離散数理工学 第 5 回
離散代数：整数と有限体

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2015 年 11 月 17 日

最終更新：2015 年 11 月 17 日　13:21

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

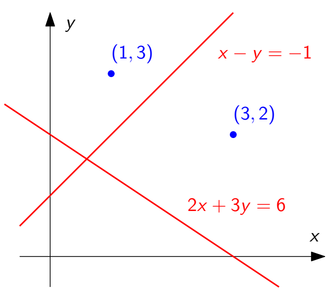
今日の目標

今日の目標

整数の剰余に関する基礎を身につける
- 剰余とモジュラ算術
- 有限体

$\mathbb{R}^2$ における点と直線

- 点は 2 つの実数の組 $(x, y) \in \mathbb{R}^2$ で与えられる
- 直線は方程式 $ax + by = c$ を満たす実数の組 $(x, y) \in \mathbb{R}^2$ 全体の集合 ($a, b, c \in \mathbb{R}$)



$\mathbb{R}^2$ における点と直線：2 直線の交点

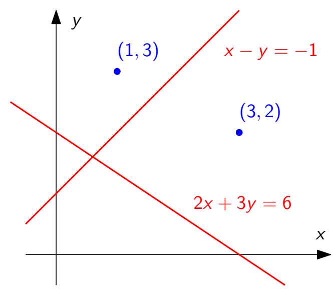
2 つの異なる直線は，交わるならば，1 点で交わる
(交わらない場合は平行)

直線 $2x + 3y = 6$ と $x - y = -1$ の交点は？

⇝ 連立方程式

$$\begin{aligned} 2x + 3y &= 6 \\ x - y &= -1 \end{aligned}$$

解くと，$(x, y) = (3/5, 8/5)$



$\mathbb{Z}_2^2$ における点と直線

$\mathbb{Z}_2 = \{0, 1\}$ (加算，乗算は mod 2 で行う)

考えるもの

$\mathbb{Z}_2^2$ における点と直線

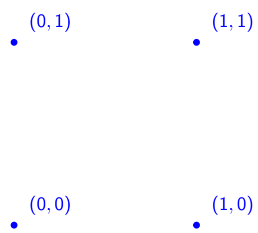
- 点は 2 つの $\mathbb{Z}_2$ の要素の組 $(x, y) \in \mathbb{Z}_2^2$ で与えられる
- 直線は方程式 $ax + by = c$ を満たす $\mathbb{Z}_2$ の要素の組 $(x, y) \in \mathbb{Z}_2^2$ 全体の集合 ($a, b, c \in \mathbb{Z}_2$)

$\mathbb{Z}_2^2$ における点

- 点は 2 つの $\mathbb{Z}_2$ の要素の組 $(x, y) \in \mathbb{Z}_2^2$ で与えられる

つまり，次のものしかありえない

$$(0, 0), \quad (0, 1), \quad (1, 0), \quad (1, 1)$$

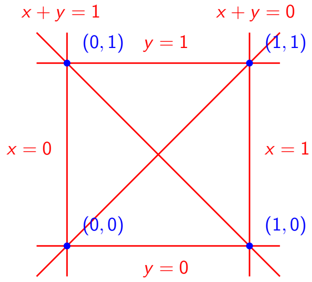


$\mathbb{Z}_2^2$ における直線

- 直線は方程式 $ax + by = c$ を満たす $\mathbb{Z}_2$ の要素の組 $(x, y) \in \mathbb{Z}_2^2$ 全体の集合 $(a, b, c \in \mathbb{Z}_2)$

つまり，次の方程式しかありえない

$$x = 0, \quad y = 0, \quad x + y = 0, \quad x = 1, \quad y = 1, \quad x + y = 1$$



$\mathbb{Z}_2^2$ における点と直線：2 直線の交点

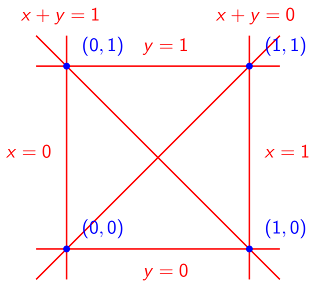
2 つの異なる直線は，交わるならば，1 点で交わる
(交わらない場合は平行)

