

補足と演習問題 (12/18 配布)

問 1. (可換環論の復習) 可換環 R の積閉集合 S に関する分数化 $S^{-1}R$ の構成を考えよう。

- (1) S を積閉集合 ($a, b \in S \implies ab \in S$) で、 $1 \in S$ かつ $0 \notin S$ とする。このとき、 $R \times S$ 上に次で定める関係は同値関係である：

$$(a_1, b_1) \sim (a_2, b_2) \iff \exists u \in S : u(a_1b_2 - a_2b_1) = 0.$$

以下、 (a, b) の同値類を a/b と書く。

- (2) $S^{-1}R := (R \times S)/\sim$ 上に次で加法・乗法を定めると、可換環を成す：

$$a_1/b_1 + a_2/b_2 := (a_1b_2 + a_2b_1)/(b_1b_2), \quad a_1/b_1 \cdot a_2/b_2 := (a_1a_2)/(b_1b_2).$$

- (3) $\iota : R \longrightarrow S^{-1}R; a \longmapsto a/1$ は環準同型。 S が零因子を含まないならば、 ι : 単射。
 (4) 組 $(S^{-1}R, \iota)$ は次の普遍性で特徴付けられる：可換環 T と環準同型 $f : R \longrightarrow T$ との組 (T, f) が $f(S) \in T^\times$ を満たすならば、環準同型 $\tilde{f} : S^{-1}R \longrightarrow T$ で $f \circ \iota = \tilde{f}$ となるものが一意に存在する。
 (5) R が整域で $S = R \setminus \{0\}$ のとき、 $S^{-1}R$ は体。 $(R$ の商体 (quotient field) という。)

問 2. (可換環論の復習) 可換環 R の ideal \mathfrak{a} に関する剰余環 R/\mathfrak{a} の構成を考えよう。

- (1) R 上に次で定める関係は同値関係である：

$$a \sim b \iff a - b \in \mathfrak{a}.$$

(通常、 $a \equiv b \pmod{\mathfrak{a}}$ と書く。) 以下、 a の同値類を \bar{a} と書く。

- (2) $R/\mathfrak{a} := R/\sim$ 上に次で加法・乗法を定めると、可換環を成す：

$$\bar{a} + \bar{b} := \overline{a + b}, \quad \bar{a} \cdot \bar{b} := \overline{a \cdot b}.$$

- (3) $\pi : R \longrightarrow R/\mathfrak{a}; a \longmapsto \bar{a}$ は全射環準同型。

- (4) \mathfrak{p} : 素 ideal $\iff R/\mathfrak{p}$: 整域

- (5) \mathfrak{m} : 極大 ideal $\iff R/\mathfrak{m}$: 体

問 3. (可換環論の復習) 一般に整域 R に対して、

- (1) R : Euclid 整域 $\implies R$: 単項 ideal 整域 (PID) $\implies R$: 一意分解整域 (UFD)
 (2) R : UFD のとき、 $f \in R, f \neq 0$ に対し、 f : 既約元 $\iff f$: 素元 $\iff (f)$: 素 ideal
 (3) R : PID のとき、 \mathfrak{p} : 素 ideal で $\mathfrak{p} \neq \{0\}$ $\iff \mathfrak{p}$: 極大 ideal

問 4. 体 K 上の一変数多項式環 $R := K[X]$ において、

- (1) R は次数関数 $\deg : R \setminus \{0\} \longrightarrow \mathbb{N}$ に関して Euclid 整域である。
 (2) 従って前問より、 $f \in K[X] \setminus \{0\}$ に対して、 f : 既約 $\iff f$: 素元 $\iff (f)$: 素 ideal $\iff (f)$: 極大 ideal $\iff K[X]/(f)$: 体
 (3) 合成写像 $K \hookrightarrow K[X] \longrightarrow K[X]/(f)$ は単射環準同型。従って、 $K[X]/(f)$ は K を含む体 (K の拡大体) と看做せる。

