穴埋め形式で学ぶ！ Hilbert の定理 90

Wathematica2024 春合宿

ゆーぐま

1 体の拡大と Galois 群

1.1 体の拡大とその分類

四則演算ができる体系を体というが, その体の構造を保って拡張する体の拡大という概念について学んでいく.

定義 1.1.1(体の拡大) L を体とする. 体 L の演算

$$+ : L \times L \to L, \times : L \times L \to L$$

に関して L の部分集合 K が部分体となっている, すなわち,

(i) 任意の $a, b \in K$ に対して, $a+b, ab \in K$
(ii) 任意の 0 でない元 $a \in K$ に対して, $a^{-1} \in K$ なる元が存在して, $aa^{-1} = a^{-1}a = 1$ を満たす.

であるとき, L は K の拡大体である, あるいは L/K は**体の拡大**であるという.

例 1.1.2. (体の拡大の例) $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$ は体の拡大である.

例 1.1.3. (添加した体) L/K を体の拡大とし, S を L の部分集合とする. $K(S)$ を S を含むような K の最小の拡大体とする. これを K **に** S **を添加した体**とよぶ. このとき, $K(S)/K$ は体の拡大である. S が有限集合であって $S = \{s_1, \ldots, s_n\}$ と表されるときは $K(S)$ を $K(s_1, \ldots, s_n)$ と略記する.

例 1.1.4. (添加した体の例) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(i)/\mathbb{Q}$ は体の拡大である.

例 1.1.5. (中間体) L/M, M/K が共に体の拡大であるとき, L/K は体の拡大であり, M を体の拡大 L/K の**中間体**という. また, $L/M/K$ を**体の拡大の列**という.

例題 1.1.6. d を平方因子を持たない, すなわち素因数分解したときに各素数に関する指数が高々 1 である 1 でない整数とする. 集合としての等式

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

を示せ.

解答. $\mathbb{Q}(\sqrt{d})$ は定義から $a, b \in \mathbb{Q}$ を含み, $\sqrt{d}$ を含むので, $a + b\sqrt{d}$ も含む. それゆえ, 右辺が左辺に含まれることが従う. 逆向きの包含を示すために, 右辺が体であることを示す. 右辺の元 $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d}$ に対して,

$$(a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d}$$

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}$$

より和と積は右辺に含まれる. また, 右辺の元 $a + b\sqrt{d}$ に対して, $\dfrac{a}{a^2 - db^2} - \dfrac{b}{a^2 - db^2}\sqrt{d}$ は右辺の元であり (分母が 0 でないことは d が平方因子を持たないことから従う),

$$(a + b\sqrt{d})\left(\frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d}\right) = \left(\frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d}\right)(a + b\sqrt{d}) = 1$$

であるので, 右辺は体であり, $\sqrt{d}$ を含むので, $\mathbb{Q}(\sqrt{d})$ の最小性から, 左辺は右辺に含まれ, 等式が示される. ■

例題 1.1.7. 体の拡大 L/K の中間体 M_1, M_2 に対して, $M_1 \cap M_2$ と $M_1 \cup M_2$ は常に体であるか. それぞれについて真偽を判定し, 真ならばその理由を示し, 偽ならば反例を挙げよ.

解答. $M_1 \cap M_2$: 真, $M_1 \cup M_2$: 偽

$M_1 \cap M_2$ が体であることを示すために, 定義で挙げた条件 (i)(ii) を確認する. $a, b \in M_1 \cap M_2$ について, M_1, M_2 は L の部分体なので, $a + b \in M_1$, $a + b \in M_2$, $ab \in M_1$, $ab \in M_2$ が同時に成立するため, (i) が成立する. また, 同様にして 0 でない $a \in M_1 \cap M_2$ に対して, $a^{-1} \in M_1$, $a^{-1} \in M_2$ が同時に言えるため, (ii) が成立するので, $M_1 \cap M_2$ は体である.

$L = \mathbb{R}$, $K = \mathbb{Q}$ とし, $M_1 = \mathbb{Q}(\sqrt{2})$, $M_2 = \mathbb{Q}(\sqrt{3})$ とすれば, $\sqrt{2} \in M_1$, $\sqrt{3} \in M_2$ に対して, $\sqrt{6} = \sqrt{2} \cdot \sqrt{3} \notin M_1 \cup M_2$ であるため, $M_1 \cup M_2$ は体でない.

定義 1.1.8. 体の拡大 L/K の中間体 M_1, M_2 を含む最小の体を**合成体**と呼び, M_1M_2 で表す.

例 1.1.9. (合成体の例) 体の拡大 $\mathbb{R}/\mathbb{Q}$ に関して, $M_1 = \mathbb{Q}(\sqrt{2})$, $M_2 = \mathbb{Q}(\sqrt{3})$ のとき, $M_1M_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b.c.d \in \mathbb{Q}\}$ である.

定義 1.1.10. (最小多項式・共役) L/K を体の拡大として, $\alpha \in L$ とする. α を根に持つ K 上のモニック (つまり最高次係数が 1 の) 多項式 f, すなわち, $a_0, a_1, \ldots, a_{n-1} \in K$ で

$$f(\alpha) = 0, \quad f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

となるような f を α の K 上の**最小多項式**という. α の最小多項式の根 β があったとき, α と β は K **上で共役**であるという.

定義 1.1.11. (拡大の用語) L/K を体の拡大とする. 拡大に関しては以下の用語がある.

- **拡大次数**: L を K 上ベクトル空間と見たときの次元を**拡大次数**と呼び, $[L : K]$ で表す.
- **有限次拡大**: 拡大次数 $d = [L : K]$ が有限の時, L/K を**有限次拡大**という. 特に, d 次拡大という.
- **無限次拡大**: 拡大次数 $[L : K]$ が無限の時, L/K を**無限次拡大**という.
- **代数的・代数拡大**: α を L の元とする. このとき, α が 0 でない K 係数の多項式の根となる, すなわち,

  $$f(\alpha) = 0, \quad f(x) = k_nx^n + k_{n-1}x^{n-1} + \cdots + k_0$$

  となるような多項式 $f(x)$(n は正整数, $k_0, \ldots, k_n \in K$ $(k_n \neq 0)$) が存在したとき, α は K 上代数的であるといい, L の任意の元が K 上代数的であるならば, 拡大 L/K を**代数拡大**という.
- **超越的・超越拡大**: α が K **上超越的**であるとは, 代数的でないことである. L/K が**超越拡大**とは, 代数拡大でないことを言う.
- **単拡大**: α を L の元とする. $L = K(\alpha)$ であったとき, 拡大 L/K を**単拡大**という.
- **正規拡大**: L/K を代数拡大とする. L の元の K 上の共役がすべて L に含まれるとき, L/K を**正規拡大**という.

