平成３１年度

千葉大学大学院融合理工学府　博士前期課程

学力検査問題

（数学情報科学専攻　数学・情報数理学コース）

専 門

平成３０年８月１６日（木）

検査時間　２４０分

「注意事項」

1. **問題は A0 問題が１題，A 問題が５題，B 問題が１２題ある。**

   A0 は全員が解答すること。

   A 問題: A1,...,A5 の中から 任意に３題選んで 解答すること。
   （４題以上解答することは認められない。）

   B 問題: B1,...,B12 の中から 任意に１題選んで 解答すること。
   （２題以上解答することは認められない。）

2. **解答用紙は５枚あるので，そのすべてに コース名と受験番号 を記入のこと。**

3. **各解答用紙には，解答しようとする 問題番号を明記し，**

   １枚に１題だけ を解答すること。

   解答不能の場合も，解答用紙を持ち帰ってはならない。

4. **解答用紙が不足のときには，用紙の裏面も使用してよい。**

5. **問題冊子は持ち帰ってもよい。**

$\boxed{\textbf{A0}}$

集合 A から集合 B への写像 $f\colon A \longrightarrow B$ について次の 4 条件を考える：

(i) f は単射である．

(ii) f は全射である．

(iii) 任意の集合 C と 2 つの任意の写像 $g,\ h\colon C \longrightarrow A$ に対して，$f \circ g = f \circ h$ ならば $g = h$ である．

(iv) 任意の集合 C と 2 つの任意の写像 $g,\ h\colon B \longrightarrow C$ に対して，$g \circ f = h \circ f$ ならば $g = h$ である．

このとき，以下に述べる 4 つの命題について真のときは証明し，偽のときは反例を挙げよ．

(1) 条件 (i) が満たされれば条件 (iii) も満たされる．

(2) 条件 (iii) が満たされれば条件 (i) も満たされる．

(3) 条件 (ii) が満たされれば条件 (iv) も満たされる．

(4) 条件 (iv) が満たされれば条件 (i) も満たされる．

$\boxed{\textbf{A1}}$

f は $\mathbb{R}^n$ 上の線形変換 (n は正整数) であり，$\mathbb{R}^n$ の部分空間 V，W は $f(V) \subset W$，$f(W) \subset V$ を満たすとする．このとき，以下の命題を証明せよ．

(1) $\dim V \neq \dim W$ ならば，f は単射でない．

(2) $V + W = \mathbb{R}^n$，$f(V) = W$，$f(W) = V$ ならば，f は全単射である．

(3) $V \cap W = \{\mathbf{0}\}$，$\alpha \in \mathbb{R} \setminus \{0\}$ ならば，固有値 α に対する f の固有ベクトルは，V にも W にも含まれない．

$\boxed{\textbf{A2}}$

(1) $x = 0$ の近傍で定義された関数 $f(x) = x^3 - x^2 + x + 1$ の逆関数を g とする．$g'(1)$, $g''(1)$, $g'''(1)$ を求めよ．

(2) $x = 0$ の近傍で定義された関数 $F(x) = \sin^3 x - \sin^2 x + \sin x + 1$ の逆関数を G とする．$G'(1)$, $G''(1)$, $G'''(1)$ を求めよ．

$\boxed{\textbf{A3}}$

S を実数全体のなす集合とし，S の部分集合からなる集合族 $\mathcal{U}, \mathcal{V}$ を次のように定義する．

$$\mathcal{U} = \{U \subset S \mid U = S \text{ または } U = \emptyset \text{ または，補集合 } S - U \text{ が有限集合}\}$$

$$\mathcal{V} = \{V \subset S \mid V = S \text{ または } V = \emptyset \text{ または，補集合 } S - V \text{ が高々可算集合}\}$$

これについて次の問いに答えよ．

(1) $\mathcal{U}, \mathcal{V}$ の各々が S の開集合系 (位相) になっていることを示せ．

(2) 位相空間 $(S, \mathcal{U})$ と $(S, \mathcal{V})$ はコンパクト空間であるか否か，それぞれ証明をつけて答えよ．

(3) 写像 $f : (S, \mathcal{U}) \to (S, \mathcal{V})$ と $g : (S, \mathcal{V}) \to (S, \mathcal{U})$ を $f(x) = x,\ g(x) = x\ (x \in S)$ によって定める．このとき f と g が，それぞれ連続写像となるか否か調べよ．

$\boxed{\textbf{A4}}$

$0 < p < 1$ に対して，確率変数 X の確率分布が

$$P(X = k) = \begin{cases} p(1-p)^{k-1} & k = 1, 2, \ldots \\ 0 & \text{それ以外} \end{cases}$$

