

- 有限次拡大 (応用として, 角の 3 等分の不可能性).
- 有限体 (応用として, フィボナッチ数列の周期).

記法: 体とは可換環 $R = (R, +, \cdot, 0, 1)$ であって, 以下を満たすものであった:

$$0_R \neq 1_R \text{ かつ } \forall a \in R, a \neq 0_R \Rightarrow \exists b \in R, ab = 1_R = ba.$$

体の準同型とは (可換) 環の準同型写像のことである.

命題: 体 \mathbb{F}, \mathbb{F}' の間の準同型 $\varphi: \mathbb{F} \rightarrow \mathbb{F}'$ は単射.

証明: $\text{Ker } \varphi =: I$ は \mathbb{F} のイデアルなので, $I = \{0\}, \mathbb{F}$. $0 \neq 1$ から $I \neq \mathbb{F}$ でなければならない.

注意: 以上より, 体では商を考えない. しばしば $\mathbb{F} \subseteq \mathbb{F}'$ (部分体 = 部分環で体になっている) を考え, φ は省略する.

記法: 体 $\mathbb{F} \subseteq \mathbb{F}'$ と部分集合 $S \subseteq \mathbb{F}'$ について, \mathbb{F} と S を含む \mathbb{F}' の最小の部分体を $F(S)$ と書く. $S = \{s_1, s_2, \dots\}$ のとき, $F(S) = \mathbb{F}(s_1, s_2, \dots)$ のように書くこともある.

例: $\mathbb{Q} \subseteq \mathbb{C} \ni \sqrt{2}$ で, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ であることは簡単に分かる. 同様に $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ も分かる.

記法: 拡大 $\tau: \mathbb{F} \rightarrow \mathbb{F}'$ について, \mathbb{F}' は $f \cdot f' := \tau(f)f'$ によって \mathbb{F} 線形空間の構造を持つ (ここで $f \in \mathbb{F}, f' \in \mathbb{F}'$). \mathbb{F}' が \mathbb{F} 有限生成のとき, この拡大を有限次拡大といい, $\dim_{\mathbb{F}} \mathbb{F}' = [\mathbb{F}': \mathbb{F}]_{\tau}$ を (拡大) 次数という. 以下, 拡大は主に τ が包含写像の場合を扱う.

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

命題: 体の拡大 $\mathbb{F} \subseteq \mathbb{F}' \subseteq \mathbb{F}''$ において

- (1) $\mathbb{F} \subseteq \mathbb{F}''$ が有限次拡大 $\Leftrightarrow \mathbb{F} \subseteq \mathbb{F}'$ と $\mathbb{F}' \subseteq \mathbb{F}''$ が有限次拡大.
- (2) (1) のとき $[\mathbb{F}'': \mathbb{F}] = [\mathbb{F}'': \mathbb{F}'][\mathbb{F}': \mathbb{F}]$.

証明: (1) の (\Rightarrow): 明らか

(1) の (\Leftarrow) (と (2)): \mathbb{F}' の \mathbb{F} 基底を v_1, \dots, v_m とし, \mathbb{F}'' の \mathbb{F}' 基底を w_1, \dots, w_n とすると, $\{v_i w_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ が \mathbb{F}'' の \mathbb{F} 基底であることが分かる.

応用: コンパスと定規による作図について, 以下を示す.

- (1) 一般に角の 3 等分は不可能.
- (2) 立方体の体積の 2 倍の立方体は作図不可能.

証明: まず, コンパスと定規による作図の意味をはっきりさせておく.

- 最初に $(0, 0)$ と $(1, 0)$ が与えられている.
- 円を描くときの中心と半径, 直線を書くときの 2 点はすでにあるものを使う.

- 新たな点は、直線または円の交点とする.
- 有限回のステップで終わる.

作図 n ステップ目で得られている座標の数の集合を S_n とし (例えば $S_0 = \{0, 1\}$ である), $K_n = \mathbb{Q}(S_n) (\subseteq \mathbb{R})$ とする. 以下は各自考えよ.

