Supplementary Exercises

Mitsuru Takigahira

練習 6.16

$\mathbf{Z}_2$ 上で既約な 3 次多項式を示し、それを用いて位数 8 の体 $\mathbf{F}_8$ を構成せよ。そのような多項式がちょうど 2 つあることを示し、対応する体は同型であることを示せ。

練習 6.16: 回答 (1)

3 次の多項式 $f(x)$ が既約であることは、
一次因子を持たない (すなわち $f(x) = 0$ が解をもたない) ことと同値である。
よって、$\mathbf{F}_2$ 上で既約な 3 次多項式は

- $f_\alpha(x) = x^3 + x^2 + 1$
- $f_\beta(x) = x^3 + x + 1$

の 2 つのみ存在し、解をそれぞれ α, β とおくと、2 つの位数 8 の有限体

- $\mathbf{F}_\alpha = \{a\alpha^2 + b\alpha + c \mid a, b, c \in \mathbf{F}_2\}$
- $\mathbf{F}_\beta = \{a\beta^2 + b\beta + c \mid a, b, c \in \mathbf{F}_2\}$

を構成できる。
このとき $\alpha^3 = \alpha^2 + 1$ 及び、$\beta^3 = \beta + 1$ なので、
$(\alpha + 1)^3 = \alpha^3 + \alpha^2 + \alpha + 1 = \alpha = (\alpha + 1) + 1$ となる。これを利用して、

$$g : \mathbf{F}_\beta \to \mathbf{F}_\alpha$$

$$g(a\alpha^2 + b\alpha + 1) = a\beta^2 + b\beta + (a + b + c)$$

なる写像 g を定義できる。

練習 6.16: 回答 (2)

この g は任意の

- $\gamma \in \mathbf{F}_2$
- $x = a_x\beta^2 + b_x\beta + c_x \in \mathbf{F}_\beta$
- $y = a_y\beta^2 + b_y\beta + c_y \in \mathbf{F}_\beta$

に対して

- $g(x+y) = (a_x+a_y)\alpha^2+(b_x+b_y)\alpha+(a_x+a_y+b_x+b_y+c_x+c_y) = g(x)+g(y)$
- $g(ax) = \gamma a_x\alpha^2 + \gamma b_x\alpha + \gamma c_x = \gamma(a_x\alpha^2 + b_x\alpha + c_x) = \gamma g(x)$

が成立するため線形写像である。
また、任意の $x, y \in \mathbf{F}_\beta$ に対して、
$g(x) = g(y) \Rightarrow g(x) - g(y) = g(x-y) = 0 \therefore x = y$ が成立し単射であり、
更に $|\mathbf{F}_\beta| = |\mathbf{F}_\alpha| = 8$ から全単射であることが言えるので g は同型写像である。
以上より、2 つの位数 8 の有限体 $\mathbf{F}_\alpha, \mathbf{F}_\beta$ が同型であることが示された。