実施：2018 年 7 月 8 日 (月) 14:50-16:20, 11-203 室

B4 で印刷

2019 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. **6a**, **6b**, **6c** は選択問題である. 1 問を選んで解答せよ.

1 (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.

略解
G0 $h_1, h_2\in H$ のとき $(g^{-1}h_1g)(g^{-1}h_1g)=g^{-1}(h_1h_2)g\in H$.
G1 これは G が群であるから当然成り立つ.
G2 $1=g^{-1}1g\in H$.
G3 $h\in H$ のとき $(g^{-1}hg)^{-1}=g^{-1}h^{-1}g\in H$.
以上より $H<G$.

2 (10 点) (1) 行列 $\begin{bmatrix}0&1&0\\0&0&-1\\1&0&0\end{bmatrix}$ の位数を求めよ. 但し, 演算は行列の乗法とする.
(2)* 成分のすべてが整数である 2 次の 正方行列で, その位数が 6 であるものを 1 つ見出せ.

答 (1) 位数 6.
(2) $\begin{bmatrix}0&1\\-1&1\end{bmatrix}$ など.

3 (10 点) S_4 の部分集合 $H=\{\varepsilon, (1\,2), (3\,4), (1\,2)(3\,4)\}$ は部分群であることを示せ.

略解 H の元について演算の結果は以下の通り.

	ε	$(1\,2)$	$(3\,4)$	$(1\,2)(3\,4)$
ε	ε	$(1\,2)$	$(3\,4)$	$(1\,2)(3\,4)$
$(1\,2)$	$(1\,2)$	ε	$(1\,2)(3\,4)$	$(3\,4)$
$(3\,4)$	$(3\,4)$	$(1\,2)(3\,4)$	ε	$(1\,2)$
$(1\,2)(3\,4)$	$(1\,2)(3\,4)$	$(3\,4)$	$(1\,2)$	ε

これから **G0**, **G1**, **G2**, **G3** は容易に確かめられる.

4 (10 点) 位数 42 の巡回群 $\langle a\rangle$ の生成元はいくつあるか. またそれら生成元を a^k $(0<k<42)$ の形で列記せよ.

答 約数は $\varphi(42)=\varphi(2)\varphi(3)\varphi(7)=2\times 6=12$ 個ある.
$\{a, a^5, a^{11}, a^{13}, a^{17}, a^{19}, a^{23}, a^{25}, a^{29}, a^{31}, a^{37}, a^{41}\}$.

5 (10 点) 位数 2021 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. 生成元であれば $(a^5)^m=a$ となる整数 m が存在する. その場合は, その様な m（但し $0\leqq m<2021$）を求めよ. さもなくば, 生成元ではない理由を述べよ.

略解 互除法を使ふ（使ふまでもないが）と, $2021\times 1-404\times 5=1$ がわかる. よつて $(a^5)^{-404}=a^{2021}=1$. ゆゑに $m=2021-404=1617$.

6a (10 点) $d=\gcd(m,n)$ とする．このとき次を示せ：

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

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

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

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．$\mathrm{GL}\big(2,\mathbb{Z}/7\mathbb{Z}\big)$ $(\underline{p=7})$ において，$\begin{bmatrix} \overline{3} & \overline{1} \\ \overline{0} & \overline{1} \end{bmatrix}$ の位数を求めよ．

6c (10 点) $f(x)=x^4-\overline{4}x^2+\overline{1}\in(\mathbb{Z}/7\mathbb{Z})[x]$ を因数分解せよ．

(Hint：1 次式を約元に持つとは限らない．$x^4+x^2+1=(x^2+1)^2-x^2$ を真似る．)

略解 **6a** $(\Rightarrow)$. $d=\gcd(m,n)$ だから，解 x があれば $x\equiv a \mod d$ かつ $x\equiv b \mod d$. ゆゑに $a\equiv b \mod d$.

$(\Leftarrow)$. (互除法などによれば，) $d=ms+nt$ となる $s,t\in\mathbb{Z}$ が存在する．$a-b=dk$ とすると $a-b=(ms+nt)k$ ゆゑ $a-msk=b+ntk$. この両辺を x とすると，これは与へられた合同式を満たす．

$(\Leftarrow)$ の別証) $m=m'd$, $n=n'd$ とおく．$\gcd(m',n')=1$ ゆゑ $1=m's+n't$ なる $s,t\in\mathbb{Z}$ が存在する．これを使つて $x=an't+bm's$ とおくと，これは 1 つの解である．実際，$d|(b-a)$ だから

$$an't+bm's=a(1-m's)+bm's=a+(b-a)m's\equiv a \mod m,$$
$$an't+bm's=an't+b(1-n't)=(a-b)n't+b\equiv b \mod n.$$

(補足) ここで，任意の 2 つの解を x_1,x_2 とすれば，$x_2-x_1\equiv 0 \mod m$, $x_2-x_1\equiv 0 \mod n$ である．これは $\mathrm{lcm}(m,n)\,\big|\,(x_2-x_1)$ を意味する (lcm =least common multiple, 最小公倍数)．よつて，解は $\mod \mathrm{lcm}(m,n)$ で高々 1 しかない．

6b 位数 6.

