

イントロダクション(2次方程式の場合)

我々は 体の Galois 理論についてやる。何をやりたいのか？

2次方程式

$a, b, c \in \mathbb{Q}$ であるとし、 $a \neq 0$ と仮定する。

2次方程式 $ax^2 + bx + c = 0$ について考えよう。

よりシソプローレな方程式に帰着していく。

両辺を a でわると、 $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$.

$p = \frac{b}{a}$, $q = \frac{c}{a}$ とおくと、 $x^2 + px + q = 0$

$x = X - \frac{p}{2}$ とおくと、 $X^2 - px + \frac{p^2}{4} + px - \frac{p^2}{2} + q = 0$,

$$X^2 - \frac{p^2}{4} + q = 0, \quad X^2 = \frac{p^2}{4} - q$$

$$X = \pm \sqrt{\frac{p^2}{4} - q}.$$

2次方程式は
 $X^2 = A$ 型の
2次方程式に
帰着される。
平方根で
2次方程式
は解ける。

重要なポイント 0でない数の平方根のとり方は2通りある。

たとえば、2の平方根のとり方は $\pm\sqrt{2}$ の2つある。

-1の平方根のとり方は $\pm i$ の2つある。 $(i=\sqrt{-1})$

どちらをえらんでもよい。 ← ありまいるべき方 ← どういう意味か？

どういう意味か (あわざってはな説明) ← 加減乗除 ← 体の演算

$\sqrt{2}$ を $-\sqrt{2}$ で引きかえても四則演算がたもたれる。たとえば

どう
一
定
式
と
化
す
る
か

$$(1+\sqrt{2})(2-3\sqrt{2}) = 2 - 3\sqrt{2} + 2\sqrt{2} - 3 \cdot 2 = -4 - \sqrt{2}$$

この中の $\sqrt{2}$ をすべて $-\sqrt{2}$ で引きかえても等式が成立 ←

$$(1-\sqrt{2})(2+3\sqrt{2}) = 2 + 3\sqrt{2} - 2\sqrt{2} - 3 \cdot 2 = -4 + \sqrt{2}$$

OK

これが体の Galois 理論の基本的なアイデア！

体の言葉を使った定式化

体 K を $K = \mathbb{Q}$ と定める.

この L は K の拡大体の例になつていい.

体 L を $L = \mathbb{Q}(\sqrt{2}) = (\mathbb{Q} \text{ と } \sqrt{2} \text{ を含む最小の } (R \text{ の部分) 体})$

$$= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

こうなる.

(注) $\mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$

この σ が $\sqrt{2}$ を $-\sqrt{2}$ で交換する操作になつていい.

写像 $\sigma: L \rightarrow L$ を $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ ($a, b \in \mathbb{Q}$) と定める.

このとき, σ は体 L の(自己)同型写像になつていい.

σ は全単射なのでこれを示すためには, σ が四則演算を保つことを示せば十分である.

さらに, σ は $a \in \mathbb{Q}$ について $\sigma(a) = a$ をみたす,

するわち, σ は $K = \mathbb{Q}$ の元を動かさない,

(σ は体 L の体 K 上での自己同型であるといふ.)

問題 1-1 集合 $L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ が \mathbb{Q} と $\sqrt{2}$ を含む \mathbb{R} の最小の部分体になつてゐることを証明せよ.

\mathbb{R} の部分体とは \mathbb{R} の部分環で体になつてゐるもののことである.

証明するべきこと:

$\leftarrow L \cap \mathbb{Q}, L \ni \sqrt{2}$ は自明

(1) L は \mathbb{R} の部分環でかつ体になつてゐる.

(2) M を \mathbb{R} の部分環でかつ \mathbb{Q} と $\sqrt{2}$ を含むものとするとき, $L \subset M$.

この2つを示せば十分である. \square

$\leftarrow Q[\alpha] = (\mathbb{Q} \text{ と } \alpha \text{ を含む } \mathbb{R} \text{ の最小の部分環})$

問題 1-2 $\alpha, \beta \in \mathbb{R}$ のとき, $Q(\alpha) = (\mathbb{Q} \text{ と } \alpha \text{ を含む } \mathbb{R} \text{ の最小の部分体})$,

$Q(\alpha, \beta) = (\mathbb{Q} \text{ と } \alpha, \beta \text{ を含む } \mathbb{R} \text{ の最小の部分体})$ とおく. このとき,

$$Q(\sqrt{2}) = Q(-\sqrt{2}) = Q(\sqrt{2}, -\sqrt{2})$$

となることを示せ.

\square

問題 1-3

$$L = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$
 とおき,

写像 $\sigma: L \rightarrow L$ を $\sigma(a+b\sqrt{2}) = a-b\sqrt{2}$ ($a, b \in \mathbb{Q}$) と定める。

このとき、以下が成立することを示せ: $a \in \mathbb{Q}$, $\alpha, \beta \in L$ のとき

$$(0) \quad \sigma(a) = a.$$

$$(1) \quad \sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta).$$

$$(2) \quad \sigma(\alpha - \beta) = \sigma(\alpha) - \sigma(\beta),$$

$$(3) \quad \sigma(\alpha \beta) = \sigma(\alpha) \sigma(\beta),$$

$$(4) \quad \alpha \neq 0 のとき, \quad \sigma\left(\frac{1}{\alpha}\right) = \frac{1}{\sigma(\alpha)}.$$

□

問題 1-1 集合 $L = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ が \mathbb{Q} と $\sqrt{2}$ を含む \mathbb{R} の最小の部分体になつてゐることを証明せよ.

\mathbb{R} の部分体とは \mathbb{R} の部分環で体になつてゐるもののことである.

証明するべきこと:

$\leftarrow L \subset \mathbb{Q}, L \ni \sqrt{2}$ は自明

(1) L は \mathbb{R} の部分環でかつ体になつてゐる.

(2) M を \mathbb{R} の部分環でかつ \mathbb{Q} と $\sqrt{2}$ を含むものとするとき, $L \subset M$.

この2つを示せば十分である. \square

解答例 $\mathbb{Q} \subset L \subset \mathbb{R}$, $\sqrt{2} \in L$ は自明なので (1), (2) を示せば十分である.

(1) $0, 1 \in L$ でかつ, $\alpha, \beta \in L$ のとき, $\alpha + \beta, -\alpha, \alpha\beta \in L$ でかつ $\alpha \neq 0 \Rightarrow \frac{1}{\alpha} \in L$
 と2つことを示せばよい.
部分環 さらに体

$\mathbb{Q} \subset L$ より, $0, 1 \in L$ は自明. $\alpha, \beta \in L$ を任意にとる.

α, β は $\alpha = a+b\sqrt{2}$, $\beta = c+d\sqrt{2}$ ($a, b, c, d \in \mathbb{Q}$) と表わされる.

$$\alpha + \beta = (a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in L.$$

$$-\alpha = - (a+b\sqrt{2}) = (-a) + (-b)\sqrt{2} \in L.$$

$$\alpha\beta = (a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in L,$$

$\alpha = a+b\sqrt{2} \neq 0$ のとき, 分子分母に $a-b\sqrt{2}$ をかける

$$\frac{1}{\alpha} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in L.$$

(2) M は \mathbb{R} の部分環でかつ \mathbb{Q} と $\sqrt{2}$ を含むものであるとする. \leftarrow

任意に $\alpha \in L$ とする. $\alpha = a+b\sqrt{2}$, $a, b \in \mathbb{Q}$ と書ける.

$a, b, \sqrt{2} \in M$ かつ M が加法と乗法でとじていることより,

$\alpha = a+b\sqrt{2} \in M$. これで $L \subset M$ が示された, □

全設
(1) \mathbb{R} の部分体は
常に \mathbb{Q} を含む.
(2) \mathbb{C} の部分体も
常に \mathbb{Q} を含む.

問題 1-2

$\mathbb{Q}[\alpha] = (\mathbb{Q} \text{ と } \alpha \text{ を含む } \mathbb{R} \text{ の最小の部分環}) \leftarrow \text{あまけの説}$

$\mathbb{Q}(\alpha, \beta) = (\mathbb{Q} \text{ と } \alpha, \beta \text{ を含む } \mathbb{R} \text{ の最小の部分体}),$ \uparrow \uparrow ここからかう

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$$

となることを示せ。

解答例

$$(1) \quad \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(-\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, -\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})$$

を示せばよい,

(1) $-1 \in \mathbb{Q} \subset \mathbb{Q}(-\sqrt{2}), -\sqrt{2} \in \mathbb{Q}(-\sqrt{2})$ と $\mathbb{Q}(-\sqrt{2})$ が乗法^でとじていることより,

$$\sqrt{2} = (-1)(-\sqrt{2}) \in \mathbb{Q}(-\sqrt{2}),$$

$\mathbb{Q}(\sqrt{2})$ は \mathbb{Q} と $\sqrt{2}$ を含む \mathbb{R} の部分体の中で最小である^{こと}より $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(-\sqrt{2}),$

(2) $\mathbb{Q}(\sqrt{2}, -\sqrt{2})$ は $\mathbb{Q}, \pm\sqrt{2}$ を含む \mathbb{R} の部分体^で,

$\mathbb{Q}(-\sqrt{2})$ が $\mathbb{Q}, -\sqrt{2}$ を含む \mathbb{R} の部分体の中で最小である^{こと}より $\mathbb{Q}(-\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, -\sqrt{2}),$

(3) $\mathbb{Q}(\sqrt{2})$ が $\mathbb{Q} \text{ と } \pm\sqrt{2}$ を含む \mathbb{R} の部分体^で, $-\sqrt{2} = (-1)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

$\mathbb{Q}(\sqrt{2}, -\sqrt{2})$ が $\mathbb{Q}, \pm\sqrt{2}$ を含む \mathbb{R} の部分体の中で最小である^{こと}より $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}).$ □

問題 1-3 $L = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ とすき,

写像 $\sigma: L \rightarrow L$ で $\sigma(a+b\sqrt{2}) = a-b\sqrt{2}$ ($a, b \in \mathbb{Q}$) と定める.

このとき, 以下が成立することを示せ: $a \in \mathbb{Q}$, $\alpha, \beta \in L$ のとき

$$(0) \quad \sigma(a) = a.$$

$$(1) \quad \sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta).$$

$$(2) \quad \sigma(\alpha - \beta) = \sigma(\alpha) - \sigma(\beta).$$

$$(3) \quad \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta).$$

$$(4) \quad \alpha \neq 0 \text{ のとき}, \quad \sigma\left(\frac{1}{\alpha}\right) = \frac{1}{\sigma(\alpha)}.$$

$(\sigma \text{は } L \text{ の } \mathbb{Q} \text{ 上の})$
 (自己同型になつてゐる。)

□

解答例

$$(0) \quad \sigma(a) = \sigma(a + 0\sqrt{2}) = a - 0\sqrt{2} = a$$

$\alpha = a + b\sqrt{2}$, $\beta = c + d\sqrt{2}$, $a, b, c, d \in \mathbb{Q}$ と書ける, (二の a は上の a とは別)

$$(1, 2) \quad \sigma(\alpha \pm \beta) = \sigma((a \pm c) + (b \pm d)\sqrt{2}) = (a \pm c) - (b \pm d)\sqrt{2}$$

$$\sigma(\alpha) \pm \sigma(\beta) = (a - b\sqrt{2}) \pm (c - d\sqrt{2}) \quad //$$

$$(3) \quad \sigma(\alpha\beta) = \sigma((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2}$$

$$\sigma(\alpha)\sigma(\beta) = (a - b\sqrt{2})(c - d\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} \quad //$$

(4) $\alpha = a + b\sqrt{2} \neq 0$ のとき,

$$\begin{aligned} \sigma\left(\frac{1}{\alpha}\right) &= \sigma\left(\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}\right) \\ &= \frac{a}{a^2 - 2b^2} - \frac{-b}{a^2 - 2b^2}\sqrt{2} \\ \frac{1}{\sigma(\alpha)} &= \frac{1}{a - b\sqrt{2}} = \frac{a + b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} + \frac{b}{a^2 - 2b^2}\sqrt{2} \end{aligned}$$

OK

3次方程式 (の解法に向けて)

問題 1-4 $x^3 + y^3 + z^3 - 3xyz$ を x, y, z の 1 次式の積で表せ.

ヒント $w = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2}$ を使ってよい.

実際には $w^2 + w + 1 = 0, w^3 = 1$ のみを使う. □

問題 1-5 $\alpha = \sqrt[3]{2} = 2^{\frac{1}{3}}$, $L = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$ とおく.

L が \mathbb{Q}, α を含む \mathbb{R} の最小の部分体になつてることを示せ. □

問題 1-4 $x^3 + y^3 + z^3 - 3xyz$ を x, y, z の 1 次式の積で表せ.

ヒント $w = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2}$ を使ってよい.

実際には $w^3 + w + 1 = 0, w^3 = 1$ のみを使う.

□

解答例 次を地道な計算で示せ:

$$(x+y+z)(x^2+y^2+z^2 - xy - xz - yz) = x^3 + y^3 + z^3 - 3xyz,$$

さて、

$$\begin{aligned} & (x+wy+w^2z)(x+w^2y+wz) \\ &= \left\{ \begin{array}{lcl} x^2 & + & \underline{w^2xy} \\ + \underline{wxz} & + & y^2 \\ + \underline{w^2xz} & + & \underline{wyz} \end{array} \right. \quad \begin{array}{l} \downarrow \\ w^3 = 1 \text{ を使う} \end{array} \\ &= x^2 + y^2 + z^2 - xy - xz - yz. \quad \begin{array}{l} \downarrow \\ w^2 + w + 1 = 0 \text{ より} \\ w^2 + w = -1 \text{ を使う} \end{array} \end{aligned}$$

したがって、

$$x^3 + y^3 + z^3 - 3xyz = (x+y+z)(x+wy+w^2z)(x+w^2y+wz),$$

□

余談 $(x^3 + y^3 + z^3 - 3xyz)$ の行列式表示)

$$\begin{vmatrix} x & y & z \\ z & x & y \\ y & z & x \end{vmatrix} = x^3 + y^3 + z^3 - 3xyz$$

$$= \left\{ \begin{array}{l} x(x^2 + y^2 + z^2) \\ -xyz - yzx - zxy \end{array} \right\} = x^3 + y^3 + z^3 - 3xyz.$$

以上のように見れば” 3×3 を $n \times n$ に一般化できる。

$$E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \Lambda = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \text{ とおくと, } xE + y\Lambda + z\Lambda^2 = \begin{bmatrix} x & y & z \\ z & x & y \\ y & z & x \end{bmatrix}.$$

$$\Lambda \text{ の対角化: } U = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix} \text{ とおくと, } \Lambda U = UD$$

でかつ $U^* = U^{-1}$ となることを示せる。(練習: 示してみよ!)

$$\text{ゆえに } \Lambda = UDU^{-1}. \text{ したがって, } xE + y\Lambda + z\Lambda^2 = U(xE + yD + zD^2)U^{-1}.$$

$$\therefore |xE + y\Lambda + z\Lambda^2| = |xU + yD + zD^2| = (x+y+z)(x+\omega y + \omega^2 z)(x+\omega^2 y + \omega z),$$

もう少し見易く書く,

$$\begin{aligned} xE + yA + zA^2 &= U(E + yD + zD^2)U^{-1}, \quad D = \begin{bmatrix} 1 & w & w^2 \\ & w & w^2 \\ & & w^2 \end{bmatrix}, \quad D^2 = \begin{bmatrix} 1 & w^2 & w \\ & w^2 & w \\ & & w \end{bmatrix} \\ &= U \left(\begin{bmatrix} x & & \\ & x & \\ & & x \end{bmatrix} + \begin{bmatrix} y & & \\ & wy & \\ & & w^2y \end{bmatrix} + \begin{bmatrix} z & & \\ & w^2z & \\ & & wz \end{bmatrix} \right) U^{-1} \\ &= U \begin{bmatrix} x+y+z & & \\ & x+wy+w^2z & \\ & & x+w^2y+wz \end{bmatrix} U^{-1}. \end{aligned}$$

$$\begin{aligned} \therefore |xE + yA + zA^2| &= \begin{vmatrix} x+y+z & & \\ & x+wy+w^2z & \\ & & x+w^2y+wz \end{vmatrix} \\ &= (x+y+z)(x+wy+w^2z)(x+w^2y+wz). \end{aligned}$$

練習 以上の計算を $2 \times 2, 4 \times 4, n \times n$ に一般化せよ. \square

解答例の解説を来週やる問題

来週まで準備して考えてください。

問題 1-5

$$\alpha = \sqrt[3]{2} = 2^{\frac{1}{3}}, \quad L = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$$

L が \mathbb{Q}, α を含む \mathbb{R} の最小の部分体になつてることを示せ. \square

既出

ヒント $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ の証明は問題 1-1 でやった。

それと同じようにして, $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$ を示せよ。

このとき, $\beta = a + b\alpha + c\alpha^2 \neq 0$ に対する $\frac{1}{\beta}$ の分母の有理化が必要になる。 \square

問題 1-6

x に関する 3 次方程式 $x^3 - 3px + q = 0$ の解法を作れ. \square

ヒント

$p = yz, \quad q = y^3 + z^3$ とできたらどうなるか? → 問題 1-4. \square

問題 1-7

$x^3 + 2x - 2 = 0$ を満たす正の実数 $x = \alpha$ が存在することを示せ。

さらに α の具体的な形を求めよ ($\sqrt{}$ と $\sqrt[3]{}$ を使って表せ). \square

問題 1-5

$$\alpha = \sqrt[3]{2} = 2^{\frac{1}{3}}, \quad L = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$$

L が \mathbb{Q}, α を含む \mathbb{R} の最小の部分体になつてることを示せ. \square

解答例

(1) L は \mathbb{R} の部分体であり, \mathbb{Q} と α を含む.

(2) $M \subseteq \mathbb{R}$ の部分体で \mathbb{Q}, α を含むものとすると $L \subseteq M$.

(1) L が \mathbb{R} の部分体で \mathbb{Q}, α を含むことを示す.

$\mathbb{Q} \subseteq L$ と $\alpha \in L$ は明らか.

L が \mathbb{R} の部分体であることを示すために, 0 と 1 を含み, $+, -, \times$ で閉じていて, 任意の $\beta \in L$ について $\beta \neq 0 \Rightarrow \beta^{-1} \in L$ となることを示せばよい.

$0 \in L, 1 \in L$ および L が 加法と減法で閉じていることは明らか.

L が 乗法で閉じていることを示す. $\beta, \gamma \in L$ を任意にとる. このとき,

$$\beta = a + b\alpha + c\alpha^2, \quad \gamma = a' + b'\alpha + c'\alpha^2 \quad (a, b, c, a', b', c' \in \mathbb{Q})$$

と書ける. そして,

$$\beta\gamma = (aa' + 2bc' + 2cb') + (ab' + ba' + 2cc')\alpha + (ac' + bb' + ca')\alpha^2 \in L.$$

これで L が 乗法で閉じていることがわかった.

$\beta \in L$, $\beta \neq 0$ と仮定する. $\beta = a + b\alpha + c\alpha^2$ ($a, b, c \in \mathbb{Q}$) と書ける.

$\frac{1}{\beta} = \frac{1}{a+bd+cd^2} \in L$ とすることを示す。(2)

$$\text{公式 } (x+y+z)(x^2+y^2+z^2-xy-xz-yz) = x^3+y^3+z^3-3xyz$$

$x = a$, $y = b\alpha$, $z = c\alpha^2$ に適用すると,

$$\beta(x^2+y^2+z^2-xy-xz-yz) = \overbrace{a^3+2b^3+4c^3-6abc}^{\text{これを } d \text{ と書く}} \in \mathbb{Q},$$

$\in L$ $a'+b'\alpha+c'\alpha^2 \quad (a', b', c' \in \mathbb{Q})$ と書ける

もしもこれの右边が“0”でなければ、両辺を $\beta \times (\text{右边})$ で割ることによると、

$$\frac{1}{\beta} = \frac{a' + b'd + c'd^2}{d} = \frac{a'}{d} + \frac{b'}{d}d + \frac{c'}{d}d^2 \in L.$$

(左辺) = $d \neq 0$ を示すためにには、 $\beta \neq 0$ と仮定していた $x^2 + y^2 + z^2 - xy - xz - yz \neq 0$ を示せばよい。 $x, y, z \in \mathbb{R}$ で $\beta \neq 0$ より、 x, y, z の 2 つは 0 ではないので、 $x \neq y, x \neq z, y \neq z$ のどれかは成立しているので、

$$x^2 + y^2 + z^2 - xy - xz - yz = \frac{1}{2} \left((x-y)^2 + (x-z)^2 + (y-z)^2 \right) > 0.$$

示すべきところが示された。

F.-c.d.

問題1-6 x に関する3次方程式 $x^3 - 3px + q = 0$ の解法を作れ. \square

解答例 (問題1-4の解答例を見よ.) $w^2 + w + 1 = 0$ と仮定する. wは1の原始3乗根と仮定

$p=0$ のとき, $x^3 + q = 0$ は $x = \sqrt[3]{-q}$, $w\sqrt[3]{-q}$, $w^2\sqrt[3]{-q}$ と解ける.

以下, $p \neq 0$ と仮定する. 問題1-4の結果より,

$$x^3 - 3yz \cdot x + (y^3 + z^3) = (x+y+z)(x+wz+wy)(x+w^2z+wy^2).$$

ゆえに, もともと与えられた $p(\neq 0)$, q に対して, $yz = p$, $y^3 + z^3 = q$ をみたす (y, z) を作れれば, $x^3 - 3px + q = 0$ は $x = -y - z$, $-wy - w^2z$, $-w^2y - wz$ と解ける.

$YZ = p^3$, $Y + Z = q$ をみたす Y, Z は2次方程式 $\lambda^2 - q\lambda + p^3 = 0$ の解になる.

そういう1つを (Y, Z) と書く. $y^3 = Y$ をみたす y を1つ取り, $z = \frac{p}{y}$ とおくと, $yz = p$ となり, $z^3 = \frac{p^3}{Y} = Z$ となるので, $y^3 + z^3 = Y + Z = q$. これでほしい y, z を作れた.

解法まとめ ① $\lambda^2 - q\lambda + p = 0$ の解の1つを Y と書く.

② $y^3 = Y$ をみたす y を1つ取り, $z = \frac{p}{y}$ とおく.

③ $x = -y - z$, $-wy - w^2z$, $-w^2y - wz$ ($w^2 + w + 1 = 0$). \square

問題1-7

$x^3 + 2x - 2 = 0$ を満たす正の実数 $x = \alpha$ が存在することを示せ。

さらに α の具体的な形を求めよ(根と³根を使って表せ)。

□

WolframAlpha

Input: $2/(3(\sqrt{35/27} - 1)^{(1/3)}) - (\sqrt{35/27} - 1)^{(1/3)}$

Result:

$$\frac{2}{3\sqrt[3]{\sqrt{\frac{35}{27}} - 1}} - \sqrt[3]{\sqrt{\frac{35}{3}} - 1}$$

Decimal approximation: 0.7709169970592481008251463693070269672550531193633286151005984929767351032820534076249331528876...

More digits

Alternate forms:

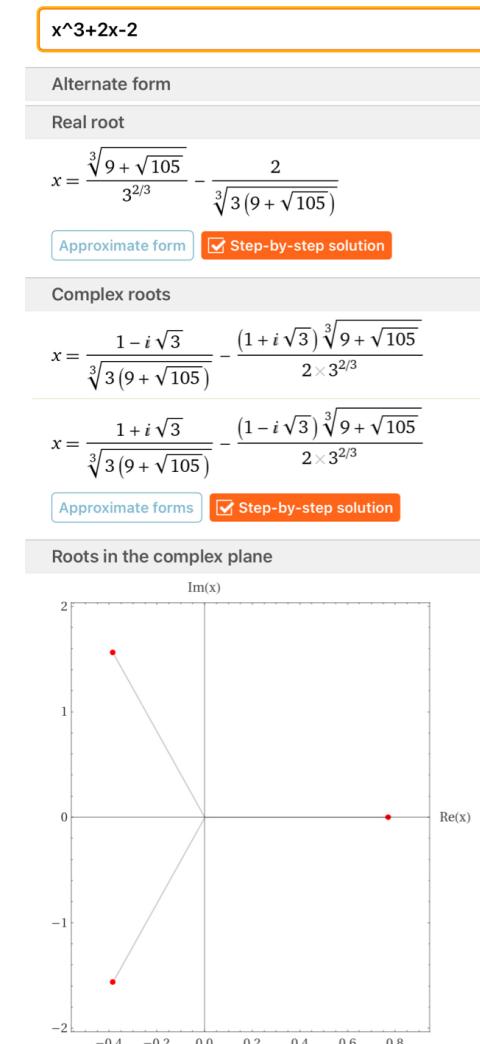
$$\frac{2 \times 3^{2/3} - \sqrt[3]{3} (\sqrt{105} - 9)^{2/3}}{3\sqrt[3]{\sqrt{105} - 9}}$$

root of $x^3 + 2x - 2$ near $x = 0.770917$

$$\frac{2}{\sqrt[3]{3}\sqrt[3]{\sqrt{105} - 9}} - \frac{\sqrt[3]{\sqrt{105} - 9}}{3^{2/3}}$$

More forms Step-by-step solution

Minimal polynomial: $x^3 + 2x - 2$



<https://www.wolframalpha.com/input/?i=2%2F283%28E%2888%9A%2835%2F27%29%20-%201%29%5E%281%2F3%29%29%20-%20%28E%2888%9A%2835%2F27%29%20-%201%29%5E%281%2F3%29>

<https://www.wolframalpha.com/input/?i=x%5E3%2B2x-2>

解答例 $x^3 + 2x - 2 \stackrel{(*)}{=} 0$ の正の実数解を求めたい。

$p = -\frac{2}{3}$, $q = -2$ とおくと, $(*)$ は $x^3 - 3px + q = 0$ と書ける。

問題1-6の解法を使おう、 $\lambda^2 - q\lambda + p^3 = \lambda^2 + 2\lambda - \frac{8}{27} = 0$ の正の実数解は

$$Y = -1 + \sqrt{1^2 + \frac{8}{27}} = \sqrt{\frac{35}{27}} - 1 > 0.$$

$y = \sqrt[3]{Y} > 0$, $z = \frac{p}{y} = -\frac{2}{3y} < 0$ とおく、問題1-6の結果より、

$$\alpha = -y - z = \frac{2}{3\sqrt[3]{Y}} - \sqrt[3]{Y} \in \mathbb{R}$$

は $(*)$ の実数解になっている。 $(\alpha \neq 0.77$ なので $\alpha > 0$ た"が, 別の方法で $\alpha > 0$ であることを示す。)

$f(x) = x^3 + 2x - 2$ とおくと, $f'(x) = 3x^2 + 2 > 0$ ($x \in \mathbb{R}$) なので, $f(x)$ は \mathbb{R} 上で狭義単調増加し, $f(0) = -2$, $f(1) = 1$ なので, $f(x) = 0$ は唯一つの実数解を持ち, その実数解は上の α になる。(さうに $0 < \alpha < 1$ も示せている。) □

問題 2-1 (易) $x^3 - 15x + 4 = 0$ の3つの解を問題1-6の解答例の方法で作り,
-4が解の1つになっていたことを使って求めた3つの解と一致することを示せ.

次ページを見る前にこの問題を解くこと、動画もここでストップ！

ためしに4の約数±1, ±2, ±4をxに代入すると, $x = -4$

$$x^3 - 15x + 4 = -4^3 + 15 \cdot 4 + 4 = -64 + 60 + 4 = 0.$$

$$\begin{array}{r} x^2 - 4x + 1 \\ \hline x+4 \sqrt{x^3 - 15x + 4} \\ \hline x^3 + 4x \\ \hline -4x - 15x \\ \hline -4x - 16x \\ \hline x + 4 \\ \hline x + 4 \\ \hline 0 \end{array}$$

$$x^3 - 15x + 4 = (x+4)(x^2 - 4x + 1)$$

$$x^2 - 4x + 1 = 0 \Leftrightarrow x = 2 \pm \sqrt{3}$$

$x^3 - 15x + 4 = 0$ の解は

$$x = -4, 2 \pm \sqrt{3}$$

解答例

$p=5, q=4$ とおく。

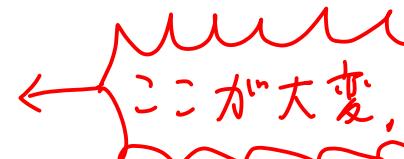
$x^3 - 15x + 4 = x^3 - 3px + q = 0$ は問題1-6の解答例によれば以下のようにして解ける。 $\lambda^2 - q\lambda + p^3 = \lambda^2 - 4\lambda + 125 = 0$ を解くと、

$$\lambda = 2 \pm \sqrt{4-125} = 2 \pm \sqrt{-121} = 2 \pm \sqrt{11}i \quad (\hat{i} = \sqrt{-1}).$$

$Y = 2 + \sqrt{11}i$ とおく、 Y の立方根の1つを $y = \sqrt[3]{2+11i}$ と書き、 $z = \frac{p}{y} = \frac{5}{y}$ とおく、このとき $x^3 - 15x + 4 = 0$ は次のように解ける：

$$x = -y - z, \quad -wy - w^2z, \quad -w^2y - wz \quad (w^2 + w + 1 = 0),$$

$$\{-y - z, \quad -wy - w^2z, \quad -w^2y - wz\} = \{-4, \quad 2 + \sqrt{3}, \quad 2 - \sqrt{3}\} \text{ を示す}.$$

γ の立法根の 1 つとして, $y = \boxed{2+i}$ がとれる. 

$$\text{実際, } (2+i)^3 = 2^3 + 3 \cdot 2^2 i + 3 \cdot 2 \cdot i^2 + i^3 = 8 + 12i - 6 - i = 2 + 11i = \gamma.$$

$$\underline{z} = \frac{5}{y} = \frac{5}{2+i} = \frac{5(2-i)}{(2+i)(2-i)} = \frac{5(2-i)}{4+1} = \boxed{2-i} = z$$

このとき, $y = 2+i$ と $z = 2-i$ より, $w = \frac{-1+\sqrt{3}i}{2}$ とおこう, $w^2 = \frac{-1-\sqrt{3}i}{2} z$

$$\left\{ \begin{array}{l} -y-z = \underline{-2-i} - \underline{2+i} = -4 \\ -wy-w^2z = \end{array} \right.$$

$$\left. \begin{array}{l} -\frac{-1+\sqrt{3}i}{2}(2+i) - \frac{-1-\sqrt{3}i}{2}(2-i) = -1 \operatorname{Re}\left(\frac{-1+\sqrt{3}i}{2}(2+i)\right) = 2+\sqrt{3} \\ \text{互いに複素共役 } z+\bar{z}=2\operatorname{Re}(z) \end{array} \right.$$

$$\left. \begin{array}{l} -w^2y-wz = -\frac{-1-\sqrt{3}i}{2}(2+i) - \frac{-1+\sqrt{3}i}{2}(2-i) = -2 \operatorname{Re}\left(\frac{-1-\sqrt{3}i}{2}(2+i)\right) = 2-\sqrt{3} \end{array} \right.$$

これで示すべきことが示された. □

ポイント

$2+11i$ の立法根の 1 つとして $2+i$ がとれること. □

Eisenstein の 判定法

$$p|ab \Rightarrow p|a \text{ or } p|b$$

準備 UFD

R を 整域 とし, K は その 商体 (分數体) であると仮定する.

$p \in R$, $p \neq 0$ に対して, $(p) = Rp$ が R の 素イデアル になるとき, p は R の 素元 であるといふ.

$p \in R$ が $p \notin R^\times$ をみなし, R^\times の元と $R^\times p$ の元以外に 約数を持たないとき,
 p は R の 既約元 であるといふ. ($K[x]$ の 既約元 と $K[x]$ に含まれる 既約多項式 は 一致する.)

注意 整域の素元は常に既約元になるが一般には逆は成立しない. \square

以下の 2 つの 同値な 条件のどちらかが成立しているとき, R は 一意分解整域 (unique factorization domain, UFD) であるといふ: (同値性 (a) \Leftrightarrow (b) は 非自明!)

(a) $a \in R$, $a \neq 0$ のとき, $a = p_1 \cdots p_n$, p_i は R の 既約元 と書け, p_1, \dots, p_n は 順序と R の 可逆元 とのかけいを除いて 一意に定まる.

(b) $a \in R$, $a \neq 0$ のとき, $a = p_1 \cdots p_n$, p_i は R の 素元 と書ける.

注意

UFD の 既約元 は 常に 素元 になるので, UFD において 素元 と 既約元 は 同じものになる. \square

UFDについて色々非自明なことはあるが、素因数分解の存在と（積の順序と可逆元倍の順序を除いた）一意性が成立している整域のことがあり、素元と既約元という2種類の素数の一般化が一致している整域であることを認識していれば、この演習について行くためには十分だと思われる。

以下をまとめ使って良いことにする：

- PIDはUFDである。
- たとえば \mathbb{Z} や体 K 上の1変数多項式環 $K[x]$ は PIDなので UFDである。
- R が UFDのとき、 $R[x]$ や $R[[x]]$ も UFDである。

我々は特に \mathbb{Z} と \mathbb{Q} の組を例として多用する。

まとめ
使ってよい



以下, R は UFD であるとし, K はその商体であるとする. UFD に該当制限

$f(x) = \sum a_i x^i \in R[x]$ の係数 a_0, a_1, a_2, \dots (有限個) の最大公約数が 1 のとき,

$f(x)$ は R 上の 原始多項式 であるといふ.

正確には $\overset{\uparrow}{R}$ 可逆元

たとえば $f(x) = 6x^2 + 10x + 15$ は \mathbb{Z} 上の原始多項式である.

しかし, $g(x) = 2f(x) = 12x^2 + 20x + 30$ はえうでではない. $\uparrow R[x]$ 内の該

$f \in K[x]$ の内容 $\rightarrow K[x]$ も出て来る.

$f(x) = \sum_i a_i x^i \in K[x], f(x) \neq 0$ のとき, a_i の中の分母をまとめることにより, \exists ,

$f(x) = \frac{1}{b} \sum_i c_i x^i, b, c_i \in R$ と書ける. c_i たちの最大公約数を d と書き,

$c_i = d c'_i, c'_i \in R$ と表わすとき, $f_0(x) = \sum_i c'_i x^i$ は原始多項式になり,

$c = \frac{d}{b} \in K$ とおくと, $f(x) = c f_0(x).$ $\leftarrow f(x)$ は K の元と R 上の原始多項式の積で書ける.

内容 C の一意性

$c f_0(x) = \tilde{c} \tilde{f}_0(x)$, $\tilde{f}_0(x)$ は R 上の原始多項式で $\tilde{c} \in K$ と仮定する. $c = \frac{b}{a}$, $\tilde{c} = \frac{\tilde{b}}{\tilde{a}}$,
 $a, b, \tilde{a}, \tilde{b} \in R$, a と b は互いに素, \tilde{a} と \tilde{b} は互いに素と書け, $\tilde{a}\tilde{b}f_0(x) = abf_0(x)$,
両辺の係数の最大公約数はそれぞれ $\tilde{a}\tilde{b}$, ab になる. a と b が互いに素で
 \tilde{a} と \tilde{b} が互いに素なことより, \tilde{a}, \tilde{b} はそれぞれ a, b の R の 可逆元倍になる.

これで, 0 キ $f(x) \in K[x]$ のとき, ある $c \in K^\times$ と R 上の原始多項式 $f_0(x)$ で
 $f(x) = c f_0(x)$ をみたすものが, R の可逆倍を除いて一意的に定まることか
わかった. このような c を f の 内容 と呼ぶ.

f の内容の 1つを $I(f)$ と書こう. ← $I(f)$ の定義

たとえば $f(x) = \frac{12}{7}x^2 + \frac{20}{7}x + \frac{30}{7} = \frac{2}{7}(6x^2 + 10x + 15)$ より, $I(f) = \frac{2}{7}$ とされる.

Gaussの補題

R は UFD であるとし, K はその商体であると仮定する.

このとき, R 上の原始多項式の積は R 上の原始多項式に^{なり},

$f, g \in K[x], f \neq 0, g \neq 0$ に対して, $I(fg)$ と $I(f)I(g)$ は R の可逆元倍のちかいを除いて等しい.

証明

内容の R の可逆元倍を除いた一意性と $fg = I(f)I(g) f_0 g_0$ (f_0, g_0 は R 上の原始多項式) より, $f_0 g_0$ も R 上の原始多項式ならば $I(fg)$ は $I(f)I(g)$ の R の可逆元倍になる.

$f, g \in R[x]$ は原始多項式であるとする. $f(x) = \sum_i a_i x^i, g(x) = \sum_j b_j x^j, a_i, b_j \in R$ と書く,
 p は R の任意の素元であるとする.

f, g は原始多項式なのである s, t が存在して, a_s, b_t は p で割り切れない.

s, t として, そのようなものの中で最小のものとすると,

$$(fg \text{ の } x^{s+t} \text{ の係数}) = \underbrace{a_0 b_{s+t} + \dots + a_{s-1} b_{t+1}}_{\substack{a_0, \dots, a_{s-1} \text{ が} \\ p \text{ で割り切れる}}}_{\substack{\text{p で} \\ \text{割り} \\ \text{切れない}}} + \underbrace{a_s b_t}_{\substack{\text{p で} \\ \text{割り} \\ \text{切れない}}} + \underbrace{a_{s+1} b_{t-1} + \dots + a_{s+t} b_0}_{\substack{b_0, \dots, b_{t-1} \text{ が} \\ p \text{ で割り切れる}}} \quad \left. \right] p \text{ で} \\ \text{割り切れない}.$$

となるので, fg の係数で p で割り切れないものが存在する.

これより, fg が R 上の原始多項式であることがわかる.

q.e.d.

(注) 自然な射影 $\pi_p: R[x] \rightarrow R[x]/(p) = (R/(p))[x]$ を使えばもっとわかりやすくなる.

準備したかった結果

R は UFD であり, K はその商体であると仮定する.

$R[x]$ に含まれる多項式で 1 次以上の 2 つの $R[x]$ の元の積に分解されないものは, $K[x]$ における既約多項式になる.

たとえば, \mathbb{Z} 係数多項式で 1 次以上の 2 つの \mathbb{Z} 係数多項式の積に分解されないものは 1 次以上の 2 つの \mathbb{Q} 係数多項式の積にも分解されない.

証明

$h \in R[x]$ かつ $h = fg$, $f, g \in K[x]$, $\deg f \geq 1$, $\deg g \geq 1$ と分解されると仮定する.

$f = I(f)f_0$, $g = I(g)g_0$, $h = I(h)h_0$, f_0, g_0, h_0 は R 上の原始多項式と書ける.

$h \in R[x]$ より, $I(h) \in R$ であることに注意せよ.

Gauss の補題より, $I(h) = a I(f) I(g)$, $a \in R^\times$ と書けるので

$$I(f) I(g) f_0 g_0 = fg = h = I(h) h_0 = a I(f) I(g) h_0,$$

$$\therefore h_0 = a^{-1} f_0 g_0, \quad h = I(h) a^{-1} f_0 g_0, \quad \leftarrow \text{これは } h \text{ の } R[x] \text{ 内での分解}$$

したがって, h は $R[x]$ でも 1 次以上の多項式の積に分解される.

以上の対偶をとれば上の補題が得られる

□

勉強の仕方

$R = \mathbb{Z}$, $K = \mathbb{Q}$ の場合に上の証明を書き直してみよ. □

Eisenstein の判定法 R は UFD であるとし, K はその商体であるとする.

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in R[x]$, $a_i \in R$ と R の素元 p について,

$p \nmid a_n, p | a_{n-1}, \dots, p | a_1, p | a_0, p^2 \nmid a_0 \Rightarrow f(x)$ は K 上既約.

証明 前ページの結果より, K 上既約であることを示すためには,

非自明な
ポイント

1次以上の $R[x]$ の2つの元の積に $f(x)$ が分解されないことを示せばよい.

結局, 次を示せばよい:

$p \nmid a_n, p | a_{n-1}, \dots, p | a_1, p | a_0$ かつ

$f(x)$ が 1次以上の $R[x]$ の2つの元の積に分解される } $\Rightarrow p^2 | a_0$.

$p \nmid a_n, p | a_{n-1}, \dots, p | a_0$ かつ $f = gh$, $g, h \in R[x]$, $\deg g \geq 1$, $\deg h \geq 1$

と仮定する. このとき, 自然な射影 $\pi_p : R[x] \rightarrow R[x]/(p) = (R/(p))[x]$ について,

$\pi_p(f) = \bar{a}_n x^n = \pi_p(g) \pi_p(h), 0 \neq \bar{a}_n \in R/(p).$

俠義を mod p で
 $R/(p)$ にうつす

ゆえに, $\pi_p(g), \pi_p(h)$ の定数項は $R/(p)$ の中で 0 になる.

すなわち, g と h の定数項はどちらも p で割り切れる.

このことから $f = gh$ の定数項 a_0 が p^2 で割り切れることがわかる. \square

易しい
部分

問題 2-2 以下の \mathbb{Z} 係数多項式たちが \mathbb{Q} 上の既約多項式になることを示せ.

$$(1) \quad x^3 + 2x - 2.$$

$$(2) \quad x^4 + 10x^3 + 15x^2 + 35x + 55.$$

$$(3) \quad \text{正の整数 } n \text{ に対する } x^n - 14.$$

$$(4) \quad \text{素数 } p \text{ に対する } x^{p-1} + x^{p-2} + \dots + x + 1. \quad \text{例: } x+1, x^2+x+1, x^4+x^3+x^2+x+1, \\ x^6+x^5+\dots+x+1, \dots$$

ヒント (1), (2), (3) は直接 Eisenstein の判定法を適用できる:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x] \text{ と 素数 } p \text{ について,}$$

$$p \nmid a_n, \quad p \mid a_{n-1}, \dots, p \mid a_1, \quad p \mid a_0, \quad p^2 \nmid a_0 \Rightarrow f(x) \text{ は } \mathbb{Q} \text{ 上既約.}$$

(4) には直接的に Eisenstein の判定法を適用できないので、少しくふりしてみよ, □

おまけ $x^3 - 15x + 4$ には、 $2^2 \mid 4$ なので Eisenstein の判定法を使えない。

$$x^3 - 15x + 4 = (x+4)(x^2 - 4x + 1) \text{ なので } x^3 - 15x + 4 \text{ は既約でない.} \quad \square$$

注意 $x^{mn-1} + x^{mn-2} + \dots + x + 1 = \frac{x^{mn} - 1}{x - 1} = \frac{x^m - 1}{x - 1} (x^{m(n-1)} + x^{m(n-2)} + \dots + x^m + 1)$
 $= (x^{m-1} + x^{m-2} + \dots + x + 1)(x^{m(n-1)} + x^{m(n-2)} + \dots + x^m + 1)$ は既約でない. □

問題 2-3

R は可換環であるとし, $p \in R$ であるとする.

$a \in R$ の R/pR での像を \bar{a} と書き, 写像 $\varphi: R[x] \rightarrow (R/pR)[x]$

$$\varphi\left(\sum_i a_i x^i\right) = \sum_i \bar{a}_i x^i \quad (a_i \in R)$$

と定める. 以下を示せ.

- (1) φ は環の準同型写像である.
- (2) φ は全射である.
- (3) $\text{Ker } \varphi = pR[x]$
- (4) 環の同型写像 $\bar{\varphi}: R[x]/pR[x] \xrightarrow{\sim} (R/pR)[x]$, $(f \bmod p) \mapsto \varphi(f)$ が得られる.