で与えられるとき，X はパラメーター p の幾何分布 $\mathrm{Ge}(p)$ に従うという．独立な確率変数 X_1 と X_2 がそれぞれ幾何分布 $\mathrm{Ge}(p_1)$ と $\mathrm{Ge}(p_2)$ に従うとき，次の問いに答えよ．ただし $p_1 \neq p_2$ とする．

(1) $Y = X_1 + X_2$ について，$P(Y = k)$ を求めよ．

(2) Y の期待値を求めよ．

(3) $Z = \min(X_1, X_2)$ について，$P(Z = k)$ を求めよ．

(4) Z のモーメント母関数を求めよ．

A5

以下の Pascal プログラムを実行して, 正整数を入力したとする．このとき下の問に答えよ．

```
program sieve(input, output);
const maxind = 200;
var table: array[0..maxind] of boolean;  n: integer;

function ti(n: integer): integer;
begin
  ti := (n div 7) * 2 + (n mod 7) div 5
end;

function fi(i: integer): integer;
begin
  if i mod 2 = 0 then fi := (i div 2) * 7 + 1
  else fi := (i div 2) * 7 + 6
end;

procedure mktab(maxnum: integer);
var n, m, d, dm, i: integer;
begin
  for i := 0 to maxind do table[i] := true;
  n := 6;  d := 2;
  while n <= maxnum do
    begin
      if table[ti(n)] then
        begin  m := n;  dm := d;
          while m <= maxnum div n do
            begin table[ti(n*m)] := false; m := m+dm; dm := 7−dm  end
        end;
      n := n+d;  d := 7−d
    end
end;

begin
  readln(n);
  if (ti(n) <= maxind) and (n = fi(ti(n))) then
    begin  mktab(n);  writeln(n, table[ti(n)])  end
end.
```

(1) 34 を入力したとき, どのような出力があるか記せ．(答だけでよい.)

(2) 正整数 n を入力したとき出力が存在する条件を述べ, それがどのような出力であるか理由と共に述べよ．

$\boxed{\textbf{B1}}$

素数 p を固定する．群 G に対して，集合 $\{g^p \mid g \in G\}$ が生成する G の部分群を G' と書く．

(1) 任意の群 G に対して，G' は G の正規部分群であることを示せ．

(2) G を有限群，H を G のシロー p 部分群の 1 つとする時，自然な群準同型写像

$$f\colon H/H' \to G/G'; \quad f(hH') = hG'$$

が全射であることを示せ．

(3) (2) の状況で，G がアーベル群ならば f は同型写像であることを示せ．

$\boxed{\textbf{B2}}$

体 K 上の 4 変数多項式環 $S = K[x_1, x_2, x_3, x_4]$ において

$$y = x_1x_4 + x_2x_3 \ , \quad z = x_3x_4$$

と定め，$R = K[y, x_2, x_3, x_4]$，$T = K[y, x_3, x_4]$ とおく．R と T を $\{1, z, z^2, \ldots\}$ で局所化した環をそれぞれ R_z と T_z で表す．さらに $a \in K$ に対して $\sigma_a : S \longrightarrow S$ は K の元と x_3, x_4 を動かさない環の自己同型写像で

$$\sigma_a(x_1) = x_1 - ax_3 \ , \quad \sigma_a(x_2) = x_2 + ax_4$$

なるものとする．以下の問いに答えよ．

(1) 各 $a \in K$ に対して $\sigma_a(y)$ を求めよ．

(2) $S \subset R_z$ を示せ．

(3) K は無限体とする．$f \in S$ が任意の $a \in K$ に対して $\sigma_a(f) = f$ を満たせば $f \in T_z$ であることを示せ．

B3

a を実数とし，写像 $f_a\colon \mathbb{R}^2 \to \mathbb{R}^2$ を $f_a(x,\, y) = (x,\, y^3 + xy + ay)$ で定める．

(1) $a = 0$ のとき，f_0 の微分 $df_0(p) : T_p\mathbb{R}^2 \to T_{f_0(p)}\mathbb{R}^2$ が全射でなくなる点 $p \in \mathbb{R}^2$ 全体の集合 (すなわち f_0 のヤコビ行列式が 0 となるような点 $p \in \mathbb{R}^2$ 全体の集合) $C_0 \subset \mathbb{R}^2$ を求めよ．また，この C_0 が $\mathbb{R}^2$ の滑らかな部分多様体となることを示せ．

