X < \infty$.

Proof. (1) ある $n \in \mathbb{N}$ が存在して $x \notin \mathfrak{m}^n X$ となる $0 \neq x \in X$ の存在を言えばよい. 今 X はハウスドルフであるから, ある 0 の近傍 U が存在して $x \notin U$ とできる. 従って, ある $n \in \mathbb{N}$ に対して $\mathfrak{m}^n X \subset U$ とできることを示せばよい. さて, X は位相 Λ 加群なので作用

$$\phi : \Lambda \times X \to X; (\lambda, x) \mapsto \lambda x$$

は連続である. $(0, x) \in \phi^{-1}(0)$ であるから, $U \subset X$ を 0 の近傍とすると ($0 \in \Lambda$ の近傍は $\mathfrak{m}^n$ という形をしているので)

$$^\forall x \in X, {}^\exists n = n_x, {}^\exists U_x; x \text{ の近傍 s.t. } \mathfrak{m}^n U_x \subset U$$

が成り立つ. (ϕ が連続であることから $\phi^{-1}(U) \supset \mathfrak{m}^n U_x$ とでき, 両辺に ϕ を作用させればよい.) $X = \cup_x U_x$ と被覆して, X はコンパクトなので $X = \cup_{i=1}^r U_{x_i}$ と有限個で被覆できる. $n = \max\{n_{x_i}\}$ とおけば今示したことから

$$\mathfrak{m}^n X = \cup_{i=1}^r \mathfrak{m}^n U_{x_i} \subset U$$

を得る. 終わり.

(2) [$\Rightarrow$] $X \cong \Lambda \oplus \cdots \oplus \Lambda \oplus$ (有限) と表せば, $X/\mathfrak{m}X \cong \Lambda/\mathfrak{m} \oplus \cdots \oplus \Lambda/\mathfrak{m} \oplus$ (有限) であること, $\Lambda/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$ であることより分かる.

[$\Leftarrow$] $\Lambda/\mathfrak{m}\Lambda$ 加群 $X/\mathfrak{m}X$ が有限ということは

$$X/\mathfrak{m}X = \langle x_1 + \mathfrak{m}X, \ldots, x_n + \mathfrak{m}X \rangle_{\Lambda/\mathfrak{m}\Lambda}$$

と表せる. $Y := \Lambda x_1 + \cdots + \Lambda x_n \subset X$ とおいて, $X = Y$, すなわち $X/Y = 0$ を示せばよい. そのためには X/Y が (ハウスドルフな) コンパクト位相 Λ 加群であること, $\mathfrak{m}^n(X/Y) = X/Y$ の二つを示せばよい. 実際 (1) の結果で X を X/Y として考えることで

$$X/Y = \cap_n (X/Y) = \cap_n \mathfrak{m}^n (X/Y) = \{0\}$$

となるからである. まず X/Y がコンパクトであることは, X/Y がコンパクト X の連続全射 $X \to X/Y$ の像として得られることから分かる. X/Y がハウスドルフであることを示す.

$$\phi^n : \Lambda \times X^n \to X; (\lambda, (x_n)_n) \mapsto \lambda x_1 + \cdots + \lambda x_n$$

によるコンパクト集合 $\Lambda \times \{x_1, \ldots, x_n\}$ の像が Y なので, Y はコンパクトである. さらにコンパクトのコンパクト部分集合は閉であるから Y は閉集合である. 従って位相群論の「X/Y はハウスドルフ $\iff$ Y は閉集合」という事実を用いれば X/Y がハウスドルフであることがわかる. 最後に $X = Y + \mathfrak{m}X$ を示せば

$$\mathfrak{m}(X/Y) = (Y + \mathfrak{m}X)/Y = X/Y$$

より証明が終わる. $X \subset Y + \mathfrak{m}X$ を示す. $^\forall x \in X$ を一つ取る. このとき

$$\begin{aligned} x + \mathfrak{m}X &= (\lambda_1 + \mathfrak{m}\Lambda)(x_1 + \mathfrak{m}X) + \cdots + (\lambda_n + \mathfrak{m}\Lambda)(x_n + \mathfrak{m}X) \\ &= \lambda_1 x_1 + \cdots + \lambda_n x_n + \mathfrak{m}X \end{aligned}$$

であるから, $x - \sum \lambda_i x_i \in \mathfrak{m}X$ が分かる. 従って

$$x = (x - \sum \lambda_i x_i) + (\sum \lambda_i x_i) \in \mathfrak{m}X + Y$$

となって ok. □

Lemma 12.3. Λ の素イデアル $\mathfrak{p}$ は

$$\Lambda, 0, (p), (p, T), (f(T))$$

のいずれかである．ここで, $f(T)$ は既約有徴多項式である．

Proof. まず $\Lambda, 0, (p), (p, T)$ が素イデアルであることは, 割って整域になることからすぐに分かる．さらに Λ は一意分解整域であったから既約元と素元は一致する．従って既約多項式で生成されるイデアルは素イデアルである．以上より, 他に素イデアルがないことを言えばよい．$0 \neq \mathfrak{p}$ を上に上げたもの以外の素イデアルとする．このとき $\mathfrak{p}$ に含まれる最小次数の多項式 $h(T)$ が存在するが, まず $\deg h = 0$ かどうかで場合分けをする．

[$\deg h = 0$] このとき h は定数であるから $h(T) = p^m$ という形をしていて, $(h(T)) \subset \mathfrak{p}$ である．ここで, $m \geq 2$ は起こり得ない．もしそうであると仮定すると $\mathfrak{p}$ が素イデアルなので $p^m \in \mathfrak{p}$ より $p \in \mathfrak{p}$ となって, p^m の最小性に反する．従って $m = 0, 1$ の可能性が残る．$m = 0$ のとき $1 \in \mathfrak{p}$ より $\mathfrak{p} = \Lambda$ となって矛盾．$m = 1$ のとき $(p) \subset \mathfrak{p}$ となる．もし $(p) = \mathfrak{p}$ なら矛盾で, $(p) \subsetneq \mathfrak{p}$ ならば $f(T) \not\equiv 0 \bmod p$ なる $f(T) \in \mathfrak{p}$ が存在する．このとき系 11.4 より $f(T)$ は有徴多項式と思ってよい．($(f(T)) = (u(T)f_0(T)) = (f_0(T))$ だから．) $f(T) = a_0 + a_1 T + \cdots + T^m$ と表せば $T^m \in \mathfrak{p}$ が分かる．($a_i \equiv 0 \bmod p$ であり, $T^m = f(T) - (a_0 + a_1 T + \cdots + a_{m-1}T^{m-1}) \in \mathfrak{p}$ より．) そして先と同様の議論 (f の最小性と $\mathfrak{p}$ が素イデアルより $m \geq 2$ は起こり得ないという議論) で $m = 1$ が分かる．従って $(p, T) \subset \mathfrak{p}$ となって, (p, T) が極大イデアルであったことから $\mathfrak{p} = (p, T)$ または $\mathfrak{p} = \Lambda$ となって矛盾．

[$\deg h \geq 1$] $h(T) = p^m f(T), f(T) \not\equiv 0 \bmod p$ と表しておく．まず $\deg h = 0$ のときの議論より $p^m \notin \mathfrak{p}$ である．従って $h(T) \in \mathfrak{p}$ より $f(T) \in \mathfrak{p}$ とならなければならない．また系 11.4 より $f(T)$ は既約有徴多項式と思ってよい．今 $(f(T)) \subset \mathfrak{p}$ であり, これが実は等号であることを以下で示せば全ての証明が終わる．$0 \neq g(T) \in \mathfrak{p}$ を取る．この $g(T)$ も有徴多項式と思ってよく, 補題 11.3 より

$$g(T) = q(T)f(T) + r(T)\ q(T), r(T) \in \mathbb{Z}_p[T],\ \deg r < \deg f$$

と一意的に表せる．($g(T)$ は多項式なので $q(T)$ も多項式として取れることに注意．) このとき $r(T) = g(T) - q(T)f(T) \in \mathfrak{p}$ となるが, $f(T)$ の最小性に反する．従って $r(T) = 0$, すなわち $g(T) = q(T)f(T) \in (f(T))$ となって, 等号 $(f(T)) = \mathfrak{p}$ が示された． □

13 擬同型による分類

補題 13.3 の反例挙げで, 以下の (本には無い (演習問題にはあるが)) 補題が必要となるので先に証明しておく．

Lemma 13.1. $^\forall f \in \Lambda^\times$ に対し $\#\Lambda/(f) = \infty$.

Proof. 方針としては $\Lambda/(f) \supset \Lambda/(g)$ かつ $\Lambda/(g)$ が無限位数となるイデアル I を探せばよいので, $(f) \subset (g)$, すなわち $g(T) | f(T)$ なる $g(T)$ で $\Lambda/(g)$ が無限位数となるものを見つければよい．Λ は UFD であったから, $g(T)$ は $f(T)$ の既約元としてよい．さらに 12.3 より $g(T) = p$ または $g(T)$: 既約有徴多項式としてよい．$g(T) = p$ のとき $\Lambda/(p) \cong \mathbb{F}_p[[T]]$ より無限位数．$g(T)$ が既約有徴多項式のとき

$$\Lambda/(g) = \varprojlim_n \mathbb{Z}_p[T]/(g) \cong \varprojlim_n \mathbb{Z}_p[\alpha]$$

と書ける．(α は g の根の一つ．) $\mathbb{Z}_p[\alpha]$ は無限位数なのでもちろんその射影極限 $\Lambda/(g)$ も無限位数．(あってる？) □

以降 Λ 加群と言えばコンパクトを仮定する．M, M' を Λ 加群とする．このとき Λ 準同型 $f : M \to M'$ が**擬同型**であるとは

$$\#\operatorname{Ker} f < \infty,$$
$$UTF00A0\#\operatorname{Coker} f < \infty$$

であることをいう．このとき $M \sim M'$ と書く．

Lemma 13.2. 擬同型は同値関係ではない. 正確には以下が成り立つ.

- $M \sim M$.
- $M \sim M' \Longrightarrow M' \not\sim M$.
- $M \sim M',\ M' \sim M'' \Longrightarrow M \sim M''$.

二つ目は正確には「反射律は一般に成り立たない. 」って書くべきだけどまあ察してくれ.

Proof. [(1)] $\mathrm{id} : M \to M$ を考えれば $\operatorname{Ker}\mathrm{id} = \operatorname{Coker}\mathrm{id} = \{0\}$ より ok.

[(3)] $f : M \to M', g : M' \to M''$ を擬同型とする. このとき

$$\tilde{f} : \operatorname{Ker}(g \circ f) \to \operatorname{Ker}(g); x \mapsto f(x)$$
$$\tilde{g} : \operatorname{Coker}(f) \to \operatorname{Im}(g)/\operatorname{Im}(g \circ f); x + \operatorname{Im}(f) \mapsto g(x) + \operatorname{Im}(g \circ f)$$

は well-defined な準同型であって, さらに $\tilde{g}$ は全射である. まず $\tilde{f}$ に準同型定理を適用して

$$\operatorname{Ker}(g \circ g)/\operatorname{Ker}(f) \cong \operatorname{Im}(\tilde{f}) \subset \operatorname{Ker}(g)$$

が得られるが, 仮定より $\operatorname{Ker}(f)$ と $\operatorname{Ker}(g)$ は有限なので $\operatorname{Ker}(g \circ f)$ も有限である. 次に well-defined な準同型

$$\Phi : \operatorname{Coker}(g \circ f) \to \operatorname{Coker}(g); x + \operatorname{Im}(g \circ f) \mapsto x + \operatorname{Im}(g)$$

を考える. 従って準同型定理と $\tilde{g}$ が全射という結果を用いることで

$$\operatorname{Coker}(g \circ f)/\operatorname{Coker}(f) \subset \operatorname{Coker}(g \circ f)/(\operatorname{Im}(g)/\operatorname{Im}(g \circ f)) \cong \operatorname{Im}(\Phi) \subset \operatorname{Coker}(g)$$

を得る. (最左辺の $\operatorname{Coker}(f)$ は全射 $\tilde{g}$ による像と同一視している.) よって $\operatorname{Coker}(f)$ と $\operatorname{Coker}(g)$ が有限なので $\operatorname{Coker}(g \circ f)$ も有限である.

