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。

練習 6.17

$p \equiv 3 \mod (4)$ なる各 p に対して、多項式 $f(x) = x^2 + 1$ が
$\mathbf{Z}_p$ 上で既約であることを示せ。
これを用いて $q = p^2$ なる位数 q の体 $\mathbf{F}_q$ を構成せよ。
どんな素数 p に対して多項式 $x^2 + x + 1$ から位数 $q = p^2$ の体を構成できるか？

練習 6.17: 回答

x^2+1 が可約と仮定する、このとき $x^2+1=0$ はなんらかの解 $\alpha \in \mathbf{Z}_p$ を持つ。
式から $\alpha^2=-1$ なので $\alpha^4=1$ となり、フェルマーの小定理から $4 \mid p$ である。
これは $p \equiv 3 \mod (4)$ に矛盾する。よって多項式 x^2+1 は $\mathbf{Z}_p$ 上で既約である。
よって x^2+1 の解 α を $\mathbf{Z}_p$ に添加し、体 $\mathbf{F}_{p^2}=\{a\alpha+b \mid a,b \in \mathbf{Z}_p\}$ を構成できる。
同様の議論から、ある素数 p に対して $\mathbf{Z}_p$ 上で x^2+x+1 が可約ということは、
$\alpha^3-1=(\alpha-1)(\alpha^2+\alpha+1)=0$ なる $\mathbf{Z}_p \ni \alpha \neq 1$ が存在し、
フェルマーの小定理から $3 \mid p$ となる。
よって $p \equiv 2 \mod (3)$ なる p に対して与式は既約となり、その解 α を用いて
$\mathbf{F}_p^2=\{a\alpha+b \mid a,b \in \mathbf{Z}_p\}$ を構成できる。

練習 6.18

シングルトン限界、つまり
$\mathbf{F}_q$ 上の符号長 n かつ最小距離 d で符号語数が M の符号に対して、
$\log M \leq n - d + 1$ が成り立つことを証明せよ。
この上界に達する符号を最大分離符号 (MDS) と呼ぶが、このような符号はどのようなものか？

回答

$M \subseteq \mathbf{F}_q^n$ より $M \leq q^n$ で、最小距離が d なので、少なくとも $d-1$ 回符号桁を削除してパンクチャド符号を構成できる。
これにより、$M \leq q^{n-d+1}$ が成立し、$\log M \leq n - d + 1$ も成り立つ。
反復符号 $\mathcal{R}_n$ 及びパリティ検査符号 $\mathcal{P}_n$ がこの上界に達する。

練習 6.19

次の計算と因数分解を行い、その結果から完全符号の存在についてどのようなことが言えるか答えよ

$$1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3} \text{ and } 1+\binom{11}{1}\cdot 2+\binom{11}{2}\cdot 2$$

回答

$$1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}=2048=2^{11},\ 1+\binom{11}{1}\cdot 2+\binom{11}{2}\cdot 2=243=3^5$$

より、前者は $q=2, M=2^{12}, t=3$ の、後者は $q=3, M=3^6, t=2$ の
ハミングの球充填限界式の等号である。
よって符号語長 23 の 2 元完全符号及び符号語長 11 の 3 元完全符号の存在が示された

練習 6.20

$i = 1, 2$ に対して C_i が $\mathcal{V} = \mathbf{F}_q^n$ 上の (n, M_i, d_i) 符号のとき、

$$C_1 \oplus C_2 = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{V} \oplus \mathcal{V} \mid \mathbf{x} \in C_1, \mathbf{y} \in C_2\}$$

が $d = \min(d_1, d_2)$ の下 $(2n, M_1 M_2, d)$ 符号であることを示せ。更に

$$C_1 * C_2 = \{(\mathbf{x}, \mathbf{x} + \mathbf{y}) \in \mathcal{V} \oplus \mathcal{V} \mid \mathbf{x} \in C_1, \mathbf{y} \in C_2\}$$

が $d = \min(2d_1, d_2)$ の下 $(2n, M_1 M_2, d')$ 符号であることを示せ。
また、各 C_i が次元 k_i で線形の場合 $C_1 \oplus C_2$ と $C_1 * C_2$ はともに線形で次元が $k_1 + k_2$ となることを示せ。