有限個の元を添加する拡大の時は, 添加した元の最小多項式を調べればよい. (この事実はここでは証明を行わない)

- **代数閉体・代数閉包:** K 係数多項式の根が K にすべて入るような体 K を**代数閉体**と言い, K の拡大体で代数閉体である物はちょうど一つ存在し (証明は容易ではないので略), **代数閉包**と言い, $\overline{K}$ で表す.
- **分離拡大:** L/K を代数拡大とする. 任意の $\alpha \in L$ に対して, α の最小多項式が $\overline{K}$ 上で重根を持たないとき, L/K を**分離拡大**という. 正規拡大同様, 有限個の添加する拡大の時は, 添加した元の最小多項式を調べればよい. (ここでは証明は行わない)
- **有限次 Galois 拡大:** 正規拡大かつ分離拡大である有限次代数拡大を**有限次 Galois 拡大**という.

例題 1.1.12. $L/M/K$ を体の有限次拡大の列とする. $[L:K] = [L:M][M:K]$ を示せ.

解答. $m = [L:M]$, $n = [M:K]$ とする. L の M ベクトル空間としての基底 $\{a_1, \ldots, a_m\}$, M の K ベクトル空間としての基底 $\{b_1, \ldots, b_n\}$ を取る. この時, $\{a_i b_j\}_{1 \le i \le m, 1 \le j \le n}$ が基底, すなわち一次独立な生成系となることを示す. L の任意の元 l は,

$$l = (k_{11}b_1 + \cdots + k_{1n}b_n)a_1 + \cdots + (k_{m1}b_1 + \cdots + k_{mn}b_n)a_m$$

すなわち,

$$l = \sum_{1 \le i \le m, 1 \le j \le n} k_{ij} a_i b_j$$

となるような $k_{ij} \in K$ $(1 \le i \le m, 1 \le j \le n)$ が取れる. よって, $\{a_i b_j\}$ が生成系であることは示される. 一方で, 線形独立なことは,

$$0 = \sum_{1 \le i \le m, 1 \le j \le n} c_{ij} a_i b_j$$

但し, $c_{ij} \in K$ $(1 \le i \le m, 1 \le j \le n)$ を仮定すると,

$$0 = (c_{11}b_1 + \cdots + c_{1n}b_n)a_1 + \cdots + (c_{m1}b_1 + \cdots + c_{mn}b_n)a_m$$

となるため, $\{a_i\}$ が M-線形独立であることから, $1 \le i \le m$ に対して,

$$c_{i1}b_1 + \cdots + c_{in}b_n = 0$$

となり, $c_{i1} = \cdots = c_{in} = 0$ となり, 各係数が 0 になり, $\{a_i b_j\}$ は線形独立. ゆえに, $\{a_i b_j\}$ は mn 個の元からなるので,

$$[L : K] = mn = [L : M][M : K]$$

■

例題 1.1.13. (環論の知識が必要となるため飛ばしてもよい) L/K を体の拡大, α を K 上代数的とし, α の K 上の最小多項式を $p(X)$ とする. $f(X) \in K[X]$ の代表元を $[f(X)] \in K[X]/(p(X))$ で表す.

(1) 環の同型 $K[X]/(p(X)) \cong K[\alpha]$ を構成せよ. 但し, $K[\alpha]$ は K に α を添加した環で, $K[X]$ は K 係数多項式環である.
(2) $K[\alpha] = K(\alpha)$ を示せ.
(3) $\mathcal{B} = \{[1], [X], \ldots, [X^{n-1}]\}$ が $K(X)/(p(X))$ の基底であることを示せ.
(4) $[K(\alpha) : K] = \deg p$ を示せ.

解答.

(1) 環準同型 $\Phi : K[X] \to K[\alpha]$ を $f(X) \mapsto f(\alpha)$ で定める. これが全射で, $\operatorname{Ker}\Phi = (p(X))$ となることを示す. 全射であることは, 定義から右辺が $f(\alpha)$ の形で表せることから従う. 核を考える為に, $f(\alpha) = 0$ となるような $f(X) \in K[X]$ を考える. $f(X)$ の $p(X)$ による剰余を考えて, $f(X) = p(X)q(X) + r(X)(\deg r < \deg p)$ とできるが, α を代入すると, $r(\alpha) = 0$ となるため, 最小多項式の最小性から, $r(X) = 0$ となるので, $f(X)$ は $p(X)$ で割り切れ, 逆に $p(X)$ で割り切れれば核に入ることは明らか. 故に, $\operatorname{Ker}\Phi = (p(X))$. 故に準同型定理から構成される同型写像 $\overline{\Phi} : K[X]/(p(X)) \to K[\alpha]; [f(X)] \to f(\alpha)$ を得る.
(2) $p(X)$ は既約多項式である. 実際既約でないとすると, 次数の最小性に反してしまう. 故に, $p(X)$ は既約元なので, 素元であるから, $(p(X))$ は素イデアルで, $K[X]$ は PID だから, $(p(X))$ は極大イデアルになって, $K[X]/(p(X)) \cong K[\alpha]$ は体となるから, $K[\alpha] = K(\alpha)$.
(3) 一次独立であることを示す.

$$\sum_{k=0}^{n-1} c_k [X^k] = 0$$

を仮定すると, 代入写像は環準同型であるから, 角括弧が外に出せて,

$$\sum_{k=0}^{n-1} c_k X^k = p(X)q(X)$$

となるが, 次数の比較により $q = 0$ となるしかないため,

$$\sum_{k=0}^{n-1} c_k X^k = 0$$

となり, $c_k = 0$. 生成系であることは, $f(X) \in K(X)$ の $p(X)$ による剰余を取ることで, $f(X) = p(X)q(X) + r(X)$ ただし, $\deg r < \deg p$ とできるので, $[f(X)] = [r(X)] = \sum_{k=0}^{n-1} r_k[X^k]$ と書けることより従う.

(4) 以上の議論から, $K(\alpha)$ の基底として, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ が取れることが分かるため (環準同型で線形独立性が保存される), $[K(\alpha) : K] = \deg p$ ■

例題 1.1.14. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$, $[\mathbb{C} : \mathbb{R}]$, $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$ を求めよ.