注意

$pR[x]$ も pR も (p) と書かれることがある. 分脈により, で区別せよ.

$$R[x]/\underline{(p)} \xrightarrow{\sim} (R/\underline{(p)})[x], (f \bmod p) \mapsto \varphi(f).$$

互いに異ることに注意

□

問題 2-4 $\omega^3 = 1$ と仮定し, $\alpha = \omega\sqrt[3]{7}$ とおき, 写像 $\varphi: \mathbb{Q}[x] \rightarrow \mathbb{Q}[\alpha]$ を
 $\varphi(f(x)) = f(\alpha) \quad (f \in \mathbb{Q}[x])$

と定める. 以下で " $\mathbb{Q}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Q}[x]\}$ " を用いて使ってよい. 以下を示せ.

- (1) φ は全射環準同型でかつ $a \in \mathbb{Q}$ に対して $\varphi(a) = a$.
- (2) $f(x) = x^3 - 7$ は \mathbb{Q} 上の既約多項式である
- (3) $\text{Ker } \varphi = (x^3 - 7)\mathbb{Q}[x]$. これを $(x^3 - 7)$ と書く.
- (4) 環として, $\mathbb{Q}[x]/(x^3 - 7) \cong \mathbb{Q}[\alpha]$.
- (5) $\mathbb{Q}[\alpha]$ は体になる.

ヒント • 準同型定理.

- Eisenstein の判定法.
- $\mathbb{Q}[x]$ の既約多項式 $f(x)$ は $\mathbb{Q}[x]$ の极大イデアルを生成する. □

問題 2-2

以下の \mathbb{Z} 係数多項式たちが \mathbb{Q} 上の既約多項式になることを示せ。

$$(1) \quad x^3 + 2x - 2.$$

$$(2) \quad x^4 + 10x^3 + 15x^2 + 35x + 55.$$

$$(3) \quad \text{正の整数 } n \text{ に対する } x^n - 14.$$

$$(4) \quad \text{素数 } p \text{ に対する } x^{p-1} + x^{p-2} + \dots + x + 1.$$

例: $x+1, x^2+x+1, x^4+x^3+x^2+x+1,$

$$x^6+x^5+\dots+x+1, \dots$$

記号

$a|b \Leftrightarrow a \tilde{|} b$ は割り切れる $\Leftrightarrow a$ は b の約数 $\Leftrightarrow b$ は a の倍数

$a|b$ の否定を $a \nmid b$ と書く。

例

- $2+1, \underline{2|0}, 2|2, 2|4, 2|6, \dots$

Eisenstein の判定法の \mathbb{Z} の場合

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \quad a_i \in \mathbb{Z}$ のとき, 素数 p について,

$p \nmid a_n, \quad p | a_{n-1}, \dots, p | a_1, \quad p | a_0, \quad p^2 \nmid a_0 \Rightarrow f(x)$ は \mathbb{Q} 上既約。

解答例

(1), (2), (3) では Eisenstein の判定法を直接使う。

(1) $x^3 + 2x - 2.$ 210 の 0 は x^2 の係数

$2 \nmid 1, 2 \nmid 0, 2 \nmid 2, 2 \nmid -2, 2^2 \nmid -2$ と Eisenstein の判定法より, これは \mathbb{Q} 上既約。

(2) $x^4 + 10x^3 + 15x^2 + 35x + 55.$

$5 \nmid 1, 5 \nmid 10, 5 \nmid 15, 5 \nmid 35, 5 \nmid 55, 5^2 \nmid 55$ と Eisenstein の判定法より, これは \mathbb{Q} 上既約。

(3) 正の整数 n に対する $x^n - 14.$

$7 \nmid 1, 7 \nmid 0, \dots, 7 \nmid 0, 7 \nmid -14, 7^2 \nmid -14$ と Eisenstein の判定法より, これは \mathbb{Q} 上既約。

この次の(4)には直接に Eisenstein の判定法を使えない、

任意の $a \in \mathbb{Q}$ と $f(x) \in \mathbb{Q}[x]$ について,

$f(x)$ は \mathbb{Q} 上既約 $\Leftrightarrow f(x+a)$ は \mathbb{Q} 上既約

を使う,

$$(\because f(x) = g(x)h(x) \Leftrightarrow f(x+a) = g(x+a)h(x+a))$$

(4) 素数 p に対する $x^{p-1} + x^{p-2} + \dots + x + 1$, これを $\varphi_p(x)$ と書く.

$\varphi_2(x) = x+1$ は 1 次なので \mathbb{Q} 上既約.

$$\varphi_3(x) = x^2 + x + 1 = \frac{x^3 - 1}{x - 1} \text{ より},$$

$$\varphi_3(x+1) = \frac{(x+1)^3 - 1}{x} = \frac{x^3 + 3x^2 + 3x + 1 - 1}{x} = x^2 + 3x + 3,$$

$3 \nmid 1, 3 \nmid 3, 3 \nmid 3, 3^2 \nmid 3$ と Eisenstein の判定法より, $\varphi_3(x+1)$ は \mathbb{Q} 上既約で, $\varphi_3(x)$ は \mathbb{Q} 上既約.

$$\varphi_p(x) = \frac{x^p - 1}{x - 1} \text{ より},$$

$$\varphi_p(x+1) = \frac{(x+1)^p - 1}{x} = \frac{\sum_{k=0}^p \binom{p}{k} x^k - 1}{x} = \sum_{k=1}^p \binom{p}{k} x^{k-1} = \binom{p}{p} x^{p-1} + \binom{p}{p-1} x^{p-2} + \dots + \binom{p}{2} x + \binom{p}{1}.$$

$$\binom{p}{p} = 1, \quad \binom{p}{p-1} = p, \quad \dots, \quad \binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!}, \quad \dots, \quad \binom{p}{2} = \frac{p(p-1)}{2}, \quad \binom{p}{1} = p.$$

$\underbrace{\qquad\qquad\qquad}_{1 \leq k \leq p-1}$

p で割り切れるが p^2 で割り切れない.

ゆえに, Eisenstein の判定法より, $\varphi_p(x+1)$ は \mathbb{Q} 上既約で, $\varphi_p(x)$ は \mathbb{Q} 上既約である. \square

注意 素数 p について、 $x^{p-1} + x^{p-2} + \cdots + x + 1$ は \mathbb{Q} 上既約になるが、

$m, n \in \mathbb{Z}, m, n \geq 2$ のとき、 $x^{mn-1} + x^{mn-2} + \cdots + x + 1$ は \mathbb{Q} 上既約でない。

なぜなら“

$$\begin{aligned} x^{mn-1} + x^{mn-2} + \cdots + x + 1 &= \frac{x^{mn}-1}{x-1} = \frac{x^m-1}{x-1} \cdot \frac{x^{mn}-1}{x^m-1} \\ &= (x^{m-1} + x^{m-2} + \cdots + x + 1) (x^{m(n-1)} + x^{m(n-2)} + \cdots + x^m + 1), \end{aligned}$$

たとえば

$$x^3 + x^2 + x + 1 = \frac{x^4 - 1}{x - 1} = \frac{x^2 - 1}{x - 1} \cdot \frac{x^4 - 1}{x^2 - 1} = (x+1)(x^2 + 1)$$

$$\begin{aligned} x^5 + x^4 + x^3 + x^2 + x + 1 &= \frac{x^2 - 1}{x - 1} \cdot \frac{x^6 - 1}{x^2 - 1} = (x+1)(x^4 + x^2 + 1) = (x+1)(x^2 + x + 1)(x^2 - x + 1) \\ &= \frac{x^3 - 1}{x - 1} \cdot \frac{x^6 - 1}{x^3 - 1} = (x^2 + x + 1)(x^3 + 1) = (x^2 + x + 1)(x+1)(x^2 - x + 1) \\ &\quad \downarrow \\ &\quad x^3 + 1 = (x+1)(x^2 - x + 1) \end{aligned}$$

$x^n - 1$ を割り切る \mathbb{Q} 上既約な多項式を 因分多項式 と呼ぶ。

□

問題 2-3

R は可換環であるとし, $p \in R$ があるとする.

$a \in R$ の R/pR での像を \bar{a} と書き, 写像 $\varphi: R[x] \rightarrow (R/pR)[x]$

$$\varphi\left(\sum_i a_i x^i\right) = \sum_i \bar{a}_i x^i \quad (a_i \in R)$$

と定める. 以下を示せ.

- (1) φ は環の準同型写像である.
- (2) φ は全射である.
- (3) $\text{Ker } \varphi = pR[x]$
- (4) 環の同型写像 $\bar{\varphi}: R[x]/pR[x] \xrightarrow{\sim} (R/pR)[x]$, $(f \bmod p) \mapsto \varphi(f)$ が得られる.

注意 $pR[x]$ も pR も (p) と書かれることがある. 分脈により, で区別せよ:

$$R[x]/(p) \xrightarrow{\sim} (R/(p))[x], (f \bmod p) \mapsto \varphi(f).$$

互いに異ることに注意

□

解答例

- (1) φ が加法と 1 と乗法を保つことを示せばよい.

任意に $f, g \in R[x]$ をとる. f, g は次のように表される:

$$f = \sum_i a_i x^i, \quad g = \sum_i b_i x^i, \quad a_i, b_i \in R,$$

有限和, 有限個で除いて $a_i = b_i = 0$.

つづく

このとき、

$$\begin{aligned}\varphi(f+g) &= \varphi\left(\sum_i (a_i + b_i)x^i\right) = \sum_i (\overline{a_i + b_i})x^i = \sum_i (\overline{a_i} + \overline{b_i})x^i \\ &= \sum_i \overline{a_i}x^i + \sum_i \overline{b_i}x^i = \varphi(f) + \varphi(g).\end{aligned}$$

$a \mapsto \overline{a}$ は環の準同型より。

$$\varphi(1) = \overline{1} = ((R/\mathfrak{p}R)[x] \text{ における乗法の単位元}).$$

$$\begin{aligned}\varphi(fg) &= \varphi\left(\sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k\right) = \sum_k \left(\overline{\sum_{i+j=k} a_i b_j}\right) x^k = \sum_k \left(\sum_{i+j=k} \overline{a_i} \overline{b_j}\right) x^k \\ &= \left(\sum_i \overline{a_i} x^i\right) \left(\sum_j \overline{b_j} x^j\right) = \varphi(f)\varphi(g).\end{aligned}$$

これで $\varphi: R[x] \rightarrow (R/\mathfrak{p}R)[x]$ が環の準同型であることが示された。

(2) φ が全射であることを示そう。

$F \in (R/\mathfrak{p}R)[x]$ を任意にとる。 $F = \sum_i d_i x^i$ (有限和), $d_i \in R/\mathfrak{p}R$ と書ける。

$R/\mathfrak{p}R$ の元はすべて \overline{a} , $a \in R$ の形をしているので, $d_i = \overline{a_i}$, $a_i \in R$ と書ける。
 $d_i = 0$ のとき, $a_i = 0$ とできるのでそろそろみてみよう。

そのとき, $f = \sum_i a_i x^i$ とし, $f \in R[x]$ を作れ, $\varphi(f) = \sum_i \overline{a_i} x^i = \sum_i d_i x^i = F$.

これで, φ の全射性を示せた。

(3) $\text{Ker } \varphi = pR[x]$ を示す.

$\text{Ker } \varphi \supset pR[x]$ を示す. 任意に $f \in pR[x]$ をとる $f = pg$, $g \in R[x]$ と書ける.

ゆえに, $\varphi(f) = \varphi(pg) = \varphi(p)\varphi(g) = \bar{p}\varphi(g) = \bar{0}\varphi(g) = \bar{0}$.

したがって, $f \in \text{Ker } \varphi$. $\bar{p} = \bar{0}$ in R/pR

これで, $\text{Ker } \varphi \supset pR[x]$ が示された.

$\text{Ker } \varphi \subset pR[x]$ を示す. 任意に $f \in \text{Ker } \varphi$ をとる. $\varphi(f) = \bar{0}$ が成立する.

$f = \sum_i a_i x^i$ と書ける. そのとき, $\varphi(f) = \sum_i \bar{a}_i x^i$.

これが $\bar{0}$ に等しいので, すべての i について, $\bar{a}_i = \bar{0}$ となる.

これは, $a_i \in pR$ と同値なので, $a_i = pb_i$, $b_i \in R$ と書ける.

ゆえに, $f = \sum_i pb_i x^i = p \sum_i b_i x^i \in pR[x]$.

これで, $\text{Ker } \varphi \subset pR[x]$ が示された.

以上によつて, $\text{Ker } \varphi = pR[x]$ が示された.

(4) 環の同型写像 $\bar{\varphi}: R[x]/pR[x] \xrightarrow{\sim} (R/pR)[x]$, $(f \bmod p) \mapsto \varphi(f)$ が得られる事を示す,

しかし、これは (1), (2), (3) に環の準同型定理を適用した結果に等しい,

環の準同型定理 環 A, B と環の準同型写像 $\varphi: A \rightarrow B$ について,

次の環の同型写像が得られる:

$$\begin{array}{ccc} \bar{\varphi}: A/\text{Ker } \varphi & \rightarrow & \text{Im } \varphi = \{ \varphi(x) \mid x \in A \} \\ \Downarrow & & \Downarrow \\ a + \text{Ker } \varphi & \longmapsto & \varphi(a). \end{array}$$

これを $A = R[x]$, $B = (R/pR)[x]$, φ を問題のものとすると, ほしい結果が得られる.

□

環の準同型定理の証明をきちんと理解しておくと,

他のことからも理解しやすくなる。

ここに基本がつまっている!

問題 2-4 $\omega^3 = 1$ と仮定し, $\alpha = \omega^3\sqrt[3]{7}$ とおき, 写像 $\varphi: \mathbb{Q}[x] \rightarrow \mathbb{Q}[\alpha]$ を
 $\varphi(f(x)) = f(\alpha) \quad (f \in \mathbb{Q}[x])$

と定める. 以下で $\mathbb{Q}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Q}[x]\}$ を用いて使ってよい. 以下を示せ.

- (1) φ は全射環準同型である. かつ $a \in \mathbb{Q}$ に対して $\varphi(a) = a$.
- (2) $f(x) = x^3 - 7$ は \mathbb{Q} 上の既約多項式である
- (3) $\text{Ker } \varphi = (x^3 - 7)\mathbb{Q}[x]$. これを $(x^3 - 7)$ と書く.
- (4) 環として, $\mathbb{Q}[x]/(x^3 - 7) \cong \mathbb{Q}[\alpha]$.
- (5) $\mathbb{Q}[\alpha]$ は体になる.

(補正: $\omega \in \mathbb{C}$)

解答例 (1) φ の定義より, $\varphi(a) = a$ ($a \in \mathbb{Q}$) は自明である.

$\mathbb{Q}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Q}[x]\}$ より, $\varphi: \mathbb{Q}[x] \rightarrow \mathbb{Q}[\alpha]$ が全射であることがわかる.

φ が環の準同型であること, すなわち, φ が加法と乗法の単位元と乗法を保つことを示そう.

$f, g \in \mathbb{Q}[x]$ を任意にとる. $f = \sum_i a_i x^i$, $g = \sum_i b_i x^i$, $a_i, b_i \in \mathbb{Q}$ と書け,

$$\varphi(f+g) = \varphi\left(\sum_i (a_i + b_i)x^i\right) = \sum_i (a_i + b_i)\alpha^i = \sum_i a_i \alpha^i + \sum_i b_i \alpha^i = \varphi(f) + \varphi(g),$$

$\varphi(1) = 1$ (自明).

$$\begin{aligned}\varphi(fg) &= \varphi\left(\sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) \alpha^k \\ &= \left(\sum_i a_i \alpha^i\right) \left(\sum_j b_j \alpha^j\right) = \varphi(f) \varphi(g).\end{aligned}$$

これで, φ が環の準同型であることも示された.

(2) $f(x) = x^3 - 7$ が \mathbb{Q} 上既約であることを示そう.

$7+1, 7|0, 7|0, 7|-7, 7^2|-7$ などの Eisenstein の判定法より, $f(x)$ は \mathbb{Q} 上既約である.

練習 $x^3 - 7$ が有理数係数の1次以上の2つの多項式の積に表されないことを高校生にもわかる方法で証明せよ. □

(3) $\text{Ker } \varphi = (x^3 - 7) \mathbb{Q}[x] (= (x^3 - 7))$ を示す.

$\text{Ker } \varphi \supset (x^3 - 7) \mathbb{Q}[x]$ を示す; $g \in (x^3 - 7) \mathbb{Q}[x]$ を任意にとる. $g(x) = (x^3 - 7)h(x)$, $h(x) \in \mathbb{Q}[x]$ と書け,
 $\varphi(g) = (x^3 - 7)h(x) = (7 - 7)h(x) = 0$. ($\alpha = \omega^{\frac{2}{3}}\sqrt[3]{7}$, $\omega^3 = 1$ より $\alpha^3 = 7$ となることを使った.)
 $g \in \text{Ker } \varphi$ を示せた. ゆえに, $\text{Ker } \varphi \supset (x^3 - 7) \mathbb{Q}[x]$ が示された.
 $\text{Ker } \varphi \subset (x^3 - 7) \mathbb{Q}[x]$ を示す; $g \in \text{Ker } \varphi$ を任意にとる. このとき, $g(\alpha) = 0$.

$\text{Ker } \varphi$ に含まれる 0 でない多項式で次数が最小でモニックなものの(最高次の
 係数が 1 のもの)が存在する. その 1 つを $f_0(x) \in \text{Ker } \varphi$ と書く.

$f(x) = x^3 - 7 \in \text{Ker } \varphi$ は $f(x) = f_0(x)q(x) + r(x)$, $q, r \in \mathbb{Q}[x]$, $\deg r < \deg f_0$
 と書ける. このとき, $0 = f(\alpha) = \underbrace{f_0(\alpha)}_{=0} q(\alpha) + r(\alpha) = r(\alpha) = \varphi(r)$ より, $r \in \text{Ker } \varphi$
 となり, f_0 は $\text{Ker } \varphi$ に含まれる 0 でない多項式の中で最低次のものなので,
 $r(x) = 0$ となり, $f(x) = f_0(x)q(x)$ となる. もとも $\deg f_0 < \deg f$ となると,
 f が \mathbb{Q} 上既約であることに反するので, $\deg f_0 = \deg f$ となり, $f_0 = f$ となる
 ことがわかる (f_0 をモニックにとっていることを使って)).

以上によつて、 $f(x) = x^3 - 7$ は $\text{Ker } \varphi$ に含まれる多項式の中で最低次のものになつてゐることがわかつた。
 ⇔ α を代入すると 0 になる

(注意 これは、 $f(\alpha) = 0$ と $f(x)$ が \mathbb{Q} 上既約であることの性を使って示されて
 いるが、もつこ一般の場合にも同様のことが言える。)

前ページの議論で任意にとってあつた $g \in \text{Ker } \varphi$ についてかえりかえり。

$$g(x) = f(x)q(x) + r(x), \quad q, r \in \mathbb{Q}[x], \quad \deg r < \deg f \text{ と書ける。}$$

$$\text{このとき, } 0 = \varphi(g) = \underbrace{f(\alpha)q(\alpha)}_{=0} + r(\alpha) = r(\alpha) = \varphi(r) \text{ となり, } r \in \text{Ker } \varphi \text{ となる。}$$

f は $\text{Ker } \varphi$ に含まれる 0 以外の多項式の中で最低次のものなので、 $r = 0$ 。

$$\text{したがつて, } g(x) = f(x)q(x) \in f(x)\mathbb{Q}[x] = (x^3 - 7)\mathbb{Q}[x].$$

これで、 $\text{Ker } \varphi \subset (x^3 - 7)\mathbb{Q}[x]$ も示された。

以上によつて、 $\text{Ker } \varphi = (x^3 - 7)\mathbb{Q}[x]$.

(注意 $g(\alpha) = 0$ をみたす 0 以外の $g \in \mathbb{Q}[x]$ の中で最低次(かつモニック)なものが
 を α の最小多項式と呼ぶ。)

(4) 環として, $\mathbb{Q}[x]/(x^3-7) \cong \mathbb{Q}[\alpha]$ という同型が得られることを示す.

$\varphi: \mathbb{Q}[x] \rightarrow \mathbb{Q}[\alpha]$, $f \mapsto f(\alpha)$ に環の準同型定理を使うと, φ が全射で
 $\text{Ker } \varphi = (x^3-7) (= (x^3-7)\mathbb{Q}[x])$ であることより, 環の同型写像

$$\bar{\varphi}: \mathbb{Q}[x]/(x^3-7) \xrightarrow{\sim} \mathbb{Q}[\alpha], \quad \underbrace{f + (x^3-7)}_{f \bmod x^3-7} \mapsto f(\alpha)$$

が得られる

$f \bmod x^3-7$ と書くことも多い.

(5) $\mathbb{Q}[\alpha]$ は体になることを示す.

(4) より, $\mathbb{Q}[x]/(x^3-7)$ が体になることを示せば十分である.

一般に PID の A と $0 \neq p \in A$ について,

p は A の既約元 $\Leftrightarrow (p) = pA$ は A の极大イデアル $\Leftrightarrow A/(p)$ は体.

そして, $f(x) = x^3 - 7$ は \mathbb{Q} 上の既約多項式なので, $\mathbb{Q}[x]$ の既約元であり,
 $\mathbb{Q}[x]/(x^3-7)$ は体になる

(注意 既約多項式は体を作るために使う!)

□

定義 K を \mathbb{C} の部分体とし, $\alpha \in \mathbb{C}$ とする.

α が K 上 作図可能 であるとは, K の元たちから出発して, 加減乗除と平方根を取る操作を有限回くりかじて α が得られることだ"と定める. \square

例 $\sqrt{2}$ や $\pm i = \pm \sqrt{-1}$ や $\sqrt{\frac{1+\sqrt{5}}{2}}$ は \mathbb{Q} 上作図可能である.

$\sqrt{\pi}$ は $\mathbb{Q}(\pi)$ 上作図可能である.

$a, b, c \in K$ のとき, $ax^2 + bx + c = 0$ の解は K 上作図可能である \square

正の整数 n に対して, $\zeta_n = e^{2\pi i/n}$ とおく.

問題 3-1 ζ_5 が \mathbb{Q} 上作図可能なことを示せ. \square

ヒント $w = \zeta_5$ とおく. 2次方程式の解と係数の関係を使う.

$$\alpha = w + w^4, \beta = w^2 + w^3 \text{ とおくと, } \alpha + \beta = ?, \alpha \beta = ?.$$

$$w + w^4 = \alpha, w \cdot w^4 = 1.$$

\square

注意 本質的に正五角形の作図可能性! \square

問題 3-2

ζ_{17} が \mathbb{Q} 上作図可能をこと示せ. $\square \leftarrow$ かなり非自明.

（これに関連した問題をすっと後にレポート課題に出す予定）

ヒント

$\omega = \zeta_{17}, \omega_0 = \omega, \omega_{k+1} = \omega_k^3$ とおく. $\begin{cases} \omega^{17} = 1, \omega \neq 1 \\ \omega^{16} + \omega^{15} + \dots + \omega + 1 = 0 \end{cases}$

$$(0) \quad \{\omega_0, \omega_1, \dots, \omega_{15}\} = \{\omega, \omega^2, \dots, \omega^{16}\}$$

$$(1) \quad d_0 = \omega_0 + \omega_2 + \dots + \omega_{14}, \quad d_1 = \omega_1 + \omega_3 + \dots + \omega_{15} \text{ とおくと,}$$

$$d_0 + d_1 = ?, \quad d_0 d_1 = ?$$

$$(2) \quad \beta_i = \omega_i + \omega_{i+4} + \omega_{i+8} + \omega_{i+12} \quad (i=0, 1, 2, 3) \text{ とおくと,}$$

$$\beta_0 + \beta_2 = d_0, \quad \beta_1 + \beta_3 = d_1, \quad \beta_0 \beta_2 = ?, \quad \beta_1 \beta_3 = ?, \quad (\beta_0 + 1) \beta_1 = \beta_0 - 1$$

$$(3) \quad \gamma_i = \omega_i + \omega_{i+8} \quad (i=0, 1, \dots, 7) \text{ とおくと,}$$

$$\gamma_0 + \gamma_4 = \beta_0, \quad \gamma_0 \gamma_4 = ?$$

$$(4) \quad \omega_0 + \omega_8 = \gamma_0, \quad \omega_0 \omega_8 = ?$$

\square

注意

本質的に正17角形の作図可能性! Carl Friedrich Gauss が発見. \square

問題 3-3

$$\frac{1}{1+\sqrt{2}+\sqrt{3}+2\sqrt{6}}$$
 の分母を有理化せよ. \square

ヒント

$$\sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3} \quad \square$$

問題 3-4

$a, b \in \mathbb{Q}$, $a \neq b$ と仮定する. $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$ を示せ.

ここで, $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ は $\mathbb{Q}, \sqrt{a}, \sqrt{b}$ を含む \mathbb{C} の部分体で最小のものを表す. \square

問題 3-5

$$\alpha = \omega \sqrt[3]{7}, \quad \omega = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2}$$
 とおく.

(1) $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ を求めよ.

(2) $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)]$ を求めよ.

(3) $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]$ を求めよ.

L が体 K の拡大体のとき,
 $[L : K] = [L/K] = \dim_K L$
 と書き,これを L/K の 拡大次数
 と呼ぶ.

\square

ヒント

α の \mathbb{Q} 上での最小多項式は $x^3 - 7$ になる, $\omega \notin \mathbb{Q}(\alpha)$. \square

定義

K を \mathbb{C} の部分体とし, $\alpha \in \mathbb{C}$ とする.

04-1

α が K 上作図可能であるとは, K の元たちから出発して, 加減乗除と平方根を取る操作を有限回くりかじて α が得られることだ"と定める. \square

例 $\sqrt{2}$ や $\pm i = \pm \sqrt{-1}$ や $\sqrt{\frac{1+\sqrt{5}}{2}}$ は \mathbb{Q} 上作図可能である.

$\sqrt{\pi}$ は $\mathbb{Q}(\pi)$ 上作図可能である.

$a, b, c \in K$ のとき, $ax^2 + bx + c = 0$ の解は K 上作図可能である \square

正の整数 n に対して, $\zeta_n = e^{2\pi i/n}$ とおく. 1の原始n乗根の1つ

問題 3-1 ζ_5 が \mathbb{Q} 上作図可能なことを示せ. \square

ヒント $w = \zeta_5$ とおく. 2次方程式の解と係数の関係を使う.

$$\alpha = w + w^4, \beta = w^3 + w^2 \text{ とおくと, } \alpha + \beta = ?, \alpha \beta = ?.$$

$$w + w^4 = \alpha, w \cdot w^4 = 1.$$

\square

注意 本質的に正五角形の作図可能性! \square

注意 $w = \zeta_5 \neq 1$ かつ $w^5 - 1 = (w-1)(w^4 + w^3 + w^2 + w + 1) = 0$ より, $w^4 + w^3 + w^2 + w + 1 = 0$.

問題 2-2(4) の結果より, $x^4 + x^3 + x^2 + x + 1$ は \mathbb{Q} 上既約な多項式である.

問題 3-1 は本質的に「加減乗除と平方根のみを使って方程式 $x^4 + x^3 + x^2 + x + 1 = 0$ を解け」という問題とみなされる. \square

問題3-1 解答例 $w = \zeta_5 = e^{2\pi i/5}$ とおく。 $w^5 = 1$, $w \neq 1$ である。

条件 $w^4 + w^3 + w^2 + w + 1 = 0$, $\operatorname{Re} w > 0$, $\operatorname{Im} w > 0$ で w は一意に唯一付けられる。

1) $\alpha = w + w^4$, $\beta = w^2 + w^3$ とおく。このとき, $\alpha + \beta = -1$ かつ

$$\alpha\beta = (w + w^4)(w^2 + w^3) \stackrel{w^5=1}{=} w^3 + w^4 + w + w^2 = -1. \quad \text{ゆえに, } \alpha \text{ と } \beta \text{ は}$$

方程式 $\lambda^2 + \lambda - 1 = 0$ の解である。 $\alpha = w + w^4 = w + \bar{w} \in \mathbb{R}_{>0}$ なので,

$$\alpha = \frac{-1 + \sqrt{5}}{2}. \quad \text{ゆえに, } \beta = \frac{-1 - \sqrt{5}}{2}, \quad \left(\alpha^2 = \frac{3 - \sqrt{5}}{2}, \quad \alpha^2 - 4 = -\frac{5 + \sqrt{5}}{2} \right)$$

2) $w + w^4 = \alpha$ と $w \cdot w^4 = 1$ より, w と w^4 は方程式 $\mu^2 - \alpha\mu + 1 = 0$ の解である。 $\operatorname{Im} w > 0$ より, $w = \frac{\alpha + \sqrt{\alpha^2 - 4}}{2} = \frac{\alpha + \sqrt{4 - \alpha^2}i}{2}$.

これで, w は有理数から出発して, 加減乗除と平方根をとる操作を有限回くりかえすことによって得られることがわかった。つまり, w は作図可能である。□

注意 以上の方針はそのまま 3-2 の場合(問題3-2)にも使える。□

追記

問題3-1は本質的に

4次方程式 $x^4 + x^3 + x^2 + x + 1 = 0$ を 2次方程式たちに帰着して解け
という問題に等しい。これを以下のようにして解くこともできる。

「 $x^4 + x^3 + x^2 + x + 1 = 0$ 」は 「 $x \neq 0$ かつ $x^2 + x + 1 + x^{-1} + x^{-2} = 0$ 」と同値である。
以下、 $x \neq 0$ と仮定する。

$y = x + x^{-1}$ とおくと、 $y^2 = x^2 + 2 + x^{-2}$ なので、

$x^2 + x + 1 + x^{-1} + x^{-2} = 0$ は $y^2 + y - 1 = 0$ と同値である。

$y = x + x^{-1}$ は $x^2 - yx + 1 = 0$ と同値である。

以上より、 $x^4 + x^3 + x^2 + x + 1 = 0$ の解法は、連立方程式

$$\begin{cases} y^2 + y - 1 = 0 & \cdots \textcircled{1} \\ x^2 - yx + 1 = 0 & \cdots \textcircled{2} \end{cases}$$

の解法に帰着できることがわかる。

①の解の全体は、 $y = \frac{-1 \pm \sqrt{5}}{2}$.

$$y^2 + y - 1 \downarrow \\ y^2 - 4 = -(y+3) = -\frac{5 \pm \sqrt{5}}{2}$$

y が与えられたときの②の解の全体は、 $x = \frac{y \pm \sqrt{y^2 - 4}}{2}$.

□

問題 3-2

ζ_{17} が \mathbb{Q} 上作図可能なことを示せ. $\square \leftarrow$ かなり非自明.

（これに関連した問題を「」と後にレポート課題に出す予定）

解答例 $\omega = \zeta_{17} = e^{2\pi i/17}$ とおく. このとき, $\omega^{17} = 1$, $\omega \neq 1$, $1 + \omega + \omega^2 + \dots + \omega^{16} = 0$. ※

$\omega_0 = \omega$, $\omega_{k+1} = \omega_k^3$ ($k = 0, 1, \dots, 15$) とおく. これらを計算すると,

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ω_k	ω	ω^3	ω^9	ω^{10}	ω^{13}	ω^5	ω^{15}	ω^{11}	ω^{16}	ω^{14}	ω^8	ω^7	ω^4	ω^{12}	ω^2	ω^6	ω

つまり, $\{\omega_0, \omega_1, \dots, \omega_{15}\} = \{\omega, \omega^2, \dots, \omega^{16}\} = \{z \in \mathbb{C} \mid 1 + z + z^2 + \dots + z^{16} = 0\}$.

□ $d_0 = \sum_{i=0}^7 \omega_{2i}$, $d_1 = \sum_{i=0}^7 \omega_{2i+1}$ とおく. $d_0 + d_1 \stackrel{*}{=} -1$ もかつ

$$d_0 d_1 = (8 \times 8 = 64 \text{ 項を整理する}) = 4 \sum_{k=1}^{16} \omega^k \stackrel{*}{=} -4.$$

つまり, d_0, d_1 は方程式 $K^2 + K - 4 = 0$ の解になる.

2 $\beta_{\bar{i}} = \sum_{j=0}^3 \omega_{4j+\bar{i}}$ ($\bar{i}=0,1,2,3$) とおく, $\beta_0 + \beta_2 = \alpha_0$, $\beta_1 + \beta_3 = \alpha_1$ かつ

$$\beta_0 \beta_2 = (4 \times 4 = 16 \text{ 項}) = \sum_{k=1}^{16} \omega^k \stackrel{*}{=} -1, \quad \beta_1 \beta_3 = (4 \times 4 = 16 \text{ 項}) = \sum_{k=1}^{16} \omega^k = -1.$$

ゆえに, β_0, β_2 は $\lambda^2 - \alpha_0 \lambda - 1 = 0$ の解であり, β_1, β_3 は $\lambda^2 - \alpha_1 \lambda - 1 = 0$ の解になる.

3 $\gamma_{\bar{i}} = \omega_{\bar{i}} + \omega_{\bar{i}+8}$ ($\bar{i}=0,1,\dots,7$) とおく, $\gamma_{\bar{i}} + \gamma_{\bar{i}+4} = \beta_{\bar{i}}$ ($\bar{i}=0,1,2,3$) かつ

$$\gamma_{\bar{i}} \gamma_{\bar{i}+4} = \beta_{\bar{i}+1} \quad (\bar{i}=0,1,2,3 \quad \beta_4 = \beta_0 \text{ とおく}), \quad \text{たとえば},$$

$$\begin{aligned} \gamma_0 \gamma_4 &= (\omega_0 + \omega_8)(\omega_4 + \omega_{12}) = (\omega + \omega^{16})(\omega^{13} + \omega^4) = \omega^{14} + \omega^5 + \omega^{12} + \omega^3 \\ &= \omega_9 + \omega_5 + \omega_{13} + \omega_1 = \beta_1 \end{aligned}$$

ゆえに, $\gamma_{\bar{i}}, \gamma_{\bar{i}+4}$ は $\mu^2 - \beta_{\bar{i}} \mu + \beta_{\bar{i}+1} = 0$ の解になる.

4 $\omega_{\bar{i}} + \omega_{\bar{i}+8} = \gamma_{\bar{i}}$ かつ $\omega_{\bar{i}} \omega_{\bar{i}+8} = 1$ ($\bar{i}=0,1,\dots,7$).

$$\text{たとえば} \quad \omega_0 \omega_8 = \omega \cdot \omega^{16} = \omega^{17} = 1.$$

ゆえに, $\omega_{\bar{i}}, \omega_{\bar{i}+8}$ は $v^2 - \gamma_{\bar{i}} v + 1 = 0$ の解になる.

以上によつて, $\omega_0 = \omega$ を含む $\omega_{\bar{i}}$ の全体が 有理数から出発して 四則演算と
二次方程式を解くことの有限回のくりかえして作られることがわかった.

特に ω は作図可能である,

□

注意 $\sigma(\omega) = \omega^3$, $\sigma(a) = a$ ($a \in \mathbb{Q}$) をみたす体 $L = \mathbb{Q}(\omega)$ の自己同型 σ が存在することを示せる. (ヒント: $\mathbb{Q}(\omega^k) \cong \mathbb{Q}[x]/(1+x+\dots+x^{16})$, $k=1, 2, \dots, 16$)
このとき, $\{\sigma^k(\omega) \mid k=0, 1, \dots, 15\} = \{\omega^k \mid k=1, 2, \dots, 16\} = \{z \in \mathbb{C} \mid 1+z+\dots+z^{16}=0\}$ で
この集合は $\mathbb{Q}(\omega)$ の \mathbb{Q} 上で"の基底になる ($1+x+\dots+x^{16}$ の \mathbb{Q} 上で"の既約性より)).

このことを使うと, 前ページまでの計算を簡略化できる.

たとえば, $\omega_k = \sigma^k(\omega)$, $d_k = \sum_{\lambda=0}^7 \sigma^{2\lambda+k}(\omega)$, $\sigma(d_k) = d_{k+1}$, $d_{k+2} = d_k$ より),
特に, $\sigma(d_0 d_1) = \sigma(d_0) \sigma(d_1) = d_1 d_0 = d_0 d_1$ と σ の作用で" $d_0 d_1$ は不变になる.
 $d_0 d_1$ は ω のべきたるの $8^2 = 64$ 個の和になるので"

$$d_0 d_1 = \sum_{k=0}^{15} c_k \sigma^k(\omega), \quad c_k \in \mathbb{Z}_{\geq 0}, \quad \sum_{k=0}^{15} c_k = 64$$

と表わされる. $\sigma^k(\omega)$ ($k=0, 1, \dots, 15$) は \mathbb{Q} 上で"独立で", $\sigma(d_0 d_1) = d_0 d_1$ より,
 c_k たちは互いに等しいことがわかる. したがって, $c_k = 4$, すなはち,

$$d_0 d_1 = 4 \sum_{k=0}^{15} \sigma^k(\omega) = 4 \sum_{l=1}^{16} \omega^l = -4.$$

しかし, エレガントでない素朴な方法で" $d_0 d_1 = -4$ を示す経験も重要である. \square

追記 $\beta_k = \sum_{i=0}^3 \sigma^{4i+k}(\omega)$, $\sigma(\beta_k) = \beta_{k+1}$, $\beta_{k+4} = \beta_k$ より, $\sigma^2(\beta_k \beta_{k+2}) = \beta_k \beta_{k+2}$.

$\beta_0 \beta_2$ は $4^2 = 16$ 個の $\omega_\ell = \sigma^\ell(\omega)$ の和になります, σ^2 の作用で不变で, 項として, $\omega_0 \omega_2 = \omega_3$ と $\omega_0 \omega_6 = \omega_8$ を含むので, $\beta_0 \beta_2 = \sum_{\ell=0}^{15} \omega_\ell = -1$.

これの両辺に σ^k を作用させると, $\beta_k \beta_{k+2} = -1$.

$$\gamma_k = \sum_{i=0}^1 \sigma^{8i+k}(\omega), \quad \sigma(\gamma_k) = \gamma_{k+1}, \quad \gamma_{k+8} = \gamma_k \text{ より}, \quad \sigma^4(\gamma_k \gamma_{k+4}) = \gamma_k \gamma_{k+4}.$$

$$\begin{aligned} \gamma_0 \gamma_4 &= (\omega_0 + \omega_8)(\omega_4 + \omega_{12}) = (\omega + \omega^{16})(\omega^{13} + \omega^4) = \omega^{14} + \omega^5 + \omega^{12} + \omega^3 \\ &= \omega_9 + \omega_5 + \omega_{13} + \omega_1 = \beta_1 \end{aligned}$$

これに, σ^k を作用させると, $\gamma_k \gamma_{k+4} = \beta_{k+1}$.

$$\omega_0 \omega_8 = \omega \cdot \omega^{16} = \omega^{17} = 1. \quad \text{これに } \sigma^k \text{ を作用させると, } \omega_k \omega_{k+8} = 1.$$

以上によって, 前々ページまでで略した計算がすべて埋めた. \square

以上を見すぎてしまう前に自分で計算することを準備してほしいです!
特に数学を教える仕事に興味がある人は色々計算してみてください!
数学の研究でも素朴な計算が重要である!

問題 3-3

$$\frac{1}{1+\sqrt{2}+\sqrt{3}+2\sqrt{6}}$$
 の分母を有理化せよ. \square

解答例 分子分母に $(1-\sqrt{2}+\sqrt{3}-2\sqrt{6})(1+\sqrt{2}-\sqrt{3}-2\sqrt{6})(1-\sqrt{2}-\sqrt{3}+2\sqrt{6})$ をかけて、かんはって計算すると分母が有理化される.

$$(1+\sqrt{2}+\sqrt{3}+2\sqrt{6})(1-\sqrt{2}+\sqrt{3}-2\sqrt{6})(1+\sqrt{2}-\sqrt{3}-2\sqrt{6})(1-\sqrt{2}-\sqrt{3}+2\sqrt{6}) = 376$$

$$(1-\sqrt{2}+\sqrt{3}-2\sqrt{6})(1+\sqrt{2}-\sqrt{3}-2\sqrt{6})(1-\sqrt{2}-\sqrt{3}+2\sqrt{6}) = -4 - 14\sqrt{2} - 16\sqrt{3} + 38\sqrt{6}.$$

$$\therefore \frac{1}{1+\sqrt{2}+\sqrt{3}+2\sqrt{6}} = \frac{-4-14\sqrt{2}-16\sqrt{3}+38\sqrt{6}}{376} = -\frac{1}{94} - \frac{7}{188}\sqrt{2} - \frac{2}{47}\sqrt{3} + \frac{19}{188}\sqrt{6}. \quad \square$$

考え方

$1+\sqrt{2}+\sqrt{3}+2\sqrt{6} = 1+\sqrt{2}+\sqrt{3}+2\sqrt{2}\sqrt{3}$ の $\sqrt{2}, \sqrt{3}$ を $\pm\sqrt{2}, \pm\sqrt{3}$ に書きかえて得られる 4つの数をかけあわせると有理数（この場合は整数）になる。このような観察が Galois 理論に至る道になつていく。

 \square

注意

一般に

$$\begin{aligned}
 & (a+b\sqrt{m}+c\sqrt{n}+d\sqrt{mn})(a-b\sqrt{m}+c\sqrt{n}-d\sqrt{mn}) \\
 &= (a+c\sqrt{n})^2 - m(b+d\sqrt{n})^2 \\
 &= \underbrace{a^2 - mb^2 + nc^2 - mnd^2}_{=: A} + \underbrace{2(ac - mbd)\sqrt{n}}_{=: B}.
 \end{aligned}$$

$$(A+B\sqrt{n})(A-B\sqrt{n}) = A^2 - nB^2.$$

以上の計算より, $a, b, c, d, m, n \in \mathbb{Q}$ のとき,

$a+b\sqrt{m}+c\sqrt{n}+d\sqrt{mn}$ の中の \sqrt{m}, \sqrt{n} をそれぞれ $\pm\sqrt{m}, \pm\sqrt{n}$ で置きかえてできる4つの数をかけあわせると有理数になることわかる, \square

注意

$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ の体の自己同型 σ, τ で

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

とめたものが一意に存在する. このような σ, τ をうまく利用すること
が Galois 理論になつている, \square

問題 3-4 $a, b \in \mathbb{Q}$, $a \neq b$ と仮定する. $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$ を示せ.

ここで, $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ は $\mathbb{Q}, \sqrt{a}, \sqrt{b}$ を含む \mathbb{C} の部分体で最小のものを表す. \square

解答例

① $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \supset \mathbb{Q}(\sqrt{a} + \sqrt{b})$ を示そう. $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ は \mathbb{Q} と $\sqrt{a} + \sqrt{b}$ を含む.

$\mathbb{Q}(\sqrt{a} + \sqrt{b})$ は \mathbb{Q} と $\sqrt{a} + \sqrt{b}$ を含む \mathbb{C} の最小の部分体なので, $\mathbb{Q}(\sqrt{a} + \sqrt{b}) \subset \mathbb{Q}(\sqrt{a}, \sqrt{b})$.

② $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \subset \mathbb{Q}(\sqrt{a} + \sqrt{b})$ を示そう. $a \neq b$ より $\sqrt{a} \neq \pm \sqrt{b}$, 特に $\sqrt{a} + \sqrt{b} \neq 0$ なので,

$$\mathbb{Q}(\sqrt{a} + \sqrt{b}) \ni \frac{a - b}{\sqrt{a} + \sqrt{b}} = \sqrt{a} - \sqrt{b},$$

$$\mathbb{Q}(\sqrt{a} + \sqrt{b}) \ni \frac{(\sqrt{a} + \sqrt{b}) + (\sqrt{a} - \sqrt{b})}{2} = \sqrt{a}, \quad \left. \begin{array}{l} \mathbb{Q}(\sqrt{a} + \sqrt{b}) \text{ は } \mathbb{Q} \text{ と} \\ \sqrt{a}, \sqrt{b} \text{ を含む.} \end{array} \right\}$$

$$\mathbb{Q}(\sqrt{a} + \sqrt{b}) \ni \frac{(\sqrt{a} + \sqrt{b}) - (\sqrt{a} - \sqrt{b})}{2} = \sqrt{b}.$$

$\mathbb{Q}(\sqrt{a}, \sqrt{b})$ は $\mathbb{Q}, \sqrt{a}, \sqrt{b}$ を含む \mathbb{C} の最小の部分体なので, $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \subset \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

以上により, $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$ が示された. \square

問題 3-5

$$\alpha = \omega^3\sqrt[3]{7}, \quad \omega = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2} \text{ とおく.}$$

(1) $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ を求めよ.(2) $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)]$ を求めよ.(3) $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]$ を求めよ.