(2) C_0 の f_a による像 $f_a(C_0) \subset \mathbb{R}^2$ が滑らかな部分多様体となるための a の条件を求めよ．

B4

$D,\, E$ を 2 つの単位円板，C を単位円周とする．以下では，単位円板と単位円周を複素数平面内の部分集合として，それぞれ

$$\{z \in \mathbb{C} \mid |z| \leqq 1\},\ \{z \in \mathbb{C} \mid |z| = 1\}$$

と同一視して考える．ただし，$D,\, E,\, C$ は互いに交わりはないものとする．また，∂D と ∂E はそれぞれ D と E の境界とする．

n を整数とし，写像 $f_n\colon \partial D \to C$ と $g_n\colon \partial D \to E$ をこの同一視を用いて $f_n(z) = z^n$, $g_n(z) = z^n$ で定める．

D と E を写像 g_n によって貼り合わせてできる位相空間を $Y_n = D \cup_{g_n} E$ とする．すなわち Y_n は交わりのない和集合 $D \cup E$ において，$\partial D \ni x \simeq g_n(x) \in \partial E$ によって生成される同値関係 $\simeq$ を考えたときの商位相空間 $Y_n = (D \cup E)/\simeq$ である．また，D と C を写像 f_n によって貼り合わせてできる位相空間を $X_n = D \cup_{f_n} C$ とする．

(1) $X_1,\, Y_1$ の整数係数ホモロジー群 $H_q(X_1,\, \mathbb{Z}),\, H_q(Y_1,\, \mathbb{Z})$ $(q = 0,\, 1,\, 2)$ を求めよ．

(2) $X_0,\, Y_0$ の整数係数ホモロジー群 $H_q(X_0,\, \mathbb{Z}),\, H_q(Y_0,\, \mathbb{Z})$ $(q = 0,\, 1,\, 2)$ を求めよ．

(3) $X_2,\, Y_2$ の整数係数ホモロジー群 $H_q(X_2,\, \mathbb{Z}),\, H_q(Y_2,\, \mathbb{Z})$ $(q = 0,\, 1,\, 2)$ を求めよ．

$\boxed{\textbf{B5}}$

複素平面内の図形 $C_R \ \ (R > 0)$ を

$$C_R = \left\{ z \in \mathbb{C} \setminus \{0\} \;\middle|\; \mathrm{Re}\,\frac{1}{z} = \frac{1}{R} \right\}$$

で定義する．ここで記号 Re は複素数の実部を表す.

(1) C_R の概形を図示せよ.

(2) n を自然数とするとき，積分

$$\int_{C_R} z^{n-1} e^{1/z}\, dz$$

の値を求めよ．ここで C_R の向きは反時計回りとする．(C_R は原点を含んでいないので広義積分になることに注意せよ.)

$\boxed{\textbf{B6}}$

y, z, w を変数 x の関数, y', z', w' をそれぞれの導関数とする.

(1) 微分方程式　$y' + xy = 0$ を解け.

(2) 微分方程式　$y' + xy = x^3$ を解け.

(3) 微分方程式

$$\begin{pmatrix} y' \\ z' \\ w' \end{pmatrix} = \begin{pmatrix} -x & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} y \\ z \\ w \end{pmatrix} + \begin{pmatrix} x^3 \\ x \\ -x^2 + 3 \end{pmatrix}$$

の解 $y(x)$, $z(x)$, $w(x)$ で初期条件

$$y(0) = -2,\ z(0) = -\frac{1}{9},\ w(0) = -\frac{1}{3}$$

を満たすものを求めよ.

$\boxed{\textbf{B7}}$

V を実数上の内積 $(\,\cdot\,,\,\cdot\,)$ を持つ線形空間とする. $x \in V$ に対してノルム

$$\|x\| = \sqrt{(x, x)}$$

を定義する.

(1) 内積の性質を用いて次の Cauchy-Schwartz の不等式を示せ.

$$|(x, y)| \leq \|x\| \cdot \|y\|, \qquad x, y \in V.$$

(2) $f : V \longrightarrow \mathbb{R}$ を線形写像とし

$$\|x\| = 1 \Rightarrow |f(x)| \leq M$$

となる実数 M が存在するとする. このとき, N 個の互いに直交する長さ 1 のベクトル x_1, x_2,..., x_N, つまり

$$(x_i, x_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

を満たすベクトルに対して,

$$\sum_{i=1}^{N} |f(x_i)|^2 \leq M^2$$

が成立することを示せ.