直線 $x + y = 1$ と $y = 1$ の交点は？

$\rightsquigarrow$ 連立方程式

$$\begin{aligned} x + y &= 1 \\ y &= 1 \end{aligned}$$

解くと，$(x, y) = (0, 1)$



疑問と回答

疑問

1. このように「点」と「直線」を定められる (有限) 集合は何か？
2. それは何の役に立つのか？

回答

1. 有限体
2. いろいろな場面で役に立つ
   - この講義では組合せデザインを扱う
   - 組合せデザイン：規則性を持った配置に関する話題

目次

整数：記法

この講義での記法

- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$：整数全体の集合
- $\mathbb{N} = \{0, 1, 2, \ldots\}$：自然数全体の集合 (0 以上の整数全体の集合)
- $\mathbb{Z}_+ = \{1, 2, \ldots\}$：正整数全体の集合 (1 以上の整数全体の集合)

研究者や著者，分野によって，記号法が異なる場合があるので注意

整数の商と剰余

商と剰余

整数 a と正の整数 b に対して，次を満たす整数 q, r が一意に存在する

$$a = bq + r, \qquad 0 \leq r \leq b - 1$$

用語

- q：a を b で割った商 (quotient)
- r：a を b で割った剰余 (あるいは，余り，residue)

「一意に」 $=$ 「ただ一つ」

例

- $a = 8, b = 3$ のとき：$8 = 3 \cdot 2 + 2$ (商は 2，剰余は 2)
- $a = 9, b = 11$ のとき：$9 = 11 \cdot (-1) + 2$ (商は -1，剰余は 2)
- $a = -5, b = 3$ のとき：$-5 = 3 \cdot (-2) + 1$ (商は -2，剰余は 1)

約数，倍数

整数 a, b

約数，倍数

ある整数 q が存在して $a = bq$ となるとき，次のように言う

- a は b の倍数である
- b は a の約数である
- a は b で割り切れる (整除される)
- b は a を割る

また，これを $b \mid a$ と書くことがある (整除関係)

例：

- 72 は 9 の倍数であり，9 は 72 の約数である
- -12 は 2 の倍数であり，2 は -12 の約数である

最大公約数

整数 $a_1, a_2, \ldots, a_n$ $(n \geq 2)$

公約数とは？

$a_1, a_2, \ldots, a_n$ の公約数とは，
すべての $i = 1, \ldots, n$ に対して a_i の約数であるような整数

最大公約数とは？

$a_1, a_2, \ldots, a_n$ の最大公約数とは，
$a_1, a_2, \ldots, a_n$ の公約数の中で最大のもの

$a_1, a_2, \ldots, a_n$ の最大公約数を $\gcd(a_1, a_2, \ldots, a_n)$ と書く

最大公約数の性質

$a > b > 0$ のとき，$\gcd(a, b) = \gcd(a - b, b)$ (ユークリッドの互除法)

素数

正整数 p

素数とは？

p が素数であるとは，p が 1 と p 以外の約数を持たないこと

素数でない数 (合成数) の例：

- 4 は 2 を約数として持つ
- 793 は 13 を約数として持つ

目次

剰余：記法

整数 m

剰余

整数 a を m で割った剰余を $a \bmod m$ と書く

性質

- $0 \leq a \bmod m \leq m-1$

モジュラ算術

モジュラ算術とは？

剰余を考慮した整数に対する算術

正整数 $m \in \mathbb{Z}_+$

- 考える集合は $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$
- $a, b \in \mathbb{Z}_m$ に対して
  a と b の加算は $(a+b) \bmod m$
  a と b の乗算は $ab \bmod m$

このような加算・乗算は m を法とする加算・乗算と呼ぶ

記法

$a \bmod m = b \bmod m$ であることを

$$a \equiv b \pmod{m}$$

とも書く (a, b は m を法として合同)

モジュラ算術の法則

モジュラ算術の法則

正整数 $m \in \mathbb{Z}_+$ と整数 $a, b \in \mathbb{Z}$ に対して

1. $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
2. $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