問 5. 体の有限次拡大 $L \supset M \supset K$ に於ける拡大次数の連鎖律 $[L : K] = [L : M][M : K]$ を示せ。(具体的には、 (x_1, \dots, x_n) が L の M 上の基底、 (y_1, \dots, y_m) が M の K 上の基底であるとき、 $(x_i y_j)_{1 \leq i \leq n, 1 \leq j \leq m}$ が L の K 上の基底であることを示せばよい。)

問 6. K を体とし、その代数閉包 \bar{K} を 1 つ取って固定する。 $f(X) \in K[X]$ を K 上の既約多項式とし、その一つの根を $\alpha \in \bar{K}$ とする。

- (1) (準備) 体上有限次元な整域は体である。
 (2) K 上の環準同型 $\varphi : K[X] \rightarrow \bar{K}; X \mapsto \alpha$ について、 $\text{Im} \varphi = K(\alpha)$ である。
 (3) $\text{Ker} \varphi = (f)$ である。これより、 $K[X]/(f) \simeq K(\alpha)$ となる。
 (4) $\iota : K(\alpha) \hookrightarrow \bar{K}$ を K 上の埋込とする。 $\iota(\alpha)$ も f の根である。
 (5) 逆に f の根 $\beta \in \bar{K}$ に対し、 $\iota(\alpha) = \beta$ となる K 上の埋込 $\iota : K(\alpha) \hookrightarrow \bar{K}$ が一意に存在する。
 (6) 以上により、 $K(\alpha)$ の \bar{K} への K の埋込全体と、 f の根全体とは、一対一に対応する。

問 7. $f(X) \in K[X]$ を K 上の n 次 monic 多項式とし、その根を (重複度を込めて) w_1, \dots, w_n とする。根の差積の平方

$$D(f) := \prod_{1 \leq i < j \leq n} (w_i - w_j)^2$$

を f の判別式 (discriminant) という。

(1) $f(X) = X^3 + pX + q$ の 3 根を x_1, x_2, x_3 とする。 x_1, x_2, x_3 の基本対称式と p, q との関係を用いて、判別式 $D(f) = \prod_{1 \leq i < j \leq 3} (x_i - x_j)^2 = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$

を p, q で表せ。

(2) f の微分 f' の根を v_1, \dots, v_{n-1} (重根は重複度込みで考える) とするとき、

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n f'(w_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^{n-1} f(v_j).$$

(3) $f(X) = X^n - aX - b$ について判別式 $D(f)$ を求めよ。(ヒント: f, f' について互除法を用いて計算せよ。)

問 8. $f(X) = X^4 + pX^2 + qX + r$ の 4 根を x_i ($i = 1, \dots, 4$) とする。

(1) x_i の基本対称式と p, q, r との関係は?

(2) $x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3$ を 3 根とする 3 次多項式を求めよ (係数を p, q, r で表せ)。

(3) $(x_1 + x_2)(x_3 + x_4), (x_1 + x_3)(x_2 + x_4), (x_1 + x_4)(x_2 + x_3)$ を 3 根とする 3 次多項式を求めよ (係数を p, q, r で表せ)。

問 9. K を標数 $p > 0$ の体とするとき、 $a, b \in K$ に対し、 $(a+b)^p = a^p + b^p, (ab)^p = a^p b^p$ となることを示せ。(ヒント: 二項展開して、素数 p と $1 \leq k \leq p-1$ とに対し $p \mid \binom{p}{k}$

となることを用いる。) 即ち、 $\varphi: K \rightarrow K; a \mapsto a^p$: (中への) 体同型。特に、 K が有限体ならば、 φ は K の体自己同型。

問 10. 素数 p と自然数 r との組 (p, r) で $q := p^r \leq 10$ なるもの $(p, r) = (2, 2), (2, 3), (3, 2)$ (即ち $q = 4, 8, 9$) に対し、

(1) 素体 $F_p = \mathbb{Z}/p\mathbb{Z}$ 上 r 次の既約多項式 $f(X) \in F_p[X]$ を、とにかく見付けよ。

(2) $f(X)$ が F_p 上既約であることを、とにかく示せ。

(3) $K := F_p[X]/(f)$ により q 元体 K を構成し、その乗積表を書け。

(4) Frobenius 同型 $\varphi: K \rightarrow K; a \mapsto a^p$ の関数表 (a と $\varphi(a)$ との対応表) を作れ。

