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

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

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

をみたすものが唯一つ存在することを示せ.

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

$\|$ おおざっぱ

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

$\|$

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

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

$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$ を示そう.

$[L:K] = \dim_K L$

$2\times 2 = 4$

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.

$\sqrt{2}$ で 0 になる $\mathbb{Q}$ 上のモニックな多項式で次数が最小のもの

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

$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

基底として $1, \sqrt{2}$ がとれる $\Longleftrightarrow$ 基底として, $\bar{1}, \bar{x}$ がとれる.

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ 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.
両辺を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, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

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

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, $x=\sqrt{2}+\sqrt{3}$ で 0 になる $f(x) \in \mathbb{Q}[x]$ でモニックで4次のものが $\sqrt{2}+\sqrt{3}$ の $\mathbb{Q}$ 上での最小多項式になる。

← 天くだり的でもうしわけない

$$f(x) = \left(x-(\sqrt{2}+\sqrt{3})\right)\left(x-(-\sqrt{2}+\sqrt{3})\right)\left(x-(\sqrt{2}-\sqrt{3})\right)\left(x-(-\sqrt{2}-\sqrt{3})\right)$$

← ここがおかしい

$$= \left((x-\sqrt{3})^2-2\right)\left((x+\sqrt{3})^2-2\right) = \left(x^2+1+2\sqrt{3}x\right)\left(x^2+1-2\sqrt{3}x\right)$$

$$= (x^2+1)^2 - 12x^2 = x^4 - 10x + 1 \in \mathbb{Q}[x].$$

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 $a,b,c,d\in\mathbb{Q}$ によって,

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

と表される.

もしも, $a,b,c,d\in\mathbb{Q}$ かつ $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=(a1+b\sqrt{2})\cdot1+(c1+d\sqrt{2})\sqrt{3}=0$ 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.

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

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

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

が成立することの証明の特殊化になっている.

(3) 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 τ と書く。τ 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 τ 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 τ の一意性も示された。

$\sqrt{3}$ を $-\sqrt{3}$ にうつす τ の作り方と一意性

σ 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。□

σ の唯一存在の証明も自分で書き下せ。

(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 σ と τ 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。□

$\varphi:\mathbb{Q}[x,y]\to\mathbb{Q}(\sqrt{2},\sqrt{3})$, $f(x,y)\mapsto f(\sqrt{2},\sqrt{3})$ に準同型を使え。

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

← $\omega^3 = 1$, $\omega \neq 1$ なので ω^k は $1, \omega, \omega^2$ のどれかになる．

(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

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

をみたすものが唯一つ存在する．

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

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

(問題4-1 の $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ を $\mathbb{Q}(\omega^k \sqrt[3]{7}, \omega)$ におきかえたのがこの問題)

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

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

をみたすものが唯一つ存在する．　□

$\boxed{\text{解答例}}$ (1) $\alpha, \omega\alpha, \omega^2\alpha \in \mathbb{Q}(\alpha, \omega)$ より，$\mathbb{Q}(\alpha, \omega) \supset \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$．

$\alpha \in \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ でかつ $\omega = \dfrac{\omega\alpha}{\alpha} \in \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ より，$\mathbb{Q}(\alpha, \omega) \subset \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$．

ゆえに，$\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\underbrace{\alpha, \omega\alpha, \omega^2\alpha}_{\alpha,\ \omega\alpha,\ \omega^2\alpha\ \text{は}\ x^2 - 7 = 0\ \text{の解の全体}})$．

(2) (問題3-5(2)と同様)

ωが1の原始3乗根でかつ $\alpha = \omega^k \sqrt[3]{7}$ 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、もしも $\omega \in \mathbb{Q}(\alpha)$ ならば虚数である $\underbrace{\text{1の原始3乗根}}$

が $\mathbb{Q}(\sqrt[3]{7})$ に含まれることになって矛盾する。ゆえに、$\omega \notin \mathbb{Q}(\alpha)$ である。

$x^2+x+1=0$ の解

$x = \dfrac{-1 \pm \sqrt{-3}}{2}$

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

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

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

$\left(\begin{array}{c} \alpha = \underset{\uparrow}{\omega^k} \sqrt[3]{7} \\ \text{ここに}\omega\text{があっても} \\ \omega \notin \mathbb{Q}(\alpha) \end{array} \right)$

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、

$$\mathbb{Q}(\alpha,\omega) = \mathbb{Q}(\alpha)1 \oplus \mathbb{Q}(\alpha)\omega$$

となることがわかる。

(3) $\alpha, \omega^2 \in \mathbb{Q}(\alpha, \omega)$ と $\alpha, \omega = (\omega^2)^2 \in \mathbb{Q}(\alpha, \omega^2)$ より, $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega^2)$ 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 を ω^2 にうつす同型を作る問題）

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

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

合成を 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,

$\mathbb{Q}(\alpha, \omega) = \{a + b\omega \mid a, b \in \mathbb{Q}(\alpha)\}$ でかつ任意の $a, b \in \mathbb{Q}(\alpha)$ について,

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

これより, ほしい τ の一意性がわかる.

