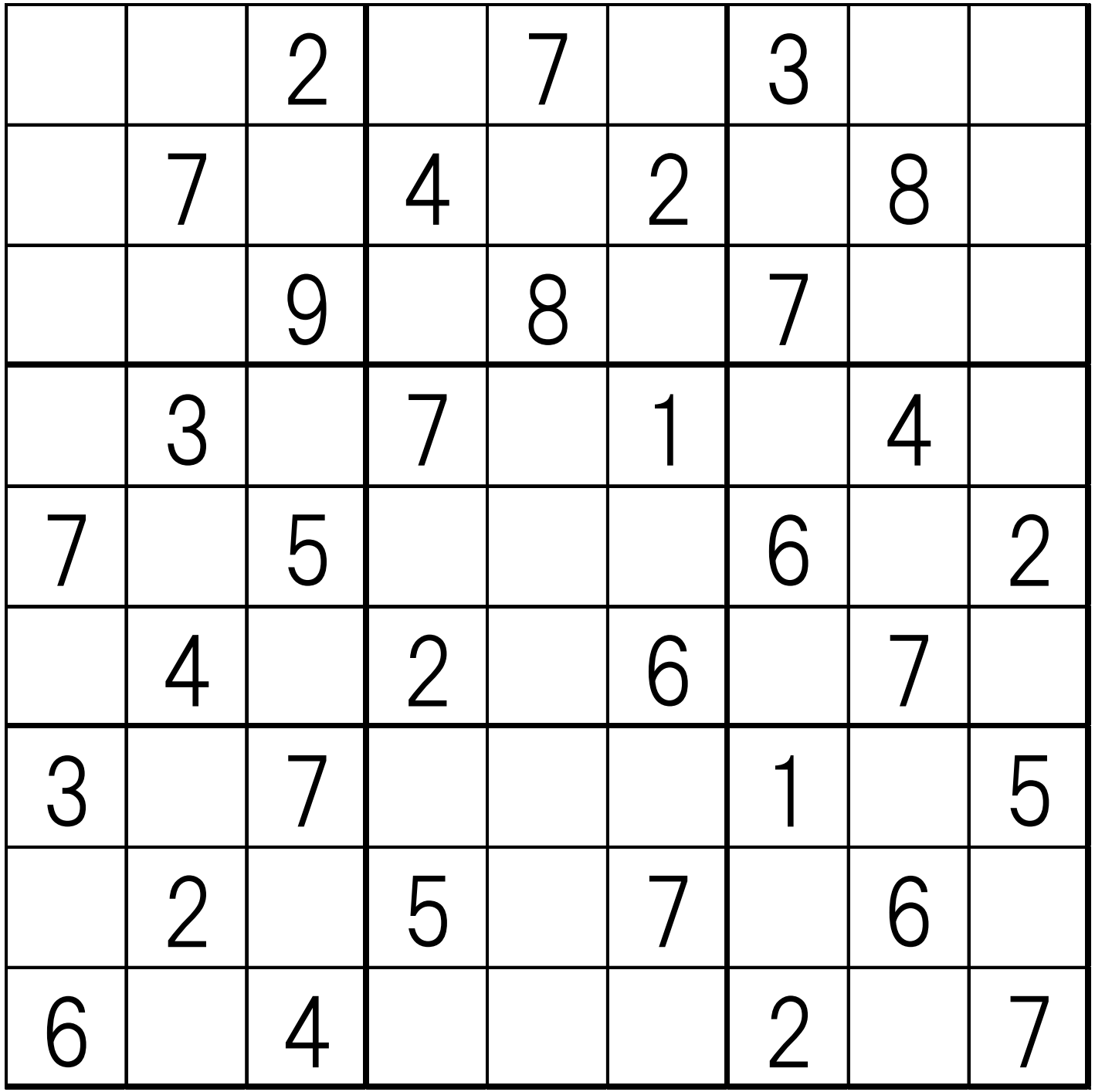
01. 集合，群の復習

代数 II



4	9	2
3	5	7
8	1	6

16	9	7	2
3	6	12	13
10	15	1	8
5	4	14	11

集合とは

- *もの*の集まり
- 集合を構成している*もの*をその集合の*要素*あるいは*元*という

- 数の集合
  自然数，整数，有理数，実数，複素数

→　ハミルトンの4元数

集合の定義

- 外延的定義法

$$S = \{0,1,2,3,4,5,6,7,8,9\}$$

- 内包的定義法

$$S = \{x \mid x\text{は整数で},0 \leq x \leq 9\}$$

集合の演算と法則

- 全集合 Ω をとする集合 A, B すなわち，
  $A, B \subseteq \Omega$ なる集合 A, B に対して，
  これらの2項演算として
  - 和集合（合併集合）
    $$A \cup B = \{x \mid x \in A \text{ または } x \in B\}$$
  - 積集合（共通部分）
    $$A \cap B = \{x \mid x \in A \text{ かつ } x \in B\}$$
  - 対称差集合
    $$A \triangle B = \{x \mid x \in A \cup B \text{ かつ } x \notin A \cap B\}$$

