

離散数理工学 第 7 回
離散代数：多項式環による有限体の構成

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2015 年 12 月 1 日

最終更新：2015 年 11 月 30 日 10:58

スケジュール 前半 (予定)

- | | | |
|---|----------------------|---------|
| 1 | 数え上げの基礎：二項係数と二項定理 | (10/6) |
| ★ | 休講 (体育祭) | (10/13) |
| 2 | 数え上げの基礎：漸化式の立て方 | (10/20) |
| 3 | 数え上げの基礎：漸化式の解き方 (基礎) | (10/27) |
| ★ | 祝日で休み | (11/3) |
| 4 | 数え上げの基礎：漸化式の解き方 (発展) | (11/10) |
| 5 | 離散代数：整数と有限体 | (11/17) |
| 6 | 離散代数：多項式環 | (11/24) |
| 7 | 離散代数：多項式環による有限体の構成 | (12/1) |
| 8 | 離散代数：有限体の応用 | (12/8) |

注意：予定の変更もありうる

スケジュール 後半 (予定)

- | | | |
|----|---------------------------|---------|
| 9 | 離散確率論：確率の復習と確率不等式 | (12/15) |
| ★ | 中間試験 | (12/22) |
| 10 | 離散確率論：確率的離散システムの解析 | (1/5) |
| 11 | 離散確率論：乱択データ構造とアルゴリズム (基礎) | (1/12) |
| 12 | 離散確率論：乱択データ構造とアルゴリズム (発展) | (1/19) |
| 13 | 離散確率論：マルコフ連鎖 (基礎) | (1/26) |
| 14 | 離散確率論：マルコフ連鎖 (発展) | (2/2) |
| ★ | 予備日 | (2/9) |
| ★ | 期末試験 | (2/16?) |

注意：予定の変更もありうる

今日の目標

有限体の構成法を理解し、実際に構成できるようになる

鍵となる概念

- ▶ 多項式環の剰余環
- ▶ 既約多項式

目次

- ① 多項式環の剰余環
- ② 多項式環による有限体の構成法
- ③ 多項式環による有限体の構成法：逆元の求め方
- ④ 今日のまとめ

多項式による剰余

素数 p , 多項式環 $\mathbb{Z}_p[x]$, 多項式 $f(x), g(x) \in \mathbb{Z}_p[x]$

多項式による剰余：記法

$f(x)$ を $g(x)$ で割った剰余を次のように書く

$$f(x) \bmod g(x)$$

例： $p = 2$ のとき，次のように $f(x), g(x)$ をとる

▶ $f(x) = x^5 + x^3 + 1$

▶ $g(x) = x^2 + x + 1$

このとき，

$$f(x) = g(x) \cdot (x^3 + x^2 + x) + (x + 1)$$

なので， $f(x) \bmod g(x) = x + 1$

多項式環の剰余環

素数 p , 多項式環 $\mathbb{Z}_p[x]$, 多項式 $g(x) \in \mathbb{Z}_p[x]$

多項式環の剰余環とは？

$\mathbb{Z}_p[x]$ を $g(x)$ で割った剰余環とは, 次の集合

$$\mathbb{Z}_p[x]/(g(x)) = \{f(x) \bmod g(x) \mid f(x) \in \mathbb{Z}_p[x]\}$$

注: 加算と乗算を行うことができる

例:

$$\mathbb{Z}_2[x]/(x^2 + 1) = \{0, 1, x, x + 1\},$$

$$\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, x, x + 1\}$$

この2つは集合としては等しいが, 演算の結果が異なる

(環として等しくない)

多項式環の剰余環：乗算

 $\mathbb{Z}_2[x]/(x^2 + 1) = \{0, 1, x, x + 1\}$ において

$$\begin{aligned}(x + 1) \cdot (x + 1) &= x^2 + 2x + 1 = x^2 + 1 \\ &= 0\end{aligned}$$

 $\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, x, x + 1\}$ において

$$\begin{aligned}(x + 1) \cdot (x + 1) &= x^2 + 2x + 1 = (x^2 + x + 1) + x \\ &= x\end{aligned}$$

和表と積表 (1)

 $\mathbb{Z}_2[x]/(x^2 + 1) = \{0, 1, x, x + 1\}$ における和表と積表

+	0	1	x	x + 1
0	0	1	x	x + 1
1	1	0	x + 1	x
x	x	x + 1	0	1
x + 1	x + 1	x	1	0

·	0	1	x	x + 1
0	0	0	0	0
1	0	1	x	x + 1
x	0	x	1	x + 1
x + 1	0	x + 1	x + 1	0

和表と積表 (2)

