

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 <small>月曜 2 時限, 教科書: Original</small>			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 3. 試験場の静粛を保つために、途中退場は開始 60 分後の時点の一回限りとする。

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 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。

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

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。

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。

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 $0 \leq m < 2021$) を求めよ。さもなければ、生成元ではない理由を述べよ。

6a (10 点) $d = \gcd(m, n)$ とする. このとき次を示せ:

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

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

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

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

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

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

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.

7 (15 点) 次の問に答へよ.

(1) $\mathbb{Z}/2021\mathbb{Z}$ において $\bar{5}$ 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 \bar{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 関数の値 $\varphi(2021)$ 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))

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.)

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) $a, b, \dots, c \in \mathbb{Z}$ に対して,
$$\{ax + by + \dots + cz \mid x, y, \dots, z \in \mathbb{Z}\} = d\mathbb{Z}$$
 となる $d \in \mathbb{Z} (d \geq 0)$ が唯一つ存在する. このとき $d = \gcd(a, b, \dots, c)$ 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 $G \times G \rightarrow G, (a, b) \mapsto ab$ 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である.
- (5) 群 G がある $a \in G$ について $G = \{a^m \mid m \in \mathbb{Z}\}$ と表されるとき G を a によって生成された 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, $d \mid m$ 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 $ax \in M$
- が成り立つとき, R の ideal と呼ばれる. たとえば, $qR (q \in R)$ 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, $\mathbb{Z}[x] = \{a + bx \mid a, b \in \mathbb{Z}\}$, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ 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 $\{x_i \mid i \in \Lambda\}$ 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, $\#\{x \in G \mid x^m = 1\} \leq m$ 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 $(k \bmod n) (= \bar{k}$ と略記する) 達のなす可換環.
- 例えば $\mathbb{Z}/5\mathbb{Z} = \{0 \bmod 5, 1 \bmod 5, 2 \bmod 5, 3 \bmod 5, 4 \bmod 5\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.
- (18) $\varphi(n) = “(\mathbb{Z}/n\mathbb{Z})^\times$ の要素の個数” = “ $1, \dots, n-1$ の中で n と互いに素なものの個数”.
- ただし $\varphi(1) = 1$.
- (19) $(\mathbb{Z}/n\mathbb{Z})^\times = \{j \bmod n \mid \gcd(j, n) = 1\}$. 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.