解答. $\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ ベクトル空間の基底として $\{1, \sqrt{2}\}$ が取れ (例題 1.1.6, または $\sqrt{2}$ が代数的なことより例題 1.1.13 を用いることができる), $\mathbb{C}$ は定義より $\mathbb{R}$ ベクトル空間の基底として, $\{1, i\}$ が取れるので, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{C} : \mathbb{R}] = 2$. $\sqrt{2} + \sqrt{3}$ の最小多項式は $T^4 - 10T^2 + 1$ であるので (既約でない, すなわち 1 次式と 3 次式または 2 次式同士に因数分解できるとして矛盾を導ける), $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$

例題 1.1.15. (少し難しい) $[\mathbb{Q}(X) : \mathbb{Q}(X + X^{-1})]$, $[\mathbb{Q}(X) : \mathbb{Q}(X^2 + X^{-2})]$, $\left[\mathbb{Q}(X) : \mathbb{Q}(X^{2^{2025}} + X^{-2^{2025}})\right]$ を求めよ.

解答. 拡大 $\mathbb{Q}(X)/\mathbb{Q}(X + X^{-1})$ は, X を添加する単拡大である. X の $\mathbb{Q}(X + X^{-1})$ 上最小多項式を考える. すると, $T^2 - (X + X^{-1})T + 1$ が最小多項式である. 実際, 一次式が最小多項式だとすると, $T - X$ しかないはずで, $X \in \mathbb{Q}(X + X^{-1})$ となるはずだが, X は $X \mapsto X^{-1}$ で不変ではないので, $X \notin \mathbb{Q}(X + X^{-1})$ より矛盾. 故に, $[\mathbb{Q}(X) : \mathbb{Q}(X + X^{-1})] = 2$.

拡大 $\mathbb{Q}(X + X^{-1})/\mathbb{Q}(X^2 + X^{-2})$ は, $X + X^{-1}$ を添加する単拡大である. $X + X^{-1}$ の $\mathbb{Q}(X^2 + X^{-2})$ 上最小多項式を考える. すると, $T^2 - 2 - X^2 - X^{-2}$ が最小多項式である. 実際, 一次式が最小多項式だとすると, $T - X - X^{-1}$ しかないはずで, $X + X^{-1} \in \mathbb{Q}(X^2 + X^{-2})$ となるしかないが, $S = X + X^{-1}$ と置いてしまえば, $\mathbb{Q}(X^2 + X^{-2})$ の元は $S^2 - 2$ の多項式の分数環となるので, $S = X + X^{-1}$ は含まれない. ゆえに, $[\mathbb{Q}(X + X^{-1}) : \mathbb{Q}(X^2 + X^{-2})] = 2$. 以上より,

$$\begin{aligned}[\mathbb{Q}(X) : \mathbb{Q}(X^2 + X^{-2})] &= [\mathbb{Q}(X) : \mathbb{Q}(X + X^{-1})][\mathbb{Q}(X + X^{-1}) : \mathbb{Q}(X^2 + X^{-2})] \\ &= 2 \cdot 2 = 4\end{aligned}$$

拡大 $\mathbb{Q}(X^{2^n}+X^{-2^n})/\mathbb{Q}(X^{2^{n+1}}+X^{-2^{n+1}})$ は, $X^{2^n}+X^{-2^n}$ を添加する単拡大である. $X^{2^n}+X^{-2^n}$ の $\mathbb{Q}(X^{2^{n+1}}+X^{-2^{n+1}})$ 上最小多項式を考える. すると, $T^2-2-X^{2^n}-X^{-2^n}$ が最小多項式である. これは, 先ほどと同様に示せる. ゆえに, $[\mathbb{Q}(X^{2^n}+X^{-2^n}):\mathbb{Q}(X^{2^{n+1}}+X^{-2^{n+1}})]=2$ となり, $\left[\mathbb{Q}(X):\mathbb{Q}(X^{2^{2025}}+X^{-2^{2025}})\right]$ は,

$$[\mathbb{Q}(X):\mathbb{Q}(X^2+X^{-2})]\prod_{n=1}^{2024}[\mathbb{Q}(X^{2^n}+X^{-2^n}):\mathbb{Q}(X^{2^{n+1}}+X^{-2^{n+1}})]=2^{2026}$$

例題 1.1.16. L/K が有限次拡大ならば代数拡大であることと, L/K が超越拡大ならば無限次拡大であることを示せ.

解答. 後半は前半の対偶なので, 前半のみ示す. 任意の元 $\alpha\in L$ を取り, $d=[L:K]$ とすると, $\{1,\alpha,\dots,\alpha^d\}$ は $d+1$ 個であるから, L において K-線形従属なので,

$$k_d\alpha^d+\cdots+k_1\alpha+k_0=0$$

となるような, $k_0,k_1,\dots,k_d\in K$ で, いずれかは 0 でないようなものが存在するため, 代数拡大である. ■

例題 1.1.17. 以下の拡大の中で, (1)-(5) に当てはまるものをそれぞれ全て選択せよ. 同じ拡大を選んでもよい. 但し, 素数 p に対し, $\mathbb{F}_p:=\mathbb{Z}/p\mathbb{Z}$ である.

$$\mathbb{R}/\mathbb{Q},\quad \mathbb{C}/\mathbb{R},\quad \mathbb{Q}(\sqrt{2})/\mathbb{Q},\quad \mathbb{F}_2(X)/\mathbb{F}_2(X^2),\quad \mathbb{Q}(2^{1/3})/\mathbb{Q}$$
$$\mathbb{Q}(X,Y)/\mathbb{Q}(X),\quad \mathbb{Q}(X)/\mathbb{Q}(X+X^{-1})$$

(1) 代数拡大
(2) 超越拡大
(3) 正規拡大
(4) 分離拡大
(5) 有限次 Galois 拡大

解答.

(1) $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{F}_2(X)/\mathbb{F}_2(X^2)$, $\mathbb{Q}(2^{1/3})/\mathbb{Q}$, $\mathbb{Q}(X)/\mathbb{Q}(X+X^{-1})$
(2) $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(X,Y)/\mathbb{Q}(X)$
(3) $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{F}_2(X)/\mathbb{F}_2(X^2)$, $\mathbb{Q}(X)/\mathbb{Q}(X+X^{-1})$

(4) $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(2^{1/3})/\mathbb{Q}$, $\mathbb{Q}(X)/\mathbb{Q}(X+X^{-1})$
(5) $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(X)/\mathbb{Q}(X+X^{-1})$

$\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(X,Y)/\mathbb{Q}(X)$ が超越的であるのは, それぞれ π(超越数でよい), Y が超越的であるからである. $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(X)/\mathbb{Q}(X+X^{-1})$ が Galois 拡大なのは, それぞれ i, $\sqrt{2}$, X の単拡大であることから, これらの最小多項式の根が分離的で, なおかつすべて拡大体に入ってることが確かめられるためである. $\mathbb{F}_2(X)/\mathbb{F}_2(X^2)$, $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ についてみていく. まず, $\mathbb{F}_2(X)/\mathbb{F}_2(X^2)$ が正規であり分離的でないであることは, まずこれが X を添加する単拡大であることを考える. X の最小多項式は T^2-X^2 であるが, $X+X=2X=0$ より, $X=-X$ なので, $T^2-X^2=(T-X)(T+X)=(T-X)^2$ となり, 共役はすべて $\mathbb{F}_2(X)$ に入っており正規だが, 重根を持ち, 分離的でない. 一方で, $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ は $2^{1/3}$ の最小多項式は T^3-2 なので, 1 の虚三乗根を ω として, $T=2^{1/3}, \omega\cdot 2^{1/3}, \omega^2\cdot 2^{1/3}$ となるしかないが, $\omega\cdot 2^{1/3}$ は $\mathbb{Q}(2^{1/3})$ には入らないので, 正規ではないが, 重根はないので分離的である.