L が体 K の拡大体のとき,

$$[L : K] = [L/K] = \dim_K L$$

と書き, これを L/K の 拡大次数 と呼ぶ.

□

ヒント α の \mathbb{Q} 上での最小多項式は $x^3 - 7$ になる, $\omega \notin \mathbb{Q}(\alpha)$. □

解答例 (1) $\alpha = \omega^3\sqrt[3]{7}$ は $x^3 - 7 = 0$ の解だから, $x^3 - 7$ は \mathbb{Q} 上既約なので,

$x^3 - 7$ は α の \mathbb{Q} 上での最小多項式になる (問題 2-4 の解答例を見よ).

ゆえに, 体の同型 $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(x^3 - 7)$ ($f(\alpha) \leftrightarrow \bar{f(x)} = (f(x) \bmod x^3 - 7)$) を得る.

$\mathbb{Q}[x]/(x^3 - 7)$ の \mathbb{Q} 上のベクトル空間としての基底として, $1, x, x^2$ の像をとれる.

特に, $\dim_{\mathbb{Q}} \mathbb{Q}[x]/(x^3 - 7) = 3$. ゆえに, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = 3$.

$\mathbb{Q}[x]/(x^3 - 7)$ の中で $\bar{x}^3 = 7$ なので \bar{x} の 3 乗以上の項は
 \bar{x} の 2 乗以下の項の和で書ける.

(2) $w \notin \mathbb{Q}(\alpha)$ であることを示そう、(1) と同様にして、 $\mathbb{Q}(\sqrt[3]{7}) \cong \mathbb{Q}[x]/(x^3 - 7)$ なので、
 $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt[3]{7})$ となる。もしも $w \in \mathbb{Q}(\alpha)$ ならば $\mathbb{Q}(\sqrt[3]{7})$ も 1 の原始 3 乗根を
 含むことになり、矛盾する。ゆえに、 $w \notin \mathbb{Q}(\alpha)$ である。
 (注) $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt[3]{7})$

ゆえに、 $\mathbb{Q}(\alpha, w) = \mathbb{Q}(\alpha)(w) \supsetneq \mathbb{Q}(\alpha)$ 。すなわち $[\mathbb{Q}(\alpha, w) : \mathbb{Q}(\alpha)] > 1$.

w は $x^2 + x + 1 = 0$ の解になっているので、 $[\mathbb{Q}(\alpha, w) : \mathbb{Q}(\alpha)] \leq 2$.

したがって、 $[\mathbb{Q}(\alpha, w) : \mathbb{Q}(\alpha)] = 2$.
 $w^2 = -w - 1$ なので w の 2 乗以上 の 項は
 w の 1 乗以下の 項の \mathbb{Q} 上での一次結合で書ける。

(3) $[\mathbb{Q}(\alpha, w) : \mathbb{Q}] = [\mathbb{Q}(\alpha, w) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6$. □

注意 以上の議論を見直せば、

$\mathbb{Q}(\alpha, w)$ の $\mathbb{Q}(\alpha)$ 上のベクトル空間としての基底として $1, w$ がとれ、

$\mathbb{Q}(\alpha)$ の \mathbb{Q} 上のベクトル空間の基底として $1, \alpha, \alpha^2$ がとれ、

$\mathbb{Q}(\alpha, w)$ の \mathbb{Q} 上のベクトル空間の基底として、 $1, \alpha, \alpha^2, w, w\alpha, w\alpha^2$ がとれる
 ことわかる。□

以上で出てきた拡大体の例のまとめ

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ (問題1-2, 問題1-3)

- $\sqrt{2}$ の \mathbb{Q} 上での最小多項式は $x^2 - 2$: $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$,
- $\mathbb{Q}(\sqrt{2})$ は $x^2 - 2 = 0$ の 2つの解 $\pm\sqrt{2}$ を含む: $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$,
- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2}$.
- 体の自己同型 σ : $\mathbb{Q}(\sqrt{2}) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2})$ で $\sigma(\sqrt{2}) = -\sqrt{2}$ をめたすものが唯一つ存在する,
 $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ ($a, b \in \mathbb{Q}$). □

注意 $x^2 - 2x - 1 = 0$ の解は $x = 1 \pm \sqrt{2}$.

$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1 + \sqrt{2}) = \mathbb{Q}(1 - \sqrt{2}) = \mathbb{Q}(1 + \sqrt{2}, 1 - \sqrt{2})$ であることに注意せよ.

体 \mathbb{Q} 係数の 2 次方程式の解の 1 つを付け加えてできる体は $\mathbb{Q}(\sqrt{a})$, $a \in \mathbb{Q}$ の形になり, その 2 次方程式の解をすべて言む. □

$\mathbb{Q}(\omega^k \sqrt[3]{7}) / \mathbb{Q}$ ($k=0,1,2$, $\omega = e^{2\pi i/3}$) (問題3-5)

- $\omega^k \sqrt[3]{7}$ の \mathbb{Q} 上での最小多項式は $x^3 - 7$: $\mathbb{Q}(\omega^k \sqrt[3]{7}) \cong \mathbb{Q}[x]/(x^3 - 7)$, $f(\omega^k \sqrt[3]{7}) \leftrightarrow \overline{f(x)}$
- $\omega, \omega^2 \notin \mathbb{Q}(\omega^k \sqrt[3]{7})$ ($\because \mathbb{Q}(\omega^k \sqrt[3]{7}) \cong \mathbb{Q}[x]/(x^3 - 7) \cong \mathbb{Q}(\sqrt[3]{7}) \oplus \mathbb{Q}\omega, \mathbb{Q}\omega^2$)
- $\mathbb{Q}(\omega^k \sqrt[3]{7})$ は $x^3 - 7 = 0$ の 3 つの解 $\sqrt[3]{7}, \omega \sqrt[3]{7}, \omega^2 \sqrt[3]{7}$ のうち 1 つだけしか含まない。
たとえば $\mathbb{Q}(\sqrt[3]{7}, \omega^2 \sqrt[3]{7}) \ni \frac{\omega^2 \sqrt[3]{7}}{\sqrt[3]{7}} = \omega^2$ やから $\mathbb{Q}(\sqrt[3]{7}, \omega^2 \sqrt[3]{7}) \ni (\omega^2)^3 = \omega$
であることから, $\mathbb{Q}(\sqrt[3]{7}, \omega^2 \sqrt[3]{7}) = \mathbb{Q}(\sqrt[3]{7}, \omega) \neq \mathbb{Q}(\sqrt[3]{7}), \mathbb{Q}(\omega^2 \sqrt[3]{7})$ であることがわかる。(問題3-4と同様の方法を使う。)
- $\alpha = \omega^k \sqrt[3]{7}$ とおくと, $\mathbb{Q}(\omega^k \sqrt[3]{7}) = \mathbb{Q}(\alpha) \cong \mathbb{Q}1 \oplus \mathbb{Q}\alpha \oplus \mathbb{Q}\alpha^2$.
- $[\mathbb{Q}(\omega^k \sqrt[3]{7}) : \mathbb{Q}] = 3$
- $\sqrt[3]{7}$ を $\omega^k \sqrt[3]{7}$ にうつす $\mathbb{Q}(\sqrt[3]{7})$ の体の自己同型は存在しない。
- $k, l = 0, 1, 2$ のとき, $\omega^k \sqrt[3]{7}$ を $\omega^l \sqrt[3]{7}$ にうつす体の同型

$\sigma_{kl} : \mathbb{Q}(\omega^k \sqrt[3]{7}) \xrightarrow{\sim} \mathbb{Q}(\omega^l \sqrt[3]{7})$ が存在する, \leftarrow

$$\begin{aligned} \mathbb{Q}(\omega^k \sqrt[3]{7}) &\cong \mathbb{Q}[x]/(x^3 - 7) \cong \mathbb{Q}(\omega^l \sqrt[3]{7}) \\ f(\omega^k \sqrt[3]{7}) &\leftrightarrow \overline{f(x)} \longleftrightarrow f(\omega^l \sqrt[3]{7}) \end{aligned}$$

$$\mathbb{Q}(\omega^k \sqrt[3]{7}, \omega) / \mathbb{Q}(\omega^k \sqrt[3]{7}) \quad (k=0,1,2, \omega = e^{2\pi i/3}) \quad (\text{問題 3-5})$$

- $\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2}$ の $\mathbb{Q}(\omega^k \sqrt[3]{7})$ 上での最小多項式は $x^2 + x + 1$.
- $\mathbb{Q}(\omega^k \sqrt[3]{7}, \omega) \cong \mathbb{Q}(\omega^k \sqrt[3]{7})1 \oplus \mathbb{Q}(\omega^k \sqrt[3]{7})\omega$, $[\mathbb{Q}(\omega^k \sqrt[3]{7}, \omega) : \mathbb{Q}(\omega^k \sqrt[3]{7})] = 2$.
- $\mathbb{Q}(\sqrt[3]{7}, \omega) = \mathbb{Q}(\omega \sqrt[3]{7}, \omega) = \mathbb{Q}(\omega^2 \sqrt[3]{7}, \omega) = \mathbb{Q}(\sqrt[3]{7}, \omega \sqrt[3]{7}, \omega^2 \sqrt[3]{7}) \leftarrow \begin{array}{l} (x^3 - 7 \text{ の解を}) \\ \text{すべて含む。} \end{array}$
- $\bar{\omega} = \omega^2$ なので、複素共役とする操作は体 $\mathbb{Q}(\sqrt[3]{7}, \omega)$ の自己同型を定める.

$$\mathbb{Q}(\sqrt[3]{7}, \omega) / \mathbb{Q} \quad (\omega = e^{2\pi i/3}) \quad (\text{問題 3-5})$$

↑ 新主張

- $[\mathbb{Q}(\sqrt[3]{7}, \omega) : \mathbb{Q}] = 6$.
- $\mathbb{Q}(\sqrt[3]{7}, \omega)$ の \mathbb{Q} 上のベクトル空間としての基底として,
 $1, \sqrt[3]{7}, (\sqrt[3]{7})^2, \omega, \omega \sqrt[3]{7}, \omega (\sqrt[3]{7})^2$ がとれる.
- $\mathbb{Q}(\sqrt[3]{7}, \omega) = \mathbb{Q}(\sqrt[3]{7}, \omega \sqrt[3]{7}, \omega^2 \sqrt[3]{7})$.
 すなわち, $\mathbb{Q}(\sqrt[3]{7}, \omega)$ は $x^3 - 7 = 0$ のすべての解を \mathbb{Q} に付け加えて
できる体に等しい. ↑ $\mathbb{Q}(\sqrt[3]{7}, \omega)$ は \mathbb{Q} 上の方程式 $x^3 - 7 = 0$ に
 対応する \mathbb{Q} の Galois 扩大になっている

$\boxed{\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}}$ (問題 3-3, 3-4)

- $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{6}$, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
- $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
 $\sqrt{6} = \sqrt{2}\sqrt{3}$
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の体の自己同型 σ, τ "

$$\sigma(a) = a \quad (a \in \mathbb{Q}), \quad \sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}$$

$$\tau(a) = a \quad (a \in \mathbb{Q}), \quad \tau(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt{3}) = -\sqrt{3}$$

とみたすものが唯一つ存在する。

問題 4-1 を解け。

$$\boxed{\mathbb{Q}(\zeta_5)/\mathbb{Q}, \zeta_5 = e^{2\pi i/5}} \quad (\text{問題 3-1})$$

- $k=1, 2, 3, 4$ について ζ_5^k の \mathbb{Q} 上での最小多項式は $x^4 + x^3 + x^2 + x + 1 = 0$.
- $k=1, 2, 3, 4$ について $\mathbb{Q}(\zeta_5^k) = \mathbb{Q}(\zeta_5)$.
- $\mathbb{Q}(\zeta_5) \cong \mathbb{Q}[1] \oplus \mathbb{Q}\zeta_5 \oplus \mathbb{Q}\zeta_5^2 \oplus \mathbb{Q}\zeta_5^3$, $[\mathbb{Q}(\zeta_5):\mathbb{Q}] = 4$.
- $k=1, 2, 3, 4$ について, $\mathbb{Q}(\zeta_5^k) \cong \mathbb{Q}[x]/(x^4 + x^3 + x^2 + x + 1)$.
- $\mathbb{Q}(\zeta_5) = \mathbb{Q}\left(\sqrt[4]{5}, \sqrt{-\frac{5+\sqrt{5}}{2}}\right)$

$$\boxed{\mathbb{Q}(\zeta_{17})/\mathbb{Q}, \zeta_{17} = e^{2\pi i/17}} \quad (\text{問題 3-2})$$

- $k=1, 2, \dots, 16$ について, ζ_{17}^k の \mathbb{Q} 上での最小多項式は $x^{16} + x^{15} + \dots + x + 1 = 0$.
- 以下は上の ζ_5 の場合と“同様”
- 略 (自分でノートをまとめよ.)

以上の2つの例は円分体 $\mathbb{Q}(\zeta_n)$ の特別な場合になっている。

問題 4-1 ($\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ に関する問題)

(1) $\alpha = \sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上での最小多項式を求めよ,

(2) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{6}$ を示せ.

(3) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の体の自己同型 σ, τ で

$$\sigma(a) = a \quad (a \in \mathbb{Q}), \quad \sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}$$

$$\tau(a) = a \quad (a \in \mathbb{Q}), \quad \tau(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt{3}) = -\sqrt{3}$$

をみたすものが唯一つ存在することを示せ.

ヒント (1) $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ なので, $\alpha = \sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上での最小多項式は4次式になる. α を解に持つ \mathbb{Q} 上の4次方程式を求めよ.

(2), (3) はノーヒント. 色々なやり方がある,

□

問題4-2 $\alpha = \omega^k \sqrt[3]{7}$, $\omega = e^{2\pi i/3}$, $k \in \mathbb{Z}$ とする. 以下を示せ.

(1) $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ (= (\mathbb{Q} に $x^3 - 7 = 0$ の3つの解を付け加えた体)).

(2) $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha)1 \oplus \mathbb{Q}(\alpha)\omega$. (既出の問題の解答例の結果)
(を自由に使ってよい.)

(3) $\mathbb{Q}(\alpha, \omega)$ の体の自己同型 τ で

$$\tau(a) = a \quad (a \in \mathbb{Q}(\alpha)),$$

$$\tau(\omega) = \omega^2$$

をみたすものが唯一つ存在する.

$$\left(\begin{array}{l} \alpha = \sqrt[3]{7} のとき \\ \tau(\beta) = \bar{\beta} \quad (\beta \in \mathbb{Q}(\alpha, \omega)) \\ \alpha = \omega \sqrt[3]{7}, \omega^2 \sqrt[3]{7} の \\ 場合はどうなるか? \end{array} \right)$$

(4) $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] = 3$, $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\omega)1 \oplus \mathbb{Q}(\omega)\alpha \oplus \mathbb{Q}(\omega)\alpha^2$.

(5) $\mathbb{Q}(\alpha, \omega)$ の体の自己同型 σ で

$$\sigma(a) = a \quad (a \in \mathbb{Q}(\omega)), \quad \sigma(\alpha) = \omega\alpha$$

をみたすものが唯一つ存在する.

□

問題 4-3 n は正の整数で“あるとし, $\omega = \zeta_n = e^{2\pi i/n}$ とおく、以下を示せ、

(1) $k \in \mathbb{Z}$ と n の最大公約数が d のとき, $\mathbb{Q}(\omega^k) = \mathbb{Q}(\omega^d)$,

特に $k \in \mathbb{Z}$ と n の最大公約数が 1 のとき, $\mathbb{Q}(\omega^k) = \mathbb{Q}(\omega)$.

以下, $n = p$ は素数で“あるとし, $\omega = \zeta_p$ について考える。

(2) $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^k) = \mathbb{Q}(\omega, \omega^2, \dots, \omega^{p-1}) \quad (k=1, 2, \dots, p-1),$

(3) $\mathbb{Q}(\omega) = \mathbb{Q}1 \oplus \mathbb{Q}\omega \oplus \mathbb{Q}\omega^2 \oplus \dots \oplus \mathbb{Q}\omega^{p-2}.$ \mathbb{Q} に $x^{p-1} + x^{p-2} + \dots + x + 1 = 0$ のすべての解を付け加えても できる体 □

ゆえに, $\omega, \omega^2, \dots, \omega^{p-1}$ は \mathbb{Q} 上一次独立である。できる体 □

ヒント

(1) $\{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ は位数 n の巡回群になる。

(2), (3) 問題 2-2(4). □

$\left(\begin{array}{l} \text{W は オ X ガ}, \text{ W' は ダ' グ' リ ジ} \\ \text{リ は ニ ュ -}, \text{ ツ は ウ イ}, \text{ ユ は ユ -} \end{array} \right)$

問題 4-1 ($\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ に関する問題)

05-1

- (1) $\alpha = \sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上での最小多項式を求めよ,
- (2) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{6}$ を示せ.
- (3) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の体の自己同型 σ, τ で

$$\sigma(a) = a \quad (a \in \mathbb{Q}), \quad \sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}$$

$$\tau(a) = a \quad (a \in \mathbb{Q}), \quad \tau(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt{3}) = -\sqrt{3}$$

とみなすものが唯一つ存在することを示せ.

解答例 問題 3-4 の結果より, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

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

$x^2 - 2$ は \mathbb{Q} 上既約なので $\sqrt{2}$ の \mathbb{Q} 上での最小多項式になる.

ゆえに, $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$ なので $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = \dim_{\mathbb{Q}} \mathbb{Q}[x]/(x^2 - 2) = 2$ で
 $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ である, もしも $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ ならば " $\sqrt{3} = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ " と書ける
 左辺を 2乗すると, $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ なので $3 = a^2 + 2b^2$ かつ $ab = 0$ となる.
 しかし, これは不可能なので, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$,

$\mathbb{Q}[x]/(x^2 - 2)$

|| みみざっぽ

$(\mathbb{Q}[x] \text{ の中で } x^2 - 2 \text{ を } 0 \text{ とみなして } \text{ できる環})$

||

$(\mathbb{Q}[x] \text{ の中で } x^2 = 2 \text{ とみなして } \text{ できる環})$

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ より, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] > 1$.

$\sqrt{3}$ は $x^2 - 3 = 0$ の解なので $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$.
したがって, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$,

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

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

問題 3-5 の

解答例を

参照せよ.

別の方法もある.

($x^2 - 3$ は $\mathbb{Q}(\sqrt{2})$ 上既約)

(1) $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ より, $\sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上での最小多項式
は 4 次式になる. ゆえに, $x = \sqrt{2} + \sqrt{3} \neq 0$ となる $f(x) \in \mathbb{Q}[x]$ で 4 次のものが
 $\sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上での最小多項式になる.

$$\begin{aligned} f(x) &= (x - (\sqrt{2} + \sqrt{3})) (x - (-\sqrt{2} + \sqrt{3})) (x - (\sqrt{2} - \sqrt{3})) (x - (-\sqrt{2} - \sqrt{3})) \quad \leftarrow \text{ここがかしこい} \\ &= ((x + \sqrt{3})^2 - 2)((x - \sqrt{3})^2 - 2) = (x^2 + 1 + 2\sqrt{3}x)(x^2 + 1 - 2\sqrt{3}x) \\ &= (x^2 + 1)^2 - 12x^2 = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]. \end{aligned}$$

この $f(x)$ が $\sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上での最小多項式になる.

(2) $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ より, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2}$,

$[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ より, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})1 \oplus \mathbb{Q}(\sqrt{2})\sqrt{3}$

これらより, 任意の $\beta \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ は, ある $a, b, c, d \in \mathbb{Q}$ により,

$$\beta = (a1 + b\sqrt{2})1 + (c1 + d\sqrt{2})\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

と表される.

もしも, $a, b, c, d \in \mathbb{Q}$ かつ $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = (a1 + b\sqrt{2})1 + (c1 + d\sqrt{2})\sqrt{3} = 0$ ならば;

1 と $\sqrt{3}$ の $\mathbb{Q}(\sqrt{2})$ 上での一次独立性より, $a1 + b\sqrt{2} = c1 + d\sqrt{2} = 0$ となり,

1 と $\sqrt{2}$ の \mathbb{Q} 上での一次独立性より, $a = b = c = d = 0$ となる.

ゆえに, $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ は \mathbb{Q} 上一次独立である.

以上により, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{6}$ が示された.

以上の証明は, 体の拡大の列 $M/L, L/K$ ($M \supset L \supset K$) が与えられると,

$$[M : K] = [M : L][L : K] \quad ([M/K] = [M/L][L/K])$$

が成立することの証明の特殊化になっている,

$$(3) \text{ 体の同型写像たち } \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2})[x]/(x^2 - 3) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2})(-\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$f(\sqrt{3}) \longmapsto \overline{f(x)} \longmapsto f(-\sqrt{3})$$

の合成をてと書く、ても体の同型写像で

$\tau(\beta) = \beta$ ($\beta \in \mathbb{Q}(\sqrt{2})$) ゆえに $\tau(a) = a$ ($a \in \mathbb{Q}$) かつ $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$ をみたす。これでほしいての存在が示された。

τ が $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の体の自己同型でかつ $\tau(a) = a$ ($a \in \mathbb{Q}$), $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$ をみたしているならば、任意の $a, b, c, d \in \mathbb{Q}$ について

$$\begin{aligned}\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= \tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}) \\ &= \tau(a) + \tau(b)\tau(\sqrt{2}) + \tau(c)\tau(\sqrt{3}) + \tau(d)\tau(\sqrt{2})\tau(\sqrt{3}) \\ &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}.\end{aligned}$$

τ の形が一意に決まってしまった。これでほしいての一意性も示された。

τ の存在と一意性は $\sqrt{2}$ と $\sqrt{3}$ の立場を取り換えた同様の議論で証明される。□

注 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong \mathbb{Q}[x, y]/(x^2 - 2, y^2 - 3)$ を用いて、ほしい τ との存在を示すこともできる。この方針の証明も自分で考えてみよ。□

\$\sqrt{2} \mapsto -\sqrt{3}\$ にうつすてのやり方と一意性

問題4-2

$\alpha = \omega^k \sqrt[3]{7}$, $\omega = e^{2\pi i/3}$, $k \in \mathbb{Z}$ とする. 以下を示せ. $\leftarrow \omega^3 = 1, \omega \neq 1$ なので

$$(1) \quad \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) (= (\mathbb{Q}[\alpha] \cap x^3 - 7 = 0 の 3 つの解を付け加えた体)).$$

$$(2) \quad \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha)1 \oplus \mathbb{Q}(\alpha)\omega. \quad \text{(既出の問題の解答例の結果)} \\ \text{を自由に使ってよい.}$$

(3) $\mathbb{Q}(\alpha, \omega)$ の体の自己同型 τ で

$$\tau(\alpha) = \alpha \quad (\alpha \in \mathbb{Q}(\alpha)),$$

$$\tau(\omega) = \omega^2 \quad \leftarrow \begin{cases} \alpha = \sqrt[3]{7} のとき \\ \tau(\beta) = \bar{\beta} \quad (\beta \in \mathbb{Q}(\alpha, \omega)) \\ \alpha = \omega \sqrt[3]{7}, \omega^2 \sqrt[3]{7} の \\ 場合はどうなるか? \end{cases}$$

ω^k は $1, \omega, \omega^2$ のどれか
になる.

(問題4-1の $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ を
 $\mathbb{Q}(\omega^k \sqrt[3]{7}, \omega)$ における考え方)
この問題

$$(4) \quad [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] = 3, \quad \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\omega)1 \oplus \mathbb{Q}(\omega)\alpha \oplus \mathbb{Q}(\omega)\alpha^2.$$

(5) $\mathbb{Q}(\alpha, \omega)$ の体の自己同型 σ で

$$\sigma(\alpha) = \alpha \quad (\alpha \in \mathbb{Q}(\omega)), \quad \sigma(\omega) = \omega\alpha$$

をみたすものが唯一つ存在する.

□

解答例

$$(1) \quad \alpha, \omega\alpha, \omega^2\alpha \in \mathbb{Q}(\alpha, \omega) より, \quad \mathbb{Q}(\alpha, \omega) \supset \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha).$$

$$\alpha \in \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \text{ かつ } \omega = \frac{\omega\alpha}{\alpha} \in \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \text{ より}, \quad \mathbb{Q}(\alpha, \omega) \subset \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha),$$

$$\text{ゆえに, } \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\underbrace{\alpha, \omega\alpha, \omega^2\alpha}).$$

$\alpha, \omega\alpha, \omega^2\alpha$ は $x^2 - 7 = 0$ の解の全体

(2) (問題3-5(2)と同様)

ω が“1の原始3乗根”かつ $\alpha = \omega^k \sqrt[3]{7}$ の \mathbb{Q} 上で“の最小多項式が $x^3 - 7$ ”であることより,
 $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(x^3 - 7) \cong \mathbb{Q}(\sqrt[3]{7})$ となり, そして $\omega \in \mathbb{Q}(\alpha)$ ならば虚数である 1の原始3乗根
 が $\mathbb{Q}(\sqrt[3]{7})$ に含まれることになることを示す. ゆえに, $\omega \notin \mathbb{Q}(\alpha)$ である.

$$\text{これより}, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(\omega), \mathbb{Q}(\alpha)] > 1.$$

$$\omega^2 + \omega + 1 = 0 \text{ より}, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(\omega), \mathbb{Q}(\alpha)] \leq 2.$$

$$\text{ゆえに}, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = 2.$$

したがって, $x^2 + x + 1$ は ω の $\mathbb{Q}(\alpha)$ 上での最小多項式になり,

$$\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha)[1 + \mathbb{Q}(\alpha)\omega]$$

となることがわかる.

$$\begin{aligned} &x^2 + x + 1 = 0 \text{ の解} \\ &x = \frac{-1 \pm \sqrt{-3}}{2} \end{aligned}$$

$$\left. \begin{array}{l} \alpha = \omega^k \sqrt[3]{7} \\ \quad \uparrow \\ \text{---に } \omega \text{ がある} \\ \omega \notin \mathbb{Q}(\alpha) \end{array} \right)$$

(3) $\alpha, \omega^2 \in \mathbb{Q}(\alpha, \omega)$ と $\alpha, \omega = (\omega^2)^2 \in \mathbb{Q}(\alpha, \omega^2)$ であり, $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega^2)$ である.

ω^2 も 1 の原始 3 乗根なので, ω^2 の \mathbb{Q} 上での最小多項式も $x^2 + x + 1$ になる.

(ω と ω^2 は
うつす同型を
作る問題)

体の同型写像 $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha)(\omega) \cong \mathbb{Q}(\alpha)[x]/(x^2 + x + 1) \cong \mathbb{Q}(\alpha)(\omega^2) = \mathbb{Q}(\alpha, \omega)$ の

$$f(\omega) \longmapsto \overline{f(x)} \longmapsto f(\omega^2)$$

今成を τ と書く. τ も体の自己同型で $\tau(a) = a$ ($a \in \mathbb{Q}(\alpha)$), $\tau(\omega) = \omega^2$ をみたす.
これで, ほしい τ の存在は示された.

τ が $\mathbb{Q}(\alpha, \omega)$ の体の自己同型で $\tau(a) = a$ ($a \in \mathbb{Q}(\alpha)$) と $\tau(\omega) = \omega^2$ をみたしているならば,
 $\mathbb{Q}(\alpha, \omega) = \{a + b\omega \mid a, b \in \mathbb{Q}(\alpha)\}$ かつ任意の $a, b \in \mathbb{Q}$ につけて,

$$\tau(a + b\omega) = \tau(a) + \tau(b)\tau(\omega) = a + b\omega^2 = a + b(-1 - \omega) = (a - b) - b\omega.$$

これより, ほしい τ の一意性がわかる.

注意 $\alpha = \sqrt[3]{7}$ のとき, $\mathbb{Q}(\alpha) \subset \mathbb{R}$ かつ $\omega^2 = (\omega \text{ の複素共役})$ なので

上の τ は複素共役を取る操作に一致する.

しかし, $\alpha = \omega \sqrt[3]{7}$, $\omega^2 \sqrt[3]{7}$ の場合はそうではない.

(4) α の \mathbb{Q} 上での最小多項式 $x^7 - 7$ は 3 次なので, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

上の (2) より, $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = 2$.

ゆえに, $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 3 = 6$.

一方, $6 = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] \underbrace{[\mathbb{Q}(\omega) : \mathbb{Q}]}_{\mathbb{Q}(\omega) \text{ 上の最小多項式は } x^2 + x + 1 \text{ なので } 2 \text{ に等しい}} = 2 [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)]$,

ω の \mathbb{Q} 上での最小多項式は $x^2 + x + 1$ なので 2 に等しい

ゆえに, $[\mathbb{Q}(\omega)(\alpha) : \mathbb{Q}(\omega)] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] = 3$.

したがって, $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\omega)(\alpha) = \mathbb{Q}(\omega)1 \oplus \mathbb{Q}(\omega)\alpha \oplus \mathbb{Q}(\omega)\alpha^2$.

注意 $\alpha, \omega\alpha, \omega^2\alpha$ の $\mathbb{Q}(\omega)$ 上での最小多項式が $x^3 - 7$ であることを示された.

(5) α と $w\alpha$ の $\mathbb{Q}(\omega)$ 上での最小多項式はどうしても $x^3 - 7$ で、
(1) の α が α と $w\alpha$ の場合より、 $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, w\alpha, w^2\alpha) = \mathbb{Q}(w\alpha, \omega)$. (α を $w\alpha$ に置く
自己同型を作る
問題)

体の同型写像たち $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\omega)(\alpha) \cong \mathbb{Q}(\omega)[x]/(x^3 - 7) \cong \mathbb{Q}(\omega)(w\alpha) = \mathbb{Q}(\alpha, \omega)$
 $f(\alpha) \longmapsto \overline{f(x)} \longmapsto f(w\alpha)$

の合成を σ と書く。 σ も体の同型で、 $\sigma(\alpha) = \alpha$ ($\alpha \in \mathbb{Q}(\omega)$)、 $\sigma(\alpha) = w\alpha$ をみたす。
これでほしい σ の存在が示された。

σ は $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\omega)(\alpha)$ の体の自己同型で $\sigma(\alpha) = \alpha$ ($\alpha \in \mathbb{Q}(\omega)$)、 $\sigma(\alpha) = w\alpha$ をみたしていようとする。このとき、任意の $a, b, c \in \mathbb{Q}(\omega)$ について、

$$\sigma(a + b\alpha + c\alpha^2) = \sigma(a) + \sigma(b)\sigma(\alpha) + \sigma(c)\sigma(\alpha)^2 = \underbrace{a}_{\text{左}} + \underbrace{bw\alpha}_{\text{右}} + \underbrace{cw^2\alpha^2}_{\text{左}} \quad \text{どれも } \in \mathbb{Q}(\omega)$$

これでほしい σ の一意性も示された。 □

ポイント ほしい体の同型写像は、最小多項式と準同型定理から得られる
体の同型写像の合成として構成可能である。 □

注意

(1) 体の同型写像たち $\mathbb{Q}(\alpha) \xrightarrow{\sim} \mathbb{Q}[x]/(x^3-1) \xrightarrow{\sim} \mathbb{Q}(w\alpha)$ の合成を $\tilde{\sigma}$ と書くと,

$$f(\alpha) \longmapsto \overline{f(x)} \longmapsto f(w\alpha)$$

$\tilde{\sigma} : \mathbb{Q}(\alpha) \xrightarrow{\sim} \mathbb{Q}(w\alpha)$ と $\tilde{\sigma}$ の定義域 $\mathbb{Q}(\alpha)$ と値域 $\mathbb{Q}(w\alpha)$ は異なる.

(2) 体の同型写像たち $\mathbb{Q}(w)(\alpha) \xrightarrow{\sim} \mathbb{Q}(w)[x]/(x^3-1) \xrightarrow{\sim} \mathbb{Q}(w)(w\alpha)$ の合成 σ の場合には,

$$f(\alpha) \longmapsto \overline{f(x)} \longmapsto f(w\alpha)$$

$\mathbb{Q}(w)(\alpha) = \mathbb{Q}(w, \alpha) = \mathbb{Q}(\alpha, w\alpha, w^2\alpha) = \mathbb{Q}(w, w\alpha) = \mathbb{Q}(w)(w\alpha)$ なので,²

σ の定義域と値域は等しくなり, σ は $\mathbb{Q}(w, \alpha) = \mathbb{Q}(\alpha, w\alpha, w^2\alpha)$ の自己同型になる.

以上の(1)と(2)のちがいは $w\alpha \notin \mathbb{Q}(\alpha)$ と $w\alpha \in \mathbb{Q}(w, \alpha)$ のちがいである.

$\mathbb{Q}(w, \alpha)$ は w を含むので, α を $w\alpha$ にうつす操作で $\mathbb{Q}(w, \alpha)$ が閉じることが可能になる. これらの中間を認識しておくことは重要である.

□

問題 4-3 n は正の整数であるとし, $\omega = \zeta_n = e^{2\pi i/n}$ とおく. 以下を示せ.

(1) $k \in \mathbb{Z}$ と n の最大公約数が d のとき, $\mathbb{Q}(\omega^k) = \mathbb{Q}(\omega^d)$,

特に $k \in \mathbb{Z}$ と n の最大公約数が 1 のとき, $\mathbb{Q}(\omega^k) = \mathbb{Q}(\omega)$.

以下, $n=p$ は素数であるとし, $\omega = \zeta_p$ について考える.

$$(2) \quad \mathbb{Q}(\omega) = \mathbb{Q}(\omega^k) = \mathbb{Q}(\omega, \omega^2, \dots, \omega^{p-1}) \quad (k=1, 2, \dots, p-1),$$

$$(3) \quad \mathbb{Q}(\omega) = \mathbb{Q}1 \oplus \mathbb{Q}\omega \oplus \mathbb{Q}\omega^2 \oplus \dots \oplus \mathbb{Q}\omega^{p-2}$$

ゆえに, $\omega, \omega^2, \dots, \omega^{p-1}$ は \mathbb{Q} 上一次独立である.

\mathbb{Q} に $x^{p-1} + x^{p-2} + \dots + x + 1 = 0$
 のすべての解を付け加えて
 できる体 \square

訂正あり

$$\begin{aligned} \mathbb{Q}\omega^{p-1} &\rightarrow \mathbb{Q}\omega^{p-2} \\ \mathbb{Q}, \omega, \dots &\rightarrow \mathbb{Q}, \omega, \omega^3, \dots \end{aligned}$$

解答例

(1) k と n の最大公約数が d のとき, $ks + nt = d$ をみたす $s, t \in \mathbb{Z}$ が存在するので, $\omega^d = \omega^{ks+nt} = (\omega^k)^s \in \mathbb{Q}(\omega^k)$. ゆえに, $\mathbb{Q}(\omega^d) \subset \mathbb{Q}(\omega^k)$

d は k の約数なので $k = du$, $u \in \mathbb{Z}$ と書けるので $\omega^k = (\omega^d)^u \in \mathbb{Q}(\omega^d)$, ゆえに $\mathbb{Q}(\omega^k) \subset \mathbb{Q}(\omega^d)$.

これで $\mathbb{Q}(\omega^k) = \mathbb{Q}(\omega^d)$ が示された.

$d=1$ ならば $\mathbb{Q}(\omega^k) = \mathbb{Q}(\omega)$.

以下, $n=p$ は素数であるとし, $\omega = \zeta_p$ であるとする.

(2) $k=1, 2, \dots, p-1$ と p の最大公約数は $d=1$ なので (1) より $\mathbb{Q}(\omega^k) = \mathbb{Q}(\omega)$.

ゆえに, $\omega, \omega^2, \dots, \omega^{p-1} \in \mathbb{Q}(\omega)$ なので, $\mathbb{Q}(\omega) = \mathbb{Q}(\omega, \omega^2, \dots, \omega^{p-1})$ となることがわかる.

(3) 問題 2-2(4) の結果より, $x^{p-1} + x^{p-2} + \dots + x + 1$ は \mathbb{Q} 上の既約多項式になる.

$\omega^p = 1$ かつ $\omega \neq 1$ と $\omega^p - 1 = (\omega - 1)(\omega^{p-1} + \omega^{p-2} + \dots + \omega + 1)$ より,

$\omega^{p-1} + \omega^{p-2} + \dots + \omega + 1 = 0$ となることがわかる.

以上より, ω の \mathbb{Q} 上の最小多項式は $x^{p-1} + x^{p-2} + \dots + x + 1$ になることがある.

これより, $\mathbb{Q}(\omega) \cong \mathbb{Q}[x]/(x^{p-1} + x^{p-2} + \dots + x + 1)$, $[\mathbb{Q}(\omega) : \mathbb{Q}] = p-1$,

$$\mathbb{Q}(\omega) = \mathbb{Q}1 \oplus \mathbb{Q}\omega \oplus \mathbb{Q}\omega^2 \oplus \dots \oplus \mathbb{Q}\omega^{p-2}$$

特に, $1, \omega, \omega^2, \dots, \omega^{p-2}$ は \mathbb{Q} 上一次独立である.

ω をかける操作は $\mathbb{Q}(\omega)$ の \mathbb{Q} 上での線形同型になるので,

$\omega, \omega^2, \omega^3, \dots, \omega^{p-1}$ も \mathbb{Q} 上一次独立である.

□

最小多項式に関するまとめ

05-4

定理 体 K とその拡大体 L と $\alpha \in L$ と K 係数の 0 でない多項式 $F(x) \in K[x]$ で α を根に持つもの ($x = \alpha$ とすると 0 になるもの) について、以下の条件は互いに同値である。

(1) $F(x)$ は α の K 上での最小多項式である。

($F(x)$ は α を根に持つ 0 でない K 係数多項式の中で次数が最小のものである。)

(2) $F(x)$ は K 上既約である。

(3) 自然な環の準同型写像 $\bar{\varphi}: K[x]/(F(x)) \rightarrow K(\alpha)$, $\bar{f}(x) \mapsto f(\alpha)$ は同型写像になる。

(4) $[K(\alpha) : K] = \deg F(x)$. 以下 の 証明も大事だが、

以上の 同値性は 空気のごとく使われることに注意せよ！

証明

(1) \Rightarrow (2) の対偶 $F(x)$ は体 K 上既約でないと仮定する。そのとき、ある 1 次以上の

$G(x), H(x) \in K[x]$ が存在して、 $F(x) = G(x)H(x)$ 、このとき、 $G(x), H(x)$ の次数は 1 次以上でかつ $F(x)$ の次数より真に小さくなる。 $F(x)$ は α を根に持つので、

$0 = F(\alpha) = G(\alpha)H(\alpha)$. ゆえに $G(\alpha) = 0$ または $H(\alpha) = 0$.

ゆえに $F(x)$ は α の K 上での最小多項式でない。

以下の設定をこの証明中で自由に使う.

環の準同型写像 $\varphi: K[x] \rightarrow K(\alpha)$ を $\varphi(f(x)) = f(\alpha) \quad (f(x) \in K[x])$ と定める.

$\text{Ker } \varphi = \{f(x) \in K[x] \mid f(\alpha) = 0\}$ は $K[x]$ のイデアルになる,

$K[x]$ は PID なので $\text{Ker } \varphi = (F_\alpha(x))$, $F_\alpha(x) \in K[x]$ と書ける, $\leftarrow (F_\alpha(x) \text{ と } F(x) \text{ を区別せよ.})$

$0 \neq F(x) \in \text{Ker } \varphi$ なので $\text{Ker } \varphi \neq \{0\}$ かつ $F_\alpha(\alpha) \neq 0$,

$F_\alpha(x)$ は α の K 上での最小多項式になる (最小多項式の存在),

(証明 $0 \neq f(x) \in K[x]$ かつ $f(\alpha) = 0$ のとき, $f(x) \in \text{Ker } \varphi = (F_\alpha(x))$ なので $f(x) = F_\alpha(x)g(x)$, $g(x) \in K[x]$ と書け, $g(x) \neq 0$ でなければいけない, $\deg f(x) \geq \deg F_\alpha(x)$, ゆえに, そのような $f(x)$ の中で $F_\alpha(x)$ の次数は最小になっている.)

$F(x) \in \text{Ker } \varphi = (F_\alpha(x))$ より, ある $0 \neq G(x) \in K[x]$ が存在して, $F(x) = F_\alpha(x)G(x)$.

(2) \Rightarrow (1) の対偶 $F(x)$ は α の K 上での最小多項式ではないと仮定する.

そのとき $\deg F(x) > \deg F_\alpha(x)$ なので, 上の $F(x) = F_\alpha(x)G(x)$ より, $F(x)$ は K 上既約でないことがわかる.

以上によて, (1) \Leftrightarrow (2) が示された.

(1) \Rightarrow (3) $F(x)$ は α の K 上で "最小多項式" であると仮定する.

そのとき, $\deg F(x) = \deg F_\alpha(x)$ なので, 上の $F(x) = F_\alpha(x)G(x)$ において, $G(x) \in K[x]$ となる. ゆえに, $(F(x)) = (F_\alpha(x)) = \text{Ker } \varphi$ となる.

したがって環の準同型定理によて, 次の環の同型写像が得られる:

$$\bar{\varphi}: K[x]/(F(x)) \xrightarrow{\sim} \text{Im } \varphi, \quad \bar{\varphi}(\bar{f(x)}) = f(\alpha).$$

(1) と (2) の同値性より, $F(x)$ は K 上既約になるので,

PID では既約元 α で
生成される單項 ideal は
极大イデアルになる.

PID に関する一般論より, $\text{Ker } \varphi = (F(x))$ は $K[x]$ の极大イデアルになる.

ゆえに, $K[x]/(F(x))$ は体になり, $\text{Im } \varphi$ は K と α を含む L の部分体になることわかる.

K と α を含む L の部分体は任意の $f(x) \in K[x]$ に対する $f(\alpha)$ も含むので, $\text{Im } \varphi$ を含む.

$K(\alpha)$ は K と α を含む L の部分体の中で最小のもので, K と α を含む L の部分体 $\text{Im } \varphi$ が $K(\alpha)$ に含まれることになる. ゆえに, $\text{Im } \varphi = K(\alpha)$.

これで, $\bar{\varphi}: K[x]/(F(x)) \xrightarrow{\sim} K(\alpha), \quad \bar{f(x)} \mapsto f(\alpha)$ という同型が得られた.

(3) \Rightarrow (4) 同型 $K[x]/(F(x)) \cong K(\alpha)$, $\overline{f(x)} \leftrightarrow f(\alpha)$ が成立しているとき,

$$[K(\alpha) : K] = \dim_K K(\alpha) = \dim_K K[x]/(F(x)) = \deg F(x).$$

(4) \Rightarrow (1) α の K 上で "の最小多項式" $F_\alpha(x)$ について, (1) \Rightarrow (3) の証明より,

同型 $K[x]/(F_\alpha(x)) \cong K(\alpha)$, $\overline{f(x)} \leftrightarrow f(\alpha)$ が得られ, (3) \Rightarrow (4) の証明より,

$$[K(\alpha) : K] = \deg F_\alpha(x) \text{ が得られる.}$$

$[K(\alpha) : K] = \deg F(x)$ と仮定する. このとき, $\deg F(x) = \deg F_\alpha(x)$ なので,

$F(x)$ は α の K 上で "の最小多項式" になる.

q.e.d.

