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

$\mathbb{Q}$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 □

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

訂正あり
「$\mathbb{Q}\omega^{p-1}$」→「$\mathbb{Q}\omega^{p-2}$」
「$1,\omega,\cdots$」→「$\omega,\omega^2,\cdots$」

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

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

$\omega^p=1$ 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，$1,\omega,\omega^2,\cdots,\omega^{p-2}$ 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，

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

□