

# 京都大学数学・数理解析専攻院試過去問

北窓

<https://seasawher.github.io/kitamado/>

2019 年 9 月 18 日

## 目次

---

1	はじめに	6
2	平成 31 年度 基礎科目	7
	問 1	7
	問 2	8
	問 3	9
	問 4	10
	問 5	12
	問 6	13
	問 7	14
3	平成 31 年度 専門科目	16
	問 1	16
	問 2	17
	問 3	18
	問 4	19
	問 5	20
4	平成 30 年度 基礎科目	22
	問 1	22
	問 2	23
	問 3	24
	問 4	26
	問 5	28
	問 6	30
	問 7	32
5	平成 30 年度 専門科目	33

問 1	33
問 2	34
問 3	35
6 平成 29 年度 基礎科目	38
問 1	38
問 2	39
問 3	41
問 4	42
問 5	43
問 6	44
問 7	45
7 平成 29 年度 専門科目	46
問 1	46
問 2	47
問 3	48
8 平成 28 年度 基礎科目 I	50
問 1	50
問 2	51
問 3	52
問 4	53
9 平成 28 年度 基礎科目 II	54
問 1	54
問 2	55
問 3	56
問 4	57
問 5	58
問 6	59
10 平成 28 年度 専門科目	60
問 1	60
問 2	61
問 3	63
11 平成 27 年度 基礎科目 I	66
問 1	66
問 2	67
問 3	68
問 4	69

12	平成 27 年度 基礎科目 II	70
	問 1	70
	問 2	72
	問 3	73
	問 4	74
	問 5	75
	問 6	77
	問 7	78
13	平成 27 年度 専門科目	79
	問 1	79
	問 2	80
	問 3	82
14	平成 26 年度 基礎科目 I	85
	問 1	85
	問 2	86
	問 3	88
	問 4	89
15	平成 26 年度 基礎科目 II	90
	問 1	90
	問 2	91
	問 3	92
	問 4	93
	問 5	94
	問 6	95
	問 7	96
16	平成 26 年度 専門科目	97
	問 1	97
	問 2	99
	問 3	100
17	平成 25 年度 基礎数学	102
	問 1	102
	問 2	103
	問 3	104
	問 4	105
18	平成 25 年度 数学 I	106
	問 1	106

	問 2	107
	問 3	108
	問 4	109
	問 5	110
19	平成 25 年度 数学 II	111
	問 1	111
	問 2	113
20	平成 24 年度 基礎数学	114
	問 1	114
	問 2	115
	問 3	117
	問 4	118
21	平成 24 年度 数学 I	119
	問 1	119
	問 2	120
	問 3	121
	問 4	122
	問 5	124
22	平成 24 年度 数学 II	126
	問 1	126
	問 2	127
23	平成 23 年度 基礎数学	128
	問 1	128
	問 2	129
	問 3	130
	問 4	131
24	平成 23 年度 数学 I	132
	問 1	132
	問 2	133
	問 3	134
	問 4	136
	問 5	137
25	平成 23 年度 数学 II	139
	問 1	139
	問 2	141

26	平成 22 年度 基礎数学	142
	問 1 . . . . .	142
	問 2 . . . . .	143
	問 3 . . . . .	144
	問 4 . . . . .	145
27	平成 22 年度 数学 I	146
	問 1 . . . . .	146
	問 2 . . . . .	147
	問 3 . . . . .	148
	問 4 . . . . .	149
	問 5 . . . . .	150
28	Appendix 1. 半直積と Galois 群	151
29	Appendix 2. Dirichlet の Diophantus 近似定理	157

## ■ はじめに

---

京都大学数学・数理解析専攻の院試の問題と解答です。問題文は <https://www.math.kyoto-u.ac.jp/ja/past-exams> から入手したものを使用しています。なお Microsoft Edge で閲覧することを推奨いたします。

この解答を作るにあたって、協力してくださった方々に感謝します。すむーずぶりんちゃん (@mat\_der.D) 氏には平成 31 年度基礎問 4 を解いていただきました。キヅ (@28Vittorio) さんと、ひろ (@azureh97) さんは院試ゼミのメンバーとして協力してくださいました。また、ナカトウ氏による解答も大変参考にさせていただきました。お礼申し上げます。また、私が難しい問題に悩んでいるときにいつも適切なアドバイスをくれた M 君にこの場を借りて謝意を表します。

解答作成には万全を期しましたが、この解答を使用することにより使用者に不利益が生じたとしても、解答執筆者である私 (北窓) は責任を負いません。したがって書かれていることが正しいかどうかはよくご自分で確認されるようにお願いします。とくに私 (北窓) は計算間違いや救いようのない勘違いをよくするので。

この PDF のコピー・再配布を許可します。ただし再配布の際にも「コピー・再配布は自由」として下さい。加筆・改変は私 (北窓) の GitHub アカウント (<https://github.com/Seasawher>) を通してくださればと思います。

## 平成 31 年度 基礎科目

### 問 1

$\alpha$  は  $0 < \alpha < \frac{\pi}{2}$  を満たす定数とする。このとき広義積分

$$\iint_D e^{-(x^2+2xy \cos \alpha+y^2)} dx dy$$

を計算せよ。ただし、 $D = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0, y \geq 0\}$  とする。

解答.  $x = r \cos \theta$ ,  $y = r \sin \theta$  と変数変換する。領域  $D$  は、 $\{(r, \theta) \mid r \geq 0, 0 \leq \theta \leq \frac{\pi}{2}\}$  へ移る。すると  $dx dy = r dr d\theta$  であって

$$\begin{aligned} \iint_D e^{-(x^2+2xy \cos \alpha+y^2)} dx dy &= \int_0^{\frac{\pi}{2}} d\theta \int_0^\infty e^{-r^2(1+\sin 2\theta \cos \alpha)} r dr \\ &= \frac{1}{2} \int_0^{\frac{\pi}{2}} d\theta \int_0^\infty e^{-r(1+\sin 2\theta \cos \alpha)} dr \\ &= \frac{1}{2} \int_0^{\frac{\pi}{2}} \frac{d\theta}{1 + \sin 2\theta \cos \alpha} \\ &= \frac{1}{4} \int_0^\pi \frac{d\theta}{1 + \sin \theta \cos \alpha} \end{aligned}$$

と計算できる。さらに  $t = \tan \frac{\theta}{2}$  として変数変換を行う。 $d\theta = 2(1+t^2)^{-1}dt$  で、 $\sin \theta = 2t/(1+t^2)$  だから

$$\begin{aligned} \iint_D e^{-(x^2+2xy \cos \alpha+y^2)} dx dy &= \frac{1}{4} \int_0^\infty \frac{2(1+t^2)^{-1}dt}{1 + 2t(1+t^2)^{-1} \cos \alpha} \\ &= \frac{1}{2} \int_0^\infty \frac{dt}{(t + \cos \alpha)^2 + \sin^2 \alpha} \\ &= \frac{1}{2} \int_{\cos \alpha}^\infty \frac{dt}{t^2 + \sin^2 \alpha} \\ &= \frac{1}{2 \sin \alpha} \int_{1/\tan \alpha}^\infty \frac{dt}{t^2 + 1} \\ &= \frac{1}{2 \sin \alpha} \left( \frac{\pi}{2} - \arctan \left( \frac{1}{\tan \alpha} \right) \right) \end{aligned}$$

である。ここで、 $\tan(\frac{\pi}{2} - \alpha) = \frac{1}{\tan \alpha}$  であることから、結論として次を得る。

$$\iint_D e^{-(x^2+2xy \cos \alpha+y^2)} dx dy = \frac{\alpha}{2 \sin \alpha}$$

## 問 2

複素数  $\alpha$  に対し、3 次複素正方行列  $A(\alpha)$  を次のように定める。

$$A(\alpha) = \begin{pmatrix} \alpha - 4 & \alpha + 4 & -2\alpha + 1 \\ -2 & 2\alpha + 1 & -2\alpha + 2 \\ -1 & \alpha & -\alpha + 2 \end{pmatrix}$$

- (1)  $A(\alpha)$  の行列式を求めよ。
- (2)  $A(\alpha)$  の階数を求めよ。

解答.

- (1) ある行に別の行の定数倍を足す操作を繰り返し行っていくと

$$\begin{aligned} A(\alpha) &\sim \begin{pmatrix} \alpha - 3 & 4 & -\alpha - 1 \\ 0 & 1 & -2 \\ -1 & \alpha & -\alpha + 2 \end{pmatrix} \\ &\sim \begin{pmatrix} \alpha - 3 & 0 & -\alpha + 7 \\ 0 & 1 & -2 \\ -1 & 0 & \alpha + 2 \end{pmatrix} \\ &\sim \begin{pmatrix} 0 & 0 & (\alpha - 1)^2 \\ 0 & 1 & -2 \\ -1 & 0 & \alpha + 2 \end{pmatrix} \end{aligned}$$

と変形できる。よって  $\det A(\alpha) = (\alpha - 1)^2$  である。

- (2)  $\alpha = 1$  のときは階数 2 である。それ以外のときは正則で、階数は 3 である。



### 問 3

$(x_0, y_0) \in \mathbb{R}^2 \setminus \{(0, 0)\}$  に対して、 $\mathbb{R}$  上の連立常微分方程式

$$\begin{cases} \frac{dx}{dt} = -x^2y - y^3 \\ \frac{dy}{dt} = x^3 + xy^2 \end{cases} \quad \begin{cases} x(0) = x_0 \\ y(0) = y_0 \end{cases}$$

の解  $(x(t), y(t))$  は周期を持つことを示し、最小の周期を求めよ。ただし正の実数  $T$  が  $(x(t), y(t))$  の周期であるとは、任意の  $t \in \mathbb{R}$  に対して

$$(x(t+T), y(t+T)) = (x(t), y(t))$$

が成り立つことである。

解答. 与式より

$$\begin{aligned} x \frac{dx}{dt} + y \frac{dy}{dt} &= 0 \\ \frac{d}{dt}(x^2 + y^2) &= 0 \end{aligned}$$

を得る。したがって  $C = x^2 + y^2$  は定数であり、 $C = x_0^2 + y_0^2$  が成り立つ。ゆえに与式は

$$\begin{cases} \frac{dx}{dt} = -Cy \\ \frac{dy}{dt} = Cx \end{cases}$$

と書き直せる。この連立方程式を一変数にまとめると

$$\frac{d^2x}{dt^2} = -C^2x$$

となるが、この解空間は  $\cos(Ct)$  と  $\sin(Ct)$  で張られる。したがって、一般解はこの線形結合で書けるのだから

$$\begin{aligned} x(t) &= x_0 \cos(Ct) - y_0 \sin(Ct) \\ y(t) &= y_0 \cos(Ct) + x_0 \sin(Ct) \end{aligned}$$

でなくてはならない。常微分方程式の初期値問題の解の一意性より、解はこれだけである。よって求める周期は  $2\pi/C$  である。

問 4

$f$  は  $\mathbb{R}$  上の実数値  $C^1$  級関数で任意の  $x \in \mathbb{R}$  に対して  $f(x+1) = f(x)$  を満たすとする。このとき以下の 2 条件は同値であることを示せ。

(A) 広義積分

$$\int_1^{\infty} \frac{1}{x^{1+f(x)^2}} dx$$

が収束する。

(B)  $f(x) = 0$  となる  $x \in \mathbb{R}$  が存在しない。

解答.

(B) $\Rightarrow$ (A) このときある  $\varepsilon > 0$  が存在して  $\forall x f(x)^2 > \varepsilon$  が成り立つ。よって

$$\int_1^{\infty} \frac{1}{x^{1+f(x)^2}} dx \leq \int_1^{\infty} \frac{dx}{x^{1+\varepsilon}} \leq \frac{1}{\varepsilon}$$

より積分は有界である。被積分関数は正の値しかとらないので、これで広義積分の収束がいえた。

(A) $\Rightarrow$ (B) 対偶を示そう。 $f(a) = 0$  なる  $a$  があったとする。周期性から  $f(a_1) = 0$  なる  $1 \leq a_1 < 2$  がとれる。 $n \geq 2$  に対し  $n \leq a_n < n+1$  を  $a_n = a_1 + n - 1$  で定める。 $f(x) = f(x+1)$  より、 $f$  はコンパクト空間  $\mathbb{R}/\mathbb{Z}$  上の  $C^1$  級関数である。とくに  $f'$  は有界であり、 $\forall x |f'(x)| \leq M$  なる  $M > 0$  をとることができる。したがって平均値の定理を適用することにより、任意の  $n$  について

$$|f(x)| = |f(x) - f(a_n)| \leq M |x - a_n|$$

が成り立つことがわかる。ここまでの議論を踏まえると次の補題が示せる。

補題. ある  $r > 0$  が存在して、任意の自然数  $n \geq 2$  に対して

$$\int_{2n-2}^{2n} x^{-f(x)^2} dx \geq \frac{r}{\sqrt{\log 2n}}$$

が成り立つ。

証明. 以下のように計算できる。

$$\begin{aligned} \int_{2n-2}^{2n} x^{-f(x)^2} dx &\geq \int_{2n-2}^{2n} \exp \{ -(\log x) f(x)^2 \} dx \\ &\geq \int_{2n-2}^{2n} \exp \{ -(\log 2n) f(x)^2 \} dx \\ &\geq \int_{a_{2n-2}}^{a_{2n-2}+1} \exp \{ -(\log 2n) f(x)^2 \} dx \\ &\geq \int_{a_{2n-2}}^{a_{2n-2}+1} \exp \{ -M^2 (\log 2n) (x - a_{2n-2})^2 \} dx \\ &\geq \int_{a_{2n-2}}^{a_{2n-2}+1} \exp \{ -(M \sqrt{\log 2n} (x - a_{2n-2}))^2 \} dx \end{aligned}$$

変数変換  $y = M\sqrt{\log 2n}(x - a_{2n-2})$  を行つて

$$\begin{aligned} \int_{2n-2}^{2n} x^{-f(x)^2} dx &\geq \frac{1}{M\sqrt{\log 2n}} \int_0^{M\sqrt{\log 2n}} e^{-y^2} dy \\ &\geq \frac{1}{M\sqrt{\log 2n}} \int_0^{M\sqrt{\log 4}} e^{-y^2} dy \end{aligned}$$

したがって

$$r = \frac{1}{M} \int_0^{M\sqrt{\log 4}} e^{-y^2} dy$$

とおけばよい。 □

(A) $\Rightarrow$ (B) の証明に戻る。  $R \geq 4$  に対し、  $4 \leq 2N \leq R$  を満たす最大の  $N \in \mathbb{Z}$  を  $N_R$  とおく。すると

$$\begin{aligned} \int_1^R \frac{dx}{x^{1+f(x)^2}} &\geq \sum_{n=2}^{N_R} \int_{2n-2}^{2n} \frac{dx}{x^{1+f(x)^2}} \\ &\geq \sum_{n=2}^{N_R} \frac{1}{2n} \int_{2n-2}^{2n} \frac{dx}{x^{f(x)^2}} \\ &\geq \sum_{n=2}^{N_R} \frac{r}{2n\sqrt{\log 2n}} \end{aligned}$$

