資料04-2

以上で出て来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 $\sigma : \mathbb{Q}(\sqrt{2}) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2})$ で $\sigma(\sqrt{2}) = -\sqrt{2}$ をみ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 $x = 1 \pm \sqrt{2}$.

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

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含む.

□

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

- $\omega^k\sqrt[3]{7}$ の $\mathbb{Q}$ 上での最小多項式は x^3-7 : $\mathbb{Q}(\omega^k\sqrt[3]{7}) \cong \mathbb{Q}[x]/(x^3-7)$, $f(\omega^k\sqrt[3]{7}) \leftrightarrow \overline{f(x)}$
- $\omega,\ \omega^2 \notin \mathbb{Q}(\omega^k\sqrt[3]{7})$ $(\because\ \mathbb{Q}(\omega^k\sqrt[3]{7}) \cong \mathbb{Q}[x]/(x^3-7) \cong \mathbb{Q}(\sqrt[3]{7}) \ni \omega,\ \omega^2)$
- $\mathbb{Q}(\omega^k\sqrt[3]{7})$ 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 $\mathbb{Q}(\sqrt[3]{7},\ \omega^2\sqrt[3]{7}) \ni \dfrac{\omega^2\sqrt[3]{7}}{\sqrt[3]{7}} = \omega^2$ でかつ $\mathbb{Q}(\sqrt[3]{7},\ \omega^2\sqrt[3]{7}) \ni (\omega^2)^2 = \omega$

  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 $\omega\sqrt[3]{7}$ 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.

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

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

- $w=e^{2\pi i/3}=\dfrac{-1+\sqrt{3}i}{2}$ の $\mathbb{Q}(w^k\sqrt[3]{7})$ 上での最小多項式は x^2+x+1.
- $\mathbb{Q}(w^k\sqrt[3]{7}, w)\cong \mathbb{Q}(w^k\sqrt[3]{7})1\oplus \mathbb{Q}(w^k\sqrt[3]{7})w$, $[\mathbb{Q}(w^k\sqrt[3]{7}, w):\mathbb{Q}(w^k\sqrt[3]{7})]=2$.
- $\mathbb{Q}(\sqrt[3]{7}, w)=\mathbb{Q}(w\sqrt[3]{7}, w)=\mathbb{Q}(w^2\sqrt[3]{7}, w)=\mathbb{Q}(\sqrt[3]{7}, w\sqrt[3]{7}, w^2\sqrt[3]{7})$ ← (x^3-7の解をすべて含む)
- $\overline{w}=w^2$ なので，複素共役をとる操作は体 $\mathbb{Q}(\sqrt[3]{7}, w)$ の自己同型を定める.

↖新主張

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

- $[\mathbb{Q}(\sqrt[3]{7}, w):\mathbb{Q}]=6$. ← x^3-7の3つの解をすべて含む.
- $\mathbb{Q}(\sqrt[3]{7}, w)$ の $\mathbb{Q}$ 上のベクトル空間としての基底として，
  $1, \sqrt[3]{7}, (\sqrt[3]{7})^2, w, w\sqrt[3]{7}, w(\sqrt[3]{7})^2$ がとれる.
- $\mathbb{Q}(\sqrt[3]{7}, w)=\mathbb{Q}(\sqrt[3]{7}, w\sqrt[3]{7}, w^2\sqrt[3]{7})$.
  すなわち，$\mathbb{Q}(\sqrt[3]{7}, w)$ 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.

$\mathbb{Q}(\sqrt[3]{7}, w)=\mathbb{Q}(\sqrt[3]{7}, w\sqrt[3]{7}, w^2\sqrt[3]{7})$ は $x^3-7=0$ を完全に解くことに対応する体になっている.

($\mathbb{Q}(\sqrt[3]{7})$, $\mathbb{Q}(w\sqrt[3]{7})$, $\mathbb{Q}(w^2\sqrt[3]{7})$ とは異なる)

↖ $\mathbb{Q}(\sqrt[3]{7}, w)$ は $\mathbb{Q}$ 上の方程式 $x^3-7=0$ に対応する $\mathbb{Q}$ の Galois 拡大になっている

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

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

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

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

  をみたすものが唯一つ存在する.

問題 4-1 を解け.

$\mathbb{Q}(\zeta_5)/\mathbb{Q}$, $\zeta_5 = e^{2\pi i/5}$ (問題3-1) ← 正5角形の作図問題

- $k=1,2,3,4$ 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, $\mathbb{Q}(\zeta_5^k) \cong \mathbb{Q}[x]/(x^4+x^3+x^2+x+1)$.
- $\mathbb{Q}(\zeta_5) = \mathbb{Q}\left(\sqrt{5}, \sqrt{-\frac{5+\sqrt{5}}{2}}\right)$

$\mathbb{Q}(\zeta_5) = \mathbb{Q}\zeta_5 \oplus \mathbb{Q}\zeta_5^2 \oplus \mathbb{Q}\zeta_5^3 \oplus \mathbb{Q}\zeta_5^4$

$\mathbb{Q}(\zeta_{17})/\mathbb{Q}$, $\zeta_{17} = e^{2\pi i/17}$ (問題3-2) ← 正17角形の作図問題

- $k=1,2,\dots,16$ について, ζ_{17}^k の $\mathbb{Q}$ 上での最小多項式は $x^{16}+x^{15}+\cdots+x+1=0$.
- 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.

(αを根として持つ$\mathbb{Q}$係数の最低次の多項式でモニックなものを求めよ.)

(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

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

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

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

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

(2) $\mathbb{Q}(\alpha, w) = \mathbb{Q}(\alpha)1 \oplus \mathbb{Q}(\alpha)w$.

(既出の問題の解答例の結果を自由に使ってよい.)

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

$$\tau(a) = a \ (a \in \mathbb{Q}(\alpha)), \quad \tau(w) = w^2$$

をみたすものが唯一つ存在する.

($\alpha = \sqrt[3]{7}$ のとき $\tau(\beta) = \overline{\beta}$ $(\beta \in \mathbb{Q}(\alpha, w))$ ← $\alpha = w\sqrt[3]{7}, w^2\sqrt[3]{7}$ の場合はどうなるか?)

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

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

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

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

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

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

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

ヒント (1) $\{1, \omega, \omega^2, \cdots, \omega^{n-1}\}$は位数$n$の巡回群になる．

(2), (3) 問題 2-2 (4)． □

(ωはオメガ，wはダブリュ
νはニュー，vはヴィ，uはユー)