離散数理工学 第 6 回
離散代数：多項式環

岡本 吉央
okamotoy@uec.ac.jp
電気通信大学

2015 年 11 月 24 日

最終更新：2015 年 12 月 2 日　08:31

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

今日の目標

多項式に関する基礎を身につける
- 多項式に対する除法の定理
- 多項式の根，因数定理，既約多項式

ただし，ここでの多項式は「体の上の一変数多項式」に限る

目次

いままでよく見た多項式

いままでよく見た多項式の例

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

用語
- $f(x)$ の変数，あるいは，不定元：x
- $f(x)$ の次数：$\deg(f(x)) = 2$

$f(x)$ の各項の係数は実数

$\mathbb{R}$ の上の多項式：定義

$\mathbb{R}$ の上の多項式とは？
- $\mathbb{R}$ の上の多項式とは，すべての項の係数が $\mathbb{R}$ の要素である多項式
- つまり，ある自然数 $n \geq 0$ と実数 $a_0, a_1, \dots, a_n$ に対して
$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$
と，変数 x を用いて書ける式のこと

注意：上の多項式を $\displaystyle\sum_{i=0}^{n} a_i x^i$ と書くこともある

多項式の次数とは？

$a_n \neq 0$ のとき，上の多項式の次数は n であるとする

$\mathbb{Z}_2$ の上の多項式：定義

$\mathbb{Z}_2$ の上の多項式とは？
- $\mathbb{Z}_2$ の上の多項式とは，すべての項の係数が $\mathbb{Z}_2$ の要素である多項式
- つまり，ある自然数 $n \geq 0$ と $\mathbb{Z}_2$ の要素 $a_0, a_1, \dots, a_n$ に対して
$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$
と，変数 x を用いて書ける式のこと

注意：上の多項式を $\displaystyle\sum_{i=0}^{n} a_i x^i$ と書くこともある

多項式の次数とは？

$a_n \neq 0$ のとき，上の多項式の次数は n であるとする

$\mathbb{Z}_2$ の上の多項式：例

復習：$\mathbb{Z}_2 = \{0, 1\}$

$\mathbb{Z}_2$ の上の多項式で，次数が 2 のもの

次の 4 つ

- $x^2 + x + 1$
- $x^2 + x$
- $x^2 + 1$
- x^2

$\mathbb{Z}_2$ の上の多項式：多項式どうしの加算と乗算

多項式どうしを足す：例

$\mathbb{Z}_2$ において

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

多項式どうしを掛ける：例

$\mathbb{Z}_2$ において

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

$\cdot$	x^2	x	1
x^2	x^4	x^3	x^2
1	x^2	x	1

体 K の上の多項式：定義

体 K

K の上の多項式とは？

- K の上の多項式とは，すべての項の係数が K の要素である多項式
- つまり，ある自然数 $n \geq 0$ と K の要素 $a_0, a_1, \ldots, a_n$ に対して
$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$
と，変数 x を用いて書ける式のこと

注意：上の多項式を $\sum_{i=0}^{n} a_i x^i$ と書くこともある

多項式の次数とは？

$a_n \neq 0$ のとき，上の多項式の次数は n であるとする

典型的な K の例：$\mathbb{R}$，$\mathbb{C}$，$\mathbb{Z}_2$，$\mathbb{Z}_3$，素数 p に対する $\mathbb{Z}_p$，...

体の上の多項式環

体 K

K の上の多項式環とは？

- K の上の多項式環とは，
K の上の多項式をすべて集めた集合 (加算と乗算を行なえる)
- 記法：$K[x]$

例えば，

$$\begin{aligned}\mathbb{Z}_2[x] = \{&0, 1,\\ &x, x+1,\\ &x^2, x^2+1, x^2+x, x^2+x+1,\\ &\ldots\}\end{aligned}$$