[(2)] 反例を挙げる. $M = (p, T), M' = \Lambda$ とする. このとき $(p, T) \hookrightarrow \Lambda$ を考えると単射なので $\#\operatorname{Ker} = 1$, さらに $\#\operatorname{Coker} = \#\mathbb{Z}/p\mathbb{Z}$ より $(p, T) \sim \Lambda$. あとは $\varphi : \Lambda \not\sim (p, T)$ を示したいので擬同型 $\Lambda \to (p, T)$ が存在すると仮定する. $\varphi(1) =: f(T)$ とおく. このとき

$$\begin{aligned}\varphi(g(T)) &= \varphi(g(T) \cdot 1) \\ &= g(T)\varphi(1)\ (\because \Lambda\text{はΛ加群}) \\ &= g(T)f(T)\end{aligned}$$

となるから, $\operatorname{Im}(\varphi) = (f(T))(\subset (p, T))$ が成り立つ. 従って

$$\operatorname{Coker}(\varphi) = (p, T)/\operatorname{Im}(\varphi) = (p, T)/(f(T))$$

が無限位数であることを見ればよい. それは

$$(\Lambda/(f))\,/\,((p, T)/(f)) \cong \Lambda/(p, T) \cong \mathbb{Z}/p\mathbb{Z}$$

より分かる. 何故なら $(p, T)/(f)$ が位数有限なら $\Lambda/(f)$ も有限とならなければならないが, 補題 13.1 より矛盾するからである. □

Lemma 13.3. $f, g \in \Lambda$ に対して, f と g は互いに素とする. (すなわち $h|f$ かつ $h|g$ ならば $h \in \Lambda^\times$.) このとき以下が成り立つ.

- $\#\Lambda/(f, g) < \infty$.
- $\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g)$.
- $\Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg)$.

Proof. (1) $h \in (f,g)$ を次数最小のものとする．このとき後半で示すように $\Lambda/(f,g) \subset \Lambda/(h,f)$ と出来るから，$\Lambda/(h,f)$ が有限であることを示せばよい．まず p べきを括れるだけ括って，$h(T) = p^s H(T)$ と表しておく．ここで系 11.4 より $H(T) = 1$ または有徴多項式であるとしてよい．まず $H(T) = 1$ であること，すなわち $H(T)$ が有徴多項式であると仮定して矛盾を導く．f と g は互いに素なので，H は f で割り切れないとしてよい．このとき補題 11.3 より

$$f = Hq + r,\ \deg r < \deg H = \deg h,$$

すなわち $p^s f = hq + p^s r$ が成り立つ．しかし $p^s r = p^s f - hq \in (f,g)$ となってしまうが，$\deg(p^s r) < \deg h$ であるのでこれは h の取り方に矛盾する．従って $H = 1$，すなわち $h = p^s$ である．一般性を失うことなく f は p で割り切れなく，そして有徴的であると仮定してよい．(何故なら，$f = p^t F$ と表すとき，$(f) \subset (F)$ であるから $\Lambda/(F,g) \subset \Lambda(f,g) \subset \Lambda/(h,f)$ となって，$\Lambda/(h,f)$ の有限性を示すのに影響無いからである．) Weierstrass の準備定理達を用いて g を f で割って，単元も無視して，ってやると

$$(f,g) \supset (h,f)$$

とできる．ここで，$\Lambda/(p^s,f)$ はべき級数を f で割ったもの，さらに $\mathrm{mod} p^s$ したもの全体の集合であることを考えると，次数は $\deg f$ より小さいもの，さらに係数も $Z_p/p^s\mathbb{Z}_p$ なので有限通りとなる．従って $\Lambda/(p^s,f)$ が有限となり $\Lambda/(f,g)$ も有限．

(2) 単射 $\varphi : \Lambda/(fg) \to \Lambda/(f) \oplus \Lambda/(g); a \mapsto (a \bmod f, a \bmod g)$ を考える．$\#\operatorname{Coker}\varphi < \infty$ を示せばよい．$a, b \in \Lambda$ に対して

$$\begin{aligned} a - b \in (f,g) &\Longrightarrow {}^{\exists} p, q \in \Lambda \text{ such that } a - b = pf + qg \\ &\Longrightarrow a - pf = b + qg \\ &\Longrightarrow (a \bmod f, b \bmod g) = (a - pf \bmod f, b + qg \bmod g) \in \operatorname{Im}\varphi \end{aligned}$$

が成り立つ．(1) の結果を用いて $\Lambda/(f,g) = \{[r_1], \ldots, [r_n]\}$ と表しておく．このとき $[a-b] = [r_i]$ となる $r_i \in \Lambda$ があるから ($[*]$ は $\Lambda/(f,g)$ の代表元を表す記号)，$a - b - r_i \in (f,g)$ となる．従って上の議論から

$$(a \bmod f, b \mod g) - (r_i \bmod f, 0 \bmod g) \in \operatorname{Im}\varphi$$

を得る．これはまさに $\operatorname{Coker}\varphi = (\Lambda/(f) \oplus \Lambda/(g))/\operatorname{Im}\varphi$ の全ての元が有限個の元 $(r_i \bmod f, 0 \bmod g)$ で表されるということを意味している．ok.

(3) (2) の記号を用いて $M = \operatorname{Im}\varphi, N = \Lambda/(f) \oplus \Lambda/(g)$ とおく．このとき $N \supset M \cong \Lambda/(fg)$ であって $(N:M) < \infty$ を示していた．ここで示したいことは $N \sim M$ であるから，以下で擬同型 $\psi : N \to M$ を構成する．まず $(fg,h) = 1$ となる有徴多項式 h を一つ固定する．このとき任意の $([x],[y]) \in N$ に対し $(N:M) < \infty$ であるから鳩の巣原理を用いて $h^i([x],[y]) \equiv h^j([x],[y]) \bmod M$ となる $i < j$ が存在する．すなわち

$$h^i(1 - h^{j-i})([x],[y]) \in M$$

を得る．ここで $1 - h^{j-i} \in \Lambda^\times$ なのでなので $h^i([x],[y]) \in M$ である．k を十分大きく取って h^k を改めて h とすることにより，準同型

$$\psi : N \to M; ([x],[y]) \mapsto h([x],[y])$$

を得る．簡単に分かるように ψ は単射である．Coker についても

$$\begin{aligned} \#\operatorname{Coker}\psi = \#M/\operatorname{Im}\psi = \#(\Lambda/(fg))/h(N) &\le \#N/h(N)\ (\because \varphi \text{ の単射性}) \\ &= \#\Lambda/(fg,h) < \infty\ (\because (1)) \end{aligned}$$

となって有限性が分かる． □

以下の補題 13.4 は，この chapter の目的である有限生成 Λ 加群の構造定理の証明に用いられるものである．まず準備をする．$\{u_1, \ldots, u_n\} \subset \Lambda$ に対して，それらで生成される Λ 加群 $M := \langle u_1, \ldots, u_n \rangle_\Lambda$ を考える．このとき全射準同型

$$\varphi : \Lambda^n \to M; (x_1, \ldots, x_n) \mapsto x_1 u_1 + \cdots + x_n u_n$$

の核を I とすると準同型定理より $\Lambda^n/I \cong M$ である. Λ はネーターであるという事実, ネーターの部分加群は有限生成という事実から I は有限生成 Λ 加群であることが分かる. 従って $I = \langle y_1, \dots, y_m \rangle$ $(y_i = (y_{i1}, \dots, y_{in}) \in \Lambda^n,\ 1 \leq i \leq m)$ と表せる. $\iota : I \hookrightarrow \Lambda^n$ を包含写像, Λ^n の基底を $\{e_1, \dots, e_n\}$ とする. このとき

$$\iota \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{m1} & y_{m2} & \cdots & y_{mn} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} =: R \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

なる行列 $R \in M_{m,n}(\Lambda)$ が存在する. この R を M の**関係行列**という. $(0 \to I \xrightarrow{R} \Lambda^n \xrightarrow{\varphi} M \to 0$ が完全列より $I \cong \operatorname{Im} R = \operatorname{Ker} \varphi$ であることに注意する.) 例えば M の構造が知りたければ, $M \cong \Lambda^n/I$ より実質 $I = \langle y_1, \dots, y_m \rangle$ を調べればよい. そして $(\iota(y_1), \dots, \iota(y_n))^t = R(e_1, \dots, e_n)^t$ より行列 R を調べればよい. 逆に $R' \in M_{m,n}(\Lambda)$ が与えられたら $(\iota(y_1), \dots, \iota(y_n))^t = R'(e_1, \dots, e_n)^t$ を用いて Λ 加群 $N = \Lambda^n/(\iota(y_1), \dots, \iota(y_n))$ を作ることが出来る. この N と M の関係はどうなっているだろうか? 例えば $R' := PRQ$ と変形して R' が simple な形かつ P, Q が正則ならば

$$P \begin{pmatrix} \iota(y_1) \\ \vdots \\ \iota(y_n) \end{pmatrix} = PR \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \longrightarrow P \begin{pmatrix} \iota(y_1) \\ \vdots \\ \iota(y_n) \end{pmatrix} = R'Q^{-1} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$
$$\longrightarrow \begin{pmatrix} y'_1 \\ \vdots \\ y'_n \end{pmatrix} = R' \begin{pmatrix} e'_1 \\ \vdots \\ e'_n \end{pmatrix}$$

のように, I の基底を $\langle y'_1, \dots, y'_n \rangle$ と, Λ^n の基底を $\langle e'_1, \dots, e'_n \rangle$ と取り替えることで, 関係行列が simple な R' に変えることができる. そうして先の手順で Λ 加群 $\Lambda^n/(y'_1, \dots, y'_n)$ を構成し, その構造も簡単に分かる, というのが単因子論の流れである. 上の説明では R から行基本変形と列基本変形をして $R' := PRQ$ という形に変形したが, 今回はこれに加えて 3 つの操作が必要になる.

op. A 二つの行 (列) を入れ替える.
op. B ある行 (列) の λ 倍 $(\lambda \in \Lambda)$ を他の行 (列) に加える.
op. C ある行 (列) に $\Lambda^\times$ の元をかける.
op. 1 $p \nmid \lambda_1$ のとき

$$R_1 : \begin{pmatrix} \lambda_1 & p\lambda_2 & \dots & p\lambda_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \beta_1 & \beta_2 & \dots & \beta_n \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_n \\ p\alpha_1 & \alpha_2 & \dots & \alpha_n \\ p\beta_1 & \beta_2 & \dots & \beta_n \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

op. 2 $p \nmid \lambda_1$ のとき

$$R_2 : \begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \dots & p^k\lambda_n \\ p^k\alpha_1 & \dots & \dots & \vdots \\ p^k\beta_1 & \dots & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_n \\ p^k\alpha_1 & \dots & \dots & \vdots \\ p^k\beta_1 & \dots & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

op. 3 p で割れない $\lambda \in \Lambda$ が存在し, $\lambda(\lambda_1, \dots, \lambda_n) \in \operatorname{Ker} \varphi = I$ のとき

$$R_3 : \begin{pmatrix} p\lambda_1 & p\lambda_2 & \dots & p\lambda_n \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_n \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

Lemma 13.4. 以上のいずれかの操作を 1 回行い $R \to R'$ とし, R' によって定まる Λ 加群を M' とする. このとき以下が成り立つ.