1.2 Galois 群

体の有限次 Galois 拡大の列に対しては実は Galois 群という群の列が対応付けられるという Galois 理論の要を見ていく.

定義 1.2.1. (体の同型写像) K, L を体とする. この時, 写像 $\sigma : K \to L$ が**体準同型写像**であるとは,

(i) $\sigma(a+b)=\sigma(a)+\sigma(b)$
(ii) $\sigma(ab)=\sigma(a)\sigma(b)$
(iii) $\sigma(1_K)=1_L$

が成立することである. この時, $\sigma(0_K)=0_L$ が成立する. 体の準同型写像が全単射であるとき, **同型写像**であるといい, $K \to L$ の同型写像が存在する場合は, K と L は同型であるという.

例 1.2.2. 埋め込み写像 $\iota : \mathbb{Q} \to \mathbb{R}$; $x \mapsto x$ は単射な準同型である.

例 1.2.3. 恒等写像 $\mathrm{id} : \mathbb{Q} \to \mathbb{Q}$; $x \mapsto x$ は同型である.

例 1.2.4. $\iota : \mathbb{Q}(i) \to \mathbb{C}$; $a+bi \mapsto a-bi$ $(a,b \in \mathbb{R})$ は単射な準同型である. これは, 複素数 z, w に対して, $\overline{zw}=\overline{z}\cdot\overline{w}$, $\overline{z+w}=\overline{z}+\overline{w}$ であることから従う.

定義 1.2.5. (体の自己同型写像, Galois 群) 体 K の**自己同型写像**とは, 定義域が一致した体の同型写像 $\sigma : K \to K$ のことである.

L/K を体の拡大とする. このとき, K **の元を固定する** L **の自己同型写像** $\sigma : L \to L$ とは, 任意の $k \in K$ に対して,

$$\sigma(k) = k$$

となるようなものである. K の元を固定する L の自己同型写像全体が群をなし, $\mathrm{Aut}(L/K)$ と書かれる. 特に, L/K が (有限次)Galois 拡大であるとき, $\mathrm{Gal}(L/K)$ と書かれ, Galois 群と呼ばれる.

例 1.2.6. Galois 拡大 $\mathbb{C}/\mathbb{R}$ に関して, その Galois 群を求めよう. $\mathbb{R}$ を固定するような自己同型写像 $\sigma : \mathbb{C} \to \mathbb{C}$ を考える. この時, 実数 a に対しては, $\sigma(a) = a$ である. $\mathbb{C}$ の元は $a, b \in \mathbb{R}$ を用いて, $a + ib$ と書け,

$$\sigma(a + ib) = \sigma(a) + \sigma(i)\sigma(b) = a + \sigma(i)b \qquad (*)$$

なので, 結局 $\sigma(i)$ の行き先を定めてしまえばよい. ここで, i の $\mathbb{R}$ 上の最小多項式 $f(T) = T^2 + 1$ を考えると,

$$\sigma(f(T)) = \sigma(T^2 + 1) = \sigma(T)^2 + 1$$

これに i を代入すると, $f(i) = 0$ なので,

$$\sigma(i)^2 + 1 = 0$$

となり, これを解くと, $\sigma(i) = \pm i$ とするしかなくなる. よって, $(*)$ より, $\sigma(a + ib) = a + ib$ または複素共役を取る操作 $\sigma(a + ib) = a - ib$ とするしかない. よって, 複素共役を取る写像を ϕ と置くと, $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\phi\} = \langle\phi\rangle$ となる.

例題 1.2.7. (有限次正規拡大の意義 1/2) L/K を体の有限次拡大, $\sigma \in \mathrm{Aut}(L/K)$ として, α が K 上代数的とする.

(i) $\sigma(\alpha)$ が K 上代数的であることを示せ.

(ii) $\beta \in \overline{L}$ が α と K 上共役であったとする. $K(\alpha) \cong K(\beta)$ を示せ. (ヒント: 例 1.1.13(1))

(iii) また, $[L : K(\alpha)] > 1$ であり, $\gamma_1 \in L \setminus K(\alpha)$ とする. γ_1 **の最小多項式を考え,** $\phi(\alpha) = \beta$ となるような単射準同型で, $\phi : K(\alpha, \gamma_1) \to \overline{L}$ となるようなものを作れ.

(iv) $[L : K(\alpha)]$ がどのようなときにも, $\phi(\alpha) = \beta$ となるような単射準同型で, $\phi : L \to \overline{L}$ となるようなものが存在することを示せ.

解答.

(i) α が K 上代数的ならば,

$$k_n\alpha^n + k_{n-1}\alpha^{n-1} + \cdots + k_0 = 0$$

となるような多項式 $f(X) = \sum_{i=0}^{n} k_i X^i (k_i \in K)$ が存在するから, 両辺 f に入れると, σ は K を固定する体準同型だから,

$$k_n\sigma(\alpha)^n + k_{n-1}\sigma(\alpha)^{n-1} + \cdots + k_0 = 0$$

となり, $f(\sigma(\alpha)) = 0$ となり, $\sigma(\alpha)$ は K 上代数的.

(ii) $K(\alpha)$ と $K(\beta)$ は最小多項式が同じなので, 最小多項式を $p(X)$ と置くと, $K(\alpha) \cong K(X)/p(X) \cong K(\beta)$. 具体的な同型は $\alpha \mapsto \beta$ によって与えられる.