というように評価できる。さらに  $1/x\sqrt{\log x}$  は単調減少なので

$$\begin{aligned} \int_1^R \frac{dx}{x^{1+f(x)^2}} &\geq r \int_2^{N_R+1} \frac{dx}{2x\sqrt{\log 2x}} \\ &\geq \frac{r}{2} \int_4^{2N_R+2} \frac{dy}{y\sqrt{\log y}} \\ &\geq r(\sqrt{\log(2N_R+2)} - \sqrt{\log 4}) \\ &\geq r(\sqrt{R} - \sqrt{\log 4}) \end{aligned}$$

である。ゆえに結論が従う。

問 5

$n$  を 2 以上の整数、 $A$  を  $n$  次複素正方行列とする。 $A^{n-1}$  は対角化可能でないが、 $A^n$  が対角化可能であるとき、 $A^n = 0$  となることを示せ。

解答.  $\mathbb{C}$  係数なので、Jordan 標準形が存在する。 $A$  ははじめから Jordan 標準形であるとしてよい。

$$A = \bigoplus_{i=1}^r J_{\lambda_i}(a_i)$$

とする。 $a_1, \dots, a_r$  は (異なるとは限らない) 固有値であり、 $\lambda_i$  はそれぞれのジョルダン細胞のサイズである。

$$A^n = \bigoplus_{i=1}^r J_{\lambda_i}(a_i)^n$$

は対角化可能なので、各  $J_{\lambda_i}(a_i)^n$  も対角化可能。ここで  $J_{\lambda_i}(a_i)$  の Jordan 分解

$$S_i = \begin{pmatrix} a_i & & \\ & \ddots & \\ & & a_i \end{pmatrix} \quad N_i = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}$$

を考える。

$$J_{\lambda_i}(a_i)^n = S_i^n + \sum_{k=1}^n \binom{n}{k} S_i^{n-k} N_i^k$$

であって、 $S_i^n$  は対角行列で  $\sum_{k=1}^n \binom{n}{k} S_i^{n-k} N_i^k$  はべき零行列だから、Jordan 分解の一意性より

$$\sum_{k=1}^n \binom{n}{k} S_i^{n-k} N_i^k = 0$$

を得る。左辺は具体的に書くことができ、次のような  $\lambda_i$  次行列

$$\begin{pmatrix} 0 & \binom{n}{1}a_i^{n-1} & \binom{n}{2}a_i^{n-2} & \cdots & \binom{n}{\lambda_i-1}a_i \\ & 0 & \binom{n}{1}a_i^{n-1} & \cdots & \binom{n}{\lambda_i-2}a_i^2 \\ & & \ddots & & \vdots \\ & & & & 0 \end{pmatrix}$$

である。 $\lambda_i = 1$  のときにはこの等式から情報を得ることはできない。しかし  $\lambda_i \geq 2$  ならば  $a_i = 0$  であることがわかる。つまりサイズが 2 以上の Jordan 細胞はべき零である。実はサイズが 1 の Jordan 細胞は存在しない。ハイリホーで示す。仮に存在したとする。 $n \geq 2$  という仮定より、このときサイズが 2 以上の Jordan 細胞のサイズは  $n-1$  以下でなくてはならない。したがって、サイズが 2 以上の Jordan 細胞はすべて  $n-1$  乗するとゼロである。よって  $A^{n-1}$  は対角化可能となるが、これは仮定に反しており矛盾。ゆえにサイズが 1 の Jordan 細胞は存在しないことが判るので、 $A$  の Jordan 細胞はことごとくべき零であり、 $A^n = 0$  であることが導かれる。

## 問 6

$\mathbb{R}^2$  上の実数値連続関数  $f$  についての次の条件 (\*) を考える。

(\*) 任意の正の実数  $R$  に対して、次の集合は有界である。

$$\{(x, y) \in \mathbb{R}^2 \mid |f(x, y)| \leq R\}$$

以下の問に答えよ。

- (1) 条件 (\*) をみたす連続関数  $f$  の例を与え、それが (\*) をみたすことを示せ。
- (2) 連続関数  $f$  が条件 (\*) を満たすとき、次のいずれかが成り立つことを示せ。
  - (a)  $f$  は最大値を持つが、最小値は持たない。
  - (b)  $f$  は最小値を持つが、最大値は持たない。

解答.

- (1) たとえば  $f(x, y) = x^2 + y^2$  とすればよい。これが (\*) を満たすことはあきらか。
- (2)  $f$  が条件 (\*) を満たすとする。 $f$  の可能性としては、次の 4 通りが考えられる。

- (A1)  $f$  は上にも下にも有界
- (A2)  $f$  は上に有界だが下に有界でない
- (A3)  $f$  は下に有界だが上に有界でない
- (A4)  $f$  は上にも下にも有界でない

それぞれの場合について考えていく。まず (A1) の場合、任意の  $x$  について  $|f(x)| \leq M$  なる  $M > 0$  が存在する。よって仮定より、 $\mathbb{R}^2$  が有界となって矛盾。つまりそんな関数はない。

次に (A2) の場合。  $\sup f(x) = R$  とする。仮定から集合

$$V = \{(x, y) \in \mathbb{R}^2 \mid |f(x, y)| \leq R\}$$

は有界閉集合である。よって  $V$  はコンパクト。 $f(V)$  もコンパクトなので、 $f(V)$  は最大値  $M$  を持つ。あきらかに  $M \leq R$  である。任意に  $0 < \varepsilon \leq R/2$  が与えられたとしよう。 $\sup f(x) = R$  より  $R - \varepsilon < f(z)$  なる  $z$  がある。このとき  $z \in V$  だから  $R - M \leq \varepsilon$  であり、 $0 < \varepsilon \leq R/2$  は任意だったから  $R \leq M$  でなくてはならない。よって  $R = M$  であり、 $f$  は最大値を持つが、最小値は持たない関数である。(A3) は (A2) と同様で、このとき  $f$  は最小値を持つが最大値を持たない。

残る (A4) について考えよう。 $K = \{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\}$  とすると、仮定から  $K$  は有界閉集合である。 $M$  を十分に大きな正の実数として、 $K$  をすっぽり含むような閉円板  $B = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq M\}$  をとることができる。 $\mathbb{R}^2$  を全体として補集合をとることになると、このとき  $B^c$  は連結開集合である。

$$U = \{(x, y) \in \mathbb{R}^2 \mid f(x, y) > 0\} \quad V = \{(x, y) \in \mathbb{R}^2 \mid f(x, y) < 0\}$$

とおく。このとき  $U$  と  $V$  の共通部分は空であり、ともに開集合である。だから、 $B^c = (U \cap B^c) \cup (V \cap B^c)$  から、 $B^c$  が連結集合であることに矛盾。よってそのような関数はない。以上により示すべきことがいえた。

問 7

2 以上の整数  $n$  に対し、 $(i, j)$  成分が  $|i - j|$  となる  $n$  次正方行列を  $A_n$  とする。すなわち

$$A_n = \begin{pmatrix} 0 & 1 & 2 & \cdots & n-1 \\ 1 & 0 & 1 & \cdots & n-2 \\ 2 & 1 & 0 & \cdots & n-3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n-1 & n-2 & n-3 & \cdots & 0 \end{pmatrix}$$

とする。 $A_n$  の行列式を求めよ。

解答.  $n \leq 4$  のときに具体的に求めることは省略する。説明の都合上、 $n \geq 5$  とする。行または列に関する基本変形によって行列式は不変であることを利用しよう。1 列目に  $n$  列目を足すと

$$\det A_n = \det \begin{pmatrix} n-1 & 1 & 2 & \cdots & n-1 \\ n-1 & 0 & 1 & \cdots & n-2 \\ n-1 & 1 & 0 & \cdots & n-3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n-1 & n-2 & n-3 & \cdots & 0 \end{pmatrix}$$

のように数字が揃えられる。1 行目を 2 行目以降から引くことにより、ある  $n-1$  次正方行列  $B_n$  に関して

$$\det A_n = (n-1) \det \begin{pmatrix} 1 & * \\ 0 & B_n \end{pmatrix}$$

という形になる。ここで  $B_n$  の  $(i, j)$  成分を  $b_{i,j}$  とすると

$$b_{i,j} = |i - j| - j = \begin{cases} -i & (i \leq j, \text{上半分}) \\ i - 2j & (i \geq j, \text{下半分}) \end{cases}$$

である。つまり、具体的に書けば

$$B_n = \begin{pmatrix} -1 & -1 & -1 & \cdots & -1 \\ 0 & -2 & -2 & \cdots & -2 \\ 1 & -1 & -3 & \cdots & -3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n-3 & n-5 & n-7 & \cdots & -(n-1) \end{pmatrix}$$

ということである。 $B_n$  の 1 行目の  $i-2$  倍を  $i$  行目に加えることにより、ある  $n-2$  次正方行列  $C_n$  に関して

$$B_n \sim \begin{pmatrix} -1 & * \\ 0 & C_n \end{pmatrix}$$

という形になる。ここで  $C_n$  の  $(i, j)$  成分を  $c_{i,j}$  とすると

$$\begin{aligned} c_{i,j} &= b_{i+1,j+1} - (i-1) \\ &= \begin{cases} -2i & (i \leq j, \text{上半分}) \\ -2j & (i \geq j, \text{下半分}) \end{cases} \end{aligned}$$

が成り立つ。つまり、具体的に書けば

$$C_n = \begin{pmatrix} -2 & -2 & -2 & \cdots & -2 \\ -2 & -4 & -4 & \cdots & -4 \\ -2 & -4 & -6 & \cdots & -6 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -2 & -4 & -6 & \cdots & -2(n-2) \end{pmatrix}$$

ということである。この行列は行基本変形で対角成分がすべて  $-2$  であるような上三角行列に変形できる。したがって  $\det C_n = (-2)^{n-2}$  である。ゆえに

$$\det A_n = (n-1) \det B_n = (n-1)(-1) \det C_n = -(n-1)(-2)^{n-2}$$

である。 $n \geq 5$  という仮定は  $C_n$  があまり小さくならないようにするためだけの仮定であり、この式は一般に成り立つ。そのことの確認は読者に任せる。

## 平成 31 年度 専門科目

### 問 1

$\mathbb{R}[X, Y]$  を変数  $X, Y$  に関する実数係数の 2 変数多項式環とする。 $I$  を  $X^2 + Y^2$  で生成された  $\mathbb{R}[X, Y]$  のイデアルとする。 $A = \mathbb{R}[X, Y]/I$  とおく。このとき、以下の問に答えよ。

- (i)  $A$  は整域であることを示せ。
- (ii)  $A$  の商体を  $K$  とおき、 $A$  の  $K$  における整閉包を  $B$  とおく。 $A$  加群としての  $B$  の生成系を一組与えよ。

解答.

- (i)  $\mathbb{R}[X, Y]$  は UFD なので、 $X^2 + Y^2$  が既約元であることを示せばよい。ハイリホーによる。可約であると仮定しよう。そうするとある実数  $a, b, c, d$  が存在して  $X^2 + Y^2 = (aX + bY)(cX + dY)$  が成り立つことになるが、その場合  $ac - 1 = ad + bc = bd - 1 = 0$  でなくてはならない。これは  $a, b, c, d$  が実数であったことに矛盾。よって  $X^2 + Y^2$  は既約元であり、 $I \subset \mathbb{R}[X, Y]$  は素イデアル。
- (ii)  $a = Y/X$  とする。 $a^2 + 1 = 0$  なので  $a \in B$  である。 $B = A[a]$  を示そう。それには、 $A[a]$  が整閉であることを示せば十分である。 $\mathbb{R}$  代数の準同形  $\varphi: \mathbb{R}[X, \sqrt{-1}] \rightarrow A[a]$  を  $\varphi(\sqrt{-1}) = a, \varphi(X) = X$  で定める。これは well-defined であり、あきらかに全射。  
また逆写像が構成できるので  $\varphi$  は単射。よって  $\varphi$  は同型であり、 $A[a] \cong \mathbb{R}[X, \sqrt{-1}] \cong \mathbb{C}[X]$  である。 $\mathbb{C}[X]$  は PID であり、とくに UFD でもあるから整閉である。よって  $A[a]$  も整閉だから  $B = A[a]$  が示された。よって、 $B$  の  $A$  加群としての生成系としては  $\{1, a\}$  がとれる。



## 問 2

有限群  $G$  に対して、次の条件 (\*) を考える。

(\*) 任意の正整数  $n$  に対して、 $G$  の部分群のうち、位数が  $n$  のものの個数は 1 以下である。

以下の問に答えよ。

- (i)  $G$  は有限 Abel 群で (\*) を満たすとする。このとき、 $G$  は巡回群であることを示せ。
- (ii)  $G$  は有限群で (\*) を満たすとする。 $H$  を  $G$  の正規部分群とする。このとき、 $G/H$  も (\*) を満たすことを示せ。
- (iii)  $G$  は有限群で (\*) を満たすとする。このとき、 $G$  は巡回群であることを示せ。

証明.

