第 1 章　体

体について述べる。

1.1　体

定義 1.1.1 (素体). k を体とする。k の部分体すべての共通部分を k の**素体 (prime field)** という。

定義 1.1.2 (標数). k を体とし、環準同型 $\mathbb{Z} \to k,\ n \mapsto n1_k$ を ϕ とおく。$1_k = \phi(1) \in \operatorname{Im}\phi$ ゆえに $\operatorname{Im}\phi \neq 0$ であり、また $\operatorname{Im}\phi$ は整域だから、準同型定理より $\operatorname{Ker}\phi$ は $\mathbb{Z}$ の素イデアルである。よって $\operatorname{Ker}\phi = (p)$ (p は 0 または素数) と表せる。p を k の**標数 (characteristic)** という。

1.2　有限体

定義 1.2.1 (有限体). 濃度が有限の体を**有限体 (finite field)** という。

定理 1.2.2 (有限体の濃度). 有限体の濃度は素数の冪である。

証明.　k を有限体とし、k の標数を p とおく。$p = 0$ だとすると k が $\mathbb{Z}$ と同型な部分環を含むことになり k の濃度が有限であることに反するから、p は素数である。よって k は $\mathbb{Z}/p\mathbb{Z}$ と同型な部分環、より強く部分体をもつ。k を左正則加群とみなせば、係数制限により k は $\mathbb{Z}/p\mathbb{Z}$ 上のベクトル空間となり、いま k の濃度は有限だから $\dim_{\mathbb{Z}/p\mathbb{Z}} k =: n \in \mathbb{Z}_{\geq 1}$ である。よって k の濃度は $\sharp k = p^n$ である。 □

第 2 章　体の拡大

2.1　体の拡大

多角形の対称変換と多項式の Galois 群との関連は次のように整理できる：

[TODO] なぜここに書いてある？

多角形 P	多項式 $f(x) \in F[x]$
平面	$f(x)$ の分離体 E
頂点 $\mathrm{Vert}(P) = \{v_1, \ldots, v_n\}$	根 $\alpha_1, \ldots, \alpha_n$
線型変換	E の自己同型
直交変換	F を固定する E の自己同型
P を固定する直交変換の群	Galois 群 $\mathrm{Gal}(f) = \mathrm{Gal}(E/F)$
正多角形	既約多項式

定義 2.1.1 (体の拡大). L を体とする。L の部分環 K が体であるとき、K を L の**部分体 (subfield)** といい、L を K の**拡大体 (extension field)** という。L/K **は体の拡大である**ともいう。L の K-ベクトル空間としての次元を $[L : K]$ と書き、L の K 上の**拡大次数 (degree of field extensioni)** という。

例 2.1.2 (拡大体の例).

- $\mathbb{R}$ は $\mathbb{Q}$ の拡大体である。
- $\mathbb{C}$ は $\mathbb{R}$ の拡大体である。$\mathbb{C}$ は $\mathbb{R}$-ベクトル空間として基底 $\{1, \sqrt{-1}\}$ がとれるので $[\mathbb{C} : \mathbb{R}] = 2$ である。したがって $\mathbb{C}$ は $\mathbb{R}$ の 2 次拡大である。
- $d \neq 1$ を square-free な整数とする（e.g. $d = 6$）。$L = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \in \mathbb{Q} : a, b \in \mathbb{Q}\}$ は $\mathbb{C}$ の部分体である（実際、$\mathbb{Q}[\sqrt{d}] \cong \mathbb{Q}[x]/(x^2 - d)$ であり、$x^2 - d$ は $\mathbb{Q}[x]$ の既約元（$\because$ L は $\mathbb{C}$ の部分環ゆえに整域）だから、$\mathbb{Q}$ が体であることと併せて $\mathbb{Q}[x]/(x^2 - d)$ は体である）。$\sqrt{d} \notin \mathbb{Q}$ ゆえに $[L : \mathbb{Q}] \geq 2$ である。L は $\mathbb{Q}$-ベクトル空間として基底 $\{1, \sqrt{d}\}$ がとれるので $[L : \mathbb{Q}] = 2$ である。
- K を体とする。$A = K[x_1, \ldots, x_n]$ を n 変数多項式環、$L = K(x_1, \ldots, x_n)$ を n 変数有理関数体とする。A の K-ベクトル空間としての次元は ∞ である。さらに A は整域なので、その商体 $K(x_1, \ldots, x_n)$ への自然な準同型は単射、したがって A は $K(x_1, \ldots, x_n)$ に含まれ

