

2017年度 前期定期試験 (問題兼解答用紙)

開講学部	評点
理工学部	

問題枚数	両面印刷	別紙解答用紙	試験時間	試験科目名	クラス	出題者
2/1	有	なし	80分	代数学 I <small>木曜 2, 1 時限, 教科書: Original</small>	A, B	大西良博
持込許可物件	所属学部	所属学科	学年	学籍番号 (9桁)	氏名	
なし	理工学部	数学科	年			

注意 1. 最終的な答に至る途中の説明をできるだけ詳しく書くこと。最終結果だけでは得点できない。  
 注意 3. 試験場の静粛を保つために、退場は開始 60 分後の時点の一回限りとする。

注意 2. 学生証、記名用のペン、鉛筆またはシャープペンシル、消しゴム以外は机の上に置かないこと。  
 注意 4. **2a**, **2b**, **6a**, **6b**, **10a**, **10b** は選択問題である。どちらか 1 問選んで解答せよ。

**1** (10点)  $G$  を群,  $H < G$ ,  $c \in G$  とする。このとき  $c^{-1}Hc < G$  を示せ。

**3** (10点) 23201 は素数である。法 23201 の原始根はいくつあるか。

**2a** (10点)  $i$  を虚数単位として  $\omega = \frac{-1+\sqrt{3}i}{2}$  ( $1$  の 3 乗根の 1 つ) とする。このとき 9 つの 2 次正方行列からなる集合

$$\left\{ \begin{bmatrix} \omega^a & 0 \\ 0 & \omega^b \end{bmatrix} \mid a = 0, 1, 2; b = 0, 1, 2 \right\}$$

は、行列の積を演算として巡回群でない有限 Abel 群となることを示せ。

**2b** (10点)  $\begin{bmatrix} -1 & -1 & 0 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{bmatrix}$  の行列の積に関する位数を求めよ。

**4** (15点) 位数 61 の元  $a$  から生成される巡回群  $G$  がある。このとき、 $a^{13}$  は  $G$  の生成元であるか。もし、そうならば  $(a^{13})^m = a$  となる整数  $m$  が存在する筈である。そのような  $m$  で  $0 \leq m < 61$  なるものを求めよ。

**5** (10点) 位数が素数の群は巡回群であることを示せ。(Hint: Lagrange の定理)

**6a** (10点)  $d = \gcd(m, n)$  とする. 連立方程式  $x \equiv a \pmod{m}, x \equiv b \pmod{n}$  が解を持つためには,  $a \equiv b \pmod{d}$  であることが必要十分であることを示せ.

**6b** (10点) 素数  $p$  に対し,  $\mathbb{Z}/p\mathbb{Z}$  の元を成分とする行列の集合

$$\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}/p\mathbb{Z}, ad - bc \neq \bar{0} \right\}$$

は, 通常の行列の積を  $\mathbb{Z}/p\mathbb{Z}$  演算として群をなす.  $\mathrm{GL}(2, \mathbb{Z}/7\mathbb{Z})$  ( $p=7$ ) において,

$\begin{bmatrix} \bar{1} & \bar{2} \\ \bar{1} & \bar{6} \end{bmatrix}$  の逆元を求め, 単一の行列として記せ.

**8** (10点) 2 と 3 は法 23 の原始根ではない. 法 23 の原始根をすべて求めよ.

**9** (10点)  $S_4$  の部分群  $V = \{\varepsilon, (12)(34), (13)(24), (14)(23)\}$  (Klein の 4 元群) に関する左剰余類分解  $S_4/V$  を要素を並べて書き下せ.

**7** (10点)  $\mathbb{R}[x]$  においては

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

なる因数分解ができる (これ以上分解できない).

これを参考にして  $(\mathbb{Z}/11\mathbb{Z})[x]$  において,  $f(x) = x^4 + \bar{1}$  を因数分解せよ.