- (i) ハイリホーによる。(\*) を満たし巡回群でない  $G$  があったとする。有限生成 Abel 群の構造定理により  $G$  は巡回群の直和で表されており、

$$G = \bigoplus_{i=1}^t \mathbb{Z}/m_i\mathbb{Z}$$

なる  $m_i$  がある。 $G$  は巡回群ではないので  $t \geq 2$  であり、中国剰余定理により  $m_i$  のなかには少なくとも一組互いに素でないものがある。その最大公約数を  $e$  とすると、 $G$  は位数  $e$  の部分群を少なくとも二つもつことになり矛盾。よって示せた。

- (ii)  $G/H$  の部分群全体  $X$  と、 $G$  の  $H$  を含む部分群全体  $Y$  の間には全単射がある。それは自然な写像  $\pi: G \rightarrow G/H$  を用いて次のようにあらわせる。

$$\begin{aligned} X &\rightarrow Y \text{ s.t. } M \mapsto \pi^{-1}(M) \\ Y &\rightarrow X \text{ s.t. } K \mapsto \pi(K) \end{aligned}$$

この全単射により、位数が等しい部分群の組は位数が等しい部分群の組に送られるため、これで示すことができる。

- (iii)  $G$  の部分群  $H$  と  $g \in G$  に対して、 $gHg^{-1} = H$  でなくてはならないため、 $H$  は正規部分群であることに注意しておく。そうすると、 $G$  の Sylow- $p$  部分群はどの  $p$  についても正規部分群である。そこで  $\#G$  の異なる素因子を  $p_1, \dots, p_t$  として対応する Sylow 部分群を  $H_i$  とする。任意の  $i, j$  について交換子  $[H_i, H_j]$  は  $H_i \cap H_j = 1$  の部分集合だから、異なる  $H_i$  の元同士は可換である。よって積をとる写像  $\prod_{i=1}^t H_i \rightarrow G$  は準同形であり、全射であり、位数の考察から全単射でもある。位数が互いに素な巡回群の直積は巡回群なので、 $G$  ははじめから  $p$  群であるとしてよい。

$\#G = p^e$  とする。 $e$  についての帰納法で示そう。 $e = 1$  ならば  $G$  はあきらかに巡回群であるから  $e \geq 2$  とする。よく知られているように、 $p$  群の中心は自明ではない。(雪江 [1] 命題 4.4.3) そこで位数  $p$  の元  $\pi \in Z(G)$  が存在することがわかる。 $G/\langle \pi \rangle$  は (ii) と帰納法の仮定により巡回群である。 $G/\langle \pi \rangle$  の生成元の代表元として  $\sigma \in G$  をとる。そうすると積をとる写像  $\langle \pi \rangle \times \langle \sigma \rangle \rightarrow G$  は準同形でありかつ全射で、位数の考察から全単射でもある。ゆえに  $G \cong \langle \pi \rangle \times \langle \sigma \rangle$  だから  $G$  は Abel 群であり、したがって (i) より巡回群である。よって帰納法は回り、示すべきことが言えた。

□

### 問 3

多項式  $f(X) = X^4 + 6X^2 + 2 \in \mathbb{Q}[X]$  の  $\mathbb{Q}$  上の最小分解体を  $K$  とおく。  $K$  を  $\mathbb{C}$  の部分体とみなし、  $F = K \cap \mathbb{R}$  とおく。このとき、次の間に答えよ。

- (i) 拡大次数  $[F : \mathbb{Q}]$  を求めよ。
- (ii)  $F/\mathbb{Q}$  は Galois 拡大であることを示せ。

証明. 以下この解答では  $[\mathbb{Q}(\sqrt{2}, \sqrt{7}) : \mathbb{Q}] = 4$  は認めて使う。

- (i)  $X^4 + 6X^2 + 2$  は複 2 次式なので因数分解ができる。

$$\begin{aligned} X^4 + 6X^2 + 2 &= (X^2 + 3)^2 - 7 \\ &= (X^2 + 3 + \sqrt{7})(X^2 + 3 - \sqrt{7}) \end{aligned}$$

なので、この多項式の根は  $\pm i\sqrt{3 \pm \sqrt{7}}$  である。  $\alpha = i\sqrt{3 + \sqrt{7}}$ ,  $\beta = i\sqrt{3 - \sqrt{7}}$  とおく。  $K = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \sqrt{2})$  である。

$$\begin{array}{ccccc} \mathbb{Q}(\sqrt{2}) & \longrightarrow & F & \longrightarrow & K \\ \uparrow & & \uparrow & & \uparrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}(\sqrt{7}) & \longrightarrow & \mathbb{Q}(\alpha) \end{array}$$

多項式  $f(X)$  は  $p = 2$  に関する Eisenstein 多項式だから  $\mathbb{Q}[X]$  の元として既約。ゆえに  $f(X)$  は  $\alpha$  の  $\mathbb{Q}$  上の最小多項式であるから  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$  である。さらに  $[K : \mathbb{Q}] = 8$  であることを示そう。  $K = \mathbb{Q}(\alpha, \sqrt{2})$  なので  $\sqrt{2} \notin \mathbb{Q}(\alpha)$  を示せばよい。ハイリホーでこれを示す。仮に  $\sqrt{2} \in \mathbb{Q}(\alpha)$  だったとする。このときある  $b, c \in \mathbb{Q}(\sqrt{7})$  が存在して

$$\sqrt{2} = b\alpha + c$$

である。この式から

$$\begin{cases} bc = 0 \\ c^2 - (3 + \sqrt{7})b^2 = 2 \end{cases}$$

を得る。  $bc = 0$  より  $b = 0$  または  $c = 0$  である。  $b = 0$  なら  $\sqrt{2} \in \mathbb{Q}(\sqrt{7})$  ということになり矛盾。  $c = 0$  なら  $N : \mathbb{Q}(\sqrt{7}) \rightarrow \mathbb{Q}$  をノルムとすると  $2 = N(b)^2$  となり  $\sqrt{2} \in \mathbb{Q}$  となって矛盾。いずれにせよ矛盾が得られたので、  $\sqrt{2} \notin \mathbb{Q}(\alpha)$  が示せた。よって  $[K : \mathbb{Q}] = 8$  である。

一方で  $\mathbb{Q}(\sqrt{7}, \sqrt{2}) \subset F$  より  $[F : \mathbb{Q}] \geq 4$  である。かつ  $F \subsetneq K$  から  $[F : \mathbb{Q}] < 8$  なので、  $[F : \mathbb{Q}] = 4$  でなくてはならない。

- (ii) 包含関係があつて  $\mathbb{Q}$  上の次元が同じなので  $F = \mathbb{Q}(\sqrt{7}, \sqrt{2})$  である。  $\mathbb{Q}$  は標数 0 なので完全体であり、したがって  $F/\mathbb{Q}$  は分離拡大。かつ  $F$  を  $\mathbb{Q}$  上生成する  $\sqrt{7}$  と  $\sqrt{2}$  の共役はすべて  $F$  に含まれているので、  $F/\mathbb{Q}$  は Galois 拡大である。

□

問 4

$n \geq 2$  に対して、

$$S^{n-1} = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid x_1^2 + \dots + x_n^2 = 1\} \quad \mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

とし、写像  $\Phi: S^{n-1} \times \mathbb{S}^1 \rightarrow \mathbb{C}^n$  を

$$\Phi(x_1, \dots, x_n) = (x_1 z, \dots, x_n z)$$

と定める。

- (1)  $\Phi$  の像  $M$  が  $\mathbb{C}^n$  の実  $n$  次元部分多様体であることを示せ。
- (2)  $n$  が偶数のとき、 $M$  が向き付け可能であることを示せ。

解答.

- (1)  $\Phi(x, z) = \Phi(y, w)$  とする。すると  $\forall i \ x_i z = y_i w$  である。 $S^{n-1}$  の定義により  $x_i \neq 0$  なる  $i$  がある。よって  $z/w = y_i/x_i \in \mathbb{R}$  であるので、 $z = w$  または  $z = -w$  である。したがって  $w \in M$  に対して  $\#\Phi^{-1}(w) = 2$  であることが分かった。

$N = S^{n-1} \times \mathbb{S}^1$  とおく。 $N$  に  $(x, z) \sim (-x, -z)$  で生成される同値関係  $\sim$  を定義する。このとき  $\Phi(x, z) = \Phi(y, w)$  と  $(x, z) \sim (y, w)$  は同値である。ゆえに次の図式

$$\begin{array}{ccc} N & \xrightarrow{\Phi} & M \\ P \downarrow & \nearrow \tilde{\Phi} & \\ N/\sim & & \end{array}$$

を可換にするような全単射連続写像  $\tilde{\Phi}$  がある。 $N/\sim$  はコンパクトで、 $M$  は Hausdorff なので  $\tilde{\Phi}$  は同相でなければならない。したがって  $M$  の代わりに  $N/\sim$  が  $n$  次元位相多様体であることをいえばよいが、 $P$  が被覆写像であるためこれはあきらか。

- (2)  $n$  は偶数と仮定されているので  $n = 2k$  とおける。接ベクトル束  $TM$  の切断  $s$  であって、至る所ゼロでないものの存在をいえば十分である。 $\beta = (x, z) \in N$  に対して

$$\tilde{z} = (x_2, -x_1, \dots, x_{2k}, -x_{2k-1}, -y_2, y_1)$$

と定めておき、これによりベクトル場  $N \rightarrow TN$  s.t.  $z \mapsto (z, \tilde{z})$  を定める。このベクトル場は  $N/\sim$  上のベクトル場を誘導し、あきらかに至る所ゼロでない。よって示せた。

問 5

$\mathbb{C}$  の部分空間

$$X = \{1 - e^{i\theta} \in \mathbb{C} \mid 0 \leq \theta < 2\pi\} \cup \{-1 + e^{i\theta} \in \mathbb{C} \mid 0 \leq \theta < 2\pi\}$$

を考える。整数  $p, q$  に対して、写像  $f: X \rightarrow X$  を

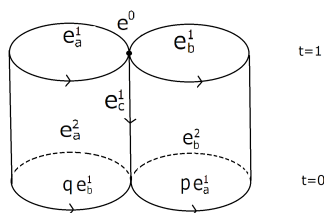
$$\begin{aligned} f(1 - e^{i\theta}) &= -1 + e^{ip\theta} \\ f(-1 + e^{i\theta}) &= 1 - e^{iq\theta} \end{aligned}$$

で定め、 $X \times [0, 1]$  に

$$(x, 0) \sim (f(x), 1)$$

$(x \in X)$  で生成される同値関係  $\sim$  を与える。商空間  $Y = (X \times [0, 1])/\sim$  の整数係数ホモロジー群を計算せよ。

解答．セル複体を使ってホモロジーを求めよう。空間  $Y$  を直接書くことは難しいが、次のようなものを想像することはできる。



この対になった円筒は、 $X \times I$  および  $Y$  を表している。上下の円盤に見える部分は円周であり、ちくわを2つつくつけたような形をしている。側面も輪郭しか書かれていないが、面になっている。垂直方向が  $I$  成分を表しており、上が  $t = 1$  で下が  $t = 0$  であるものとしよう。また右を実軸のプラス方向、奥を虚軸のプラス方向とする。上部にある点は原点を表す。図に  $e$  と書かれているのはセルである。それぞれ具体的には次のように与えられる。

$$\begin{aligned} e^0 &= (0, 1) \\ e_a^1 &= \{(-1 + e^{i\theta}, 1) \mid 0 < \theta < 2\pi\} \\ e_b^1 &= \{(1 - e^{i\theta}, 1) \mid 0 < \theta < 2\pi\} \\ e_c^1 &= \{(0, t) \mid 0 < t < 1\} \\ e_a^2 &= \{(-1 + e^{i\theta}, t) \mid 0 < \theta < 2\pi, 0 < t < 1\} \\ e_b^2 &= \{(1 - e^{i\theta}, t) \mid 0 < \theta < 2\pi, 0 < t < 1\} \end{aligned}$$

このとき、次に注意する。

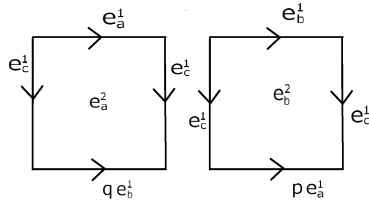
$$\begin{aligned} e^0 &= (0, 0) \\ pe_a^1 &= \{(1 - e^{i\theta}, 0) \mid 0 < \theta < 2\pi\} \\ qe_b^1 &= \{(-1 + e^{i\theta}, 0) \mid 0 < \theta < 2\pi\} \end{aligned}$$

さて以上の準備の下セル複体のホモロジーを計算しよう。 $Y$  の 0 セル、1 セル、2 セルの数はそれぞれ 1, 3, 2

個なので

$$0 \longrightarrow \mathbb{Z}^2 \xrightarrow{\partial} \mathbb{Z}^3 \xrightarrow{\sigma} \mathbb{Z} \longrightarrow 0$$

という図式に表されるような状況になっている。まず  $\sigma$  だが、0 セルはただひとつしかないのでこれはゼロ写像である。よって  $H_0(Y) = \mathbb{Z}$  がわかる。次に  $\partial$  を計算する。次の図



のような状況になっているので

$$\partial(e_a^2) = e_a^1 - q e_b^1 \quad \partial(e_b^2) = e_b^1 - p e_a^1$$

である。したがって  $\partial$  は次の行列

$$\partial = \begin{pmatrix} 1 & -p \\ -q & 1 \\ 0 & 0 \end{pmatrix}$$

で表される写像である。この行列の階数は  $pq = 1$  のとき 1 でそうでないとき 2 である。よって  $pq = 1$  のとき

$$\begin{aligned} H_1(Y) &= \mathbb{Z}^3 / \text{Im } \partial \\ &= \mathbb{Z}^2 \\ H_2(Y) &= \text{Ker } \partial \\ &= \mathbb{Z} \end{aligned}$$

である。 $pq \neq 1$  ならば

$$\begin{aligned} H_1(Y) &= \mathbb{Z}^3 / \text{Im } \partial \\ &= (a\mathbb{Z} \oplus b\mathbb{Z} \oplus c\mathbb{Z}) / (a - qb, b - pa) \\ &= (a\mathbb{Z} \oplus b\mathbb{Z}) / ((1 - pq)a, b - pa) \oplus c\mathbb{Z} \\ &= \mathbb{Z} / (1 - pq)\mathbb{Z} \oplus \mathbb{Z} \\ H_2(Y) &= \text{ker } \partial \\ &= 0 \end{aligned}$$

である。以上により求めるホモロジーは、 $pq = 1$  のとき

$$H_i(Y) = \begin{cases} \mathbb{Z} & (i = 0, 2) \\ \mathbb{Z}^2 & (i = 1) \\ 0 & (\text{otherwise}) \end{cases}$$

であり、 $pq \neq 1$  のとき

$$H_i(Y) = \begin{cases} \mathbb{Z} & (i = 0) \\ \mathbb{Z} / (pq - 1)\mathbb{Z} \oplus \mathbb{Z} & (i = 1) \\ 0 & (\text{otherwise}) \end{cases}$$

## ■ 平成 30 年度 基礎科目

---

### 問 1

広義積分

$$\iiint_V \frac{1}{(1+x^2+y^2)z^{\frac{3}{2}}} dx dy dz$$

を計算せよ。ただし、 $V = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 \leq z\}$  とする。

解答. 極座標変換  $(x, y, z) \mapsto (r, \theta, z)$  を考える。このとき  $dx dy dz = r dr d\theta dz$  であり、

$$\begin{aligned} \iiint_V \frac{1}{(1+x^2+y^2)z^{\frac{3}{2}}} dx dy dz &= \int_0^{2\pi} d\theta \int_0^\infty \frac{r}{1+r^2} \left( \int_{r^2}^\infty z^{-\frac{3}{2}} dz \right) dr \\ &= 2\pi \int_0^\infty \frac{r}{1+r^2} \left[ (-2)z^{-\frac{1}{2}} \right]_{r^2}^\infty dr \\ &= 4\pi \int_0^\infty \frac{r}{1+r^2} \frac{1}{r} dr \\ &= 4\pi \int_0^\infty \frac{1}{1+r^2} dr \\ &= 4\pi \cdot \frac{\pi}{2} \\ &= 2\pi^2 \end{aligned}$$

と計算できる。

## 問 2

$a, b$  を実数とする。実行列

$$A = \begin{pmatrix} 1 & 1 & a & b \\ 0 & 1 & 2 & 0 \\ 2 & 0 & 1 & 4 \end{pmatrix}$$

について、以下の問に答えよ。

- (1) 行列  $A$  の階数を求めよ。
- (2) 連立 1 次方程式

$$A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

が解を持つような実数  $a, b$  をすべて求めよ。

解答.