注意 体 K とその拡大体 L と $\alpha \in L$ について, ある $0 \neq F(x) \in K[x]$ で α を根に持つものが存在するとき, α は K 上 代数的であるという.
そうでないとき, α は K 上 超越的であるという.

$\sqrt{2}$ や $\sqrt{-1}$ は \mathbb{Q} 上代数的, e や π は \mathbb{Q} 上超越的である.

□

使い方

L は体 K の拡大体であり $\alpha \in L$ は体 K 上代数的元素であるとし,
 $F(x)$ は α の K 上でのモニックな最小多項式であるとする.

M は L の拡大体であるとし, $F(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, $\alpha_1, \dots, \alpha_n \in M$
と仮定する. ($K = \mathbb{Q}$ の場合には $M = \mathbb{C}$ と取れることが多い.)

このとき, $F(x)$ は K 上既約であり, $F(\alpha_i) = 0$ なので,

$F(x)$ は各 α_i の K 上での最小多項式にもなる.

ゆえに, 体の同型写像たち

$$\begin{aligned}\bar{\varphi} : K[x]/(F(x)) &\xrightarrow{\sim} K(\alpha), & \bar{\varphi}_i : K[x]/(F(x)) &\xrightarrow{\sim} K(\alpha_i) \\ \overline{f(x)} &\longmapsto f(\alpha) & \overline{f(x)} &\longmapsto f(\alpha_i)\end{aligned}$$

が得られ, 次の体の同型写像を作れる:

$$\bar{\varphi}_i \circ \bar{\varphi}^{-1} : K(\alpha) \xrightarrow{\sim} K(\alpha_i), \quad f(\alpha) \mapsto f(\alpha_i) \quad (f(x) \in K[x]).$$

もしも $K(\alpha_i) = K(\alpha)$ ならば, これは $K(\alpha)$ の自己同型になる.

□

α_i たゞは α の共役元
K 上での

例 $K = \mathbb{Q}$, $\alpha = \sqrt[3]{7}$ の場合、 $\omega = e^{2\pi i/3}$ とおく、

α の \mathbb{Q} 上での最小多項式は $x^3 - 7$ であり、その根の全体は $\alpha, \omega\alpha, \omega^2\alpha$ 。
 $\mathbb{Q}(\alpha), \mathbb{Q}(\omega\alpha), \mathbb{Q}(\omega^2\alpha)$ は互いに異なるが、互いに体として同型になる：

$\mathbb{Q}(\alpha) \cong \mathbb{Q}(\omega^k\alpha)$, $f(\alpha) \leftrightarrow f(\omega^k\alpha)$ ($k \in \mathbb{Z}, f(x) \in K[x]$). □

\mathbb{Q} 上での
αの共役元

$x^3 - 7 = 0$ の
解を1つ
だけ
 \mathbb{Q} に追加
した場合

例 $K = \mathbb{Q}(\omega), \omega = e^{2\pi i/3}$ で $\alpha = \sqrt[3]{7}$ の場合、

α の $K = \mathbb{Q}(\omega)$ 上での最小多項式も $x^3 - 7$ になる。

$K(\alpha) = K(\omega^k\alpha)$ ($k \in \mathbb{Z}$) が成立しており、 $K(\alpha)$ の 自己同型写像

$\sigma: K(\alpha) \xrightarrow{\sim} K(\omega^k\alpha) = K(\alpha)$, $\sigma(f(\alpha)) = f(\omega^k\alpha)$ ($k \in \mathbb{Z}, f(x) \in K[x]$)
 が得られる。

$x^3 - 7$ の
解をすべて
 \mathbb{Q} に追加
した場合

$K(\alpha) = \mathbb{Q}(\omega, \alpha) = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ は \mathbb{Q} に $x^3 - 7 = 0$ のすべての解
を付け加えてできる体になっている。 □

注意 共役元から作られる体の同型は本質的に最小多項式の話になっている。初学者は最小多項式についてまず理解するとよい。 □

メインの問題は次ページの問題です。

定義 体 K の中にて正の整数個の 1 の和 $1+1+\cdots+1$ が決して 0 にならないとき,
 K の**標数**は 0 であるという。

正の整数 N で体 K の中での N 個の 1 の和が 0 になるものが存在するとき,
 K は**正標数**であるといい, そのような N の最小値を K の**標数**と呼ぶ。 \square

問題 5-1 K は標数 0 の体であるとし, L はその任意の拡大体であるとする。
 K 上の既約多項式が L の中に重根を持たないことを示せ。 \square

問題 5-2 正標数の体の標数が常に素数になることを示せ。 \square

素数 p に対して, $\mathbb{F}_p = \mathbb{Z}/(p)$ とおく、

\mathbb{F}_p は位数 p (元の個数が p) の体になり, \mathbb{F}_p の標数も p になる。

体 K に対して, $K(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], g(x) \neq 0 \right\}$ を K 上の(1変数)**有理函数体**と呼ぶ。
x は文字

問題 5-3 p は素数であるとし, $L = \mathbb{F}_p(t) = (1$ 变数 t の \mathbb{F}_p 上の有理函数体) とおく、
 L の部分体 K と K 上の既約多項式 $F(x) \in K[x]$ の組 $(K, F(x))$ で
 $F(x)$ が L の中に重根を持つものの 1 つを具体的に構成せよ。 \square

Cの部分体の单拡大定理 K は C の部分体であるとし, $\alpha_1, \dots, \alpha_r \in C$ は K 上

代数的であると仮定する. このとき, ある $\theta \in C$ が存在して, $K(\alpha_1, \dots, \alpha_r) = K(\theta)$ \square

この定理の証明(講義でやったはず)を読んで以下の問いに答えるよ.

問題 5-4 $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbb{Q}(\theta)$ をみたす $\theta \in C$ を具体的に与え,

実際にその等号が成立することを証明せよ,

\square

問題 5-5 上の定理の $r=2$ の場合の証明を書け、すなわち、次を示せ:

K は C の部分体であるとし, $\alpha, \beta \in C$ は K 上代数的であると仮定する.

このとき, ある $\theta \in C$ が存在して, $K(\alpha, \beta) = K(\theta)$.

\square

注意 上の定理は問題 5-5 の結果を使うと、以下をみたす $\theta_1, \dots, \theta_{n-1} \in C$ が
次々に得られることがわかる:

$$K(\alpha_1, \alpha_2) = K(\theta_1), \quad K(\alpha_1, \alpha_2, \alpha_3) = K(\theta_1, \alpha_3) = K(\theta_2), \quad K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = K(\theta_2, \alpha_4) = K(\theta_3), \dots,$$

$$K(\alpha_1, \dots, \alpha_{n-1}, \alpha_n) = K(\theta_{n-2}, \alpha_n) = K(\theta_{n-1}).$$

\square

問題 5-1 K は標数 0 の体であるとし, L はその任意の拡大体であるとする.

K 上の既約多項式が L の中に重根を持たないことを示せ. \square

解答例 $f(x) = \sum_k a_k x^k \in L[x]$, $a_k \in L$ に対して, $f'(x)$ を $f'(x) = \sum_k a_k k x^{k-1}$ と定める.] 準備
 L の標数も 0 になるので, $\deg f(x) \geq 1$ ならば $\deg f'(x) = \deg f(x) - 1$ となる.] 今後自由に利用する.
 $\left(\begin{array}{l} n = \deg f(x) \text{ とおくと, } f(x) = a_n x^n + \dots + a_1 x + a_0 \text{ なので, } f'(x) = n a_n x^{n-1} + \dots + a_1 \\ \text{なので } \deg f'(x) = n-1. \text{ 注意 } \deg f(x) = 0 \text{ ならば } f(x) = a_0 \text{ の形になります, } f'(x) = 0 \text{ となります.} \\ \deg f'(x) = \deg 0 = -\infty \end{array} \right)$

$f(x) \in K[x]$ を任意にとる.

$f(x)$ と $f'(x) \in K[x]$ の最大公約多項式を $d(x) \in K[x]$ と書く. \leftarrow (最大公約多項式は Euclid の互除法により $K[x]$ 内で計算される.)

$f(x)$ が重根 $\alpha \in L$ を持つとき, $f(x)$ が K 上既約でないことを (対偶) を示せばよい.

$f(x)$ の重根 $\alpha \in L$ が存在すると仮定する.

このとき, $f(x) = (x-\alpha)^2 g(x)$, $g(x) \in L[x]$ と書ける. これ自体は $L[x]$ の元で $K[x]$ の元とは限らない.

$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$ より, $f(x)$ と $f'(x)$ には共通因子 $x-\alpha$ を持つ.

ゆえに $f(x)$ と $f'(x)$ の最大公約多項式 $d(x) \in K[x]$ の次数は 1 以上 $\deg f'(x) = \deg f(x) - 1$ 以下になる. $f(x)$ は, そのような $d(x) \in K[x]$ で割り切れるので, K 上既約でない. \square

問題 5-2 正擇数の体の擇数が常に素数になることを示せ. \square

解答例 K は正擇数の体であると仮定する. (より一般に整域の定義の中に)
 (体の定義の中に 1 キ 0 が入っている.)

N は正の整数であり, K の中での N 個の 1 の和が 0 になると仮定する.

もしも N が素数でないならば $N = mn$ (m, n は 2 以上の整数) と書ける.

そのとき,

$$\underbrace{\left(\underbrace{1 + \dots + 1}_{m} \right) + \dots + \left(\underbrace{1 + \dots + 1}_{m} \right)}_{n} = 0.$$

両辺を $\underbrace{1 + \dots + 1}_{m}$ で割ると, $\underbrace{1 + \dots + 1}_{n} = 0$ となって, N より小さな正の整数 n で, K の中での n 個の 1 の和が 0 になる. ($n < mn$ に注意せよ.)

ゆえに, 正の整数 N で K の中での N 個の 1 の和が 0 になるものの最小値 (= K の擇数) は素数でなければいけない.

例 素数 p に対して, $F_p = \mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$ とおく. F_p は擇数 p で位数 p の体になる. \square

元の個数
 \downarrow
 \square

問題5-3 p は素数であるとし, $L = \mathbb{F}_p(t) = (1\text{変数} t\text{の } \mathbb{F}_p\text{上の有理函数体})$ とおく.
 L の部分体 K と K 上の既約多項式 $F(x) \in K[x]$ の組 $(K, F(x))$ で
 $F(x)$ が L の中に重根を持つものの 1 つを具体的に構成せよ. \square

解答例 $K = \mathbb{F}_p(t^p) = \left\{ \frac{f(t^p)}{g(t^p)} \mid f(t), g(t) \in \mathbb{F}_p[t], g(t) \neq 0 \right\}$ と L の部分体 K を定め, $F(x) = x^p - t^p \in K[x]$ とおく. (大 $\notin K$ が重要ポイント, $t^p \in K$)

$K = \mathbb{F}_p(t^p)$ は UFD $\mathbb{F}_p[t^p]$ の商体であり, t^p は $\mathbb{F}_p[t^p]$ の既約元である.
 $(\mathbb{F}_p[t^p]$ は t, t^2, \dots, t^{p-1} を含まないので, t^p は非自明な約数を持たない.)

ゆえに, $F(x) = x^p - t^p$ に, Eisenstein の判定法を適用すると,

$$t^p \nmid 1, t^p \nmid 0, \dots, t^p \nmid 0, t^p \mid (-t^p), (t^p)^2 + t^p$$

なので, $F(x) = x^p - t^p$ は $K = \mathbb{F}_p(t^p)$ 上の既約多項式であることがわかる.

L の標数は p なので, $F(x) = (x-t)^p$ なので $F(x)$ は p 重根 $t \in L$ を持つ. \square

↑ 次ページで証明

注意 上の $L/K = \mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ は 純非分離拡大 の例になっている. \square

注意 前ページの $(x-t)^p = x^p - t^p$ を示すためには次を示せば十分, \square

補題 p は素数であるとし, 可換環 A の中で p 個の 1 の和は 0 であると仮定する.

このとき, 任意の $a, b \in A$ について, $(a+b)^p = a^p + b^p$ かつ $(-a)^p = -a^p$.

証明 $p=2$ のとき, $a+a = a(1+1) = a \cdot 0 = 0$ なので $-a = a$ となるので, $(-a)^p = -a^p$ が成立する. p が奇素数の場合は $(-a)^p = -a^p$ は自明である.

以下, A の中で n 個の 1 の和を単に n と書く.

二項定理より,

$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k, \quad \binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!} \in \mathbb{Z}$$

$k=1, \dots, p-1$ のとき, $\binom{p}{k}$ は p で割り切れるので A の中で 0 になる. ゆえに,

$$(a+p)^p = \binom{p}{0} a^p + \binom{p}{p} b^p = a^p + b^p.$$

\square

注意 $a \mapsto a^p$ は A から A 自身への環の準同型になっている. $\leftarrow (ab)^p = a^p b^p$
これを A の Frobenius 準同型 と呼ぶ. \square は自明

单拡大定理について

06-2

問題 5-4 $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbb{Q}(\theta)$ をみたす $\theta \in \mathbb{C}$ を具体的に与え,
実際にその等号が成立することを証明せよ.

□

問題 5-5 次を示せ:

K は \mathbb{C} の部分体であるとし, $\alpha, \beta \in \mathbb{C}$ は K 上代数的であると仮定する.
このとき, ある $\theta \in \mathbb{C}$ が存在して, $K(\alpha, \beta) = K(\theta)$.

□

まず“最初に後者について非常に詳しく解説する. → 次ページ”

(**方針** 適切に $\theta = \alpha + c\beta$, $c \in K$, $G(x) \in K(\theta)[x]$ を作って,
 $G(x)$ と β の K 上での最小多項式の共通根が β だけになるようにする.)

そしてその証明の方法を使って前者の問題を解く.
後で前者の問題の例を非常に詳しく取り扱う.

問題5-5の解答例 K は \mathbb{C} の部分体であるとし, $\alpha, \beta \in \mathbb{C}$ は K 上代数的だと仮定する.

α と β の K 上でのモニックな最小多項式をそれぞれ $F_\alpha(x), F_\beta(x) \in K[x]$ と書く.

$F_\alpha(x)$ の $\alpha = \alpha_1$ 以外の互いに異なる根全体を $\alpha_2, \dots, \alpha_m$ と書く.

$F_\beta(x)$ の $\beta = \beta_1$ 以外の互いに異なる根全体を β_2, \dots, β_n と書く.

$G(t, x) = F_\alpha(\alpha + t\beta - tx) \in K(\alpha, \beta)[t, x]$ とおく.

このとき, $G(t, \beta) = F_\alpha(\alpha) = 0$ ($K(\alpha, \beta)[t]$ の元として 0).

$$\begin{aligned} G(t, \beta_j) &= 0 \quad \leftarrow j \neq 1 \text{ と仮定} \\ \Leftrightarrow \exists i &= 1, \dots, m \text{ s.t. } \alpha + (\beta - \beta_j)t = \alpha_i \\ \Leftrightarrow \exists i &= 1, \dots, m \text{ s.t. } t = -\frac{\alpha - \alpha_i}{\beta - \beta_j} \end{aligned}$$

$j = 2, \dots, n$ のとき, $\beta_1 - \beta_j \neq 0$ より, $G(t, \beta_j) = F_\alpha(\alpha + (\beta_1 - \beta_j)t) \in \mathbb{C}[t]$ の次数は $F_\alpha(x)$ と等しくなり, 特に $G(t, \beta_j)$ は t の多項式として 0 ではないので, t の多項式としての根は有限個になる.

K は 様数が 0 なので “無限個の元” と言ふ. ゆえに, 有限集合 $\bigcup_{j=2}^n \{t \in \mathbb{C} \mid G(t, \beta_j) = 0\}$ に含まれない元 $c \in K$ が存在する.

ここで $K(\theta)$ にできることがポイント

$\theta = \alpha + c\beta$, $G(x) = G(c, x) = F_\alpha(\theta - cx) \in K(\theta)[x]$ とおく.

このとき, $G(\beta) = G(c, \beta) = 0$ で, c の取り方より, $j = 2, \dots, n$ について $G(\beta_j) = G(c, \beta_j) \neq 0$.

K の次数は0で、 $F_\beta(x)$ は K 上既約なので重根を持たない。

ゆえに、 $F_\beta(x) = \prod_{j=1}^n (x - \beta_j)$ ($\beta_1 = \beta$ と β_1, \dots, β_n が互いに異ることに注意)。

$G(x)$ は $G(\beta) = 0$ と $j=2, \dots, n$ について $G(\beta_j) \neq 0$ をめたすので、 $G(x)$ と $F_\beta(x)$ の共通根は $\beta = \beta_1$ しか存在しない。

したがって、 $G(x)$ と $F_\beta(x)$ のモニックな最大公約多項式 $H(x)$ は $H(x) = x - \beta$ になる。

$K \subset K(\theta)$ ので $F_\beta(x)$ も $G(x)$ と同じく $K(\theta)[x]$ の元であることに注意せよ。

ゆえに、 $G(x)$ と $F_\beta(x)$ のモニックな最大公約多項式 $H(x)$ についても $H(x) \in K(\theta)[x]$ となる。

これで、 $x - \beta = H(x) \in K(\theta)[x]$ が示された。つまり、 $\beta \in K(\theta)$.

$\theta = \alpha + c\beta, c \in K$ だったので $\alpha = \theta - c\beta \in K(\theta)$.

したがって、 $K(\alpha, \beta) \subset K(\theta)$.

$\theta = \alpha + c\beta \in K(\alpha, \beta)$ より、 $K(\theta) \subset K(\alpha, \beta)$.

以上によて、 $K(\alpha, \beta) = K(\theta)$ が示された。 \square

注意 $F_\beta(x)$ が重根を持たないことを仮定すれば” $\leftarrow (\beta \text{の } K \text{ 上での分離性})$

以上の証明法は正標数の無限体でも使える。 \square

問題5-4の解答例

$\theta = \sqrt{2} + \sqrt[3]{3}$ とおくと, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbb{Q}(\theta)$ となる.

証明

$\sqrt{2}, \sqrt[3]{3}$ の \mathbb{Q} 上での最小多項式はそれぞれ $f(x) = x^2 - 2$, $g(x) = x^3 - 3$.

$$h(x) = f(\theta - x) = f(\sqrt{2} + \sqrt[3]{3} - x) = (\sqrt[3]{3} - x)(2\sqrt{2} + \sqrt[3]{3} - x) \text{ とおく.}$$

$$f(x) = (x - \sqrt{2})(x + \sqrt{2}).$$

$h(x)$ と $g(x)$ の共通根は $\sqrt[3]{3}$ だけであることがわかる.

ここに複雑な
計算がつまっている.

(→ 次ページへ)

$h(x)$ と $g(x)$ のモニックな最大公約多項式は $x - \sqrt[3]{3}$ になる.

そして, $h(x) \in g(x) \in \mathbb{Q}(\theta)[x]$ の元なので Euclid の互除法より, $x - \sqrt[3]{3} \in \mathbb{Q}(\theta)[x]$ となる. ゆえに, $\sqrt[3]{3} \in \mathbb{Q}(\theta)$, $\sqrt{2} = \theta - \sqrt[3]{3} \in \mathbb{Q}(\theta)$ なので $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \subset \mathbb{Q}(\theta)$.
 $\theta = \sqrt{2} + \sqrt[3]{3} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ なので $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$.

これで, $\theta = \sqrt{2} + \sqrt[3]{3}$ のとき, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbb{Q}(\theta)$ となることが示された. \square

次ページ以降でこの例をさらに詳しく見ていく.

別解

$\theta = \sqrt{2} + \sqrt[3]{3}$ とおくと, $\theta^4 = 12\sqrt[3]{3}$ なので $\sqrt[3]{3} = \theta^4/12 \in \mathbb{Q}(\theta)$ かつ
 $\sqrt{2} = \theta/\sqrt[3]{3} = 12/\theta^3 \in \mathbb{Q}(\theta)$ なので $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. \square

Euclidの互除法 $\alpha = \sqrt{2}$, $\beta = \sqrt[3]{3}$, $\theta = \alpha + \beta = \sqrt{2} + \sqrt[3]{3}$ とおく。

$f(x) = x^2 - 2$, $g(x) = x^3 - 3$, $h(x) = f(\theta - x) = (x - \theta)^2 - 2 = x^2 - 2\theta x + \theta^2 - 2$ とおく。

$g(x)$ と $h(x)$ のモニックな最大公約多項式は $x - \sqrt[3]{3}$ 。

$$\begin{array}{r} x+2\theta \\ \hline x^2-2\theta x+\theta^2-2 \sqrt{x^3} \\ \hline x^3-2\theta x^2+(\theta^2-2)x \\ \hline 2\theta x^2-(\theta^2-2)x-3 \\ \hline 2\theta x^2-4\theta^2 x+2\theta(\theta^2-2) \\ \hline (3\theta^2+2)x-(2\theta(\theta^2-2)+3) \end{array}$$

$$g(x) = (x+2\theta) h(x) + (3\theta^2+2)x - (2\theta(\theta^2-2)+3)$$

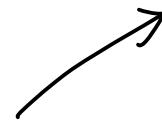
↑
Euclidの互除法より,
これが "g(x) と h(x) の g.c.d. になる。

これより, $x - \sqrt[3]{3} = x - \frac{2\theta(\theta^2-2)+3}{3\theta^2+2}$.

つまり, $\sqrt[3]{3} = \frac{2\theta(\theta^2-2)+3}{3\theta^2+2} \in \mathbb{Q}(\theta)$

非自明だが手計算で確認可能 → 次ページ

このコンピュータによる確認
↓



($2t(t^2-2)+3)/(3t^2+2)$ where $\{t=\sqrt{2}+3^{(1/3)}\}$)

Assuming the principal root | Use the real-valued root instead

Input interpretation

$$\frac{2t(t^2-2)+3}{3t^2+2} \text{ where } t = \sqrt{2} + \sqrt[3]{3}$$

Result

$$\frac{3+2(\sqrt{2}+\sqrt[3]{3})((\sqrt{2}+\sqrt[3]{3})^2 - 2)}{2+3(\sqrt{2}+\sqrt[3]{3})^2}$$

Alternate forms

$\sqrt[3]{3}$ OK!

$\theta = \sqrt{2} + \sqrt[3]{3}$ のとの $\sqrt[3]{3} = \frac{2\theta(\theta^2-2)+3}{3\theta^2+2}$ の手計算での確認

$\alpha = \sqrt{2}, \beta = \sqrt[3]{3}$ とおく。 $\theta = \alpha + \beta, \alpha^2 = 2, \beta^3 = 3$ となる。

$$\begin{aligned} 2\theta(\theta^2-2)+3 &= 2\theta^3 - 4\theta + 3 \\ &= 2\alpha^3 + 6\alpha^2\beta + 6\alpha\beta^2 + 2\beta^3 - 4\alpha - 4\beta + 3 \\ &= 4\alpha + 12\beta + 6\alpha\beta^2 + 6 - 4\alpha - 4\beta + 3 \\ &= 6\alpha\beta^2 + 8\beta + 9 \end{aligned}$$

$$3\theta^2 + 2 = 3\alpha^2 + 6\alpha\beta + 3\beta^2 + 2 = 6 + 6\alpha\beta + 3\beta^2 + 2 = 6\alpha\beta + 8 + 3\beta^2 \text{ より}$$

$$\beta(3\theta^2 + 2) = 6\alpha\beta^2 + 8\beta + 9 = 2\theta(\theta^2-2)+3.$$

$$\text{ゆえに, } \frac{2\theta(\theta^2-2)+3}{3\theta^2+2} = \beta = \sqrt[3]{3}.$$

注意 以上の計算では $\alpha^2 = 2, \beta^3 = 3, \theta = \alpha + \beta$ のとき, $\frac{2\theta(\theta^2-2)+3}{3\theta^2+2} = \beta$

となることを示しているので、結論は $\alpha = \pm\sqrt{2}, \beta = \sqrt[3]{3}, \omega\sqrt[3]{3}, \omega^2\sqrt[3]{3}$ ($\omega = e^{2\pi i/3}$) の場合も成立している。

□

問題5-4の $\theta = \sqrt{2} + \sqrt[3]{3}$ を使う方針の場合の易しい別解

2021-11-12 追記

$$\alpha = \sqrt{2}, \beta = \sqrt[3]{3}, \alpha = 2, \beta = 3 \text{ とおくと, } \alpha^2 - \alpha = 0, \beta^3 - \beta = 0, \theta = \alpha + \beta \text{ とおく. }$$

$$\alpha = \theta - \beta \text{ より, } 0 = \alpha^2 - \alpha = \beta^2 - 2\theta\beta + \theta^2 - \alpha \text{ なので } \beta^2 = 2\theta\beta - \theta^2 + \alpha.$$

$$\text{ゆえに, } 0 = \beta^3 - \beta = \beta(2\theta\beta - \theta^2 + \alpha) - \beta = 2\theta\beta^2 + (-\theta^2 + \alpha)\beta - \beta$$

$$= \underbrace{2\theta(2\theta\beta - \theta^2 + \alpha)}_{= 4\theta^2\beta - 2\theta^3 + 2\alpha\theta} + (-\theta^2 + \alpha)\beta - \beta = (3\theta^2 + \alpha)\beta - (2\theta^3 - 2\alpha\theta + \beta).$$

$$\text{したがって, } \beta = \frac{2\theta^3 - 2\alpha\theta + \beta}{3\theta^2 + \alpha} \left(= \frac{2\theta(\theta^2 - \alpha) + \beta}{3\theta^2 + \alpha} = \frac{2\theta(\theta^2 - 2) + 3}{3\theta^2 + 2} \right),$$

前ページまでに紹介した計算とこれを比較してみよ.

$$\begin{array}{c} x^3 - p \\ \parallel \\ g(x) = (x+2\theta) h(x) \\ + \underbrace{(3\theta^2 + \alpha)x - (2\theta^3 - 2\alpha\theta + p)}_{\uparrow} \end{array}$$

Euclidの互除法より,
これが "g(x)" と "h(x)" の g.c.d. になる.

$$\begin{array}{ccc} \beta^2 - 2\theta\beta + \theta^2 - \alpha = 0 \text{ を使った計算} & & \\ 0 = \beta^3 - \beta & \swarrow & \\ \longleftrightarrow & & = (3\theta^2 + \alpha)\beta - (2\theta^3 - 2\alpha\theta + p) \\ & & \therefore \beta = \frac{2\theta^3 - 2\alpha\theta + p}{3\theta^2 + \alpha} \end{array}$$

これは易しい計算

最小多項式

<https://www.wolframalpha.com/input/?i=%E2%88%9A2%2B3%5E%281%2F3%29>

$$\sqrt{2+3^{1/3}}$$

Assuming the principal root | Use the real-valued root instead

Input

$$\sqrt{2} + \sqrt[3]{3}$$

Decimal approximation

2.8564631326805034311233270349898076669615411288762

More digits

Alternate form

root of $x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$ near $x = 2.85646$

Minimal polynomial

$$x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$$

$$\theta = \sqrt{2} + \sqrt[3]{3}$$

\mathbb{Q} 上で最小多項式は

$$x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$$



この根全体 \rightarrow 次ページへ

最小多項式の根の全体

[https://www.wolframalpha.com/input/?i=%28x-%28a%2Bb%29%29%28x-%28-a%2Bb%29%29%28x-%28a%2Bbc%29%29%28x-%28-a%2Bbc%29%29%28x-%28a%2Bbc%5E2%29%29%28x-%28-a%2Bbc%5E2%29%29+where+%7Ba%3D%E2%88%9A2%2C+b%3D3%5E%281%2F3%29%2C+c%3D%28-1%2B%E2%88%9A%28-3%29%29%29%2F2%7D&lang=ja](https://www.wolframalpha.com/input/?i=%28x-%28a%2Bb%29%29%28x-%28-a%2Bb%29%29%28x-%28a%2Bbc%29%29%28x-%28-a%2Bbc%29%29%28x-%28a%2Bbc%5E2%29%29%28x-%28-a%2Bbc%5E2%29%29+where+%7Ba%3D%E2%88%9A2%2C+b%3D3%5E%281%2F3%29%2C+c%3D%28-1%2B%E2%88%9A%28-3%29%29%2F2%7D&lang=ja)

Input interpretation

$$(x - (a + b))(x - (-a + b))(x - (a + bc))(x - (-a + bc))\left(x - \left(a + b c^2\right)\right)\left(x - \left(-a + b c^2\right)\right)$$

where $a = \sqrt{2}$, $b = \sqrt[3]{3}$, $c = \frac{1}{2}(-1 + \sqrt{-3})$

Result

$$\begin{aligned} & \left(x - \sqrt[3]{3} - \sqrt{2}\right) \left(x - \sqrt[3]{3} + \sqrt{2}\right) \left(x - \frac{1}{2} \sqrt[3]{3} (-1 + i\sqrt{3}) - \sqrt{2}\right) \\ & \left(x - \frac{1}{2} \sqrt[3]{3} (-1 + i\sqrt{3}) + \sqrt{2}\right) \left(x - \frac{1}{4} \sqrt[3]{3} (-1 + i\sqrt{3})^2 - \sqrt{2}\right) \left(x - \frac{1}{4} \sqrt[3]{3} (-1 + i\sqrt{3})^2 + \sqrt{2}\right) \end{aligned}$$

Expanded form

$$x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$$

$$\alpha = \sqrt{2}, \quad \beta = \sqrt[3]{3}, \quad \omega = e^{2\pi i / 3} = \frac{-1 + \sqrt{-3}}{2} \text{ のとき,}$$

$\theta = \alpha + \beta$ の \mathbb{Q} 上での最小多項式 $x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$ の根の全体は $\alpha + \beta, -\alpha + \beta, \alpha + \omega\beta, -\alpha + \omega\beta, \alpha + \omega^2\beta, -\alpha + \omega^2\beta$

になる。逆にこのことから、 θ の \mathbb{Q} 上での最小多項式が決まる。

单拡大定理の例

注 $\mathbb{Q}(\omega, \sqrt[3]{7}) \subsetneq \mathbb{Q}(\omega, \sqrt[3]{7})$ に注意

1 $\mathbb{Q}(\omega, \sqrt[3]{7}) = \mathbb{Q}(\omega + \sqrt[3]{7})$, ここで $\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}$,

$\omega + \sqrt[3]{7}$ の \mathbb{Q} 上での最小多項式は $x^6 + 3x^5 + 6x^4 - 7x^3 - 15x^2 + 24x + 64$.

<https://www.wolframalpha.com/input/?i=%28x-%28w%2Ba%29%29%28x-%28w%5E2%2Ba%29%29%28x-%28w%2Bwa%29%29%28x-%28w%5E2%2Bwa%29%29%28x-%28w%2Bw%5E2a%29%29+where+%7Ba%3D7%5E%281%2F3%29%2C+w%3D%28-1%2B%2888%9A%28-3%29%29%2F2%7D&lang=ja>



<https://www.wolframalpha.com/input/?i=Is+64+24+x+-+15+x%5E2+-+7+x%5E3+%2B+6+x%5E4+%2B+3+x%5E5+%2B+x%5E6+irreducible%3F&lang=ja>



Input interpretation

$$(x - (w + a))(x - (w^2 + a))(x - (w + w a))(x - (w^2 + w a))(x - (w + w^2 a))(x - (w^2 + w^2 a)) \text{ where } a = \sqrt[3]{7}, w = \frac{1}{2}(-1 + \sqrt{-3})$$

Result

$$\begin{aligned} & \left(x + \frac{1}{2}(1 - i\sqrt{3}) - \sqrt[3]{7}\right) \left(x - \frac{1}{2}\sqrt[3]{7}(-1 + i\sqrt{3}) + \frac{1}{2}(1 - i\sqrt{3})\right) \\ & \left(x - \frac{1}{4}(-1 + i\sqrt{3})^2 - \sqrt[3]{7}\right) \left(x - \frac{1}{4}(-1 + i\sqrt{3})^2 - \frac{1}{2}\sqrt[3]{7}(-1 + i\sqrt{3})\right) \\ & \left(x - \frac{1}{4}\sqrt[3]{7}(-1 + i\sqrt{3})^2 + \frac{1}{2}(1 - i\sqrt{3})\right) \left(x - \frac{1}{4}\sqrt[3]{7}(-1 + i\sqrt{3})^2 - \frac{1}{4}(-1 + i\sqrt{3})^2\right) \end{aligned}$$

Expanded form

$$x^6 + 3x^5 + 6x^4 - 7x^3 - 15x^2 + 24x + 64$$

Is $64 + 24 x - 15 x^2 - 7 x^3 + 6 x^4 + 3 x^5 + x^6$ irreducible?

Input

IrreduciblePolynomialQ[64 + 24 x - 15 x^2 - 7 x^3 + 6 x^4 + 3 x^5 + x^6]

Result

True

つづく

$$\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}, \quad \alpha = \sqrt[3]{7}, \quad \theta = \omega + \alpha \text{ とおく。}$$

$$F_\omega(x) = x^2 + x + 1, \quad F_\alpha(x) = x^3 - 7,$$

$$G(x) = F_\omega(\theta - x) = (x - \theta)^2 + (\theta - x) + 1 = x^2 - (2\theta + 1)x + \theta^2 + \theta + 1 \quad \text{とおく。}$$

$$\begin{aligned} & \gcd(G(x), F_\alpha(x)) \\ &= x - \sqrt[3]{7} = x - \frac{(2\theta+1)(\theta^2+\theta+1)+7}{3\theta(\theta+1)} \\ & \sqrt[3]{7} = \frac{(2\theta+1)(\theta^2+\theta+1)+7}{3\theta(\theta+1)} \end{aligned}$$

$$\begin{array}{r} x + (2\theta+1) \\ \hline x^3 - (2\theta+1)x^2 + (\theta^2+\theta+1)x \\ \hline (2\theta+1)x^2 - (\theta^2+\theta+1)x - 7 \\ \hline (2\theta+1)x^2 - (2\theta+1)^2 x + (2\theta+1)(\theta^2+\theta+1) \\ \hline 3\theta(\theta+1)x - ((2\theta+1)(\theta^2+\theta+1)+7) \end{array}$$

<https://www.wolframalpha.com/input/?i=%28t%2B1%29%28t%5E2%2B1%29%2B7%29%2F%283t%2B1%29+where+t%3D%28-1%2B%28-3%29%29%2F2%2B7%281%2B3%29%29%7D&lang=ja>

Input interpretation

$$\frac{(2t+1)(t^2+t+1)+7}{3t(t+1)} \text{ where } t = \frac{1}{2}(-1 + \sqrt{-3}) + \sqrt[3]{7}$$

Result

$$\frac{7 + \left(1 + 2\left(\sqrt[3]{7} + \frac{1}{2}(-1 + i\sqrt{3})\right)\right)\left(1 + \sqrt[3]{7} + \frac{1}{2}(-1 + i\sqrt{3}) + \left(\sqrt[3]{7} + \frac{1}{2}(-1 + i\sqrt{3})\right)^2\right)}{3\left(\sqrt[3]{7} + \frac{1}{2}(-1 + i\sqrt{3})\right)\left(1 + \sqrt[3]{7} + \frac{1}{2}(-1 + i\sqrt{3})\right)}$$

Alternate forms

$$\sqrt[3]{7}$$

手書き
のとき、

$$\frac{(2\theta+1)(\theta^2+\theta+1)+7}{3\theta(\theta+1)} = \sqrt[3]{7}$$

$$\theta = \omega + \sqrt[3]{7}, \quad \omega = e^{2\pi i/3}$$

2 $\mathbb{Q}(\omega, \sqrt[3]{7}) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{7}) = \mathbb{Q}(\sqrt{-3} + \sqrt[3]{7})$ ($\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}$) である。

$\sqrt{-3} + \sqrt[3]{7}$ の \mathbb{Q} 上での最小多項式は $x^6 + 9x^4 - 14x^3 + 27x^2 + 126x + 76$

<https://www.wolframalpha.com/input/?i=%28x-%28v%2Ba%29%29%28x-%28-v%2Ba%29%29%28x-%28v%2Bw%29%28x-%28-v%2Bw%5E2a%29%29%28x-%28-v%2Bw%5E2a%29%29%20where%20%7Ba%3D7%5E%281%2F3%29%2C%20v%3D%28%2F88%9A%28-3%29%2C%20w%3D%28-1%2Bv%29%2F2%7D>



https://www.wolframalpha.com/input/?i=Is+76+126*x+27*x^2-14*x^3+9*x^4+x^6+irreducible



Input interpretation

$$(x - (v + a))(x - (-v + a))(x - (v + w a))(x - (-v + w a))(x - (v + w^2 a))(x - (-v + w^2 a)) \text{ where } a = \sqrt[3]{7}, v = \sqrt{-3}, w = \frac{1}{2}(-1 + \nu)$$

Result

$$\begin{aligned} & \left(x - \sqrt[3]{7} - i\sqrt{3}\right) \left(x - \sqrt[3]{7} + i\sqrt{3}\right) \left(x - \frac{1}{2}\sqrt[3]{7}(-1 + i\sqrt{3}) - i\sqrt{3}\right) \\ & \left(x - \frac{1}{2}\sqrt[3]{7}(-1 + i\sqrt{3}) + i\sqrt{3}\right) \left(x - \frac{1}{4}\sqrt[3]{7}(-1 + i\sqrt{3})^2 - i\sqrt{3}\right) \left(x - \frac{1}{4}\sqrt[3]{7}(-1 + i\sqrt{3})^2 + i\sqrt{3}\right) \end{aligned}$$

Expanded form

$$x^6 + 9x^4 - 14x^3 + 27x^2 + 126x + 76$$

Is $76 + 126 x + 27 x^2 - 14 x^3 + 9 x^4 + x^6$ irreducible?

Input

IrreduciblePolynomialQ[76 + 126 x + 27 x^2 - 14 x^3 + 9 x^4 + x^6]

Result

True

つづく

$\alpha = \sqrt[3]{7}$, $\beta = \sqrt{-3}$, $\gamma = \beta + \alpha$ とおく。

$$F_\beta(x) = x^2 + 3, \quad F_\alpha(x) = x^3 - 7.$$

$$H(x) = F_\beta(\gamma - x) = (x - \gamma)^2 + 3 = x^2 - 2\gamma x + \gamma^2 + 3 \text{ とおく。}$$

$$\gcd(H(x), F_\alpha(x)) = x - \sqrt[3]{7}$$

$$= x - \frac{2\gamma(\gamma^2 + 3) + 7}{3(\gamma^2 - 1)}$$

$$\sqrt[3]{7} = \frac{2\gamma(\gamma^2 + 3) + 7}{3(\gamma^2 - 1)}.$$

$$\begin{array}{r}
 x + 2\gamma \\
 \hline
 x^2 - 2\gamma x + \gamma^2 + 3 \quad | \quad -7 \\
 \hline
 x^3 - 2\gamma x^2 + (\gamma^2 + 3)x \\
 \hline
 2\gamma x^2 - (\gamma^2 + 3)x - 7 \\
 \hline
 2\gamma x^2 - 4\gamma^2 x + 2\gamma(\gamma^2 + 3) \\
 \hline
 3(\gamma^2 - 1)x - (2\gamma(\gamma^2 + 3) + 7)
 \end{array}$$

<https://www.wolframalpha.com/input/?i=%28t%28t%5E2+3%29+7%29%2F%283%28t%5E2-1%29%29+where+t%3D%28%2B%28-3%29%2B7%29%28t%5E2+1%29%29%29&lang=ja>

Input interpretation

$$\frac{2t(t^2 + 3) + 7}{3(t^2 - 1)} \text{ where } t = \sqrt{-3} + \sqrt[3]{7}$$

Result

$$\frac{7 + 2(\sqrt[3]{7} + i\sqrt{3})(3 + (\sqrt[3]{7} + i\sqrt{3})^2)}{3(-1 + (\sqrt[3]{7} + i\sqrt{3})^2)}$$

Alternate forms

$$\sqrt[3]{7}$$

等しい

$\gamma = \sqrt{-3} + \sqrt[3]{7}$ のとき、

$$\frac{2\gamma(\gamma^2 + 3) + 7}{3(\gamma^2 - 1)} = \sqrt[3]{7}$$

3 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ である. $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$, $\theta = \alpha + \beta$ とおく. 特別に易い場合

$$F_\alpha(x) = x^2 - 2, \quad F_\beta(x) = x^2 - 3. \quad G(x) = F_\alpha(\theta - x) = x^2 - 2\theta x + \theta^2 - 2 \text{ とおく,}$$

$$\gcd(G(x), F_\beta(x)) = x - \sqrt{3}.$$

$$\begin{array}{c} 1 \\ x^2 - 2\theta x + \theta^2 - 2 \longdiv{x^2 \quad -3} \\ \underline{x^2 - 2\theta x + \theta^2 - 2} \\ 2\theta x - (\theta^2 + 1) \end{array} \quad F_\beta(x) = G(x) + 2\theta \left(x - \frac{\theta^2 + 1}{2\theta} \right)$$

$$\gcd(G(x), F_\beta(x)) = x - \frac{\theta^2 + 1}{2\theta}$$

$$\text{ゆえに, } \sqrt{3} = \frac{\theta^2 + 1}{2\theta}.$$

$$\left(\text{確認} \quad \frac{1}{\theta} = \frac{1}{\sqrt{3} + \sqrt{2}} = \sqrt{3} - \sqrt{2}, \quad \frac{\theta^2 + 1}{2\theta} = \frac{1}{2} \left(\theta + \frac{1}{\theta} \right) = \frac{1}{2} \left(\sqrt{3} + \sqrt{2} + \sqrt{3} - \sqrt{2} \right) = \sqrt{3} \right)$$

$\theta = \sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上での最小多項式:

$$\begin{aligned} F_\theta(x) &= (x - (\sqrt{2} + \sqrt{3}))(x - (-\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x - (-\sqrt{2} - \sqrt{3})) \\ &= ((x + \sqrt{3})^2 - 2)((x - \sqrt{3})^2 - 2) = (x^2 + 2\sqrt{3}x + 1)(x^2 - 2\sqrt{3}x + 1) \\ &= (x^2 + 1)^2 - (2\sqrt{3}x)^2 = x^4 + 2x^2 + 1 - 12x = x^4 - 10x + 1. \end{aligned}$$
□

4 $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{2} + \sqrt[3]{3})$ である, $\alpha = \sqrt[3]{2}$, $\beta = \sqrt[3]{3}$, $\theta = \alpha + \beta$ とおく.

$F_\alpha(x) = x^3 - 2$, $F_\beta(x) = x^3 - 3$ とおく.

$G(x) = -F_\alpha(\theta - x) = (x - \theta)^3 + 2 = x^3 - 3\theta x^2 + 3\theta^2 x - \theta^3 + 2$ とおく.

$\gcd(G(x), F_\beta(x)) = x - \beta$ となることを示せる (共通根は β だけ), ← 自分で示せ.

