第13章　補足

13.1　補題12.7の証明

整数係数多項式 $f(x)$ によって $f(\zeta_p)$ で表される複素数全体の集合が R であった． ところで，$\zeta_p^p = 1$ なので，$f(x)$ の次数は p 未満であるとしてよい． すなわち，

$$R = \left\{ a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1} \;\middle|\; a_0, a_1, \ldots, a_{p-1} \in \boldsymbol{Z} \right\}.$$

(実は，$p-1$ 次未満にできるが，以下の議論には影響ないのでこのまま証明を続ける．)
さて，$\alpha \in R \cap \boldsymbol{Q}$ を任意にとる． このとき，$\alpha\zeta_p^i \in R$ だから

$$\alpha\zeta_p^i = \sum_{j=0}^{p-1} a_{ij}\zeta_p^j \qquad (i = 0, 1, \ldots, p-1)$$

をみたす $a_{ij} \in \boldsymbol{Z}$ がとれる． p 次正方行列 $A = (a_{ij})$ を考えれば，上式は

$$\alpha \begin{pmatrix} 1 \\ \zeta_p \\ \zeta_p^2 \\ \vdots \\ \zeta_p^{p-1} \end{pmatrix} = A \begin{pmatrix} 1 \\ \zeta_p \\ \zeta_p^2 \\ \vdots \\ \zeta_p^{p-1} \end{pmatrix}$$

と書き換えられ，これは α が A の固有値であることを示している． A の成分はすべて整数であるから，その固有多項式 $g(x)$ は

$$g(x) = x^p + c_{p-1}x^{p-1} + \cdots + c_1x + c_0 \qquad (c_i \in \boldsymbol{Z})$$

の形をしている． いま，$\alpha \in \boldsymbol{Q}$ でもあったから，これを既約分数

$$\alpha = \frac{s}{t} \qquad (s, t \in \boldsymbol{Z}\text{：互いに素，かつ}\ \ t > 0)$$

で表しておく． このとき，$g(\alpha) = 0$ より

$$\frac{s^p}{t^p} + c_{p-1}\frac{s^{p-1}}{t^{p-1}} + \cdots + c_1\frac{s}{t} + c_0 = 0,$$

$$\therefore \quad s^p + c_{p-1}s^{p-1}t + \cdots + c_1st^{p-1} + c_0t^p = 0.$$

よって，$s^p \equiv 0 \pmod{t}$ となるから，もし $t \neq 1$ ならば，s, t が互いに素であることに反する． したがって $t = 1$，すなわち $\alpha = s \in \boldsymbol{Z}$． よって $R \cap \boldsymbol{Q} \subset \boldsymbol{Z}$ であるが，逆の包含関係は明らかなので，補題 12.7 が証明された． □