(Hint:  $x^4 + 1 = (x^4 - 2x^2 + 1) + 2x^2$ )

**10a** (5点)  $n$  は自然数で,  $p = 2^n + 1$  は素数であるとせよ. (その様な  $p$  は Fermat 素数と呼ばれる.)

(1)  $n$  は 2 の冪でなければならないことを示せ. (Hint: 法  $p$  での 2 の位数を調べよ.) (2)  $p > 5$  ならば 2 は法  $p$  の原始根ではないことを示せ.

**10b** (5点)  $2185 - 1045i$  を  $\mathbb{Z}[i]$  内で素元分解 (Gauss 素数の積に分解) せよ.

### 既習事項のまとめ

- (1)  $\mathbb{N}$  は自然数全体,  $\mathbb{Z}$  は整数全体のなす環,  $\mathbb{Q}$  は有理数全体のなす体,  $\mathbb{R}$  は実数全体のなす体,  $\mathbb{C}$  は複素数全体のなす体.
- (2)  $a, b, \dots, c \in \mathbb{Z}$  に対して,
 
$$\{ax + by + \dots + cz \mid x, y, \dots, z \in \mathbb{Z}\} = d\mathbb{Z}$$
 となる  $d \in \mathbb{Z}$  ( $d \geq 0$ ) が唯一つ存在する. このとき  $d = \gcd(a, b, \dots, c)$  である.
- (3) 1 つの演算  $(a, b) \mapsto ab$  が定義された集合  $G$  が群であるとは, 次の **G1**, **G2**, **G3** の 3 つが成り立つときをいう: (ただし  $a, b, c$  は  $G$  の任意の元を表す.)
  - G1** 結合法則:  $(ab)c = a(bc)$ .
  - G2** 単位元の存在: ある元  $1 \in G$  が存在して任意の  $a \in G$  について  $1a = a1 = a$  が成り立つ.  $1$  は 単位元 と呼ばれる.
  - G3** 逆元の存在: 任意の元  $a \in G$  に対し,  $ax = xa = 1$  を満たす元  $x \in G$  が存在する. その様な  $x$  を  $a$  の 逆元 と呼ぶ. 一般的な状況では, その様な  $x$  を  $a^{-1}$  と記すことがある.
- さらに
  - G4** 交換法則:  $ab = ba$   
が満たされているとき,  $G$  は Abel 群 または 可換群 と呼ばれる.
- (4) 部分群とは群の部分集合であって, その群の演算について, それ自体で群になっているものである.
- (5) 群  $G$  といくつかの元の部分集合  $\{a, b, \dots, c\} \subset G$  について, これらの元の逆元をとること, あるいは, それらの間のできる限りの演算をほどこすことよって得られる (生成される) 元を集め, さらに, そうして得られた (生成された) あらゆる元に対して同様のことを行う. これを何度も繰り返して得られた (生成された) 元を全て集めてできる群を,  $\{a, b, \dots, c\}$  で生成される (部分) 群と呼ぶ.
- (6) 巡回群とは 1 つの元  $a$  で生成される群のことである. それを  $\langle a \rangle$  と記す.
- (7)  $G$  を  $x$  で生成された位数  $m$  の巡回群とする.  $G$  の任意の部分群  $H$  はまた巡回群であり,  $d \mid m$  なる  $d$  が存在して,  $x^d$  が  $H$  を生成する.
- (8) 加法と呼ばれる演算  $(a, b) \rightarrow a + b$  と乗法と呼ばれる演算  $(a, b) \rightarrow ab$  の定義された集合  $R$  が 可換環 であるとは,  $R$  が次の 5 つの条件を満たすことである: (ただし  $a, b, c$  は  $R$  の任意の元を表す)
  - R1**  $R$  は加法に関して可換群である. (単位元は通常  $0$  で表す)
  - R2** 乗法の結合法則:  $(ab)c = a(bc)$ .
  - R3** 左右の分配法則:  $a(b+c) = ab+ac, (b+c)a = ba+ca$ .
  - R4** 単位元の存在: 加法の単位元  $0$  とは異なるある元  $1 \in R$  が存在して,  $R$  の任意の元  $x$  に対して  $1x = x1 = x$  が満たされる.
  - R5** 乗法の交換法則:  $ab = ba$
