実施：2015 年 7 月 27 日 (月) 10:40-12:10, H-602 室

2015 年度　前期　期末試験 (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
1/1	有	なし	80 分	代数学 I　木曜 2 時限, 教科書：Original	A,B	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. **6** および **8** は選択問題である. **6a** と **6b**, **8a** と **8b** と **8c** のうち, それぞれから 1 問選んで解答せよ.

1 (15 点) $A = \begin{bmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}$ が行列の積に関して生成する巡回群の位数を求めよ.

2 (10 点) 位数 $2^2 \cdot 3^3 \cdot 5^2 = 2700$ の元 a を生成元とする巡回群 $\langle a \rangle = \{ a^m \mid 0 \leqq m \leqq 2699 \}$ の生成元はいくつあるか. また, 生成元を m が小さい順に 5 つ記せ.

3 (10 点) Euler 関数 φ について, $\varphi(41 \cdot 7^3)$ を求めよ.

4 (10 点) 位数 53 の元 a から生成される巡回群 G がある. このとき, a^{39} は G の生成元であるか. もし, そうならば $(a^{39})^m = a$ となる整数 m が存在する筈である. その様な m で $0 \leqq m < 53$ なるものを求めよ.

5 (15 点) $d = \gcd(m, n)$ とする. 連立方程式 $x \equiv a \bmod m,\ x \equiv b \bmod n$ が解を持つためには, $a \equiv b \bmod d$ であることが必要十分であることを示せ.

6a (15 点) x, y, z は整数とする. $x^2+y^2=z^2$ ならば, $xyz \equiv 0 \bmod 60$ であることを示せ.

6b (15 点) $(\mathbb{Z}/11\,\mathbb{Z})[x]$ の元 $f(x)=x^3+\overline{3}x^2+\overline{4}x+\overline{4}$ について, $f(x)=\overline{0}$ の根をすべて見つけ, $f(x)$ を因数分解せよ.

7 (10 点) 4 次の対称群 S_4 の元のうち数字 4 を動かさない元の全体, つまり $\{1,2,3\}$ の置換の全体 S_3 は S_4 の部分群をなす. S_4 を部分群 S_3 に関して左剰余類に分解し, 各左剰余類を要素を列記して記述せよ.

8a (15 点) 2 は $\bmod 19$ の原始根である. これ以外の全ての原始根を求めよ. また x の方程式 $x^6 \equiv 1 \bmod 19$ を解け.

8b (15 点) p が素数のとき $(p-1)! \equiv -1 \bmod p$ であることを証明せよ.

8c (15 点) p は奇素数であつて, $a^{2^n}+1$ の約数であるとせよ. このとき $p \equiv 1 \bmod 2^{n+1}$ であることを示せ.

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.
(2) $\mathbb{Z}$ は整数全体のなす可換環. (下記 (12) を参照)
(3) $\mathbb{Q}$ は有理数全体のなす体. (下記 (14) を参照)
(4) $\mathbb{R}$ は実数全体のなす体.
(5) $\mathbb{C}$ は複素数全体のなす体.
(6) $a_1, a_2, \cdots, a_n \in \mathbb{Z}$ に対して,
$$\{a_1x_1 + a_2x_2 + \cdots + a_nx_n \,|\, x_1, x_2, \cdots, x_n \in \mathbb{Z}\} = d\mathbb{Z}$$
となる $d \in \mathbb{Z}$ $(d \geqq 0)$ が唯 1 つ存在する. このとき $d = \gcd(a_1, a_2, \cdots, a_n)$ である.
(7) 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.
(8) 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.
(9) 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.
(10) 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.
(11) G を a 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, a^d が H を生成する.
(12) 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 : $ab = ba$.
(13) 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 $\mathbb{Z}[i] = \{\, a + bi \,|\, a,\ b \in \mathbb{Z} \,\}$, $\mathbb{Z}[\sqrt{5}] = \{\, a + b\sqrt{5} \,|\, a, b \in \mathbb{Z} \,\}$.
(14) 可換環 R について, 0 以外のどの元も乗法に関して逆元を持つとき R は 体(たい) と称される.
(15) 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.
(16) (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.
(17) (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.
(18) 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.
(19) $\mathbb{Z}/m\mathbb{Z}$ 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 $\mathbb{Z}/5\mathbb{Z} = \{(0 \mod 5), (1 \mod 5), (2 \mod 5), (3 \mod 5), (4 \mod 5)\,\} = \{\, \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4} \,\}$.
(20) $(\mathbb{Z}/m\mathbb{Z})^\times = \{(j \bmod m) \in \mathbb{Z}/m\mathbb{Z} \,|\, \gcd(j, g) = 1\}$. 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.
(21) $\varphi(n) =$ " $(\mathbb{Z}/n\mathbb{Z})^\times$ 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 $\varphi(1) = 1$.