- op. A, op. B, op. C に対しては $M \cong M'$.
- op. 1, op. 3 に対しては $M \sim M'$.
- op. 2 に対しては $M \sim M' \oplus \Lambda/(p^k)$.

Proof. □

Theorem 13.5. X を有限生成 Λ 加群とする. このとき $e \geq 1, e_i \geq 1, f_j \geq 1$ と既約有徴多項式 $g_j(T)$ が存在して

$$X \sim \Lambda^e \oplus \left(\oplus_{i=1}^r \Lambda/(p^{e/i})\right) \oplus \left(\oplus_{j=1}^s \Lambda/(g_j(T)^{f_j})\right)$$

が成り立つ. 特に $e = 0$ のときに限り X は捻れ加群になる.

Proof. 自主ゼミで, この証明の論理が破綻しているという結論になったので省略. □

14 構造定理からの帰結

Lemma 14.1.
- Λ 加群 M_1, M_2 に対し, $M_1 \oplus M_2/\nu_{0,n}(M_1 \oplus M_2) \simeq M_1/\nu_{0,n}M_1 \oplus M_2/\nu_{0,n}M_2$.
- $M = \Lambda/(p^m)$ のとき

$$|M/\nu_{0,n}M| = p^{m(p^n-1)}$$
$$UTF00A0(n \geq 0).$$

- $M = \Lambda/(g(T))$ (g: d 次有徴多項式) のとき, $(g, \nu_{0,n}) = 1$ ならば定数 c と e が存在して

$$|M/\nu_{0,n}M| = p^{dn+c} \ (n \geq e).$$

Proof. (1) よくある同型なので省略.

(2) $\nu_{0,n}$ は次数 $p^n - 1$ の有徴多項式であることを考えると, 簡単な計算により

$$(\Lambda/(p^m))/(\nu_{0,n}(\Lambda/(p^m))) \simeq \Lambda/(p^m, \nu_{0,n}) \simeq \oplus_{i=1}^{p^n-1}\mathbb{Z}/p^m\mathbb{Z}$$

となる. 従って位数 $(p^m)^{p^n-1}$ となって ok.

(3) $g = T^d + pf_0$ のように表しておく. このとき当然 $T^d \equiv -pf_0 \bmod g$ である. また, $p^{e-1} \geq d$ となる e を一つ固定すると

$$\begin{aligned}
T^{p^{e-1}} &\equiv T^d \cdot T^{(p^{e-1})-d} \equiv -pf_0 \cdot T^{(p^{e-1})-d} =: -pf_1 \bmod g \\
(1+T)^{p^{e-1}} &\equiv 1 + pf_2 + T^{p^{e-1}} \equiv 1 + pf_3 \bmod g \\
(1+T)^{p^e} &= ((1+T)^{p^{e-1}})^p \equiv (1+pf_3)^p \equiv 1 + p^2 f_4 \bmod g \\
\nu_{e,e+1} &= ((1+T)^{p^{e+1}} - 1)/((1+T)^{p^e} - 1) = 1 + (1+T)^{p^e} + \cdots + (1+T)^{(p-1)p^e} \equiv p(1+pf_5) \bmod g
\end{aligned}$$

ということが分かる. $1 + pf_5 \in \Lambda^\times$ なので上の最後の式より $\nu_{e,e+1}M = pM$ が分かる. 従って

$$(M : \nu_{0,e+1}M) = (M : \nu_{e,e+1}\nu_{0,e}M) = (M : p\nu_{0,e}M) = (M : pM)(pM : p\nu_{0,e}M) = p^d \cdot (M : \nu_{0,e}M)$$

を得る. ただし最後の等式は p 倍写像 $M/\nu_{0,e}M \to M/\nu_{0,e}M; [f] \mapsto [pf]$ が単射であるため定義域と像の位数が同じということにより従う. この操作を繰り返すことで主張を得る. □

Lemma 14.2. M, N を有限生成捻れ Λ 加群とする. $M \sim N$ であり, 全ての $n \geq 0$ に対し $|M/\nu_{0,n}M| < \infty$ であれば, 全ての $n \geq 0$ に対して $|N/\nu_{0,n}N| < \infty$ であり, 定数 c と e が存在して

$$|M/\nu_{0,n}| = p^c|N/\nu_{0,n}N| \ (n \geq e)$$

が成り立つ.

Proof. まず $|N/\nu_{0,n}N| < \infty$ に対しては, 主張の等式を示せば十分であることに注意する. 何故なら $n \geq e$ なる n に対しては等式から $|N/\nu_{0,n}N| < \infty$ がすぐに分かり, $n < e$ に対しては, $\infty > |N/\nu_{0,e+1}| > |N/\nu_{0,e}| > |N/\nu_{0,e-1}| > \cdots > |N/\nu_{0,1}|$ から有限が分かるためである.

さて, $f : M \to N$ を擬同型とする. このとき自然に Λ 加群の準同型

$$f_n : M/\nu_{0,n}M \to N/\nu_{0,n}N; [x] \mapsto [f(x)]$$
$$f'_n : \nu_{0,n}M \to \nu_{0,n}N; \nu_{0,n}x \mapsto \nu_{0,n}f(x)$$

が誘導される. このとき

$$|M/\nu_{0,n}M| = |\operatorname{Ker} f_n||\operatorname{Im} f_n| = \frac{|\operatorname{Ker} f_n|}{|\operatorname{Coker} f_n|}|N/\nu_{0,n}N|$$

であるから, 十分大きな n に対して $|\operatorname{Ker} f_n|$ と $|\operatorname{Coker} f_n|$ が一定の値になればよい. (そうすれば補題 14.1 よりよりその位数は p べきになる.) $\operatorname{Coker} f_n$ の方は

$$|\operatorname{Coker} f_n| = |N/(f(M) + \nu_{0,n}N)| \leq |N/f(M)| = |\operatorname{Coker} f|$$

であることから単調減少かつ上に有界で収束する. で ok. $|\operatorname{Ker} f_n|$ の方を示す. まず可換図式

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \nu_{0,n}M & \xrightarrow{i} & M & \xrightarrow{p} & M/\nu_{0,n}M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'_n} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_n} & & \\ 0 & \longrightarrow & \nu_{0,n}N & \xrightarrow{i} & N & \xrightarrow{p} & N/\nu_{0,n}N & \longrightarrow & 0 \end{array}$$

より蛇の補題を使って完全列

$$0 \to \operatorname{Ker} f'_n \to \operatorname{Ker} f \to \operatorname{Ker} f_n \to \operatorname{Coker} f'_n \to \operatorname{Coker} f \to \operatorname{Coker} f_n \to 0$$

を得る. 従って簡単に $|\operatorname{Ker} f_n| = |\operatorname{Ker} f| - |\operatorname{Ker} f'_n| + |\operatorname{Coker} f'_n| + |\operatorname{Coker} f_n| - |\operatorname{Coker} f|$ が分かるから, あとは $|\operatorname{Ker} f'_n|$ と $|\operatorname{Coker} f'_n|$ が一定の値になればよい. $\operatorname{Ker} f'_n$ の方は

$$|\operatorname{Ker} f'_n| = |\operatorname{Ker} f \cap \nu_{0,n}M|$$

が単調減少かつ下に有界なので一定の値になる. $\operatorname{Coker} f'_n$ の方を示す. $\nu_{0,n} : N \to N$ と考えて,

$$|\operatorname{Coker} f| = (N : f(M)) = (\nu_{0,n}N : \nu_{0,n}f(M))(\operatorname{Ker} \nu_{0,n} : \operatorname{Ker} \nu_{0,n} \cap f(M)) = |\operatorname{Coker} f'_n|(\operatorname{Ker} \nu_{0,n} + f(M) : f(M))$$

より単調減少で下に有界より一定の値になる. 終わり. □

Theorem 14.3. *X が有限生成捻れ Λ 加群で, 全ての $n \geq 0$ に対し $|X/\nu_{0,n}X| < \infty$ ならば, ある整数 $\mu \geq 0, \lambda \geq 0, \nu$ が存在して, 十分大きな全ての n に対し*

$$|X/\nu_{0,n}X| = p^{\mu p^n + \lambda n + \nu}$$

が成り立つ.

Proof. まず構造定理 13.5 より

$$X \sim (\oplus_{i=1}^{r} \Lambda/(p^{e_i})) \oplus \left(\oplus_{j=1}^{s} \Lambda/(g_j(T)^{f_j})\right)$$

と表せる. このとき $\mu = \sum e_i, \lambda = \sum f_j \deg g_j$ とおけば, 十分大きな n に対し

$$\begin{aligned} |X/\nu_{0,n}X| &= p^c \left\{ \prod_{i=1}^{r} |\Lambda/(p^{e_i}, \nu_{0,n})| + \prod_{j=1}^{s} |\Lambda/(g_j(T)^{f_j}, \nu_{0,n})| \right\} \\ &= p^c \left(\prod_{i=1}^{r} p^{m(p^n-1)} + \prod_{j=1}^{s} p^{dn+c'} \right) \\ &= p^{\mu p^n + \lambda n + \nu} \end{aligned}$$

となる. (細かい数値は無視.) □

Lemma 14.4. X が有限生成 Λ 加群なら, 全ての $n \geq 0$ に対し $\mathrm{rank}_\Lambda X/\omega_n X < \infty$. さらに以下は同値.

- X は捻れ Λ 加群.
- $\mathrm{rank}_{\mathbb{Z}_p} X < \infty$.

Proof. 最初の主張は構造定理からすぐに従う. 同値の方も, 構造定理で $e = 0$ とすればすぐに分かる. □

第 V 部
岩澤の類数公式

15 $\mathbb{Z}_p$ 拡大の基本性質

前置き. あとで書く.

Lemma 15.1 ([?, p.31, 命題 1.6.5])**.** $\mathcal{O}_K$ を整閉整域, K を $\mathcal{O}_K$ の商体, L/K をガロア拡大, $\mathcal{O}_L$ を $\mathcal{O}_K$ の L での整閉包, $\mathfrak{P}$ を $\mathcal{O}_L$ の素イデアルとする. このとき $\mathfrak{P}$ の分解群 $D_\mathfrak{P}$, 惰性群 $I_\mathfrak{P}$ は $\mathrm{Gal}(L/K)$ の閉部分群である.