 $\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, x, x + 1\}$ における和表と積表

+	0	1	x	x + 1
0	0	1	x	x + 1
1	1	0	x + 1	x
x	x	x + 1	0	1
x + 1	x + 1	x	1	0

·	0	1	x	x + 1
0	0	0	0	0
1	0	1	x	x + 1
x	0	x	x + 1	1
x + 1	0	x + 1	1	x

積表の違い

問題

0 ではない $f(x) \in \mathbb{Z}_p[x]/(g(x))$ に対して

$$f(x)h(x) = 1$$

となる $h(x) \in \mathbb{Z}_p[x]/(g(x))$ が必ず存在するか？

$\mathbb{Z}_2[x]/(x^2 + 1)$ における積表

\cdot	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

$\mathbb{Z}_2[x]/(x^2 + x + 1)$ における積表

\cdot	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

必ず存在するわけではない
 $((x+1)h(x) = 1??)$

必ず存在する

積表の違い：なぜ違うのか？

なぜ違うのか？

$x^2 + 1 \in \mathbb{Z}_2[x]$ は
既約多項式ではない

$x^2 + x + 1 \in \mathbb{Z}_2[x]$ は
既約多項式である

$\mathbb{Z}_2[x]/(x^2 + 1)$ における積表

\cdot	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

$\mathbb{Z}_2[x]/(x^2 + x + 1)$ における積表

\cdot	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

必ず存在するわけではない
($(x+1)h(x) = 1$??)

必ず存在する

目次

- ① 多項式環の剰余環
- ② 多項式環による有限体の構成法
- ③ 多項式環による有限体の構成法：逆元の求め方
- ④ 今日のまとめ

多項式環による有限体の構成法

素数 p , 整数 m

目標

位数 p^m の有限体を構成すること

(位数 = 要素数)

手順

- 1 次数 m の既約多項式 $g(x) \in \mathbb{Z}_p[x]$ を見つける
- 2 剰余環 $\mathbb{Z}_p[x]/(g(x))$ を考える

この剰余環が位数 p^m の有限体となる

- ▶ これが体であることは,
 \mathbb{Z}_p が体であることの証明と同じように証明できる
 - ▶ 記号がややこしくなるので, 割愛
- ▶ 位数が p^m であることの証明: 後述

手順

- 1 次数 m の既約多項式 $g(x) \in \mathbb{Z}_p[x]$ を見つける

$g(x) = x^2 + x + 1$ とする

- ▶ $g(x)$ が既約であることを確認する必要があるが
 $x^2 + x + 1 \in \mathbb{Z}_2[x]$ が既約であることは証明済み

手順

2 剰余環 $\mathbb{Z}_p[x]/(g(x))$ を考える

$g(x) = x^2 + x + 1$ なので, $\mathbb{Z}_2[x]/(g(x)) = \{0, 1, x, x + 1\}$

+	0	1	x	x + 1
0	0	1	x	x + 1
1	1	0	x + 1	x
x	x	x + 1	0	1
x + 1	x + 1	x	1	0

·	0	1	x	x + 1
0	0	0	0	0
1	0	1	x	x + 1
x	0	x	x + 1	1
x + 1	0	x + 1	1	x

構成した有限体の位数

素数 p , 多項式 $g(x) \in \mathbb{Z}_p[x]$

命題

$\deg g(x) = m$ であるとき, $|\mathbb{Z}_p[x]/(g(x))| = p^m$

証明: $\mathbb{Z}_p[x]/(g(x))$ の要素は次数 $m-1$ 以下の多項式すべて

- ▶ それは, ある $a_0, a_1, a_2, \dots, a_{m-1} \in \mathbb{Z}_p$ を用いて

$$a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1}$$

と書けるものすべて

- ▶ すなわち,

$$|\mathbb{Z}_p[x]/(g(x))| = |\mathbb{Z}_p|^m = p^m$$

□

構成した有限体の標数 (1)

素数 p , 多項式 $g(x) \in \mathbb{Z}_p[x]$

命題

任意の $f(x) \in \mathbb{Z}_p[x]/(g(x))$ に対して, $p \cdot f(x) = 0$

証明:

