離散数理工学 (7) 2015 年 12 月 1 日

演習問題 岡本 吉央

提出締切： 2015 年 12 月 8 日 講義終了時

復習問題 7.1 多項式 $f(x), g(x) \in \mathbb{Z}_2[x]$ を次のように定義する．

- $f(x) = x^5 + x^3 + 1$.
- $g(x) = x^2 + x + 1$.

このとき，$f(x) \bmod g(x)$ が何であるか，答えよ．

復習問題 7.2 剰余環 $\mathbb{Z}_2[x]/(x^2+1)$ の和表と積表を与えよ．そこから，なぜ $\mathbb{Z}_2[x]/(x^2+1)$ が体ではないか，説明せよ．

復習問題 7.3 剰余環 $\mathbb{Z}_2[x]/(x^2+x+1)$ の和表と積表を与えよ．

復習問題 7.4 素数 p と既約多項式 $g(x) \in \mathbb{Z}_p[x]$ を考える．

1. 体 $\mathbb{Z}_p[x]/(g(x))$ の位数が p^m であることを証明せよ．ただし，$m = \deg g(x)$ とする．
2. 体 $\mathbb{Z}_p[x]/(g(x))$ の標数が p であることを証明せよ．

復習問題 7.5 位数 9 の有限体を構成したい．以下の問いに答えよ．

1. 多項式 $x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ が既約であることを証明せよ．
2. 剰余環 $\mathbb{Z}_3[x]/(x^2+2x+2)$ の和表と積表を与えよ．

復習問題 7.6 次を満たす多項式 $h(x) \in \mathbb{Z}_3[x]/(x^3+2x+2)$ をすべて答えよ．

$$(x^2+2) \cdot h(x) \bmod (x^3+2x+2) = 1.$$

(注：$x^3+2x+2 \in \mathbb{Z}_3[x]$ が既約であることを使ってもよい．(演習問題 6.8))

復習問題 7.7 次を満たす多項式 $h(x) \in \mathbb{Z}_5[x]/(x^3+x^2+2)$ をすべて答えよ．

$$(4x^2+2x+3) \cdot h(x) \bmod (x^3+x^2+2) = 1.$$

(注：$x^3+x^2+2 \in \mathbb{Z}_5[x]$ が既約であることを使ってもよい．(演習問題 6.13))

追加問題 7.8 位数 8 の有限体を構成したい．以下の問いに答えよ．

1. 多項式 $x^3 + x + 1 \in \mathbb{Z}_2[x]$ が既約であることを証明せよ．
2. 剰余環 $\mathbb{Z}_2[x]/(x^3+x+1)$ の和表と積表を与えよ．

追加問題 7.9 位数 9 の有限体を構成するために，以下の問いに答えよ．

1. 多項式 $x^2 + x + 2 \in \mathbb{Z}_3[x]$ が既約であることを証明せよ．
2. 剰余環 $\mathbb{Z}_3[x]/(x^2+x+2)$ の和表と積表を与えよ．

追加問題 7.10 次を満たす多項式 $h(x) \in \mathbb{Z}_7[x]/(x^2+x+3)$ をすべて答えよ．

$$(5x+3) \cdot h(x) \bmod (x^2+x+3) = 1.$$

(注：$x^2+x+3 \in \mathbb{Z}_7[x]$ が既約であることを使ってもよい．(演習問題 6.12))

追加問題 7.11 演習問題 7.5 と演習問題 7.9 では，位数 9 の有限体を構成した．この 2 つは異なるが，「構造」は同じである．より正確に述べると，ある全単射

$$\varphi\colon \mathbb{Z}_3[x]/(x^2+x+2) \to \mathbb{Z}_3[x]/(x^2+2x+2)$$

が存在して，任意の $f(x), g(x) \in \mathbb{Z}_3[x]/(x^2+x+2)$ に対して，

$$\begin{aligned} \varphi(f(x)) + \varphi(g(x)) &= \varphi(f(x)+g(x)), \\ \varphi(f(x)) \cdot \varphi(g(x)) &= \varphi(f(x) \cdot g(x)) \end{aligned}$$

が成り立つ．そのような φ を具体的に記述せよ．