実施：2018 年 7 月 23 日 (月) 11:50-12:20, 11-204 室

B4 で印刷

2018 年度　**前 期　定 期 試 験**　(問題 兼 解答用紙)

開講学部	評点小計
理工学部	

評　点

問題枚数	両面印刷	別紙解答用紙	試験時間	試 験 科 目 名	出 題 者
2/1	有	なし	80 分	代 数 学 I　月曜 2 時限, 教科書：Original	大 西 良 博

持込許可物件	所属学部	所属学科	学年	クラス	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, 途中退出は開始 60 分後の時点の一回限りとする.

注意 4. **1a**, **1b** および **9a**, **6b** は選択問題である. それぞれ 1 問を選んで解答せよ.

1a (10 点)　G を群, $H < G$ とする. また任意に $g \in G$ をとり, 固定する. このとき G の部分集合 $g^{-1}Hg$ は G の部分群であることを示せ.

1b (10 点)　群 G のどの要素 a も $a^2 = 1$ を満たすとせよ. このとき G は Abel 群であることを証明せよ.

2 (10 点)　次の 2 つの問に答へよ.

(1) S_4 の S_4 自身とは異る部分群で, 巡回群でない有限 Abel 群の例を挙げよ. なぜ, 巡回群でないとわかるのかも述べること.

(2) S_4 の位数 3 の部分群をすべて挙げよ.

3 (10 点)　位数 $1107 = 41 \times 3^3$ の元 a から生成される巡回群 G がある. このとき, a^5 は G の生成元であるか. もし, さうならば $(a^5)^m = a$ となる整数 m が存在する筈である. その様な m（但し $0 \leqq m < 1107$）を求めよ.

4 (10 点)　多項式　$f(x) = x^4 + \overline{4}x^3 + \overline{4}x^2 + \overline{2}x + \overline{4} \in (\mathbb{Z}/5\mathbb{Z})[x]$　と $g(x) = \overline{2}x^2 + \overline{3}x + \overline{1}$　に対して　$f(x) = g(x)\,q(x) + r(x)$,　$\deg r(x) < \deg g(x)$ となる多項式　$q(x), r(x) \in (\mathbb{Z}/5\mathbb{Z})[x]$　を求めよ. 但し deg は多項式の次数を示す.

学籍番号

5 (10 点) (1) $\mathbb{Z}/1107\mathbb{Z}$ において $\overline{5}$ の乗法に関する逆元を求めよ. 答は $0 < n < 1107$ なる整数 n によつて $\overline{n}$ の形で与へよ.
(2) Euler 函数の値 $\varphi(1107)$ を求めよ.
(3) 5^{723} および 5^{719} を 1107 で割つた余りを求めよ.
(Hint : Euler の定理と (1).)

6 (10 点) S_4 の部分群 $H = \langle (1\ 2\ 3\ 4) \rangle$ に関する左剰余類分解 S_4/H を要素を列記して記せ.

7 (14 点) 正の有理数の全体 $(\mathbb{Q}^\times)_+$ は乗法に関して群をなす. これは巡回群でないことを示せ.
(Hint : 巡回群であるとして, その生成元 を $\frac{a}{b}$ (但し $\gcd(a,b) = 1$) とおく. $p \nmid a$, $p \nmid b$ なる素数 p を考へて矛盾を導け.)

8 (14 点) $\overline{6} = (6 \mod 41)$ は $(\mathbb{Z}/41\mathbb{Z})^\times$ の原始根である.
(1) 6^{20} を 41 で割つた余りを求めよ. (Hint : $20 = (41-1) \div 2$)
(2) $(\mathbb{Z}/41\mathbb{Z})^\times$ の原始根はいくつあるか.

9a (13 点) $-726 + 1232i$ を Gauss 整数環において素元分解 (Gauss 素数の積に分解) せよ.

9b (13 点) 等式 $(17+8i)\,\xi + (7+8i)\,\eta = 1$ を満たす $\xi, \eta \in \mathbb{Z}[i]$ を 1 組求めよ. (Hint : Gauss 整数環において “互除法” を行ふ.)

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 がある $a \in G$ について $G = \{\, a^m \,|\, m \in \mathbb{Z} \,\}$ と表されるとき G を a によつて 生成 された 巡回群 と呼ぶ．この状況を $G = \langle a \rangle$ と記し，a を G の 生成元 と呼ぶ.

(6) 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.

(7) 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：$ab = ba$

(8) 可換環 R の 0 以外のどの元も乗法に関する逆元を持つとき，R は 体 であるといはれる.

(9) この科目で登場した可換環には，$\mathbb{Z}[i] = \{\, a+bi \,|\, a,\ b \in \mathbb{Z} \,\}$，$\mathbb{Z}[\sqrt{2}\,] = \{\, a+b\sqrt{2} \,|\, a, b \in \mathbb{Z} \,\}$，$\mathbb{Z}[\sqrt{-5}\,] = \{\, a+b\sqrt{-5} \,|\, a,\ b \in \mathbb{Z} \,\}$ や下の (17) に記す $\mathbb{Z}/m\mathbb{Z}$ などがある.

(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) (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.

(12) Euler の φ 函数．$1, \cdots, n$ の中で n と互ひに素なものの個数を $\varphi(n)$ で表す．$\varphi(1) = 1$.
$\gcd(m, n) = 1$ なら $\varphi(mn) = \varphi(m)\varphi(n)$．素数の冪 p^n については $\varphi(p^n) = p^n - p^{n-1}$.

(13) Euler の定理．$n \in \mathbb{Z}, \neq 0$ と $\gcd(a, n) = 1$ なる $a \in \mathbb{Z}$ について $a^{\varphi(n)} \equiv 1 \bmod n$.
Fermat の定理．特に，素数 p と $p \not| a$ なる $a \in \mathbb{Z}$ について $a^{p-1} \equiv 1 \bmod p$.

(14) 群 G と $H < G$ に対して $\{x_i \,|\, i \in \Lambda\}$ が存在して $G = \bigsqcup_{i \in \Lambda} x_i H$ となる．これを G の H による 左剰余類分解 と称する.

(15) 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.

(16) 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.

(17) $\mathbb{Z}/m\mathbb{Z}$ 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 $\mathbb{Z}/5\mathbb{Z} = \{(0 \bmod 5), (1 \bmod 5), (2 \bmod 5), (3 \bmod 5), (4 \bmod 5)\,\} = \{\, \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4} \,\}$.

(18) $\varphi(n)$ = “$(\mathbb{Z}/n\mathbb{Z})^\times$ 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 $\varphi(1) = 1$.

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

(20) 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.

(21) 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.

(22) $\mathbb{Z}[i]$ 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，α と 同伴 であるいわれる.

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

(24) $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$ に対し $\alpha = q\beta + r$, $N(r) < \frac{1}{2}N(\beta)$ を満たす q, $r \in \mathbb{Z}[i]$ が存在する.

(25) 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.