る。よって $K(x_1,...,x_n)/K$ は無限次拡大である。

定義 2.1.3 (代数体). $\mathbb{Q}$ の有限次拡大体を**代数体 (algebraic field)** という。

定義 2.1.4 (合成体). L を体とし、M_1, M_2 を L の部分体とする。[TODO]

命題 2.1.5 (体の準同型). K を体とし、L, M を K の拡大体とする。

(1) $S \subset L$ に対し包含写像 $S \hookrightarrow K(S)$ は K の拡大体の圏のエピ射である。

$$S \hookrightarrow K(S) \rightrightarrows \bullet \tag{1}$$

すなわち、K の拡大体の間の準同型 $K(S) \to \bullet$ は S 上の値で決まる。

(2) [TODO]

証明. cf. [雪江] p.163 □

2.2 添加

定義 2.2.1 (添加). L/K を体の拡大、$S \subset L$ を部分集合とする。

- S が有限集合 $S = \{\alpha_1,...,\alpha_n\}$ なら

$$K(S) := \left\{ \frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)} \in L : \frac{f(x_1,...,x_n)}{g(x_1,...,x_n)} \text{ は } K \text{ 係数有理式}, \ g(\alpha_1,...,\alpha_n) \neq 0 \right\} \tag{1}$$

- S が無限集合なら

$$K(S) := \bigcup_{\substack{S' \subset S \\ |S'| < \infty}} K(S') \tag{2}$$

と定義する。$K(S)$ を K に S を**添加 (adjunction)** した体という。

- S が有限集合ならば $K(S)$ は K 上**有限生成 (finitely-generated)** といい、
- S が 1 元集合ならば $K(S)$ は K の**単拡大** であるという。

例 2.2.2 (有限生成だが有限次拡大でない例). K を体とする。K 上の 1 変数有理関数体 $K(x)$ は K 上有限生成である。しかし拡大次数は ∞ である。

定義 2.2.3 (代数拡大と超越拡大). L/K を体の拡大、$x \in L$ とする。$a_0, \ldots, a_n \in K$、少なくともひとつは 0 でない、が存在して

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0 \tag{3}$$

が成り立つとき、x は K 上**代数的 (algebraic)** であるといい、そうでなければ x は K 上**超越的 (trancendental)** であるという。L のすべての元が K 上代数的ならば、L/K は**代数拡大 (algebraic extension)** といい、そうでなければ L/K は**超越拡大 (trancendental extension)** という。

例 2.2.4 (有限生成と代数拡大).

- $\mathbb{Q}(\pi)/\mathbb{Q}$ は有限生成だが代数拡大でない。
- $\mathbb{Q}(\{\sqrt[n]{2} \colon n = 1, 2, \ldots\})$ は代数拡大だが有限生成でない。

命題 2.2.5 (有限次拡大は代数拡大). 体の拡大 L/K が有限次拡大ならば、L/K は代数拡大である。

証明. 省略 □

命題 2.2.6 (有限群の Lagrange の定理の類似). $L/M, M/K$ を体の有限次拡大とする。このとき、L/K も有限次拡大で

$$[L \colon K] = [L \colon M][M \colon K] \tag{4}$$

が成り立つ。

証明. 省略 □

定義 2.2.7 (最小多項式). L/K を体の代数拡大とし、$\alpha \in L$ とする。K 上の 0 でないモニック多項式 f で $f(\alpha) = 0$ をみたすもののうち $\deg f(x)$ が最小となるものが一意に存在する（証明略)。これを α の K 上の**最小多項式 (minimal polynomial)** という。

定義 2.2.8 (共役). L, M を K の拡大体、$\alpha \in L$ とする。α の K 上の最小多項式を f とするとき、f の根で M に属するものを、α の M における K 上の**共役 (conjugate)**、あるいは単に K 上の

共役という。

$$
\begin{tikzcd}[column sep=small]
\alpha \arrow[d, phantom, "\rotatebox{90}{$\in$}"] & & \\
L \arrow[dr, no head] & & M \arrow[dl, no head] \\
& K &
\end{tikzcd}
\tag{5}
$$

例 2.2.9 (共役の例)**.** $d \neq 1$ を square-free な整数とする (e.g. $d = 6$)。$\sqrt{d}$ の $\mathbb{Q}$ 上の最小多項式は $x^2 - d = (x - \sqrt{d})(x + \sqrt{d})$ なので、$\sqrt{d}$ の $\mathbb{Q}$ 上の共役は $\pm\sqrt{d}$ である。

$$
\begin{tikzcd}[column sep=small]
\sqrt{d} \arrow[d, phantom, "\rotatebox{90}{$\in$}"] & & -\sqrt{d} \arrow[d, phantom, "\rotatebox{90}{$\in$}"] \\
\mathbb{Q}[\sqrt{d}] \arrow[dr, no head] & & \mathbb{Q}[\sqrt{d}] \arrow[dl, no head] \\
& \mathbb{Q} &
\end{tikzcd}
\tag{6}
$$