- ▶ $f(x) \in \mathbb{Z}_p[x]/(g(x))$ は, ある $a_0, a_1, a_2, \dots, a_{m-1} \in \mathbb{Z}_p$ を用いて

$$a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1}$$

と書ける

- ▶ ここで, 任意の $i \in \{1, \dots, m-1\}$ に対して $p \cdot a_i \bmod p = 0$
- ▶ すなわち, p を法として, $p \cdot f(x) = 0$ □

構成した有限体の標数 (2)

素数 p

命題

任意の $c \in \mathbb{Z}_p - \{0\}$ と任意の正整数 $n \in \mathbb{Z}_+$ に対して

$$n < p \Rightarrow n \cdot c \bmod p \neq 0$$

証明 : 対偶を証明するために, $n \cdot c \bmod p = 0$ と仮定

- ▶ $n \cdot c$ は p を因数として持つ
- ▶ $c < p$ であり, p は素数なので, n が p を因数として持つ
- ▶ つまり, $n \geq p$

□

帰結

体 $\mathbb{Z}_p[x]/(g(x))$ の標数は p である

手順

1 次数 m の既約多項式 $g(x) \in \mathbb{Z}_p[x]$ を見つける

$g(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ として, $g(x)$ が既約であることを確認

▶ 次を満たす多項式 $g_1(x), g_2(x) \in \mathbb{Z}_3[x]$ が存在すると仮定

$$g(x) = g_1(x)g_2(x), \quad \deg g_1(x) \geq 1, \quad \deg g_2(x) \geq 1$$

▶ $\deg g(x) = 2$ なので, $\deg g_1(x) = \deg g_2(x) = 1$

▶ 因数定理より, $g(x)$ の根が存在

▶ しかし, $g(0) = 2, g(1) = 2, g(2) = 1$ であり,
0 も 1 も 2 も $g(x)$ の根ではないので, 矛盾

□

例：位数 9 の有限体：和表

 $(p = 3, m = 2)$

手順

2 剰余環 $\mathbb{Z}_p[x]/(g(x))$ を考える

$$\mathbb{Z}_3[x]/(x^2 + 2x + 2) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$$

+	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
1	1	2	0	x + 1	x + 2	x	2x + 1	2x + 2	2x
2	2	0	1	x + 2	x	x + 1	2x + 2	2x	2x + 1
x	x	x + 1	x + 2	2x	2x + 1	2x + 2	0	1	2
x + 1	x + 1	x + 2	x	2x + 1	2x + 2	2x	1	2	0
x + 2	x + 2	x	x + 1	2x + 2	2x	2x + 1	2	0	1
2x	2x	2x + 1	2x + 2	0	1	2	x	x + 1	x + 2
2x + 1	2x + 1	2x + 2	2x	1	2	0	x + 1	x + 2	x
2x + 2	2x + 2	2x	2x + 1	2	0	1	x + 2	x	x + 1

例：位数 9 の有限体：積表

 $(p = 3, m = 2)$

手順

2 剰余環 $\mathbb{Z}_p[x]/(g(x))$ を考える

$$\mathbb{Z}_3[x]/(x^2 + 2x + 2) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$$

\cdot	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
2	0	2	1	$2x$	$2x + 2$	$2x + 1$	x	$x + 2$	$x + 1$
x	0	x	$2x$	$x + 1$	$2x + 1$	1	$2x + 2$	2	$x + 2$
$x + 1$	0	$x + 1$	$2x + 2$	$2x + 1$	2	x	$x + 2$	$2x$	1
$x + 2$	0	$x + 2$	$2x + 1$	1	x	$2x + 2$	2	$x + 1$	$2x$
$2x$	0	$2x$	x	$2x + 2$	$x + 2$	2	$x + 1$	1	$2x + 1$
$2x + 1$	0	$2x + 1$	$x + 2$	2	$2x$	$x + 1$	1	$2x + 2$	x
$2x + 2$	0	$2x + 2$	$x + 1$	$x + 2$	1	$2x$	$2x + 1$	x	2