$\boxed{\textbf{B8}}$

X を実数値確率変数とし，$M(X)$ を

$$P\bigl(X > M(X)\bigr) \le 1/2 \text{ かつ } P\bigl(X < M(X)\bigr) \le 1/2$$

を満たす実数とする．

(1) $M(X)$ は少なくとも 1 つ存在することを示せ．

(2) $E[X] < \infty$, $E[X^2] < \infty$ とする．このとき

$$M(X) \le E[X] + \sqrt{2\,\mathrm{Var}(X)}$$

を示せ．ただし $\mathrm{Var}(X)$ は X の分散を表す．

(3) X_1 を以下の確率密度関数 $p(x)$ を持つ実数値確率変数とする．

$$p(x) = \begin{cases} Ce^{-\lambda x}, & 0 < x < 1/3, \\ 0, & x \le 0 \text{ または } 1/3 \le x \le 2/3 \text{ または } 1 \le x, \\ Ce^{(1-\lambda)(x-1)}, & 2/3 < x < 1. \end{cases}$$

ただしパラメータ λ は $0 \le \lambda \le 1$ を満たす実数である．このとき定数 C を求め，$M(X_1)$ の集合が 1 点でないときの λ の値およびそのときの集合を求めよ．

$\boxed{\textbf{B9}}$

二項分布 $B(n,p)$ に従う母集団から大きさ m の標本 $X_1, X_2, \ldots, X_m$ を無作為抽出し，その標本平均を $\overline{X} = \dfrac{1}{m}\displaystyle\sum_{k=1}^{m} X_k$ とする．n を既知とし，母数 p の推定に関する次の問いに答えよ．

(1) $\overline{X}/n$ が p の不偏推定量であることを示せ．

(2) 得られた全ての標本に基づいた p のフィッシャー情報量を求めよ．

(3) クラメル・ラオの不等式を用いて，$\overline{X}/n$ が p の有効推定量であることを示せ．

(4) m が十分大きいとき，中心極限定理を用いて p の信頼度 $1-\alpha$ の信頼区間を求めよ．

B10

E を鍵空間 $\{0,1\}^k$ をもつ，n-ビットブロック暗号方式 Π における暗号化関数とする．つまり，$E:\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ とする．いま，鍵空間 $\{0,1\}^{2k}$ を持つ n-ビットブロック暗号方式 Π' の暗号化関数 F を次のように定める．

$$F(K_1||K_2, M) \stackrel{\mathrm{def}}{=} E(K_2, E(K_1, M)), \quad (\text{ただし } K_1, K_2 \in \{0,1\}^k \text{ とする．})$$

このとき，平文と暗号文の 2 つのペア $((m_1,\, c_1)$ および $(m_2,\, c_2))$ を入手できた場合を想定し，暗号方式 Π が安全であったとしても，暗号方式 Π' は安全ではないことを示せ．ただし，暗号方式が安全であるとは，その解読計算量が (鍵に対する) 全数探索未満となるアルゴリズムが発見されていないことを言うものとする．

B11

命題変数 p, q,$\ldots$ と記号 $\perp$ から論理記号 $\to$ によってつくられる命題論理の論理式を考える．論理式 A に $\nu(A) \in \{0,1\}$ を対応させる写像 ν は, $\nu(\perp) = 0$ かつ $\nu(A \to B) = \max\{1-\nu(A), \nu(B)\}$ を満たすときに付値と呼ばれる．論理式 A に対して $\neg A :\equiv (A \to \perp)$ とおく. また論理式の集合 Γ の任意の有限部分集合 Γ_0 に対して $\forall A \in \Gamma_0(\nu_0(A) = 1)$ を満たす付値 ν_0 が存在するとき, Γ は有限充足可能であるという．有限充足可能な論理式の集合全体の集合 $\mathcal{G}$ を集合の包含関係 $\Gamma_0 \subset \Gamma_1$ によって順序付ける．

(1) 論理式の集合 Γ は順序集合 $\mathcal{G}$ において極大であるとする．このとき Γ は以下の条件 $(*)$ を満たすことを証明せよ．

$$\text{任意の論理式 } A \text{ について } A, \neg A \text{ の内で一方のみが } \Gamma \text{ に属す．} \qquad (*)$$

(2) $\perp \notin \Gamma$ かつ条件 $(*)$ を満たす論理式の集合 Γ で有限充足可能でないものを 1 つつくれ．

B12

次の Scheme のプログラムについて, 以下の問に答えよ.

```
(define (r x) (lambda (z) x))
(define (b g f) (lambda (z) ((f (g z)) z)))

(define t1
  (b (lambda (z) (* 2 z)) r))

(define t2
  (b car
     (lambda (u) (b cadr
                    (lambda (v) (r (+ u v)))))))

(define (tn f a)
  (if (null? f) (r a)
      (b (car f)
         (lambda (u) (tn (cdr f) (cons u a))))))
```

(1) `(t1 2)` の評価結果を, 理由と共に記せ.

(2) `(t2 '`ℓ`)` の評価結果が `0` になるには ℓ はどのような式であればよいか, 理由と共に記せ.

(3) ℓ をリストとしたとき, `((tn (list cadr car caddr) '(0)) '`ℓ`)` の評価結果を, 理由と共に記せ.