Proof. まず $D_\mathfrak{P}$ が閉であることを示す. $\mathrm{Gal}(L/K) \setminus D_\mathfrak{P}$ が開であることを示せばよい. 従って ${}^\forall\sigma \in \mathrm{Gal}(L/K) \setminus D_\mathfrak{P}$ に対して, ある σ の近傍 σH が $D_\mathfrak{P}$ と共通部分をもたなければよい. まず σ の取り方から, ある $x \in \mathfrak{P}$ に対して $\sigma(x) \notin \mathfrak{P}$ が成り立つ. M を $K(x, \sigma(x))$ のガロア閉包, $H = \mathrm{Gal}(L/M)$ とする. このとき $x, \sigma(x)$ は代数的数であるから M は有限次ガロア拡大であり, 従ってあとは $\sigma H \cap D_\mathfrak{P} = \varnothing$ を示せばよい. $\tau \in \sigma H \cap D_\mathfrak{P}$ が一つ取れたとする. このとき $\tau \in D_\mathfrak{P}$ から $\tau(x) \in \mathfrak{P}$ であるが, $\tau \in \sigma H$ から $h \in H$ を用いて $\tau(x) = \sigma h(x) = \sigma(x) \notin \mathfrak{P}$ となって矛盾する. ok.

次に $I_\mathfrak{P}$ が $\mathrm{Gal}(L/K)$ の中で closed であることを示す, 従って $\mathrm{Gal}(L/K) \setminus I_\mathfrak{P}$ が open であることを示せばよい. もし $I_\mathfrak{P}$ が $D_\mathfrak{P}$ の中で closed が示せたとする, すなわち $I_\mathfrak{P}$ の任意の点列の収束先がまた $I_\mathfrak{P}$ に属すならば, それは $\mathrm{Gal}(L/K)$ の中で考えても同じことである. 従って $I_\mathfrak{P}$ が $D_\mathfrak{P}$ の中で closed, すなわち $D_\mathfrak{P} \setminus I_\mathfrak{P}$ が open, すなわち ${}^\forall\sigma \in D_\mathfrak{P} \setminus I_\mathfrak{P}$ に対して, ある σ の近傍 σH が $I_\mathfrak{P}$ と共通部分をもたなければよい. 今 σ の取り方から, ある $x \in \mathcal{O}_L$ が存在して $\sigma(x) \not\equiv x \bmod \mathfrak{P}$ が成り立つ. M を $K(x)/K$ のガロア閉包, $H = \mathrm{Gal}(M/K)$ とする. このとき $\sigma H \cap I_\mathfrak{P} = \varnothing$ を示せばよい. $\tau \in \sigma H \cap I_\mathfrak{P}$ が一つ取れたとする. $\tau \in I_\mathfrak{P}$ であるから, 任意の $y \in \mathcal{O}_L$ に対して $\tau(y) \equiv y \bmod \mathfrak{P}$ が成り立つ. 特に $y = x$ とすれば $\tau(x) \equiv x \bmod \mathfrak{P}$ が成り立つ. また, $\tau = \sigma h$ $(h \in H)$ と表すと $\tau(x) = \sigma h(x) = \sigma(x) \not\equiv x \bmod \mathfrak{P}$ となり矛盾. ok. □

Lemma 15.2 ([?, p.17, 定理 2.6])**.** K/k を有限次代数体の $\mathbb{Z}_p$ 拡大とする. このとき以下が成り立つ.

- K/k で分岐する素点は p 上の素点に限る.
- K/k では少なくとも一つの素点が分岐する.

Proof. (1) $\ell \neq p$ を $\mathbb{Q}$ の有限素点として, ℓ の上にある k の素点を λ とする. このとき K/k で λ が不分岐であることを示せばよい, すなわち λ に対する惰性群 I が自明であることを示せばよい. 補題 15.1 より I は $\mathrm{Gal}(K/k)$ の閉部分群であるから, $I \simeq \{0\}$ または $I \simeq p^n\mathbb{Z}_p$ $(n \geq 1)$ という形をしている. 前者の場合は既に証明は終わっているから, 後者と仮定して矛盾を導く. 無限素点の惰性群は位数が 1 または 2, 特に有限である. $I \simeq p^n\mathbb{Z}_p$ とするとこれは位数無限なので, この場合無限素点が分岐することはない. 従って以下では有限素点の場合のみ考える.

$p^m\mathbb{Z}_p$ により固定される K の部分体を K_m とし, 体の列 $k = K_0 \subset K_1 \subset \cdots \subset \cup K_n = K$ を考える. k の正規化 ℓ 進付値を一つ固定し, それを $K_1, K_2, \ldots, K$ に順に延長していく. そうして新たな ℓ 進体の列 $k_\ell = K_{0,\ell} \subset K_{1,\ell} \subset \cdots \subset K_\ell$ を得る. 完備化によって惰性群は変わらないので (正確には $\mathrm{Gal}(K_\ell/k_\ell)$ の惰性群と同型), その惰性体を K_ℓ^{ur} と書く, すなわち $I \simeq \mathrm{Gal}(K_\ell^{ur}/k_\ell)$ である. このとき局所類体論により

$$\mathcal{O}_{k_\ell}^\times \simeq \mathrm{Gal}(k_\ell^{ab}/k_\ell) \overset{res}{\twoheadrightarrow} \mathrm{Gal}(K_\ell^{ur}/k_\ell) \simeq I$$

という全射が得られる. この全射と ℓ 進 log による同型 $\mathcal{O}_{k_\ell}^\times \simeq (finite) \times \mathbb{Z}_\ell^m$ を用いて

$$\mathbb{Z}_\ell^m \overset{\iota}{\hookrightarrow} \mathcal{O}_{k_\ell}^\times \overset{f}{\twoheadrightarrow} p^n\mathbb{Z}_p \twoheadrightarrow p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$$

なる連続写像を得ることが出来る. さらにこれは全射である. 全射であることを示すには $\mathcal{O}_{k_\ell}^\times \setminus \mathbb{Z}_\ell^m$ の任意の元, すなわち有限位数の元 $x \in \mathcal{O}_{k_\ell}^\times$ を f で送ったときに消えていればよい. x は有限位数であるから, ある $t \in \mathbb{Z}$ を用いて $tx = 0$ である. 従って $tf(x) = f(tx) = f(0) = 0$ となって $f(x)$ は $p^n\mathbb{Z}_p$ 内で有限位数となる. しかし明らかに $p^n\mathbb{Z}_p$ 内に有限位数の点は 0 しかない. よって ok. さて, 閉部分群 H により $\mathbb{Z}_\ell^m/H \simeq \mathbb{F}_p$ が成り立つが, 右辺は位数 p の元が存在するのに対し左辺は位数 p の元が存在しない. 矛盾.

(2) 背理法で示す. p の上にある K の素イデアル $\mathfrak{p}$ も K/k で不分岐であると仮定する. このとき K/k は不分岐拡大となるから, $K \subset K^{ur}$ が分かる. 従って大域類体論 (有限次代数体の最大不分岐アーベル拡大はイデアル類群に同型) により $\mathbb{Z}_p \simeq \mathrm{Gal}(K/k) \subset \mathrm{Gal}(k^{ur}/k) \simeq Cl(k) < \infty$ となって, $\mathbb{Z}_p$ が無限群であることに矛盾する. ok. □

上の補題により, p の上にある素点のみが分岐する可能性がある拡大が重要になることが分かると思う. このような拡大を p **外不分岐拡大**という. 有限次代数体 k の p 外不分岐最大アーベル p 拡大を M とする. (つまり拡大次数が p べきとなるアーベル拡大 M/k で, p 以外の上にある k の素点は全て M で分岐するもの全ての合併.) このとき $\mathrm{Gal}(M/k)$ の大きさは以下の定理のように評価できる.

Theorem 15.3. k の次数を d, 符号を (r_1, r_2) とすれば以下が成り立つ.

- $\mathrm{rank}\,\mathrm{Gal}(M/k) < \infty$.
- $r_2 + 1 \leq \mathrm{rank}_{\mathbb{Z}_p} G(M/k) \leq d$.

Proof. まず

$$U_{\mathfrak{p},1} := \left\{\alpha \in k_\mathfrak{p}^\times \mid \alpha \equiv 1 \bmod \mathfrak{p}\right\}, \quad U := \prod_{\mathfrak{p}|p} U_{\mathfrak{p},1}$$

とおく. このとき p 進 log による同型 $\mathcal{O}_\mathfrak{p} \simeq (finite) \times U_{\mathfrak{p},1}$ と [**?**, p.24, 定理 1.3.23] により

$$\begin{aligned}\prod_{\mathfrak{p}|p} \mathcal{O}_\mathfrak{p} &\simeq \mathcal{O}_k \otimes_\mathbb{Z} \mathbb{Z}_p \\ &\simeq \mathbb{Z}^d \otimes_\mathbb{Z} \mathbb{Z}_p \quad (\because \text{chapter1, 定理 1.1}) \\ &\simeq \mathbb{Z}_p^d\end{aligned}$$

が成り立つ. 従って $\mathrm{rank}_{\mathbb{Z}_p} U = d$ が分かる. 次に, $E_1 = \left\{\varepsilon \in k^\times \mid {}^\forall\mathfrak{p}|p,\ \varepsilon \equiv 1 \bmod \mathfrak{p}\right\}$ として, E_1 を対角に U に埋め込み, その位相閉包を $\bar{E}_1$ と書くことにする. $\mathcal{O}_k^\times/E_1$ は有限群であるから $\mathrm{rank}_\mathbb{Z} E_1 = \mathrm{rank}_\mathbb{Z} \mathcal{O}_k^\times$ となり, さらにディリクレの単数定理よりそれは $r_1 + r_2 - 1$ に等しい. ($\mathcal{O}_k^\times/E_1$ が有限であることは以下のようにして示される. 任意の $\mathcal{O}_k^\times$ の元が有限回冪乗して E_1 に入ることを示せばよい. ディリクレの単数定理から, $\mathcal{O}_k^\times$ の元を $(x_1, \ldots, x_n)$ $(x_i \in \mathbb{Z})$ と取る. このとき全ての i について $x_i \equiv a_i \bmod \mathfrak{p}$ なる $a_i \in \mathbb{Z}$ が存在するが, 適切にべき乗することにより $x_i^{n_1} \equiv 1 \bmod \mathfrak{p}$ とすることができる. 従って n_i の最小公倍数を l とすれば $(x_1, \ldots, x_n)^l \in E_1$ を得る.) また, $\mathbb{Z}-\mathrm{rank}$ を $\mathbb{Z}_p-\mathrm{rank}$ にすると一般に階数は減るので, $0 \leq \mathrm{rank}_{\mathbb{Z}_p} \bar{E}_1 \leq r_1 + r_2 - 1$ である. (右辺の等号が成り立つと主張するのが **Leopoldt's conjecture** である.)

