資料14-1

**問題13-1** $F(x) = x^3 - 21x + 28$ 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。

このDは判別式と呼ばれている。

(2) $F(x)$ の3つの根を $\alpha, \beta, \gamma$ 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、$\mathrm{Gal}(L/\mathbb{Q}) \cong C_3$. □

$\cong A_3$ ← 3次の交代群

**解答例** $F(x) = x^3 + ax + b = (x-\alpha)(x-\beta)(x-\gamma)$ のとき、

$$D := (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = -4a^3 - 27b^2$$ となることを示そう。

$\alpha+\beta+\gamma = 0,\ \alpha\beta+\alpha\gamma+\beta\gamma = a,\ \alpha\beta\gamma = -b$ なので、

$$\alpha^2+\beta^2+\gamma^2 = (\alpha+\beta+\gamma)^2 - 2(\alpha\beta+\alpha\gamma+\beta\gamma) = -2a,$$

$$\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2 = (\alpha\beta+\alpha\gamma+\beta\gamma)^2 - 2\alpha\beta\gamma(\alpha+\beta+\gamma) = a^2.$$

$F'(\alpha) = 3\alpha^2 + a = (\alpha-\beta)(\alpha-\gamma)$, $F'(\beta) = 3\beta^2 + a = (\beta-\alpha)(\beta-\gamma)$, $F'(\gamma) = 3\gamma^2 + a = (\gamma-\alpha)(\gamma-\beta)$ より、

$$(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = -F'(\alpha)F'(\beta)F'(\gamma)$$

$$= -\Big(a^3 + 3\underbrace{(\alpha^2+\beta^2+\gamma^2)}_{=-2a}a^2 + 9\underbrace{(\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2)}_{=a^2}a + 27\underbrace{\alpha^2\beta^2\gamma^2}_{=b^2}\Big)$$

$$= -(a^3 - 6a^3 + 9a^3 + 27b^2) = -4a^3 - 27b^2.$$

(1) $F(x)=x^3-21x+28$ は $7\nmid 1$, $7\mid 0$, $7\mid -21$, $7\mid 28$, $7^2\nmid 28$ 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,

$$D=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2=-4a^3-27b^2$$

$$=4\cdot 21^3-27\cdot 28^2=2^2\cdot 3^3\cdot 7^3-2^4\cdot 3^3\cdot 7^2$$

$$=2^2\cdot 3^3\cdot 7^2(7-2^2)=2^2\cdot 3^4\cdot 7^2=(2\cdot 3^2\cdot 7)^2=126^2.$$

(3) $F(x)$の$\mathbb{Q}$上での最小分解体を$L$と書き, $G=Gal(L/\mathbb{Q})$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.

$\Delta=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$ とおくと, $\Delta^2=D=126^2$ より $\Delta=\pm 126\in\mathbb{Q}$ となる.

ゆえに, 任意の$\sigma\in G$について, $\sigma(\Delta)=\Delta$となり, $\sigma$は$\{\alpha,\beta,\gamma\}$の偶置換になる.

これより, $G\cong A_3\cong C_3$.

偶置換 $\Longleftrightarrow$ その作用で差積が不変

$\square$

**問題13-2** $F(x)=x^3+3x^2-3$ とおく，以下を示せ．

(1) $F(x)$ は $\mathbb{Q}$ 上既約である．

判別式

(2) $F(x)$ の3つの根を $\alpha,\beta,\gamma$ 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，$\mathrm{Gal}(L/\mathbb{Q})\cong C_3$．

**解答例** $F(x)=x^3+ax^2+b=(x-\alpha)(x-\beta)(x-\gamma)$ のとき，

$$(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2=-b(4a^3+27b)$$ となることを示そう．

$\alpha+\beta+\gamma=-a$，$\alpha\beta+\alpha\gamma+\beta\gamma=0$，$\alpha\beta\gamma=-b$．

$F'(\alpha)=3\alpha^2+2a\alpha=(\alpha-\beta)(\alpha-\gamma)$，$F'(\beta)=3\beta^2+2a\beta=(\beta-\alpha)(\beta-\gamma)$，$F'(\gamma)=3\gamma^2+3a\gamma=(\gamma-\alpha)(\gamma-\beta)$ より，

$$(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2=-F'(\alpha)F'(\beta)F'(\gamma)=-\alpha\beta\gamma(3\alpha+2a)(3\beta+2a)(3\gamma+2a)$$

$$=\underbrace{-\alpha\beta\gamma}_{=b}(8a^3+12\underbrace{(\alpha+\beta+\gamma)}_{-a}a^2+18\underbrace{(\alpha\beta+\alpha\gamma+\beta\gamma)}_{=0}a+27\underbrace{\alpha\beta\gamma}_{-b})$$

$$=b(8a^3-12a^3-27b)=-b(4a^3+27b).$$

(1) $F(x) = x^3+3x^2-3$ は, $3\nmid 1$, $3\mid 3$, $3\mid 0$, $3\mid -3$, $3^2\nmid -3$ 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,

$$D = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = -b(4a^3+27b) = 3\big(\overbrace{4\cdot 3^3 - \overset{3^3}{\overset{\parallel}{27}}\cdot 3}^{3^3}\big) = 3^4 = 9^2$$

(3) $F(x)$ の $\mathbb{Q}$ 上での最小分解体を $L$ と書き, $G = \mathrm{Gal}(L/\mathbb{Q})$ 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, $\Delta^2 = D = 9^2$ より, $\Delta = \pm 9 \in \mathbb{Q}$ となる
ゆえに, 任意の $\sigma \in G$ について, $\sigma(\Delta) = \Delta$ となり, $\sigma$ は $\{\alpha, \beta, \gamma\}$ の偶置換になる.
したがって, $G \cong A_3 \cong C_3$. $\square$

$\boxed{\text{注意}}$ $F(x-1) = (x-1)^3+3(x-1)^2-3 = x^3-3x^2+3x-1+3x^2-6x+3-3 = x^3-3x-1$.
$x^3-3x-1$ 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,
$\mathrm{Gal}(L/\mathbb{Q}) \cong A_3 \cong C_3$ となる. $\square$