注：「 $x^2 + 2x + 2$ で割る」 \equiv 「 x^2 を $-2x - 2$ で置き換える」

目次

- ① 多項式環の剰余環
- ② 多項式環による有限体の構成法
- ③ 多項式環による有限体の構成法：逆元の求め方
- ④ 今日のまとめ

逆元の求め方：例 1

例 1

次を満たす $h(x) \in \mathbb{Z}_3[x]/(x^3 + 2x + 2)$ を求めよ

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

注： $x^3 + 2x + 2 \in \mathbb{Z}_3[x]$ は既約多項式なので，そのような $h(x)$ は唯一

- ▶ $\mathbb{Z}_3[x]$ において多項式の除算を行い，次を得る

$$x^3 + 2x + 2 = (x^2 + 2) \cdot x + 2$$

- ▶ したがって， $\mathbb{Z}_3[x]$ において

$$(x^2 + 2) \cdot x = (x^3 + 2x + 2) - 2 = (x^3 + 2x + 2) + 1$$

- ▶ ゆえに， $(x^2 + 2) \cdot x \bmod (x^3 + 2x + 2) = 1$

- ▶ したがって， $h(x) = x$



逆元の求め方：例 2

例 2

次を満たす $h(x) \in \mathbb{Z}_5[x]/(x^3 + x^2 + 2)$ を求めよ

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

注： $x^3 + x^2 + 2 \in \mathbb{Z}_5[x]$ は既約多項式なので，そのような $h(x)$ は唯一

- ▶ $\mathbb{Z}_5[x]$ において多項式の除算を行い，次を得る

$$x^3 + x^2 + 2 = (4x^2 + 2x + 3)(4x + 2) + 4x + 1$$

$$4x^2 + 2x + 3 = (4x + 1)(x + 4) + 4$$

- ▶ したがって， $\mathbb{Z}_5[x]$ において

$$\begin{aligned} 1 &= 4 \cdot 4 = 4(4x^2 + 2x + 3 - (4x + 1)(x + 4)) \\ &= 4(4x^2 + 2x + 3 - (x^3 + x^2 + 2 - (4x^2 + 2x + 3)(4x + 2))(x + 4)) \\ &= (4x^2 + 2x + 3)(4 + 4(4x + 2)(x + 4)) + (x^3 + x^2 + 2)(-4(x + 4)) \\ &= (4x^2 + 2x + 3)(x^2 + 2x + 1) + (x^3 + x^2 + 2)(x + 4) \end{aligned}$$

逆元の求め方：例 2 (続き)

例 2

次を満たす $h(x) \in \mathbb{Z}_5[x]/(x^3 + x^2 + 2)$ を求めよ

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

得られた式

$\mathbb{Z}_5[x]$ において

$$1 = (4x^2 + 2x + 3)(x^2 + 2x + 1) + (x^3 + x^2 + 2)(x + 4)$$

- ▶ ゆえに, $(4x^2 + 2x + 3)(x^2 + 2x + 1) \bmod (x^3 + x^2 + 2) = 1$
- ▶ したがって, $h(x) = x^2 + 2x + 1$ □

逆元の求め方：例 2 — 検算

例 2

次を満たす $h(x) \in \mathbb{Z}_5[x]/(x^3 + x^2 + 2)$ を求めよ

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

求められた $h(x) = x^2 + 2x + 1$

格言

検算を怠らない

検算： $\mathbb{Z}_5[x]$ において

$$\begin{aligned} (4x^2 + 2x + 3)(x^2 + 2x + 1) &= 4x^4 + 10x^3 + 11x^2 + 8x + 3 \\ &= 4x^4 + x^2 + 3x + 3 \\ &= (x^3 + x^2 + 2)(4x + 1) + 1 \end{aligned}$$

すなわち， $\mathbb{Z}_5[x]$ において

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

目次

- ① 多項式環の剰余環
- ② 多項式環による有限体の構成法
- ③ 多項式環による有限体の構成法：逆元の求め方
- ④ 今日のまとめ

今日のまとめ

今日のまとめ

有限体の構成法を理解し、実際に構成できるようになる

鍵となる概念

- ▶ 多項式環の剰余環
- ▶ 既約多項式

知られていること

任意の正整数 $m \geq 1$ と任意の素数 p に対して、
次数 m の既約多項式が $\mathbb{Z}_p[x]$ に存在する

証明法 (のいくつか)

- ▶ 実際に構成する (例: コンウェイ多項式)
- ▶ 次数 m の既約多項式の数 N_m が 1 以上であることを数学的帰納法で証明する

残った時間の使い方

- ▶ 演習問題をやる
 - ▶ 相談推奨 (ひとりでやらない)
- ▶ 質問をする
 - ▶ 教員と TA は巡回
- ▶ 退室時, 小さな紙に感想など書いて提出する ← 重要
 - ▶ 内容は何でも OK
 - ▶ 匿名で OK

目次

- ① 多項式環の剰余環
- ② 多項式環による有限体の構成法
- ③ 多項式環による有限体の構成法：逆元の求め方
- ④ 今日のまとめ