さて, L_0 を k の最大不分岐アーベル p 拡大とする. このとき $[L_0 : k]$ は (イデアル類群の位数の p 部分に等しいので) 有限であり, 従って $\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(L_0/k) = 0$ であり, さらに同型 $\mathrm{Gal}(M/k)/\mathrm{Gal}(M/L_0) \simeq \mathrm{Gal}(L_0/k)$ から $\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(M/k) = \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(M/L_0)$ が分かる. . このとき類体論より

$$\mathrm{Gal}(M/L_0) \simeq U/\bar{E}_1$$

が得られる. 実際, C_k を k のイデアル類群とすれば大域類体論のイデール ver. により

$$\mathrm{Gal}(M/k) \simeq C_k/\left(\prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}} \times \prod_{\mathfrak{p}\nmid p} \mathcal{O}_\mathfrak{p}^\times \times \prod_{p|\infty} K_\mathfrak{p}^\times\right) \text{の } p\text{-Sylow 部分群}$$

$$\mathrm{Gal}(L_0/k) \simeq C_k/\left(\prod_{\mathfrak{p}|p} \mathcal{O}_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\nmid p} \mathcal{O}_\mathfrak{p}^\times \times \prod_{p|\infty} K_\mathfrak{p}^\times\right) \text{の } p\text{-Sylow 部分群}$$

である. 従って

$$\mathrm{Gal}(M/L_0) \simeq \mathrm{Gal}(M/k)/\mathrm{Gal}(L_0/k) \simeq \left(\prod_{\mathfrak{p}|p} \mathcal{O}_{\mathfrak{p}}^{\times}\right) / \left(\prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}\right) = U/\bar{E}_1$$

を得る. (ここの議論ガバガバ. 最初の同型はそう計算してはいけないし, 閉包の事実を使っていない.) 以上より

$$\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(M/k) = \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(M/L_0) = \mathrm{rank}_{\mathbb{Z}_p} U - \mathrm{rank}_{\mathbb{Z}_p} \bar{E}_1$$

を得るので, これまで得られた数値と不等式を用いることで題意を得る. □

Corollary 15.4. k のすべての $\mathbb{Z}_p$ 拡大の合併を $\bar{k}$ とすると

$$\mathrm{Gal}(\bar{k}/k) \simeq \mathbb{Z}_p^r, \quad r_2 + 1 \leq r \leq [k:\mathbb{Q}]$$

が成り立つ. つまり任意の有限次代数体 k に対し, k の $\mathbb{Z}_p$ 拡大は必ず存在する. その個数は 1 個, または連続濃度である.

Proof. K/k を $\mathbb{Z}_p$ 拡大とする. このとき補題 15.2 より K は p 外不分岐拡大, すなわち $K \subset M$ である. 従って $\bar{k} = M$ であり, 定理 15.3 より主張を得る. □

16 Γ 加群から Λ 加群へ

ここでは岩澤類数公式の証明のためのメインとなる定理を証明する. あとで詳しく述べるが, K/k を $\mathbb{Z}_p$ 拡大, L_n を (大体)k_n の最大不分岐アーベル p 拡大とする. このとき類体論より k_n のイデアル類群の p 部分は $G(L_n/k_n)$ と同型であることが従う. さらに $G(L_nK/K) \simeq G(L_n/k_n)$ であることから, 岩澤類数公式の証明のためには $G(L_nK/K)$ のようなガロア群, すなわち K 上の最大不分岐アーベル拡大 L_∞ に対して $G(L_\infty/K)$ の性質を調べることが必要になる. それらを以下で行う.

今述べたことよりも, もう少し一般の状況を設定する. F/K をアーベル p 拡大, $X = G(F/K)$ とする. また, F/k もガロア拡大であると仮定する. 作用 $\Gamma \curvearrowright X$ を

$$\Gamma \curvearrowright X; \quad x^\gamma := \tilde{\gamma} x \tilde{\gamma}^{-1}$$

と定義する. ただし $\tilde{\gamma}$ は γ の $\mathrm{Gal}(F/k)$ への延長を一つ固定したものである. (作用の well-definedness は省略.) 従って X には Γ 加群の構造が, そして $\Lambda = \mathbb{Z}_p[[T]]$ 加群の構造が入ることを思い出しておこう. その作用とは同型 $\Lambda \simeq \mathbb{Z}_p[[\Gamma]]; \gamma \mapsto 1+T$ を用いて

$$\Lambda \curvearrowright X; (1+T)x := x^\gamma = \tilde{\gamma} x \tilde{\gamma}^{-1}$$

を $\mathbb{Z}_p$ 線形的に延長したものの形で書けた. さて, 本の補題 4.10 にあるように, X の性質を $X/\omega_n X$ を経由して調べることが多い. そこで, まず $\omega_n X$ の意味について考えることにする.

Lemma 16.1. $\omega_n X$ は, $G_n = G(F/k_n)$ の交換子群 $[G_n, G_n]$ に等しい. 従って $X/\omega_n X \simeq G(k_n^{ab} \cap F/K)$ が成り立つ.

Proof. ($\omega_n X \subset [G_n, G_n]$) $x \in X$ に対して

$$\omega_n x = ((1+T)^{p^n} - 1)x = x^{\gamma^{p^n}-1} = \tilde{\gamma}^{p^n} x \tilde{\gamma}^{-p^n} x^{-1}$$

であって, $\tilde{\gamma}^{p^n}$ は k_n を固定するから $\tilde{\gamma}^{p^n} \in G_n$ である. 従って $\omega_n X \subset [G_n, G_n]$.

($[G_n, G_n] \subset \omega_n X$) まず以下の主張を示す.

Lemma 16.2. 完全列

$$1 \longrightarrow X \longrightarrow G_n \overset{\text{res to } K}{\longrightarrow} \Gamma_n \longrightarrow 1$$

は分裂する. すなわち Γ_n と同型な部分群 $H_n \subset G$ が存在し, $G = H_n X, H_n \cap X = 1$ が成り立つ.

Proof. まず完全列が成り立つのは位相同型 $\mathrm{Gal}(F/k_n)/\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(K/k_n)$, すなわち $G_n/X \simeq \Gamma_n$ による. この完全列が分裂することを示すためには $\varphi : \Gamma_n \to G_n$ で $\mathrm{res} \circ \varphi = \mathrm{id}$ となるものを構成すればよい. Γ の位相的生成元を γ_0 とすると Γ_n の任意の元は $\lim_m \gamma_0^{p^n a_m}$, すなわち $c \in \mathbb{Z}_p$ を用いて $\gamma_0^{p^n c}$ と表せる. 従って

$$\varphi(\gamma_0^{p^n c}) := \tilde{\gamma_0}^{p^n c}$$

と定義すれば明らかに $\mathrm{res} \circ \varphi = \mathrm{id}$ を満たす. □

従って任意の $a, b \in G$ は $a = \alpha x, b = \beta y$ $(\alpha, \beta \in H_n, x, y \in X)$ と表せる. また, $\alpha, \beta \in H_n$ に対応する Γ_n の元を σ, τ とすると H_n はアーベル群であるから ($p^n\mathbb{Z}_p$ と同型だから.)

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= (\alpha x \alpha^{-1}) \alpha \beta y x^{-1} (\beta^{-1} \alpha^{-1} \beta) y^{-1} \beta^{-1} \\ &= (\alpha x \alpha^{-1})(\alpha\beta) y x^{-1} (\alpha\beta)^{-1} (\beta y^{-1} \beta^{-1}) \\ &= x^\sigma (y x^{-1})^{\sigma\tau} (y^{-1})^\tau \\ &= x^\sigma x^{-\sigma\tau} y^{\sigma\tau} y^{-\tau} \\ &= (x^\sigma)^{1-\tau} (y^\tau)^{\sigma-1} \end{aligned}$$

を得る. さらに, γ_0 を位相的生成元をとしたとき $\tau \in \Gamma_n = \overline{\langle \gamma_0^{p^n} \rangle}$ は $c \in \mathbb{Z}_p$ を用いて $\tau = (\gamma_0^{p^n})^c$ と表せる. 従って

$$1 - \tau = 1 - (\gamma_0^{p^n})^c \leftrightarrow 1 - (1+T)^{p^n c} = (1 - (1+T)^{p^n})(1 + \dots) \in \omega_n \Lambda$$

であるから $(x^\sigma)^{1-\tau} \in \omega_n X$. 同様にして $(y^\tau)^{\sigma-1} \in \omega_n X$. 以上より $aba^{-1}b^{-1} \in \omega_n X$ が分かった.

最後の主張を示す. 第三同型定理と今示したことを用いれば

$$\begin{aligned} G(k_n^{ab} \cap F/k_n)/G(k_n^{ab} \cap F/K) &\simeq G(K/k) \\ &\simeq G(F/k_n)/G(F/K) \\ &\simeq \{G(F/k_n)/[G(F/k_n), G(F/k_n)]\} \,/\, \{G(F/K)/[G(F/k_n), G(F/k_n)]\} \\ &\simeq G(k_n^{ab} \cap F/k_n)/(X/\omega_n X) \end{aligned}$$

なる同型が得られ, 両辺の分母を見ることで分かる. □

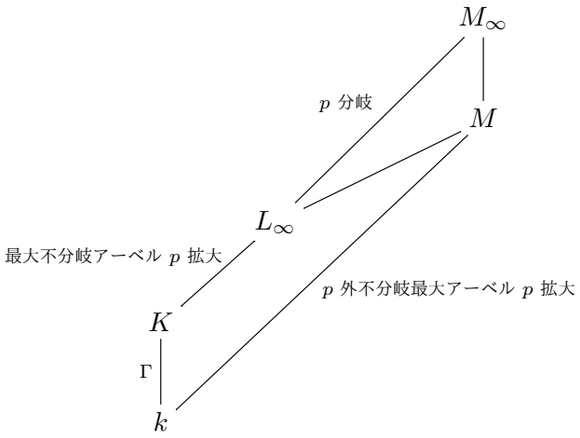
$\omega_n X$ は連続写像 $X \to X; x \mapsto \omega_n x$ の像であって, X はコンパクトなので $\omega_n X$ はコンパクトである. 従って上の補題から $[G_n, G_n]$ はコンパクトであって, 閉集合 G_n の部分群であるから $[G_n, G_n]$ は閉部分群である.

惰性群について少し述べる. まず一般論から $\mathbb{Z}_p$ 拡大 K/k で分岐する k の素点は有限個で, それらの惰性群は閉なので Γ_n という形をしていなければならない. 従って分岐する素点の惰性群の全ての共通部分も閉なので Γ_{n_0} という形をしている. このとき惰性群の定義から K/k_{n_0} において分岐する素点は totally ramified になることを覚えておく.

M_∞ を K の p 外不分岐最大アーベル p 拡大, L_∞ を K の最大不分岐アーベル p 拡大, そして

$$\mathcal{X} := \mathrm{Gal}(M_\infty/K), \;\; X = \mathrm{Gal}(L_\infty/K)$$

とおく. 様々な記号が現れてややこしいので, 一旦分かりやすく図示しておく.



簡単に $L_\infty \subset M$ であること, $M \subset M_\infty$ であることを確認しておく. 前者を示すには L_∞/k が p 外不分岐アーベル p 拡大であることを見ればよい. p 外不分岐は K/k が p 外不分岐であること, L_∞/K が不分岐であることから従う. アーベル拡大も p 拡大も同様. ok. 次に後者を示すには M/K が p 外不分岐アーベル p 拡大であることを見ればよい. アーベル拡大と p 拡大であることは L_∞/K と K/k がアーベル p 拡大であることから従う. あとは p 外不分岐であることを見ればよい. $\ell \neq p$ の上にある K の素点 λ が M で分岐したと仮定する. しかしこれは k の素点 ℓ が M で分岐していることを意味するので, M の定義に矛盾. ok.

Theorem 16.3.
- $\mathcal{X}, X$ は有限生成 Λ 加群である.
- X は捻れ Λ 加群である.