$H(x) = F_\beta(x) - G(x) = 3\theta x^2 - 3\theta^2 x + \theta^3 - 5$ とおく,

$$\begin{array}{r} x - 2\theta \\ \hline 3\theta x^2 - 3\theta^2 x + \theta^3 - 5 \end{array} \left| \begin{array}{r} 3\theta G(x) \\ 3\theta x^3 - 9\theta^2 x^2 + 9\theta^3 x - 3\theta^4 + 6\theta \\ \hline 3\theta x^3 - 3\theta^2 x^2 + (\theta^3 - 5)x \\ -6\theta^2 x^2 + (8\theta^3 + 5)x - 3\theta^4 + 6\theta \\ -6\theta^2 x^2 + 6\theta^3 \end{array} \right. \begin{array}{l} \text{---} \\ \text{---} \\ \text{---} \\ (2\theta^3 + 5)x - (\theta^4 + 4\theta) \end{array}$$

H(x)

$R(x) = 3\theta G(x) - (x - 2\theta)H(x) = (2\theta^3 + 5)x - (\theta^4 + 4\theta)$ とおく,

$$\therefore x - \beta = \gcd(G(x), H(x)) = \frac{R(x)}{2\theta^3 + 5} = x - \frac{\theta(\theta^3 + 4)}{2\theta^3 + 5}, \quad \begin{array}{c} \nearrow \\ a=2, p=3 \end{array}$$

$$\therefore \boxed{\frac{\theta(\theta^3 + 4)}{2\theta^3 + 5}} = \beta.$$

これより, $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \beta)$ であることがわかる.

```
In [23]: f = x^3 - a
g = x^3 - p
displayresults(z, x, f, g)
```

0.034458 seconds (430.12 k allocations: 27.470 MiB, 32.49% gc time)

$$F_\alpha(x) = x^3 - a$$

$$F_\beta(x) = x^3 - p$$

$$R_{\alpha+\beta}(z) = z^9 + (-3a - 3p)z^6 + (3a^2 - 21ap + 3p^2)z^3 - a^3 - 3a^2p - 3ap^2 - p^3$$

$$R_{\alpha+\beta}(\alpha + \beta) = 0$$

$$\beta_{\text{plus}}(z) = \frac{z^4 + (-a + 2p)z}{2z^3 + a + p}$$

$$\beta_{\text{plus}}(\alpha + \beta) = \beta \text{ is true}$$

$$R_{\alpha\beta}(z) = z^9 - 3apz^6 + 3a^2p^2z^3 - a^3p^3$$

$$R_{\alpha\beta}(\alpha\beta) = 0$$

$$\beta_{\text{mult}}(z) = -1$$

$$\beta_{\text{mult}}(\alpha\beta) = \beta \text{ is false}$$

$$1\text{-subresultant} = (6z^4 + (3a + 3p)z)x - 3z^5 + (3a - 6p)z^2$$

$$\text{root of 1-subresultant} = \frac{z^4 + (-a + 2p)z}{2z^3 + a + p}$$

$$\frac{\theta(\theta^3+4)}{2\theta^3+5} = \beta \text{ の確定:}$$

$$(\text{分母}) = 2\theta^3 + 5 = 6\alpha^2\beta + 6\alpha\beta^2 + \underbrace{15}_{\substack{\nearrow 2(2+3)+5}}$$

$$(\text{分母}) \times \beta = 6\alpha^2\beta^2 + 18\alpha + 15\beta$$

$$\begin{aligned} (\text{分子}) &= \theta(\theta^3+4) = (\alpha+\beta)(3\alpha^2\beta + 3\alpha\beta^2 + 9) \\ &= 6\beta + 3\alpha^2\beta^2 + 9\alpha + 3\alpha^2\beta^2 + 9\alpha + 9\beta \\ &= 6\alpha^2\beta^2 + 18\alpha + 15\beta = (\text{分母}) \times \beta. \end{aligned}$$

$$\therefore \frac{\theta(\theta^3+4)}{2\theta^3+5} = \beta.$$

$\sqrt[3]{2}, \sqrt[3]{3}$
 $\parallel \quad \parallel$

$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 9$ を別に示せるので、 θ の \mathbb{Q} 上での最小多項式は 9 次になる。

$$\theta^3 = \alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + \beta^3 = 3\alpha^2\beta + 3\alpha\beta^2 + 5 = 3\alpha\beta\theta + 5,$$

$$3\alpha\beta\theta = \theta^3 - 5 \text{ の両辺を 3 乗すると } \underbrace{162\theta^3}_{\substack{\nearrow 3^3 \cdot 2 \cdot 3}} = \theta^9 - 15\theta^6 + 75\theta^3 - 125.$$

すなわち、 $\boxed{\theta^9 - 15\theta^6 - 87\theta^3 - 125 = 0.}$

$3^3 \cdot 2 \cdot 3 = 2 \cdot 3^4 = 2 \cdot 81 = 162$

ゆえに、 θ の \mathbb{Q} 上での最小多項式は $F_\theta(x) = x^9 - 15x^6 - 87x^3 - 125$.

□

終結式との関係 (この説明については理解できなくてよい。)

多項式 $f(x) = \sum_{i=0}^m a_i x^i$ と $g(x) = \sum_{j=0}^n b_j x^j$ に対して、 $(m+n) \times (m+n)$ の行列式で

$$\text{res}_x(f, g) = \begin{vmatrix} a_m & \cdots & a_1, a_0 \\ & \ddots & \vdots \\ & a_m & \cdots & a_1, a_0 \\ b_n & \cdots & b_1, b_0 \\ & \ddots & \vdots \\ b_n & \cdots & b_1, b_0 \end{vmatrix}_{\substack{n \\ m}}$$

と定義される $\text{res}_x(f, g)$ を f と g の
resultant

例 $f(x) = ax^2 + bx + c$
 $g(x) = px^2 + qx + r$
 のとき,

$$\text{res}_x(f, g) = \begin{vmatrix} a & b & c & 0 \\ 0 & a & b & c \\ p & q & r & 0 \\ 0 & p & q & r \end{vmatrix}$$

(Sylvesterの) 終結式と呼ぶ。 $f(x) = a_m \prod_{i=1}^m (x - \alpha_i)$, $g(x) = b_n \prod_{j=1}^n (x - \beta_j)$ のとき,

$$(*) \quad \text{res}_x(f, g) = a_m^n b_n^m \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j). \quad \leftarrow \text{証明は佐武一郎『線型代数学』の}\text{pp.70-74にある。}$$

これより、 z の多項式 $h(z)$ を $h(z) = \text{res}_x(f(z-x), g(x))$ と定めると、

$h(\alpha_1 + \beta_1) = 0$ が成立する。

(*) をみとめれば「証明は易しいので挑戦してみよ」

$\deg h(z) = mn$ となることを示せる。

これらの結果は $\alpha_1 + \beta_1$ の最小多項式を求めるために役に立つ。

$f(x), g(x)$ の係数は不定元であると仮定する. ← 簡単のための仮定

$\alpha_1 + \beta_1$ の有理式で β_1 になるものは $f(z-x)$ と $g(x)$ の 1 次の部分終結式の根として得られる. $f(x)$ と $g(x)$ の k 次の部分終結式は次のように定義される.

$$S_k^x(f, g) := \begin{vmatrix} a_m & \cdots & a_{1+k-(n-k-1)} & x^{n-k-1} f(x) \\ & \ddots & \vdots & \vdots \\ a_m & \cdots & a_{1+k} & f(x) \\ b_n & \cdots & b_{1+k-(m-k-1)} & x^{m-k-1} g(x) \\ & \ddots & \vdots & \vdots \\ b_n & \cdots & b_{1+k} & g(x) \end{vmatrix}$$

(m+n-2k) × (m+n-2k)
の行列式
(これは x について
 k 次以下にくる)
← 注 $S_0^x(f, g) = \text{res}_x(f, g)$
となることを示せる.
自分で示してみよ.

たとえば $f(x) = ax^2 + bx + c$, $g(x) = px^3 + qx^2 + rx + s$ のとき,

$$S_1^x(f, g) = \begin{vmatrix} a & b & xf(x) \\ 0 & a & f(x) \\ p & q & g(x) \end{vmatrix} = \begin{vmatrix} a & b & ax^3 + bx^2 + cx \\ 0 & a & ax^2 + bx + c \\ p & q & px^3 + qx^2 + rx + s \end{vmatrix} = \begin{vmatrix} a & b & cx \\ 0 & a & bx + c \\ p & q & rx + s \end{vmatrix}.$$

x^2 倍してく
 x^3 倍してく

$S_1^x(f(z-x), g(x))$ は 2 の多項式を係数とする x の 1 次式になり,

その根として得られる 2 の有理函数に $\alpha_1 + \beta_1$ を代入すると値は β_1 になる

```
In [13]: f = x^2 - a
g = x^3 - p
dispallresults(z, x, f, g)
subresultant(f(z-x), g, 1) |> rootdeg1 |> rhs -> dispseq("\text{root of 1-subresultant}", rhs)
```

0.057067 seconds (201.86 k allocations: 12.256 MiB, 28.52% gc time, 83.09% compilation time)

$$F_\alpha(x) = x^2 - a$$

$$F_\beta(x) = x^3 - p$$

$$R_{\alpha+\beta}(z) = z^6 - 3az^4 - 2pz^3 + 3a^2z^2 - 6apz - a^3 + p^2$$

$$R_{\alpha+\beta}(\alpha + \beta) = 0$$

$$\beta_{\text{plus}}(z) = \frac{2z^3 - 2az + p}{3z^2 + a}$$

$$\beta_{\text{plus}}(\alpha + \beta) = \beta \text{ is true}$$

$$R_{\alpha\beta}(z) = z^6 - a^3p^2$$

$$R_{\alpha\beta}(\alpha\beta) = 0$$

$$\beta_{\text{mult}}(z) = \frac{ap}{z^2}$$

$$\beta_{\text{mult}}(\alpha\beta) = \beta \text{ is true}$$

$$\text{root of 1-subresultant} = \frac{2z^3 - 2az + p}{3z^2 + a}$$

$$f(z-x) = x^2 - 2zx + z^2 - a \text{ より}$$

$$S_1(f(z-x), g(x)) = \begin{vmatrix} 1 & -2z & (z^2-a)x \\ 0 & 1 & -2zx + z^2 - a \\ 1 & 0 & -p \end{vmatrix} = (3z^2+a)x - (2z^3 - 2az + p)$$

参考

$$F_\alpha(\alpha) = 0, \text{ i.e., } \alpha^2 = a,$$

$$F_\beta(\beta) = 0, \text{ i.e., } \beta^3 = p \text{ とすると,}$$

$$R_{\alpha+\beta}(\alpha + \beta) = 0 \text{ かつ}$$

$$\beta_{\text{plus}}(\alpha + \beta) = \beta \text{ となる.}$$

$$\text{特に } a=2, b=3 \text{ のとき,}$$

$$\begin{aligned} \beta_{\text{plus}}(z) &= \frac{2z^3 - 4z + 3}{3z^2 + 2} \\ &= \frac{2z(z^2 - 2) + 3}{3z^2 + 2} \end{aligned}$$

問題5-4の
場合

Galois 拡大について

06-4.

以下, K, L, M, \dots は \mathbb{C} の部分体であると仮定する. ← 簡単のための仮定

(注) 以下の内容は 擇数 0 の場合一般にも通用する.)

L/K は 有限次拡大であると仮定する. ←

L の K 上でのベクトル空間としての基底を $\alpha_1, \dots, \alpha_n$ と書くと,
各 α_i は K 上代数的かつ $L = K\alpha_1 \oplus \dots \oplus K\alpha_n = K(\alpha_1, \dots, \alpha_n)$ が成立しているので,
单拡大定理より, $L = K(\theta)$, $\theta \in L$ と書ける. このとき, 次のように定める.

定義. L/K が (有限次) Galois 拡大 であるとは以下の同値な条件の

どれかが成立していることだと定める:

(1) L の K 上での任意の共役体は L に等しい.

(注) ψ は 单射 だが
全射 とは限らない.)

(K 上での任意の体の同型 $\psi: L \hookrightarrow \mathbb{C}$ について $\psi(L) = L$.)

($\psi: L \rightarrow \mathbb{C}$ は 環の準同型(体の準同型, 单射になる)で $\psi(a) = a$ ($a \in K$ をみたすもの))

(2) θ の K 上での任意の共役元は L に含まれる.

(θ の K 上での最小多項式のすべての根が L に含まれる.)

□

さらに次の条件も(1), (2)と同値である:

(3) ある $F(x) \in K[x]$ が存在して, L は $F(x)$ の最小分解体になる。
(L は K に $F(x)$ のすべての根を付け加えてできる体になる.)

以下において, (1), (2), (3) の同値性と次の定理をまとめさせてよい.

定理 以上の記号のもとで, L/K は有限次 Galois 拡大であるとし,
 $\theta \in L$ で $L = K(\theta)$ をみたすものと取るとき, 次の写像は全単射になる:

$$\text{Gal}(L/K) = \left\{ K \text{上で} \text{の} \text{体} L \text{の自己同型全体} \right\} \xrightarrow{\text{定義}} \left\{ \theta \text{の} K \text{上で} \text{の} \text{共役元全体} \right\}, \sigma \mapsto \sigma(\theta).$$

このことから, $|\text{Gal}(L/K)| = (\theta \text{の} K \text{上で} \text{の} \text{共役元の個数}) = [L : K]$ が得られる. \square

問題 6-1 K, L は \mathbb{C} の部分体であるとし, L/K は有限次拡大であるとする.

このとき, L/K が Galois 拡大であることと次の条件 (4) が同値であることを示せ.

(4) 任意の $\alpha \in L$ について, α の K 上での任意の共役元が L に含まれる. \square

④ (4) は (2) より強い: (4) \Rightarrow (2) は自明. (1), (2), (3) \Rightarrow (4) を示せ.

問題 6-2 M/K は体の拡大であるとし, L_1, L_2 はその中間体であるとする.

このとき, $L_1/K, L_2/K$ が有限次拡大ならば $L_1 \cap L_2/K$ も $L_1 L_2/K$ も有限次拡大になり,

$$[L_1 \cap L_2 : K] \leq \min\{[L_1 : K], [L_2 : K]\}, \quad [L_1 L_2 : K] \leq [L_1 : K][L_2 : K]$$

となることを示せ.

ここで $L_1 L_2$ は L_1 と L_2 の両方を含む M の最小の部分体を表す (L_1, L_2 は合成体). \square

問題 6-3 K, L_1, L_2 は \mathbb{C} の部分体であるとする.

L_1/K と L_2/K が有限次 Galois 拡大ならば

$L_1 \cap L_2/K$ と $L_1 L_2/K$ も有限次 Galois 拡大になることを示せ.

ここで $L_1 L_2$ は L_1 と L_2 の両方を含む \mathbb{C} の最小の部分体を表す. \square

問題 6-4 以下の体の拡大が Galois 拡大であるかどうかを判定せよ.

- (1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, (2) $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$, (3) $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$,
(4) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, (5) $\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})/\mathbb{Q}$, (6) $\mathbb{Q}(\sqrt[4]{7}, \sqrt{-1})/\mathbb{Q}$,
(7) $\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})/\mathbb{Q}(\sqrt{-3})$, (8) $\mathbb{Q}(\sqrt[4]{7}, \sqrt{-1})/\mathbb{Q}(\sqrt{-1})$.

これが
もとも
易しい
はず

問題6-1 K, L は \mathbb{C} の部分体であるとし, L/K は有限次拡大であるとする.

このとき, L/K が Galois 拡大であることと次の条件 (4) が同値であることを示せ.

(4) 任意の $\alpha \in L$ について, α の K 上でのすべての共役元が L に含まれる.

解答例

① (4) $\Rightarrow L/K$ は Galois 拡大を示そう.

(4) の条件における α として, $L = K(\theta)$ をみたす $\theta \in L$ をとると,

(4) より θ のすべての共役元は L に含まれる. これより, L/K は Galois 拡大である.

注 以下の条件は 有限次拡大 ($\text{次数} n$) L/K が Galois 拡大であることを特徴づける互いに同値な条件になっている:

(1) L の K 上での任意の共役体は L に等しい.

(K 上での任意の体の同型 $\varphi: L \hookrightarrow \mathbb{C}$ について $\varphi(L) = L$.)

(2) θ の K 上での任意の共役元は L に含まれる. $\leftarrow L = K(\theta)$ と仮定している.

(θ の K 上での最小多項式のすべての根が L に含まれる.)

(3) ある $F(x) \in K[x]$ が存在して, L は $F(x)$ の K 上での最小分解体になる.

(L は K に $F(x)$ のすべての根を付け加えてできる体になる.)

② L/K が Galois 拡大 $\Rightarrow (4)$ を示す.

L/K は Galois 拡大であるとし、任意に $\alpha \in L$ をとる。

$\beta \in \mathbb{C}$ は K 上での α の任意の共役元であるとする。

(4) を示すためには $\beta \in L$ を示せばよい。

$$\left\{ \begin{array}{l} K(\alpha) \cong K[x]/(F_\alpha(x)) \cong K(\beta) \\ (F_\alpha(x) \text{ は } \alpha \text{ の } K \text{ 上での最小多項式}) \\ (\beta \text{ は } F_\alpha(x) \text{ の根}) \end{array} \right.$$

このとき、 K 上の体同型 $\psi: K(\alpha) \hookrightarrow \mathbb{C}, f(\alpha) \mapsto f(\beta) \quad (f(x) \in K[x])$ が存在する。

もしも $K(\alpha) = L$ ならば L/K が Galois 拡大であることより、 $L = \psi(L) = \psi(K(\alpha)) = K(\beta) \ni \beta$.

$K(\alpha) \subsetneq L$ と仮定する。单拡大定理より、 $L = K(\alpha)(\theta), \theta \in L$ と書ける。

θ の $K(\alpha)$ 上での最小多項式を $F(x) = \sum_i a_i x^i \in K(\alpha)[x], a_i \in K(\alpha)$ と書く。

$G(x) = \sum_i \psi(a_i) x^i \in \psi(K[\alpha])[x] = K(\beta)[x]$ と書き、 $G(x)$ の根 $\eta \in \mathbb{C}$ を任意にとる。

このとき、 K 上の体の同型 $\tilde{\psi}: L \hookrightarrow \mathbb{C}$ を $\tilde{\psi}\left(\sum_i b_i \theta^i\right) = \sum_i \psi(b_i) \eta^i \quad (b_i \in K(\alpha))$ と作れる：

$$L = K(\alpha)(\theta) \cong K(\alpha)[x]/(F(x)) \cong K(\beta)[x]/(G(x)) \cong K(\beta)(\eta) \subset \mathbb{C}$$

$$\sum a_i \theta^i \leftrightarrow \overline{\sum a_i x^i} \leftrightarrow \overline{\sum \psi(a_i) x^i} \leftrightarrow \sum \psi(a_i) \eta^i.$$

L/K が Galois 拡大であることより、 $L = \tilde{\psi}(L) = K(\beta)(\eta) \ni \beta$.

これで (4) が示された。 □

問題 6-2 M/K は体の拡大であるとし, L_1, L_2 はその中間体であるとする.

このとき, $L_1/K, L_2/K$ が有限次拡大ならば $L_1 \cap L_2/K$ も $L_1 L_2/K$ も有限次拡大になり,

$$[L_1 \cap L_2 : K] \leq \min\{[L_1 : K], [L_2 : K]\}, \quad [L_1 L_2 : K] \leq [L_1 : K][L_2 : K]$$

となることを示せ.

ここで $L_1 L_2$ は L_1 と L_2 の両方を含む M の最小の部分体を表す. \square

解答例 $[L_1 : K] = m < \infty, [L_2 : K] = n < \infty$ と仮定する.

① $[L_1 \cap L_2 : K] \leq \min\{m, n\}$ を示す.

$L_1 \cap L_2 \subset L_1$ より, $[L_1 \cap L_2 : K] = \dim_K L_1 \cap L_2 \leq \dim_K L_1 = m$.

$L_1 \cap L_2 \subset L_2$ より, $[L_1 \cap L_2 : K] = \dim_K L_1 \cap L_2 \leq \dim_K L_2 = n$.

ゆえに, $[L_1 \cap L_2 : K] \leq \min\{m, n\}$,

2 $[L_1 L_2 : K] \leq mn$ を示す.

单拡大定理より, K 上代数的なある $\theta \in L_1$ が存在して, $L_1 = K(\theta)$ となる.

$L_1 L_2$ は L_2 と θ を含むので, $L_2(\theta)$ の最小性より $L_2(\theta) \subset L_1 L_2$.

任意の $\beta \in L_1 = K(\theta)$ はある $f(x) \in K[x]$ によって $\beta = f(\theta)$ と表わされ,

$f(x) \in L_2[x]$ もあるので $\beta = f(\theta) \in L_2(\theta)$ となり, $L_2(\theta)$ は L_1 と L_2 の商である. ゆえに, $L_1 L_2$ の最小性より, $L_1 L_2 \subset L_2(\theta)$.

これで, $L_1 L_2 = L_2(\theta)$ となることが示された.

$F_\theta(x) \in K[x]$ を θ の K 上での最小多項式とすると, $F_\theta(x) \in L_2[x]$ もかつ $F_\theta(\theta) = 0$ となるので,

$$[L_1 L_2 : L_2] = [L_2(\theta) : L_2] = (\theta \text{ の } L_2 \text{ 上での最小多項式の次数})$$

$$\leq \deg F_\theta(x) = [K(\theta) : K] = [L_1 : K].$$

ゆえに,

$$[L_1 L_2 : K] = [L_1 L_2 : L_2] [L_2 : K] \leq [L_1 : K] [L_2 : K] = mn.$$

(注) $[L : K]$ は
 $[L/K] \geq$
零くこともある.) □

問題 6-3 K, L_1, L_2 は \mathbb{C} の部分体であるとする。

L_1/K と L_2/K が有限次 Galois 拡大ならば、

$L_1 \cap L_2/K$ と $L_1 L_2/K$ も有限次 Galois 拡大になることを示せ。

ここで $L_1 L_2$ は L_1 と L_2 の両方を含む \mathbb{C} の最小の部分体を表す。 \square

解答例 $L_1 \cap L_2/K$ と $L_1 L_2/K$ が有限次拡大になることは問題 6-2 の解答例で示した。

① $L_1 \cap L_2/K$ が Galois 拡大になることを示そう。

$\alpha \in L_1 \cap L_2$ を任意にとる。

$i = 1, 2$ について、 L_i/K が Galois 拡大であること

問題 6-1 の結果と $\alpha \in L_i$ より、 α のすべての K 上での共役元は L_i に含まれる。

ゆえに、 α のすべての K 上での共役元は $L_1 \cap L_2$ に含まれる。

したがって、問題 6-1 の結果より、 $L_1 \cap L_2/K$ は Galois 拡大である。

② $L_1 L_2 / K$ が Galois 拡大になることを示す。

L_1, L_2 の任意の元 γ は、ある $\alpha_1, \dots, \alpha_r \in L_1, \beta_1, \dots, \beta_s \in L_2$ と $f(x_1, \dots, x_r, y_1, \dots, y_s) \in K(x_1, \dots, x_r, y_1, \dots, y_s)$ が存在して、
 $\gamma = f(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$ と表される。

このとき、 K 上の体同型 $\varphi: L_1 L_2 \hookrightarrow \mathbb{C}$ について、
その L_k 上への制限が K 上の体同型になると、 L_k / K が Galois 拡大であることより、
 $\varphi(\alpha_i) \in L_1, \varphi(\beta_j) \in L_2$ となる。ゆえに、

$$\varphi(\gamma) = f(\varphi(\alpha_1), \dots, \varphi(\alpha_r), \varphi(\beta_1), \dots, \varphi(\beta_s)) \in L_1 L_2.$$

これで $L_1 L_2 / K$ が Galois 拡大であることがわかった。 \square

(注) 上で $\varphi(L_1 L_2) \subset L_1 L_2$ が示せており、 $L_1 L_2$ と $\varphi(L_1 L_2)$ の K 上のベクトル空間としての次元は有限次元で等しいので $\varphi(L_1 L_2) = L_1 L_2$ 。

問題 6-4 以下の体の拡大が Galois 拡大であるかどうかを判定せよ.

- (1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$,
- (2) $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$,
- (3) $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$,
- (4) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$,
- (5) $\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})/\mathbb{Q}$,
- (6) $\mathbb{Q}(\sqrt[4]{7}, \sqrt{-1})/\mathbb{Q}$,
- (7) $\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})/\mathbb{Q}(\sqrt{-3})$,
- (8) $\mathbb{Q}(\sqrt[4]{7}, \sqrt{-1})/\mathbb{Q}(\sqrt{-1})$.

解答例 (1), (4), (5), (6), (7), (8) は Galois 拡大た"か, (2), (3) はそぞれ はない,

$$\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}, \quad i = \sqrt{-1} \text{ とおく.}$$

$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, $\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3}) = \mathbb{Q}(\sqrt[3]{3}, \omega)$, $\mathbb{Q}(\sqrt[4]{7}, \sqrt{-1})$ はそれぞれ

$x^2 - 2$, $x^4 - 10x^2 + 1$ $x^3 - 3$ $x^4 - 7$ の \mathbb{Q} 上での

最小分解体なので \mathbb{Q} の Galois 拡大である.

$\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3}) = \mathbb{Q}(\sqrt[3]{3}, \omega) = \mathbb{Q}(\sqrt[3]{3}, \omega^3 \sqrt[3]{3}, \omega^2 \sqrt[3]{3})$ は

$\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$ 上での $x^3 - 3$ の最小分解体なので $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$ の Galois 拡大である.

$\mathbb{Q}(\sqrt[4]{7}, \sqrt{-1}) = \mathbb{Q}(\sqrt[4]{7}, i) = \mathbb{Q}(\sqrt[4]{7}, i \sqrt[4]{7}, -\sqrt[4]{7}, -i \sqrt[4]{7})$ は

$\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ 上での $x^4 - 7$ の最小分解体なので $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ の Galois 拡大である.

$\mathbb{Q}(\sqrt[3]{3})$ は \mathbb{Q} 上での $\sqrt[3]{3}$ の共役元 $\omega \sqrt[3]{3}$ を含まないので \mathbb{Q} の Galois 拡大ではない.

$\mathbb{Q}(\sqrt[4]{7})$ は \mathbb{Q} 上での $\sqrt[4]{7}$ の共役元 $i \sqrt[4]{7}$ を含まないので \mathbb{Q} の Galois 拡大ではない. \square

Galois 対応 L/K は有限次 Galois 拡大であると仮定する.

このとき, $\text{Gal}(L/K) = \{L \text{の } K \text{ 上での体の自己同型全体}\}$ について,

$$|\text{Gal}(L/K)| = [L : K]$$

でかつ以下の一一対応が得られる:

$$\{L/K \text{の中間体全体}\} \xleftrightarrow{\sim} \{\text{Gal}(L/K) \text{の部分群全体}\}$$

$$M \quad \longmapsto \quad \{\sigma \in \text{Gal}(L/K) \mid \sigma(a) = a \ (a \in M)\}$$

$$L^H = \{\beta \in L \mid \sigma(\beta) = \beta \ (\sigma \in H)\} \quad \longleftrightarrow \quad H$$

さらに,

- (1) この対応は包含関係を逆転させる.
- (2) L/L^H が Galois 拡大になり, $\text{Gal}(L/L^H) = H$. 特に $[L : L^H] = |H|$.
- (3) L^H/K が Galois 拡大 $\iff H$ は $\text{Gal}(L/K)$ の正規部分群.

(2) より, 位数 r の $\text{Gal}(L/K)$ の部分群 H に対応する L/K の部分体 M は $[L : M] = r$ かつ $\sigma(\beta) = \beta$ ($\beta \in M, \sigma \in H$) を満たすものになる.

よく使われる有限群の記号

$S_n = (n \text{次の置換群}) \supset A_n = (n \text{次の交代群}) = \{n \text{次の偶置換全体}\},$

$C_n = (\text{位数 } n \text{の巡回群}) = \langle \sigma \mid \sigma^n = 1 \rangle \cong \mathbb{Z}/n\mathbb{Z}.$

$D_n = (\text{位数 } 2n \text{の } n \text{次の二面体群}) = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle.$

$D_3 \cong S_3, \quad \sigma \leftrightarrow (1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau \leftrightarrow (1, 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$

$$\begin{aligned} S_3 &= \left\{ 1, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3) \right\} \\ &= \left\{ 1, (1, 2, 3), (1, 2, 3)^2, (1, 2), (1, 2, 3)(1, 2), (1, 2, 3)^2(1, 2) \right\} \end{aligned}$$

$$C_3 \cong A_3 = \left\{ 1, (1, 2, 3), (1, 2, 3)^2 \right\}.$$

$$V = \left\{ 1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3) \right\} \cong C_2 \times C_2, \quad V \triangleleft S_4$$

\nwarrow Klein の四元群

問題 7-1 $F(x) = x^3 - 3$, $\alpha = \sqrt[3]{3}$, $\omega = \frac{-1 + \sqrt{-3}}{2}$ とおく. 以下を示せ.

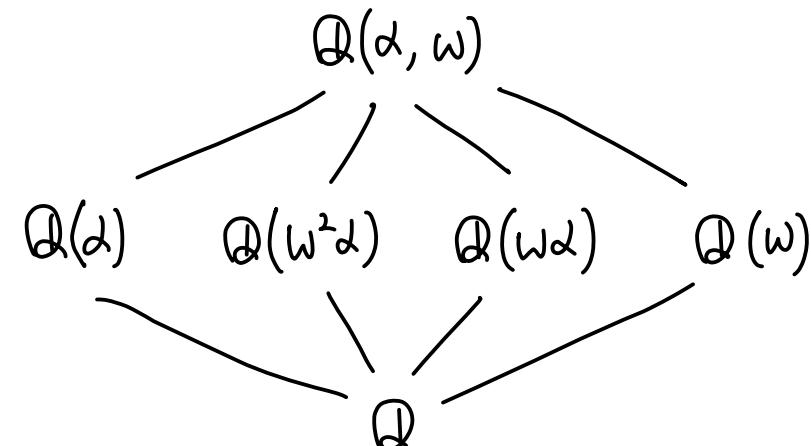
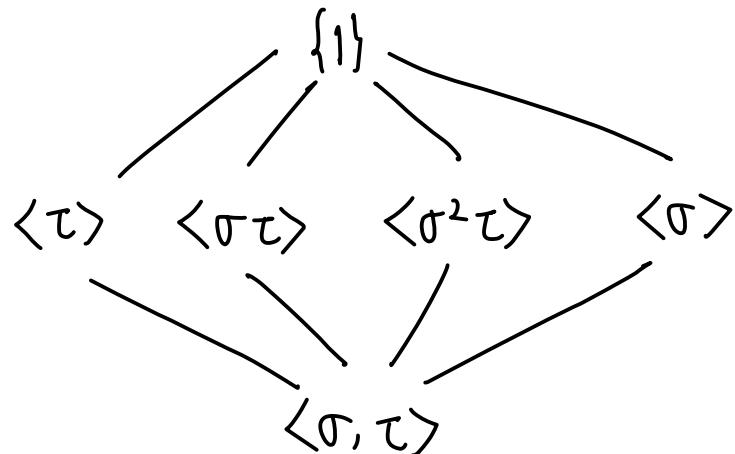
- (1) $F(x)$ は \mathbb{Q} 上で 最小多項式である.
- (2) $F(x)$ の \mathbb{Q} 上で 最小分解体は $\mathbb{Q}(\alpha)$ に等しくない.
- (3) $F(x)$ の \mathbb{Q} 上で 最小分解体は $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \sqrt{-3})$ に等しい.

以下, $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6$ を認めて使ってよい. (問題3-5, 4-2の解答例も参照)

- (4) $\mathbb{Q}(\alpha, \omega)$ の体の自己同型 τ, τ を次のように定義できる:

$$\tau(f(\alpha)) = f(\omega\alpha) \quad (f(x) \in \mathbb{Q}(\omega)[x]), \quad \tau(g(\omega)) = g(\omega^2) \quad (g(x) \in \mathbb{Q}(\alpha)[x]),$$

- (5) $\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = \langle \tau, \tau \rangle \cong D_3 \cong S_3$
- (6) $\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})$ の部分群全体と $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$ の中間体の Galois 対応は以下のようになつてゐる:



← 為に(6)をやってほしい.

問題7-2

$F(x) = x^4 - 4x^2 + 2$, $\alpha = \sqrt{2+\sqrt{2}}$ とおく. 以下を示せ.

- (1) $F(x)$ は α の \mathbb{Q} 上での最小多項式である.
- (2) $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha)$ に等しい. F(x)のすべての根が
 $\mathbb{Q}(\alpha)$ に含まれる.
- (3) $\mathbb{Q}(\alpha)$ の体の自己同型 σ を $\sigma(f(\alpha)) = f(\sqrt{2-\sqrt{2}})$ ($f(x) \in \mathbb{Q}[x]$) 定義できる.
- (4) $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma \rangle \cong C_4$
- (5) $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ の部分群全体と $\mathbb{Q}(\alpha)/\mathbb{Q}$ の中間体全体の Galois 対応は以下の図のようになっている:



□

Galois 対応の証明

K, L, M, \dots は \mathbb{C} の部分体であるとする。

補題1 L/K が有限次 Galois 拡大ならば $|Gal(L/K)| = [L : K]$.

証明 單拡大定理より, ある $\theta \in L$ が存在して $L = K(\theta)$.

θ の K 上での最小多項式を $F_\theta(x) \in K[x]$ と書き, $r = [L : K]$ とおく.

このとき, $L = K(\theta) \cong K[x]/(F_\theta(x))$ より, $r = [L : K] = \dim_K L = \deg F_\theta(x)$.

$F_\theta(x)$ は重根を持たないので互いに異なる r 個の根 $\theta_1 = \theta, \theta_2, \dots, \theta_r$ を持つ
($\theta_1, \dots, \theta_r$ は θ の K 上での 共役元 と呼ばれる.)

$\sigma \in Gal(L/K)$ に対して, $\theta = \sigma(F_\theta(\theta)) = F_\theta(\sigma(\theta))$ なので $\sigma(\theta) \in \{\theta_1, \dots, \theta_r\}$.

ゆえに写像 $\kappa: Gal(L/K) \rightarrow \{\theta_1, \dots, \theta_r\}$, $\sigma \mapsto \sigma(\theta)$ が定まる.

任意の $\lambda = 1, \dots, r$ について, K 上の体の自己同型 $\sigma_\lambda: L \rightarrow L$, $f(\theta) \mapsto f(\theta_\lambda)$ ($f(x) \in K[x]$)
が定まり, $\kappa(\sigma) = \sigma(\theta) = \theta_\lambda$ ので, κ は全射であることがわかる.

$\sigma \in Gal(L/K)$ が " $\kappa(\sigma) = \sigma(\theta) = \theta_\lambda$ " を満たすとき, 任意の $f(x) \in K[x]$ について,
 $\sigma(f(\theta)) = f(\sigma(\theta)) = f(\theta_\lambda)$ ので $\sigma = \sigma_\lambda$. ゆえに κ は単射である.

したがって, $|Gal(L/K)| = |\{\theta_1, \dots, \theta_r\}| = r = [L : K]$, □

次の補題2の証明は易しい。

補題2 L/K が有限次 Galois 拡大であるとき,

その任意の中間体 M について, L/M も有限次 Galois 拡大になる。

証明 $\infty > [L:K] = [L:M][M:K]$ より, $[L:M] < \infty$ なので L/M も有限次拡大になる。 $([M:K] < \infty$ も成立するので M/K も有限次拡大になる。)

L/K が Galois 拡大なので, 任意の K 上での体の同型 $\psi: L \hookrightarrow \mathbb{C}$ について, $\psi(L) = L$. Mの元を固定 Kの元を固定

$\psi: L \hookrightarrow \mathbb{C}$ を M 上での 体の同型とすると, ψ は K 上での 同型でもあるので $\psi(L) = L$.

ゆえに, L/M も Galois 拡大である.

□

以下, L/K は有限次 Galois 拡大であると仮定し, $G = \text{Gal}(L/K)$ とおく.

L/K の中間体 M に対して, G の部分群 G_M を次のように定める:

$$G_M = \text{Gal}(L/M) = \{\sigma \in G \mid \sigma(\beta) = \beta \ (\forall \beta \in M)\}$$

G の部分群 H に対して, L/K の中間体 L^H を次のように定める:

$$L^H = \{\beta \in L \mid \sigma(\beta) = \beta \ (\forall \sigma \in H)\},$$

G_M と L^H の定義からほぼ自明に以下の補題 3, 4 が得られる.

補題 3 (1) $M \subset L^{G_M}$ (2) $H \subset G_{L^H}$

証明 (1) $\beta \in M$ のとき, G_M の定義より $\sigma(\beta) = \beta$ ($\forall \sigma \in G_M$) なので $\beta \in L^{G_M}$.
ゆえに, $M \subset L^{G_M}$.

(2) $\sigma \in H$ のとき, L^H の定義より $\sigma(\beta) = \beta$ ($\forall \beta \in L^H$) なので $\sigma \in G_{L^H}$.

ゆえに $H \subset G_{L^H}$.

□

補題4 対応 $M \mapsto G_M$ と $H \mapsto L^H$ は包含関係を逆転させる。すなわち、

(1) L/K の中間体 $M' \subset M$ に対して、 $G_{M'} \subset G_M$.

(2) G の部分群 $H' \subset H$ に対して、 $L^{H'} \subset L^H$.

証明 (1) $\sigma \in G_{M'}$ (すなわち、 $\sigma(\beta') = \beta'$ ($\forall \beta' \in M'$)) のとき、任意の $\beta \in M$ について、 $M' \subset M$ より $\beta \in M'$ であるので $\sigma(\beta) = \beta$ となるので、 $\sigma \in G_M$. ゆえに、 $G_{M'} \subset G_M$.

(2) $\beta \in L^H$ (すなわち、 $\sigma(\beta) = \beta$ ($\forall \sigma \in H$)) のとき、任意の $\sigma' \in H'$ について、 $H' \subset H$ より $\sigma' \in H$ であるので $\sigma'(\beta) = \beta$ となるので、 $\beta \in L^{H'}$. ゆえに、 $L^{H'} \subset L^H$.

□

補題5 L/K の中間体 $M' \subset M$ について $G_{M'} = G_M$ ならば $M' = M$.

証明 L/K の中間体 $M' \supseteq M$ について $G_{M'} \subsetneq G_M$ となることを示せばよい。
補題2より, L/M も有限次 Galois 拡大になる。

单拡大定理より, ある $\theta \in M'$ が存在して, $M' = M(\theta)$ となる。

θ の M 上での最小多項式を $F(x) \in M[x]$ と書く, $F(x)$ は重根を持たない。

$M' \supsetneq M$ より, $2 \leq [M':M] = \deg F(x)$ なので,

$F(x)$ は θ と異なる根 θ' を持つ (θ と異なる M 上での θ の共役元 θ' が存在)。

L/M は Galois 拡大なので $\theta' \in L$.

M 上での体の同型 $\varphi: M' = M(\theta) \hookrightarrow L$, $f(\theta) \mapsto f(\theta')$ ($f(x) \in M[x]$) が得られる。

\uparrow $M' \hookrightarrow L$, $\beta' \mapsto \beta'$ とは異なる \uparrow

$\varphi: M' \hookrightarrow L$, $f(\theta) \mapsto f(\theta')$ を作れた。

单拡大定理より、ある $\eta \in L$ が存在して、 $L = M'(\eta) = M(\theta, \eta)$.

η の $M' = M(\theta)$ 上で^るの最小多項式を $G(x) = \sum_i a_i x^i$ ($a_i \in M' = M(\theta)$) と書き、
 $H(x) = \sum_i \varphi(a_i) x^i \in M(\theta')[x]$ とおき、 $H(x)$ の根の 1つを $\tilde{\eta}$ と書く。

$$\left\{ \begin{array}{l} L = M'(\eta) \cong M'[x]/(G(x)), f(\eta) \leftrightarrow \overline{f(x)} \quad (f(x) \in M'[x]), \\ M(\theta')[\tilde{\eta}] \cong M(\theta')[x]/(H(x)), g(\tilde{\eta}) \leftrightarrow \overline{g(x)} \quad (g(x) \in \varphi(M')[x]) \\ M'[x] \cong M(\theta')[x], \sum_i a_i x^i \leftrightarrow \sum_i \varphi(a_i) x^i \quad (a_i \in M'), G(x) \leftrightarrow H(x) \end{array} \right.$$

\cong は $M(\theta)$ の拡大

M 上の体の同型 $\psi: L = M'(\eta) \hookrightarrow \mathbb{C}$, $\sum_i a_i \eta^i \mapsto \sum_i \varphi(a_i) \tilde{\eta}^i$ ($a_i \in M'$) が得られる:

$$L = M'(\eta) \cong M'[x]/(G(x)) \cong M(\theta')[x]/(H(x)) \cong M(\theta')[\tilde{\eta}] \subset \mathbb{C}.$$

$$\sum_i a_i \eta^i \leftrightarrow \overline{\sum_i a_i x^i} \leftrightarrow \overline{\sum_i \varphi(a_i) x^i} \leftrightarrow \sum_i \varphi(a_i) \tilde{\eta}^i$$

L/M は Galois 拡大^るの^る $\psi(L) = L$ となり,

$\sigma \in \text{Gal}(L/M) = G_M$ を $\sigma(\gamma) = \psi(\gamma)$ ($\gamma \in L$) と作れる.

$\theta \in M' = M(\theta)$ について、 $\sigma(\theta) = \varphi(\theta) = \theta' \neq \theta$ との^る $\sigma \notin G_{M'}$.

補題 4(1) より $G_{M'} \subset G_M$ となり、 $\sigma \in G_M \setminus G_{M'}$ との^る $G_{M'} \nsubseteq G_M$. □

問題 6-1
 解答例
 ② と
 同様の
 構成

定理 (Galois 対応) $M \mapsto G_M$ と $H \mapsto L^H$ は互いに相手の逆写像である.

証明

① $G_{L^H} = H$ を示そう. 補題3(2)より $G_{L^H} \supset H$ なので $G_{L^H} \subset H$ を示せばよい.

そのためには, $|G_{L^H}| \leq |H|$ を示せば十分である.

单拡大定理より, ある $\theta \in L$ が存在して, $L = L^H(\theta)$ となる.

$$f(x) = \prod_{\tau \in H} (x - \tau(\theta)) = \sum_i c_i x^i \quad (c_i \in L) \text{ とおく.} \quad \rho \in \sigma \tau$$

$$\text{このとき, } \sigma \in H \text{ について, } \sum_i \sigma(c_i) x^i = \prod_{\tau \in H} (x - \sigma \tau(\theta)) \stackrel{\downarrow}{=} \prod_{\rho \in H} (x - \rho(\theta)) = f(x)$$

なので $\sigma(c_i) = c_i$ となるので, $c_i \in L^H$, $f(x) \in L^H[x]$ である.

$f(\theta) = 0$ なので,

$$|H| = \deg f(x) \geq \deg (\theta \text{ の } L^H \text{ 上での最小多項式}) = [L^H(\theta) : L^H] = [L : L^H]$$

補題1より, $[L : L^H] = |\text{Gal}(L/L^H)| = |G_{L^H}|$.

ゆえに, $|H| \geq |G_{L^H}|$, したがって, $G_{L^H} \subset H$ ($\therefore G_{L^H} = H$).

2 $L^{G_M} = M$ を示そう.

補題3(1)より, $L^{G_M} \supset M$.

1の結果を $H = G_M$ に適用すると $G_{L^{G_M}} = G_M$.

補題5を $M' = L^{G_M}$ に適用すると, $L^{G_M} = M$ が得られる. \square

以上によって, ①の部分体の場合の Galois 対応が証明された.

注意 (1) 標数 0 の一般的な場合は ①を K を含む代数閉包におけるかえれば"同様の方法で" Galois 対応が証明される.

(2) 標数 $p > 0$ の場合にも, 最小多項式が重根を持たず"にすむための適切な定式化 (分離性の仮定) をすれば" 本質的に同じ方法で Galois 対応を証明可能である \square

追記 2021-11-17

Galois 対応の ② は以下のようにすれば"容易に示せました、

(めんどうな
補題 5 の
証明は必要ない。)

易しい ② の別証

$$L^{G_M} = M \text{ を示す。}$$

ほぼ自明の補題 3 (1) より、 $L^{G_M} \subset M$.

ゆえに、 $L^{G_M} = M$ を示すためには $[L^{G_M} : K] = [M : K]$ を示せば"十分"である。

(K 上の有限次元ベクトル空間 V とその部分空間 W について、 $V = W \Leftrightarrow \dim_K V = \dim_K W$.)
(これを $V = L^{G_M}$, $W = M$ に適用した、

補題 2 より、 L/L^{G_M} も L/M も Galois 扩大で"あり、

←(注意
 $G_M = \text{Gal}(L/M)$)

補題 1 より、 $[L:L^{G_M}] = |G_{L^{G_M}}|$, $[L:M] = |G_M|$.