- (1) ある行に別の行の定数倍を足す操作を繰り返すと

$$\begin{aligned} A &\sim \begin{pmatrix} 1 & 1 & a & b \\ 0 & 1 & 2 & 0 \\ 0 & -2 & 1-2a & 4-2b \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 1 & a & b \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 5-2a & 4-2b \end{pmatrix} \end{aligned}$$

と変形できる。したがって  $\text{rank } A \geq 2$  であり、 $(a, b) = (\frac{5}{2}, 2)$  のときは  $\text{rank } A = 2$  で、 $(a, b) \neq (\frac{5}{2}, 2)$  のときは  $\text{rank } A = 3$  である。

- (2)  $(a, b) \neq (\frac{5}{2}, 2)$  ならば、 $A: \mathbb{R}^4 \rightarrow \mathbb{R}^3$  は全射なので、解がある。 $(a, b) = (\frac{5}{2}, 2)$  のとき、拡大係数行列を考えると

$$\begin{pmatrix} 1 & 1 & \frac{5}{2} & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 4 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & \frac{5}{2} & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 \\ 0 & -2 & -4 & 0 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & \frac{5}{2} & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

となるので、解はない。

### 問 3

広義積分

$$\int_{-\infty}^{\infty} \frac{\cos(\pi x)}{1+x^2+x^4} dx$$

を求めよ。

解答.  $f, F$  を

$$f(x) = \frac{\cos(\pi x)}{1+x^2+x^4}, \quad F(z) = \frac{e^{\sqrt{-1}\pi z}}{1+z^2+z^4}$$

により定める。 $x \in \mathbb{R}$  なら  $f(x) = \operatorname{Re} F(x)$  である。

ここで分母の  $1+z^2+z^4$  を因数分解しておく。 $\zeta = \exp(\sqrt{-1}\pi/3) = (1+\sqrt{-3})/2$  とする。 $1+z+z^2$  の根は 1 の原始 3 乗根であることから

$$\begin{aligned} z^4 + z^2 + 1 &= (z^2 - \zeta^2)(z^2 - \zeta^4) \\ &= (z - \zeta)(z + \zeta)(z - \zeta^2)(z + \zeta^2) \end{aligned}$$

である。

上反平面に含まれる半径  $R$  の半円を  $C_R$  とする。留数定理により、任意の  $R > 1$  について

$$2\pi\sqrt{-1}(\operatorname{Res}_{z=\zeta} F + \operatorname{Res}_{z=\zeta^2} F) = \int_{-R}^R F(x) dx + \int_{C_R} f(z) dz$$

が成り立つ。

ここで、

$$\begin{aligned} \left| \int_{C_R} f(z) dz \right| &\leq \int_0^\pi \left| \frac{R \exp(\sqrt{-1}R\pi e^{\sqrt{-1}\theta})}{1 + R^2 e^{2\sqrt{-1}\theta} + R^4 e^{4\sqrt{-1}\theta}} \right| d\theta \\ &\leq \int_0^\pi \frac{R e^{-R\pi \sin \theta}}{R^4 - R^2 - 1} d\theta \\ &\leq \frac{R}{R^4 - R^2 - 1} \int_0^\pi d\theta \\ &\leq \frac{R\pi}{R^4 - R^2 - 1} \end{aligned}$$

だから、 $R \rightarrow \infty$  のとき  $\int_{C_R} f(z) dz \rightarrow 0$  である。したがって

$$\int_{-\infty}^{\infty} f(x) dx = \operatorname{Re}(2\pi\sqrt{-1}(\operatorname{Res}_{z=\zeta} F + \operatorname{Res}_{z=\zeta^2} F))$$

であることがわかる。



実際に留数を計算しよう。詳細は省略するが、堅実な計算により

$$\begin{aligned}\operatorname{Res}_{z=\zeta} F &= \frac{\exp(\sqrt{-1}\pi \frac{1+\sqrt{-3}}{2})}{(2\zeta)(\zeta-\zeta^2)(\zeta+\zeta^2)} \\ &= \frac{-\sqrt{-1}\exp(-\frac{\sqrt{3}\pi}{2})}{2(1-\zeta^2)} \\ \operatorname{Res}_{z=\zeta^2} F &= \frac{\exp(\sqrt{-1}\pi \frac{-1+\sqrt{-3}}{2})}{(\zeta^2-\zeta)(\zeta^2+\zeta)(\zeta^2+\zeta^2)} \\ &= \frac{-\sqrt{-1}\exp(-\frac{\sqrt{3}\pi}{2})}{2(1+\zeta)}\end{aligned}$$

がわかる。 $\alpha = \exp(-\frac{\sqrt{3}\pi}{2})$  とおこう。すると

$$\begin{aligned}2\pi\sqrt{-1}(\operatorname{Res}_{z=\zeta} F + \operatorname{Res}_{z=\zeta^2} F) &= \alpha\pi \left( \frac{1}{1-\zeta^2} + \frac{1}{1+\zeta} \right) \\ &= \alpha\pi \left( \frac{2-\zeta}{1-\zeta^2} \right) \\ &= \alpha\pi\end{aligned}$$

である。 $\alpha \in \mathbb{R}$  だから、

$$\int_{-\infty}^{\infty} f(x) \, dx = e^{-\frac{\sqrt{3}\pi}{2}} \pi$$

が結論される。

#### 問 4

閉区間  $[0, 1]$  上の実数値関数列  $\{f_n\}_{n=1}^{\infty}$  について、各  $f_n$  は広義単調増加であるものとする。つまり、 $0 \leq x < y \leq 1$  なら、 $f_n(x) \leq f_n(y)$  である。この関数列  $\{f_n\}_{n=1}^{\infty}$  が  $n \rightarrow \infty$  で関数  $f$  に各点収束したとする。

- (1) 任意の  $0 \leq x < y \leq 1$  に対し、不等式

$$\sup_{x \in [x, y]} |f_n(z) - f(z)| \leq \max\{|f_n(x) - f(y)|, |f_n(y) - f(x)|\}$$

を示せ。

- (2) 関数  $f$  が連続であるとき、関数列  $\{f_n\}_{n=1}^{\infty}$  は  $f$  に  $[0, 1]$  上で一様収束することを示せ。

解答.

- (1) まず  $f$  が広義単調増加であることを示す。 $0 \leq x < y \leq 1$  とする。 $\varepsilon > 0$  が与えられたとする。 $f_n$  が  $f$  に各点収束することにより

$$n \geq N(x) \rightarrow |f(x) - f_n(x)| < \varepsilon$$

$$n \geq N(y) \rightarrow |f(y) - f_n(y)| < \varepsilon$$

なる  $N(x), N(y)$  の存在がわかる。したがって  $n \geq \max\{N(x), N(y)\}$  のとき

$$\begin{aligned} f(y) - f(x) + 2\varepsilon &= (f(y) + \varepsilon) - f(x) + \varepsilon \\ &\geq f_n(y) - f(x) + \varepsilon & (-\varepsilon < f(y) - f_n(y) < \varepsilon \text{ より}) \\ &\geq f_n(y) - f_n(x) & (-\varepsilon < f(x) - f_n(x) < \varepsilon \text{ より}) \\ &\geq 0 \end{aligned}$$

がわかる。 $\varepsilon > 0$  は任意だったから、 $f(y) \geq f(x)$  がわかる。つまり  $f$  は広義単調増加である。

したがって任意の  $z \in [x, y]$  に対して

$$f_n(z) - f(z) \leq f_n(y) - f(x)$$

$$f(z) - f_n(z) \leq f(y) - f_n(x)$$

が成り立つので、

$$|f_n(z) - f(z)| \leq \max\{|f_n(x) - f(y)|, |f_n(y) - f(x)|\}$$

である。右辺は  $z$  の取り方によらないので、

$$\sup_{x \in [x, y]} |f_n(z) - f(z)| \leq \max\{|f_n(x) - f(y)|, |f_n(y) - f(x)|\}$$

がいえた。

- (2)  $\varepsilon > 0$  が与えられたとする。 $I = [0, 1]$  はコンパクトなので、 $f$  は一様連続であることまでいえる。そこで

$$|x - y| < \delta \rightarrow |f(x) - f(y)| < \varepsilon$$

なる  $\delta > 0$  がある。この  $\delta$  を固定し、 $B(z) = [z - \delta/3, z + \delta/3] \cap I$  とする。 $\delta > 0$  なので、 $I = \bigcup_{i=1}^m B(z_i)$  なる有限個の  $z_i \in I$  をとることができる。 $B(z_i) = [x_i, y_i]$  と表すことにする。

$f_n$  は  $f$  に各点収束しているので、

$$\begin{aligned} n \geq N(x_i) &\rightarrow |f(x_i) - f_n(x_i)| < \varepsilon \\ n \geq N(y_i) &\rightarrow |f(y_i) - f_n(y_i)| < \varepsilon \end{aligned}$$

なる  $N(x_i), N(y_i)$  がある。そこで

$$n \geq \max\{N(x_1), \dots, N(x_m), N(y_1), \dots, N(y_m)\}$$

とする。このとき

$$\begin{aligned} |f_n(x_i) - f(y_i)| &\leq |f_n(x_i) - f(x_i)| + |f(x_i) - f(y_i)| \\ &\leq 2\varepsilon \\ |f_n(y_i) - f(x_i)| &\leq |f_n(y_i) - f(y_i)| + |f(y_i) - f(x_i)| \\ &\leq 2\varepsilon \end{aligned}$$

が成り立つ。したがって (1) により、不等式評価を端点に押しつけることができ

$$\begin{aligned} \sup_{z \in I} |f_n(z) - f(z)| &\leq \max_{1 \leq i \leq m} \sup_{x \in [x_i, y_i]} |f_n(z) - f(z)| \\ &\leq \max_{1 \leq i \leq m} \max\{|f_n(x_i) - f(y_i)|, |f_n(y_i) - f(x_i)|\} \\ &\leq 2\varepsilon \end{aligned}$$

である。これで一様収束がいえた。

問 5

$p$  を素数とし、 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  を位数  $p$  の有限体とする。行列の乗法による群  $G$  を

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\}$$

で定める。このとき、 $G$  から乗法群  $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$  への準同形写像の個数を求めよ。

解答. 次の事実に注意する。

補題.  $\pi: G \rightarrow G/[G, G]$  は自然な写像とする。すると  $\pi$  が誘導する Abel 群の準同型

$$p: \text{Hom}(G/[G, G], \mathbb{C}^\times) \rightarrow \text{Hom}(G, \mathbb{C}^\times)$$

は同型である。

証明.  $\pi$  は全射なので、 $p$  は単射である。また  $p$  は全射でもある。なぜならば！  $g \in \text{Hom}(G, \mathbb{C}^\times)$  が任意に与えられたとしよう。このとき  $\mathbb{C}^\times$  が Abel 群であることにより、 $[G, G] \subset \text{Ker } g$  が成り立つ。したがって準同型定理により、 $p(f) = g$  となるような  $f \in \text{Hom}(G/[G, G], \mathbb{C}^\times)$  が存在する。ゆえにかくのごとし。これで  $p$  が同型であることがいえた。  $\square$

したがって  $G/[G, G]$  の構造を決定すればよい。そのためにまず  $[G, G]$  を決定する。

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & \delta & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}$$

とおく。 $(\alpha$  は  $a$  と間違えやすいので、 $\delta$  を使った。) 計算すれば、このとき

$$ABA^{-1}B^{-1} = \begin{pmatrix} 1 & 0 & a\gamma - c\delta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

であることが判る。 $a\gamma - c\delta$  は  $\mathbb{F}_p$  全体をわたるので、

$$[G, G] = \left\{ \begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid d \in \mathbb{F}_p \right\}$$

が結論できる。

次に  $G/[G, G]$  の構造を決定したい。

$$E_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

とし、 $E_1, E_2 \in G/[G, G]$  と見なす。

$$E_1^n = \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad E_2^m = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix}$$

なので、 $E_1, E_2$  は位数がちょうど  $p$  である。また、 $C = E_1^n = E_2^m$  とするとき

$$1 = E_1^n E_2^{-m} = \begin{pmatrix} 1 & n & -nm \\ 0 & 1 & -m \\ 0 & 0 & 1 \end{pmatrix}$$

だから  $n = m = 0$  が従う。つまり  $\langle E_1 \rangle \cap \langle E_2 \rangle = 1$  である。 $G/[G, G]$  は Abel 群なので積による準同形  $\langle E_1 \rangle \times \langle E_2 \rangle \rightarrow G/[G, G]$  がある。これは、 $\langle E_1 \rangle \cap \langle E_2 \rangle = 1$  により単射である。位数  $p^2$  の有限群の間の単射なので、とくに同型である。よって  $G/[G, G] \cong \mathbb{F}_p^2$  がわかった。

あとは  $\# \text{Hom}(\mathbb{F}_p^2, \mathbb{C}^\times)$  を求めよう。これは  $\# \text{Hom}(\mathbb{F}_p, \mathbb{C}^\times)$  の 2 乗である。 $\# \text{Hom}(\mathbb{F}_p, \mathbb{C}^\times) = p$  より求める答えは  $p^2$  である。

問 6

$\mathbb{R}^4$  の部分空間  $M$  を

$$M = \{(x, y, z, w) \in \mathbb{R}^4 \mid x^2 + y^2 + z^2 + w^2 = 1, xy + zw = 0\}$$

で定める。

(1)  $M$  が 2 次元微分可能多様体になることを示せ。

(2)  $M$  上の関数  $f$  を

$$f(x, y, z, w) = x$$

で定めるとき、 $f$  の臨界点をすべて求めよ。ただし、 $p \in M$  が  $f$  の臨界点であるとは、 $p$  における  $M$  の局所座標  $(u, v)$  に関して

$$\frac{\partial f}{\partial u}(p) = \frac{\partial f}{\partial v}(p) = 0$$

となることである。

解答.