■ 主張: $[K_n : K_{n-1}] = 1, 2$

(2) を示す. $\sqrt[3]{2} \in K_n$ となったとすると, $\mathbb{Q}(\sqrt[3]{2}) \subseteq K_n$. 一方で $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ なので $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. 連鎖律より $\dim_{\mathbb{Q}} K_n$ は 2 のべきかつ 3 の倍数となって, 矛盾が生じた.

(1) を示すのも同様に, $\cos 30^\circ$ は作図可能だが, $\cos 10^\circ$ が作図不可能であることが ($[\mathbb{Q}(\cos 10^\circ) : \mathbb{Q}] = 3$ より) 分かる.

定義: 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ について

- (1) $\theta \in \mathbb{F}'$ が \mathbb{F} 代数的 $\Leftrightarrow \exists f \in \mathbb{F}[x], f(\theta) = 0$.
- (2) 拡大が代数拡大 $\Leftrightarrow \forall \theta \in \mathbb{F}'$ は \mathbb{F} 代数的.

例: $\mathbb{Q} \subseteq \mathbb{R}$ や $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ は代数拡大ではないが, $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ は有限次拡大でない代数拡大で, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ は有限次拡大で代数拡大. ここで $\overline{\mathbb{Q}}$ は代数的数のなす (非自明だが) 体である.

命題: 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ が有限次拡大ならば代数拡大.

証明: $n = [\mathbb{F}' : \mathbb{F}]$ とする. $\theta \in \mathbb{F}'$ について, $\theta^0, \dots, \theta^n$ は \mathbb{F} 線形関係式をもつ.

記法: 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ と $\theta \in \mathbb{F}'$ について,

$$I := \{f(x) \in \mathbb{F}[x] \mid f(\theta) = 0\}$$

は $\mathbb{F}[x]$ のイデアルである. 「 θ が \mathbb{F} 代数的 $\Leftrightarrow \{0\} \subsetneq I$ 」だが, このとき I の生成元で最高次の係数が 1 のものを θ の \mathbb{F} 最小多項式といって, この講義では $\text{Irr}(\mathbb{F}; \theta)$ と書く.

命題: 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ において, $\theta \in \mathbb{F}'$ は \mathbb{F} 代数的で $f(x) = \text{Irr}(\mathbb{F}; \theta)$ とすると, $f(x)$ は既約で

$$\mathbb{F}(\theta) = \mathbb{F}[\theta] \xrightarrow{\sim} \mathbb{F}[x]/(f(x)).$$

証明: 写像 $\mathbb{F}[x] \rightarrow \mathbb{F}(\theta), f(x) \mapsto f(\theta)$ は環準同型なので, $\mathbb{F}[x]/(f(x)) \hookrightarrow \mathbb{F}(\theta)$. よって $\mathbb{F}[x]/(f(x))$ は整域なので, $0 \neq f(x)$ は既約で, $\mathbb{F}[x]/(f(x))$ は体でもある. つまり $\mathbb{F}[x] \twoheadrightarrow \mathbb{F}[\theta] \subseteq \mathbb{F}(\theta)$ が $\mathbb{F}[x]/(f(x)) \xrightarrow{\sim} \mathbb{F}[\theta] \subseteq \mathbb{F}(\theta)$ を誘導し, $\mathbb{F}[\theta]$ が体なので $\mathbb{F}[\theta] = \mathbb{F}(\theta)$.

系: 命題の設定で, $\mathbb{F}(\theta)$ は \mathbb{F} の有限次拡大で, $[\mathbb{F}(\theta) : \mathbb{F}] = \deg \text{Irr}(\mathbb{F}; \theta)$.

系: 体の拡大 $\mathbb{F} \subseteq \mathbb{F}' \subseteq \mathbb{F}''$ において, $\mathbb{F} \subseteq \mathbb{F}''$ が代数拡大 $\Leftrightarrow \mathbb{F} \subseteq \mathbb{F}'$ と $\mathbb{F}' \subseteq \mathbb{F}''$ が代数拡大.

証明: (\Rightarrow): 明らか.