多項式の同等性

体 K

多項式の同等性：定義

多項式 $f(x), g(x) \in K[x]$ が

$$f(x) = \sum_{i=0}^{n} a_i x^i, \qquad g(x) = \sum_{i=0}^{m} b_i x^i$$

と書けるとき，(ただし，$a_n \neq 0$, $b_m \neq 0$)
$f(x) = g(x)$ であることを次の両方が満たされることで定義する

- $n = m$ (つまり，$\deg f(x) = \deg g(x)$)
- すべての $i \in \{1, \ldots, n\}$ に対して，$a_i = b_i$

多項式の次数：性質

体 K，多項式 $f(x), g(x) \in K[x]$，$f(x) \neq 0, g(x) \neq 0$

多項式の次数が持つ性質

- $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$
- $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$

例：$x^2 + 1, x^2 + x + 1 \in \mathbb{Z}_2[x]$ に対して，

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

体の上の多項式環：注意

注意：次のような問いは意味を成さない

多項式 $x^2 + 2x + 1$ は $\mathbb{Z}_5$ の上の多項式か？

無理に回答するならば，「状況に依存する」

つまり，⋯

多項式を使う場合には，どの体の上の多項式なのか，明確に書かないといけない

- $\mathbb{Z}_7$ の上の多項式 $x^2 + 2x + 1$ に対して，⋯ $(x^2 + 2x + 1 \in \mathbb{Z}_7[x])$
- $\mathbb{Z}_5$ の上の多項式 $x^2 + 2x + 1$ に対して，⋯ $(x^2 + 2x + 1 \in \mathbb{Z}_5[x])$
- $\mathbb{Z}_2$ の上の多項式 $x^2 + 2x + 1$ に対して，⋯ $(x^2 + 2x + 1 \in \mathbb{Z}_2[x])$
- $\mathbb{R}$ の上の多項式 $x^2 + 2x + 1$ に対して，⋯ $(x^2 + 2x + 1 \in \mathbb{R}[x])$
- $\mathbb{C}$ の上の多項式 $x^2 + 2x + 1$ に対して，⋯ $(x^2 + 2x + 1 \in \mathbb{C}[x])$

今から行うこと

今から行うこと

- 「K の上の多項式」が
「$\mathbb{R}$ の上の多項式」や「$\mathbb{C}$ の上の多項式」のような性質を
持つことの確認
- 「K の上の多項式」が
「$\mathbb{R}$ の上の多項式」や「$\mathbb{C}$ の上の多項式」が持つすべての性質を
持つわけではないことの確認

目次

多項式に対する除法の定理

体 K

多項式に対する除法の定理

多項式 $f(x), g(x) \in K[x]$ (ただし，$\deg(g(x)) \geq 1$) に対して
次を満たす多項式 $q(x), r(x) \in K[x]$ が一意に存在する

$$f(x) = g(x)q(x) + r(x), \quad \deg(r(x)) < \deg(g(x))$$

用語

- $q(x)$：$f(x)$ を $g(x)$ で割った商 (quotient)
- $r(x)$：$f(x)$ を $g(x)$ で割った剰余 (remainder, residue)

多項式に対する除法の定理：例 1

例 1：$f(x), g(x) \in \mathbb{Z}_2[x]$ を次のように定める

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

このとき，

$$\begin{aligned} f(x) &= x^5 + x^3 + 1 \\ &= (x^2 + x + 1)(x^3 + x^2 + x) + x + 1 \\ &= g(x) \cdot (x^3 + x^2 + x) + x + 1 \end{aligned}$$

したがって，$f(x)$ を $g(x)$ で割った商は $x^3 + x^2 + x \in \mathbb{Z}_2[x]$ で，
剰余は $x + 1 \in \mathbb{Z}_2[x]$ である □

多項式に対する除法の定理：例 1 — 筆算

例 1：$f(x), g(x) \in \mathbb{Z}_2[x]$ を次のように定める

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

$$\begin{array}{r|cccccc} & x^3 & -x^2 & +x & & & \\ \hline x^2+x+1 & x^5 & & +x^3 & & & +1 \\ & x^5 & +x^4 & +x^3 & & & \\ \hline & & -x^4 & & & & \\ & & -x^4 & -x^3 & -x^2 & & \\ \hline & & & x^3 & +x^2 & & \\ & & & x^3 & +x^2 & +x & \\ \hline & & & & & -x & +1 \end{array}$$