(1)  $F: \mathbb{R}^4 \rightarrow \mathbb{R}^2$  を

$$F(x, y, z, w) = \begin{pmatrix} x^2 + y^2 + z^2 + w^2 - 1 \\ xy + zw \end{pmatrix}$$

により定める。 $M = F^{-1}(O)$  である。 $p = (x, y, z, w) \in M$  としよう。 $p$  におけるヤコビアンを計算すると

$$JF_p = \begin{pmatrix} 2x & 2y & 2z & 2w \\ y & x & w & z \end{pmatrix}$$

である。ここで  $p \neq O$  より  $\text{rank } JF_p \geq 1$  である。仮に  $\text{rank } JF_p = 1$  ならば、 $JF_p$  の 2 つの行は 1 次従属である。よって、 $p \neq O$  により  $(y, x, w, z) = c(x, y, z, w)$  なる定数  $c \in \mathbb{R}$  がある。このとき  $xy + zw = c(x^2 + z^2) = 0$  となり、 $p \neq O$  に矛盾。よって  $\text{rank } JF_p = 2$  である。ゆえに  $p$  は  $F$  の正則点であり、 $M$  は  $\mathbb{R}^4$  の 2 次元部分多様体。 $F$  は  $\mathbf{C}^\infty$  級なので、 $M$  は微分可能になる。

(2)  $f: M \rightarrow \mathbb{R}$  の  $\mathbb{R}^4$  への自然な拡張を  $\tilde{f}$  とする。このとき  $p \in M$  に対して  $T_p M \subset \mathbb{R}^4$  と見なせば、 $T_p M = \text{Ker } JF_p$  であるから、

$$\begin{aligned} p \text{ が } f \text{ の臨界点} &\iff \text{rank}(df_p: T_p M \rightarrow \mathbb{R}) < 1 \\ &\iff \dim \text{Ker } df_p = 2 \\ &\iff \dim \text{Ker } \begin{pmatrix} JF_p \\ J\tilde{f}_p \end{pmatrix} = 2 \\ &\iff \text{rank} \begin{pmatrix} 2x & 2y & 2z & 2w \\ y & x & w & z \\ 1 & 0 & 0 & 0 \end{pmatrix} = 2 \\ &\iff \text{rank} \begin{pmatrix} 0 & 2y & 2z & 2w \\ 0 & x & w & z \\ 1 & 0 & 0 & 0 \end{pmatrix} = 2 \end{aligned}$$

である。いま  $p = (x, y, z, w) \in M$  が臨界点であったと仮定する。このとき  $(x, w, z)$  と  $(y, z, w)$  は 1 次従属である。よって  $(y, w, z) = 0$  かまたは、ある  $c \in \mathbb{R}$  が存在して  $(x, w, z) = c(y, z, w)$  であ

る。 $(y, w, z) = 0$  なら  $p = (\pm 1, 0, 0, 0)$  である。 $(x, w, z) = c(y, z, w)$  なら、 $c(y^2 + z^2) = 0$  より  $p = (0, \pm 1, 0, 0)$  である。

逆に  $p = (\pm 1, 0, 0, 0), (0, \pm 1, 0, 0)$  ならば  $p \in M$  であり、 $f$  の臨界点であることはあきらかなので、臨界点はこれですべて求まったことになる。

### 問 7

$A$  を実正方行列、 $k$  を正の整数とし、 $\text{rk}(A^{k+1}) = \text{rk}(A^k)$  が成り立つとする。このとき、任意の整数  $m \geq k$  に対し、 $\text{rk}(A^m) = \text{rk}(A^k)$  であることを証明せよ。ここで行列  $X$  に対し、 $\text{rk}(X)$  は  $X$  の階数を表す。

証明. 仮定から、 $\text{Ker } A^{k+1}$  の次元と  $\text{Ker } A^k$  の次元は等しい。包含関係があつて次元が等しいので、 $\text{Ker } A^{k+1} = \text{Ker } A^k$  である。ここで  $m \geq k+2$  に対して  $x \in \text{Ker } A^m$  と仮定する。そうすると  $A^m x = A^{m-k-1} A^{k+1} x$  だから  $A^{m-k-1} x \in \text{Ker } A^{k+1} = \text{Ker } A^k$  である。よつて  $A^k A^{m-k-1} x = A^{m-1} x = 0$  であり、 $x \in \text{Ker } A^{m-1}$  がわかる。これを帰納的に繰り返して、 $\text{Ker } A^m \subset \text{Ker } A^{m-1} \subset \cdots \subset \text{Ker } A^k$  を得る。逆はあきらかなので  $\text{Ker } A^m = \text{Ker } A^k$  である。よつてとくに階数も等しい。  $\square$



## 平成 30 年度 専門科目

### 問 1

$k$  を可換体とする。 $k[X, Y]$  を  $k$  上の 2 変数多項式環として、 $f \in k[X, Y]$  の零点集合  $V(f)$  を

$$V(f) = \{(a, b) \in k \times k \mid f(a, b) = 0\}$$

によって定義する。次の 2 条件は同値であることを示せ。

- (1)  $k$  は代数的閉体ではない。
- (2)  $V(f) = \{(0, 0)\}$  となる  $f \in k[X, Y]$  が存在する。

解答.

- (1) $\Rightarrow$ (2)  $k$  は代数的閉体ではないので、ある 1 次以上の多項式  $g \in k[X]$  であって、 $k$  上根を持たないものが存在する。 $n = \deg g$  とおいて、

$$f(X, Y) = Y^n g\left(\frac{X}{Y}\right)$$

とおく。別の言い方をすれば  $g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$  とするとき、 $f(X, Y) = X^n + a_{n-1}X^{n-1}Y + \cdots + a_1XY^{n-1} + a_0Y^n$  である。 $X \in k, Y \in k \setminus \{0\}$  に対して  $Y^n$  と  $g(X/Y)$  は決して 0 にならないので、 $f(X, Y) = 0$  となるのは  $Y = 0$  のときだけである。 $f(X, 0) = X^n$  なので、 $V(f) = \{(0, 0)\}$  が成り立つ。

- (2) $\Rightarrow$ (1) 対偶をとり、 $k$  が代数閉体であってかつ  $V(f) = \{(0, 0)\}$  となる  $f \in k[X, Y]$  が存在すると仮定し矛盾を示そう。このとき  $k$  は無限体 ( $k$  が有限体であっても、アイゼンシュタイン多項式は無限個あるため) であることに注意する。またここではそもそも  $k$  は零環ではないとして考えていることに注意する。

さて  $a, b \in k^\times$  を任意にとると、 $f(a, Y) \in k[Y]$ 、 $f(X, b) \in k[X]$  は決して 0 にならないので、定数でなければならない。このとき  $f(a, Y) = f(a, b) = f(X, b)$  であるので、常にこの 2 つは一致する。割り算を実行して

$$\begin{aligned} f(X, Y) &= (X - a)g(X, Y) + f(a, Y) \\ f(X, Y) &= (Y - b)h(X, Y) + f(X, b) \end{aligned}$$

なる  $g, h \in k[X, Y]$  をとってくる。すると辺々引いて

$$0 = (X - a)g(X, Y) - (Y - b)h(X, Y)$$

が成り立つ。この等式は任意の  $a, b \in k^\times$  について成り立つので、 $g = h = 0 \in k[X, Y]$  が判る。ゆえに  $f$  は定数となるがこれは矛盾。

- 別解 (2) $\Rightarrow$ (1) を示す部分については Hilbert の零点定理を知っていればすこし議論を省略できる。 $k$  が代数閉体だと仮定し  $V(f) = \{(0, 0)\}$  となる  $f \in k[X, Y]$  が存在するとしよう。 $k[X, Y]$  は UFD なので、 $f$  は既約であるとしてよい。すると  $(f)$  は根基イデアルなので Hilbert の零点定理により  $(f) = (X, Y)$  である。しかし右辺は単項イデアルではないので矛盾。

## 問 2

$p$  を素数,  $k, m$  を正の整数で、 $k$  と  $p^2 - p$  は互いに素であるとする。位数  $kp^m$  の有限群  $G$  が次の性質を満たす部分群  $N, H$  をもつとする。

- (1)  $N$  は位数  $p^m$  の巡回群で  $G$  の正規部分群である。
- (2)  $H$  は位数  $k$  の群である。

このとき、 $G$  は  $N$  と  $H$  の直積であることを示せ。

解答.  $H \triangleleft G$  を示せば十分である。(付録の「半直積と Galois 群」を参照のこと)  $N \triangleleft G$  なので、 $H$  の共役による  $N$  への作用  $\Phi: H \rightarrow \text{Aut } N$  を  $\Phi_h(q) = hqh^{-1}$  により定義できる。 $H/\text{Ker } \Phi$  は  $\text{Aut } N$  の部分群とみなせる。

$$\begin{aligned}\#(\text{Aut } N) &= \#((\mathbb{Z}/p^m\mathbb{Z})^\times) \\ &= p^m - p^{m-1}\end{aligned}$$

なので、 $\#(H/\text{Ker } \Phi)$  は  $\#H = k$  と  $p^m - p^{m-1}$  の両方を割り切る。したがって  $\#(H/\text{Ker } \Phi) \leq \gcd(k, p^m - p^{m-1})$  であるが、右辺は仮定により 1 だから  $\Phi$  は自明な作用であって、 $H$  の元はすべての  $N$  の元と可換である。

よって、 $G$  の元  $g = hq$  ( $h \in H, q \in N$ ) と  $x \in N$  に対して  $g^{-1}xg = x^g = x^{hq} = (x^h)^q = x^h \in N$  だから、 $H \triangleleft G$  が言えた。

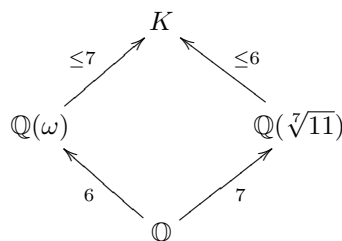
### 問 3

多項式  $X^7 - 11$  の有理数体  $\mathbb{Q}$  上の最小分解体を  $K \subset \mathbb{C}$  とする。このとき、次の問に答えよ。

- (1) 拡大次数  $[K : \mathbb{Q}]$  を求めよ。
- (2)  $\mathbb{Q}$  と  $K$  の間の ( $\mathbb{Q}$  でも  $K$  でもない) 真の中間体の個数を求めよ。
- (3) 上記 (2) の中間体のうち、 $\mathbb{Q}$  上 Galois 拡大になるものの個数を求めよ。

解答.

- (1)  $\omega = \exp(2\pi\sqrt{-1}/7)$  とする。あきらかに  $K = \mathbb{Q}(\omega, \sqrt[7]{11})$  である。状況を図式で表すと次のようになる。



円分体の一般論から  $6 = [\mathbb{Q}(\omega) : \mathbb{Q}]$  である。また  $X^7 - 11$  は Eisenstein 多項式なので既約であり  $7 = [\mathbb{Q}(\sqrt[7]{11}) : \mathbb{Q}]$  である。7 と 6 は互いに素なので  $\mathbb{Q}(\omega) \cap \mathbb{Q}(\sqrt[7]{11}) = \mathbb{Q}$  である。 $\mathbb{Q}(\omega)/\mathbb{Q}$  は Galois 拡大なので、Galois 拡大の推進定理により  $\text{Gal}(K/\mathbb{Q}(\sqrt[7]{11})) \cong \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$  であり、とくに  $[K : \mathbb{Q}(\sqrt[7]{11})] = [\mathbb{Q}(\omega) : \mathbb{Q}] = 6$  である。したがって、 $[K : \mathbb{Q}] = 42$  である。

- (2)  $G = \text{Gal}(K/\mathbb{Q})$  とする。付録「半直積と Galois 群」により、 $G$  は半直積

$$\text{Gal}(K/\mathbb{Q}(\omega)) \rtimes \text{Gal}(K/\mathbb{Q}(\sqrt[7]{11}))$$

と同型である。素数次数なので  $\text{Gal}(K/\mathbb{Q}(\omega)) = \mathbb{Z}/7\mathbb{Z}$  であり、円分体の一般論から

$$\text{Gal}(K/\mathbb{Q}(\sqrt[7]{11})) \cong \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = (\mathbb{Z}/7\mathbb{Z})^\times = \mathbb{Z}/6\mathbb{Z}$$

である。つまりともに有限巡回群である。 $\sigma \in \text{Gal}(K/\mathbb{Q}(\omega))$  を  $\sigma(\sqrt[7]{11}) = \sqrt[7]{11}\omega$  により定め、 $\tau \in \text{Gal}(K/\mathbb{Q}(\sqrt[7]{11}))$  を  $\tau(\omega) = \omega^3$  により定める。 $\sigma, \tau$  はそれぞれ生成元となる。 $\tau\sigma\tau^{-1}(\sqrt[7]{11}) = \sqrt[7]{11}\omega^3$  より  $\tau\sigma\tau^{-1} = \sigma^3$  である。したがって次の表示

$$G \cong \{\sigma, \tau \mid \sigma^7 = \tau^6 = 1, \tau\sigma\tau^{-1} = \sigma^3\} \cong \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z}$$

を得る。

Galois の基本定理により、 $G$  の自明でない部分群の個数を求めればよい。そこでまずすべての元の位数を決定する。 $\langle \sigma \rangle \rtimes \langle \tau \rangle \rightarrow \langle \tau \rangle$  は群準同型なので、 $x = \sigma^i \tau^j \in G$  の共役は  $\sigma^* \tau^j$  という形をしてい

る。具体的には

$$\begin{aligned}
\sigma x \sigma^{-1} &= \sigma \sigma^i \tau^j \sigma^{-1} \\
&= \sigma \sigma^i (\tau^j \sigma^{-1} \tau^{-j}) \tau^j \\
&= \sigma \sigma^i (\sigma^{3^j})^{-1} \tau^j \\
&= \sigma^{1-3^j} \sigma^i \tau^j \\
&= \sigma^{1-3^j} x
\end{aligned}$$

である。そこで共役元を求めることにより次のような位数の表をつくることができる。

位数	元	個数
1	1	1
2	$\sigma^i \tau^3 \ (0 \leq i \leq 6)$	7
3	$\sigma^i \tau^2 \ (0 \leq i \leq 6), \sigma^i \tau^4 \ (0 \leq i \leq 6)$	14
6	$\sigma^i \tau \ (0 \leq i \leq 6), \sigma^i \tau^5 \ (0 \leq i \leq 6)$	14
7	$\sigma^i \ (1 \leq i \leq 6)$	6

次に部分群を列挙する作業に移る。 $G$  の位数は 42 なので、自明でない部分群の位数としてありえるのは 2, 3, 6, 7, 14, 21 である。まず位数 2 の部分群は位数 2 の元と同じ数だけあるので、7 個である。位数 3 の部分群は、素数位数なのですべて巡回群であり、生成元はひとつの群に対して 2 つある。よって位数 3 の部分群は  $14/2 = 7$  個ある。

位数 6 の部分群  $M \subset G$  が与えられたとする。このとき次のような各行が完全な可換図式がある。

$$\begin{array}{ccccccc}
1 & \longrightarrow & \mathbb{Z}/7\mathbb{Z} & \xrightarrow{j} & \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z} & \xrightarrow{p} & \mathbb{Z}/6\mathbb{Z} \longrightarrow 1 \\
& & \uparrow & & \uparrow & & \uparrow \\
1 & \longrightarrow & j^{-1}(M) & \xrightarrow{j} & M & \xrightarrow{p} & p(M) \longrightarrow 1
\end{array}$$