命題 2.2.10 (共役は K 準同型で保たれる)**.** L/K を代数拡大、F/K を拡大とする。各 $\alpha \in L$ と $\phi \in \mathrm{Hom}_K^{\mathrm{al}}(L, F)$ に対し、$\phi(\alpha)$ は α の共役である。

$$
\begin{tikzcd}[column sep=small]
\alpha \arrow[rr, mapsto] \arrow[d, phantom, "\rotatebox{90}{$\in$}"] & & \phi(\alpha) \arrow[d, phantom, "\rotatebox{90}{$\in$}"] \\
L \arrow[rr, "\phi"] \arrow[dr, no head] & & F \arrow[dl, no head] \\
& K &
\end{tikzcd}
\tag{7}
$$

証明. cf. [雪江] p.167 □

2.3 代数閉包

定義 2.3.1 (代数閉包)**.** K を体とする。L/K が代数拡大であり L が代数的閉体であるとき、L を K の**代数閉包 (algebraic closure)** という。

定理 2.3.2 (代数閉包の存在 (Steinitz))**.** [TODO]

証明. 省略 □

2.4 分離拡大

定義 2.4.1 (分離拡大)**.**

- $f(x) \in K[x], \alpha \in \overline{K}$ で、$f(x)$ が $\overline{K}[x]$ で $(x-\alpha)^2$ で割り切れるとき、α を $f(x)$ の**重根 (multiple root)** という。
- $f(x)$ が $\overline{K}$ に重根を持たないとき、$f(x)$ を**分離多項式 (separable polynomial)** という。
- $\alpha \in \overline{K}$ の K 上の最小多項式が分離多項式であるとき、α は K 上**分離的 (separable)** であるといい、そうでなければ**非分離的 (inseparable)** であるという。
- K の代数拡大 L のすべての元が K 上分離的であるとき、L を K の**分離拡大 (separable extension)** といい、そうでなければ**非分離拡大 (inseparable extension)** であるという。
- K の任意の代数拡大が K の分離拡大ならば、K を**完全体 (perfect field)** という。

多項式が分離多項式かどうかは、微分をみて判定することができる。

命題 2.4.2 (分離多項式と微分)**.** K を体とし、$f(x) \in K[x]$ とする。このとき、次は同値である：

(1) $f(x)$ は分離多項式である。
(2) $f(x)$ と $f'(x)$ は互いに素である。

証明. 省略 □

例 2.4.3 (分離的な元)**.** p を素数、K を標数 p の体とする。$a \in K, f(x) = x^p - x - a$ とおく。$\alpha \in \overline{K}$ が $f(x)$ の根なら、$f'(x) = -1$ なので、α は K 上分離的である（実際、もし α が K 上分離的でなかったとすれば、α の K 上の最小多項式 $g(x)$ は $\overline{K}$ に重根を持つ。よって、いま $f(\alpha) = 0$ ゆえに f は g で割り切れることから、f は $\overline{K}$ に重根を持つ。一方、$f(x)$ と $f'(x)$ は互いに素だから、$f(x)$ は $\overline{K}$ に重根を持たず、矛盾)。

例 2.4.4 (非分離拡大の例)**.** [TODO]

代数拡大が分離拡大かどうかを考えるとき、もとの体が完全体ならば話は簡単である。次の命題は体が完全体であるための十分条件を与える。

命題 2.4.5 (完全体であるための十分条件)**.** 標数 0 の体と有限体は完全体である。

証明. 省略 □

定義 2.4.6 (分離閉包)**.** L/K を代数拡大とする。L の元で K 上分離的なもの全体の集合を L_s と書き、L における K の**分離閉包 (separable closure)** という。また、$\overline{K}$ における K の分離閉包を K^s と書き、K の**分離閉包**という。

定義 2.4.7 (分離次数)**.** L/K を有限次拡大とする。

- $[L_s : K]$ を L の K 上の**分離次数 (separable degree)** といい、$[L : K]_s$ と書く。
- $[L : L_s]$ を L の K 上の**非分離次数 (inseparable degree)** といい、$[L : K]_i$ と書く。

命題 2.4.8 (分離次数とホムセットの濃度)**.** L/K を有限次拡大とする。

(1) [TODO]
(2) $[L : K]_s = |\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})|$