補集合

$$\Omega = \left\{ x \middle| x : \text{整数}, 1 \leq x \leq 10 \right\},$$

$$A = \{1,3,5,8,9\}, B = \{2,4,5,7,8,10\}$$

$$\overline{A} = \{2,4,6,7,10\}$$

$$\overline{B} = \{1,3,6,9\}$$

集合Aの集合Bに関する補集合

$$B - A = \left\{ x \middle| x \in B \text{かつ} x \notin A \right\} = B \cap \overline{A}$$

$$= \{2,4,7,10\}$$

数え上げ

$$|A| + |\overline{A}| = |\Omega|$$

$$|A \cup B| + |A \cap B| = |A| + |B|$$

- あるクラスに学生が40人いるとする．そのうち，国語が好きな学生は23人，数学が好きな学生は15人，国語も数学も好きな学生は7人いたとする．このとき，クラスにいる40人の学生の集合を全集合 Ω，そのうち国語が好きな学生の集合をA，数学が好きな学生の集合をBとする．
  - 国語あるいは数学のいずれかが好きな学生の数を示せ．

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$= 23 + 15 - 7 = 31$$

部分集合

- 集合 $A=\{1,2,3,4,5\}$ に対して
  - ① 空でない部分集合は何個あるか？ 31
  - ② 空でない真部分集合は何個あるか？ 30
  - ③ 要素数が3個の部分集合を全て示せ？

    {1,2,3},{1,2,4},{1,2,5},{1,3,4},{1,3,5},{1,4,5},{2,3,4},{2,3,5},{2,4,5},{3,4,5}

  - ④ 要素数が偶数個の部分集合は何個あるか？ 16
  - ⑤ 要素数が奇数個の部分集合は何個あるか？ 16
  - ⑥ 要素1を含む部分集合は何個あるか？ 16
  - ⑦ 要素1を含む奇数個からなる部分集合は何個あるか？ 8

群

- 空でない集合Gに対して，ある演算＊が定義

（1）閉鎖律

（2）結合律　$(x*y)*z = x*(y*z)$

（3）単位元 e の存在　$e*x = x*e = x$

（4）逆元 x'の存在　$x'*x = x*x' = e$

（5）可換律　$x*y = y*x$

可換群

群表 → ラテン方陣

- 群表においては，表の各行と各列にその群のすべての元が漏れなく重複無く丁度1回づつ現れる.

$$S = \{e, a, b, c, d\}$$

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

同型

- 演算の記号の違いを除けば完全に等しい構造を持つとき，同型

$$G \cong G'$$

- 位数1,2,3の群は同型を除くと次の場合のみ

$n=1$

	e
e	e

$n=2$

	e	a
e	e	a
a	a	e

$n=3$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

クラインの4元数

- どの元もその元自身を逆元とし，異なる二つの積は残りの元となる.

$$a^2 = b^2 = c^2 = e$$

$$ab = c,\ bc = a,\ \ ca = b$$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

次回：中間試験

合同式

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

$\Leftrightarrow a-b$がmの倍数である$\Leftrightarrow m \mid a-b$

$\Leftrightarrow a$をmで割った余り$=b$をmで割った余り

$\Leftrightarrow a$とbは法mで合同である

合同式の法則

nを1より大きい整数とする．このとき，任意の整数a,b,c,dについて，次のことが成り立つ

(1)反射律　$a \equiv a \pmod{m}$

(2)対称律　$a \equiv b \pmod{m}$ならば，$b \equiv a \pmod{m}$

(3)推移律　$a \equiv b \pmod{m}$かつ　$b \equiv c \pmod{m}$ならば　$a \equiv c \pmod{m}$

(4)　$a \equiv b \pmod{m}$かつ　$c \equiv d \pmod{m}$ならば

$a \pm c \equiv b \pm d \pmod{m}$,　$a \cdot c \equiv b \cdot d \pmod{m}$

剰余類の定義と定理

aを任意の整数とするとき，

$C_a = \{x \in Z \,|\, x \equiv a \pmod{n}\} = a + nZ = \{a + nt \,|\, t \in Z\}$を

nを法とするaの剰余類という．

また，nを法とする剰余類の集合をZ_nで表す．

すなわち，$Z_n = \{C_a \,|\, a \in Z\}$

nを1より大きい整数，a, bを任意の整数とするとき，

$$a \equiv b \pmod{n} \Leftrightarrow C_a = C_b$$

剰余類の性質

C_aをnを法とするaの剰余類を表すものとする.

このとき，次のことが成り立つ.

(1)$a = C_a$

(2)$C_a \cap C_b \neq \phi \Leftrightarrow C_a = C_b$

(3)Z_nは相異なるn個の元$C_0, C_1, \cdots, C_{n-1}$から構成される.

$Z_n = \{C_0, C_1, \cdots, C_{n-1}\}, C_i \cap C_j = \phi (i \neq j)$

また，このとき$Z = C_0 \cup C_1 \cup \cdots \cup C_{n-1}$となっている

既約剰余類

nを法とするaの剰余類C_aは$(a,n)=1$であるとき，既約剰余類であるという．nを法とする剰余類の集合Z_nにおいて，既約剰余類の集合を$Z_n^{\times}$と表す

剰余類Z_nから0を除外した集合をZ_n^*と表す$(P.70)$

例題

以下の集合に対して，加法と乗法について群となるか考えよう.

- 法7の剰余類
- 法7の既約剰余類