$j^{-1}(M) = 1$  でなくてはならないため、 $M \cong p(M)$  でありしたがって  $M$  は巡回群である。位数 6 の巡回群の生成元はひとつの群に対して 2 つなので、位数 6 の部分群は  $14/2 = 7$  個ある。位数 7 の部分群は、Sylow-7 部分群なのですべて共役である。ところが  $\langle \sigma \rangle$  は正規部分群だったので、ひとつしかない。位数 14 の部分群は、Sylow の定理より位数 2 の元と位数 7 の元で生成される。したがって  $\langle \sigma, \tau^3 \rangle$  しかない。よって 1 個。位数 21 の部分群も、Sylow の定理により位数 3 の元と位数 7 の元で生成される。したがって  $\langle \sigma, \tau^2 \rangle$  しかない。よって 1 個。以上により、次の表のようになる。

位数	部分群	個数
2	$\langle \sigma^i \tau^3 \rangle \ (0 \leq i \leq 6)$	7
3	$\langle \sigma^i \tau^2 \rangle \ (0 \leq i \leq 6)$	7
6	$\langle \sigma^i \tau \rangle \ (0 \leq i \leq 6)$	7
7	$\langle \sigma \rangle$	1
14	$\langle \sigma, \tau^3 \rangle$	1
21	$\langle \sigma, \tau^2 \rangle$	1

したがって非自明な部分群は  $7 + 7 + 7 + 1 + 1 + 1 = 24$  個ある。

- (3) Galois の基本定理により、 $G$  の自明でない正規部分群の個数を求めればよい。 $x = \sigma^i \tau^j \in G$  の共役  $\sigma x \sigma^{-1}$  は  $\sigma^{1-3^j} x$  であることを思い出そう。これをみると、位数  $2, 3, 6$  の群のなかに正規部分群は存在しない。また、位数  $7, 14, 21$  の群はすべて正規部分群である。よって自明でない正規部分群は  $3$  個である。

## ■ 平成 29 年度 基礎科目

---

### 問 1

次の重積分を求めよ。

$$\iint_D e^{-\max\{x^2, y^2\}} dx dy$$

ここで  $D = \{(x, y) \in \mathbb{R}^2 \mid 0 \leq x \leq 1, 0 \leq y \leq 1\}$  とする。

解答.  $E = \{(x, y) \in D \mid x \geq y\}$  とおく。このとき

$$\begin{aligned} \iint_D e^{-\max\{x^2, y^2\}} dx dy &= 2 \iint_E e^{-x^2} dx dy \\ &= 2 \int_0^1 \left( \int_0^x e^{-x^2} dy \right) dx \\ &= 2 \int_0^1 x e^{-x^2} dx \\ &= \int_0^1 e^{-z} dz && (z = x^2 \text{とおいた}) \\ &= 1 - e^{-1} \end{aligned}$$

## 問 2

実行列

$$A = \begin{pmatrix} 1 & -2 & -1 & 1 & 0 \\ -2 & 5 & 3 & -2 & 1 \\ 1 & 1 & 2 & 0 & -1 \\ 5 & 0 & 5 & 3 & 2 \end{pmatrix}$$

について、以下の問に答えよ。

(i) 連立一次方程式

$$A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

の解をすべて求めよ。

(ii) 連立一次方程式

$$A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 1 \\ c \\ c \end{pmatrix}$$

が解を持つような実数  $c$  をすべて求めよ。

解答.

(i) 行列  $A$  に行基本変形を繰り返し行っていく。

$$\begin{aligned} A &= \begin{pmatrix} 1 & -2 & -1 & 1 & 0 \\ -2 & 5 & 3 & -2 & 1 \\ 1 & 1 & 2 & 0 & -1 \\ 5 & 0 & 5 & 3 & 2 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & -2 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 3 & 3 & -1 & -1 \\ 0 & 10 & 10 & -2 & 2 \end{pmatrix} & \begin{pmatrix} R_1 \\ R_2 + 2R_1 \\ R_3 - R_1 \\ R_4 - 5R_1 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & -1 & -4 \\ 0 & 0 & 0 & -2 & -8 \end{pmatrix} & \begin{pmatrix} R_1 + 2R_2 \\ R_2 \\ R_3 - 3R_2 \\ R_4 - 10R_2 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 0 & 1 & 0 & -2 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} R_1 + R_3 \\ R_2 \\ -R_3 \\ R_4 - 2R_3 \end{pmatrix} \end{aligned}$$

したがって、 $A\mathbf{x} = \mathbf{0}$  の解空間は  $x_3, x_5 \in \mathbb{R}$  で貼られる 2 次元実ベクトル空間

$$S = x_3 \begin{pmatrix} -1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + x_5 \begin{pmatrix} 2 \\ -1 \\ 0 \\ -4 \\ 1 \end{pmatrix}$$

である。

(ii) 次の事実に気を付ける。

**命題.**  $k$  は体、 $A$  は  $k$  係数の  $(n, m)$  行列であり  $\mathbf{x} \in k^m, \mathbf{b} \in k^n$  であるとする。このとき  $\mathbf{x}$  についての一次方程式  $A\mathbf{x} = \mathbf{b}$  が解を持つことと、 $\text{rank } A = \text{rank}(A \ \mathbf{b})$  は同値。

**証明.** まず次は同値である。

$$\exists \mathbf{x} \ A\mathbf{x} = \mathbf{b} \iff \exists \mathbf{x} \ (A \ \mathbf{b}) \begin{pmatrix} \mathbf{x} \\ -1 \end{pmatrix} = \mathbf{0}$$

ここで、 $\text{Ker } A \rightarrow \text{Ker}(A \ \mathbf{b})$  s.t.  $\mathbf{x} \mapsto {}^t(\mathbf{x} \ 0)$  によって  $\text{Ker } A$  は  $\text{Ker}(A \ \mathbf{b})$  の部分空間  $\text{Ker}(A \ \mathbf{b}) \cap \{\mathbf{y} \in k^{m+1} \mid y_{m+1} = 0\}$  だと思えることに気を付けると

$$\begin{aligned} \exists \mathbf{x} \ A\mathbf{x} = \mathbf{b} &\iff \dim \text{Ker}(A \ \mathbf{b}) > \dim \text{Ker } A \\ &\iff 0 \leq \text{rank}(A \ \mathbf{b}) - \text{rank } A < 1 \\ &\iff \text{rank } A = \text{rank}(A \ \mathbf{b}) \end{aligned}$$

であることがわかる。 □

(ii) の解答に戻る。 $\mathbf{b} = {}^t(0 \ -1 \ 1 \ c)$  とおく。拡大係数行列  $(A \ \mathbf{b})$  は行基本変形により

$$(A \ \mathbf{b}) \sim \begin{pmatrix} 1 & 0 & 1 & 0 & -2 & 2 \\ 0 & 1 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 4 & -4 \\ 0 & 0 & 0 & 0 & 0 & c+2 \end{pmatrix}$$

と変形できる。したがって求める  $c$  の値は  $c = -2$  である。



### 問 3

$m, n$  を正の整数とし、 $A$  を複素  $(n, m)$  行列、 $B$  を複素  $(m, n)$  行列とする。複素数  $\lambda \neq 0$  について、以下の間に答えよ。

- (i)  $\lambda$  が  $BA$  の固有値ならば、 $\lambda$  は  $AB$  の固有値でもあることを示せ。
- (ii)  $\mathbb{C}^m, \mathbb{C}^n$  の部分空間  $V, W$  をそれぞれ

$$V = \{\mathbf{x} \in \mathbb{C}^m \mid \text{ある正の整数 } k \text{ に対して } (BA - \lambda I_m)^k \mathbf{x} = \mathbf{0} \text{ が成り立つ}\}$$

$$W = \{\mathbf{y} \in \mathbb{C}^n \mid \text{ある正の整数 } l \text{ に対して } (AB - \lambda I_n)^l \mathbf{y} = \mathbf{0} \text{ が成り立つ}\}$$

で定める。ただし、 $I_m, I_n$  は単位行列、 $\mathbf{0}$  は零ベクトルを表す。このとき、 $\dim V = \dim W$  であることを示せ。

解答.

- (i)  $BA\mathbf{v} = \lambda\mathbf{v}$  なる  $\mathbf{v} \neq \mathbf{0}$  があったとする。このとき

$$\begin{aligned} AB(A\mathbf{v}) &= A(BA\mathbf{v}) \\ &= A(\lambda\mathbf{v}) \\ &= \lambda A\mathbf{v} \end{aligned}$$

である。もしも  $A\mathbf{v} = \mathbf{0}$  ならば  $\lambda\mathbf{v} = \mathbf{0}$  となり矛盾。したがって  $A\mathbf{v} \in \mathbb{C}^n$  は  $AB$  の固有ベクトルである。

- (ii)  $M = AB, N = BA$  とする。 $MA = AN$  である。いま  $\mathbf{x} \in V$  とする。ある  $k$  が存在して  $(N - \lambda I_m)^k \mathbf{x} = \mathbf{0}$  である。このとき

$$(M - \lambda I_n)^k (A\mathbf{x}) = A(N - \lambda I_m)^k \mathbf{x} = \mathbf{0}$$

であるから  $A\mathbf{x} \in W$  である。したがって行列  $A$  は線形写像  $A: V \rightarrow W$  であるとみなせる。このとき  $A$  は  $V$  の定義および  $\lambda \neq 0$  により単射だから、 $\dim V \leq \dim W$  である。同様にして逆が言えるので  $\dim V = \dim W$  が従う。

問 4

$f$  を  $I = \{x \in \mathbb{R} \mid x \geq 0\}$  上の実数値連続関数とする。正の整数  $n$  に対し、 $I$  上の関数  $f_n$  を

$$f_n(x) = f(x+n)$$

で定める。関数列  $\{f_n\}_{n=1}^{\infty}$  が  $I$  上で一様収束するとき、以下の問に答えよ。

(i)  $I$  上の関数  $g$  を

$$g(x) = \lim_{n \rightarrow \infty} f_n(x)$$

で定める。このとき  $g$  は  $I$  上で一様連続であることを示せ。

(ii)  $f$  は  $I$  上で一様連続であることを示せ。

解答. 以下  $I$  上の連続関数  $h$  に対してその一様ノルムを  $\|h\| = \sup_{x \in I} |h(x)|$  とかく。

- (i) 連続関数  $f_n$  の一様極限なので  $g$  は連続である。さらに定義より  $g(x+1) = g(x)$  だから、 $g$  はコンパクト集合  $\mathbb{R}/\mathbb{Z}$  上の連続関数であるとみなせ、したがって一様連続である。
- (ii)  $\varepsilon > 0$  が与えられたとする。 $g$  の一様連続性から

$$\forall x, y \in I \quad |x - y| < \delta_0 \rightarrow |g(x) - g(y)| < \varepsilon$$

なる  $\delta_0 > 0$  がある。 $f_n$  は  $g$  に一様収束するので

$$n \geq N \rightarrow \|f_n - g\| < \varepsilon$$

なる  $N \in \mathbb{Z}$  がある。このとき

$$\forall x, y \in [N, \infty) \quad |x - y| < \delta_0 \rightarrow |f(x) - f(y)| \leq 3\varepsilon$$

が成り立つ。なぜなら

$$|f(x) - f(y)| \leq |f_N(x - N) - g(x - N)| + |g(x) - g(y)| + |g(y - N) - f_N(y - N)|$$

であるから。また  $f$  は連続なので、コンパクト集合  $[0, N]$  上ではとくに一様連続である。したがって

$$\forall x, y \in [0, N] \quad |x - y| < \delta_1 \rightarrow |f(x) - f(y)| \leq \varepsilon$$

なる  $\delta_1 > 0$  がある。したがって  $\delta = \min_i \delta_i$  とすると

$$\forall x, y \in I \quad |x - y| < \delta \rightarrow |f(x) - f(y)| \leq 4\varepsilon$$

であり、これで  $f$  が  $I$  上一様連続であることがいえた。

問 5

$p$  を正の実数とし、 $f(t)$  を  $\mathbb{R}$  上の実数値連続関数で

$$\int_0^\infty |f(t)| \, dt < \infty$$

を満たすものとする。このとき  $\mathbb{R}$  上の常微分方程式

$$\frac{dx}{dt} = -px + f(t)$$

の任意の解  $x(t)$  に対し  $\lim_{t \rightarrow \infty} x(t) = 0$  が成り立つことを示せ。

解答. 任意に  $\varepsilon > 0$  が与えられたとする。仮定により

$$\int_R^\infty |f(t)| \, dt < \varepsilon$$

となるような  $R \geq 0$  がある。 $x = ye^{-pt}$  と置いて変数変換をすると

$$\frac{dy}{dt} = e^{pt} f(t)$$

となる。よってある定数  $C$  により

$$y(t) = \int_0^t f(s)e^{ps} \, ds + C$$

と表せる。 $C$  の値は  $t \rightarrow \infty$  での  $x$  の振る舞いに関与しないので、はじめから  $C = 0$  と仮定してよい。これにより

$$x(t) = \int_0^t f(s)e^{p(s-t)} \, ds$$

であることがわかる。そこで  $M = \int_0^R |f(s)| \, ds$  とおき、 $t > \max\{R, R + \frac{1}{p} \log \frac{M}{\varepsilon}\}$  とする。このとき

$$\begin{aligned} |x(t)| &\leq \int_0^R |f(s)| e^{p(s-t)} \, ds + \int_R^t |f(s)| e^{p(s-t)} \, ds \\ &\leq e^{p(R-t)} M + \int_R^t |f(s)| \, ds \\ &\leq \varepsilon + \int_R^\infty |f(s)| \, ds \\ &\leq 2\varepsilon \end{aligned}$$

である。よって  $\lim_{t \rightarrow \infty} x(t) = 0$  である。

## 問 6

$X, Y$  を位相空間とし、直積集合  $X \times Y$  を積位相によって位相空間とみなす。写像  $f: X \times Y \rightarrow Y$  を  $f(x, y) = y$  で定める。 $X$  がコンパクトならば、 $X \times Y$  の任意の閉集合  $Z$  に対し、 $f(Z)$  は  $Y$  の閉集合であることを示せ。

注意.  $X$  がコンパクトという仮定は必要である。例えば、 $X = Y = \mathbb{R}$  かつ  $Z = \{(x, y) \in \mathbb{R}^2 \mid xy = 1\}$  としてみればわかる。

