実施：2018 年 7 月 9 日 (水) 11:50-12:20, 11-204 室

B4 で印刷

2018 年度　**前 期　中 間 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 **6a**, **6b**, **6c** 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．

1a の略解

G0　任意の $g^{-1}xg,\ g^{-1}yg \in g^{-1}Hg\ (x,\ y \in H)$ について

$$(g^{-1}xg)(g^{-1}yg) = g^{-1}xyg \in g^{-1}Hg$$

である．

G1　G についての **G0** により正しい．

G2　$1 = g^{-1}1g \in g^{-1}Hg$ であるから G についての **G1** により正しい．

G3　任意の $g^{-1}xg \in g^{-1}Hg\ (x \in H)$ について $g^{-1}x^{-1}g \in g^{-1}Hg$ は $g^{-1}xg$ の逆元である．実際

$$(g^{-1}x^{-1}g)(g^{-1}xg) = g^{-1}x^{-1}xg = g^{-1}g = 1.$$

同様に $(g^{-1}xg)(g^{-1}x^{-1}g) = 1$ がわかる．

1b　任意の $x \in G$ について $x^2 = 1$ より $x^{-1} = x$．ゆゑに，任意の $a,\ b \in G$ について $a^{-1} = a,\ b^{-1} = b$ であり，一般に $(xy)^{-1} = y^{-1}x^{-1}$ ゆゑ

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

2 (10 点)　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．

略解　$V = \{\varepsilon,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}$ は位数 4 の部分群であるが，これらの元の位数は 1 または 2 であり，位数 4 の元が存在しない．よつて巡回群ではない．

3 (15 点)　S_3 の部分群をすべて挙げよ．「すべて」である理由も述べること．

略解　$S_3 = \{\varepsilon,\ (1\,2),\ (1\,3),\ (2\,3),\ (1\,2\,3),\ (1\,3\,2)\}$ の各元の位数（ord）は

順に 1, 2, 2, 2, 3, 3 である．

Lagrange の定理により，部分群の位数は $|S_3| = 3! = 6$ の約数．

位数 1 の部分群は $\{\varepsilon\}$ に他ならない．

次に，位数が 2 の（部分）群は，位数が 2 の巡回群に他ならないので，

$$\{\varepsilon,\ (1\,2)\},\ \{\varepsilon,\ (1\,3)\},\ \{\varepsilon,\ (2\,3)\}$$

の 3 つしかない．

位数 3 の部分群は（3 は素数だから）位数 3 の部分群しかない．それは

$$\{\varepsilon,\ (1\,2\,3),\ (1\,3\,2)\}.$$

に他ならない．

位数 6 の部分群はもちろん S_3 である．

答は

$$\{\varepsilon\},\ \{\varepsilon,\ (1\,2)\},\ \{\varepsilon,\ (1\,3)\},\ \{\varepsilon,\ (2\,3)\},\ \{\varepsilon,\ (1\,2\,3),\ (1\,3\,2)\},\ S_3$$

の 6 個．

4 (10 点)　位数 24 の巡回群 $\langle a \rangle$ の生成元を $a^k\ (0 < k < 24)$ の形で列記せよ．

略解　$a,\ a^5,\ a^7,\ a^{11},\ a^{13},\ a^{17},\ a^{19},\ a^{23}$ の 8 個である．

5 (10 点)　位数 2727 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 $0 \leqq m < 2727$）を求めよ．

略解　互除法により

$$5 \times 1091 - 2727 \times 2 = 1$$

であるから $m = 1091$ について $(a^5)^{1091} = a^{5\times 1091} = a^{1-2727\times 2} = a(a^{2727})^{-2} = a\,1^{-2} = a$．Ans. $m = 1091$.

6a (10 点) $d=\gcd(m,n)$ とする．このとき次を示せ：

連立方程式 $\begin{cases} x\equiv a \bmod m, \\ x\equiv b \bmod n \end{cases}$ が解を持つ $\Longleftrightarrow a\equiv b \bmod d$.