(iii) γ_1 の $K(\alpha)$ 上の最小多項式を $p_1(X) = \sum_{i=0}^{n} p_{1i}X^n$ と置いて, $p_1'(X) = \sum_{i=0}^{n} \sigma(p_{1i})X^n$ も上の同型から $K(\beta)$ 上の最小多項式となって, その根を一つ選んで ($\overline{L}$ は代数閉体), γ_1' とすれば, $\phi(\gamma_1) = \gamma_1'$ とすれば, 生成元の行き先が決まり, K-線形写像と見たときに, 基底の行き先がすべて別となるので, 単射な ϕ が構成できる.

(iv) (iii) を繰り返し行う, つまり $\gamma_k \in L \setminus K(\alpha, \gamma_1, \ldots, \gamma_{k-1})$ を添加し続けることによって, 拡大次数を小さくすることができ, 拡大次数が 1 の時は, それらの体は一致するので, 十分大きな n に対して, $\phi : L = (\alpha, \gamma_1, \ldots, \gamma_n) \to \overline{L}$ を構成することができる. ■

この例題から以下の系が従う.

系 1.2.8. (有限次正規拡大の意義 2/2) L/K が有限次正規拡大だった時, $\alpha, \beta \in L$ に対し, 以下は同値である:

(i) α と β は K 上共役

(ii) $\phi(\alpha) = \beta$ なる体の自己同型 $\phi : L \to L$ が存在する.

証明. (ii)⇒(i) は例題 1.2.7(i) から従う. (i)⇒(ii) は例題 1.2.7(iv) から $\phi : L \to \overline{L}$ が存在し, あとは $\phi(L) = L$ を示せばいいが, $\phi(L) \subset L$ は正規性から共役が L に入るので上の定理の証明を $\overline{L}$ でなく L ですることができ, 終域を制限して $\phi : L \to L$ になって, K-線形写像で次元が同じ空間への写像とみなすと, 単射性と全単射性が同値になって同型となり題意は示される. □

例題 1.2.9. (有限次分離拡大の意義 1/3, Rotman 演習 83 改)
M/K を有限次拡大とする. 拡大 L/M で L がある多項式 $f(X) \in K(X)$ の**分解体**, すなわち $f(X)$ が根 α_i を用いて一次式 $X - \alpha_i$ と $c \in L$ の積に分解できるものが存在することを示したい.

(i) M/K は代数的で, $\alpha_1, \ldots, \alpha_n \in M$ で, $M = K(\alpha_1, \ldots, \alpha_n)$ となるようなものが存在する.
(ii) $p_i(X) \in K[X]$ が α_i の最小多項式とする. $f(X) = p_1(X) \cdots p_n(X)$ の分解体 L が存在することを証明せよ. 但し, 代数閉包の存在は認めてよい.

解答.

(i) M/K は有限次拡大なので代数拡大 (例題 1.1.16). $\alpha_1 \in M \setminus K$ を取って, $[M : K] = [M : K(\alpha_1)][K(\alpha_1) : K]$ となり, $[K(\alpha_1) : K] > 1$ となるから, $[M : K] > [M : K(\alpha_1)]$ となる. 同様に, $\alpha_{k+1} \in M \setminus K(\alpha_1, \ldots, \alpha_k)$ を添加していくと,

$$[M : K] > [M : K(\alpha_1)] > [M : K(\alpha_1, \alpha_2)] > \cdots$$

となり拡大次数は正整数なので, 十分大きい n に対して, $[M : K(\alpha_1, \cdots, \alpha_n)] = 1$ となり $M = K(\alpha_1, \cdots, \alpha_n)$ となる.
(ii) 代数閉包 $\overline{K}$ から, $p_i(X)$ の根を全て選んですべて K に添加すれば, L が構成できる.

例題 1.2.10. (有限次分離拡大の意義 2/3) K を無限体とし, $\alpha, \beta \in \overline{K}$ として, β を K 上分離的, すなわち最小多項式が重根を持たないとして, $K(\alpha, \beta)$ について考える. 以下, 最小多項式の存在は仮定してよい.

(i) $T = \{t \mid 0 = \alpha - \alpha' + t(\beta - \beta')$ 但し α', β' は α, β の K 上共役, $\beta \neq \beta'\}$ が有限集合なことに注意し, $K \setminus T$ が空でないことを示せ.

(ii) $t \in K \setminus T$ とし, $\gamma = \alpha + t\beta$ とする. $\beta \notin K(\gamma)$ **を仮定する.** β の $K(\gamma)$ 上共役が β 以外にも存在することを示せ. (ヒント: 例題 1.1.13(iv))

(iii) (ii) で存在が保証される β の $K(\gamma)$ 上共役を β' とする. $p(X)$ を α の最小多項式とし, $P(X) = p(\gamma - tX)$ に対して $P(\beta) = P(\beta') = 0$ を示せ.

(iv) $\gamma = \alpha' + t\beta'$ となるように α' を取れることと, β' が β の K 上共役であることを示せ.

(v) $t \in T$ を示して, (ii) の仮定は誤りであることを示すことによって, $K(\alpha, \beta) = K(\gamma)$ を示せ.

解答.

(i) 共役は有限個 (無限個を仮定すると最小多項式の存在に矛盾) なので, T は有限集合で, K は無限集合なので, $K \setminus T$ は空でない.

(ii) 拡大 $K(\beta, \gamma)/K(\gamma)$ を考えると, β の最小多項式は K 上分離的であり, $K(\gamma)$ 上でも分離的であるので, β の最小多項式の根の個数と次数は一致するので, これは拡大次数 $[K(\beta, \gamma) : K(\gamma)]$ とも一致するが, $\beta \notin K(\gamma)$ より, これは 1 より大きいので, β 以外の共役も存在する.

(iii)
$$P(\beta) = p(\gamma - t\beta) = p(\alpha) = 0$$
となり, さらに, β' は $K(\gamma)$ 上の β の共役なので, $K(\gamma)$ 多項式 $P(X)$ は β の最小多項式で割れて (割れないとすると剰余が次数が最小多項式より小さくなってしまい矛盾), $P(\beta') = 0$.

(iv) $\alpha' = \gamma - t\beta'$ とすればよい. β の最小多項式は $K(\gamma)$ 上より K 上の方が (係数に制限がかかるため) 次数が大きくなるから, β' が β が $K(\gamma)$ 上の共役であるので, K 上共役でもある.

(v) $0 = \gamma - \gamma = (\alpha - \alpha') + t(\beta - \beta')$ より, $t \in T$ なので, これは $K \setminus T$ に矛盾して, $\beta \in K(\gamma)$ となり, $\beta \in K(\gamma)$ と $\alpha = \gamma - t\beta \in K(\gamma)$ となり, $K(\alpha, \beta) \subset K(\gamma)$. 逆向きの包含は γ の定義から明らか. ■

例題 1.2.11. (有限次分離拡大の意義 3/3, 原始元定理)
K を無限体, L/K を体の有限次分離拡大とする. L/K が単拡大であることを示せ.