解答.  $Y \setminus f(Z)$  の元  $y$  が任意に与えられたとする。このとき  $f^{-1}(y) \subset X \times Y \setminus Z$  である。ここで  $Z$  が  $X \times Y$  の閉集合という仮定から、 $X \times Y \setminus Z \subset_{\text{open}} X \times Y$  である。したがって積位相の定義により、ある開集合の族  $U_i \subset X$  と  $V_i \subset Y$  であって  $X \times Y \setminus Z = \bigcup_{i \in I} U_i \times V_i$  なるものがある。 $f^{-1}(y) = X \times \{y\} \cong X$  はコンパクトであると仮定したので、ある有限集合  $J \subset I$  が存在して  $X \times \{y\} = f^{-1}(y) \subset \bigcup_{i \in J} U_i \times V_i$  が成り立つ。

ここで  $V = \bigcap_{i \in J} V_i$  とおく。 $J$  は有限集合なので  $V$  は  $Y$  の開集合であり、かつ  $y$  を含む。また  $X = \bigcup_{i \in J} U_i$  であることより  $Z \cap f^{-1}(V) = Z \cap (X \times V) = Z \cap \bigcup_{i \in J} (U_i \times V) \subset Z \cap (X \times Y \setminus Z) = \emptyset$  となる。これは  $V \cap f(Z) = \emptyset$  を意味し、 $y$  は内点であったことがわかった。よって  $f(Z)$  は  $Y$  の閉集合。

問 7

$n$  を正の整数とし、 $\mathbb{R}^n$  の 2 点  $x = (x_1, \dots, x_n)$ ,  $y = (y_1, \dots, y_n)$  の距離  $d(x, y)$  を

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}$$

と定める。 $\mathbb{R}^n$  の空でない部分集合  $A$  に対し、関数  $f: \mathbb{R}^n \rightarrow \mathbb{R}$  を

$$f(x) = \inf_{z \in A} d(x, z)$$

で定めるとき、 $\mathbb{R}^n$  の任意の 2 点  $x, y$  に対して  $|f(x) - f(y)| \leq d(x, y)$  が成り立つことを示せ。

解答.  $d(x, 0) = |x|$  と書くことにする。任意に  $\varepsilon > 0$  が与えられたとしよう。このとき  $f$  の定義から、 $f(y) + \varepsilon > |y - w| \geq f(y)$  なる  $w \in A$  が存在する。このとき  $f(x) \leq |x - w|$  が成り立つので、

$$\begin{aligned} f(x) - f(y) - \varepsilon &\leq f(x) - |y - w| \\ &\leq |x - w| - |y - w| \\ &\leq |x - y| \end{aligned}$$

である。 $\varepsilon > 0$  は任意だったので、 $f(x) - f(y) \leq |x - y|$  でなくてはならない。同様にして  $f(y) - f(x) \leq |x - y|$  がいえるので、示すべきことがいえた。

## 平成 29 年度 専門科目

### 問 1

$G$  を有限群とする。 $G$  の自己準同形全体のなす群を  $\text{Aut}(G)$  とおく。また、 $G$  および  $\text{Aut}(G)$  の位数をそれぞれ  $a = |G|$ ,  $b = |\text{Aut } G|$  とおく。以下の問に答えよ。

- (i)  $b = 1$  のとき、 $G$  は自明群であるか、または  $\mathbb{Z}/2\mathbb{Z}$  と同型であることを示せ。
- (ii)  $a$  が奇数で  $b = 2$  となるような  $G$  をすべて求めよ。

解答. この解答では集合の元の個数を  $\#$  で表記する。

- (i) 群準同形  $\phi: G \rightarrow \text{Aut } G$  を  $\phi_g(x) = gxg^{-1}$  により定める。 $\# \text{Aut } G = 1$  という仮定より、 $G = \text{Ker } \phi = Z(G)$  である。したがって  $G$  は Abel 群。よって有限生成 Abel 群の基本定理により、ある素数の集合  $M \subset \mathbb{Z}$  と写像  $I: M \rightarrow P(\mathbb{Z})$  が存在して

$$G = \bigoplus_{p \in M} \bigoplus_{i \in I(p)} \mathbb{Z}/p^{e_i}\mathbb{Z}$$

と表すことができる。このとき乗法群  $(\prod_{p,i} \mathbb{Z}/p^{e_i}\mathbb{Z})^\times$  は  $\text{Aut } G$  の部分群とみなせるので

$$\prod_{p,i} p^{e_i-1}(p-1) = 1$$

である。したがって  $M = \{2\}$  である。また任意の  $i \in I(2)$  に対して  $e_i = 1$  である。よって  $G = (\mathbb{Z}/2\mathbb{Z})^n$  と表せるが、 $\text{Aut } G = 1$  という仮定から  $n = 1$  でなくてはならない。 $(n \geq 2$  なら、たとえば順番を入れ替える写像などがある)

- (ii) 仮定から  $G/Z(G) = G/\text{Ker } \phi$  の位数は 2 以下である。写像  $f: G \rightarrow G$  を  $f(x) = x^2$  で定義する。 $x, y \in G$  に対して、もしも  $x \in Z(G)$  または  $y \in Z(G)$  ならば  $f(xy) = f(x)f(y)$  である。また  $x, y \in G \setminus Z(G)$  であれば、 $xy \in Z(G)$  なので  $f(xy) = xy(xy) = f(x)f(y)$  である。したがって  $f$  は群準同形となる。 $\#G$  は奇数なので  $f$  は単射であり、位数の考察から同型となる。このことから結局  $G = Z(G)$  であり、 $G$  は Abel 群である。ゆえに有限生成 Abel 群の基本定理から

$$G = \bigoplus_{p \in M} \bigoplus_{i \in I(p)} \mathbb{Z}/p^{e_i}\mathbb{Z}$$

と表すことができる。このとき乗法群  $(\prod_{p,i} \mathbb{Z}/p^{e_i}\mathbb{Z})^\times$  は  $\text{Aut } G$  の部分群とみなせるので

$$\prod_{p,i} p^{e_i-1}(p-1) \leq 2$$

である。 $p$  としては 3 以上のものしか現れないから、 $M = \{3\}$  である。また  $\#I(3) = 1$  かつ  $i \in I(3)$  に対して  $e_i = 1$  であることもわかる。したがって  $G = \mathbb{Z}/3\mathbb{Z}$  である。

問 2

$n$  は 2 以上の整数とし、 $\zeta = e^{2\pi\sqrt{-1}/n}$  を 1 の原始  $n$  乗根とする。 $\mathbb{C}[X, Y]$  は変数  $X, Y$  に関する複素数係数の 2 変数多項式環とする。

$$R = \{f(X, Y) \in \mathbb{C}[X, Y] \mid f(\zeta X, \zeta Y) = f(X, Y)\}$$

とおく。以下の問に答えよ。

- (i)  $\mathbb{C}$  代数として  $R$  は  $n+1$  個の元  $X^n, X^{n-1}Y, \dots, XY^{n-1}, Y^n$  で生成されることを示せ。
- (ii) 複素数  $a, b, c, d$  に対し  $m_{a,b} = (X-a, Y-b)$ ,  $m_{c,d} = (X-c, Y-d)$  を  $\mathbb{C}[X, Y]$  のイデアルとする。  $m_{a,b} \cap R = m_{c,d} \cap R$  が成り立つための  $a, b, c, d$  に関する必要十分条件を求めよ。

解答.

- (i)  $X^n, X^{n-1}Y, \dots, XY^{n-1}, Y^n$  で  $\mathbb{C}$  上生成される環を  $R'$  とおく。  $f \in R$  が与えられたとする。  $f$  をゼロでない  $d$  次斉次元  $f_d$  の和として  $f = \sum_{d \in I} f_d$  と書く。このとき仮定から  $0 = f(\zeta X, \zeta Y) - f(X, Y) = \sum_{d \in I} (\zeta^d - 1) f_d(X, Y)$  である。したがって  $I$  の元はすべて  $n$  の倍数である。これはつまり  $f \in R'$  を意味する。よって  $R \subset R'$  である。逆は明らかだから  $R = R'$  がいえた。
- (ii) 1 の  $n$  乗根全体がなす位数  $n$  の巡回群を  $G$  と書くことにする。このとき、 $(za, zb) = (c, d)$  なる  $z \in G$  が存在すれば  $m_{a,b} \cap R = m_{c,d} \cap R$  が成り立つことはあきらか。逆を示そう。  
 $m_{a,b} \cap R = m_{c,d} \cap R$  が成り立ったと仮定する。このとき  $X^n - a^n$  と  $Y^n - b^n$  はともに  $m_{a,b} \cap R = m_{c,d} \cap R$  の元である。よって  $c^n - a^n = d^n - b^n = 0$  であり、ある  $z, w \in G$  が存在して  $c = za$ ,  $d = wb$  が成り立つ。ここでさらに  $(bX - aY)^n$  も  $m_{a,b} \cap R = m_{c,d} \cap R$  の元だから、 $\mathbb{C}$  は整域なので  $bc - ad = 0$  である。よって  $(z - w)ab = 0$  である。このとき  $ab = 0$  または  $z - w = 0$  であるが、いずれにせよ  $(za, zb) = (c, d)$  なる  $z \in G$  が存在することには違いがないので、示すべきことがいえた。

### 問 3

以下の問に答えよ。

- (i)  $S_5$  を文字  $1, 2, 3, 4, 5$  に関する対称群とする。 $S_3$  を文字  $1, 2, 3$  に関する対称群とし、 $S_3$  を  $S_5$  の部分群とみなす。 $\sigma = (1\ 2\ 3) \in S_5$  を長さ 3 の巡回置換とし、 $\sigma$  で生成された  $S_5$  の部分群を  $G = \langle \sigma \rangle$  とおく。 $\tau = (4\ 5) \in S_5$  を互換とし、 $\tau$  で生成された  $S_5$  の部分群を  $H = \langle \tau \rangle$  とおく。 $S_5$  の部分群  $G$  の正規化群を

$$N_{S_5}(G) = \{ \eta \in S_5 \mid \eta G \eta^{-1} = G \}$$

で定める。このとき、 $N_{S_5}(G) = S_3 \times H$  であることを示せ。

- (ii)  $f(X)$  は  $\mathbb{Q}$  係数の 5 次の多項式とする。 $K \subset \mathbb{C}$  を  $f(X)$  の  $\mathbb{Q}$  上の最小分解体とする。 $K$  は次の条件 (\*) を満たすとする。

(\*)  $[K : F] = 3$  となる  $K$  の部分体  $F$  がただ一つ存在する。

このとき、 $f(X)$  は  $\mathbb{Q}$  係数の 3 次の既約多項式で割り切れることを示せ。

解答.

- (i)  $S_3$  の元と  $H$  の元は互いに可換なので、積をとる写像  $S_3 \times H \rightarrow S_5$  は準同型となる。 $G \triangleleft S_3$  より、 $(s, t) \in S_3 \times H$  としたとき

$$(st)\sigma(st)^{-1} = s\sigma s^{-1} \in G$$

だから積  $st$  は  $N_{S_5}(G)$  に含まれる。よって準同型  $\varphi: S_3 \times H \rightarrow N_{S_5}(G)$  が構成できたことになる。 $S_3 \cap H = 1$  より  $\varphi$  は単射である。全射であることを示そう。

$h \in N_{S_5}(G)$  が与えられたとする。このとき定義から  $h\sigma h^{-1} \in G$  である。よって  $x \in \{4, 5\}$  への作用を考えると  $h\sigma h^{-1}(x) = x$ , つまり  $\sigma h^{-1}(x) = h^{-1}(x)$  がわかる。 $\sigma$  が固定するのは  $\{4, 5\}$  の元だけなので  $h^{-1}(x) \in \{4, 5\}$  である。まとめると、任意の  $h \in N_{S_5}(G)$  に対して  $h = \sigma_0 \tau_0$  なる  $\sigma_0 \in S_3$  と  $\tau_0 \in H$  があることが判ったことになり、したがって  $\varphi$  は全射、ゆえに同型である。

- (ii) Galois の基本定理により、 $F \mapsto \text{Gal}(K/F)$  で与えられる対応

$$\{K/\mathbb{Q} \text{ の部分体} \} \rightarrow \{ \Gamma := \text{Gal}(K/\mathbb{Q}) \text{ の部分群} \}$$

は全単射である。ゆえに  $\Gamma$  は位数 3 の部分群をただひとつしかもたない。とくに  $\text{Gal}(K/F)$  の  $\Gamma$  での共役はただひとつなので  $\text{Gal}(K/F) \triangleleft \Gamma$  である。 $G = \text{Gal}(K/F)$  とおく。 $f$  の根を  $\alpha_1, \dots, \alpha_5$  とすると  $\Gamma$  は  $\{\alpha_1, \dots, \alpha_5\}$  への作用により 5 次対称群  $S_5$  の部分群とみなせる。 $G \cong \mathbb{Z}/3\mathbb{Z}$  なので必要ならば番号を付けなおすことにより  $G$  は  $\sigma = (1\ 2\ 3)$  で生成されているとしてよい。いま  $G \triangleleft \Gamma$  により  $\Gamma \subset N_{S_5}(G)$  である。(i) により  $N_{S_5}(G) \cong S_3 \times H$  であるので、 $\Gamma \subset S_3 \times H$  とみなせる。

$f$  は 5 次多項式であるので、 $f$  の  $\mathbb{Q}[X]$  における既約分解の様相には次の可能性がある。

- (1)  $f$  は既約
- (2)  $f = (4 \text{ 次式}) \times (1 \text{ 次式})$
- (3)  $f = (3 \text{ 次式}) \times (2 \text{ 次式})$
- (4)  $f = (3 \text{ 次式}) \times (1 \text{ 次式}) \times (1 \text{ 次式})$
- (5)  $f = (2 \text{ 次式}) \times (2 \text{ 次式}) \times (1 \text{ 次式})$
- (6)  $f = (2 \text{ 次式}) \times (1 \text{ 次式}) \times (1 \text{ 次式}) \times (1 \text{ 次式})$



(7)  $f = (1 \text{ 次式}) \times (1 \text{ 次式}) \times (1 \text{ 次式}) \times (1 \text{ 次式}) \times (1 \text{ 次式})$

ここで (5),(6),(7) は条件 (\*) を満たさないので却下される。(1),(2) の場合  $\Gamma$  は集合  $\{1, 2, 3, 4, 5\}$  の位数 4 以上の部分集合に推移的に作用しなければならないが、これは  $\Gamma \subset S_3 \times H$  に反する。したがって残る可能性は (3),(4) のみであり、示すべきことがいえた。

## ■ 平成 28 年度 基礎科目 I

### 問 1

線形写像  $f: \mathbb{R}^4 \rightarrow \mathbb{R}^3$  を行列

$$A = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 4 & 0 & 2 & 1 \\ 2 & -1 & 1 & 2 \end{pmatrix}$$

を用いて  $f(x) = Ax$  ( $x \in \mathbb{R}^4$ ) として定める。 $V$  を 3 つのベクトル

$$\begin{pmatrix} 1 \\ 2 \\ -2 \\ -4 \end{pmatrix}, \begin{pmatrix} 0 \\ -2 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ -4 \end{pmatrix}$$

が張る  $\mathbb{R}^4$  の部分空間としたとき、 $f$  の  $V$  への制限  $g = f|_V: V \rightarrow \mathbb{R}^3$  の階数を求めよ。ただし、 $g$  の階数とは、 $g(V)$  の次元のこととする。

解答. 与えられたベクトルをそれぞれ  $v_1, v_2, v_3$  とする。このとき  $B = (gv_1, gv_2, gv_3)$  であるとする。このとき  $B$  は基本変形で

$$B = \begin{pmatrix} 2 & -1 & 3 \\ -4 & 5 & 0 \\ -10 & 8 & -7 \end{pmatrix} \sim \begin{pmatrix} 2 & -1 & 3 \\ 0 & 3 & 6 \\ 0 & 0 & 2 \end{pmatrix}$$

と変形できる。したがって  $\text{rank } B = 3$  であり、 $g$  の階数は 3 である。

## 問 2

$a$  を実数とする。3 次正方行列

$$A = \begin{pmatrix} a & 1 & 2 \\ 0 & 1 & 0 \\ -2 & 0 & 0 \end{pmatrix}$$

について、以下の問に答えよ。

- (i) 行列  $A$  の固有値を求めよ。
- (ii) 行列  $A$  が対角化可能となる実数  $a$  をすべて求めよ。ただし、 $A$  が対角化可能であるとは、複素正則行列  $P$  で  $P^{-1}AP$  が対角行列となるものが存在することをいう。

解答.