（$\boxed{\text{注意}}$ $\alpha = \sqrt[3]{7}$ のとき, $\mathbb{Q}(\alpha) \subset \mathbb{R}$ でかつ $\omega^2 = (\omega$ 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^3-7 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, $6=[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]=[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\omega)]\underbrace{[\mathbb{Q}(\omega):\mathbb{Q}]}_{\omega\text{ の }\mathbb{Q}\text{ 上での最小多項式は }x^2+x+1\text{ なので }2\text{ に等しい}}=2[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\omega)]$.

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

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

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

(5) α と $\omega\alpha$ の $\mathbb{Q}(\omega)$ 上での最小多項式はどちらも x^3-7 で，

(αをωαにうつす自己同型を作る問題)

(1) の α が α と $\omega\alpha$ の場合より，$\mathbb{Q}(\alpha,\omega) = \mathbb{Q}(\alpha,\omega\alpha,\omega^2\alpha) = \mathbb{Q}(\omega\alpha,\omega)$.

体の同型写像たち

$$\begin{array}{ccccc} \mathbb{Q}(\alpha,\omega)=\mathbb{Q}(\omega)(\alpha) & \xrightarrow{\sim} & \mathbb{Q}(\omega)[x]/(x^3-7) & \xrightarrow{\sim} & \mathbb{Q}(\omega)(\omega\alpha)=\mathbb{Q}(\alpha,\omega) \\ f(\alpha) & \longmapsto & \overline{f(x)} & \longmapsto & f(\omega\alpha) \end{array}$$

の合成を σ と書く．σ も体の同型で，$\sigma(a)=a$ $(a\in\mathbb{Q}(\omega))$，$\sigma(\alpha)=\omega\alpha$ 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 $\sigma(a)=a$ $(a\in\mathbb{Q}(\omega))$，$\sigma(\alpha)=\omega\alpha$ をみたしているとする．このとき，任意の $a,b,c\in\mathbb{Q}(\omega)$ について，

$$\sigma(a+b\alpha+c\alpha^2) = \sigma(a)+\sigma(b)\sigma(\alpha)+\sigma(c)\sigma(\alpha)^2 = \underbrace{a}+\underbrace{b\omega}\alpha+\underbrace{c\omega^2}\alpha^2$$

どれも $\in\mathbb{Q}(\omega)$

これでほしい σ の一意性も示された．

□

$\boxed{\text{ポイント}}$ 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．

□

$\boxed{\text{注意}}$

(1), (2) のちがいは 非正規拡大と正規拡大のちがいになっている。

(1) 体の同型写像たち $\mathbb{Q}(\alpha) \xrightarrow{\sim} \mathbb{Q}[x]/(x^3-7) \xrightarrow{\sim} \mathbb{Q}(\omega\alpha)$ の合成を $\tilde{\sigma}$ と書くと、

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

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

$\tilde{\sigma}$ は体の<u>自己</u>同型ではない。

(2) 体の同型写像たち $\mathbb{Q}(\omega)(\alpha) \xrightarrow{\sim} \mathbb{Q}(\omega)[x]/(x^3-7) \xrightarrow{\sim} \mathbb{Q}(\omega)(\omega\alpha)$ の合成 σ の場合には、

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

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

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

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

$\mathbb{Q}(\omega, \alpha)$ は ω を含むので、α を $\omega\alpha$ にうつす操作で $\mathbb{Q}(\omega, \alpha)$ が閉じることが可能になる。これらのちがいを認識しておくことは重要である。 $\square$

$\boxed{\text{問題 4-3}}$ 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) $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^k) = \mathbb{Q}(\omega, \omega^2, \cdots, \omega^{p-1})$ $(k = 1, 2, \cdots, p-1)$．

$\mathbb{Q}$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

(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． $\square$

$\boxed{\text{解答例}}$ (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，$\omega^d = \omega^{ks+nt} \underset{\omega^n=1}{=} (\omega^k)^s \in \mathbb{Q}(\omega^k)$．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) $\mathbb{Q}(\omega)\subset\mathbb{Q}(\omega,\omega^2,\dots,\omega^{p-1})$ は自明であり，$\omega,\omega^2,\dots,\omega^{p-1}\in\mathbb{Q}(\omega)$ なので $\mathbb{Q}(\omega)\supset\mathbb{Q}(\omega,\omega^2,\dots,\omega^{p-1})$．
ゆえに，$\mathbb{Q}(\omega)=\mathbb{Q}(\omega,\omega^2,\dots,\omega^{p-1})$．

(3) 問題2-2(4)の結果より，$x^{p-1}+x^{p-2}+\cdots+x+1$ は $\underbrace{\mathbb{Q}\text{上の既約多項式}}$ になる．
pが素数なので

$\omega^p=1$ かつ $\omega\neq1$ と $\omega^p-1=(\omega-1)(\omega^{p-1}+\omega^{p-2}+\cdots+\omega+1)$ より，
$\omega^{p-1}+\omega^{p-2}+\cdots+\omega+1=0$ となることがわかる．

以上より，ω の $\mathbb{Q}$ 上での最小多項式は $x^{p-1}+x^{p-2}+\cdots+x+1$ になることがわかる．
これより，$\mathbb{Q}(\omega)\cong\mathbb{Q}[x]/(x^{p-1}+x^{p-2}+\cdots+x+1)$，$[\mathbb{Q}(\omega):\mathbb{Q}]=p-1$，

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

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

$\mathbb{Q}$上のベクトル空間としての同型

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．

□