(\Leftarrow): $\theta \in \mathbb{F}'$ は \mathbb{F}' 代数的なので, $\text{Irr}(\mathbb{F}'; \theta) = x^m + a_1 x^{m-1} + \cdots + a_m \in \mathbb{F}'[x]$ を取ると,

$$\mathbb{K} = \mathbb{F}(a_1, \dots, a_m) = \mathbb{F}(a_1, \dots, a_{m-1})(a_m) = \cdots$$

は \mathbb{F} の有限次拡大. また $[\mathbb{K}(\theta) : \mathbb{K}] = m$ でもあるので, $\mathbb{K}(\theta)$ は \mathbb{F} の有限次拡大. よって θ は \mathbb{F} 代数的.

注意: 代数拡大 $\mathbb{F} \subseteq \mathbb{F}'$ が分離的とは, 任意の $\theta \in \mathbb{F}'$ について, $\text{Irr}(\mathbb{F}; \theta)$ が「重根を持たない」ことである. しかし重根についてきちんと論じるのは, 一般の設定では意外と面倒なため, この講義では主に「 $\overline{\mathbb{Q}}$ の部分体の中の拡大」または「有限体の中の拡大」を考えることにする (このとき自動的に拡大は分離的になる).

記法: 体 \mathbb{F} は可換環なので, ただ 1 つの環準同型 $\mathbb{Z} \rightarrow \mathbb{F}$ が存在する. よって $\mathbb{Z}/\text{Ker} \hookrightarrow \mathbb{F}$ で, 左辺は整域でなければならないので $\text{Ker} = (0)$ または $\text{Ker} = (p)$ (ここで p は素数). それぞれに応じて, \mathbb{F} は標数 0 または p と言って, $\text{char } \mathbb{F} = 0$ または $\text{char } \mathbb{F} = p$ のように書く.

例: $\text{char } \mathbb{R} = 0$ で, 素数 p について $\text{char } \mathbb{Z}/p\mathbb{Z} = p$.

記法: $\text{char } \mathbb{Z}/p\mathbb{Z}$ を (体であることを強調する際には) \mathbb{F}_p と書く.

命題: 有限体 \mathbb{F} の $\text{char } \mathbb{F}$ は素数で (p とする), $|\mathbb{F}|$ は p のべき.

証明: \mathbb{F} は標数に応じて \mathbb{Q} または \mathbb{F}_p (と同型な部分体) を含む. \mathbb{F} はこれらの素体上の線形空間の構造を持つ.

注意: 商体 (可換環のイデアルによる商環とは異なる概念) について述べる. R が整域ならば,

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

は $R \times (R \setminus \{0\})$ 上の同値関係となる. (a, b) の同値類を $\frac{a}{b}$ と書くことにすると, $\text{Frac}(R) := (R \times (R \setminus \{0\})) / \sim$ には

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}$$

で 2 項演算が定義でき, $\left(\text{Frac}(R), +, \cdot, \frac{0}{1}, \frac{1}{1} \right)$ は体になることが確認できる.

例: $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$, $\text{Frac}(\mathbb{Z}[x]) = \text{Frac}(\mathbb{Q}[x]) = \mathbb{Q}(x)$ (1 変数有理関数体)

注意: 構成法 Frac より, 整域は体の部分環と同じ概念であることが分かる. 実際

$$\iota : R \hookrightarrow \text{Frac}(R), r \mapsto \frac{r}{1}$$

は単射環準同型である.

注意: $\text{Frac}(R)$ は以下の普遍性を持つことが確認できる.

任意の可換環 S と任意の環準同型 $f : R \rightarrow S$ について

$$\forall r \in R \setminus \{0\}, f(r) \in S^\times$$

ならば, $\bar{f} \circ \iota = f$ となる環準同型 $\bar{f} : \text{Frac}(R) \rightarrow S$ がただ 1 つ存在する. ここで $\iota : R \hookrightarrow \text{Frac}(R)$ は, 前の注意にある単射環準同型である.

注意: 以上より, $\mathbb{Z} \hookrightarrow \mathbb{Q} \xrightarrow{f,g} R$ は, 任意の可換環 R と環準同型 $\mathbb{Q} \xrightarrow{f,g} R$ について, $f \circ \iota = g \circ \iota \Rightarrow f = g$ を導く. これは $\mathbb{Z} \xrightarrow{\iota} \mathbb{Q}$ が環の圏で「全射のようなもの」(エピ射という) だと言っている.