6c

$$\begin{aligned}(\text{与式}) &= (x^2-\overline{1})^2-\overline{2}x^2\\ &= (x^2-\overline{2})^2-\overline{3}^2x^2\\ &= (x^2+\overline{3}x-\overline{2})(x^2-\overline{3}x-\overline{2}).\end{aligned}$$

7 (15 点) 次の問に答へよ．

(1) $\mathbb{Z}/2021\mathbb{Z}$ において $\overline{5}$ の乗法に関する逆元を求めよ．
答は $0<n<2021$ なる整数 n によつて $\overline{n}$ の形で与へよ．

(2)* 2021 を素因数分解せよ．(Hint：2021 は素数ではない！)

(3) Euler 函数の値 $\varphi(2021)$ を求めよ．

(4) 5^{1931} および 5^{1934} を 2021 で割つた余りを求めよ．
(Hint：Euler の定理と (1), (3))

略解 (1) $2021\times 1-5\times 404=1$ だから $\overline{5}^{-1}=\overline{-404}=\overline{1617}$.

(2) $2021=43\times 47$.

(3) $\varphi(2021)=\varphi(43)\varphi(47)=42\times 48=1932$.

(4) Euler の定理により $\overline{5}^{1932}=\overline{1}$.

ゆゑに (1) の結果から $\overline{5}^{1931}=\overline{5}^{-1}=\overline{-404}=\overline{1617}$.

また，$\overline{5}^{1934}=\overline{5}^{2}=\overline{25}$.

Ans. 1617, 25.

学籍番号

8 (10 点) S_4 の部分群 $H=\{\varepsilon,\ (1\,2),\ (3\,4),\ (1\,2)(3\,4)\}$ に関する左剰余類分解 S_4/H を要素を列記して記せ．

答

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

となり

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

(完全代表系のとり方は他にもある．)

9 (15 点) 位数が素数の群は巡回群に限ることを示せ．(Hint：位数が 2 以上であるから，単位元以外にも元がある．その 1 つ a をとり，部分群 $\langle a\rangle$ を考へよ．これに Lagrange の定理を適用．)

略解 与へられた群を G とし，その位数が素数 p であるとする．Hint の部分群を $H=\langle a\rangle$ とおく．$|H|$ は $|G|=p$ の約数であるが $a\neq 1$ より $|H|=p$ でなくてはならない．よつて $H=G$ でなくてはならない．

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 **G0**, **G1**, **G2**, **G3** の 4 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.)

G0 演算 $G \times G \to G$, $(a, b) \mapsto ab$ が定義されている. この演算について, 以下が成立 :

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 $(a, b) \mapsto a + b$ と 乗法 と呼ばれる演算 $(a, b) \mapsto ab$ 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 $1x = x1 = x$.

R5 乗法の交換法則 : $ab = ba$

(8) 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. たとへば, qR $(q \in R)$ は R の ideal である.

(9) 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.

(10) 可換環 R について 1 の約元は 単元 と呼ばれる. 単数の全体 $R^\times$ と書く. これは乗法に関して群をなす.

(11) R を零因子をもたない可換環とする.
0 でもなく, R の単元でもない $q \in R$ は, 任意の $a, b \in R$ に対し, 「$q = ab$ ならば $a \in R^\times$ または $b \in R^\times$ である」が成り立つとき, R の 既約元 であるといはれる.
0 でもなく, R の単元でもない $q \in R$ は任意の $a, b \in R$ に対して「$ab \in qR$ ならば, $a \in qR$ または $b \in qR$」が成り立つとき, 素元 であるといはれる.

(12) 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.

(13) (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.

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

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

(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) $(\mathbb{Z}/n\mathbb{Z})^\times = \{(j \mod n) \in \mathbb{Z}/n\mathbb{Z} \,|\, \gcd(j, g) = 1\}$. これは積に関して群をなす. 法 n に関する 既約剰余類群 と呼ばれる.

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