証明： 1 だけ証明する (2 は演習問題)

- $a = mq + r, b = mq' + r'$ と一意に書ける
  (ただし，$0 \leq r \leq m-1, 0 \leq r' \leq m-1$)
- このとき，$a \bmod m = r, b \bmod m = r'$
- また，$a + b = mq + r + mq' + r' = m(q+q') + r + r'$ なので，
  $(a+b) \bmod m = (r + r') \bmod m$ □

モジュラ算術における逆操作：減算

次はどのように行うか？

- 減算：加算の逆演算 (これは問題ない：b は負でもよいから)
- 除算：乗算の逆演算 (これは注意が必要)

減算の例

次を満たす $x \in \mathbb{Z}_7$ は何か？

$$(3-x) \bmod 7 = 6$$

解：$3 - x = 6$ という方程式を解いて，最後に 7 を法とすればよい

- $\mathbb{Z}$ において方程式 $3 - x = 6$ を x について解くと，$x = -3$
- $-3 \bmod 7 = 4$ であるので，$x = -3 \bmod 7 = 4$ □

モジュラ算術における逆操作：除算？

次はどのように行うか？

- 減算：加算の逆演算 (これは問題ない：b は負でもよいから)
- 除算：乗算の逆演算 (これは注意が必要)

除算の例？

次を満たす $x \in \mathbb{Z}_7$ は何か？

$$3x \bmod 7 = 2$$

解 (間違い)：$3x = 2$ という方程式を解いて，最後に 7 を法とすればよい？

- 方程式 $3x = 2$ を x について解くと，$x = 2/3 = 0$
- $0 \bmod 7 = 0$ であるので，$x = 0 \bmod 7 = 0$

これは正しくない ($3 \cdot 0 \bmod 7 = 0 \neq 2$)

モジュラ算術における逆操作：除算？

次はどのように行うか？

- 減算：加算の逆演算 (これは問題ない：b は負でもよいから)
- 除算：乗算の逆演算 (これは注意が必要)

除算の例？

次を満たす $x \in \mathbb{Z}_7$ は何か？

$$3x \bmod 7 = 2$$

疑問

- このような方程式をどのように解けばよいのか？
- そもそも，解はあるのか？
- 解があるとしたら，いくつあるのか？

モジュラ算術における逆操作：除算 — まずやってみる

除算の例？

次を満たす $x \in \mathbb{Z}_7$ は何か？

$$3x \bmod 7 = 2$$

解：

- ある整数 y が存在して，$3x = 7y + 2$
- つまり，$7y + 2$ は 3 の倍数
- $y = 1$ のとき，$7y + 2 = 7 \cdot 1 + 2 = 9$ となり，これは 3 の倍数
- したがって，$x = 3$ は解の候補
- 実際，$x = 3$ とすると，$3x \bmod 7 = 3 \cdot 3 \bmod 7 = 9 \bmod 7 = 2$ □

もう少しシステマティックにやるには？

除算：ちゃんとやる

正整数 $m \in \mathbb{Z}_+$，整数 $a, b \in \mathbb{Z}$

モジュラ演算における除算

$\gcd(m, a) = 1$ であるとき，次の方程式

$$ax \bmod m = b \bmod m$$

はただ 1 つだけ解を持つ

当面の目標：これを証明する

互いに素である整数の性質 A

$a, b \in \mathbb{Z}_+$ で，$\gcd(a, b) = 1$ とする

補題 A (重要)

ある整数 $u, v \in \mathbb{Z}$ が存在して，$ua + vb = 1$

証明：$a + b$ に関する数学的帰納法による
[基底段階]

- $a = b = 1$ のとき，$2a - b = 2 - 1 = 1$

注：$\gcd(a, b) = 1$ なので，$a = b$ ならば，$a = b = 1$

互いに素である整数の性質 A (続き)

$a, b \in \mathbb{Z}_+$ で，$\gcd(a, b) = 1$ とする

補題 A (重要)