したがって，$\mathbb{Z}_2[x]$ において

$$\begin{aligned} x^5 + x^3 + 1 &= (x^2 + x + 1)(x^3 - x^2 + x) - x + 1 \\ &= (x^2 + x + 1)(x^3 + x^2 + x) + x + 1 \end{aligned}$$

多項式に対する除法の定理：例 2

例 2：$f(x), g(x) \in \mathbb{Z}_3[x]$ を次のように定める

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

このとき，

$$\begin{aligned} f(x) &= x^5 + x^3 + 1 \\ &= (x^2 + x + 1)(x^3 + 2x^2 + x) + 2x + 1 \\ &= g(x) \cdot (x^3 + 2x^2 + x) + 2x + 1 \end{aligned}$$

したがって，$f(x)$ を $g(x)$ で割った商は $x^3 + 2x^2 + x \in \mathbb{Z}_3[x]$ で，
剰余は $2x + 1 \in \mathbb{Z}_3[x]$ である □

多項式に対する除法の定理：例 2 — 筆算

例 2：$f(x), g(x) \in \mathbb{Z}_3[x]$ を次のように定める

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

$$\begin{array}{r|cccccc} & x^3 & -x^2 & +x & & & \\ \hline x^2+x+1 & x^5 & & +x^3 & & & +1 \\ & x^5 & +x^4 & +x^3 & & & \\ \hline & & -x^4 & & & & \\ & & -x^4 & -x^3 & -x^2 & & \\ \hline & & & x^3 & +x^2 & & \\ & & & x^3 & +x^2 & +x & \\ \hline & & & & & -x & +1 \end{array}$$

したがって，$\mathbb{Z}_3[x]$ において

$$\begin{aligned} x^5 + x^3 + 1 &= (x^2 + x + 1)(x^3 - x^2 + x) - x + 1 \\ &= (x^2 + x + 1)(x^3 + 2x^2 + x) + 2x + 1 \end{aligned}$$

約元，倍元

体 K，多項式 $f(x), g(x) \in K[x]$

約元，倍元とは？

ある多項式 $q(x) \in K[x]$ が存在して $f(x) = g(x)q(x)$ となるとき，
次のように言う

- $f(x)$ は $g(x)$ の倍元である
- $g(x)$ は $f(x)$ の約元である (因子である)
- $f(x)$ は $g(x)$ で割り切れる (整除される)
- $g(x)$ は $f(x)$ を割る

また，これを $g(x) \mid f(x)$ と書くことがある (整除関係)

約元，倍元：例

- $x^2 + 1, x + 1 \in \mathbb{Z}_2[x]$ に対して

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

  であるので，$\mathbb{Z}_2[x]$ において，$x^2 + 1$ は $x + 1$ で割り切れる
- $x^3 + x + 2, x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ に対して

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

  であるので，$\mathbb{Z}_3[x]$ において，$x^3 + x + 2$ は $x^2 + 2x + 2$ で割り切れる

公約元，最大公約元

体 K，多項式 $f_1(x), f_2(x), \dots, f_n(x) \in K[x]$ $(n \geq 2)$

公約元とは？

$f_1(x), f_2(x), \dots, f_n(x)$ の公約元とは，
すべての $i = 1, \dots, n$ に対して $f_i(x)$ の約元であるような，
体 K の上の多項式

最大公約元とは？

$f_1(x), f_2(x), \dots, f_n(x)$ の最大公約元とは，
$f_1(x), f_2(x), \dots, f_n(x)$ の公約元の中で「最大」のもの

つまり，$g(x)$ が $f_1(x), f_2(x), \dots, f_n(x)$ の最大公約元であるとは，
$g(x)$ が $f_1(x), f_2(x), \dots, f_n(x)$ の公約元であり，
$f_1(x), f_2(x), \dots, f_n(x)$ の任意の公約元 $h(x)$ に対して，$h(x) \mid g(x)$ となる