① の結果を $H = G_M$ に適用すると $G_{L^{G_M}} = G_M$ なので $[L:L^{G_M}] = [L:M]$.

これと、 $[L:L^{G_M}][L^{G_M}:K] = [L:K] = [L:M][M:K]$ より、 $[L^{G_M}:K] = [M:K]$.

したがって、 $L^{G_M} = M$.

□

ムダにめんどうな証明を紹介して申しわけありませんでした。

問題 7-1 $F(x) = x^3 - 3$, $\alpha = \sqrt[3]{3}$, $\omega = \frac{-1 + \sqrt{-3}}{2}$ とおく. 以下を示せ.

- (1) $F(x)$ は \mathbb{Q} 上での最小多項式である.
- (2) $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha)$ に等しくない.
- (3) $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \sqrt{-3})$ に等しい.

\mathbb{Q} 上の方程式 $x^3 - 3 = 0$ の Galois 対応の記述

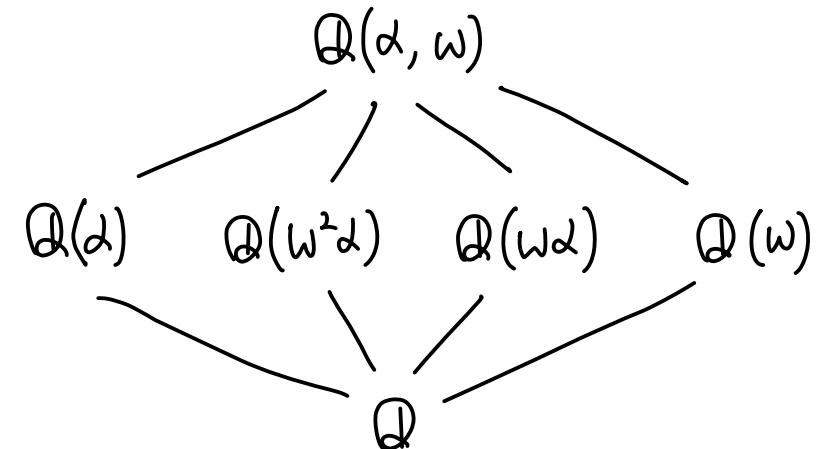
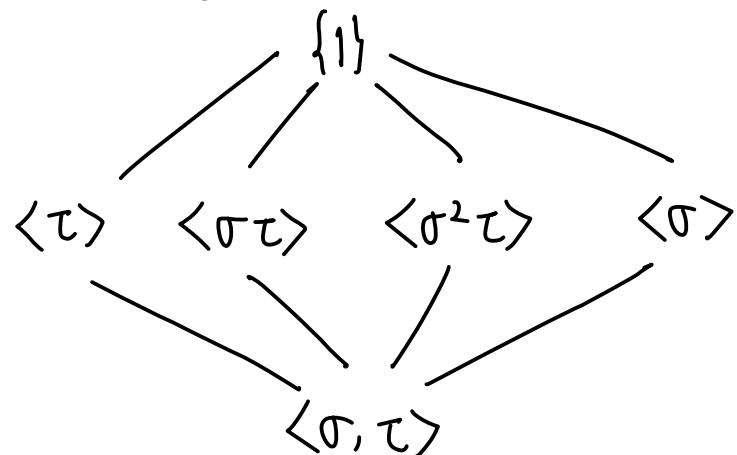
以下, $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6$ を認めて使ってよい. (問題 3-5, 4-2 の解答例も参照)

- (4) $\mathbb{Q}(\alpha, \omega)$ の体の自己同型 τ, τ を次のように定義できる:

$$\tau(f(\alpha)) = f(\omega\alpha) \quad (f(x) \in \mathbb{Q}(\omega)[x]), \quad \tau(g(\omega)) = g(\omega^2) \quad (g(x) \in \mathbb{Q}(\alpha)[x]),$$

$$(5) \text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = \langle \tau, \tau \rangle \cong D_3 \cong S_3 \quad \leftarrow \text{特に (6) をやってほしい.}$$

- (6) $\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})$ の部分群全体と $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$ の中間体の Galois 対応は以下のようになつてゐる:



問題 7-1 解答例 ($F(x) = x^3 - 3$, $\alpha = \sqrt[3]{3}$, $\omega = \frac{-1 + \sqrt{-3}}{2}$, $\omega^3 = 1$, $\omega^2 + \omega + 1 = 0$)

(1) $3 \nmid 1, 3 \nmid 0, 3 \nmid 0, 3 \mid (-3), 3^2 \nmid (-3)$ と Eisenstein の判定法より $F(x) = x^3 - 3$ は
 ① 上で既約である。($x^3 - 3$ が ① に根を持たないこともその ① 上既約性がわかる。) ← どうしてか?

$F(x)$ は ① 上で既約で $F(\alpha) = 0$ をみたすので, α の \mathbb{Q} 上の最小多項式である。

(2) $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$ である。($\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(F(x))$ より)
 $f(\alpha) \leftrightarrow \overline{f(x)}$

$F(x) = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$ の \mathbb{Q} 上の最小分解体は $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \subset \mathbb{R}$ である。
 しかし, $\mathbb{Q}(\alpha)$ は $F(x)$ の \mathbb{Q} 上の最小分解体ではない。

(3) $\alpha, \omega = \frac{\omega\alpha}{\alpha} \in \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ より $\mathbb{Q}(\alpha, \omega) \subset \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$. } しかし
 $\alpha, \omega\alpha, \omega^2\alpha \in \mathbb{Q}(\alpha, \omega)$ より $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \subset \mathbb{Q}(\alpha, \omega)$, } $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$.

$\alpha, \omega = \frac{-1 + \sqrt{-3}}{2} \in \mathbb{Q}(\alpha, \sqrt{-3})$ より $\mathbb{Q}(\alpha, \omega) \subset \mathbb{Q}(\alpha, \sqrt{-3})$ } しかし
 $\alpha, \sqrt{-3} = 2\omega + 1 \in \mathbb{Q}(\alpha, \omega)$ より, $\mathbb{Q}(\alpha, \sqrt{-3}) \subset \mathbb{Q}(\alpha, \omega)$ } $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \sqrt{-3})$.

$$(4) [\mathbb{Q}(\omega) : \mathbb{Q}] = 2, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6 \text{ より}, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] = \frac{[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]}{[\mathbb{Q}(\omega) : \mathbb{Q}]} = 3.$$

$F(x) = x^3 - 3 \in \mathbb{Q}(\omega)[x]$, $F(\alpha) = 0$, $\deg F(x) = 3 = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)]$

なので, $F(x)$ は $\mathbb{Q}(\omega)$ 上での ω の最小多项式である,

ゆえに, 以下のようにして, $\mathbb{Q}(\alpha, \omega)$ の $\mathbb{Q}(\omega)$ 上での自己同型 τ を作れる:

$$\mathbb{Q}(\alpha, \omega) \cong \mathbb{Q}(\omega)[x]/(F(x)) \cong \mathbb{Q}(\omega\alpha, \omega) = \mathbb{Q}(\alpha, \omega)$$

$$f(\alpha) \longleftrightarrow \overline{f(x)} \longleftrightarrow f(\omega\alpha)$$

τ

F(x) は $\mathbb{Q}(\omega)$ 上既約で
 $\omega\alpha$ を根になるので,
 F(x) は $\omega\alpha$ の $\mathbb{Q}(\omega)$ 上での
 最小多项式にもなっている.

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6 \text{ より}, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = \frac{[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = 2,$$

$G(x) = x^2 + x + 1$ とおくと, $G(x) \in \mathbb{Q}(\alpha)[x]$, $G(\omega) = 0$, $\deg G(x) = 2 = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)]$

なので, $G(x)$ は $\mathbb{Q}(\alpha)$ 上での ω の最小多项式である,

ゆえに, 以下のようにして, $\mathbb{Q}(\alpha, \omega)$ の $\mathbb{Q}(\alpha)$ 上での自己同型 τ を作れる:

$$\mathbb{Q}(\alpha, \omega) \cong \mathbb{Q}(\alpha)[x]/(G(x)) \cong \mathbb{Q}(\alpha, \omega^2) = \mathbb{Q}(\alpha, \omega) \quad (\omega^2 = \omega^{-1})$$

$$g(\omega) \longleftrightarrow \overline{g(x)} \longleftrightarrow g(\omega^2)$$

τ

上と同様に $G(x)$ は ω^2 の
 $\mathbb{Q}(\alpha)$ 上での最小多项式にもなっている.

(5) $\mathbb{Q}(\alpha, \omega)$ は $F(x) = x^3 - 3$ の \mathbb{Q} 上での最小分解体なので,

$\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$ は有限次 Galois 拡大である.

$$\text{ゆえに, } |\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})| = [\mathbb{Q}(\alpha, \omega):\mathbb{Q}] = 6.$$

(4) の記号のもとで, $\sigma, \tau \in \text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})$ である. そして,

$$\textcircled{1} \quad \sigma(\alpha) = \alpha, \quad \sigma(\omega) = \omega$$

$$\textcircled{2} \quad \sigma(\alpha) = \omega\alpha, \quad \sigma(\omega) = \omega$$

$$\textcircled{3} \quad \sigma^2(\alpha) = \omega^2\alpha, \quad \sigma^2(\omega) = \omega$$

$$\underline{\sigma^3(\alpha) = \alpha, \quad \sigma^3(\omega) = \omega}$$

$$\textcircled{4} \quad \tau(\alpha) = \alpha, \quad \tau(\omega) = \omega^2$$

$$\textcircled{5} \quad \tau\sigma(\alpha) = \omega\alpha, \quad \tau\sigma(\omega) = \omega^2$$

$$\textcircled{6} \quad \tau^2\sigma(\alpha) = \omega^2\alpha, \quad \tau^2\sigma(\omega) = \omega^2$$

$$\underline{\tau^2(\alpha) = \alpha, \quad \tau^2(\omega) = \omega^4 = \omega}$$

$$\underline{\tau\sigma\tau(\alpha) = \omega^2\alpha, \quad \tau\sigma\tau(\omega) = \omega}$$

ゆえに, $\therefore 1 \text{ は } \text{id}_{\mathbb{Q}(\alpha, \omega)}$

$$1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$$

は互いに異なるので,

$$\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

さて $\sigma^3 = \tau^2 = 1$, $\tau\sigma\tau = \sigma^2 = \sigma^{-1}$,
 これより $(\tau\sigma = \sigma^{-1}\tau)$

$$\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) \cong D_3 \cong S_3.$$

$$(b) G = \text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = \{1, \sigma, \overset{\leq \sigma^{-1}}{\sigma^2}, \tau, \sigma\tau, \sigma^2\tau\} \quad (\sigma^3 = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau)$$

の部分群をすべて求めよ; $\begin{array}{cccccc} 1 & 3 & 3 & 2 & 2 & 2 \end{array}$ ←元の位数
←自分で確認せよ.

位数6の群Gの部分群の位数はその約数1, 2, 3, 6のどれかになる,

位数1 $\{1\}$ しかない. (Lagrangeの定理より)↑

位数2 位数2の部分群は位数2の元から生成される巡回群になる.

Gの位数2の部分群全体は $\langle \tau \rangle, \langle \sigma\tau \rangle, \langle \sigma^2\tau \rangle$.

位数3 位数3の部分群は位数3の元から生成される巡回群になる.

Gの位数3の部分群は $\langle \sigma \rangle = \langle \sigma^2 \rangle$ の1つだけ.

位数6 Gの位数6の部分群はGそのものになる.

$L = \mathbb{Q}(\alpha, \omega)$ とおく、 G の部分群 H に対応する L/\mathbb{Q} の中間体 L^H を求めよう。

$$[L : L^H] = |Gal(L/L^H)| = |H|, [L^H : \mathbb{Q}] = \frac{[L : \mathbb{Q}]}{[L : L^H]} = \frac{|G|}{|H|} \text{ に注意せよ,}$$

$L^{(1)}$ $L^{(1)} = \{\beta \in L \mid \tau(\beta) = \beta\} = L = \mathbb{Q}(\alpha, \omega).$

$$L^H = \{\beta \in L \mid \rho(\beta) = \beta \ (\forall \rho \in H)\}$$

$L^{(2)}$ $\tau(\alpha) = \alpha$ より $\alpha \in L^{(2)}$ なので $\mathbb{Q}(\alpha) \subset L^{(2)}$ であり,

$$[L^{(2)} : \mathbb{Q}] = \frac{|G|}{|\langle \tau \rangle|} = \frac{6}{2} = 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] \text{ なので } L^{(2)} = \mathbb{Q}(\alpha).$$

$L^{(\sigma\tau)}$ $\sigma\tau(\omega^2\alpha) = \sigma(\omega\alpha) = \omega^2\alpha$ なので $\mathbb{Q}(\omega^2\alpha) \subset L^{(\sigma\tau)}$ であり,

$$[L^{(\sigma\tau)} : \mathbb{Q}] = \frac{|G|}{|\langle \sigma\tau \rangle|} = \frac{6}{2} = 3 = [\mathbb{Q}(\omega^2\alpha) : \mathbb{Q}] \text{ なので } L^{(\sigma\tau)} = \mathbb{Q}(\omega^2\alpha).$$

$L^{(\sigma^2\tau)}$ $\sigma^2\tau(\omega\alpha) = \sigma^2(\omega^2\alpha) = \omega^2\omega^2\alpha = \omega\alpha$ なので $\mathbb{Q}(\omega\alpha) \subset L^{(\sigma^2\tau)}$ であり,

$$[L^{(\sigma^2\tau)} : \mathbb{Q}] = \frac{|G|}{|\langle \sigma^2\tau \rangle|} = \frac{6}{2} = 3 = [\mathbb{Q}(\omega\alpha) : \mathbb{Q}] \text{ なので } L^{(\sigma^2\tau)} = \mathbb{Q}(\omega\alpha).$$

$L^{(\sigma)}$ $\sigma(\omega) = \omega$ より $\mathbb{Q}(\omega) \subset L^{(\sigma)}$ あり

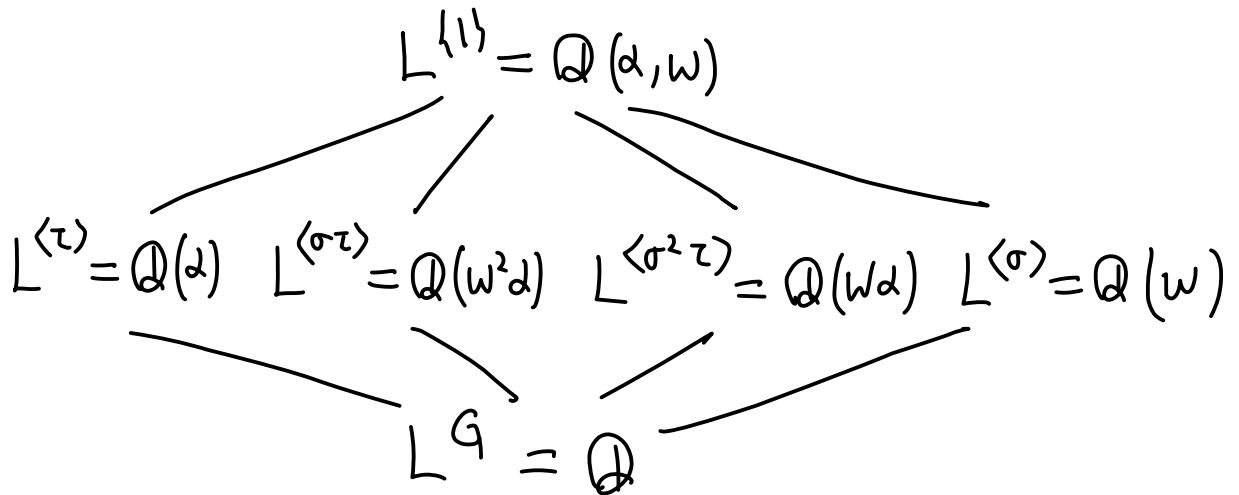
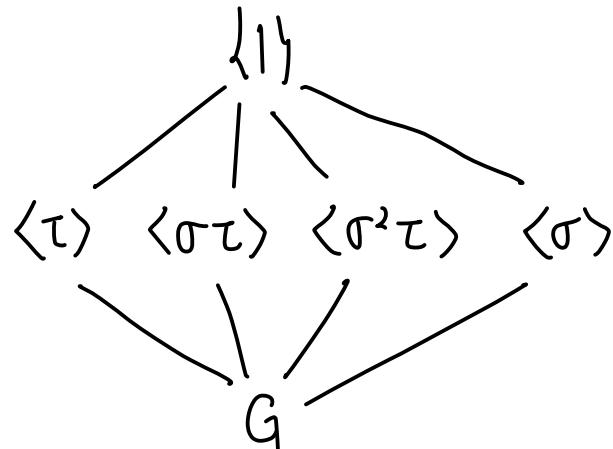
$$[L^{(\sigma)} : \mathbb{Q}] = \frac{|G|}{|\langle \sigma \rangle|} = \frac{6}{3} = 2 = [\mathbb{Q}(\omega) : \mathbb{Q}] \text{ なので } L^{(\sigma)} = \mathbb{Q}(\omega).$$

L^G $[L^G : \mathbb{Q}] = \frac{|G|}{|G|} = 1$ なので $L^G = \mathbb{Q}.$

\mathbb{Q} 上のベクトル空間として,
 $\mathbb{Q}(\alpha) \subset L^{(2)}$
 両方 \mathbb{Q} 上の次元が 3
 ゆえに $\mathbb{Q}(\alpha) = L^{(2)}$

↑
上と同様

以上を図で描くと



上の図は①上での方程式 $x^3 - 3 = 0$ がどのように解けて行くかを記述しているとみなせる。

- $L = \mathbb{Q}(\alpha, \omega) \longleftrightarrow x^3 - 3 = 0$ を解き切った結果
- L/\mathbb{Q} の中間体 \longleftrightarrow $x^3 - 3 = 0$ を解く途中の様子
- $L^{(τ)} = \mathbb{Q}(\alpha) \longleftrightarrow x^3 - 3 = 0$ の解の1つめが得られた様子
- $L^{(σ)} = \mathbb{Q}(\omega) \longleftrightarrow x^3 - 3 = 0$ を解き切るために必要な ω が得られた様子

問題7-2

$F(x) = x^4 - 4x^2 + 2$, $\alpha = \sqrt{2+\sqrt{2}}$ とおく. 以下を示せ.

- (1) $F(x)$ は α の \mathbb{Q} 上での最小多項式である.
- (2) $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha)$ に等しい. F(x)のすべての根が
 $\mathbb{Q}(\alpha)$ に含まれる.
- (3) $\mathbb{Q}(\alpha)$ の体の自己同型 σ を $\sigma(f(\alpha)) = f(\sqrt{2-\sqrt{2}})$ ($f(x) \in \mathbb{Q}[x]$) 定義できる.
- (4) $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma \rangle \cong C_4$
- (5) $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ の部分群全体と $\mathbb{Q}(\alpha)/\mathbb{Q}$ の中間体全体の Galois 対応は以下の図のようになっている:



\mathbb{Q} 上の方程式

$$x^4 - 4x^2 + 2 = 0$$

に関する Galois 対応を
求める問題

問題7-2の解答例

$$x^2 = 2 \pm \sqrt{2}, \quad x = \sqrt{2 \pm \sqrt{2}}, -\sqrt{2 \pm \sqrt{2}} \text{ と解ける.}$$

$$F(x) = x^4 - 4x^2 + 2, \quad \alpha = \sqrt{2+\sqrt{2}} \text{ とおく.}$$

$$\alpha^2 = 2 + \sqrt{2}, \quad \alpha^4 = 6 + 4\sqrt{2} \text{ より, } \alpha^4 - 4\alpha^2 + 2 = 0, \quad F(\alpha) = 0.$$

(1) $2 \nmid 1, 2 \mid 0, 2 \mid (-4), 2 \mid 0, 2 \mid 2, 2^2 \nmid 2$ と Eisenstein の判定法より,

$F(x)$ は \mathbb{Q} 上で既約である.

$F(\alpha) = 0$ であるので, $F(x)$ は α の \mathbb{Q} 上での最小多項式である.

$$(2) \quad \alpha = \sqrt{2+\sqrt{2}} \text{ の他に, } \beta = \sqrt{2-\sqrt{2}}, \quad \gamma = -\alpha, \quad \delta = -\beta \text{ とおく.}$$

$X^2 - 4X + 2 = 0$ の解は $X = 2 \pm \sqrt{2}$ なので $F(x)$ の根の全体は $\{\alpha, \beta, \gamma, \delta\}$ となる.

ゆえに $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha, \beta, \gamma, \delta) = \mathbb{Q}(\alpha, \beta)$ となる.

$$\frac{1}{\alpha} = \sqrt{\frac{1}{2+\sqrt{2}}} = \sqrt{\frac{2-\sqrt{2}}{2}} = \frac{\beta}{\sqrt{2}}, \quad \alpha^2 - 2 = \sqrt{2} \text{ より} \quad \beta = \frac{\sqrt{2}}{\alpha} = \frac{\alpha^2 - 2}{\alpha} \in \mathbb{Q}(\alpha).$$

ゆえに, $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \beta).$

$$(3) \text{ 上と同様にして, } \alpha = \frac{\sqrt{2}}{\beta} = \frac{2 - \beta^2}{\beta} \in \mathbb{Q}(\beta) \text{ なので } \mathbb{Q}(\beta) = \mathbb{Q}(\alpha, \beta).$$

ゆえに, $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$. $F(x)$ は β の \mathbb{Q} 上での最小多項式である.

以下のようにして, 体 $\mathbb{Q}(\alpha)$ の \mathbb{Q} 上での自己同型 σ を作れる:

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(F(x)) \cong \mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$$

$$\begin{array}{ccc} f(\alpha) & \longleftrightarrow & \overline{f(\alpha)} & \longleftrightarrow & f(\beta) \\ & & \downarrow \sigma & & \end{array}$$

$$(4) |\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha):\mathbb{Q}] = \deg F(x) = 4.$$

$$\sigma(\alpha) = \beta = \frac{\alpha^2 - 2}{\alpha}$$

$$\sigma^2(\alpha) = \sigma(\beta) = \frac{\beta^2 - 2}{\beta} = -\alpha = \gamma$$

$$\sigma^3(\alpha) = \sigma(-\alpha) = -\sigma(\alpha) = -\beta = \delta$$

$$\sigma^4(\alpha) = \sigma(-\beta) = -\sigma(\beta) = -(-\alpha) = \alpha,$$

$$\left. \begin{array}{l} 1, \sigma, \sigma^2, \sigma^3 \text{ は互いに異なる} \\ \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3\}, \\ \text{さて} \vdash \sigma^4 = 1 \text{ なる} \\ \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma \rangle \cong C_4. \end{array} \right\}$$

(5) $G = Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \sigma^3\} \cong C_4$ とおく.
 $\begin{matrix} 1 & 4 & 2 & 4 \end{matrix} \leftarrow$ 元の位数.

G の部分群の全体は $\{\{1\}, \langle \sigma^2 \rangle, \langle \sigma \rangle = G\}$ の 3つである.

$$\begin{matrix} \text{S1} \\ C_1 \\ \text{SII} \\ C_2 \\ \text{SIII} \\ C_4 \end{matrix}$$

(i) $\underline{\mathbb{Q}(\alpha)^{\{1\}}} = \{\eta \in \mathbb{Q}(\alpha) \mid 1(\eta) = \eta\} = \underline{\mathbb{Q}(\alpha)},$

$$\begin{pmatrix} \sqrt{2} = \alpha^2 - 2 \text{ より } \sigma^2(\alpha) = -\alpha \text{ な } \sigma \\ \sigma^2(\sqrt{2}) = \sqrt{2}. \end{pmatrix}$$

(ii) $\sigma^2(\sqrt{2}) = \sigma^2(\alpha^2 - 2) = (-\alpha)^2 - 2 = \alpha^2 - 2 = \sqrt{2}$ より $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha)^{\langle \sigma^2 \rangle}$ であり,
 $\sigma^2(\alpha) = -\alpha$

$$[\mathbb{Q}(\alpha)^{\langle \sigma^2 \rangle} : \mathbb{Q}] = \frac{|G|}{|\langle \sigma^2 \rangle|} = \frac{4}{2} = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \text{ なので } \underline{\mathbb{Q}(\alpha)^{\langle \sigma^2 \rangle}} = \underline{\mathbb{Q}(\sqrt{2})}.$$

(iii) $[\mathbb{Q}(\alpha)^G : \mathbb{Q}] = \frac{|G|}{|G|} = 1$ より $\underline{\mathbb{Q}(\alpha)^G} = \underline{\mathbb{Q}},$

以上を図で描くと,

$\{1\}$	$\mathbb{Q}(\alpha)^{\{1\}} = \mathbb{Q}(\alpha)$	$x^2 = 2 \pm \sqrt{2}$ を解くと 解は $\alpha = \sqrt{2 \pm \sqrt{2}}$ で書ける.
$\langle \sigma^2 \rangle$	$\mathbb{Q}(\alpha)^{\langle \sigma^2 \rangle} = \mathbb{Q}(\sqrt{2})$	$x^2 - 4x + 2 = 0$ は $x = 2 \pm \sqrt{2}$ を解ける.
$G = \langle \sigma \rangle$	$\mathbb{Q}(\alpha)^{\langle \sigma \rangle} = \mathbb{Q}$	

Artinの補題

群 G から体 K の乗法群 K^\times への互いに異なる群の準同型たち

$\sigma_1, \dots, \sigma_n$ は K 上一次独立である。(注意 G から K への写像全体の集合は
 K 上のベクトル空間とみなされる。)

証明

次の $(*)_n$ を $n = 1, 2, \dots$ に関する数学的帰納法で示せばよい。

$(*)_n$ $\sigma_1, \dots, \sigma_n$ は G から K^\times への互いに異なる群の準同型で、

$$a_1, \dots, a_n \in K \text{ かつ } a_1\sigma_1(x) + \dots + a_n\sigma_n(x) = 0 \quad (x \in G) \text{ ならば } a_1 = \dots = a_n = 0,$$

$(*)_1$ を示そう。 $a_1\sigma_1(x) = 0 \quad (x \in G)$ と $\sigma_1(x) \in K^\times \quad (x \in G)$ より $a_1 = 0$.

$n \geq 2$ であるとし、 $(*)_{n-1}$ が成立していると仮定する。 $(*)_n$ を示せばよい。

$\sigma_1, \dots, \sigma_n$ は G から K^\times への互いに異なる群の準同型であり、

$a_1, \dots, a_n \in K$ かつ $a_1\sigma_1(x) + \dots + a_n\sigma_n(x) \stackrel{(*)}{=} 0 \quad (x \in G)$ と仮定する。

$\sigma_1 \neq \sigma_n$ なので、ある $y \in G$ が存在して $\sigma_1(y) \neq \sigma_n(y)$ となる。

任意に $x \in G$ をとる。

$$(\star) \text{より}, \quad 0 = \sigma_n(y)(a_1\sigma_1(x) + \cdots + a_n\sigma_n(x)) = a_1\sigma_n(y)\sigma_1(x) + \cdots + a_n\sigma_n(y)\sigma_n(x)$$

(†) yx におけるときと,

$$0 = a_1\sigma_1(yx) + \cdots + a_n\sigma_n(yx) = a_1\sigma_1(y)\sigma_1(x) + \cdots + a_n\sigma_n(y)\sigma_n(x),$$

これらの差を考えると, $\neq 0$

$$0 = \underbrace{a_1(\sigma_n(y) - \sigma_1(y))}_{\in K}\sigma_1(x) + \cdots + \underbrace{a_{n-1}(\sigma_n(y) - \sigma_1(y))}_{\in K}\sigma_{n-1}(x).$$

ゆえに $(*)_{n-1}$ より, $a_1 = \cdots = a_{n-1} = 0$ が得られ, (†) より $a_n = 0$ も得られる. \square

注意 G を体 L の自己同型群の部分群であるとき, この G は Artin の補題の G として使われないことに注意せよ。

各 $\sigma \in G$ は L^X から L^X への群の準同型写像を与え, σ から定まる L^X から L^X への群の準同型写像からもとの σ は 0 を 0 にうつすという拡張で一意に決まるので,

Artin の補題を (G, K) が (L^X, L) の場合に適用することによって,

G は L 上一次独立な集合になってしまことわかる.

ここがポイント

\square

Artinの定理

G は体 L の自己同型群の有限部分群であるとし,

その部分体 K を $K = L^G = \{\beta \in L \mid \sigma(\beta) = \beta \ (\sigma \in G)\}$ と定める.
このとき, L/K は有限次 Galois 拡大であり, $[L:K] = |G|$.

Galois 拡大 L/K の
 K が L を作るのではなく,
 L から K を作る言葉

証明

まず“トレース写像” $T: L \rightarrow K$ を定義しよう.

① $\beta \in L$ に対して, $T(\beta) \in L$ を $T(\beta) = \sum_{\sigma \in G} \sigma(\beta)$ と定める. (T はトレース写像と呼ばれる.)

このとき, 任意の $\sigma \in G$ に対して, $\sigma(T(\beta)) = \sum_{\tau \in G} \sigma\tau(\beta) = \sum_{\rho \in G} \rho(\beta) = T(\beta)$ なので,
 $T(\beta) \in L^G = K$ となる.

← σ は K 上の線形写像である.

$\sigma \in G, a \in K, \beta \in L$ について, $\overline{\sigma(a\beta)} = \sigma(a)\sigma(\beta) = a\sigma(\beta)$ なので,

G の元は K 上での L の体の自己同型になっている.

これで, K 上の線形写像 $T = \sum_{\sigma \in G} \sigma: L \rightarrow K$ が得られたことになる.

Artinの補題より, G は L 上一次独立な集合になる (前ページの注意を参照).
Artinの補題の(G, K)が(L, L^x)の場合より

特に, $T = \sum_{\sigma \in G} \sigma \neq 0$ なので, ある $a \in L$ が存在して $T(a) \neq 0$.

① $[L:K] \leq |G|$ を示そう.

任意に $\beta_1, \dots, \beta_{|G|+1} \in L$ をとる. $\beta_1, \dots, \beta_{|G|+1}$ が一次従属であることを示せばよい.

$|G|$ 連立の $x_1, \dots, x_{|G|+1}$ に関する一次方程式 $\sum_{i=1}^{|G|+1} \sigma^{-1}(\beta_i) x_i = 0 \ (\sigma \in G)$ の非自明な解 $(x_1, \dots, x_{|G|+1}) = (\gamma_1, \dots, \gamma_{|G|+1})$, $\gamma_i \in L$ が存在する. (非自明な解はこれがかかってない解)

$\gamma_1 \neq 0$ と仮定してよい. $\kappa = \frac{\alpha}{\gamma_1} \neq 0$ とおくと, $(\kappa \gamma_1, \dots, \kappa \gamma_{|G|+1})$ も非自明な解になり, $\kappa \gamma_1 = \alpha$ なので, $\gamma_1 = \alpha$ と仮定できる.

このとき, $\sum_{i=1}^{|G|+1} \sigma^{-1}(\beta_i) \gamma_i = 0$ の両辺に T を作用させると, $\sum_{i=1}^{|G|+1} \beta_i T(\gamma_i) = 0 \ (\sigma \in G)$, これを $\sigma \in G$ について足し上げると, $\sum_{i=1}^{|G|+1} \beta_i T(\gamma_i) = 0$ が得られ, $T(\gamma_1) = T(\alpha) \neq 0$ と $T(\gamma_i) \in K$ より, $\beta_1, \dots, \beta_{|G|+1}$ が K 上一次従属であることがわかる.

注意 特にこれで L/K は有限次拡大であることがわかった.

2 $[L:K] \geq |G|$ を示す.

$[L:K] < |G|$ と仮定して矛盾を導こう.

$[L:K] = r < |G|$ であると仮定し, L の K 上の基底 β_1, \dots, β_r をとる.

r 連立の $|G|$ 個の $x_\sigma (\sigma \in G)$ たちに関する一次方程式 $\sum_{\sigma \in G} \sigma(\beta_i) x_\sigma = 0 \quad (i=1, \dots, r)$ の非自明な解 $(x_\sigma)_{\sigma \in G} = (\gamma_\sigma)_{\sigma \in G}$, $\gamma_\sigma \in L$ が存在する.

任意に $\beta \in L$ をとる. $\beta = \sum_{i=1}^r a_i \beta_i$, $a_i \in K$ と書ける.

このとき, $\sigma(a_i \beta_i) = \sigma(a_i) \sigma(\beta_i) = a_i \sigma(\beta_i)$ と $\sum_{\sigma \in G} \sigma(\beta_i) \gamma_\sigma = 0 \quad (i=1, \dots, r)$ より,

$$\sum_{\sigma \in G} \gamma_\sigma \sigma(\beta) = \sum_{\sigma \in G} \gamma_\sigma \sum_{i=1}^r a_i \sigma(\beta_i) = \sum_{i=1}^r a_i \sum_{\sigma \in G} \sigma(\beta_i) \gamma_\sigma = 0 \quad \begin{matrix} \text{これが } \forall \beta \in L \\ \text{について成立} \end{matrix}$$

となる. ある $\sigma \in G$ が存在して $\gamma_\sigma \neq 0$ となっているので,

G が L 上一次従属になつて (Artin の補題に) 矛盾する.

3 L/K が分離的であることを示す、
 $\theta \in L$ を任意にとる、 θ が K 上分離的であることを示せばよい。
 (L/K が分離的であることの定義(の1つ)は、 L の任意の元の K 上での最小多項式
 が重根を持たないことである。)

ポイント L/K は有限次拡大なので θ は K 上代数的である。

L に含まれる θ の K 上での共役元で互いに異なるものの全体を $\theta_1, \dots, \theta_r$ と書く。

任意の $\sigma \in G$ について、 $\sigma(\theta_n)$ も θ の K 上での共役元になるので、

σ は集合 $\{\theta_1, \dots, \theta_r\}$ に作用している: $\{\sigma(\theta_1), \dots, \sigma(\theta_r)\} = \{\theta_1, \dots, \theta_r\}$ ($\sigma \in G$)。

$$f(x) = \prod_{i=1}^r (x - \theta_i) = \sum_{i=0}^r c_i x^i \quad (c_i \in L) \text{ とおく。 } f(x) \text{ は重根を持たない。}$$

$$\text{このとき, 任意の } \sigma \in G \text{ について, } \sum_{i=0}^r \sigma(c_i) x^i = \prod_{i=1}^r (x - \sigma(\theta_i)) = \prod_{i=1}^r (x - \theta_i) = f(x)$$

なので $\sigma(c_i) = c_i$ となり、 $c_i \in K$, $f(x) \in K[x]$ となることがわかる。

θ の K 上での最小多項式は $f(x)$ を割り切るので重根を持たない。

これで θ が K 上分離的であることが示された。

④ L/K が正規拡大であることを示す。

上に続けて、 θ の K 上でのすべての共役元が L に含まれることを示せばよい。

$(L/K$ が正規であることの定義(の1つ)は、 L の任意の元の K 上での最小多項式のすべての根(K 上でのすべての共役元)が L に含まれることである)

しかし、 θ の K 上での最小多項式が $f(x)$ を割り切ることが示されているので、 θ の K 上での任意の共役元は $\theta_i \in L$ のどれかに一致する。

これで L/K が正規拡大であることも示された。 Galois 拡大 = 分離的かつ正規な拡大

⑤ 以上によって、 L/K が有限次 Galois 拡大であり、 $[L:K] = |G|$ となることが示された。(有限次拡大 L/K が Galois 拡大であることの定義は L/K が分離的かつ正規であることである。) □

注意 Artin の定理の状況のもとで、 $G \subset \text{Gal}(L/K)$, $[L:K] = |\text{Gal}(L/K)|$ なので、 $\text{Gal}(L/K) = G$ なることもわかる。 □

問題 8-1 K, L は \mathbb{C} の部分体であるとする。 次数0を使う。

- (1) L/K が 2 次拡大ならば L/K は Galois 拡大であることを示せ。
- (2) 2 次以上の有限次拡大 L/K で L の K 上での体の自己同型が id_L しか存在しないものの例を具体的に 1 つ挙げよ。

ヒント (1) L は $L = K(\alpha)$, $\alpha \in L$, $\alpha \notin K$, $\alpha^2 \in K$ の形になる。

(2) \mathbb{Q} の 3 次拡大でそのような例を作れる。
- $\alpha \neq \bar{\alpha}$ を使う。
 (注) 次数2だと $-\alpha = \alpha$)

もしも 3 次拡大 L/\mathbb{Q} が Galois 拡大ならば,
 $|\text{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 3$ なので $\text{Gal}(L/\mathbb{Q}) \cong C_3 \neq \{\text{id}_L\}$ となる。
 だから, L/\mathbb{Q} の自己同型 (L の \mathbb{Q} 上での自己同型) が id_L しか存在しないものを作るためには, Galois 拡大では ない 3 次拡大 L/\mathbb{Q} を作らなければいけない。
 しかし, そのような例は問題?-?ですでに作っている。 □

定義 n 次の置換群 S_n の部分群 G が 推移的 (可移的, transitive) であるとは、
任意の $i, j \in \{1, 2, \dots, n\}$ についてある $\sigma \in G$ で $\sigma(i) = j$ をみたすものが
存在することをと定める。

問題 8-2 S_3 の推移的部分群をすべて挙げよ。 \square

問題 8-3 S_4 の以下の 11 個の部分群を考える：

$$H_1 = \{1\}, \quad H_2 = \langle (1, 2) \rangle, \quad H_3 = \langle (1, 2)(3, 4) \rangle, \quad H_4 = \langle (1, 2, 3) \rangle,$$

$$H_5 = \langle (1, 2, 3, 4) \rangle, \quad H_6 = \langle (1, 2), (3, 4) \rangle, \quad H_7 = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\},$$

$$H_8 = \langle (1, 2), (2, 3) \rangle \cong S_3, \quad H_9 = \langle (1, 2, 3, 4), (1, 3) \rangle, \quad H_{10} = A_4, \quad H_{11} = S_4.$$

(1) 各々の位数を求めよ。

(2) 各々について S_4 の正規部分群かどうか判定せよ。

(3) 各々について推移的であるかどうか判定せよ。 \square

定理

p は素数であるとする. このとき, S_p の推移的な部分群 G で“互換を 1つ以上含むものは S_p 全体に一致する.

証明

① $\{1, 2, \dots, p\}$ に同値関係 \sim を

$$i \sim j \Leftrightarrow i = j \text{ または } i \neq j \text{ で } (i, j) \in G$$

と定められることを示そう.

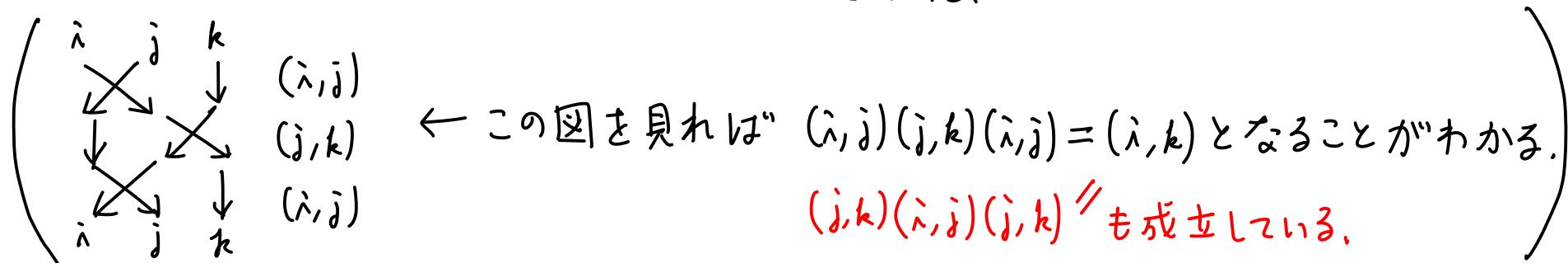
反射律 ($i \sim i$) と対称律 ($i \sim j \Rightarrow j \sim i$) をめたすことは自明なので,
推移律 ($i \sim j$ かつ $j \sim k \Rightarrow i \sim k$) のみを示せばよい.

$i \sim j$ かつ $j \sim k \Rightarrow i \sim k$ を i, j, k が互いに異なる場合に示せばよい.

$i \neq j, i \neq k, j \neq k, i \sim j, j \sim k$ と仮定する.

$(i, j), (j, k) \in G$ なので $G \ni (i, j)(j, k)(i, j) = (i, k)$ となり, $i \sim k$ となる.

これで \sim が同値関係になることが示された.



2 $\sigma \in G$ かつ $i \sim j \Rightarrow \sigma(i) \sim \sigma(j)$ となることを示そう.

$\sigma \in G$, $i \sim j$ と仮定する.

(i) $i = j$ のとき $\sigma(i) = \sigma(j)$ なので $i \sim j$,

(ii) $i \neq j$, $(i, j) \in G$ のとき, $\sigma(i) \neq \sigma(j)$ でかつ $G \ni \sigma(i, j) \sigma^{-1} = (\sigma(i), \sigma(j))$ なので $\sigma(i) \sim \sigma(j)$.

σ は全単射

一般に, 巡回置換 (i_1, \dots, i_ℓ) (i_1, \dots, i_ℓ が互いに異なり, $i_{\ell+1} = i_1$ とおくと,
 (i_1, \dots, i_ℓ) は i_ν を $i_{\nu+1}$ にうつす) について,

$$\sigma(i_1, \dots, i_\ell) \sigma^{-1}(\sigma(i_\nu)) = \sigma(i_1, \dots, i_\ell)(i_\nu) = \sigma(i_{\nu+1})$$

$$\text{なので } \sigma(i_1, \dots, i_\ell) \sigma^{-1} = (\sigma(i_1), \dots, \sigma(i_\ell)).$$

これで, $\sigma \in G$ かつ $i \sim j \Rightarrow \sigma(i) \sim \sigma(j)$ が示された.

3 へのすべての同値類の元の個数が等しいことを示そう。

への同値類を $[i]$ と書き、 $i, j \in \{1, 2, \dots, p\}$ を任意にとる。

G は推移的なのである $\sigma \in G$ が存在して $\sigma(i) = j$ となる。

2 より、任意の $i', j' \in \{1, 2, \dots, p\}$ について、

$$i \sim i' \stackrel{\text{①}}{\Rightarrow} j \sim \sigma(i') \quad \text{かつ} \quad j \sim j' \stackrel{\text{②}}{\Rightarrow} i \sim \sigma^{-1}(j')$$

なので、 $\sigma([i]) = \{\sigma(i') \mid i \sim i'\} = [j]$ となることがわかる。 ←

$j' \in \sigma([i])$ のとき、 $j' = \sigma(i')$ 、 $i \sim i'$ と書けるので ① より $j \sim j'$ なので $j' \in [j]$ 。
 $j' \in [j]$ のとき、 $i' = \sigma^{-1}(j')$ とおくと、② より $i \sim i'$ となり、 $j' = \sigma(i')$ となるので
 $j' \in \sigma([i])$ となる。

σ は $\{1, 2, \dots, p\}$ からそれ自身への全単射なので、

$[i]$ と $[j]$ の元の個数は等しい。

これで へのすべての同値類の元の個数が等しいことが示された。

④ ~の同値類は $\{1, 2, \dots, p\}$ の全体になることを示そう. (ここで p が素数)
(なことを使う.)

G は互換を 1つ以上含むので、2つ以上の元を含む同値類が存在する.

③ より、 $\{1, 2, \dots, p\}$ は 2 以上の同じ個数の元を含む同値類たちに分割されていくことになる.

しかし、 p は素数なので そのような分割での同値類は $\{1, 2, \dots, p\}$ のただ 1つだけになる.