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

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

は群である．但し演算は通常の行列の積を $\mathbb{Z}/p\mathbb{Z}$ の演算により行ふものである．$\mathrm{GL}(2,\mathbb{Z}/7\mathbb{Z})$ ($\underline{p=7}$) において，$\begin{bmatrix} \overline{5} & \overline{4} \\ \overline{1} & \overline{3}\end{bmatrix}$ の逆元を求めよ．

6c (10 点) $f(x)=x^4+\overline{4}x^3+\overline{4}x^2+\overline{2}x+\overline{4}\in(\mathbb{Z}/5\mathbb{Z})[x]$ を因数分解せよ．

6a 講義中に印刷したものを配布済み．

6b Ans. $\begin{bmatrix} \overline{6} & \overline{6} \\ \overline{5} & \overline{3}\end{bmatrix}$.

6c Ans. $(x+\overline{2})(x+\overline{4})(x^2+\overline{3}x+\overline{3})$.

7 (10 点) (1) $\mathbb{Z}/2727\mathbb{Z}$ において $\overline{5}$ の乗法に関する逆元を求めよ．
答は $0<n<2727$ なる整数 n によつて $\overline{n}$ の形で与へよ．
(2) Euler 函数の値 $\varphi(2727)$ を求めよ．
(3) 5^{1802} および 5^{1799} を 2727 で割つた余りを求めよ．
(Hint：Euler の定理と (1)．)

略解
(1) **5** の解答から $5\times1091-2727\times2=1$．つまり $\mathbb{Z}/2727\mathbb{Z}$ において $\overline{5}\times\overline{1091}=\overline{1}$．よつて，答は $\overline{1091}$.

(2) $2727=101\times3^3$ だから $\varphi(2727)=\varphi(101)\,\varphi(3^3)=(101-1)(3^3-3^2)=100\times18=\underline{1800}$ ····· Ans.

(3) Euler の定理により $5^{1800}\equiv1 \bmod 2727$.
ゆゑに $5^{1802}\equiv5^2=25 \bmod 2727$.
Ans. 5^{1802} を 2727 で割つた余りは 25.
また Euler の定理と (1) から $5^{1799}\equiv5^{-1}\equiv1091 \bmod 2727$.
Ans. 5^{1799} を 2727 で割つた余りは 1091.

学籍番号

8 (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．

略解 まづ $H=\{\varepsilon,\ (1\,2\,3\,4),\ (1\,3)(2\,4),\ (1\,4\,3\,2)\}=\varepsilon H$ である．

$$\begin{aligned}
(1\,2)H&=\{(1\,2),\ (2\,3\,4),\ (1\,3\,2\,4),\ (1\,4\,3)\},\\
(1\,3)H&=\{(1\,3),\ (1\,2)(3\,4),\ (2\,4),\ (1\,4)(3\,2)\},\\
(1\,4)H&=\{(1\,4),\ (1\,2\,3),\ (1\,3\,4\,2),\ (2\,4\,3)\},\\
(2\,3)H&=\{(2\,3),\ (1\,3\,4),\ (1\,2\,4\,3),\ (1\,4\,2)\},\\
(3\,4)H&=\{(3\,4),\ (1\,2\,4),\ (1\,4\,2\,3),\ (1\,3\,2)\}.
\end{aligned}$$

ゆゑに

$$S_4=H\sqcup(1\,2)H\sqcup(1\,3)H\sqcup(1\,4)H\sqcup(2\,3)H\sqcup(3\,4)H.$$

または

$$S_4/H=\{H,\ (1\,2)H,\ (1\,3)H,\ (1\,4)H,\ (2\,3)H,\ (3\,4)H\}.$$

9 (15 点) 0 以外の正の有理数の全体 $\mathbb{Q}^\times$ 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．)

証明の概略 $\mathbb{Q}^\times$ が巡回群だと仮定して，その生成元を $\frac{a}{b}$ $(\gcd(a,b)=1)$ とせよ．素数は無限に存在するから $p\nmid a$ かつ $p\nmid b$ なる素数 p が存在する．このとき，任意の整数 n について $\left(\frac{a}{b}\right)^n$ の分母も分子も p で割り切れない．特に $\frac{a}{b}$ の冪は決して p とはならない．しかるに $p\in\mathbb{Q}^\times$ だから矛盾である．

別証 $\mathbb{Q}^\times$ は無限群であるから，これが巡回群ならば無限巡回群である．しかるに $(-1)^2=1$ であつて 1 以外に有限位数の元 $-1\in\mathbb{Q}^\times$ が存在し矛盾である．

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 (15) 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) 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.

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