11. 体の標数・有限体

11–1. **体の標数.** 体 K に対し、

- $\exists!\iota : \boldsymbol{Z} \to K$: 環準同型 $(\iota(1) = 1_K)$
- $\mathrm{Ker}\iota$: $\boldsymbol{Z}$ の素 ideal で、$\mathrm{Ker}\iota = (p)$ (p: 素数または 0)
  この p を体 K の**標数 (characteristic)** といい、$\mathrm{ch}(K)$ と書く。
- $\mathrm{ch}(K) = 0$ ならば K は $\boldsymbol{Q}$ と同型な体を一意に含む。
- $\mathrm{ch}(K) = p > 0$ ならば K は $\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$ と同型な体を一意に含む。
- この $\boldsymbol{Q}, \boldsymbol{F}_p$ (と同型な体) を**素体 (prime field)** という。

11–2. **Frobenius 写像.** K : 標数 $p(> 0)$ の体に対し、

- $\varphi : K \to K; a \mapsto a^p$: 体の (一般には中への) 同型
  (即ち $(a+b)^p = a^p + b^p, (ab)^p = a^p b^p$) これを K の **Frobenius 写像** という。
- 特に $\#K < \infty$ の時は全単射 $(\varphi \in \mathrm{Aut}(K))$。

11–3. **有限体.** 元の数が有限な体を**有限体 (finite field)** という。

- 素数 p と正整数 $r \geq 1$ とに対し、元数 $q := p^r$ の体が存在し、同型を除き一意的。
  ($\boldsymbol{F}_q$ と書く。)
- 体の乗法群の有限部分群は巡回群。特に、$\boldsymbol{F}_q^\times$ は位数 $q-1$ の巡回群。

12. 重根・分離拡大

12–1. **重根・分離的多項式.** $f(X) \in K[X]$ に対し、

- f が $a \in \overline{K}$ を**重根 (multiple root)** に持つ $\overset{\leftarrow}{\iff} (X-a)^2 | f(X) \Leftrightarrow f(a) = f'(a) = 0$
- f : **分離的 (separable)** $\overset{\leftarrow}{\iff}$ f が重根を持たない
- $\mathrm{ch}(K) = p > 0$ の時、$\exists! r \geq 0, g(X) \in K[X] : f(X) = g(X^{p^r})$, かつ $g(X)$: 分離的
- 既約多項式 $f(X) \in K[X]$ が重根を持つ
  $\Leftrightarrow (\mathrm{ch}(K) = p > 0$ かつ $\exists g(X) \in K[X] : f(X) = g(X^p))$
- 特に $\mathrm{ch}(K) = 0$ の時は、既約多項式は重根を持たない。

12–2. **分離元.** 体 K に対し、

- $x \in \overline{K}$ が K **上分離的 (separable over K)**
  $\overset{\leftarrow}{\iff} K$ 上の最小多項式 $\mathrm{Irr}(x, K)(X) \in K[X]$ が分離的 (重根を持たない)
  $\iff \#\mathrm{Emb}_K(K(x), \overline{K}) = [K(x) : K]$

12–3. **分離拡大.** 代数拡大 L/K に対し、

- L/K: **分離拡大 (separable extention)** $\overset{\leftarrow}{\iff} \forall x \in L$ が K 上分離的
- $L = K(x)$: 単拡大の時、L/K : 分離的 $\Leftrightarrow x$: K 上分離的
- 有限次 (代数) 拡大 L/K に対し、L/K : 分離的 $\Leftrightarrow \#\mathrm{Emb}_K(L, \overline{K}) = [L : K]$
- **定理**: 有限次分離拡大は単拡大。
- 標数 0 なら、全ての代数拡大は分離的。従って、全ての有限次拡大は単拡大。
- 標数 p でも、有限体の代数拡大は分離的。

12–4. **分離閉包.** 代数拡大 L/K に対し、K 上分離的な L の元全体は体を成す。(K の L 内での**分離閉包 (separable closure)** という。)

- $L/M/K$ に於いて、L/K : 分離的 $\Leftrightarrow L/M, M/K$: 共に分離的
- $L_1, L_2/K$: 分離拡大に対し、$L_1L_2, L_1 \cap L_2$: 再び分離的
- 特に K の代数閉包 $\overline{K}$ 内での分離閉包を、単に K の **分離閉包**という。

12–5. **純非分離拡大.** 代数拡大 L/K に対し、

- L/K: **純非分離的 (purely inseparable)** $\overset{\leftarrow}{\iff} K$ の L 内での分離閉包が K と一致
  $\Leftrightarrow \mathrm{Emb}_K(L, \overline{K}) = \{\mathrm{id}_L\} \Leftrightarrow L$ は K の元の p 冪乗根で生成