Proof. (1) 制限写像 $\mathcal{X} = \mathrm{Gal}(M_\infty/K) \twoheadrightarrow \mathrm{Gal}(L_\infty/K) = X$ を考えれば, $\mathcal{X}$ が有限生成 Λ 加群であることを示せば十分である. そして本の補題 4.4(2) より, $\mathcal{X}/(p,T)\mathcal{X}$ が有限群であることを示せばよい. さらに $\mathcal{X}/\omega_0\mathcal{X} = \mathcal{X}/T\mathcal{X}$ の $\mathbb{Z}_p$-rank が有限ならば $\mathcal{X}/(p,T)\mathcal{X}$ が ($\mathbb{F}_p$ の有限個の直和となって) 有限になる. 従って以下では $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{X}/\omega_0\mathcal{X} < \infty$ を示す.

まず k の最大アーベル拡大を k^{ab} と表すと, $k^{ab} \cap M_\infty = M$ が成り立つ.

($k^{ab} \cap M_\infty \subset M$) $(k^{ab} \cap M_\infty)/k$ が p 外不分岐アーベル p 拡大であることを示せばよい. k^{ab}/k がアーベル拡大であるから, M_∞/k が p 外不分岐かつ p 拡大であることを示せばよい. M_∞/K が定義から p 外不分岐かつ p 拡大なので, K/k が p 外不分岐かつ p 拡大を示せばよい. p 拡大は明らかで p 外不分岐は補題 15.2 より分かる.

($k^{ab} \cap M_\infty \supset M$) M/k は定義からアーベル拡大なので $k^{ab} \supset M$ である. あとは $M_\infty \supset M$ を示せばよい, すなわち M/K が p 外不分岐アーベル p 拡大であることを示せばよい. M/k がアーベル p 拡大であるから M/K もアーベル p 拡大なので, あとは M/K が p 外不分岐であることを示せばよい. もし M/K が p 外不分岐でない, すなわち $\ell \neq p$ の上にある K の素点 λ が M で分岐したと仮定すると, これは M/k で λ の下にある k の素点が分岐したことになり, M/k が p 外不分岐であることに矛盾する. ok.

つまり M は M_∞ に含まれる k の最大アーベル拡大であるから, 補題 16.1 より

$$\mathcal{X}/\omega_0\mathcal{X} \simeq \mathrm{Gal}(M/K)$$

が成り立つ. 従って $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{X}/\omega_0\mathcal{X} < \infty$ を示すためには $\mathrm{rank}_{\mathbb{Z}_p} G(M/K) < \infty$ を示せばよいが, 同型 $\mathrm{Gal}(M/k)/\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(K/k)$ と定理 15.3 より $\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(M/K) < \infty$ が分かる. ok.

(2) まず本の補題 4.10 により, 任意の $n \in \mathbb{N}$ について $\mathrm{rank}_{\mathbb{Z}_p} X/\omega_n X < \infty$ を示せばよい. さらに $X/\omega_n X$ は n について単調増加であるから, $n \geq n_0$ についてのみ考えればよい. 以下,

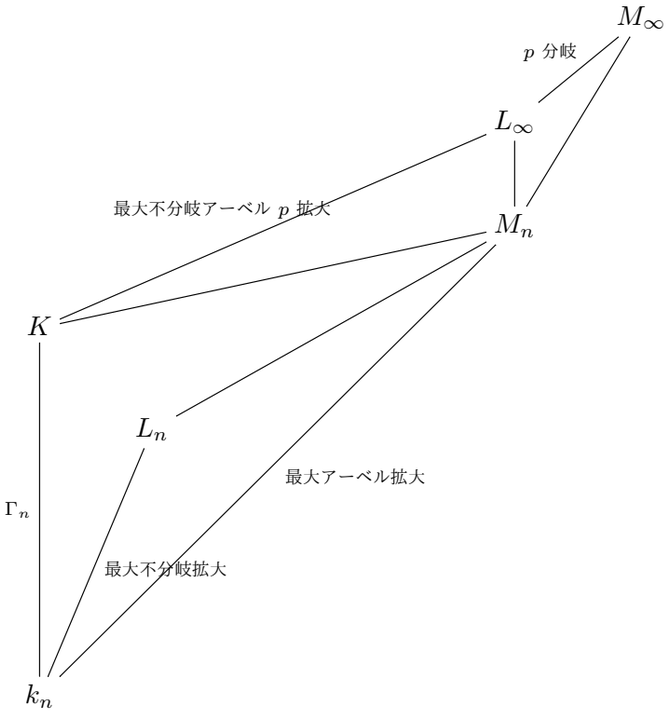
$$M_n = (L_\infty\text{内の}, k_n\text{の最大アーベル拡大}), \quad L_n = (M_n\text{内の}, k_n\text{の最大不分岐拡大})$$

とする. まず (1) と同様 $X/\omega_n X \simeq G(M_n/K)$ である. また, $G(M_n/k_n)/G(M_n/K) \simeq G(K/k_n)$ より $\mathrm{rank}_{\mathbb{Z}_p} G(M_n/k_n)$ が有界であることを見ればよい. さらに, L_n は k_n の最大不分岐アーベル p 拡大であるから $[L_n : k_n] = (k_n$のイデアル類群の p 部分$) < \infty$ であるので, 同型 $G(M_n/k_n)/G(M_n/L_n) \simeq G(L_n/k_n)$ より $\mathrm{rank}_{\mathbb{Z}_p} G(M_n/L_n)$ が有界であることを見ればよい.

$k_n^{ur,ab,p}$ を k_n の最大不分岐アーベル p 拡大とおき, $k_n^{ur,ab,p} = L_n$ を示す.

($k_n^{ur,ab,p} \subset L_n$) $k_n^{ur,ab,p}/k_n$ が M_n に含まれる不分岐拡大ならよい. 不分岐であることは定義から明らかなので, $k_n^{ur,ab,p}$ が M_n に含まれること, すなわち $k_n^{ur,ab,p}$ が L_∞ に含まれるアーベル拡大ならよい. アーベル拡大であることは定義から明らかなので, $k_n^{ur,ab,p}$ が L_∞ に含まれればよい. これが示せない. たぶん (1) 同様, L_∞ に含まれる k_n の最大不分岐アーベル p 拡大, が正しいんじゃないかなと思う. それでも有限性は変わらないのでよし.

($k_n^{ur,ab,p} \supset L_n$) L_n/k_n が不分岐アーベル p 拡大ならよい. 定義から不分岐拡大であることはよいので, 不分岐かつ p 拡大ならよい. $M_n/L_n/k_n$ が L_∞ に含まれる不分岐拡大なので不分岐はよい. そして L_∞/K が p 拡大で K/k_n も p 拡大なので p 拡大も ok.



これまでの状況を上の図に表した. ただし包含 $K \subset M_n$ と $M_n \subset M_\infty$ は同様に示せるので省略する. $n \geq n_0$ とし, K/k_n で分岐する k_n の素点 $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ の, M_n/k_n における惰性群をそれぞれ $I_1, \ldots, I_s$ とすると

$$G(M_n/L_n) = I_1 \cdots I_s \tag{16.4}$$

が成り立つ.

びみょう.

また, 同型 $I_i \to G(K/k_n)$ が存在する.

まず全射を示す. 制限写像

$$G(M_n/k_n) \twoheadrightarrow G(K/k_n)$$

の I_i の像は $I_i \cap G(K/k_n)$ であり, これは $G(K/k_n)$ の惰性群となる. 従ってあとは $I_i \cap G(K/k_n) = G(K/k_n)$ を示せばよい, すなわち $G(M_n^{I_i}/k_n) = I_i \supset G(K/k_n)$ を示せばよい, すなわち $M_n^{I_i} \subset K$ を示せばよい. そしてこれは $\mathfrak{p}_i$ が K/k_n で totally ramified ということから分かる.

単射を示す. 核は $I_i \cap G(M_n/K)$ であるから M_n/K が $\mathfrak{p}_i$ で不分岐ならばよい. もし $\mathfrak{p}_i$ の上にある K の素点が M_n で分岐したと仮定すると, 当然 L_∞/K は $\mathfrak{p}_i$ で分岐することになる. しかしこれは L_∞/K が最大不分岐であることに矛盾する. ok.

従って $I_i \simeq p^n\mathbb{Z}_p \simeq \mathbb{Z}_p$ が得られ, (16.4) より $\mathrm{rank}_{\mathbb{Z}_p} G(M_n/L_n) \leq s$ となり ok. □

17　最大不分岐アーベル p 拡大

A_n を k_n のイデアル類群の p 部分, L_n を定理 16.3 と同じように (M_n 内の)k_n の最大不分岐アーベル p 拡大とし, $X_n := G(L_n/k_n)$ とおく. A_n, X_n は共に Γ 加群, すなわち Λ 加群である. 類体論より, 同型

$$A_n \xrightarrow{\simeq} X_n; [\mathfrak{p}] \mapsto \left(\frac{L_n/k_n}{\mathfrak{p}}\right)$$

が成り立つことを思い出す. $X = G(M_\infty/K)$ は X_n の情報をもっており, それを上手く引き出すことで類数公式が証明される. X と X_n の関係は以下の定理より分かる.

Theorem 17.1. $L_\infty = \cup_n L_n$ が成り立つ.

Proof. かなり長いので各自読んでください $\cdots$ □

18　類数公式の証明と特性多項式

$n \geq n_0$ ならば K/k_n には分岐する素点 (特に全て完全分岐) が必ず含まれるので, $K \cap L_n = k_n$ となることが分かる. 従ってガロアの推進定理から $G(L_nK/K) \simeq G(L_n/K \cap L_n) = G(L_n/k_n)$ となり, さらに補題 7.3 と定理 17.1 より

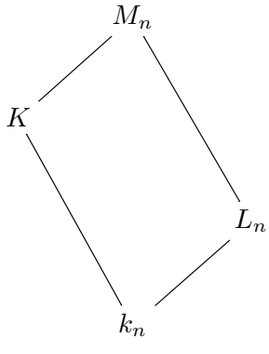
$$X \simeq \varprojlim_n G(L_nK/K) \simeq \varprojlim_n X_n \simeq \varprojlim_n A_n$$

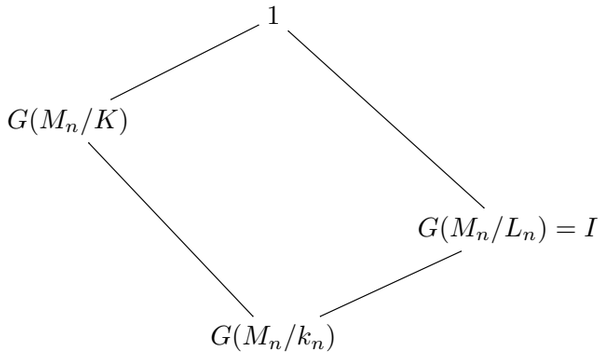
が成り立つ. つまり X には A_n の情報が集約されている. X から A_n の情報を引き出すには定理 18.1 あるいは定理 18.2 を用いる. (定理 18.1 は定理 18.2 の系として従うが, 定理 18.2 の証明の理解の手助けになるので, 別々の証明を与えることにする.)