解答. 例題 1.2.9(i) より, $L = K(\alpha_1, \ldots, \alpha_n)$ と書け, 分離拡大なので, 各 α_i は分離的なので, 例題 1.2.10 を繰り返し使うことにより, 一つの元にまとめることができ, 単拡

大である.

注意 1.2.12. 有限体でも同様の定理が成立するが, 別の証明が必要となるため, ここでは省略する.

以上の系 1.2.8. と例題 1.2.11 から, 有限次 Galois 拡大の拡大次数と Galois 群の位数が結び付けられることが分かる.

例題 1.2.13. (拡大次数と位数, 少し難しい)
L/K を体の有限次 Galois 拡大とする. $|\mathrm{Gal}(L/K)| = [L : K]$ を示せ.

解答. L/K は有限次分離拡大なので, 例題 1.2.11 から, 単拡大, すなわち $L = K(\alpha)$ とできるが, α の最小多項式 $p(X)$ を考えると, 共役の個数は分離拡大なのでその次数と一致し, 系 1.2.8. から K を固定するような L の自己同型は α の像 (これは例題 1.2.7.(i) の議論を α の最小多項式 $p(X)$ に適用して, α と共役となる) と対応付けられるので, $|\mathrm{Gal}(L/K)|$ は共役の個数と一致する. 故に, 例題 1.1.13(iv) を用いて,

$$|\mathrm{Gal}(L/K)| = \deg p = [L : K]$$

■

この例題により, 以下の重要な定理が示せる.

定理 1.2.14. (Galois 理論の基本定理)
L/K を有限次 Galois 拡大, $G = \mathrm{Gal}(L/K)$ とする. L/K の中間体全体の集合を $\mathrm{Lat}(L/K)$, G の部分群全体を $\mathrm{Sub}(G)$ とするとこれらには 1 対 1 対応がある.

$$\Phi : \mathrm{Sub}(G) \to \mathrm{Lat}(L/K); H \mapsto L^H := \{x \in L \mid {}^\forall\sigma \in H, \sigma(x) = x\}$$

$$\Psi : \mathrm{Lat}(L/K) \to \mathrm{Sub}(G); M \mapsto \mathrm{Gal}(L/M)$$

は互いの逆写像になり, 特に全単射となる. また, $H_1 \subset H_2$ ならば $\Phi(H_1) \supset \Phi(H_2)$ のように順序を逆にする写像になる.

証明. 順序を逆にすることは, 固定するものが多くなれば自己同型は減るので明らか. $\Phi \circ \Psi = \mathrm{Id}$ を示す. 定義より $M \subset L^{\mathrm{Gal}(L/M)}$ で,

$$[L : M] = [L : L^{\mathrm{Gal}(L/M)}][L^{\mathrm{Gal}(L/M)} : M] \geq [L : L^{\mathrm{Gal}(L/M)}] = |\mathrm{Gal}(L/M)| = [L : M]$$

から, $[L^{\mathrm{Gal}(L/M)} : M] = 1$ なので, $M = L^{\mathrm{Gal}(L/M)}$. $\Psi \circ \Phi = \mathrm{Id}$ を示す. G の部分群 H に関して, L/L^H が Galois 拡大で, $\mathrm{Gal}(L/L^H) \supset H$ を示す. $X \in L$ の H による

軌道を $H \cdot X$ と表すと,

$$f_X(T) = \prod_{\widetilde{X} \in H \cdot X} (T - \widetilde{X})$$

は X を根に持つ重根を持たない L^H 係数 (各係数は $H \cdot X$ の元の対称式になるため H の作用で不変) 多項式だから, L/L^H は分離拡大で,

$$[L^H(X) : L^H] \leq |H| \tag{$*1$}$$

となる. ここで, $[L^H(X) : L^H]$ が最大となるような $X \in L$ を $X_{\max}$ と置くと, $L^H(X_{\max}) = L$ となることが示せる. (ヒント: 背理法, 例題 1.2.9(i)) $X_{\max}$ の最小多項式 $g(T)$ を考えると, 異なる $\sigma, \tau \in H$ に関して, $X_{\max}$ の像は異なるから,

$$|H| \leq (y\text{の共役の個数}) \overset{\text{分離的}}{=} \deg g = [L : L^H] \tag{$*2$}$$

となって, $(*1)(*2)$ より, $|H| = [L : L^H]$. $H \subset \mathrm{Gal}(L/L^H)$ は明らかだから, $H = \mathrm{Gal}(L/L^H)$. なお, 写像の well-defined 性だが, σ が自己同型だから, 固定される元は和と積, 乗法逆元についても固定されるので, Φ は well-defined. L/M は有限次なのは明らかで, 正規拡大・分離拡大なのは, 上で示したとおりである. ■

基本定理の嬉しさは, 中間体の様子を, 部分群と対応付けて書くことができるという点にある.

例 1.2.15. 体の拡大 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ の中間体 M を全て決定しよう. $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ を考えると,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

となり, Galois 群は

$$\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}) = \sqrt{3}$$
$$\tau(\sqrt{2}) = \sqrt{2}, \tau(\sqrt{3}) = -\sqrt{3}$$

となるような体自己同型 σ, τ を用いて,

$$G = \langle \sigma, \tau \mid \sigma^2 = \mathrm{id}, \tau^2 = \mathrm{id}, \sigma\tau = \tau\sigma \rangle$$

と表示できる. $\langle \mathrm{id} \rangle$, $\langle \sigma \rangle$, $\langle \tau \rangle$, $\langle \sigma\tau \rangle$ に対応する中間体は, 上記定理の Φ を見ることで, それぞれ,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{6})$$

が分かる.

2 群コホモロジー

2.1 群の加群

群の性質を見るためには, Galois 群のように, 何かに作用させることが重要である. そこで, 体だけではなく, Abel 群に群を作用させてみることを考える.

定義 2.1.1. (群の加群) G を群とする. **(左)G 加群** M とは, Abel 群 M と, 作用と呼ばれる写像 $\cdot : G \times M \to M$ で, $g \in G$ と $a, b \in M$ に対して,

(i) $g \cdot (a + b) = g \cdot a + g \cdot b$
(ii) $(gh) \cdot a = g \cdot (h \cdot a)$
(iii) $e_G \cdot a = a$

となるようなものの組である. 但し Abel 群を加法群として書いたが, 乗法として記す場合は

(i) $g \cdot (ab) = (g \cdot a)(g \cdot b)$
(ii) $(gh) \cdot a = g \cdot (h \cdot a)$
(iii) $e_G \cdot a = a$

となることに注意しよう.