(5) $\varphi^n = \text{id}_K$ となる最小の正整数 n は何か。

問 11. 体 K の乗法群 K^\times の有限部分群 G は巡回群。(ヒント: 有限アーベル群の構造定理と、体では $x^n = 1$ となる x が高々 n 個であることを用いよ。) 特に、 $K = F_q$: 有限体に対し、 F_q^\times は巡回群。

問 12. 前問により、素数 p に対し、 $(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群である。その生成元を、法 p に関する原始根 (primitive root) という。幾つかの素数 p に対し、原始根をとにかく求めよ。

問 13. (Fermat の小定理) p を素数とすると、 $a \in \mathbb{Z}$ に対し $a^p \equiv a \pmod{p}$ となる。これを二通りで証明しよう。

(1) (乗法的) $a \not\equiv 0 \pmod{p}$ ならば $a^{p-1} \equiv 1 \pmod{p}$ であることを示すことにより証明せよ。

(2) (加法的) 二項係数の性質から $(a+b)^p \equiv a^p + b^p \pmod{p}$ を導き、 a に関する帰納法を用いて証明せよ。(Fermat による原証明はこちらだったと言われている。)

問 14. 次の体拡大 L/K が Galois 拡大でないことを簡潔に説明せよ。また、 L を含む拡大体 \tilde{L} で、 \tilde{L}/K が Galois 拡大となるようなものが存在するか。存在するならその最小なもの (L/K の Galois 閉包という) は何か。

(1) $L = \mathbb{Q}(\sqrt[3]{2}), K = \mathbb{Q}$

(2) $L = \mathbb{F}_p(T), K = \mathbb{F}_p(T^p)$ (ここに、 T は \mathbb{F}_p 上超越的)

問 15. Z 上の monic な多項式 $f(X) = \sum_{i=0}^n a_i X^i \in Z[X]$ ($a_n = 1$) に対し、

- (1) (Gauss の補題) f が Q 上可約ならば、 Z 上でも可約である。従って (対偶を取ると)、 f が Z 上既約ならば、 Q 上でも既約である。
- (2) 特に、 f が有理数の根 $x \in Q$ を持つならば、 $x \in Z$ かつ $x|a_0$ である。

問 16. 上問を用いて、次の多項式が Z 上 (従って Q 上) 既約であることを示せ。

- (1) $f(X) = X^3 + 2X - 1$
- (2) $f(X) = X^3 + X - 6$
- (3) $f(X) = X^4 - 10X^2 + 1$ (ヒント: まづ 1 次因子を持たないこと、次に 2 次式 2 つの積にならないことを確かめよ。)

問 17. 素数 p に対し、自然な射影 $Z \rightarrow Z/pZ = F_p$ から定まる環準同型 $Z[X] \rightarrow F_p[X]$ による $f(X) \in Z[X]$ の像を $\bar{f}(X) \in F_p[x]$ と書くことにする。 $f(X) \in Z[X]$ に対し、或る素数 p について $\bar{f}(X) \in F_p[x]$ が既約なら、 f は Z 上 (従って Q 上) 既約。

問 18. 次の多項式 $f(X) \in Z[X]$ の既約性を、幾つかの素数 p に対する $\text{mod } p$ での分解 ($\bar{f}(X) \in F_p[x]$ の分解) を考えることにより、判定せよ。

- (1) $f(X) = X^3 + 3X + 9$
- (2) $f(X) = X^3 + 2X + 8$
- (3) $f(X) = X^4 + 5X^2 + 2X + 15$

問 19. 第 8 円分多項式 $\Phi_8(X) \in Z[X]$ について、

- (1) $\Phi_8(X)$ を求め、その Z 上での既約性を直接判定せよ。
- (2) $\Phi_8(X)$ が $\text{mod } p$ で 1 次式の積に分解するような素数 p の条件を決定せよ。(ヒント: F_p^\times 内に 1 の原始 8 乗根が存在する条件は?)
- (3) 任意の素数 p に対し、 $\Phi_8(X)$ は $\text{mod } p$ で可約 (若干の初等整数論の知識が要る)。