注意: $\text{Frac}(R)$ は, 「 R が UFD ならば $R[x]$ も UFD」の証明にも使われる ($K := \text{Frac}(R)$ について, $K[x]$ は PID なので UFD であることを用いる).

命題: 任意の素数 $p \geq 2$ と素数 $n \geq 1$ について, 位数 p^n の体が存在する.

証明: $\mathbb{F}_p[x]$ の n 次既約モニック多項式の個数を a_n とし, $a_n > 0$ を言えばよい. これは

$$a_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d \quad (1)$$

から従う. ここで

$$\mu(d) = \begin{cases} 0 & d \text{ が平方因子を持つ} \\ (-1)^r & d = p_1 \cdots p_r \text{ (各 } p_i \text{ は相異なる素数)} \end{cases}$$

事実 (メビウス反転公式): $(x_d)_{d \geq 1}$ について, $\sum_{d|n} x_d = y_n$ なら $x_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) y_d$.

(1) の証明: 形式的べき級数環 $\mathbb{C}[[u]]$ において

$$\prod_{d \geq 1} \left(\frac{1}{1 - u^d} \right)^{a_d} = \sum_{k \geq 0} p^k u^k = \frac{1}{1 - pu}$$

が成立する (左の等号に $\mathbb{F}_p[x]$ が UFD であることを用いた). よって

$$-\sum_{d \geq 1} a_d \log(1 - u^d) = -\log(1 - pu).$$

$-\log(1 - u) = u + \frac{u^2}{2} + \frac{u^3}{3} + \cdots$ より u^n の係数を比較すると, $\sum_{d|n} da_d = p^n$.

注意: 普通, 任意の体 \mathbb{F} について, それを含む代数閉包 $\bar{\mathbb{F}}$ の存在 (シュタイニッツの定理) を示し, $\mathbb{F}_{p^m} = \{u \in \bar{\mathbb{F}}_p \mid u^{p^m} = u\}$ を示す. しかしこの講義では $\bar{\mathbb{F}}$ の構成 (選択公理を用いる) やその「一意性」を示さないため, 初等的な有限体の存在証明を行った. $\bar{\mathbb{F}}$ に触れないことは, 重根の議論を避けたこととも関係している (参考: 分離拡大).

命題: p が素数で $n \geq 1$ とする. 体 \mathbb{F}, \mathbb{F}' が $|\mathbb{F}| = |\mathbb{F}'| = p^n$ ならば $\mathbb{F} \cong \mathbb{F}'$.

証明: $\mathbb{F}^\times \cong C_{p^n-1}$ だったことを思い出す (有限アーベル群の構造定理を仮定して証明した). よって $\forall x \in \mathbb{F}^\times, x^{p^n-1} = 1$ なので $\forall x \in \mathbb{F}^\times, x^{p^n} = x$. \mathbb{F}^\times の原始根 x_0 を選び, $f(x) = \text{Irr}(\mathbb{F}_p; x_0)$ と

する. $f(x)|x^{p^n} - x$ である. $\mathbb{F} = \mathbb{F}_p[x_0] \cong \mathbb{F}_p[x]/(f(x))$ で, $\forall y \in \mathbb{F}', y^{p^n} - y = 0$ でもあるので, $\exists y_0 \in \mathbb{F}', f(y_0) = 0$. $\mathbb{F}' \supseteq \mathbb{F}_p[y_0] \cong \mathbb{F}_p[x]/(f(x))$ なので, $\mathbb{F}' = \mathbb{F}_p[y_0] \cong \mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}$.

記法: 位数 p^n の有限体を \mathbb{F}_{p^n} とか $\text{GF}(p, n)$ のように書く. これは同型を除いて一意のだが, 上の命題で自然な同型を選ぶことはできない (と思う).

応用 (フィボナッチ数列の周期): $a_0 = 0, a_1 = 1, a_{n+2} = a_n + a_{n+1}$ ($n \geq 2$) で定まる数列 $(a_n)_{n \geq 0}$ を (この講義では) フィボナッチ数列という. 一般項の公式

$$a_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right)$$

は, 素数 $p \neq 2, 5$ について \mathbb{F}_p または \mathbb{F}_{p^2} で意味を持つ.

事実: 素数 $p \neq 2, 5$ について, $x^2 - 5$ が $\mathbb{F}_p[x]$ で既約 $\Leftrightarrow p \equiv \pm 2 \pmod{5}$.