⑤ G が S_p のすべての互換を含むことを示そう.

$i \in \{1, 2, \dots, p\}$ を任意にとる. ④ より

$$[\hat{i}] = \{j \mid i=j \text{ または } i \neq j \text{ で } (i, j) \in G\} = \{1, 2, \dots, p\}$$

なので、 \hat{i} とは異なるすべての j について $(\hat{i}, j) \in G$.

⑥ S_p はすべての互換から生成されるので ⑤ より $G = S_p$. □

問題 8-4 $f(x) \in \mathbb{Q}[x]$ は \mathbb{Q} 上既約な多項式であるとし,

L は f の \mathbb{Q} 上での最小分解体であるとし, $G = \text{Gal}(L/\mathbb{Q})$ とおく. 以下を示せ.

(1) $f(x)$ の互いに異なる根全体を $\alpha_1, \dots, \alpha_n \in L$ と書くと,
 $G = \text{Gal}(L/\mathbb{Q})$ は $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ に推移的に作用する.
(↑ f の \mathbb{Q} 上で既約性を使う.)

(任意の $i, j \in \{1, 2, \dots, n\}$ についてある $\sigma \in G$ が存在して $\sigma(\alpha_i) = \alpha_j$)

(2) $n = \deg f$ が素数かつ $f(x)$ がちょうど $n-2$ 個の実根を持つならば
 $G = \text{Gal}(L/\mathbb{Q}) \cong S_n$ となる.

(3) $f(x) = x^5 - 16x + 2$ が \mathbb{Q} 上既約で,

f の \mathbb{Q} 上での最小分解体 L について, $\text{Gal}(L/\mathbb{Q}) \cong S_5$.

□

問題 8-1 K, L は \mathbb{C} の部分体であるとする。 次数0を使う。

(1) L/K が 2 次拡大ならば L/K は Galois 拡大であることを示せ。

(2) 2 次以上の有限次拡大 L/K で L の K 上での体の自己同型が id_L しか存在しないものの例を具体的に 1 つ挙げよ。 LからLへの写像

解答例 K, L は \mathbb{C} の部分体であると仮定する。

(1) L/K は 2 次拡大であると仮定し、

L の K 上のベクトル空間としての基底 $1, \theta$ をとる。

このとき、 $L = K(\theta)$ かつ $\theta^2 \in L$ は $\theta^2 = a + b\theta$, $a, b \in K$ と表わされる。

θ は $F(x) = x^2 - ax - b \in K[x]$ の根になり、

もう 1 つの根は解と係数の関係より $-\frac{b}{a} \in L$ と表わされる。 ← ポイント！

ゆえに、 L は $F(x)$ の 2 つの根を含み、 K 上での $F(x)$ の最小分解体になり、

L/K は 2 次の Galois 拡大になる。

注意 $\alpha = \theta - \frac{b}{2}$ とおくと $\alpha^2 = \theta^2 - b\theta + \frac{b^2}{4} = a + b\theta - b\theta + \frac{b^2}{4} = \frac{b^2 + 4a}{4} \in K$.

$L = K(\alpha)$ となり、 $\text{Gal}(L/K) = \langle \sigma \rangle$, $\sigma(f(\alpha)) = f(-\alpha)$ ($f(x) \in K[x]$) となる。

つづき

(2) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$ とおくと, $[L:K] = 3$ で, $L \cong \mathbb{Q}[x]/(x^3 - 2)$

$\text{Aut}_K L := \{\sigma: L \rightarrow L \mid \sigma \text{ は } K \text{ 上での体の自己同型}\} = \{\text{id}_L\}$.

$\omega = \frac{-1 + \sqrt{-3}}{2}$ とおくと, $\sqrt[3]{2}$ の \mathbb{Q} 上での共役元の全体は $\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2}$

の 3 つになるが, $\omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$ なので, $\sigma \in \text{Aut}_K L$ について,

$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ が成立しており, $\sigma = \text{id}_L$ となる.

L の元を

その K 上での共役元にうつす.

□

Galois 拡大になっている拡大とそうでない拡大をノータイムで
挙げられるようになっておいてください!

定義 n 次の置換群 S_n の部分群 G が 推移的 (可移的, transitive) であるとは、
任意の $i, j \in \{1, 2, \dots, n\}$ についてある $\sigma \in G$ で $\sigma(i) = j$ をみたすものが
存在することをと定める。

問題 8-2 S_3 の推移的部分群をすべて挙げよ。 \square

解答例 以前やったように S_3 のすべての部分群は

$\{1\}, \{1, (1, 2)\}, \{1, (1, 3)\}, \{1, (2, 3)\}, A_3 = \{1, (1, 2, 3), (1, 3, 2)\}, S_3$
の6個である。この中で推移的なのは、 A_3 と S_3 の2つだけである。
推移的であるかどうかはその部分群の作用で1を2, 3に移せるかどうかを
石窟認すればよい。

$\{1\}$ は1を2にも3にも移せない。

$\{1, (1, 2)\}$ は1を3に移せず、 $\{1, (1, 3)\}$ は1を2に移せず、

$\{1, (2, 3)\}$ は1を2にも3にも移せない。

$\{1, (1, 2, 3), (1, 3, 2)\}$ の $(1, 2, 3)$ によると1を2に移せ、 $(1, 3, 2)$ によると1を3に
移せる。 $\{1, (1, 2, 3), (1, 3, 2)\} \subset S_3$ なので S_3 についても同様である。 \square

問題8-3 S_4 の以下の 11 個の部分群を考える:

$$H_1 = \{1\}, H_2 = \langle(1, 2)\rangle, H_3 = \langle(1, 2)(3, 4)\rangle, H_4 = \langle(1, 2, 3)\rangle,$$

$$H_5 = \langle(1, 2, 3, 4)\rangle, H_6 = \langle(1, 2), (3, 4)\rangle, H_7 = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\},$$

$$H_8 = \langle(1, 2), (2, 3)\rangle \cong S_3, H_9 = \langle(1, 2, 3, 4), (1, 3)\rangle, H_{10} = A_4, H_{11} = S_4.$$

(1) 各々の位数を求めよ.

(2) 各々について S_4 の正規部分群かどうか判定せよ.

(3) 各々について推移的であるかどうか判定せよ.

$$\begin{array}{ccc} C_4 & C_2 \times C_2 & C_2 \times C_2 \\ \text{SII} & \text{SII} & \text{SII} \end{array}$$

解答例 (1) $|H_1| = 1, |H_2| = |H_3| = 2, |H_4| = 3, |H_5| = |H_6| = |H_7| = 4,$

$$|H_8| = 6, |H_9| = 8, |H_{10}| = 12, |H_{11}| = 24.$$

(2) 以前 S_4 の正規部分群は $H_1 = \{1\}, H_7 = (\text{Klein の四元群}), H_{10} = A_4, H_{11} = S_4$ の 4つしかないことを示した.

(3) 推移的かどうかは 1 を 2, 3, 4 に移せることを確認すればよい,

推移的なのは, $H_5 \cong C_4, H_7 = (\text{Klein の四元群}) \cong C_2 \times C_2, H_9 \cong D_4,$

$H_{10} = A_4, H_{11} = S_4$ の 5つ, (既約な4次式の最小分解体の Galois 群はこれら 5つの中からになる。)

□

定理 p は素数であるとする. このとき, S_p の推移的な部分群 G で互換を 1 つ以上含むものは S_p 全体に一致する. \square

← 08-3 で証明した.

問題 8-4 $f(x) \in \mathbb{Q}[x]$ は \mathbb{Q} 上既約な多項式であるとし,

L は f の \mathbb{Q} 上での最小分解体であるとし, $G = \text{Gal}(L/\mathbb{Q})$ とおく. 以下を示せ.

(1) $f(x)$ の互いに異なる根全体を $\alpha_1, \dots, \alpha_n \in L$ と書くと,
 $G = \text{Gal}(L/\mathbb{Q})$ は $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ に推移的に作用する.

（ f の \mathbb{Q} 上での既約性を使う.）

（任意の $i, j \in \{1, 2, \dots, n\}$ についてある $\sigma \in G$ が存在して $\sigma(\alpha_i) = \alpha_j$.）

(2) $n = \deg f$ が素数かつ $f(x)$ がちょうど $n-2$ 個の実根を持つならば
 $G = \text{Gal}(L/\mathbb{Q}) \cong S_n$ となる.

(3) $f(x) = x^5 - 16x + 2$ が \mathbb{Q} 上既約で,

f の \mathbb{Q} 上での最小分解体 L について, $\text{Gal}(L/\mathbb{Q}) \cong S_5$. \square

解答例 (1) $\text{Gal}(L/\mathbb{Q})$ が $\{\alpha_1, \dots, \alpha_n\}$ に推移的に作用していないならば $f(x)$ が \mathbb{Q} 上既約にならなことを示せば十分である. ($f(x)$ の既約性に反する.)

$\text{Gal}(L/\mathbb{Q})$ が $\{\alpha_1, \dots, \alpha_n\}$ に推移的に作用していないと仮定する.

$A = \{\sigma(\alpha_i) \mid \sigma \in \text{Gal}(L/\mathbb{Q})\}$ とおく, A は $\text{Gal}(L/\mathbb{Q})$ の作用で閉じている.

$\text{Gal}(L/\mathbb{Q})$ は $\{\alpha_1, \dots, \alpha_n\}$ に推移的に作用していないとすると,

$|A| < n$ となる.

$$g(x) = \prod_{\beta \in A} (x - \beta) = \sum_k c_k x^k, \quad c_k \in L \text{ とおくと,}$$

$$\begin{pmatrix} \forall \sigma \in \text{Gal}(L/\mathbb{Q}) \\ \sigma(c_k) = c_k \end{pmatrix}$$

↑

$$\text{任意の } \sigma \in \text{Gal}(L/\mathbb{Q}) \text{ について } \sum_k \sigma(c_k) x^k = \prod_{\beta \in A} (x - \sigma(\beta)) = \prod_{\gamma \in A} (x - \gamma) = g(x)$$

又のて, $c_k \in L^{\text{Gal}(L/\mathbb{Q})} = \mathbb{Q}$, $g(x) \in \mathbb{Q}[x]$.

n 次の $f(x) \in \mathbb{Q}[x]$ はより低次の $g(x) \in \mathbb{Q}[x]$ で割りきれるので,
 $f(x)$ は \mathbb{Q} 上既約ではない,

- (2) ① \mathbb{Q} 上既約な $f(x) \in \mathbb{Q}[x]$ の次数 n は素数であり,
 $f(x)$ はちょうど $n-2$ 個の実根 $\alpha_1, \dots, \alpha_{n-2}$ を持つと仮定する.
このとき, $f(x)$ はちょうど 2 つの虚根 $\beta, \bar{\beta} \in \mathbb{C} \setminus \mathbb{R}$ を持つ.
- ② $f(x)$ の \mathbb{Q} 上での最小分解体 $L = \mathbb{Q}(\alpha_1, \dots, \alpha_{n-2}, \beta, \bar{\beta})$ には
複素共役を取る操作で \mathbb{Q} 上での自己同型として作用する.
ゆえに, $\text{Gal}(L/\mathbb{Q})$ は $\{\alpha_1, \dots, \alpha_{n-2}, \beta, \bar{\beta}\}$ の β と $\bar{\beta}$ の互換で言む.
- ③ $f(x)$ は \mathbb{Q} 上既約なので, (1) より, $\text{Gal}(L/\mathbb{Q})$ は $\{\alpha_1, \dots, \alpha_{n-2}, \beta, \bar{\beta}\}$
に推移的に作用する.
- ④ n は素数なので定理を適用でき, $\text{Gal}(L/\mathbb{Q})$ が $\{\alpha_1, \dots, \alpha_{n-2}, \beta, \bar{\beta}\}$
の置換全体に一致することがわかる: $\text{Gal}(L/\mathbb{Q}) \cong S_n$.

(3) $f(x) = x^5 - 16x + 2$ とおく、
 Eisenstein の判定法で既約性を示せる場合はまれである。
 わざわざ そのように問題を作っている。

$2+1, 2|0, 2|0, 2|0, 2|-16, 2|2, 2^2+2$ と Eisenstein の判定法より、
 $f(x)$ は \mathbb{Q} 上既約である。実函数としての $f(x)$ のグラフの形を調べよう。

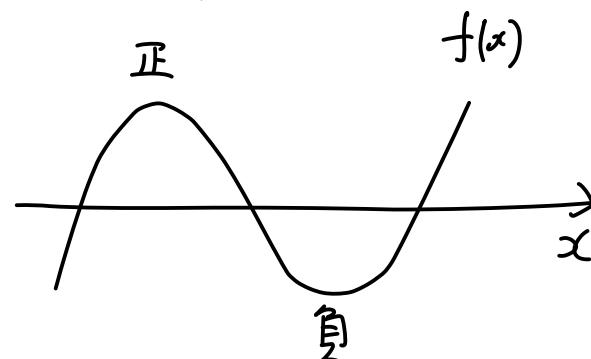
$$f'(x) = 5x^4 - 16 = 5\left(x^4 - \frac{16}{5}\right) = 5\left(x + \frac{2}{5^{1/4}}\right)\left(x - \frac{2}{5^{1/4}}\right)\left(x^2 + \frac{4}{\sqrt{5}}\right).$$

$$f\left(-\frac{2}{5^{1/4}}\right) = -\frac{32}{5 \cdot 5^{1/4}} + \frac{32}{5^{1/4}} + 2 = 2 + \frac{128}{5 \cdot 5^{1/4}} > 0 \quad \text{(注) } \frac{128}{5 \cdot 5^{1/4}} = 17.11975\dots$$

$$f\left(\frac{2}{5^{1/4}}\right) = \frac{32}{5 \cdot 5^{1/4}} - \frac{32}{5^{1/4}} + 2 = 2 - \frac{128}{5 \cdot 5^{1/4}} < 2 - \frac{128}{5 \cdot 2} < 0$$

$5^{1/4} < 2$ より

x	$-\infty$	$-2/5^{1/4}$	$2/5^{1/4}$	∞
$f(x)$	$-\infty$	↑ 正	↓ 負	↑ ∞
$f'(x)$	∞	+	0	- 0 + ∞

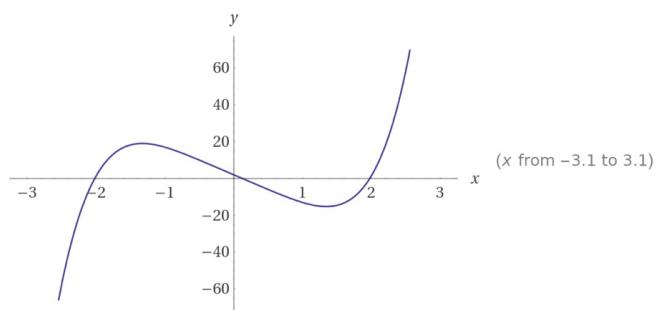
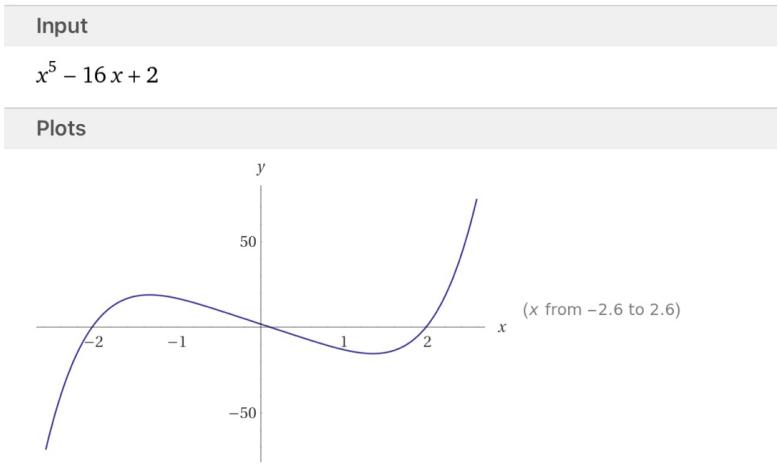


これより、 $f(x)$ はちょうど 3 つの実根をもつ。

ゆえに、(2) より、このとき $\text{Gal}(L/\mathbb{Q}) \cong S_5$ となる。

□

<https://www.wolframalpha.com/input/?i=x%5E5%20-%2016x%20%2B%202>



Local maximum

$$\max\{x^5 - 16x + 2\} = 2 + \frac{128}{5\sqrt[4]{5}} \text{ at } x = -\frac{2}{\sqrt[4]{5}}$$

[Approximate form](#)

[Step-by-step solution](#)

Local minimum

$$\min\{x^5 - 16x + 2\} = 2 - \frac{128}{5\sqrt[4]{5}} \text{ at } x = \frac{2}{\sqrt[4]{5}}$$

[Approximate form](#)

[Step-by-step solution](#)

Real roots

$$x \approx 0.125002$$

$$x \approx 1.96745$$

$$x \approx -2.0301$$

[Exact forms](#) [More digits](#)

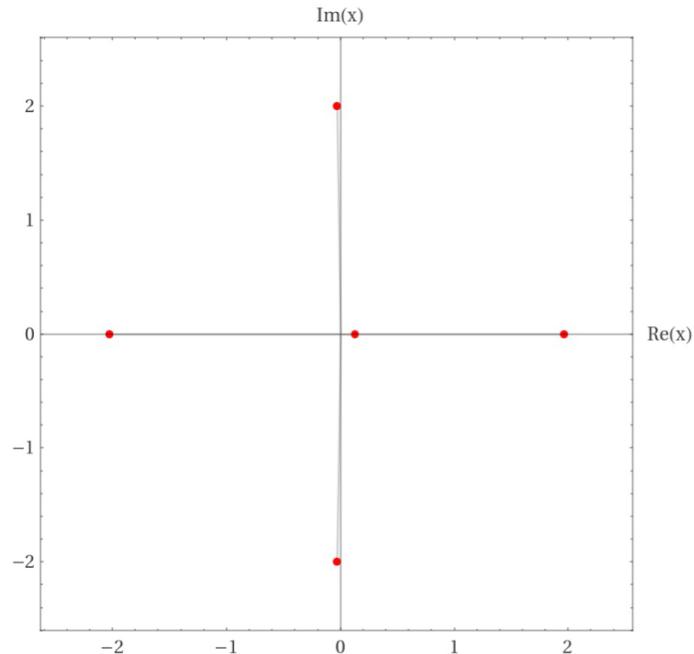
Complex roots

$$x = -0.0311742 - 2.00122i$$

$$x = -0.0311742 + 2.00122i$$

[Exact forms](#)

Roots in the complex plane



問題 9-1 (\mathbb{F}_p の代数閉包)

p は素数であるとし, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ とおく. \mathbb{F}_p は位数 p で標数 p の有限体になる.

且つは代数閉体であるような \mathbb{F}_p の拡大体であるとする. $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ と書く.
(このような Ω の存在は Steinitz の定理によって保証される.) 以下を示せ:

(1) Ω の任意の部分体 K は \mathbb{F}_p を含む.

(2) $n = 1, 2, 3, \dots$ について, $F_n(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ とおく,

Ω における $F_n(x)$ の根全体を $L_n = \{\alpha \in \Omega \mid F_n(\alpha) = 0\}$ と書く.

このとき, L_n は Ω に含まれる唯一つの位数 p^n の有限部分体になる.

以下, $\mathbb{F}_{p^n} = L_n$ とおく.

(3) $m|n$ のとき, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$

(4) $L_\infty = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ とおく, L_∞ は \mathbb{F}_p の代数閉包になる.

□

注意 上の結果は大雑把に言って, 標数 p の Ω への有限体の和集合

といふ, \mathbb{F}_p の代数閉包が得られることを意味している: $\overline{\mathbb{F}_p} = \bigcup_n \mathbb{F}_{p^n}$.

一般の場合とちがって, \mathbb{F}_p の代数閉包は特別に易しい.

□

問題 9-2 Artin の定理 (08-2 でやった) を認めて以下を示せ.

k は体であるとし, $L = k(t_1, \dots, t_n)$ は体 k 上の n 変数有理函数体であるとする. t_1, \dots, t_n の基本対称式 e_1, \dots, e_n を次のように定める:

$$e_r = \sum_{1 \leq i_1 < \dots < i_r \leq n} t_{i_1} \cdots t_{i_r}. \quad \leftarrow \binom{n}{r} \text{ 項の式.}$$

たとえば, $n = 3$ のとき,

$$e_1 = t_1 + t_2 + t_3, \quad e_2 = t_1 t_2 + t_1 t_3 + t_2 t_3, \quad e_3 = t_1 t_2 t_3,$$

L の部分体 K を $K = k(e_1, \dots, e_n)$ と定める. 以下を示せ.

(1) L は $F(x) = x^n + \sum_{r=1}^n (-1)^r e_r x^{n-r} \in K[x]$ の K 上での最小分解体である.

(2) $[L : K] = n!$

(3) $\text{Gal}(L/K) \cong S_n.$

□

ヒント L への S_n の自然な作用に関する L^{S_n} を K' と書く.

Artin の定理より, $\text{Gal}(L/K') \cong S_n$, $[L : K'] = n!$ となる.

$K \subset K'$ なので $[L : K] \geq n!$ がわかる. $[L : K] \leq n!$ を示せば $K = K'$ が得られる. □

問題 9-1 (\mathbb{F}_p の代数閉包)

p は素数であるとし, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ とおく, \mathbb{F}_p は位数 p で標数 p の有限体になる.

且は代数閉体であるような \mathbb{F}_p の拡大体であるとする. $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ と書く、
(そのような Ω の存在は Steinitz の定理により保証される.) 以下を示せ:

(1) Ω の任意の部分体 K は \mathbb{F}_p を含む.

(2) $n = 1, 2, 3, \dots$ について, $F_n(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ とおく,

Ω における $F_n(x)$ の根全体を $L_n = \{\alpha \in \Omega \mid F_n(\alpha) = 0\}$ と書く.

このとき, L_n は Ω に含まれる唯一つの位数 p^n の有限部分体になる.

以下, $\mathbb{F}_{p^n} = L_n$ とおく.

(3) $m|n$ のとき, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$

(4) $L_\infty = \bigcup_{n=1}^{\infty} L_n = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ とおく, L_∞ は \mathbb{F}_p の代数閉包になる:

$$\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$$

解答例 (1) K は Ω の部分体であるとする. $0, 1 \in K$ で, $2 = 1+1, \dots, p-1 = \underbrace{1+\dots+1}_{p-1 \text{個}}$ も K の元になるので $\mathbb{F}_p = \{0, 1, \dots, p-1\} \subset K$.

(2) ① L_n が \mathbb{Q} の部分体になることを示す.

$\alpha, \beta \in L_n$ と仮定する. $0, 1, \alpha + \beta, \alpha\beta \in L_n$ かつ $\alpha \neq 0$ のとき $\alpha^{-1} \in L_n$ となることを示せばよい. 様数 p の世界なので $(a+b)^p = a^p + b^p$ が成立している.

$$F_n(0) = 0^{p^n} - 0 = 0 \text{ なので } 0 \in L_n.$$

$$F_n(1) = 1^{p^n} - 1 = 0 \text{ なので } 1 \in L_n$$

$$F_n(\alpha + \beta) = (\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} + \beta^{p^n} - (\alpha + \beta) = F_n(\alpha) + F_n(\beta) = 0 + 0 = 0,$$

ゆえに $\alpha + \beta \in L_n$.

α または β が 0 ならば $\alpha\beta = 0 \in L_n$ は自明なので $\alpha \neq 0, \beta \neq 0$ と仮定する.

$$\alpha, \beta \text{ は } F_n(x) = x^{p^n} - x = x(x^{p^n-1} - 1) \text{ の } 0 \text{ でない根なので } x^{p^n-1} - 1 \text{ の根になるので, } F_n(\alpha\beta) = \alpha\beta((\alpha\beta)^{p^n-1} - 1) = \alpha\beta(\underbrace{\alpha^{p^n-1}}_{=1} \underbrace{\beta^{p^n-1}}_{=1} - 1) = 0,$$

ゆえに, $\alpha\beta \in L_n$.

さて, $\alpha \neq 0$ のとき,

$$F_n(\alpha^{-1}) = \alpha^{-1}((\alpha^{-1})^{p^n-1} - 1) = \alpha^{-1}(\underbrace{(\alpha^{p^n-1})^{-1}}_{=1} - 1) = 0$$

なので $\alpha^{-1} \in L_n$.

2) $|L_n| = p^n$ を示そう,

$F_n(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ が重根を持たないことを示せばよい.

$F'_n(x) = -1$ なので $F_n(x)$ と $F'_n(x)$ の共通根は存在しない.

ゆえに, $F_n(x)$ は重根を持たない.

3) K を \mathbb{F} の位数 p^n の部分体とすると, $K = L_n$ となることを示そう.

$0 \in K$ は $F_n(x) = x(x^{p^n-1} - 1)$ の根であり, K^\times は位数 $p^n - 1$ の有限群になるので,
任意の $\alpha \in K^\times$ は $\alpha^{p^n-1} = 1$ をみたし, $F_n(x)$ の根になる

ゆえに, $K \subset L_n$, $|K| = p^n = |L_n|$ なので $K = L_n$.

以下, $\mathbb{F}_{p^n} = L_n$ とおく.

(3) $m|n$ のとき, $n = lm$ と書くと, $\therefore M$ とおく $\therefore N$ とおく.

$$p^n - 1 = p^{lm} - 1 = (p^m)^l - 1 = \overbrace{(p^m - 1)}^{} \left(\overbrace{p^{m(l-1)} + p^{m(l-2)} + \dots + p^m + 1}^{} \right).$$

$$\begin{aligned} F_n(x) &= x(x^{p^n-1} - 1) = x(x^{MN} - 1) = x(x^M - 1)(x^{M(N-1)} + x^{M(N-2)} + \dots + x^M + 1) \\ &= F_m(x)(x^{M(N-1)} + \dots + x^M + 1). \end{aligned}$$

ゆえに, $F_m(x)$ の根は $F_n(x)$ の根になるので $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$.

(4) ① $\alpha, \beta \in L_\infty$ に対して、ある m, n で $\alpha \in \mathbb{F}_{p^m}, \beta \in \mathbb{F}_{p^n}$ となるもののが存在する。

(3) より、 $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^{mn}} \subset \mathbb{F}_{p^n}$ なので $\alpha, \beta \in \mathbb{F}_{p^{mn}}, \alpha + \beta, \alpha\beta \in \mathbb{F}_{p^{mn}} \subset L_\infty$ となる。

$\alpha \neq 0$ なら $\alpha^{-1} \in \mathbb{F}_{p^{mn}} \subset L_\infty$ 。これより、 L_∞ が \mathbb{Q} の部分体になることがある。

② $\mathbb{F}_{p^n} = L_n$ の元は $F_n(x) \in \mathbb{F}_p[x]$ の根なので \mathbb{F}_p 上代数的である。

ゆえに、 $L_\infty = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ のすべての元は \mathbb{F}_p 上代数的である。

③ $\alpha \in \mathbb{Q}$ を \mathbb{F}_p 上代数的な元とする。

L_∞ が \mathbb{F}_p の代数閉包であることを示すには $\alpha \in L_\infty$ を示せばよい。

$L = \mathbb{F}_p(\alpha), n = [L : \mathbb{F}_p]$ とおくと、 L は \mathbb{F}_p 上 n 次元のベクトル空間になるので $|L| = p^n$ なので、 L は \mathbb{Q} の位数 p^n の有限部分体である。

(2) より $L = L_n = \mathbb{F}_{p^n} \subset L_\infty$ となる。これより $\alpha \in L_\infty$ が得られる。 \square

問題 9-2 Artin の定理 (08-2 でやった) を認めて以下を示せ.

(注) 有理式
||
有理函数

k は体であるとし, $L = k(t_1, \dots, t_n)$ は体 k 上の n 変数有理函数体であるとする. t_1, \dots, t_n の基本対称式 e_1, \dots, e_n を次のように定める:

$$e_r = \sum_{1 \leq i_1 < \dots < i_r \leq n} t_{i_1} \cdots t_{i_r}. \quad \leftarrow \binom{n}{r} \text{ 項の式.}$$

たとえば, $n = 3$ のとき,

$$e_1 = t_1 + t_2 + t_3, \quad e_2 = t_1 t_2 + t_1 t_3 + t_2 t_3, \quad e_3 = t_1 t_2 t_3,$$

L の部分体 K を $K = k(e_1, \dots, e_n)$ と定める. 以下を示せ.

(1) L は $F(x) = x^n + \sum_{r=1}^n (-1)^r e_r x^{n-r} \in K[x]$ の K 上での最小分解体である.

$$(2) [L : K] = n!$$

$$(3) \text{Gal}(L/K) \cong S_n.$$

$$=(-1)^r e_r$$

□

解答例 (1) $\prod_{i=1}^n (x - t_i) = x^n + \underbrace{\sum_{1 \leq i_1 < \dots < i_r \leq n} (-t_{i_1}) \cdots (-t_{i_r})}_{=(-1)^r e_r} x^{n-r} = F(x).$

ゆえに, $F(x)$ の根の全体は t_1, \dots, t_n になる.

$$L \subset K(t_1, \dots, t_n) \subset k(t_1, \dots, t_n) = L \text{ より}, \quad L = K(t_1, \dots, t_n).$$

これで, L が $F(x)$ の K 上での最小分解体であることがわかった.

(2) と (3) を示そう.

① S_n の L への作用を, $\sigma \in S_n$ と $f(t_1, \dots, t_n) \in L = k(t_1, \dots, t_n)$ について
 $\sigma(f(t_1, \dots, t_n)) = f(t_{\sigma(1)}, \dots, t_{\sigma(n)})$ と定めることがで“きる.

各 $\sigma \in S_n$ の作用は L の体の自己同型になつて“いる.

これによつて, L の自己同型群の部分群 G で “ S_n と同型なものが得られた.

$K' = L^G$ とおくと, Artin の定理より, L/K' は有限次 Galois 延長で,

$$\text{Gal}(L/K') = G \cong S_n, \quad [L : K'] = |G| = n!$$

ゆえに, $K = K'$ を示せれば (2), (3) が示されたことになる.

② $\sigma \in S_n$ について, $\sigma(e_r) = e_r$ (e_r は対称式) なので, $e_1, \dots, e_n \in K'$.
 $k \subset K'$ であるので $K = k(e_1, \dots, e_n) \subset K'$ で $[L : K] \geq [L : K'] = n!$

③ t_1, t_2, \dots, t_m の基本対称式を e'_1, \dots, e'_m と書き,
 $t_{m+1}, t_{m+2}, \dots, t_n$ の基本対称式を e''_1, \dots, e''_{n-m} と書き,
 $e'_{r'} = 0$ ($r' > m$), $e''_{r''} = 0$ ($r'' > n-m$) と約束しておく.

$$\prod_{i=1}^m (x - t_i) \times \prod_{i=m+1}^n (x - t_i) = \prod_{i=1}^n (x - t_i) \text{ より}$$

$$\left(x^m + \sum_{r'=1}^m (-1)^{r'} e'_{r'} x^{m-r'} \right) \left(x^{n-m} + \sum_{r''=1}^{n-m} (-1)^{r''} e''_{r''} x^{n-m-r''} \right) = x^n + \sum_{r=1}^n (-1)^r e_r x^{n-r}.$$

ゆえに

$$\left\{ \begin{array}{l} e''_1 + e'_1 = e_1 \\ e''_2 + e'_1 e''_1 + e'_2 = e_2 \\ e''_3 + e'_1 e''_2 + e'_2 e''_1 + e'_3 = e_3 \\ \cdots \cdots \cdots \\ e''_{n-m} + e'_1 e''_{n-m-1} + e'_2 e''_{n-m-2} + \cdots = e_{n-m} \end{array} \right.$$

これは上から順に e''_1, e''_2, \dots について解けて, e''_1, \dots, e''_{n-m} が
 e_r と $e'_{r'}$ たちの多項式で書けることがわかる.

④ $L_m = K(t_1, \dots, t_m)$ ($m=1, \dots, n$), $L_0 = K$ とおく。このとき、

$$L_m = L_{m-1}(t_m), \quad K = L_0 \subset L_1 \subset \dots \subset L_n = L.$$

⑤ さきに ③ より、 $e''_1, \dots, e''_{n-m} \in K(e'_1, \dots, e'_m) \subset K(t_1, \dots, t_m) = L_m$ である、

$F_m(x) = (x - t_{m+1})(x - t_{m+2}) \dots (x - t_n)$ ($m=0, 1, \dots, n-1$) とおくと、

$$F_m(x) = x^{n-m} + \sum_{r''=1}^{n-m} (-1)^{r''} e''_{r''} x^{n-m-r''} \in L_m[x],$$

⑥ t_{m+1} は $F_m(x)$ の根なので $[L_{m+1} : L_m] = [L_m(t_{m+1}) : L_m] \leq n-m$.

⑦ ゆえに、
 $[L : K] = [L_n : L_{n-1}] \cdots [L_2 : L_1] [L_1 : L_0] \leq n!$
 $\leq 1 \quad \leq n-1 \quad \leq n$

⑧ これと ② を合わせると、 $K = K'$ が得られる。

$$\hookrightarrow K \subset K', [L : K] \geq [L : K'] = n!$$

q.e.d.

次の定理を証明したい。

定理 (可換な) 体 K の乗法群 K^\times の有限部分群 G は巡回群になる。

証明 1 (有限生成 Abel 群の基本定理を使う方法)

G は有限 Abel 群なので有限生成 Abel 群の基本定理より,

$$G \cong C_N \times C_{N_1} \times \cdots \times C_{N_r}, \quad N_r | N_{r-1} | \cdots | N_1 | N, \quad N, N_i \in \mathbb{Z}_{>0}$$

と書ける。ここで、 C_n は位数 n の巡回群を表す。このとき、 $|G| = N N_1 \cdots N_r \geq N$ 。

N_1, \dots, N_r がすべて N の約数になっていることより,

G の任意の元の位数が N の約数になっていることがわかる。

ゆえに任意の $a \in G$ について $a^N = 1$ 。すなわち、 $G \subset \{a \in K \mid a^N = 1\}$,

K は体なので $x^N - 1$ の K に含まれる根の個数は N 以下である。

したがって、 $|G| \leq |\{a \in K \mid a^N = 1\}| \leq N$.

$|G| \geq N$ もあったので $|G| = N$.

これは $G = C_N$ を意味する。 \square

証明2 (初等的な証明)

$N = |G|$ とおく。 G が位数 N の元を含むことを示せばよい。
 そのためには、 $a \in G$ の位数 m が N より小さいならば、 a から位数が a より
 大きな G の元を作れることを示せば十分である。

$a \in G$ の位数 m は N より小さいと仮定する。

$\langle a \rangle$ の位数は m で、 $\langle a \rangle$ の元の m 乗はどれも 1 になる。

K は体なので K に含まれる $x^m - 1$ の根の個数は m 以下である。

ゆえに、 $\langle a \rangle = \{x \in K \mid x^m = 1\}$ 。

$m < N$ より $\langle a \rangle \neq G$ となるので、ある $b \notin \langle a \rangle$ が存在する。

b の位数 n は、 $b \notin \langle a \rangle = \{x \in K \mid x^m = 1\}$ より、 m の約数ではない。

$$\left(\begin{array}{l} m = nm' \text{ ならば} \\ b^m = b^{nm'} = 1, \\ \therefore b \in \langle a \rangle \\ \text{で矛盾する。} \end{array} \right)$$

a の位数 m と b の位数 n の最大公約数を g と書き、 $c = b^g$ とおく。

n は g で割り切れるが、 n は m の約数ではないので $n > g$ 。

c の位数は $\frac{n}{g} > 1$ になり、 $\frac{n}{g}$ と m の最大公約数は 1 になる。

このことから、 ac の位数が $m \frac{n}{g} > m$ となることがわかる。

次ページで示す。

□

上の証明の最後で次を使いたく。

補題 G は群であるとし、 $a, b \in G$ は互いに可換であると仮定する。

a の位数 m と b の位数 n の最大公約数が 1 ならば ab の位数は mn になる。

証明 (本質的に中国式剰余定理)

ab の位数を ℓ と書く。

$(ab)^{mn} = (a^m)^n (b^n)^m = 1^n 1^m = 1$ より、 ℓ は mn の約数になる。

m と n の最大公約数は 1 なので、ある $r, s \in \mathbb{Z}$ が存在して $rm + sn = 1$. ← Euclid の互除法

このとき、
$$(ab)^{sn} = a^{\frac{1-rm}{n}} b^{\frac{1}{n}} = a^{1-rm} = a, \quad (ab)^{rm} = a^{\frac{1}{rm}} b^{\frac{1-sn}{rm}} = b^{1-sn} = b.$$

ゆえに、

$$a^\ell = ((ab)^{sn})^\ell = \left(\underbrace{(ab)}_1^{\frac{\ell}{n}} \right)^{sn} = 1, \quad b^\ell = ((ab)^{rm})^\ell = \left(\underbrace{(ab)}_1^{\frac{\ell}{rm}} \right)^{rm} = 1.$$

したがって、 ℓ は m と n で割り切れる。

以上を合わせると、 $\ell = mn$ が得られる。 □

定理の主な応用

空気のごとく使われる!



① 位数 q の有限体 \mathbb{F}_q の乗法群 \mathbb{F}_q^\times は位数 $q-1$ の巡回群になる。

例 $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ と書くとき,

$$2 \neq 1, 2^2 = 4 \neq 1, 2^3 = 3 \neq 1, 2^4 = 1 \text{ より}, \mathbb{F}_5^\times = \langle 2 \rangle.$$

例 $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, \dots, 6\}$ と書くとき,

$$2 \neq 1, 2^2 = 4 \neq 1, 2^3 = 1 \text{ なので } \mathbb{F}_7^\times \not\simeq \langle 2 \rangle,$$

$$3 \neq 1, 3^2 = 2 \neq 1, 3^3 = 6 \neq 1, 3^4 = 4 \neq 1, 3^5 = 5 \neq 1, 3^6 = 1 \text{ より}, \mathbb{F}_7^\times = \langle 3 \rangle.$$

例 $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1) = \{0, 1, \omega, 1+\omega\}, \omega = \overline{x}$ と書くとき,

$$\omega \neq 1, \omega^2 = -\omega - 1 = 1 + \omega, \omega^3 = \omega + \omega^2 = \omega + 1 + \omega = 1 \text{ より}, \mathbb{F}_4^\times = \langle \omega \rangle.$$

② 任意の体 K と正の整数 n について, $\{x \in K \mid x^n = 1\}$ も巡回群になる。

位数 q の有限体を \mathbb{F}_q と表す。(\mathbb{F}_q を $GF(q)$ と書くこともある。)
 ↗ Galois field の略

問題 10-0 問題 5-1 ~ 5-3 および問題 9-1 について復習せよ。□

問題 5-1 K は標数 0 の体であるとし, L はその任意の拡大体であるとする。
 K 上の既約多項式が L の中に重根を持たないことを示せ。□

問題 5-2 正標数の体の標数が常に素数になることを示せ。□

問題 5-3 p は素数であるとし, $L = \mathbb{F}_p(t) = (1$ 变数 t の \mathbb{F}_p 上の有理函数体) とおく。
 L の部分体 K と K 上の既約多項式 $F(x) \in K[x]$ の組 $(K, F(x))$ で
 $F(x)$ が L の中に重根を持つものの 1 つを具体的に構成せよ。□

$L = \mathbb{F}_p(t)$, $K = \mathbb{F}_p(t^p)$, $F(x) = x^p - t^p \in K[x]$ が例になっている。
 (これは純非分離拡大の典型例になっている。)

問題 10-1 $p=17, 23, 41$ について $\mathbb{F}_p^\times = \langle a \rangle$ をみたす $a \in \mathbb{F}_p^\times$ を求めよ. \square

例 $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ と書くと,

2 ≠ 1, $2^2 = \underline{4} \neq 1$, $2^3 = \underline{1}$ なので $\langle 2 \rangle \subseteq \mathbb{F}_7^\times$. (次に 1, 2, 4 以外を調べる.)

3 ≠ 1, $3^2 = \underline{2} \neq 1$, $3^3 = \underline{6} \neq 1$, $3^4 = \underline{4} \neq 1$, $3^5 = \underline{5} \neq 1$, $3^6 = \underline{1}$ なので $\mathbb{F}_7^\times = \langle 3 \rangle$. \square

問題 10-2 K は正整数 p の体で $a, b \in K$ あるとし,

$x^p - a$ と $x^p - x - b$ は K 上既約であると仮定し,

L, M をそれぞれの K 上での最小分解体であるとする.

L と M が体 K 上で同型になることはあるか? \square

問題 10-3 有限体の有限次拡大が単拡大になることを示せ. \square

問題 10-4 k は正整数 p の体であるとし, $L = k(s, t)$, $K = k(s^p, t^p)$ とおく、

このとき, 拡大 L/K について, $[L:K] = p^2$ で L が K の単拡大にならないことを示せ.

ここで, $k(s, t)$ は体 K 上の 2 変数有理函数体である. (cf. 問題 5-3) \square

問題 10-1 $p=17, 23, 41$ について $\mathbb{F}_p^X = \langle a \rangle$ をみたす $a \in \mathbb{F}_p^X$ を求めよ。□

解答例 コンピュータを使つてもよいことにしていたので <https://www.wolframalpha.com/> を使つた、まずは答えから：

$$\mathbb{F}_{17}^X = \langle 3 \rangle, \quad \mathbb{F}_{23}^X = \langle 5 \rangle, \quad \mathbb{F}_{41}^X = \langle 6 \rangle.$$

2^k mod 17 for k=1 to 16

Input

Table[2^k mod 17, {k, 1, 16}]

Result

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$2^k \text{ mod } 17$	2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1

$$\mathbb{F}_{17}^X \supseteq \langle 2 \rangle = \{2, 4, 8, 16, 15, 13, 9, 1\}$$

↓ 上のリストに3がないので 3を確認。

3^k mod 17 for k=1 to 16

Input

Table[3^k mod 17, {k, 1, 16}]

Result

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3^k \text{ mod } 17$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

$$\mathbb{F}_{17}^X = \langle 3 \rangle$$

以下より, $\mathbb{F}_{23}^X = \langle 5 \rangle$

$2^k \bmod 23$ for $k=1$ to 22

Input

Table[$2^k \bmod 23, \{k, 1, 22\}$]

Result

{2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1}

$$2^{11} \bmod 23 = 1$$

↓ 5を確認

$5^k \bmod 23$ for $k=1$ to 22

Input

Table[$5^k \bmod 23, \{k, 1, 22\}$]

Result

{5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14, 1}

以下より, $\mathbb{F}_{41}^X = \langle 6 \rangle$

$2^k \bmod 41$ for $k=1$ to 40

Input

Table[$2^k \bmod 41, \{k, 1, 40\}$]

Result

{2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1, 2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1}

$$2^{20} \bmod 41 = 1$$

$3^k \bmod 41$ for $k=1$ to 40

Input

Table[$3^k \bmod 41, \{k, 1, 40\}$]

Result

{3, 9, 27, 40, 38, 32, 14, 1, 3, 9, 27, 40, 38, 32, 14, 1, 3, 9, 27, 40, 38, 32, 14, 1, 3, 9, 27, 40, 38, 32, 14, 1, 3, 9, 27, 40, 38, 32, 14, 1}

$$3^8 \bmod 41 = 1$$

$6^k \bmod 41$ for $k=1$ to 40

Input

Table[$6^k \bmod 41, \{k, 1, 40\}$]

Result

{6, 36, 11, 25, 27, 39, 29, 10, 19, 32, 28, 4, 24, 21, 3, 18, 26, 33, 34, 40, 35, 5, 30, 16, 14, 2, 12, 31, 22, 9, 13, 37, 17, 20, 38, 23, 15, 8, 7, 1}

おまけ $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1) = \{0, 1, \omega, 1+\omega\}$

$\omega^2 + \omega + 1 = 0$, このとき,

$\mathbb{F}_4^X = \langle \omega \rangle = \{\omega, 1+\omega, 1\}$

$\omega + \omega^2 = \omega + 1 + \omega = 1$ ↑

問題 10-2 K は正整数 p の体で $a, b \in K$ であるとし,

$x^p - a$ と $x^p - x - b$ は K 上既約であると仮定し,

L, M をそれぞれの K 上での最小分解体であるとする.

