実施： 2017 年 6 月 27 日 (火) 9:10-10:40, H-201 室

2017 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
2/1	有	なし	80 分	代 数 学 I　火曜 1 時限, 教科書： Original	A	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** **2c**, **5a** **5b** は選択問題である. それぞれ 1 問を選んで解答せよ.

1 (10 点)　G を群, $H<G$, $g\in G$ とする. このとき $g^{-1}Hg<G$ を示せ.

2a (10 点)　S_6 の部分群

$H=\{\varepsilon,\ (1\,2),\ (3\,4),\ (5\,6),\ (1\,2)(3\,4),\ (3\,4)(5\,6),\ (1\,2)(5\,6),\ (1\,2)(3\,4)(5\,6)\}$

は巡回群でない有限 Abel 群である. なぜ巡回群でないとわかるのか, 述べよ.

2b (10 点)　複素数を成分とする行列 $\begin{bmatrix} 0 & i \\ -i & i \end{bmatrix}$ $(i^2=-1)$ が行列の積に関して生成する巡回群の位数を求めよ.

2c (10 点)　0 以外の有理数全体が乗法によってなす群 $\mathbb{Q}^\times$ は巡回群でないことを示せ.

3 (10 点)　位数 $81675\,(=3^3\cdot5^2\cdot11^2)$ の巡回群の生成元はいくつあるか.

4 (10 点)　位数 73 の元 a から生成される巡回群 G がある. このとき, a^{17} は G の生成元であるか. もし, そうならば $(a^{17})^m=a$ となる整数 m が存在する筈である. その様な m で $0\leqq m<73$ なるものを求めよ.

5a (10 点)　法 13 の原始根を すべて 求めよ.

また, 方程式 $x^4\equiv 3 \mod 13$ の $\mod 13$ での解をすべて求めよ.

5b (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

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

は群である. 但し演算は通常の行列の積を $\mathbb{Z}/p\mathbb{Z}$ である.

このとき, $\mathrm{GL}(2,\mathbb{Z}/7\mathbb{Z})$ ($p=7$) において, $\begin{bmatrix} \overline{3} & \overline{6} \\ \overline{1} & \overline{5} \end{bmatrix}$ の逆元を求めよ.

6 (10 点) 法 19 のすべての原始根を求めよ.

7 (10 点) $(\mathbb{Z}/7\mathbb{Z})[x]$ において, $f(x) = x^3 + \overline{2}x + \overline{5}$ を因数分解せよ.

8 (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)

9 (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.

10 (10 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) $p > 5$ ならば 2 は法 p の原始根ではないことを示せ.

(2) $p > 3$ ならば 3 は法 p の原始根であることを証明せよ.

Hint : 法 p で -1 が平方元であることを示せ. もし, 3 が原始根でないのなら平方元であることを示せ. それゆえ, $-3 \equiv a^2 \bmod p$ なる a が存在する. このとき $2u \equiv -1 + a \bmod p$ で定まる u は位数が 3 であることを示せ. これと Fermat の小定理から $3|p-1$ を示し, 矛盾を導け.

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 α について $R[\alpha]$ は α 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) （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) （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.

(13) 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.

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

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

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

(17) 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.