Theorem 18.1. K/k で分岐する k の素点がただ一つで, それが K/k で完全分岐するならば

$$A_n \simeq X/\omega_n X \quad (n \geq 0).$$

Proof. 定理 16.3 と同じ記号を用いる. K/k で分岐する k の素点 $\mathfrak{p}$ の M_n/k_n における惰性群を I とする. このとき $\mathfrak{p}$ は K/k で完全分岐なので $G(M_n/L_n) = I$ が成り立つ. 一方で M_n/K は不分岐拡大であったから $I \cap G(M_n/K) = 1$ である. 従って





とガロアの推進定理より $L_nK = M_n$ でなければならない. 分かる. 以上より

$$A_n \simeq G(L_n/k_n) \simeq G(L_nK/K) = G(M_n/K) \simeq X/\omega_n X.$$

□

以下では $\Gamma = G(K/k)$ の位相的生成元 γ_0 を固定し, $\gamma_n = \gamma_0^{p^n} \in \Gamma_n$ とおく. このとき $\nu_{n,n+1} \in \Lambda$ に対応する $\mathbb{Z}_p[[\Gamma]]$ の元は以下のように確かめられることを思い出しておく.

$$\begin{aligned}\nu_{n,n+1} &= \frac{(1+T)^{p^{n+1}} - 1}{(1+T)^{p^n} - 1} = 1 + (1+T)^{p^n} + (1+T)^{2p^n} + \cdots + (1+T)^{(p-1)p^n} \\ &\longleftrightarrow 1 + \gamma_n + \gamma_n^2 + \cdots + \gamma_n^{p-1}\end{aligned}$$

Theorem 18.2. $Y = G(L_\infty/L_{n_0}K)$ とおくと

$$A_n \simeq X/\nu_{0,n}Y \quad (n \geq n_0).$$

Proof. ここでも定理 16.3 と同じ記号を用いる．また，簡単のため $n_0 = 0$ とする．$A_n \simeq G(L_nK/K) \simeq G(L_\infty/K)/G(L_\infty/L_nK) = X/G(L_\infty/L_nK)$ であるから，$G(L_\infty/L_nK) = \nu_{0,n}Y$ を示せばよい．K/k で完全分岐する k の素点を $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ とし，$\mathfrak{P}_i$ を $\mathfrak{p}_i$ の上にある L_∞ の素点の一つとする．このとき $G(L_\infty/L_nK) = \nu_{0,n}Y$ を n について帰納的に示す．

まず $n = 0$ のときを考える．$\mathfrak{P}_i$ の L_∞/k における惰性群を I_i とすると，定理 16.3 と同じ議論により制限 $I_i \to \Gamma = G(K/k)$ は同型である．(この同型を示す際に，L_∞/K が最大不分岐より $X \cap I_i = 1$ を用いている．) また，補題 16.2 より

$$G(L_\infty/k) = I_iX = XI_i,\ I_i \cap X = 1,\ I_i \simeq \mathbb{Z}_p\ (1 \leq i \leq s)$$

が成り立つ．また，$G(L_\infty/L_0) \simeq \omega_0 X I_1 \cdots I_s$ が成り立つ．

まず以下より $\omega_0 X \simeq G(L_\infty/M_0)$ が成り立つ．

$$G(L_\infty/k_0)/\omega_0 X \simeq G(k_0^{ab} \cap L_\infty/k_0) = G(M_0/k_0) \simeq G(L_\infty/k_0)/G(L_\infty/M_0)$$

また，$\varphi : I_i \simeq G(K/k) \hookrightarrow G(M_0/k)$ に対して $G(M_0/k)$ の惰性群は $\varphi(I_i)$ で与えられる．従って

$$G(M_0/k)/\varphi(I_1)\cdots\varphi(I_s) \simeq G(L_0/k)$$

が成り立つ．以上より

$$\begin{aligned} G(L_\infty/k)/G(L_\infty/M_0) \simeq G(M_0/k) &\longrightarrow G(L_\infty/k)/(G(L_\infty/M_0)I_1\cdots I_s) \simeq G(L_0/k) \\ &\longrightarrow G(L_\infty/k)/\omega_0 X I_1 \cdots I_s \simeq G(L_\infty/k)/G(L_\infty/L_0) \end{aligned}$$

を得るので，それぞれの分母を見ることで分かる．

I_i の位相的生成元 σ_i で，$\sigma_i|_K = \gamma_0$ となるものを固定する．また，$\sigma_1 = \sigma$ とおき，$\sigma_i \in I_i \simeq I_1 \subset G(L_\infty/k) = XI_1$ より $\sigma_i = x_i\sigma$ $(2 \leq i \leq s)$ と表せば

$$\begin{aligned} I_1\cdots I_s \cdot \omega_0 X &= \overline{\langle\sigma\rangle\langle x_2\sigma\rangle}\ldots\overline{\langle x_s\sigma\rangle}\cdot\omega_0 X \\ &= \overline{\langle\sigma\rangle\langle x_2,\ldots,x_s\rangle}\omega_0 X \end{aligned}$$

であり，従って

$$Y = G(L_\infty/L_0K) \simeq G(L_\infty/L_0) \cap G(L_\infty/K) = \overline{\langle\sigma\rangle\langle x_2,\ldots,x_n\rangle}\omega_0 X \cap X = \overline{\langle x_2,\ldots,x_n\rangle}\omega_0 X$$

を得る．

$\overline{\langle\sigma\rangle\langle x_2\sigma\rangle}\ldots\overline{\langle x_s\sigma\rangle} = \overline{\langle\sigma\rangle\langle x_2,\ldots,x_s\rangle}$ と $\overline{\langle\sigma\rangle\langle x_2,\ldots,x_n\rangle}\omega_0 X \cap X = \overline{\langle x_2,\ldots,x_n\rangle}\omega_0 X$ を示す．前者は

$$\sigma^{c_1}(x_2\sigma)^{c_2}\cdots(x_s\sigma)^{c_s} = \sigma^{c_1+c_2+\cdots+c_s}x_2^{c_2}\cdots x_s^{c_s}$$

から，後者は $I_1 \cap X = \overline{\langle\sigma\rangle} \cap X = 1$ から分かる．

次に $n = 1$ のときを考える．$I_i' := I_i \cap G(L_\infty/k_1)$ は $\mathfrak{P}_i$ の L_∞/k_1 における惰性群である．これまで同様に同型 $I_i' \simeq G(K/k_1) \simeq \Gamma^p \simeq I_i^p$ が成り立つ．以上より

$$G(L_\infty/L_1) = I_1^p\cdots I_s^p\omega_1 X$$

が成り立つ．また，

$$\begin{aligned} \sigma_2^p &= x_2\sigma\cdot x_2\sigma\cdot\cdots\cdot x_2\sigma \\ &= x_2(\sigma x_2\sigma^{-1})(\sigma^2 x_2\sigma^{-2})\cdots(\sigma^{p-1}x_2\sigma^{-(p-1)})\sigma^p \\ &= x_2^{1+\gamma+\cdots+\gamma^{p-1}}\sigma^p \\ &= \nu_{0,1}x_2\sigma^p \end{aligned}$$

であるから, $n=0$ のときと同様に

$$\begin{aligned}
G(L_\infty/L_1K) &\simeq G(L_\infty/L_1)\cap G(L_\infty/K)\\
&= I_1^p\cdots I_s^p\omega_1 X\cap X\\
&= \overline{\langle\sigma^p\rangle\langle\sigma_2^p\rangle}\cdots\overline{\langle\sigma_s^p\rangle}\omega_1X\cap X\\
&= \overline{\langle\nu_{0,1}x_2,\ldots,\nu_{0,1}x_s\rangle}\omega_1X\\
&= \overline{\langle\nu_{0,1}x_2,\ldots,\nu_{0,1}x_s\rangle}\omega_0\nu_{0,1}X\\
&= \nu_{0,1}\left(\overline{\langle x_2,\ldots,x_s\rangle}\omega_0X\right)\\
&= \nu_{0,1}Y
\end{aligned}$$

を得る. この操作を繰り返すことで $G(L_\infty/L_nK)=\nu_{0,n}Y$ が得られる. □

次の定理を述べる前に, 写像を一つ定義する. 以下では $m\geq n\geq n_0$ とする.

$$\nu_{n,m}: X/\nu_{n_0,n}Y\to X/\nu_{n_0,n}Y; x+\nu_{n_0,n}Y\mapsto \nu_{n,m}x+\nu_{n_0,m}Y$$

Theorem 18.3. 次の二つの図式は可換である.

$$\begin{array}{ccc} A_m & \longrightarrow & X/\nu_{n_0,m}Y\\ \downarrow{\scriptstyle N_{m,n}} & & \downarrow{\scriptstyle proj.}\\ A_n & \longrightarrow & X/\nu_{n_0,n}Y \end{array}\qquad\qquad \begin{array}{ccc} A_m & \longrightarrow & X/\nu_{n_0,m}Y\\ \uparrow{\scriptstyle incl.} & & \uparrow{\scriptstyle \nu_{n,m}}\\ A_n & \longrightarrow & X/\nu_{n_0,n}Y \end{array}$$

Proof. 類体論より. □

Theorem 18.4 (岩澤類数公式)**.** k_n の類数の p 部分を p^{e_n} と表す. このとき定数 $\mu,\lambda,\nu\in\mathbb{Z}, \mu\geq 0, \lambda\geq 0$ が存在して, 十分大きな全ての n に対し

$$e_n=\mu p^n+\lambda n+\nu$$

が成り立つ.

Proof. 定理 18.2 より $n\geq n_0$ に対して $A_n\simeq X/\nu_{n_0,n}Y$ であるから

$$|A_n|=(X:\nu_{n_0,n}Y)=(X:Y)(Y:\nu_{n_0,n}Y)$$

である. ここで, 埋め込み $Y\hookrightarrow X$ を考えると, 余核は A_{n_0} となることが簡単に分かる. 従って $(X:Y)<\infty$ と $Y\sim X$ が分かる. よって $|A_n|$ を求めるためには $|Y/\nu_{n_0,n}Y|$ を求めればよい. 定理 16.3 より X は有限生成捻れ Λ 加群であったので構造定理より

$$Y\sim X\sim(\oplus_{i=1}^r\Lambda/(p^{e_i}))\oplus\left(\oplus_{j=1}^s\Lambda/(g_j(T)^{f_j})\right) \tag{18.5}$$

である. また, 定理 14.3 では $\nu_{0,n}$ で主張を述べたが, $\nu_{n_0,n}$ としても全く同じ等式が得られる. それを適用すると

$$|Y/\nu_{n_0,n}Y|=p^{\mu p^n+\lambda n+\nu}$$

が得られて ok. (あとは $(X:Y)$ の p べき部分だけずれるが, それは ν で調整すれば ok.) □

以上により岩澤類数公式が証明された！擬同型 (18.5) から得られる多項式

$$f(T):=\prod_{i,j}p^{e_i}g_j(T)^{f_j}$$

を X の**特性多項式**と呼び,

$$f(T)\mathbb{Z}_p=(p\text{ 進 }L\text{ 関数})\mathbb{Z}_p$$

が成り立つであろうというのが**岩澤主予想**である.

19　岩澤不変量

岩澤類数公式

$$|A_n| = p^{\mu p^n + \lambda n + \nu}$$

において, 定数 $\mu = \mu(K/k), \lambda = \lambda(K/k), \nu = \nu(K/k)$ は岩澤不変量と呼ばれ, これらを計算することは整数論において重要な問題である. K/k が円分 $\mathbb{Z}_p$ 拡大 k_∞/k のときはそれぞれ $\mu_p(k), \lambda_p(k), \nu_p(k)$ のように書かれる.