ある整数 $u, v \in \mathbb{Z}$ が存在して，$ua + vb = 1$

証明：$a + b$ に関する数学的帰納法による
[帰納段階]：$a > b \geq 1$ とする

- $a + b > a' + b'$ であり，$\gcd(a', b') = 1$ であるような任意の $a', b' \in \mathbb{Z}_+$ に対して，ある整数 u', v' が存在して $u'a' + v'b' = 1$ であると仮定
- $a > b \geq 1$ より，$1 = \gcd(a, b) = \gcd(a - b, b)$
- 帰納法の仮定から，ある整数 u', v' が存在して，$u'(a - b) + v'b = 1$
- すなわち，$u'a + (v' - u')b = 1$
- $u', v' \in \mathbb{Z}$ なので，$v' - u' \in \mathbb{Z}$ □

互いに素である整数の性質 B

$a, b \in \mathbb{Z}_+$ で，$\gcd(a, b) = 1$ とする

補題 B

$c \in \mathbb{Z}$ に対して，$bc \bmod a = 0 \Rightarrow c \bmod a = 0$

証明：補題 A より，$ua + vb = 1$ を満たす整数 u, v が存在する

- このとき，$uac + vbc = c$
- $bc \bmod a = 0$ なので，$bc = aq$ を満たす整数 q が存在
- $\therefore uac + vaq = c$
- $\therefore a(uc + vq) = c$
- $uc + vq$ は整数なので，$c \bmod a = 0$ □

集合 $\mathbb{Z}_m$ の性質

正整数 $m \in \mathbb{Z}_+$，整数 $a \in \mathbb{Z}$

補題 C

$\gcd(m, a) = 1$ のとき，集合として，

$$\mathbb{Z}_m = \{ax \bmod m \mid x \in \mathbb{Z}_m\}$$

例：$m = 5, a = 4$ のとき

- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
- 一方，

$$\begin{aligned}\{4x \bmod 5 \mid x \in \mathbb{Z}_5\} &= \{0 \bmod 5, 4 \bmod 5, 8 \bmod 5, \\ &\quad 12 \bmod 5, 16 \bmod 5\} \\ &= \{0, 4, 3, 2, 1\} = \mathbb{Z}_5\end{aligned}$$

集合 $\mathbb{Z}_m$ の性質：証明

正整数 $m \in \mathbb{Z}_+$，整数 $a \in \mathbb{Z}$

補題 C

$\gcd(m, a) = 1$ のとき，集合として，

$$\mathbb{Z}_m = \{ax \bmod m \mid x \in \mathbb{Z}_m\}$$

証明：写像 $x \mapsto ax \bmod m$ が単射であればよい

- $x, y \in \mathbb{Z}_m$ に対して，$ax \bmod m = ay \bmod m$ であるとする
- つまり，$a(x - y) \bmod m = 0$
- $\gcd(m, a) = 1$ なので，補題 B より，$(x - y) \bmod m = 0$
- すなわち，$x \bmod m = y \bmod m$
- $x, y \in \mathbb{Z}_m$ なので，$x \bmod m = x$ かつ $y \bmod m = y$
- したがって，$x = y$ □

除算：ちゃんとやる

正整数 $m \in \mathbb{Z}_+$，整数 $a, b \in \mathbb{Z}$

モジュラ演算における除算

$\gcd(m, a) = 1$ であるとき，次の方程式

$$ax \bmod m = b \bmod m$$

は $\mathbb{Z}_m$ にただ 1 つだけ解を持つ

証明：補題 C より $\mathbb{Z}_m = \{ax \bmod m \mid x \in \mathbb{Z}_m\}$

- $b \bmod m \in \mathbb{Z}_m$ なので，$ax \bmod m = b \bmod m$ となる $x \in \mathbb{Z}_m$ が存在
- $x \mapsto ax \bmod m$ は全単射なので，そのような x はただ 1 つ存在 □

除算の例 (2)

次の式を満たす $x \in \mathbb{Z}_{56}$ は何か？

$$25x \bmod 56 = 1$$

$\gcd(56,25) = \gcd(25,6) = \gcd(6,1) = 1$ なので (ユークリッドの互除法)，先ほどの命題から，解がただ 1 つ存在すると分かる