公約元，最大公約元：例

$\mathbb{Z}_3$ の上の多項式環 $\mathbb{Z}_3[x]$ を考える

- $f(x) = x^3 + x^2 + 2x + 2$, $g(x) = x^3 + 2x^2 + 2x + 1$ とする
- このとき，

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

- つまり，$(x+1)(x+2) = x^2 + 2$ は $f(x), g(x)$ の最大公約元
- また，$2(x+1)(x+2) = 2x^2 + 1$ も $f(x), g(x)$ の最大公約元

この場合，最大公約元は 定数倍を除いて 一意に定まる

- つまり，$f(x), g(x)$ の最大公約元は $x^2 + 2$ と $2x^2 + 1$

ユークリッドの互除法

体 K

ユークリッドの互除法

多項式 $f(x), g(x) \in K[x]$ に対して (ただし，$g(x) \neq 0$)

$$f(x) = g(x)q(x) + r(x), \quad \deg(r(x)) < \deg(g(x))$$

を満たす $q(x), r(x)$ を考える．このとき，

$f(x), g(x)$ の最大公約元と $g(x), r(x)$ の最大公約元は等しい

ユークリッドの互除法：例

例：$f(x)$ と $g(x)$ の最大公約元を $\gcd(f(x), g(x))$ と書くとする

- $f(x) = x^3 + x^2 + 2x + 2, g(x) = x^3 + 2x^2 + 2x + 1 \in \mathbb{Z}_3[x]$ を考える
- $x^3 + x^2 + 2x + 2 = (x^3 + 2x^2 + 2x + 1) + 2x^2 + 1$ なので，
  $\gcd(x^3+x^2+2x+2, x^3+2x^2+2x+1) = \gcd(x^3+2x^2+2x+1, 2x^2+1)$
- $x^3 + 2x^2 + 2x + 1 = (2x^2 + 1)(2x + 1)$ なので，
  $$\gcd(x^3 + 2x^2 + 2x + 2, 2x^2 + 1) = 2x^2 + 1$$
- $2x^2 + 1$ の定数倍 $2(2x^2 + 1) = x^2 + 2$ も $f(x), g(x)$ の最大公約元
- $\therefore f(x), g(x)$ の最大公約元は $2x^2 + 1$ と $x^2 + 2$

目次

多項式の根

体 K

多項式の根 (こん) とは？

K の上の多項式 $f(x) \in K[x]$ の根とは，次を満たす $\alpha \in K$ のこと

$$f(\alpha) = 0$$

例：$f(x) = x^4 + 2x \in \mathbb{Z}_3[x]$ の根は？

- $f(0) = 0^4 + 2 \cdot 0 = 0$
- $f(1) = 1^4 + 2 \cdot 1 = 3 = 0$
- $f(2) = 2^4 + 2 \cdot 2 = 20 = 2 \neq 0$

つまり，$x^4 + 2x \in \mathbb{Z}_3[x]$ の根は $0, 1$ である

多項式の根と因子分解

先ほどの例：$f(x) = x^4 + 2x \in \mathbb{Z}_3[x]$ に対して

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

つまり，

$\alpha^4 + 2\alpha = 0 \quad \Leftrightarrow \quad \alpha^3 = 0$ または $\alpha + 2 = 0 \quad \Leftrightarrow \quad \alpha = 0$ または $\alpha = 1$

因数定理

体 K，$\alpha \in K$，$f(x) \in K[x]$

因数定理

$f(x)$ が $x - \alpha$ で割り切れる $\Leftrightarrow$ $f(\alpha) = 0$
(α は $f(x)$ の根である)

証明 ($\Rightarrow$)：$f(x) \in K[x]$ が $x - \alpha$ で割り切れると仮定

- ある多項式 $q(x) \in K[x]$ が存在して，$f(x) = (x - \alpha)q(x)$
- すなわち，$f(\alpha) = (\alpha - \alpha)q(\alpha) = 0$ □

因数定理 (続き)

体 K，$\alpha \in K$，$f(x) \in K[x]$

因数定理

$f(x)$ が $x-\alpha$ で割り切れる $\Leftrightarrow$ $f(\alpha)=0$ (α は $f(x)$ の根である)