岩澤は最初, 代数関数体との類似により, 「任意の $\mathbb{Z}_p$ 拡大 K/k に対して $\mu(K/k) = 0$」と予想したが, 岩澤自身により「任意の N に対し $\mu(K/k) \geq N$ となる $\mathbb{Z}_p$ 拡大が存在する」ことが証明され, 予想は否定的に解決された. しかし円分 $\mathbb{Z}_p$ 拡大に限れば $\mu = 0$ であろうと予想しているらしい. 現在までわかっていることは以下の通りである.

Conjecture 19.1 (岩澤)**.** 任意の k および任意の p に対し $\mu_p(k) = 0$.

Theorem 19.2 (岩澤)**.** $k/\mathbb{Q}$ が p 拡大ならば $\mu_p(k) = 0$.

Theorem 19.3 (フェレロ・ワシントン)**.** 任意のアーベル体 k および任意の素数 p に対し $\mu_p(k) = 0$.

λ 不変量に関しては円分 $\mathbb{Z}_p$ 拡大以外にはほとんど知られておらず, 円分 $\mathbb{Z}_p$ 拡大に関する多くの実例から, 総実代数体 k に対しては $\lambda_p(k) = 0$ であろうと予想されている.

Conjecture 19.4 (グリーンバーグ予想)**.** 任意の総実代数体 k および任意の素数 p に対し, $\mu_p(k) = \lambda_p(k) = 0$.

Theorem 19.5 (尾崎)**.** 任意の p および任意の $N \geq 0$ に対し, $\mu(K/k) = N$ となる $\mathbb{Z}_p$ 拡大 K/k が存在する.

Theorem 19.6. 任意の p および任意の $N \geq 0$ に対し, $\lambda_p(k) \geq N$ となる k が存在する.

Theorem 19.7 (木田)**.** $p = 2$ であれば, 任意の $N \geq 0$ に対し, $\lambda_p(k) \geq N$ となる k が存在する.

Theorem 19.8 (藤井, 大木, 尾崎)**.** $p = 3, 5$ であれば, 任意の $N \geq 0$ に対し, $\lambda_p(k) = N$ となる k が存在する.

k がアーベル体であれば岩澤不変量について精密な議論が可能であり, 岩澤主予想とも関係してくる. 従って次の章からは k がアーベル体の場合を詳しく扱う.

第 VI 部
アーベル体の円分 $\mathbb{Z}_p$ 拡大

20　CM 体からの準備

この本の CM 体の定義と, 複素共役写像の扱いがかなり雑なので, きちんと定義と正当化を行う.

Definition 20.1. K が CM 体であるとは,

- K; 総虚.
- $^\exists K^+$; 総実体 such that K/K^+; 二次拡大.

と定義する.

K を CM 体とする. このとき"複素共役写像" $J : K \to K$ が定まる.

Proposition 20.2. $\sigma \in \mathrm{Emd}(K, \mathbb{C})$ と $z \in K$ に対し複素共役写像 $J : K \to K$ を

$$J(z) := \sigma^{-1}(\overline{\sigma(z)})$$

と定義する. また, J は $\sigma \in \mathrm{Emd}(K, \mathbb{C})$ の取り方に依らない.

Proof. (well-defined) $\sigma^{-1}(\overline{\sigma(z)})$ が一点集合であることを示せばよい. $\sigma : K \to \sigma(K)$ は全単射なので, $\overline{\sigma(z)} \in \sigma(K)$ であることを示せば $\sigma^{-1}(\overline{\sigma(z)})$ は一意に定まる. $\sigma(z) \in \sigma(K)$ であるから $\overline{\sigma(z)} \in \overline{\sigma(K)} = \sigma(K)$ となって ok. ただし複素共役写像は全単射であることに注意.

(σ の取り方に依らない) $\sigma \neq \tau$ を $\mathrm{Emd}(K, \mathbb{C})$ から取る. このとき $\sigma^{-1}(\overline{\sigma(z)}) = \tau^{-1}(\overline{\tau(z)})$ を示せばよい. 今, 明らかに $\sigma^{-1}(\bar{\sigma}), \tau^{-1}(\bar{\tau}) \in \mathrm{Aut}_{K^+}(K) = G(K/K^+)$ であり, (ここで K^+ が総実であることを使っている.) K は総虚なので $\sigma^{-1}(\bar{\sigma}) \neq \mathrm{id}, \tau^{-1}(\bar{\tau}) \neq \mathrm{id}$ である. 従って K/K^+ は二次拡大であることより $\sigma^{-1}(\bar{\sigma}) = \tau^{-1}(\bar{\tau})$ でなければならない. □

Example 20.3. $n \geq 3$ に対し ζ_n を 1 の原始 n 乗根の一つとする. このとき $\mathbb{Q}(\zeta_n)$ は CM 体であり, $\mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{n})$ として取れる. $\mathbb{Q}(\zeta_n)^+$ が総実であることは明らかである. 他の条件は以下より従う.
($\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$; 二次拡大) ζ_n の $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ 上最小多項式は

$$X^2 - (\zeta_n + \zeta_n^{-1})X + 1 = (X - \zeta_n)(X - \zeta_n^{-1})$$

であることより ok.
($\mathbb{Q}(\zeta_n)$; 総虚) 任意の $\sigma \in \mathrm{Emb}(\mathbb{Q}(\zeta_n), \mathbb{C})$ に対して $\sigma(\zeta_n) \notin \mathbb{R}$ を示せばよい. $(\sigma(\zeta_n))^n = \sigma(\zeta_n^n) = \sigma(1) = 1$ であるから $\sigma(\zeta_n)$ は 1 の原始 n 乗根の一つである. $n \geq 3$ なので, そのような原始 n 乗根は $\mathbb{R}$ に含まれない. ok.

Lemma 20.4. K を CM 体, $x \in \mathcal{O}_K$ とする. このとき $N_{K/K^+}(x) = 1$ ならば x は 1 のべき根である.

Proof. 補題 4.1 より, 任意の $\sigma \in \mathrm{Emb}(K, \mathbb{C})$ に対し $|\sigma(x)| = 1$ を示せばよい.

$$\begin{aligned} |\sigma(x)|^2 &= \sigma(x) \cdot J(\sigma(x)) = \sigma(x) \cdot \sigma(J(x)) \quad (\because \sigma(J(x)) = \sigma(\sigma^{-1}(\overline{\sigma(x)})) = \overline{\sigma(x)} = J(\sigma(x))) \\ &= \sigma(x \cdot J(x)) = \sigma\left(N_{K/K^+}(x)\right) = \sigma(1) = 1 \end{aligned}$$

となって ok. □

Theorem 20.5. K を CM 体, E を K の単数群, E^+ を K^+ の単数群, W を K に含まれる 1 のべき根全体とする. このとき $(E : WE^+) \leq 2$ が成り立つ.

Proof. (i) 準同型 $f : E \to W/W^2$ を構成, (i)$\mathrm{Ker}\, f = WE^+$, (ii)W/W^2 の位数は 2, という順番で示す.
まず $\varepsilon \in E$ に対して $\varepsilon \cdot J(\varepsilon)^{-1} \in W$ を示す. それには補題 20.4 より $N_{K/K^+}(\varepsilon \cdot J(\varepsilon)^{-1}) = 1$ を示せばよい.

$$N_{K/K^+}(\varepsilon \cdot J(\varepsilon)^{-1}) = \varepsilon \cdot J(\varepsilon)^{-1} \cdot J(\varepsilon) \cdot J(J(\varepsilon)^{-1}) = 1$$

となって確かに ok. 以上より, 準同型

$$f : E \to W/W^2; \varepsilon \mapsto \varepsilon J(\varepsilon)^{-1} \bmod W^2$$

が well-defined に定まる.
次に $\mathrm{Ker}\, f \subset WE^+$ を示す. $\varepsilon \in \mathrm{Ker}\, f$ とすると, ある $\zeta \in W$ が存在して $\varepsilon J(\varepsilon)^{-1} = \zeta^2 = \zeta J(\zeta)^{-1}$ が成り立つ. ただし後半の等号は

$$\zeta J(\zeta) = 1 \longrightarrow \zeta = J(\zeta)^{-1} \longrightarrow \zeta^2 = \zeta J(\zeta)^{-1}$$

より従う. さて, $\varepsilon J(\varepsilon)^{-1} = \zeta J(\zeta)^{-1}$ より

$$\zeta^{-1}\varepsilon = J(\zeta)^{-1}J(\varepsilon)^{-1} = J(\zeta^{-1}\varepsilon)$$

が成り立つので $\zeta^{-1}\varepsilon \in K^+ \cap E = E^+$ を得る. つまり $\varepsilon \in \zeta E^+ \subset WE^+$ である. 次に $\mathrm{Ker}\, f \supset WE^+$ を示す. $\varepsilon = \zeta\varepsilon^+ \in WE^+$ を取る. このとき $f(\varepsilon) = 1$, すなわち $\varepsilon \cdot J(\varepsilon)^{-1} \in W^2$ を示せばよい.

$$\begin{aligned}
\varepsilon \cdot J(\varepsilon)^{-1} &= (\zeta\varepsilon^+) \cdot J(\zeta\varepsilon^+)^{-1} \\
&= \zeta\varepsilon^+ J(\varepsilon^+)^{-1} J(\zeta)^{-1} \\
&= \zeta\varepsilon^+ (\varepsilon^+)^{-1} J(\zeta)^{-1} \quad (\because \varepsilon^+ \in \mathbb{R}) \\
&= \zeta J(\zeta)^{-1} \\
&= \zeta^2 \in W^2
\end{aligned}$$

となって ok. 以上より $\mathrm{Ker}\, f = WE^+$ となり, 準同型定理より単射

$$f : E/WE^+ \hookrightarrow W/W^2$$

が誘導される.

最後に $[W : W^2] = 2$ を示せば定理の証明が終わる. W は 1 のベキ根全体の集合なので特に巡回群である. 従って $W = \langle\alpha\rangle$ と書けば, $W/W^2 = \{[1], [\alpha]\}$ であるから ok. □

CM 体 K に対して

$$Q(K) := (E : WE^+) \leq 2$$

を**単数指数**という.

M を $\mathbb{Z}_p$ 加群とし, 作用 $J \curvearrowright M$ が存在している状況を考える. このとき簡単な計算により

$$\frac{1+J}{2} + \frac{1-J}{2} = 1, \quad \frac{1+J}{2} \cdot \frac{1-J}{2} = 0$$

が分かる.

> 例えば右側の等式は, $x \in M$ に対して
>
> $$\begin{aligned}
> \frac{1+J}{2} \cdot \frac{1-J}{2}(x) &= \frac{1+J}{2}\left(\sqrt{x \cdot J(x)^{-1}}\right) \\
> &= \sqrt{\sqrt{x \cdot J(x)^{-1}} \cdot J(\sqrt{x \cdot J(x)^{-1}})} \\
> &= \sqrt{xJ(x)^{-1}J(x)x^{-1}} \\
> &= 1 \\
> &= 0(x)
> \end{aligned}$$
>
> のような計算で分かる. ただし $\sqrt{x}$ は二乗して x になるような元の一つを指していることに注意.

このとき

$$M^+ := \frac{1+J}{2}M, \quad M^- := \frac{1-J}{2}M$$

とおくと, $M = M^+ \oplus M^-$ のように, プラス部分, マイナス部分への分解が成り立つ.

21 イデアル類群へのガロア作用

22 CM 体の円分 $\mathbb{Z}_p$ 拡大

23 アーベル拡大におけるデルタ分解