- $25x = 56y + 1$ となる整数 y が存在
- ここで (ユークリッドの互除法)，

$$56 = 25 \cdot 2 + 6, \qquad 25 = 6 \cdot 4 + 1$$

- $\therefore 1 = 25 - 6 \cdot 4 = 25 - (56 - 25 \cdot 2) \cdot 4 = 56 \cdot (-4) + 9 \cdot 25$
- $\therefore x = 9, y = 4$ とすれば $25x = 56y + 1$ は成り立つ
- $\therefore x = 9$ □

除算の例 (3)

次の式を満たす $x \in \mathbb{Z}_{583}$ は何か？

$$80x \bmod 583 = 339$$

$\gcd(583,80) = \gcd(80,23) = \gcd(23,11) = \gcd(11,1) = 1$ なので
先ほどの命題から，解がただ 1 つ存在すると分かる

- $80x = 583y + 339$ となる整数 y が存在
- ここで (ユークリッドの互除法)，

$$583 = 7 \cdot 80 + 23, \quad 80 = 3 \cdot 23 + 11, \quad 23 = 2 \cdot 11 + 1$$

- したがって，

$$\begin{aligned} 1 &= 23 - 2 \cdot 11 = 23 - 2 \cdot (80 - 3 \cdot 23) = -2 \cdot 80 + 7 \cdot 23 \\ &= -2 \cdot 80 + 7 \cdot (583 - 7 \cdot 80) = 7 \cdot 583 - 51 \cdot 80 \end{aligned}$$

除算の例 (3)

次の式を満たす $x \in \mathbb{Z}_{583}$ は何か？

$$80x \bmod 583 = 339$$

続き

- $\therefore -51 \cdot 80 = -7 \cdot 583 + 1$
- $\therefore -51 \cdot 339 \cdot 80 = -7 \cdot 339 \cdot 583 + 339$
- $\therefore x = -51 \cdot 339, y = -7 \cdot 339$ とすれば $80x = 583y + 339$ は成り立つ
- ここで，$-51 \cdot 339 \bmod 583 = -17289 \bmod 583 = 201$
- つまり，$x = 201$ □

正整数 $m \in \mathbb{Z}_+$，整数 $a, b \in \mathbb{Z}$

モジュラ演算における除算

$\gcd(m,a) = 1$ であるとき，次の方程式

$$ax \bmod m = b \bmod m$$

は $\mathbb{Z}_m$ にただ 1 つだけ解を持つ

ここから次の命題が直ちに導かれる

素数を法とする場合

m が素数であり，$a \in \mathbb{Z}_m - \{0\}$ であるとき，次の方程式

$$ax \bmod m = 1$$

は $\mathbb{Z}_m$ にただ 1 つだけ解を持つ

素数を法とする場合

m が素数であり，$a \in \mathbb{Z}_m - \{0\}$ であるとき，次の方程式

$$ax \bmod m = 1$$

は $\mathbb{Z}_m$ にただ 1 つだけ解を持つ

$\mathbb{Z}_m$ において，そのような x は乗法に関する a の「逆元」である

- つまり，m が素数のとき，
  $\mathbb{Z}_m$ において加算，減算，乗算，除算が可能

$\leadsto$ 有限体

目次

p が素数であるとき

集合 $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ を考えると，

- 加算ができる (p を法として)
- 乗算ができる (p を法として)
- 加算に関する逆元が存在する ($a + x = 0$ となる x が存在)
- 乗算に関する逆元が存在する ($a \neq 0$ のとき $ax = 1$ となる x が存在)