例 2.1.2. (Hilbert の定理 90 で使う例 1) L/K を体の拡大とする. $L^\times := L \setminus \{0\}$ の乗法に関する Abel 群 $L^\times$ は, $\sigma \in \mathrm{Gal}(L/K)$ と $l \in L^\times$ に対して,

$$\sigma \cdot l = \sigma(l)$$

とすれば, 左 $\mathrm{Gal}(L/K)$ 加群である.

例 2.1.3. (Hilbert の定理 90 で使う例 2) L/K を体の拡大とする. L の加法に関する Abel 群 L は, $\sigma \in \mathrm{Gal}(L/K)$ と $l \in L$ に対して,

$$\sigma \cdot l = \sigma(l)$$

とすれば, 左 $\mathrm{Gal}(L/K)$ 加群である.

群の表現を知っている場合は, 以下のような例もある:

例 2.1.4. (群の表現と G-加群) (V, ρ) を群 G の表現とする. この時,

$$g \cdot v = \rho(g)v$$

とすれば線形空間 V を Abel 群とみなした時, 左 G 加群である.

2.2　ホモロジー・コホモロジー

Abel 群などの環の加群を調べる手段としてよく使われる手法が, ホモロジー, コホモロジーである. まず, ホモロジーとコホモロジーが現れるチェイン複体, コチェイン複体について解説していく.

定義 2.2.1. チェイン複体 C_* とは整数で添字づけられた加群の列 $\{C_q\}_{q\in\mathbb{Z}}$ とその間の準同型 $\partial_q : C_q \to C_{q-1}$ の組で, 準同型として

$$\partial_q \circ \partial_{q+1} = 0 \quad (^\forall q \in \mathbb{Z})$$

という関係式を満たす

$$C_* : \cdots \xrightarrow{\partial_{q+2}} C_{q+1} \xrightarrow{\partial_{q+1}} C_q \xrightarrow{\partial_q} \cdots \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} C_{-1} \xrightarrow{\partial_{-1}} \cdots$$

のようなものを言う.

また, **コチェイン複体** C^* とは整数で添字づけられた加群の列 $\{C^q\}_{q\in\mathbb{Z}}$ とその間の準同型 $d^q : C^q \to C^{q+1}$ の組で, 準同型として

$$d^{q+1} \circ d^q = 0 \quad (^\forall q \in \mathbb{Z})$$

という関係式を満たす

$$C^* : \cdots \xleftarrow{d^{q+2}} C^{q+1} \xleftarrow{d^{q+1}} C^q \xleftarrow{d^q} \cdots \xleftarrow{d^2} C^1 \xleftarrow{d^1} C^0 \xleftarrow{d^0} C^{-1} \xleftarrow{d^{-1}} \cdots$$

のようなものを言う.

例 2.2.2. (群のコチェイン複体) G を群とし, M を左 G-加群とする. この時, $C^q(G,M)$ を G^q から M への写像全体のなす Abel 群とする. ただし, $q = 0$ の時 $C^0(G,M)$ を 0 から M の写像全体, $q < 0$ の時, $C^q(G,M) = 0$ とし, 準同型 $d^{q+1} : C^q(G,M) \to C^{q+1}(G,M)$ を $f \in C^q(G,M)$ に対して,

$$(d^{q+1}f)(g_1,\ldots,g_{q+1}) := g_1 \cdot f(g_2\ldots,g_{q+1}) + \sum_{i=1}^{q}(-1)^i f(g_1,\ldots,g_ig_{i+1},\ldots,g_{q+1})$$
$$+(-1)^{q+1}f(g_1,\ldots,g_q)$$

ただし,

$$(d^1 f)(g_1) = g_1 f(0) - f(0)$$

とみなす. すると, これはコチェイン複体になる.(計算は煩雑になるが単純に計算すれば示せる)

他の例は, 単体複体, 胞体複体, 特異ホモロジー, Čech コホモロジー, de Rham コホモロジーなどで調べると良い.

例題 2.2.3. コチェイン複体 C^* に関して, C^q の部分加群 $Z^q = \operatorname{Ker} d^q$, $B^q = \operatorname{Im} d^{q+1}$ に関して, $Z^q \supset B^q$ を示せ. なお, Z^q, B^q の元はコサイクル, コバウンダリと呼ばれる.

解答. Z^q の元は, C^{q+1} の元 m を用いて, $d^{q+1}(m)$ と表せるため, これは

$$d^q \circ d^{q+1}(m) = 0$$

より, $d^{q+1}(m) \in \operatorname{Ker} d^q = Z^q$ より示された. ■

この例題より, コホモロジー群と呼ばれる群を定義したくなる. これは, 準同型の核と像がどれだけ差を持っているかというデータを持っている.

定義 2.2.4. $H^q = Z^q/B^q = \operatorname{Ker} d/\operatorname{Im} d$ は**コホモロジー群**と呼ばれる. **ホモロジー群**も同様に, $H_q = Z_q/B_q = \operatorname{Ker} \partial/\operatorname{Im} \partial$ と定義する.

例題 2.2.5. G を群, M を Abel 群とする. 群のコチェイン複体 $C^*(G, M)$ に関して, $Z^1(G, M)$, $B^1(G, M)$ を書き下せ. また, $H^1(G, M) = 0$(乗法群としてみるならば 1) となるのはどのようなときか.

解答. 連結準同型は,

$$(d^1 f)(g_1) = g_1 f(0) - f(0)$$

$$(d^2 f)(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1)$$

となるので,

$$Z^1(G, M) = \{f \in C^1(G, M) \mid {}^\forall g_1, g_2 \in G, g_1 f(g_2) - f(g_1 g_2) + f(g_1) = 0\}$$

$$B^1(G, M) = \{f \in C^1(G, M) \mid {}^\exists m \in M, f(g_1) = g_1 m - m\}$$

$H^1(G, M) = 0$ となるのは, $Z^1(G, M) \subset B^1(G, M)$ という事だから, $Z^1(G, M) = B^1(G, M)$ の時. すなわち, $f \in C^1(G, M)$ に対して,

$${}^\forall g_1, g_2 \in G, g_1 f(g_2) - f(g_1 g_2) + f(g_1) = 0$$

と

$$^{\exists}m \in M, f(g_1) = g_1 m - m$$

が同値になる時である．なお乗法群の時は

$$Z^1(G, M) = \{f \in C^1(G, M) \mid {}^{\forall}g_1, g_2 \in G, (g_1 \cdot f(g_2))f(g_1 g_2)^{-1} f(g_1) = 1\}$$
$$B^1(G, M) = \{f \in C^1(G, M) \mid {}^{\exists}m \in M, f(g_1) = (g_1 \cdot m)m^{-1}\}$$

