実施：2016 年 7 月 28 日 (木) 10:50-12:20, H-302 室

2016 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　木曜 2, 1 時限, 教科書：Original | 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** 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. **2a** **2b**, **6a** **6b**, **9a** **9b** は選択問題である. どちらか 1 問選んで解答せよ.

**1** (15 点)　$G$ を群, $H < G$, $c \in G$ とする. このとき $c^{-1}Hc < G$ を示せ.

**2a** (15 点)　$S_6$ の部分群

$$\{\, \varepsilon,\ (123),\ (132),\ (456),\ (123)(456),\ (132)(456),\ (465),\ (123)(465),\ (132)(465) \,\}$$

は巡回群でない有限 Abel 群であることを説明せよ.

**2b** (15 点)　$\begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ -1 & 0 & 1 \end{bmatrix}$ の行列の積に関しての位数を求めよ.

**3** (10 点)　位数 $81675\,(=3^3\cdot 5^2\cdot 11^2)$ の巡回群の生成元はいくつあるか.

**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, $a^{11}$ は $G$ の生成元であるか. もし, そうならば $(a^{11})^m = a$ となる整数 $m$ が存在する筈である. その様な $m$ で $0 \leqq m < 61$ 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** (15 点) $d = \gcd(m, n)$ とする. 連立方程式 $x \equiv a \bmod m$, $x \equiv b \bmod n$ が解を持つためには, $a \equiv b \bmod d$ であることが必要十分であることを示せ.

**6b** (15 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

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

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

$\begin{bmatrix} \overline{1} & \overline{2} \\ \overline{1} & \overline{6} \end{bmatrix}$ の逆元を求めよ.

**7** (10 点) 法 19 の原始根をすべて求めよ.

**8** (5 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 $(\mathbb{Z}/\underline{\underline{7}}\mathbb{Z})[x]$ において, $f(x) = x^4 + 1$ を因数分解せよ.

**9a** (5 点) 整数 $n$ が $n = a^2 + b^2$ $(a, b \in \mathbb{Z},\ \gcd(a, b) = 1)$ と書けるとき, $p|n$ なる奇素数 $p$ は Gauss 素数でない（つまり Gauss 素数の norm である）ことを示せ.

**9b** (5 点) $665 + 770i$ を $\mathbb{Z}[i]$ 内で素元分解（Gauss 素数の積に分解）せよ.

ここより下に記入しないで下さい.

**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) $a$, $b$, $\cdots$, $c \in \mathbb{Z}$ に対して，
$$\{ax + by + \cdots + cz \,|\, x, y, \cdots, z \in \mathbb{Z}\} = d\mathbb{Z}$$
となる $d \in \mathbb{Z}$ $(d \geqq 0)$ が唯 1 つ存在する．このとき $d = \gcd(a, b, \cdots, c)$ 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のことである．

( 5) 群 $G$ といくつかの元の部分集合 $\{a, b, \cdots, c\} \subset G$ 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，$\{a, b, \cdots, c\}$ 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，$d|m$ 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 $(a, b) \to a + b$ と乗法と呼ばれる演算 $(a, b) \to ab$ 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 $\mathbb{Z}[i] = \{\, a + bi \,|\, a,\ b \in \mathbb{Z} \,\}$, $\mathbb{Z}[\sqrt{5}\,] = \{\, a + b\sqrt{5} \,|\, a, b \in \mathbb{Z} \,\}$,

( 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) (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．

( 14) 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，$\sharp\{\, x \in G \,|\, x^m = 1 \,\} \leqq m$ であることが必要十分．

( 15) $\mathbb{Z}/m\mathbb{Z}$ は法 $m$ による剰余類 $(k \mod m)$ $(= \overline{k}$ と略記する$)$ 達のなす可換環．
例えば $\mathbb{Z}/5\mathbb{Z} = \{(0 \mod 5), (1 \mod 5), (2 \mod 5), (3 \mod 5), (4 \mod 5)\,\} = \{\,\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\,\}$.

( 16) $\varphi(n) =$ “$(\mathbb{Z}/n\mathbb{Z})^\times$ の要素の個数” = “$1, \cdots, n-1$ の中で $n$ と互いに素なものの個数”．
ただし $\varphi(1) = 1$.

( 17) $(\mathbb{Z}/m\mathbb{Z})^\times = \{(j \bmod m) \in \mathbb{Z}/m\mathbb{Z} \,|\, \gcd(j, g) = 1\}$．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．

( 18) $p$ を素数とする．$(\mathbb{Z}/m\mathbb{Z})^\times$ は巡回群である．その生成元を法 $p$ の 原始根 と呼ぶ．

( 19) 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．

( 20) $\mathbb{Z}[i]$ 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 同伴 であるいわれる．

( 21) $\mathbb{Z}[i]$ の素元を Gauss 素数 と呼ぶ．

( 22) 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，$p \equiv 1 \bmod 4$ なる素数 $p$ は Gauss 素数の norm であり，$p \equiv 3 \bmod 4$ なる素数 $p$ は Gauss 素数である．