これは，$\mathbb{Z}_p$ が「体」であることを意味している

$\mathbb{Z}_2 = \{0, 1\}$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

加算に関する

- 0 の逆元は 0
- 1 の逆元は 1

乗算に関する

- 1 の逆元は 1

例：$\mathbb{Z}_3$

$\mathbb{Z}_3 = \{0, 1, 2\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

加算に関する
- 0 の逆元は 0
- 1 の逆元は 2
- 2 の逆元は 1

乗算に関する
- 1 の逆元は 1
- 2 の逆元は 2

例：$\mathbb{Z}_5$

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

加算に関する
- 0 の逆元は 0
- 1 の逆元は 4
- 2 の逆元は 3
- 3 の逆元は 2
- 4 の逆元は 1

乗算に関する
- 1 の逆元は 1
- 2 の逆元は 3
- 3 の逆元は 2
- 4 の逆元は 4

例：$\mathbb{Z}_4$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

加算に関する
- 0 の逆元は 0
- 1 の逆元は 3
- 2 の逆元は 2
- 3 の逆元は 1

乗算に関する
- 1 の逆元は 1
- 2 の逆元は ??? ←非存在
- 3 の逆元は 2

今から行うこと

- 有限体の定義
- ここまでの議論のまとめ

体とは？

体とは？

体とは集合 K で，
その上に定義された 2 つの演算 $+, \cdot$ が次を満たすこと
- 任意の $a, b, c \in K$ に対して，$(a + b) + c = a + (b + c)$ (和の結合法則)
- 任意の $a, b \in K$ に対して，$a + b = b + a$ (和の交換法則)
- ある要素 $0 \in K$ が存在して，任意の $a \in K$ に対して，$a + 0 = 0 + a = a$ (和の単位元)
- 任意の $a \in K$ に対して，ある $b \in K$ が存在して，$a + b = b + a = 0$ (和の逆元)

(続く)

体とは？ (続き)

体とは？

体とは集合 K で，
その上に定義された 2 つの演算 $+, \cdot$ が次を満たすこと

(続き)
- 任意の $a, b, c \in K$ に対して，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (積の結合法則)
- 任意の $a, b \in K$ に対して，$a \cdot b = b \cdot a$ (積の交換法則)
- ある要素 $1 \in K$ が存在して，任意の $a \in K$ に対して，$a \cdot 1 = 1 \cdot a = a$ (積の単位元)
- 任意の $a \in K - \{0\}$ に対して，ある $b \in K$ が存在して，$a \cdot b = b \cdot a = 1$ (積の逆元)
- 任意の $a, b, c \in K$ に対して，$a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$ (分配法則)

体 K が有限集合のとき，K を有限体と呼ぶ

体であるもの，体ではないもの

- 実数全体の集合 $\mathbb{R}$ (体である)
- 整数全体の集合 $\mathbb{Z}$ (体ではない)
- 有理数全体の集合 $\mathbb{Q}$ (体である)
- $\mathbb{Z}_2$ (体である)
- $\mathbb{Z}_3$ (体である)
- $\mathbb{Z}_4$ (体でない)
- $\mathbb{Z}_5$ (体である)

有限体の位数

有限体 K

有限体の位数とは？

有限 K の位数とは，K の要素数のこと

例
- $\mathbb{Z}_2$ の位数は 2
- $\mathbb{Z}_3$ の位数は 3

体の標数

体 K

体の標数とは？

K の標数とは，

$$\underbrace{1+1+\cdots+1}_{n\text{ 個}}=0$$

を満たす最小の自然数 n のこと
そのような n が存在しないとき，K の標数は 0 であるとする

例

- $\mathbb{Z}_2$ の標数は 2
- $\mathbb{Z}_3$ の標数は 3
- $\mathbb{R}$ の標数は 0

有限体の位数

有限体 K

有限体の位数とは？

有限 K の位数とは，K の要素数のこと

例

- $\mathbb{Z}_2$ の位数は 2
- $\mathbb{Z}_3$ の位数は 3

今日の内容のまとめ

今日のまとめ

p が素数のとき

- 位数が p で，標数が p の有限体が存在する

疑問

- 素数ではない位数の有限体は存在するか？
- 素数ではない標数の有限体は存在するか？

今後の予告

疑問

- 素数ではない位数の有限体は存在するか？
- 素数ではない標数の有限体は存在するか？

回答

- 位数 n の有限体が存在する $\Leftrightarrow$ n は素数のべき
- 標数 n の有限体が存在する $\Leftrightarrow$ n は素数
  - 位数 p^m の有限体の標数は p (p は素数，m は自然数)

予告

- 位数が素数のべきである有限体の生成法

目次

今日の目標

今日の目標

整数の剰余に関する基礎を身につける

- 剰余とモジュラ算術
- 有限体

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