- (9) 一般に可換環  $R$  と元  $\alpha$  について  $R[\alpha]$  は  $\alpha$  の  $R$  を係数とする多項式の全体のなす可換環を表す. 例えば  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ ,  $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ .
- (10) 可換環  $R$  の部分集合  $M \subset R$  は
  - I1**  $a \in M, b \in M$  ならば  $a + b \in M$ ,
  - I2**  $a \in M, x \in R$  ならば  $xa \in M$
 が成り立つとき,  $R$  の ideal と呼ばれる.
  - (11)  $R$  を可換環,  $q \in R$  とする. 任意の  $a, b \in R$  に対し 「 $p|ab \implies p|a$  または  $p|b$ 」 が成り立つとき,  $q$  は  $R$  の素元であるといわれる.
  - (12) (Euclid の) 互除法 を使うと  $\gcd(a, b) = d$  のときに  $ax + by = d$  となる  $x, y \in \mathbb{Z}$  を見付けることができる.
  - (13) 群  $G$  と  $H < G$  に対し,  $G$  を  $xH$  の形の部分集合に分解したものを  $G$  の左剰余類分解といひ,  $G/H$  と表す.
  - (14) (Lagrange の定理) 有限群  $G$  と部分群  $H < G$  について  $|H|$  は  $|G|$  の約数である.
  - (15) 有限群  $G$  が巡回群であるためには, 任意の  $m \in \mathbb{N}$  について,  $\#\{x \in G \mid x^m = 1\} \leq m$  であることが必要十分.
  - (16)  $\mathbb{Z}/m\mathbb{Z}$  は法  $m$  による剰余類 ( $k \bmod m$ ) ( $= \bar{k}$  と略記する) 達のなす可換環.  
例えば  $\mathbb{Z}/5\mathbb{Z} = \{(0 \bmod 5), (1 \bmod 5), (2 \bmod 5), (3 \bmod 5), (4 \bmod 5)\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ .
  - (17)  $\varphi(n) = “(\mathbb{Z}/n\mathbb{Z})^\times$  の要素の個数”  $= “1, \dots, n-1$  の中で  $n$  と互いに素なもの個数”.
  - (18)  $(\mathbb{Z}/m\mathbb{Z})^\times = \{(j \bmod m) \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(j, m) = 1\}$ . これは積に関して位数  $\varphi(m)$  の Abel 群になる. この群は, 法  $m$  に関する 既約剰余類群 と呼ばれる.
  - (19)  $p$  を素数とする.  $(\mathbb{Z}/p\mathbb{Z})^\times$  は位数  $p-1$  の巡回群である. その生成元を法  $p$  の 原始根 と呼ぶ.
  - (20) Gauss 整数環  $\mathbb{Z}[i]$  の元  $a + bi$  ( $a, b \in \mathbb{Z}$ ) について  $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$  と書き,  $a + bi$  の norm と呼ぶ.
  - (21)  $\mathbb{Z}[i]$  において, 1 の約数は  $1, -1, i, -i$  の 4 つに限る.  $\alpha \in \mathbb{Z}[i]$  にこれら 4 つの元のそれぞれを掛けて得られる数は,  $\alpha$  と同値であるといわれる.
  - (22)  $\mathbb{Z}[i]$  の素元を Gauss 素数 と呼ぶ.
  - (23) 素数  $p \in \mathbb{Z}$  は Gauss 素数であるか, または, Gauss 素数の norm である.  $2 = N(1 + i)$  は Gauss 素数の norm であり,  $p \equiv 1 \pmod{4}$  なる素数  $p$  は Gauss 素数の norm であり,  $p \equiv 3 \pmod{4}$  なる素数  $p$  は Gauss 素数でない.