証明. cf. [雪江] p.183 □

例 2.4.9 ($\mathbb{Q}(\sqrt{d})$ のホムセット)**.** $d \neq 1$ を square-free な整数とし (e.g. $d = 6$)、$L = \mathbb{Q}(\sqrt{d})$ とする。$\mathrm{ch}\, L = 0$ なので、$L/\mathbb{Q}$ は分離拡大である (命題 2.4.5)。よって $|\mathrm{Hom}_{\mathbb{Q}}^{\mathrm{al}}(L, \overline{\mathbb{Q}})| = 2$ である (命題2.4.8)[TODO]?。$\sigma \in \mathrm{Hom}_{\mathbb{Q}}^{\mathrm{al}}(L, \overline{\mathbb{Q}})$ とすると、L が $\mathbb{Q}$ の代数拡大であることから、命題2.2.10 より $\sigma(\sqrt{d})$ は $\sqrt{d}$ の $\mathbb{Q}$ 上の共役、すなわち $\sigma(\sqrt{d}) = \pm\sqrt{d}$ である (例2.2.9)。L は $\mathbb{Q}$ 上 $\sqrt{d}$ で生成されるので、σ は $\sqrt{d}$ での値で定まる (命題2.1.5)。σ はちょうど 2 通りあるので、両方の可能性が起きなければならない。そこで σ を $\sigma(\sqrt{d}) = -\sqrt{d}$ なるものとすれば、$\mathrm{Hom}_{\mathbb{Q}}^{\mathrm{al}}(L, \overline{\mathbb{Q}}) = \{\mathrm{id}_L, \sigma\}$ と決まる。

2.5 正規拡大

定義 2.5.1 (正規拡大)**.** L/K を代数拡大とする。すべての $\alpha \in L$ に対し α の K 上の最小多項式が L 上で 1 次式の積になるとき、L/K を**正規拡大 (normal extension)** という。

次の定理により、正規拡大かどうかはホムセットをみることで判定できる。

定理 2.5.2 (正規拡大とホムセット)**.** L/K を体の有限次拡大とする。このとき、次は同値である：

(1) L/K は正規拡大である。

(2) $\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ の元は L の元を固定する。

証明. cf. [雪江] p.185 □

正規拡大のうちとくに重要なのは、ホムセットが自己同型となる場合である。

命題 2.5.3 (ホムセットが自己同型群となる場合). L/K を正規代数拡大とする。このとき $\mathrm{Hom}_K^{\mathrm{al}}(L, L) = \mathrm{Aut}_K^{\mathrm{al}} L$ である。

証明. cf. [雪江] p.185 □

例 2.5.4 (正規拡大の例). $d \neq 1$ を square-free な整数とする (e.g. $d = 6$)。例 2.4.9 より各 $\phi \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ は $\phi(\mathbb{Q}(\sqrt{d})) \subset \mathbb{Q}(\sqrt{d})$ をみたすから、定理 2.5.2 より $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ は正規拡大である。

定義 2.5.5 (最小分解体). K を体とし、$f(x) \in K[x]$ とする。$f(x)$ を

$$f(x) = a_0(x - \alpha_1)\dots(x - \alpha_n) \quad (a_0 \in K^\times,\ \alpha_i \in \overline{K}) \tag{1}$$

と表すとき、$K(\alpha_1, \dots, \alpha_n)$ を f の K 上の**最小分解体 (splitting field)** という。

例 2.5.6 (最小分解体の例). [TODO] cf. [雪江] p.186

2.6 Galois 拡大

[TODO] キーワード: Galois の基本定理、円分体、有限体、Kummer 理論、Artin-Schreier 理論、可解性、作図

分離性と正規性を兼ね備えた拡大が Galois 拡大である。

定義 2.6.1 (Galois 拡大). L/K を代数拡大とする。

- L/K が分離拡大かつ正規拡大なら **Galois 拡大 (Galois extension)** という。

L/K をさらにガロア拡大とする。

- $\mathrm{Aut}_K^{\mathrm{al}} L$ を $\mathrm{Gal}(L/K)$ と書き、L の K 上の **Galois 群 (Galois group)** という。
- $\mathrm{Gal}(L/K)$ がアーベル群なら、L/K を**アーベル拡大 (abelian extension)** という。

- $\mathrm{Gal}(L/K)$ が巡回群なら、L/K を**巡回拡大 (cyclic extension)** という。

定義 2.6.2 (多項式の Galois 群). K を体、$f(x) \in K[x]$ とし、L を $f(x)$ の K 上の最小分解体とする。$\mathrm{Gal}(L/K)$ を $f(x)$ の K 上の **Galois 群 (Galois group)** という。