証明 ($\Leftarrow$)：$f(\alpha)=0$ であると仮定

- ある多項式 $q(x), r(x) \in K[x]$ を用いて，$f(x)=(x-\alpha)q(x)+r(x)$ と書ける (ただし，$\deg r(x) \leq (\deg(x-\alpha))-1=1-1=0$)
- つまり，ある $\beta \in K$ を用いて $r(x)=\beta$ と書ける
- このとき，$f(x)=(x-\alpha)q(x)+\beta$
- ゆえに，$0=f(\alpha)=(\alpha-\alpha)q(\alpha)+\beta=\beta$
- つまり，$f(x)=(x-\alpha)q(x)$ となり，$f(x)$ は $x-\alpha$ で割り切れる □

因子分解：例

例題

多項式 $x^4+x^3+x+1 \in \mathbb{Z}_2[x]$ を因子分解してみる

$f(x)=x^4+x^3+x+1$ とする

- $f(1)=1^4+1^3+1+1=0$ なので，$f(x)$ は $x-1$ で割り切れる
- 注：$\mathbb{Z}_2[x]$ において，$x-1=x+1$
- よって，$f(x)=(x+1)(x^3+1)$

$g(x)=x^3+1$ とする

- $g(1)=1^3+1=0$ なので，$g(x)$ は $x-1$ で割り切れる
- よって，$g(x)=(x+1)(x^2+x+1)$

$h(x)=x^2+x+1$ とする

- $h(0)=1, h(1)=1$ なので，$h(x)$ はこれ以上分解できない ←本当？

したがって，$f(x)=(x+1)^2(x^2+x+1)$

既約多項式

体 K，多項式 $f(x) \in K[x]$，$\deg f(x) \geq 1$

多項式の可約性とは？

$f(x)$ が可約であるとは，ある多項式 $g(x), h(x) \in K[x]$ が存在して

$$f(x)=g(x)h(x), \quad \deg g(x) \geq 1, \deg h(x) \geq 1$$

を満たすこと

既約多項式とは？

$f(x)$ が既約であるとは，$f(x)$ が可約ではないこと

既約分解

体 K，多項式 $f(x) \in K[x]$，$\deg f(x) \geq 1$

既約分解とは？

多項式 $f(x)$ の既約分解とは，
既約多項式 $q_1(x), q_2(x), \dots, q_m(x) \in K[x]$ を用いて

$$f(x)=q_1(x) \cdot q_2(x) \cdot \cdots \cdot q_m(x)$$

と書くこと

既約分解：例

例題：より正確に

多項式 $x^4+x^3+x+1 \in \mathbb{Z}_2[x]$ を既約分解してみる

$f(x)=x^4+x^3+x+1$ とする

- 先ほどと同様に，$f(x)=(x+1)^2(x^2+x+1)$

あと証明すべきことは

(1) $x+1 \in \mathbb{Z}_2[x]$ が既約であること
(2) $x^2+x+1 \in \mathbb{Z}_2[x]$ が既約であること

多項式の既約性 (1)

(1) $x+1 \in \mathbb{Z}_2[x]$ が既約であること

- 次を満たす多項式 $g(x), h(x) \in \mathbb{Z}_2[x]$ が存在すると仮定
  $$x+1=g(x)h(x), \quad \deg g(x) \geq 1, \quad \deg h(x) \geq 1$$
- このとき，$\deg(x+1)=1$ であり，
  $$\deg g(x)h(x)=\deg g(x)+\deg h(x) \geq 2$$
- 両辺の次数が異なるので，矛盾 □

より一般的に，次数が 1 である多項式は既約

多項式の既約性 (2)

(2) $x^2+x+1 \in \mathbb{Z}_2[x]$ が既約であること

- 次を満たす多項式 $g(x), h(x) \in \mathbb{Z}_2[x]$ が存在すると仮定
  $$x^2+x+1=g(x)h(x), \quad \deg g(x) \geq 1, \quad \deg h(x) \geq 1$$
- このとき，$\deg(x^2+x+1)=2$ であり，
  $$\deg g(x)h(x)=\deg g(x)+\deg h(x) \geq 2$$
- したがって，$\deg g(x)=\deg h(x)=1$
- 因数定理より，x^2+x+1 の根が存在
- しかし，0 も 1 も x^2+x+1 の根ではないので，矛盾 □