L と M が体 K 上で同型になることはあるか? \square

解答例

$f(x) = x^p - a, g(x) = x^p - x - b$ とおく. このとき,

$$f'(x) = \underbrace{px^{p-1}}_{=0 \text{ (正整数 } p)} = 0, \quad g'(x) = \underbrace{px^{p-1} - 1}_{\text{左と同様にして} = 0} = -1 \neq 0.$$

これより, $f(x)$ は重根を持ち, $g(x)$ は重根を持たない.

すなわち, $f(x)$ は非分離的であり, $g(x)$ は分離的である.

したがって, $f(x)$ の K 上での最小分解体は K 上の非分離拡大になり,

$g(x)$ の K 上での最小分解体は K 上の分離拡大になる.

ゆえに L と M が K 上で同型になることはない,

\square

一般に多項式 $h(x) \in K[x]$
が重根を持つことと,
 $h(x) \text{ と } h'(x)$ が共通根を持つことは同値である.

問題 10-3 有限体の有限次拡大が単拡大になることを示せ。□

解答例 有限体 K の n 次の有限次拡大 L は K 上のベクトル空間として K^n に同型なので有限集合になる。

ゆえに, L は有限体になる。

ポイント (前回, 非常に詳しく説明した。)

有限体の乗法群は巡回群になるので, ある $\alpha \in L$ が存在して $L^\times = \langle \alpha \rangle$ 。
これより, $L = K(\alpha)$ となることがわかる。

□

注意 一般に体の乗法群の有限部分群は巡回群になる。

この証明法はたくさんある:

- 有限(生成)Abel群の基本定理(大道具)を使う、使いやすい。
- 初等的な証明、色々あって面白いが少しテクニカルになる。

□

問題 10-4 k は正標数 p の体であるとし, $L = k(s, t)$, $K = k(s^p, t^p)$ とおく.

このとき, 拡大 L/K について, $[L:K] = p^2$ で " L が K の单拡大にならないことを示せ.

ここで, $k(s, t)$ は体 K 上の 2 变数有理函数体である. (cf. 問題 5-3) \square

正標数では有限次拡大が单拡大にならない場合がある.

解答例 ① $[L:K] = p^2$ を示す.

$M = k(s, t^p)$ とおく. $L = M(t)$, $M = K(s)$ である.

$f(x) \in M[x]$ を $f(x) = x^p - t^p$ とおく.

M を t^p を素元に持つ UFD $k(s)[t^p]$ の商体とみなして Eisenstein の判定法を使うと,
 $t^p+1, t^p|0, \dots, t^p|0, t^p|-t^p, (t^p)^2|-t^p$ より, $f(x)$ は M 上既約である.

$f(x)$ は t の M 上での最小多項式であるので, $[L:M] = [M(t):M] = \deg f = p$.

$g(x) \in K[x]$ を $g(x) = x^p - s^p$ とおく, $\text{注 } g(x) \in \overbrace{k(t^p)[s^p]}^{\text{UFD}}[x]$

K を s^p を素元に持つ UFD $k(t^p)[s^p]$ の商体とみなして Eisenstein の判定法を使うと,
 $s^p+1, s^p|0, \dots, s^p|0, s^p|-s^p, (s^p)^2|-s^p$ より, $g(x)$ は K 上既約である.

$g(x)$ は s の K 上での最小多項式であるので, $[M:K] = [K(s), K] = \deg g = p$.

したがって, $[L:K] = [L:M][M:K] = p^2$.

2 任意の $\alpha \in L$ について $\alpha^p \in K$ を示す. $\leftarrow (L^p \subset K)$

$$L = k(s, t) \text{ より}, \quad \alpha = \frac{\sum a_{ij} s^i t^j}{\sum b_{ij} s^i t^j}, \quad a_{ij}, b_{ij} \in k \text{ と書ける.}$$

$$\begin{aligned} \text{標数が } p \text{ なので } \alpha^p &= \frac{(\sum a_{ij} s^i t^j)^p}{(\sum b_{ij} s^i t^j)^p} = \frac{\sum a_{ij}^p (s^p)^i (t^p)^j}{\sum b_{ij}^p (s^p)^i (t^p)^j} \in k(s^p, t^p) = K, \\ ((\beta + \gamma)^p = \beta^p + \gamma^p) \uparrow \end{aligned}$$

3 任意の $\alpha \in L$ について, $[K(\alpha) : K] \leq p$ を示す.

上で $\alpha^p \in K$ となることを示したので α は $x^p - \underline{\alpha^p} \in K[x]$ の根になる
ゆえに, $[K(\alpha) : K] \leq \deg(x^p - \alpha^p) = p$.

4 任意の $\alpha \in L$ について, $L \not\supseteq K(\alpha)$ を示す.

$$[L : K] = p^2 \text{ で } [K(\alpha) : K] \leq p \text{ なので } L \not\supseteq K(\alpha),$$

これで L が K の單拡大にならないことが示された. \square

5次以下の方程式の Galois 群について

12-2

K は体であるとし, $f(x) \in K[x]$ は K 上の(既約な) n 次 分離多項式 であるとし, L は $f(x)$ の K 上での最小分解体であるとする.

L/K は K 上の有限次 Galois 扩大 になる.

問題 8-4 (1)

その Galois 群 $G = \text{Gal}(L/K)$ は $f(x)$ の根全体の集合 $\{\alpha_1, \dots, \alpha_n\}$ に 推移的に 作用する. (G は $\{\alpha_1, \dots, \alpha_n\}$ の置換群 S_n の 推移的部部分群 とみなされる.)

$n=2$, $n=2$ のとき, $G = \langle \sigma \rangle \cong S_2 \cong C_2$, (σ は 2 つの根の互換) \square

$n=p$ は素数 $K = \mathbb{Q}$ で $n=p$ が素数で $f(x)$ が 3 つ以上と $p-2$ 個の実根を持つならば $G \cong S_p$ となる. ← 問題 8-4 (2) \square

例 $K = \mathbb{Q}$, $f(x) = x^5 - 16x + 2$ のとき, $G \cong S_5$. ← 問題 8-4 (3) \square

$n=3$, S_3 の推移的部部分群は A_3 と S_3 の 2 つだけである. ← 問題 8-2

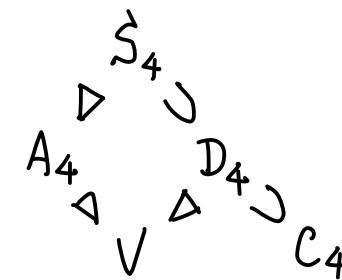
$G \cong A_3$, S_3 となる 3 次の既約多項式 $f(x) \in \mathbb{Q}[x]$ の例を作りたくる
 $\bowtie C_3 \bowtie D_3$ \square

$n=4$ 以下の 5つは S_4 の推移的部部分群である: ← 問題 8-3 (3)

$$\left\{ \begin{array}{l} \langle (1, 2, 3, 4) \rangle \cong C_4 \\ V = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \cong C_2 \times C_2 \\ \langle (1, 2, 3, 4), (1, 3) \rangle \cong D_4 \\ A_4 \\ S_4 \end{array} \right.$$

$\xrightarrow{\text{Kleinの四元群}}$

$\cancel{C_2 \times C_2}$



$G \cong C_4, V, D_4, A_4, S_4$ となる4次の既約多項式 $f(x) \in \mathbb{Q}[x]$ を作りたくなる. \square

例 $K = \mathbb{Q}$, $f(x) = x^3 - 3$ のとき, $L = \mathbb{Q}(\omega, \alpha)$ ($\omega = \frac{-1 + \sqrt{-3}}{2}$, $\alpha = \sqrt[3]{3}$), $G \cong S_3$ ← 問題 7-1 \square

例 $K = \mathbb{Q}$, $f(x) = x^4 - 4x^2 + 2$, $\alpha = \sqrt{2 + \sqrt{2}}$ のとき, $L = \mathbb{Q}(\alpha)$, $G \cong C_4$. ← 問題 7-2. \square

例 $K = \mathbb{Q}$, $f(x) = x^4 - 2$, $\omega = \sqrt{-1}$, $\alpha = \sqrt[4]{2}$ のとき, $L = \mathbb{Q}(\omega, \alpha)$, $G \cong D_4$. → 問題 12-1 \square

例 $K = \mathbb{Q}$, $f(x) = x^4 - 10x^2 + 1$ のとき, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $G \cong C_2 \times C_2$. → 問題 12-2 \square

例 $K = \mathbb{Q}$, $f(x) = x^3 - 21x + 28$ のとき, $G \cong C_3$. → 問題 12-3 \square

例 $K = \mathbb{Q}$, $f(x) = x^3 + 3x^2 - 3$ のとき, $G \cong C_3$. → 問題 12-4 \square

問題 12-1 $F(x) = x^4 - 2$, $\alpha = \sqrt[4]{2}$, $\bar{\alpha} = \sqrt{-1}$ とおく、以下を示せ、

- (1) $F(x)$ は α の \mathbb{Q} 上で"の最小多項式"である。
- (2) $F(x)$ の \mathbb{Q} 上で"の最小分解体"は $\mathbb{Q}(\alpha, \bar{\alpha})$ に等しい。 $K = \mathbb{Q}, n = 4$ で
 $G \cong D_4$ となる例
- (3) $[\mathbb{Q}(\alpha, \bar{\alpha}) : \mathbb{Q}] = 8$.

(4) $\mathbb{Q}(\alpha, \bar{\alpha})$ の体の自己同型 σ, τ を次のように定義できる:

$$\sigma(f(\alpha)) = f(i\alpha) \quad (f(x) \in \mathbb{Q}(i)[x]), \quad \tau(g(\bar{\alpha})) = g(-\bar{\alpha}) \quad (g(x) \in \mathbb{Q}(\bar{\alpha})[x]).$$

(5) $\text{Gal}(\mathbb{Q}(\alpha, \bar{\alpha})/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong D_4$.

□

問題 12-2 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ とおく、以下を示せ、

(1) $F(x) = x^4 - 10x^2 + 1$ は $\alpha = \sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上で"の最小多項式"である。

(2) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $F(x)$ の \mathbb{Q} 上で"の最小分解体"である。 $K = \mathbb{Q}, n = 4$ で
 $G \cong C_2 \times C_2$ となる例

(3) L/\mathbb{Q} は 4 次の Galois 拡大である。

(4) L の \mathbb{Q} 上で"の自己同型" σ, τ を次のように定めることとする:

$$\sigma(f(\sqrt{2})) = f(-\sqrt{2}) \quad (f(x) \in \mathbb{Q}(\sqrt{3})[x]), \quad \tau(g(\sqrt{3})) = g(-\sqrt{3}) \quad (g(x) \in \mathbb{Q}(\sqrt{2})[x]).$$

(5) $\text{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong C_2 \times C_2$ (C_n は位数 n の巡回群)。 ↑ $F(x)$ の根全体の集合の置換群の中の Klein の四元群に一致。 □

問題12-3

$$F(x) = x^3 - 21x + 28 \text{ とおく。以下を示せ。}$$

$$k = \mathbb{Q}, n = 3$$

(1) $F(x)$ は \mathbb{Q} 上既約である。

(2) $F(x)$ の 3つの根を α, β, γ と書き、 $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$ とおくと、
 $D = 126^2$ となる。

位数3の巡回群

(3) $F(x)$ の \mathbb{Q} 上での最小分解体を L と書くと、 $\text{Gal}(L/\mathbb{Q}) \cong C_3$ 。
□

注意

一般に $x^3 + ax + b = (x - \alpha)(x - \beta)(x - \gamma)$ のとき、

$(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -4a^3 - 27b^2$ となることを要領よく示してみよ。
□

問題12-4

$$F(x) = x^3 + 3x^2 - 3 \text{ とおく。以下を示せ。}$$

(1) $F(x)$ は \mathbb{Q} 上既約である。

(2) $F(x)$ の 3つの根を α, β, γ と書くとき、 $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$ とおくと、
 $D = 9^2$ となる。

(3) $F(x)$ の \mathbb{Q} 上での最小分解体を L と書くと、 $\text{Gal}(L/\mathbb{Q}) \cong C_3$ 。

注意

一般に $x^3 + ax^2 + b = (x - \alpha)(x - \beta)(x - \gamma)$ のとき、

$(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -b(4a^3 + 27b)$ となることも示せ。
□

問題 12-1 $F(x) = x^4 - 2$, $\alpha = \sqrt[4]{2}$, $\bar{\alpha} = \sqrt{-1}$ とおく。以下を示せ。

- (1) $F(x)$ は α の \mathbb{Q} 上での最小多項式である。
- (2) $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha, \bar{\alpha})$ に等しい。
 $K = \mathbb{Q}, n = 4$ で
 $G \cong D_4$ になる例
- (3) $[\mathbb{Q}(\alpha, \bar{\alpha}) : \mathbb{Q}] = 8$.
- (4) $\mathbb{Q}(\alpha, \bar{\alpha})$ の体の自己同型 σ, τ を次のように定義できる:
 $\sigma(f(\alpha)) = f(i\alpha)$ ($f(x) \in \mathbb{Q}(i)[x]$), $\tau(g(\bar{\alpha})) = g(-\bar{\alpha})$ ($g(x) \in \mathbb{Q}(\alpha)[x]$).
- (5) $\text{Gal}(\mathbb{Q}(\alpha, \bar{\alpha}) / \mathbb{Q}) = \langle \sigma, \tau \rangle \cong D_4$. □

解答例

(1) $2+1, 210, 210, 210, 21-2, 2^2+2$ などの Eisenstein の判定法より,
 $F(x) = x^4 - 2$ は \mathbb{Q} 上の既約多項式である。 $F(\alpha) = F(\sqrt[4]{2}) = (\sqrt[4]{2})^4 - 2 = 0$ 。
ゆえに, $F(x)$ は α の \mathbb{Q} 上での最小多項式である。

(2) $F(x) = x^4 - 2$ の 4 つの根は $\alpha, i\alpha, -\alpha, -i\alpha$ なので $F(x)$ の \mathbb{Q} 上での最小分解体を L と書くと, $L = \mathbb{Q}(\alpha, i\alpha, -\alpha, -i\alpha)$ 。 $i = \frac{i\alpha}{\alpha}$ なので $i \in L$ 。このことから $L = \mathbb{Q}(i, \alpha)$ であることがわかる。

(3) $L = \mathbb{Q}(\bar{i}, \alpha)$, $M = \mathbb{Q}(\alpha)$ とおく, $L = M(\bar{i})$ である. $G(x) = x^2 + 1$ とおく.

[$[M : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg F(x) = 4$.

[もしも $G(x)$ が M 上既約でないならその根 $\pm i$ は M の元になるが,

$M = \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ なのでそうならない, ゆえに $G(x)$ は M 上既約である.

$G(\bar{i}) = \bar{i}^2 + 1 = 0$ なので, $G(x)$ は $\bar{i} = \sqrt{-1}$ の M 上の最小多项式になる.
これより, $[L : M] = [M(\bar{i}) : M] = \deg G(x) = 2$.

以上より, $[\mathbb{Q}(\bar{i}, \alpha) : \mathbb{Q}] = [L : M][M : \mathbb{Q}] = 2 \times 4 = 8$.

$$(4) \quad [\mathbb{Q}(\bar{i}, \alpha) : \mathbb{Q}(\bar{i})] = \frac{[\mathbb{Q}(\bar{i}, \alpha) : \mathbb{Q}]}{[\mathbb{Q}(\bar{i}) : \mathbb{Q}]} = \frac{8}{2} = 4 = \deg F(x), \quad F(\alpha) = 0 \text{ より},$$

$F(x) = x^4 - 2$ は $\alpha = \sqrt[4]{2}$ の $\mathbb{Q}(\bar{i})$ 上での最小多項式である。

上で $G(x) = x^2 + 1$ が $i = \sqrt{-1}$ の $\mathbb{Q}(\alpha)$ 上での最小多項式であることは示してある。

$F(x), G(x)$ はそれぞれ $\mathbb{Q}(\bar{i}), \mathbb{Q}(\alpha)$ 上のそれぞれの根の最小多項式にもなっている。

したがって、以下のようにして、体 $\mathbb{Q}(\bar{i}, \alpha)$ の自己同型 σ を定めることができる：

$$\mathbb{Q}(\bar{i}, \alpha) = \mathbb{Q}(\bar{i})(\alpha) \cong \mathbb{Q}(\bar{i})[x]/(F(x)) \cong \mathbb{Q}(\bar{i})(i\alpha) = \mathbb{Q}(\bar{i}, i\alpha) = \mathbb{Q}(\bar{i}, \alpha)$$

$$f(\alpha) \longleftrightarrow \overline{f(x)} \longleftrightarrow f(\bar{i}\alpha)$$

σ

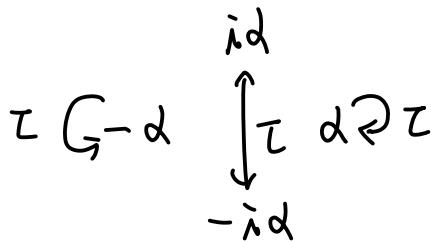
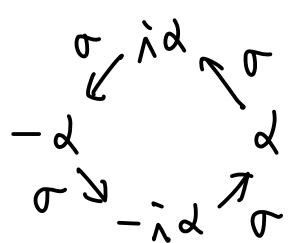
$$\mathbb{Q}(\bar{i}, \alpha) = \mathbb{Q}(\alpha)(\bar{i}) \cong \mathbb{Q}(\alpha)[x]/(G(x)) \cong \mathbb{Q}(\alpha)(-\bar{i}) = \mathbb{Q}(-\bar{i}, \alpha) = \mathbb{Q}(\bar{i}, \alpha)$$

$$g(\bar{i}) \longleftrightarrow \overline{g(x)} \longleftrightarrow g(-\bar{i})$$

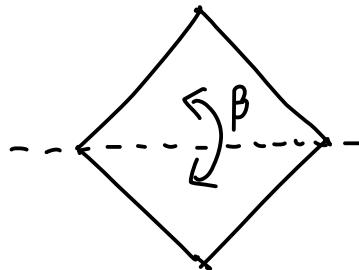
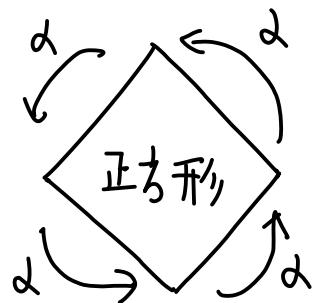
τ

$$(5) |Gal(\mathbb{Q}(\sqrt{-d})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{-d}) : \mathbb{Q}] = 8.$$

σ と τ は $F(x) = x^4 - 2$ の 4 つの根に次のように作用している:



4 次の二面体群 D_4 は正方形を 90° 回転させる操作 α と次の図の線対称変換 β から生成される位数 8 の群であった:



以上を比較すると, $Gal(\mathbb{Q}(\sqrt{-d})/\mathbb{Q}) \cong D_4$ であることがわかる.

$$\begin{array}{ccc} \sigma & \longleftrightarrow & \alpha \\ \tau & \longleftrightarrow & \beta \end{array}$$

問題 12-2. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ とおく、以下を示せ。

(1) $F(x) = x^4 - 10x^2 + 1$ は $\alpha = \sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上での最小多項式である。

(2) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $F(x)$ の \mathbb{Q} 上での最小分解体である。 $(K = \mathbb{Q}, n = 4)$

(3) L/\mathbb{Q} は 4 次の Galois 拡大である。 $(G \cong C_2 \times C_2 \text{ となる例})$

(4) L の \mathbb{Q} 上での自己同型 σ, τ を次のように定めることとする：

$$\sigma(f(\sqrt{2})) = f(-\sqrt{2}) \quad (f(x) \in \mathbb{Q}(\sqrt{3})[x]), \quad \tau(g(\sqrt{3})) = g(-\sqrt{3}) \quad (g(x) \in \mathbb{Q}(\sqrt{2})[x]).$$

(5) $\text{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong C_2 \times C_2$ (C_n は位数 n の巡回群)。 \square

↑ $F(x)$ の根全体の集合の置換群の中の Klein の四元群に一致。

解答例 ((1) ~ (4) は 問題 4-1 の解答例ですでに示してあるとみなされる。)

(1), (2), (3) をまとめて示す。

$$\begin{aligned} & (\chi - (\sqrt{2} + \sqrt{3}))(\chi - (-\sqrt{2} + \sqrt{3}))(\chi - (\sqrt{2} - \sqrt{3}))(\chi - (-\sqrt{2} - \sqrt{3})) \\ &= ((\chi - \sqrt{3})^2 - (\sqrt{2})^2)((\chi + \sqrt{3})^2 - (\sqrt{2})^2) = (x^2 + 1 - 2\sqrt{3}x)(x^2 + 1 + 2\sqrt{3}x) \\ &= (x^2 + 1)^2 - (2\sqrt{3}x)^2 = x^4 + 2x^2 + 1 - 12x^2 = x^4 - 10x^2 + 1 = F(x). \end{aligned}$$

$F(x)$ の \mathbb{Q} 上での最小分解体を L' と書こう.

$F(x)$ の 4 つの根 $\sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} - \sqrt{3}$ が $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ に含まれることより, $L' \subset L$.

$$\sqrt{2} = \frac{(\sqrt{2} + \sqrt{3}) + (\sqrt{2} - \sqrt{3})}{2}, \quad \sqrt{3} = \frac{(\sqrt{2} + \sqrt{3}) + (-\sqrt{2} + \sqrt{3})}{2} \text{ が } L' \text{ に含まれることより, } L \subset L'.$$

ゆえに, $L' = L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, これで (2) が示された,

$\sqrt{2} \notin \mathbb{Q}$ より $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ であることがわたり,

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ より, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ であることがわかる.

ゆえに, $[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$.

L は $F(x)$ の \mathbb{Q} 上での最小分解体ので Galois 扩大でもある. これで (3) が示された,

$$\frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2}, \quad \frac{(\sqrt{2} + \sqrt{3}) - (\sqrt{3} - \sqrt{2})}{2} = \sqrt{2}, \quad (\sqrt{3} - \sqrt{2}) + \sqrt{2} = \sqrt{3} \text{ が } \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

に含まれることから, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = L$ となることもわかる.

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [L : \mathbb{Q}] = 4 = \deg F(x)$ より, $F(x)$ は $\alpha = \sqrt{2} + \sqrt{3}$ の \mathbb{Q} 上での
最小多項式であることがわかる. これで (1) が示された.

(4) $G(x) = x^2 - 2$, $H(x) = x^2 - 3$ はそれぞれ $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$ 上のそれらの根の最小多項式とみなされるので、以下のようにして、 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ の自己同型 σ , τ を定めることができる：

$$L = \mathbb{Q}(\sqrt{3})(\sqrt{2}) \cong \mathbb{Q}(\sqrt{3})[x]/(G(x)) \cong \mathbb{Q}(\sqrt{3})(-\sqrt{2}) = L$$

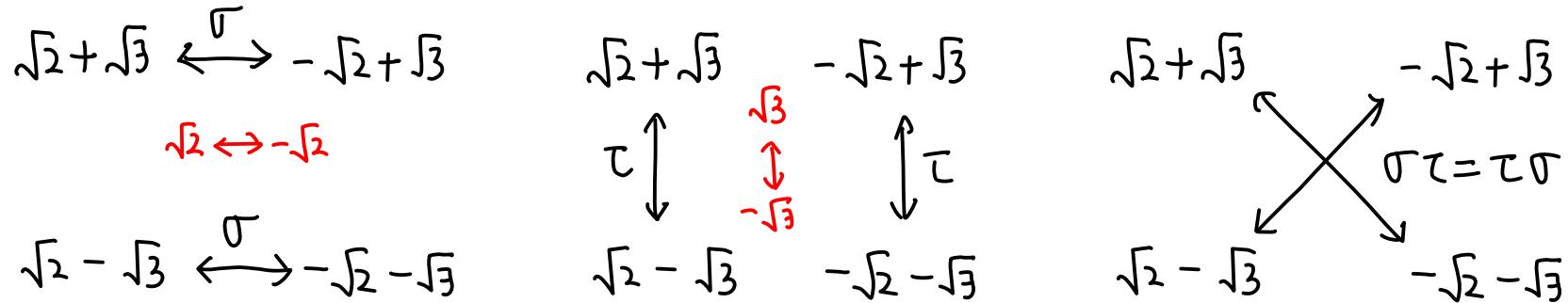
$$\begin{array}{ccc} f(\sqrt{2}) & \longleftrightarrow & \overline{f(x)} & \longleftrightarrow & f(-\sqrt{2}) \\ & \swarrow \sigma & & & \searrow \end{array}$$

$$L = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \cong \mathbb{Q}(\sqrt{2})[x]/(H(x)) \cong \mathbb{Q}(\sqrt{2})(-\sqrt{3}) = L$$

$$\begin{array}{ccc} g(\sqrt{3}) & \longleftrightarrow & \overline{g(x)} & \longleftrightarrow & g(-\sqrt{3}) \\ & \swarrow \tau & & & \searrow \end{array}$$

$$(5) |Gal(L/\mathbb{Q})| = [L:\mathbb{Q}] = 4.$$

$\sigma, \tau, \sigma\tau$ では $F(x) = x^4 - 10x^2 + 1$ の 4 つの根の集合に次のように作用している:



これより, $F(x)$ の 4 つの根を $\alpha_1 = \sqrt{2} + \sqrt{3}$, $\alpha_2 = -\sqrt{2} + \sqrt{3}$, $\alpha_3 = \sqrt{2} - \sqrt{3}$, $\alpha_4 = -\sqrt{2} - \sqrt{3}$ と書くとき, $\sigma, \tau, \sigma\tau$ はそれぞれ置換 $(1, 2)(3, 4)$, $(1, 3)(2, 4)$, $(1, 4)(2, 3)$ に対応していることがわかる,

したがって,

↙ Klein の四元群

$$Gal(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \cong \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \cong C_2 \times C_2, \quad \square$$

問題12-3

$$F(x) = x^3 - 21x + 28 \text{ とおく。以下を示せ。}$$

$$K = \mathbb{Q}, n = 3$$

(1) $F(x)$ は \mathbb{Q} 上既約である。

(2) $F(x)$ の 3つの根を α, β, γ と書き、 $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$ とおくと、
 $D = 126^2$ となる。

(3) $F(x)$ の \mathbb{Q} 上での最小分解体を L と書くと、 $\text{Gal}(L/\mathbb{Q}) \cong C_3$, \square

位数3の巡回群

$\cong A_3 \leftarrow 3\text{次の交代群}$

解答例

$$F(x) = x^3 + ax + b = (x - \alpha)(x - \beta)(x - \gamma) \text{ のとき,}$$

$$D := (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -4a^3 - 27b^2 \text{ となることを示そう。}$$

$$\alpha + \beta + \gamma = 0, \quad \alpha\beta + \alpha\gamma + \beta\gamma = a, \quad \alpha\beta\gamma = -b \text{ とおこう,}$$

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma) = -2a,$$

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 = (\alpha\beta + \alpha\gamma + \beta\gamma)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma) = a^2.$$

$$F'(\alpha) = 3\alpha^2 + a = (\alpha - \beta)(\alpha - \gamma), \quad F'(\beta) = 3\beta^2 + a = (\beta - \alpha)(\beta - \gamma), \quad F'(\gamma) = 3\gamma^2 + a = (\gamma - \alpha)(\gamma - \beta) \text{ とし,}$$

$$(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -F'(\alpha)F'(\beta)F'(\gamma)$$

$$\begin{aligned} &= -\underbrace{(a^3 + 3(\alpha^2 + \beta^2 + \gamma^2)a^2)}_{= -2a} + 9\underbrace{(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2)a}_{= a^2} + 27\underbrace{\alpha^2\beta^2\gamma^2}_{= b^2} \\ &= -(a^3 - 6a^3 + 9a^3 + 27b^2) = -4a^3 - 27b^2. \end{aligned}$$

(1) $F(x) = x^3 - 21x + 28$ は $7 \nmid 1, 7 \nmid 0, 7 \nmid -21, 7 \nmid 28, 7^2 \nmid 28$ と Eisenstein の判定法より, \mathbb{Q} 上既約である.

(2) 前ページの公式を $a = -21, b = 28$ の場合に用いると,

$$\begin{aligned} D &= (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -4a^3 - 27b^2 \\ &= 4 \cdot 21^3 - 27 \cdot 28^2 = 2^2 \cdot 3^3 \cdot 7^3 - 2^4 \cdot 3^3 \cdot 7^2 \\ &= 2^2 \cdot 3^3 \cdot 7^2 (7 - 2^2) = 2^2 \cdot 3^4 \cdot 7^2 = (2 \cdot 3^2 \cdot 7)^2 = 126^2. \end{aligned}$$

(3) $F(x)$ の \mathbb{Q} 上での最小分解体を L と書き, $G = \text{Gal}(L/\mathbb{Q})$ とおく.

$F(x)$ が \mathbb{Q} 上既約なので, G の $\{\alpha, \beta, \gamma\}$ への作用は推移的になるので $G \cong A_3$ または $G \cong S_3$ となる.

$$\Delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) \text{ とおくと, } \Delta^2 = D = 126^2 \text{ より } \Delta = \pm 126 \in \mathbb{Q} \text{ となる.}$$

ゆえに, 任意の $\sigma \in G$ について, $\sigma(\Delta) = \Delta$ となり, σ は $\{\alpha, \beta, \gamma\}$ の偶置換となる. これより, $G \cong A_3 \cong C_3$. □

問題 12-4

$$F(x) = x^3 + 3x^2 - 3 \text{ とおく, 以下を示せ.}$$

(1) $F(x)$ は \mathbb{Q} 上既約である.

(2) $F(x)$ の 3 つの根を α, β, γ と書くとき, $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$ とおくと,
 $D = q^2$ となる.

(3) $F(x)$ の \mathbb{Q} 上での最小分解体を L と書くと, $\text{Gal}(L/\mathbb{Q}) \cong C_3$.

解答例

$$F(x) = x^3 + ax^2 + b = (x - \alpha)(x - \beta)(x - \gamma) \text{ のとき,}$$

$$(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -b(4a^3 + 27b) \text{ となることを示す.}$$

$$\alpha + \beta + \gamma = -a, \quad \alpha\beta + \alpha\gamma + \beta\gamma = 0, \quad \alpha\beta\gamma = -b.$$

$$F'(\alpha) = 3\alpha^2 + 2a\alpha = (\alpha - \beta)(\alpha - \gamma), \quad F'(\beta) = 3\beta^2 + 2a\beta = (\beta - \alpha)(\beta - \gamma), \quad F'(\gamma) = 3\gamma^2 + 2a\gamma = (\gamma - \alpha)(\gamma - \beta),$$

$$(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -F'(\alpha)F'(\beta)F'(\gamma) = -\alpha\beta\gamma(3\alpha + 2a)(3\beta + 2a)(3\gamma + 2a)$$

$$= -\underbrace{\alpha\beta\gamma}_{=b} \underbrace{(8a^3 + 12(\alpha + \beta + \gamma)a^2)}_{-a} + \underbrace{18(\alpha\beta + \alpha\gamma + \beta\gamma)a}_{=0} + 27\alpha\beta\gamma$$

$$= b(8a^3 - 12a^3 - 27b) = -b(4a^3 + 27b).$$

(1) $F(x) = x^3 + 3x^2 - 3$ は, $3+1, 3|3, 3|0, 3|-3, 3^2+3$ と Eisenstein の判定法より,
 \mathbb{Q} 上既約である.

(2) 前ページの公式を $a=3, b=-3$ に用いると,

$$D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -b(4a^3 + 27b) = 3(4 \cdot 3^3 - 27 \cdot 3) = 3^4 = q^2$$

3^3
||

(3) $F(x)$ の \mathbb{Q} 上での最小分解体を L と書き, $G = \text{Gal}(L/\mathbb{Q})$ とおく.
 $F(x)$ は \mathbb{Q} 上既約なので, G の $\{\alpha, \beta, \gamma\}$ への作用は推移的になるので,
 $G \cong A_3$ または $G \cong S_3$ となる.

$\Delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$ とおくと, $\Delta^2 = D = q^2$ より, $\Delta = \pm q \in \mathbb{Q}$ となる
 ときに, 任意の $\sigma \in G$ について, $\sigma(\Delta) = \Delta$ となり, σ は $\{\alpha, \beta, \gamma\}$ の偶置換になる.
 したがって, $G \cong A_3 \cong C_3$. □

注意 $F(x-1) = (x-1)^3 + 3(x-1)^2 - 3 = x^3 - 3x^2 + 3x - 1 + 3x^2 - 6x + 3 - 3 = x^3 - 3x - 1$.

$x^3 - 3x - 1$ も \mathbb{Q} 上既約になり, その \mathbb{Q} 上での最小分解体は上と同じ L になり,
 $\text{Gal}(L/\mathbb{Q}) \cong A_3 \cong C_3$ となる. □

1の原始n乗根 $\zeta_n = e^{2\pi i/n}$ の \mathbb{Q} 上でのモニックな最小多項式を $\Phi_n(x) \in \mathbb{Q}[x]$ と書き、(等周)円分多項式と呼ぶ。次が成立している:

$$\Phi_n(x) = \prod_{\omega \text{ は } 1 \text{ の原始 } n \text{ 乗根}} (x - \omega).$$

$\Phi_n(x) \in \mathbb{Z}[x]$ となることも知られている。

問題 13-1 $\Phi_n(x)$ を $n=1, 2, \dots, 12$ について求めよ. \square

問題 13-2 以下を示せ.

(1) 素数 p と正の整数 e について, $\Phi_{pe}(x) = \Phi_p(x^{pe^{-1}})$.

(2) 正の奇数 n について, $\Phi_{2n}(x) = (-1)^{\varphi(n)} \Phi_n(-x)$. ($\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$)

(3) $\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{i}, \sqrt{2}, \sqrt{3})$. \square

問題 13-3 $\Phi_n(x)$ の係数は常に 0, ± 1 だけになるか? \square

問題 13-4 $n \in \mathbb{Z}_{>0}$, $\zeta_n = e^{2\pi i/n}$ のとき, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ となることを示せ. \square

問題13-1

 $\Phi_n(x)$ を $n=1, 2, \dots, 12$ について求めよ. \square

14-1

解答例

$$\Phi_n(x) = \prod_{\substack{w^n=1 \\ w \neq 1}} (x-w) \text{ とおこう},$$

wは1の複数のn乗根

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{w^n=1 \text{ and} \\ \exists d \text{ s.t. } d < n \text{ and } w^d=1}} (x-w)} = \frac{x^n - 1}{\prod_{d|n \text{ and } d < n} \Phi_d(x)}$$

を使う.

$$\Phi_1(x) = x-1, \quad \Phi_2(x) = \frac{x^2-1}{x-1} = x+1, \quad \Phi_3(x) = \frac{x^3-1}{x-1} = x^2+x+1, \quad \Phi_4(x) = \frac{x^4-1}{(x-1)(x+1)} = x^2+1,$$

$$\Phi_5(x) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1, \quad \Phi_6(x) = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = \frac{x^3+1}{x+1} = x^2-x+1$$

$$\Phi_7(x) = \frac{x^7-1}{x-1} = x^6+x^5+\cdots+x+1, \quad \Phi_8(x) = \frac{x^8-1}{(x-1)(x+1)(x^2+1)} = x^4+1,$$

$$\Phi_9(x) = \frac{x^9-1}{(x-1)(x^2+x+1)} = x^6+x^3+1, \quad \Phi_{10}(x) = \frac{x^{10}-1}{(x-1)(x+1)\Phi_5(x)} = x^4-x^3+x^2-x+1,$$

$$\Phi_{11}(x) = \frac{x^{11}-1}{x-1} = x^{10}+x^9+\cdots+x+1,$$

$$\Phi_{12}(x) = \frac{x^{12}-1}{(x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)} = \frac{x^6+1}{x^2+1} = x^4-x^2+1.$$

 \square

問題13-2 以下を示せ.

- (1) 素数 p と正の整数 e について, $\Phi_{pe}(x) = \Phi_p(x^{pe^{-1}})$.
- (2) 正の奇数 n について, $\Phi_{2n}(x) = (-1)^{\varphi(n)} \Phi_n(-x)$. ($\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$)
- (3) $\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{i}, \sqrt{2}, \sqrt{3})$. □

解答例

(1) 1の原始 p^e 乗根の1つを w と書くと, $\underbrace{p^e - p^{e-1}}$ 個の 1の原始 p^e 乗根全体は
 w^{k+p^el} $k \in \{1, 2, \dots, p-1\}$, $l \in \{0, 1, \dots, p^{e-1}-1\}$)
 と書ける. この p^{e-1} 乗は $\underbrace{p-1\text{個}}$ $\underbrace{p^{e-1}\text{個}}$
 $(w^{p^{e-1}})^k$ ($k \in \{1, 2, \dots, p-1\}$)

はちょうど 1の原始 p 乗根全体に一致し,

$$w^{pl} = (w^p)^l \quad (l \in \{0, 1, \dots, p^{e-1}-1\})$$

はちょうど 1の p^{e-1} 乗根全体に一致するので

$$\Phi_{pe}(x) = \prod_{k=1}^{p-1} \prod_{l=0}^{p^{e-1}-1} (x - w^{k+pl}) = \prod_{k=1}^{p-1} (x^{p^{e-1}} - (w^{p^{e-1}})^k) = \Phi_p(x^{pe^{-1}}), \quad \square$$

(2) n は正の奇数であるとする. このとき, 次が成立していることを示す:

w が 1 の原始 $2n$ 乗根 $\Leftrightarrow -w$ は 1 の原始 n 乗根

(\Rightarrow) w は 1 の原始 $2n$ 乗根であるとする.

$1 = w^{2n} = (w^n)^2$ より $w^n = \pm 1$ だが, w は 1 の原始 $2n$ 乗根なので $w^n = 1$.

n は奇数なので $(-w)^n = 1$,

$d|n, d < n$ のとき, $w^{2d} \neq 1$ なので $(-w)^d \neq 1$.

ゆえに, $-w$ は 1 の原始 n 乗根である.

(\Leftarrow) $-w$ は 1 の原始 n 乗根であるとする.

このとき, $w^{2n} = ((-w)^n)^2 = 1^2 = 1$.

$2n$ の $2n$ より小さな正の約数は $2d$ または d ($d|n, d < n$) と書ける.

もしも $w^d = 1$ ならば $(-w)^n = -(w^d)^{\frac{n}{d}} = -1$ となって $(-w)^n = 1$ に反する.

もしも $w^d \neq 1$ かつ $w^{2d} = 1$ ならば $w^d = -1$ となり, $(-w)^d = 1$ となる.

$-w$ が 1 の原始 n 乗根であることに反する.

これで, w が 1 の原始 $2n$ 乗根であることが示された.

(2) つづき、前へ⁰-シの結果より、 $w = w'$

$$\Phi_{2n}(x) = \prod_{w \text{ は } 1 \text{ の原始 } 2n \text{ 乗根}} (x - w) \stackrel{\downarrow}{=} \prod_{w' \text{ は } 1 \text{ の原始 } n \text{ 乗根}} (x + w')$$

$$= (-1)^{\varphi(n)} \prod_{w' \text{ は } 1 \text{ の原始 } n \text{ 乗根}} (-x - w') = (-1)^{\varphi(n)} \Phi_n(-x),$$

ここで、 $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = (1 \text{ の原始 } n \text{ 乗根の個数})$ であることを使、左、□

$$(3) \Phi_{24}(x) = \frac{x^{24}-1}{(x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4+1)(x^4-x^2+1)} = \frac{x^{24}-1}{(x^{12}-1)(x^4+1)}$$

$$= \frac{x^{12}+1}{x^4+1} = x^8 - x^4 + 1$$

$$\Phi_{24}(x) = 0 \Leftrightarrow x^4 \text{ について解 } < 0, \quad x^4 = \frac{1 \pm \sqrt{-3}}{2} = \frac{2 \pm 2\sqrt{-3}}{4} = \frac{(\pm \sqrt{3})^2}{4}.$$

$$\text{ゆえに, } x^2 = \pm \frac{\pm \sqrt{3}}{2} = \pm \frac{2\pm 2\sqrt{3}}{4} = \pm \frac{(\sqrt{-1} \pm \sqrt{3}\sqrt{-1})^2}{4}$$

$$\therefore \sqrt{-1} = \frac{1-\sqrt{-3}}{\sqrt{2}}, \quad \sqrt{3}\sqrt{-1} = \sqrt{3} \frac{1+\sqrt{-3}}{\sqrt{2}} \text{ とおいた. (このとき } \sqrt{-1}\sqrt{3}\sqrt{-1} = \sqrt{3})$$

$$\text{ゆえに, } x = \pm \frac{\sqrt{-1} \pm \sqrt{3}\sqrt{-1}}{2}, \quad \pm \frac{\sqrt{-1} \pm \sqrt{3}\sqrt{-1}}{2},$$

これより, $\mathbb{Q}(\zeta_{24}) = (\Phi_{24}(x) \text{ の } \mathbb{Q} \text{ 上での最小分解体}) \subset \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}).$

$$\text{逆に, } \zeta_{24}^6 = (e^{2\pi i/24})^6 = e^{\pi i/2} = \sqrt{-1},$$

$$\zeta_{24}^3 = e^{\pi i/4} = \frac{1+\sqrt{-3}}{\sqrt{2}}, \quad \zeta_{24}^4 = e^{\pi i/3} = \frac{1+\sqrt{3}\sqrt{-1}}{2} \text{ より, } \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\zeta_{24}).$$

これで, $\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3})$ が示された. □

問題 13-3 $\Phi_n(x)$ の係数は常に 0, ± 1 だけになるか? \square

解答例 $n \leq 104$ のとき, $\Phi_n(x)$ の係数は 0, ± 1 だけになる。

しかし, $\Phi_{105}(x)$ の係数には -2 が現れる。 \square

<https://www.wolframalpha.com/input/?i=Cyclotomic%5B105%2C+x%5D&lang=ja>



Cyclotomic[105, x]

Input

$C_{105}(x)$

Result

$$\begin{aligned} &x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - \\ &x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1 \end{aligned}$$

問題 13-4 $n \in \mathbb{Z}_{>0}$, $\zeta_n = e^{2\pi i/n}$ のとき, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ となることを示せ. \square

解説 $\mathbb{Q}(\zeta_n) = (\Phi_n(x)$ の \mathbb{Q} 上での最小分解体) なので ζ_n の共役元の全体は 1 の原始 n 乗根全体に一致する. そして,

$$\{1 \text{ の原始 } n \text{ 乗根全体}\} = \{\zeta_n^k \mid \bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times\}.$$

さらに, $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ は $\sigma(\zeta_n) = \zeta_n^k$ ($\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$) と一一対応している.

ゆえに, $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ に対して, $\sigma(\zeta_n) = \zeta_n^k$ という条件で定まる $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ を対応させる写像 ρ が群の準同型であることを示せばよい.

$\sigma, \tau \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ が $\sigma(\zeta_n) = \zeta_n^k$, $\tau(\zeta_n) = \zeta_n^l$ を満たすとき,

$$(\sigma\tau)(\zeta_n) = \sigma(\zeta_n^l) = \sigma(\zeta_n)^l = (\zeta_n^k)^l = \zeta_n^{kl}.$$

ゆえに, $\rho(\sigma\tau) = \bar{kl} = \bar{k}\bar{l} = \rho(\sigma)\rho(\tau)$.

これで示すべきことが示された. \square