となる．

2.3 Hilbert の定理 90

準備ができたので, 早速本定理の主張を見ていこう．

定理 2.3.1. (Hilbert の定理 90) $H^1(\mathrm{Gal}(L/K), L^\times) = \{1\}$, $H^1(\mathrm{Gal}(L/K), L) = \{0\}$

つまり, $L^\times, L$ の左 $\mathrm{Gal}(L/K)$ 加群の 1 次のコホモロジーが消滅すること, あるいは同じことだが, $\mathrm{Ker}\, d^1 = \mathrm{Im}\, d^1$ という事を主張している．証明に移る前に, この定理の強力さを見てみよう．

例題 2.3.2. (Hilbert の定理 90 と Pythagoras 数)
$H^1(\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}), \mathbb{Q}(i)^\times) = \{1\}$ から, $x^2 + y^2 = 1$ となるようなどちらかが 0 でない有理数の組 (x, y) の条件を, ある $u + vi \in \mathbb{Q}(i)$ に関する条件として表せ．

解答. まず $f \in Z^1(\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}), \mathbb{Q}(i)^\times)$ という条件は, σ を複素共役, $\alpha = f(\sigma) \in \mathbb{Q}(i)^\times$ とすると, $i, j = 0, 1$ として,

$$\sigma^i f(\sigma^j) f(\sigma^i) = f(\sigma^i \sigma^j)$$

$i = 0$ または $j = 0$ のときは明らかに成り立つから,

$$\alpha\sigma(\alpha) = f(\mathrm{id}) = 1$$

すなわち

$$\alpha\overline{\alpha} = 1$$

という条件になる．次に, $f \in B^1(\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}), \mathbb{Q}(i)^\times)$ という条件は, $\exists\varphi \in C^0(G, M)$ で, $z = \varphi(1) \in \mathbb{Q}(i)^\times$ とすると,

$$\alpha = f(\sigma) = (d^1\varphi)(\sigma) = \frac{\sigma(z)}{z} = \frac{\overline{z}}{z}$$

を満たすという条件に書き換えられる．$\alpha = x + yi$ と置くと，

$$x^2 + y^2 = 1 \Leftrightarrow \exists u + vi \in \mathbb{Q}(i), x + yi = \frac{u - vi}{u + vi} = \frac{u^2 - v^2 - 2uvi}{u^2 + v^2}$$

よって，分母の最大公約数を掛けることで，Pythagoras 数を全て求めることができる．

さて，本定理の証明に移ろう．一つ補題を用意する．

例題 2.3.3. (Dedekind の補題) K, L を体，$\chi_1, \cdots, \chi_n$ を $K \to L$ の乗法を保つ $(\chi(ab) = \chi(a)\chi(b))$ 準同型とする．この時，$\chi_1, \cdots, \chi_n$ は L-ベクトル空間の元として一次独立であることを帰納法と背理法で示せ．

証明. $n = 1$ の時明らか．$n \leq k - 1$ の時成立すると仮定して，背理法で $n = k$ の時を示す．

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$$

となるような，いずれかは 0 でないような $a_1, \ldots, a_n$ が存在すると仮定する．$a_i = 0$ となる i があるとすると，帰納法の仮定からすべて 0 となり矛盾．よってすべての i に対して $a_i \neq 0$ を仮定してよい．$\chi_1(\alpha) \neq \chi_2(\alpha)$ となるような α を取って，

$$a_2(\chi_1(\alpha) - \chi_2(\alpha))\chi_2(x) + \cdots + a_2(\chi_1(\alpha) - \chi_n(\alpha))\chi_n(x) = 0$$

しかし帰納法の仮定により，$\chi_1(\alpha) = \chi_2(\alpha)$ となり矛盾． ■

(本定理の証明，計算はところどころ省略している) $f \in Z^1(\mathrm{Gal}(L/K), L)$ を取ると，Dedekind の補題の対偶から，$\sum_{\tau \in \mathrm{Gal}(L/K)} \tau(\xi) \neq 0$ なる $x \in L$ が存在して，$\eta = \sum_{\tau \in \mathrm{Gal}(L/K)} \tau(\xi)$ は $\mathrm{Gal}(L/K)$ の作用に関して不変で，

$$\sum_{\rho \in \mathrm{Gal}(L/K)} \rho(-\eta^{-1}\xi) = -\eta^{-1} \sum_{\rho \in \mathrm{Gal}(L/K)} \rho(\xi) = -1$$

$\beta = \sum_{\tau \in \mathrm{Gal}(L/K)} f(\tau)\tau(-\eta^{-1}\xi)$ とすれば，

$$-f(\sigma) = \sum_{\rho \in \mathrm{Gal}(L/K)} f(\sigma)\rho(-\eta^{-1}\xi)$$

一方で，$h \in Z^1(\mathrm{Gal}(L/K), L)$ つまり，$f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$ に注意して計算すると，

$$\beta - \sigma(\beta) = \sum_{\rho \in \mathrm{Gal}(L/K)} f(\sigma)\rho(-\eta^{-1}\xi)$$

が示せるので, $f(\sigma) = \sigma(\beta) - \beta \in B^1(\mathrm{Gal}(L/K), L)$.

一方で乗法群については, $h \in Z^1(\mathrm{Gal}(L/K), L^\times)$ とすると, Dedekind の補題の対偶から,

$$\sum_{\tau \in \mathrm{Gal}(L/K)} h(\tau)\tau(\alpha) \neq 0$$

なる $\alpha \in L^\times$ が存在して, $\sigma \in \mathrm{Gal}(L/K)$ に対して, $\beta = \sum_{\tau \in \mathrm{Gal}(L/K)} h(\tau)\tau(\alpha)$ と置くと,

$$\begin{aligned}
\sigma(\beta) &= \sum_{\tau \in \mathrm{Gal}(L/K)} \sigma(h(\tau))\sigma\tau(\alpha) \\
&= \sum_{\tau \in \mathrm{Gal}(L/K)} h(\sigma\tau)h(\sigma)^{-1}\tau(\alpha) \qquad (h \in Z^1(\mathrm{Gal}(L/K), L^\times) \text{ を用いた.}) \\
&= h(\sigma)^{-1} \sum_{\tau \in \mathrm{Gal}(L/K)} h(\sigma\tau)\tau(\alpha) \\
&= h(\sigma)^{-1}\beta \in B^1(\mathrm{Gal}(L/K), L^\times)
\end{aligned}$$

以上により本定理が示される. ■