既約分解：例 — 結論

例題：より正確に

多項式 $x^4+x^3+x+1 \in \mathbb{Z}_2[x]$ を既約分解してみる

$f(x)=x^4+x^3+x+1$ とする

- 先ほどと同様に，$f(x)=(x+1)^2(x^2+x+1)$

あと証明すべきことは

(1) $x+1 \in \mathbb{Z}_2[x]$ が既約であること (証明済)
(2) $x^2+x+1 \in \mathbb{Z}_2[x]$ が既約であること (証明済)

したがって，$(x+1)^2(x^2+x+1)$ は x^4+x^3+x+1 の既約分解である □

多項式の既約性：例 2

次の例題

多項式 $x^3+2x+2 \in \mathbb{Z}_3[x]$ が既約であることを証明せよ

証明：$f(x)=x^3+2x+2$ とする

- 次を満たす多項式 $g(x), h(x) \in \mathbb{Z}_3[x]$ が存在すると仮定
$$f(x)=g(x)h(x), \quad \deg g(x) \geq 1, \quad \deg h(x) \geq 1$$
- このとき，$\deg f(x)=3$ であるので，$g(x)$ か $h(x)$ の次数は 1
- 因数定理より，$f(x)$ の根が存在
- このとき，$\mathbb{Z}_3$ において
$$\begin{aligned} f(0) &= 0^3+2\cdot 0+2=0+0+2=2 \\ f(1) &= 1^3+2\cdot 1+2=1+2+2=5=2 \\ f(2) &= 2^3+2\cdot 2+2=8+4+2=14=2 \end{aligned}$$
- すなわち，0 も 1 も 2 も x^3+2x+2 の根ではないので，矛盾 □

多項式の既約性：例 2 — 注意

注意

多項式 $x^3+2x+2 \in \mathbb{R}[x]$ は既約ではない

実際，$x^3+2x+2=0$ は実数解を持ち，因子分解できる

多項式の既約性：例 3

次の例題

多項式 $x^4+x^3+1 \in \mathbb{Z}_2[x]$ が既約であることを証明せよ

証明：$f(x)=x^4+x^3+1$ とする

- 次を満たす多項式 $g(x), h(x) \in \mathbb{Z}_3[x]$ が存在すると仮定
$$f(x)=g(x)h(x), \quad \deg g(x) \geq 1, \quad \deg h(x) \geq 1$$
- $f(0)=1, f(1)=1$ なので，
因数定理より，$f(x)$ は次数 1 の因子を持たない
- したがって，$\deg g(x) \geq 2, \deg h(x) \geq 2$
- $\deg f(x)=4$ なので，$\deg g(x)=\deg h(x)=2$

多項式の既約性：例 3 (続き)

次の例題

多項式 $x^4+x^3+1 \in \mathbb{Z}_2[x]$ が既約であることを証明せよ

証明 (続き)：

- $\mathbb{Z}_2[x]$ における次数 2 の多項式は以下の 4 つ
$$x^2, \quad x^2+1, \quad x^2+x, \quad x^2+x+1$$
- ここで，次のような分解が可能である
$$x^2=x\cdot x, \quad x^2+1=(x+1)^2, \quad x^2+x=x(x+1)$$
- $f(x)$ は次数 1 の因数を持たないので，
$g(x), h(x)$ も次数 1 の因数を持たない
- したがって，$g(x)=h(x)=x^2+x+1$ でなければならない
- しかし，$g(x)h(x)=(x^2+x+1)^2=x^4+x^2+1 \neq f(x)$
- これは矛盾 □

目次

今日のまとめと次回の予告

今日のまとめ

多項式に関する基礎を身につける

- 多項式に対する除法の定理
- 多項式の根，因数定理，既約多項式

ただし，ここでの多項式は「体の上の一変数多項式」に限る

次回の予告

多項式を用いて，有限体を構成する

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