問 20. K を体、 n を 1 以上の自然数とする。

- (1) K の代数閉包 \bar{K} 内に 1 の原始 n 乗根が存在するための必要十分条件は、「 $\text{ch } K = 0$ または ($p := \text{ch } K > 0$ かつ $p \nmid n$)」である。
- (2) 上の条件を満たすとき、 \bar{K} 内の 1 の原始 n 乗根の一つを ζ_n とする (一つ取って固定)。 $K(\zeta_n)$ は K 上 Galois 拡大。
- (3) $G := \text{Gal}(K(\zeta_n)/K)$ とする。 $\sigma \in G$ に対し、 $\sigma(\zeta_n) = \zeta_n^a$ となる a を取ることにより、 $G \hookrightarrow (Z/nZ)^\times$ が定まる。これは ζ_n の選び方に依らない。

問 21. p を奇素数、 ζ_p を 1 の原始 p 乗根の一つとし、 $K := Q(\zeta_p)$ とおく。

- (1) 第 p 円分多項式 $\Phi_p(X) \in Z[X]$ を求めよ。
- (2) $g(Y) := \Phi_p(Y+1) \in Z[X]$ とおくと、 g は Z 上 (従って Q 上) 既約。(ヒント: Eisenstein の既約性判定法が使える。)
- (3) Φ_p は Z 上 (従って Q 上) 既約。(従って、 $\Phi_p(X) = \text{Irr}(\zeta_p/Q)(X)$ である。)
- (4) $\prod_{\zeta \in \mu_p^*} (1 - \zeta) = p$ を示せ。また、判別式 $D(\Phi_p) = ?$
- (5) 前問の対応により $\text{Gal}(K/Q) \simeq (Z/pZ)^\times$ で、 $\text{Gal}(K/Q)$ は $(p-1)$ 次巡回群。

問 22. 前問の状況で、 $G := \text{Gal}(K/Q)$ とおき、 $\bar{a} = a \text{ mod } p \in (Z/pZ)^\times$ に対し、 $\sigma_a \in G$ を $\sigma_a(\zeta_p) = \zeta_p^{\bar{a}}$ で定める。

- (1) $(p-1)$ 次巡回群 $(Z/pZ)^\times$ の生成元 (法 p に関する原始根) を一つ取って $\bar{g} = g \text{ mod } p$ とする; $(Z/pZ)^\times = \langle \bar{g} \rangle$ 。 $(Z/pZ)^\times$ の指数 2 の部分群 H を \bar{g} で表せ。
($(p-1)/2-1$)
- (2) $\xi_i := \sum_{j=0}^{p-2} \zeta_p^{g^{2j+i}}$ ($i = 0, 1$) とする。 $\xi_i \in K^H$ を示し、 $\sigma_g(\xi_0), \sigma_g(\xi_1)$ を求めよ。
- (3) $\xi_0 + \xi_1, \xi_0 \xi_1 \in K^G = Q$ を示し、その値を求めよ。
- (4) $\xi_0 - \xi_1 = \sum_{i=0}^{p-2} (-1)^i \zeta_p^{g^i}$ は Gauss 和 (次問参照) である。 $(\xi_0 - \xi_1)^2 = ?$
- (5) Q の 2 次拡大 K^H を求めよ。

問 23. p を奇素数、 $\left(\frac{\cdot}{p}\right)$ を平方剰余記号 (Lagrange 記号)、 ζ_p を 1 の原始 p 乗根 (一つ取って固定) とする。 $G(p) := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a$ を Gauss 和 (Gaussian sum) とする。

$$(1) (k, p) = 1 \text{ のとき、 } \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) (\zeta_p^k)^a = \left(\frac{k}{p}\right) G(p)$$

$$(2) G(p)^2 = \left(\frac{-1}{p}\right) p (= : p^*)$$

$$(3) l : \text{ 奇素数に対し、平方剰余の相互律 } \left(\frac{l}{p}\right) = \left(\frac{p^*}{l}\right) \text{ を示せ。}$$

$$(4) \zeta_p = \exp\left(\frac{2\pi i}{p}\right) \in \mathbb{C} \text{ に取るとき、 } G(p) \text{ の符号 (偏角) を決定せよ。}$$

