

2015 年度 前期 中間試験 (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
1/1	有	なし	80 分	代 数 学 I <small>月曜 2 時限, 教科書 : Original</small>	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 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 3. 試験場の静粛を保つために, 退出は開始 60 分後の時点の一回限りとする。  
 注意 4. **8** は選択問題である。 **8a** と **8b** から 1 問選んで解答せよ。

**1** (15 点)  $\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$  が行列の積に関して生成する巡回群の位数を求めよ。

**3** (10 点) Euler 関数  $\varphi$  について,  $\varphi(2 \cdot 13^2 \cdot 31)$  を求めよ。

**4** (10 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,  $a^{29}$  は  $G$  の生成元であるか。もし, そうならば  $(a^{29})^m = a$  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。

**2** (10 点) 位数 35 の元  $a$  を生成元とする巡回群  $\langle a \rangle$  の生成元を全て書き上げよ。

**5** (15 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。

**6** (15 点)  $M = \{2x + (1 + \sqrt{-5})y \mid x, y \in \mathbb{Z}\}$  とおく.  
 $M = \{2\xi + (1 + \sqrt{-5})\eta \mid \xi, \eta \in \mathbb{Z}[\sqrt{-5}]\}$  を証明せよ. さ  
らに,  $M$  が  $\mathbb{Z}[\sqrt{-5}]$  の ideal であることを示せ.

**7** (10 点)  $(\mathbb{Z}/7\mathbb{Z})[x]$  において,  $f(x) = x^3 + \bar{6}x^2 + \bar{3}x + \bar{4}$  の  
とき,  $f(x) = \bar{0}$  の根をすべて見つけ,  $f(x)$  を因数分解せよ.

**8a** (15 点)  $p$  が素数のとき  $(p-1)! \equiv -1 \pmod{p}$  であることを証明せよ.

**8b** (15 点)  $p$  は奇素数であつて,  $a^{2^n} + 1$  の約数であるとせよ. このとき  $p \equiv 1 \pmod{2^{n+1}}$  であることを示せ.

## 既習事項のまとめ

- (1)  $\mathbb{N}$  は自然数全体,  
 (2)  $\mathbb{Z}$  は整数全体のなす環,  
 (3)  $\mathbb{Q}$  は有理数全体のなす体.  
 (4)  $\mathbb{R}$  は実数全体のなす体.  
 (5)  $\mathbb{C}$  は複素数全体のなす体.  
 (6) 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  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ ,  $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ,  
 (7)  $a, b, \dots, c \in \mathbb{Z}$  に対して,  

$$\{ax + by + \dots + cz \mid x, y, \dots, z \in \mathbb{Z}\} = d\mathbb{Z}$$
 となる  $d \in \mathbb{Z}$  ( $d \geq 0$ ) が唯一存在する. このとき  $d = \text{gcd}(a, b, \dots, c)$  である.  
 (8) 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.  
 (9) 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ことである.  
 (10) 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によって得られる (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.  
 (11) 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.  
 (12)  $G$  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.  
 (13) 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<sup>1</sup>:  $a(b + c) = ab + ac$ ,  $(b + c)a = ba + ca$ .  
**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:  $ab = ba$   
 (14) 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.  
 (15) (Euclid の) 互除法 を使うと  $\text{gcd}(a, b) = d$  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.  
 (16) (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.  
 (17) 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.  
 (18)  $\mathbb{Z}/m\mathbb{Z}$  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  $\mathbb{Z}/5\mathbb{Z} = \{(0 \bmod 5), (1 \bmod 5), (2 \bmod 5), (3 \bmod 5), (4 \bmod 5)\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ .  
 (19)  $(\mathbb{Z}/m\mathbb{Z})^\times = \{(j \bmod m) \in \mathbb{Z}/m\mathbb{Z} \mid \text{gcd}(j, m) = 1\}$ . これは積に関して群をなす. 法  $m$  に関する 既約剰余類群 と呼ばれる.  
 (20)  $\varphi(n) = “(\mathbb{Z}/n\mathbb{Z})^\times$  の要素の個数” = “ $1, \dots, n-1$  の中で  $n$  と互いに素なものの個数”.  
 ただし  $\varphi(1) = 1$ .