証明: 平方剰余の相互法則

$$\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

から従う. ここで $p \neq q$ は奇素数で,

$$\left(\frac{p}{q} \right) = \begin{cases} 1 & \exists x \in \mathbb{F}_q, x^2 = p \\ -1 & \text{それ以外} \end{cases}.$$

系: 素数 p について

- (1) $p \equiv \pm 1 \pmod{5}$ ならば $\forall n \geq 0, a_{n+p-1} = a_n$.
- (2) $p \equiv \pm 2 \pmod{5}$ ならば $\forall n \geq 0, a_{n+p^2-1} = a_n$.

補題: 体 \mathbb{F} の標数が素数 p のとき, $\sigma_{\mathbb{F}} : \mathbb{F} \rightarrow \mathbb{F}, x \mapsto x^p$ は準同型 (フロベニウス射).

証明: $\sigma_{\mathbb{F}}(a+b) = \sigma_{\mathbb{F}}(a) + \sigma_{\mathbb{F}}(b)$ のみ非自明で, これは $0 < \forall i < p, \binom{p}{i} \in p\mathbb{Z}$ から従う.

定義: 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ について,

$$\text{Gal}(\mathbb{F}'/\mathbb{F}) := \{f : \mathbb{F}' \xrightarrow{\sim} \mathbb{F}' \mid f|_{\mathbb{F}} = \text{id}_{\mathbb{F}}\}$$

は群 (ここで $/$ は慣習的に使われるもので, 商とは関係がない).

定理: 素数 $p \geq 2$ と $n \geq 1$ について, $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong C_n, \sigma_{\mathbb{F}_{p^n}}^x \mapsto x$ (群同型).

証明: $\sigma_{\mathbb{F}_{p^n}}$ は単射なので全単射 (つまり $\sigma_{\mathbb{F}_{p^n}} \in \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$). また $\mathbb{F}_{p^n}^\times \cong C_{p^n-1}$ だったから, $\sigma_{\mathbb{F}_{p^n}}$ の位数は n である. よって $|\text{Gal}| \geq n$. さらに $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$ とすると, $\tau \in \text{Gal}$ について $f(\tau(\theta)) = 0$ かつ $\tau \neq \tau'$ ならば $\tau(\theta) \neq \tau'(\theta)$ なので $|\text{Gal}| \leq n$.

記法: 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ と部分群 $G \subseteq \text{Gal}(\mathbb{F}'/\mathbb{F})$ について

$$\mathbb{F}'^G := \{x \in \mathbb{F}' \mid \forall \tau \in G, \tau(x) = x\}$$

は \mathbb{F} の拡大体 (で \mathbb{F}' の部分体).

定義: 有限次拡大 $\mathbb{F} \subseteq \mathbb{F}'$ がガロア拡大 $\Leftrightarrow \mathbb{F}'^{\text{Gal}(\mathbb{F}'/\mathbb{F})} = \mathbb{F}$.

系: 素数 $p \geq 2$ と $n \geq 1$ について, 拡大 $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ はガロア拡大.

注意: ガロア理論の基本定理とは, ガロア拡大 $\mathbb{F} \subseteq \mathbb{F}'$ について, 中間体 $\mathbb{F} \subseteq M \subseteq \mathbb{F}'$ と $\text{Gal}(\mathbb{F}'/\mathbb{F})$ の部分群とを 1 対 1 対応つけるものである.

応用(フィボナッチ数列の周期の精密化): 素数 $p \equiv \pm 2 \pmod{5}$ について, $\forall n \geq 0, a_{n+2(p+1)} = a_n$.

証明: このとき $\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/(x^2 - x - 1)$ で $\sigma_{\mathbb{F}_{p^2}}$ は $x^2 - x - 1 = 0$ の解を入れかえる. つまり解を $\alpha, \beta \in \mathbb{F}_{p^2}$ とすると, $\alpha^p = \beta, \beta^p = \alpha$ なので $\alpha^{p+1} = \beta^{p+1} = -1$.

注意: フィボナッチ数列の $\text{mod } n$ での周期は pisano period と呼ばれ, 様々な研究がある.