問 24. p を奇素数、 ζ_p を 1 の原始 p 乗根の一つとし、 $K := \mathbb{Q}(\zeta_p)$ とおく。 $p-1$ の各約数 d に対し、 K/\mathbb{Q} の d 次中間体が唯一つ存在する。その典型的な生成元を見付けよ。

問 25. m, n を互いに素な自然数とする。

(1) (中国剰余定理) 自然に $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (環同型)、また、これより $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ (群同型)。

(2) $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n)$ である。

(3) 上記 2 つを円分体の Galois 対応の下で結び付けよ。

(4) $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ である。

問 26. (例えば $n = 5, 7, 8, 9, 12, 15$ など) 幾つかの n に対し、 $(\mathbb{Z}/n\mathbb{Z})^\times$ の群構造を決定し、部分群を列挙すると共に、対応する $\mathbb{Q}(\zeta_n)$ の部分体とその適切な生成元の最小多項式を求めよ。

問 27. 次の値を求めよ。

$$(1) \cos 20^\circ \cos 40^\circ \cos 80^\circ$$

$$(2) \cos \frac{2\pi}{7} \cos \frac{4\pi}{7} \cos \frac{8\pi}{7}$$

(特に、“綺麗な” 値になる理由を Galois 理論から説明せよ。)

問 28. 次の \mathbb{Q} 上の多項式 $f \in \mathbb{Q}[X]$ について、 \mathbb{Q} 上の最小分解体 $K := \text{Spl}(f/\mathbb{Q})$ を求めよ。(簡単な生成元 (複数次可) を添加する形で表示せよ。) その \mathbb{Q} 上の拡大次数 $[K : \mathbb{Q}]$ は? また、 K/\mathbb{Q} 上の Galois 群 $G = \text{Gal}(K/\mathbb{Q})$ の群構造を決定した上で、 K/\mathbb{Q} の全ての部分体を、 G の部分群との Galois 対応を明らかにして求めよ。

$$(1) f(X) = X^3 - 2$$

$$(2) f(X) = X^5 - 2$$

$$(3) f(X) = X^3 - 3X + 1$$

$$(4) f(X) = X^4 - 10X^2 + 1$$

$$(5) f(X) = X^4 - 20X^2 + 32$$

$$(6) f(X) = X^4 - 10X^2 + 5$$

問 29. $f(X) \in \mathbb{Q}[X]$ を \mathbb{Q} 上の既約 monic 多項式、 α をその根の一つとして、根体 $K := \mathbb{Q}(\alpha)$ を考える。 K の元は或る $g(X) \in \mathbb{Q}[X]$ を用いて $g(\alpha)$ の形で表せるが、 $g(\alpha) \neq 0$ のとき、この逆元 $g(\alpha)^{-1} \in K$ を計算して具体的に表す方法を述べよ。(即ち、 $g(\alpha)^{-1} = h(\alpha)$ となる $h(X) \in \mathbb{Q}[X]$ を計算する具体的な方法を与えよ。)

問 30. $K = \mathbb{C}(t)$ を \mathbb{C} 上の一変数有理関数体 (t は \mathbb{C} 上超越的な元) とする。

(1) K の \mathbb{C} 上の自己同型 σ を $\sigma(t) := \zeta_n t$ で定めると、 σ は位数 n で、 $G := \langle \sigma \rangle$ は位数 n の巡回群。このとき K の G による固定体 K^G は?

(2) K の \mathbb{C} 上の自己同型 τ を $\sigma(t) := \frac{1}{t}$ で定めると、 τ は位数 2 で、 $H := \langle \tau \rangle$ は位数 2 の巡回群。このとき K の H による固定体 K^H は?