次の例より、Galois 群の元は複素共役の一般化とみなせることがわかる。

例 2.6.3 (Galois 拡大の例 1). 体の拡大 $\mathbb{C}/\mathbb{R}$ は命題 2.4.5 と定理 2.5.2 により分離拡大かつ正規拡大だから、Galois 拡大である。例 2.4.9 と同様の議論により $|\mathrm{Hom}^{\mathrm{al}}_{\mathbb{R}}(\mathbb{C},\mathbb{C})| = 2$ であるから、命題 2.5.3 より $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = |\mathrm{Aut}^{\mathrm{al}}_{\mathbb{R}}(\mathbb{C})| = 2$ である。したがって $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ である。

例 2.6.4 (Galois 拡大の例 2). $d \neq 1$ は square-free な整数とする（e.g. $d = 6$）。例 2.4.9 と例 2.5.4 により、代数拡大 $\mathbb{Q}(\sqrt{d})$ は分離拡大かつ正規拡大だから、Galois 拡大である。命題 2.5.3 より $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ が従う。

定理 2.6.5 (Galois 群は対称群の部分群). K を体とし、$f(x) \in K[x]$ を $\deg f(x) = n$ なる分離多項式とする。このとき、$f(x)$ の K 上の Galois 群は対称群 S_n の部分群と同型である。

証明. $f(x)$ の相異なる n 個の根を $\alpha_1, \ldots, \alpha_n \in \overline{K}$ とおくと、$f(x)$ の K 上の Galois 群は $L := K(\alpha_1, \ldots, \alpha_n)$ と表せる。$\sigma \in \mathrm{Gal}(L/K)$ は σ の $A := \{\alpha_1, \ldots, \alpha_n\}$ 上での値で決まるから、

$$\mathrm{Gal}(L/K) \longrightarrow S_n, \quad \sigma \mapsto \sigma|_A \tag{1}$$

は単射準同型である。 □

2.7 不変体と Artin の定理

定義 2.7.1 (不変体). L を体、G を有限群とし、G は L に忠実に作用しているとする。このとき、

$$L^G := \{\alpha \in L \colon g \cdot \alpha = \alpha \ (\forall g \in G)\} \tag{1}$$

を G の**不変体 (fixed field)** という。

命題 2.7.2 (Artin の定理). 定義 2.7.1 の設定のもとで、L/L^G は Galois 拡大であり、$\mathrm{Gal}(L/L^G) \cong G$ が成り立つ。

2.8 Galois 理論の基本定理

命題 2.8.1 (中間体の束). L/K を体の拡大とする。$\mathrm{Lat}(L/K)$ を L/K の中間体全体の集合とし、$\mathrm{Lat}(L/K)$ 上に半順序 $\leq$ を

$$B \leq C \quad \Leftrightarrow \quad B \subset C \tag{1}$$

で定めると、$(\mathrm{Lat}(L/K), \leq)$ は共通部分を交わり、合成体を結びとして束となる。

証明. 省略 □

次の補題は Galois 拡大の分離性と正規性を利用するもので、Galois 理論の基本定理の証明に重要な役割を果たす。

補題 2.8.2 (中間体と Galois 拡大). L/K を有限次 Galois 拡大とし、$M \in \mathrm{Lat}(L/K)$ とする。このとき、L/M は Galois 拡大である。

証明. [TODO] □

定理 2.8.3 (Galois 理論の基本定理). L/K を有限次 Galois 拡大とし、Galois 群を $G = \mathrm{Gal}(L/K)$ とする。

(1) 写像 $\gamma\colon \mathrm{Sub}(G) \to \mathrm{Lat}(L/K)$,

$$H \mapsto L^H \tag{2}$$

は order-reversing な全単射であり、逆写像は

$$\mathrm{Gal}(L/M) \leftarrow\!\shortmid M \tag{3}$$

で与えられる。

(2) $M \in \mathrm{Lat}(L/K)$ に関し

$$M/K \text{ が Galois 拡大} \iff \mathrm{Gal}(L/M) \text{ が } G \text{ の正規部分群} \tag{4}$$

が成り立つ。

証明. 不変体の定義から order-reversing であることは明らか。[TODO] □

2.9 Hilbert の定理 90

証明. cf. [? , p.197] □

定理 2.9.1 (Galois 拡大の推進定理)**.** [TODO] cf. [? , p.219]

定義 2.9.2 (Galois コホモロジー)**.** [TODO]

定理 2.9.3 (Hilbert の定理 90)**.** [TODO]