- (i) 与えられた  $A$  を変数  $a$  を明示して  $A(a)$  と書くことにしよう。そうして  $A(a)$  の固有多項式を  $\Phi_a(\lambda)$  で書くことにする。このとき

$$\Phi_a(\lambda) = \det(\lambda I - A(a)) = (\lambda - 1)(\lambda^2 - a\lambda + 4)$$

である。だから固有値は  $1, (a \pm \sqrt{a^2 - 16})/2$  である。

- (ii)  $\lambda^2 - a\lambda + 4$  が 1 を根に持つのは  $a = 5$  のとき。また重根を持つのは  $a = \pm 4$  のとき。だから  $a$  が  $5, \pm 4$  のいずれでもないときには  $A(a)$  は異なる 3 つの固有値を持ち、したがって対角化可能である。では  $a = 5, \pm 4$  のときはどうか。

行列  $A$  が対角化可能であることと、 $A$  の各固有値についての固有空間の直和が全体と一致することは同値であることに注意する。固有値  $\lambda$  に属する固有空間を  $V(\lambda)$  と表すことにする。

$a = 4$  のとき、 $\Phi_4(\lambda) = (\lambda - 1)(\lambda - 2)^2$  である。固有空間  $V(2)$  の次元は線形写像  $2I - A(4)$  の核の次元だから

$$2I - A(4) = \begin{pmatrix} -2 & -1 & -2 \\ 0 & -3 & 0 \\ 2 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} -2 & -1 & -2 \\ 0 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

より  $\dim V(2) = 3 - 2 = 1$  である。よって  $A(4)$  は対角化できない。 $a = -4, 5$  についても同様の考察により  $A(a)$  が対角化できないことが判るが、詳細は省略する。これですべての  $a$  について  $A(a)$  の対角化可能性が求まった。

### 問 3

次の極限値を求めよ。

$$\lim_{n \rightarrow \infty} \int_0^{\infty} e^{-x} (nx - [nx]) dx$$

ただし、 $n$  は自然数とし、 $[y]$  は  $y$  を超えない最大の整数を表す。

解答. 1 以上の  $n \in \mathbb{Z}$  を固定すると、任意の  $x \in \mathbb{R}_{\geq 0}$  に対して

$$\frac{k}{n} \leq x < \frac{k+1}{n}$$

なる  $k \in \mathbb{Z}$  が一意にある。このとき  $nx - [nx] = nx - k$  である。そこで  $M_n = \int_0^{\infty} e^{-x} (nx - [nx]) dx$  とおくと

$$M_n = \sum_{k \geq 0} \int_{k/n}^{(k+1)/n} e^{-x} (nx - k) dx$$

である。いったん  $n$  は固定して  $F_k = \int_{k/n}^{(k+1)/n} e^{-x} (nx - k) dx$  とおこう。部分積分を用いることにより

$$F_k = -(n+1)e^{-\frac{k+1}{n}} + ne^{-\frac{k}{n}}$$

が示せる。 $\zeta = e^{-\frac{1}{n}}$  とおけば  $F_k = -(n+1)\zeta^{k+1} + n\zeta^k$  である。したがって

$$M_n = (n - (n+1)\zeta) \sum_{k \geq 0} \zeta^k = \frac{n - (n+1)\zeta}{1 - \zeta}$$

を得る。あとは次のように式変形を行えばよい。

$$\begin{aligned} \lim_{n \rightarrow \infty} M_n &= \lim_{n \rightarrow \infty} \frac{n - (n+1)e^{-1/n}}{1 - e^{-1/n}} \\ &= \lim_{n \rightarrow \infty} \frac{ne^{1/n} - (n+1)}{e^{1/n} - 1} \\ &= \lim_{h \rightarrow 0} \frac{h^{-1}e^h - (h^{-1} + 1)}{e^h - 1} \\ &= \lim_{h \rightarrow 0} \frac{e^h - (1+h)}{h(e^h - 1)} \\ &= \lim_{h \rightarrow 0} \frac{h}{e^h - 1} \frac{e^h - (1+h)}{h^2} \end{aligned}$$

そうすると  $e^h = 1 + h + h^2/2 + O(h^3)$  より  $\lim_{n \rightarrow \infty} M_n = 1/2$  が結論できる。

#### 問 4

$\mathbb{R}^2$  で定義された関数

$$f(x, y) = \frac{xy(xy + 4)}{x^2 + y^2 + 1}$$

の最大値および最小値のそれぞれについて、存在するなら求め、存在しないならそのことを示せ。

解答.  $x = r \cos \theta$ ,  $y = r \sin \theta$  とおくと

$$f(x, y) = \frac{r^4 \sin^2 2\theta + 8r^2 \sin 2\theta}{4(r^2 + 1)}$$

である。さらに  $t = \sin 2\theta$  とおけば次のように変形できる。

$$f(x, y) = \frac{r^4 t^2 + 8r^2 t}{4(r^2 + 1)}$$

したがって、右辺の関数を  $g(r, t)$  とおいて  $0 \leq r, -1 \leq t \leq 1$  における  $g$  の最大値と最小値を求めればよい。最大値の方はすぐにわかる。 $t = 1$  としてみると  $g(r, 1) = (r^4 + 8r^2)/4(r^2 + 1)$  であり、あきらかに  $\lim_{r \rightarrow \infty} g(r, 1) = \infty$  なので  $g$  に最大値はない。

では最小値はどうか。 $g$  を  $t$  について平方完成すると

$$g(r, t) = \frac{r^4}{4(r^2 + 1)} \left( \left( t + \frac{4}{r^2} \right) - \frac{16}{r^4} \right)$$

である。 $h(t) = (t + 4/r^2) - 16/r^4$  とおく。 $h(t)$  のグラフは、軸が直線  $t = -4/r^2$  であるような下に凸な放物線である。そこで軸が  $-1 \leq t \leq 1$  に入るかどうかで場合分けをして

$$\min_{-1 \leq t \leq 1} h(t) = \begin{cases} h(-4/r^2) = -16/r^4 & (r \geq 2) \\ h(-1) = -8/r^2 + 1 & (0 \leq r \leq 2) \end{cases}$$

を得る。ゆえに

$$\min_{r \geq 0, -1 \leq t \leq 1} g(r, t) = \min \left\{ \min_{r \geq 2} \frac{-4}{r^2 + 1}, \min_{0 \leq r \leq 2} \frac{1}{4} \left( r^2 - 9 + \frac{9}{r^2 + 1} \right) \right\}$$

である。 $k(r) = r^2 - 9 + 9/(r^2 + 1)$  とおいて微分すると  $k(r)$  の  $0 \leq r \leq 2$  での最小値は  $k(\sqrt{2}) = -4$  であることがわかる。あきらかに  $\min_{r \geq 2} -4/(r^2 + 1) = -4/5$  だから、求める最小値は  $-1$  である。

## ■ 平成 28 年度 基礎科目 II

### 問 1

次の積分が収束するような実数  $\alpha$  の範囲を求めよ。

$$\iint_D \frac{dx \, dy}{(x^2 + y^2)^\alpha}$$

ただし、 $D = \{(x, y) \in \mathbb{R}^2 \mid -\infty < x < \infty, 0 < y < 1\}$  とする。

解答．与えられた積分を  $I(\alpha)$  と略記する。極座標変換を行うと次の形になる。

$$\begin{aligned} I(\alpha) &= 2 \iint_{0 < y < 1, 0 \leq x} \frac{dx \, dy}{(x^2 + y^2)^\alpha} \\ &= 2 \int_0^{\pi/2} d\theta \int_0^{1/\sin \theta} r^{1-2\alpha} \, dr \end{aligned}$$

ここでもし  $\alpha = 1$  ならば

$$I(1) \geq 2 \int_0^{\pi/2} d\theta \int_0^1 \frac{dr}{r} = \infty$$

より発散する。そこで  $\alpha \neq 1$  と仮定して先に進むと、次のようになる。

$$I(\alpha) = \frac{1}{1-\alpha} \int_0^{\pi/2} (\sin \theta)^{2\alpha-2} - \lim_{\varepsilon \rightarrow 0} \varepsilon^{2-2\alpha} \, d\theta$$

$\alpha > 1$  ならこれは発散する。そこで  $\alpha < 1$  と仮定して先へ進むと、次の形に帰着する。

$$\begin{aligned} I(\alpha) &= \frac{1}{1-\alpha} \int_0^{\pi/2} (\sin \theta)^{2\alpha-2} \, d\theta \\ &= \frac{1}{1-\alpha} \int_0^{\pi/2} \left( \frac{\sin \theta}{\theta} \right)^{2\alpha-2} \cdot \theta^{2\alpha-2} \, d\theta \end{aligned}$$

$\sin \theta / \theta$  は  $[0, \pi/2]$  上の連続関数であり、0 より大きい最小値と最大値を持つ。よって収束には関与しないので、 $\alpha < 1$  のとき  $I(\alpha)$  が収束することは  $\alpha > 1/2$  と同値であることがわかる。つまり  $I(\alpha)$  は、 $\alpha \leq 1/2$  または  $1 \leq \alpha$  なら無限大に発散、 $1/2 < \alpha < 1$  なら収束するということが結論できたことになる。

## 問 2

$A$  と  $B$  を複素 3 次正方行列とする。 $A$  の最小多項式は  $x^3 - 1$ ,  $B$  の最小多項式は  $(x - 1)^3$  とする。このとき

$$AB \neq BA$$

となることを示せ。

解答. 行列  $M \in M(3, \mathbb{C})$  の固有値  $\lambda$  に属する固有空間を  $E(\lambda, M)$  と書くことにする。仮定より、 $A$  の固有値は  $x^2 + x + 1$  の根のひとつを  $\omega$  として、 $1, \omega, \omega^2$  の 3 つである。もしも  $AB = BA$  ならば、 $v \in E(\lambda, A)$  に対して

$$ABv = BAv = B(\lambda v) = \lambda(Bv)$$

であるから  $Bv \in E(\lambda, A)$  である。つまり  $B$  を写像  $B: E(\lambda, A) \rightarrow E(\lambda, A)$  とみなせる。

ここで  $e_i \in E(\omega^i, A) \setminus \{0\}$  ( $0 \leq i \leq 2$ ) としよう。 $e_i$  はそれぞれ 1 次元ベクトル空間である  $E(\omega^i, A)$  の基底となる。ゆえに  $Be_i = \lambda_i e_i$  となる  $\lambda_i$  が存在することになる。つまり  $e_i$  は  $B$  の固有ベクトルである。 $e_i$  は  $\mathbb{C}^3$  全体を張るので、とくに  $B$  は対角化可能となるが、これは  $B$  の最小多項式が重根を持つことに矛盾。よって  $AB \neq BA$  でなくてはならない。

### 問 3

複素関数  $f(z)$  は  $z = 0$  の近傍で正則な関数で  $f(z)e^{f(z)} = z$  をみたすとする。以下の問に答えよ。

- (i) 非負整数  $n$  と十分小さい正数  $\varepsilon$  に対して次の式が成り立つことを示せ。

$$\frac{f^{(n)}(0)}{n!} = \frac{1}{2\pi i} \int_{C_\varepsilon} \frac{1+u}{e^{nu}u^n} du$$

ここで積分路  $C_\varepsilon$  は円周  $C_\varepsilon = \{u \in \mathbb{C} \mid |u| = \varepsilon\}$  を正の向きに一周するものとする。

- (ii)  $f(z)$  の  $z = 0$  におけるべき級数展開を求め、その収束半径を求めよ。

解答.

- (i) 仮定の式  $f(z)e^{f(z)} = z$  の両辺を微分して  $(1+f)f'e^f = 1$  を得る。とくに  $f'$  は零点を持たない。したがって逆関数定理により  $f$  は  $0$  の十分小さな近傍  $U$  に制限すれば像への同相写像となる。よって  $u = f(z)$  と変数変換することができて

$$\begin{aligned} \frac{1+u}{(e^u u)^n} du &= \frac{(1+f(z))f'(z)}{z^n} dz \\ &= \frac{e^{-f(z)}}{z^n} dz \\ &= \frac{f(z)}{z^{n+1}} dz \end{aligned}$$

であることがわかる。したがって Cauchy の積分公式から、十分小さい  $\varepsilon$  をとればすべての  $n$  に対して

$$\frac{f^{(n)}(0)}{n!} = \frac{1}{2\pi i} \int_{f^{-1}(C_\varepsilon)} \frac{f(z)}{z^{n+1}} dz = \frac{1}{2\pi i} \int_{C_\varepsilon} \frac{1+u}{e^{nu}u^n} du$$

が成り立つ。

- (ii) べき級数展開すると

$$\begin{aligned} (1+z)e^{-nz} &= (1+z) \sum_{k=0}^{\infty} \frac{(-n)^k}{k!} z^k \\ &= 1 + \sum_{k=1}^{\infty} \left( \frac{(-n)^{k-1}}{(k-1)!} + \frac{(-n)^k}{k!} \right) z^k \end{aligned}$$

である。よって  $z = 0$  のまわりでの Laurent 展開は

$$\frac{(1+z)e^{-nz}}{z^n} = \frac{1}{z^n} + \sum_{k=1}^{\infty} \left( \frac{(-n)^{k-1}}{(k-1)!} + \frac{(-n)^k}{k!} \right) z^{n-k}$$

であることがわかる。ゆえに留数定理から

$$\frac{1}{2\pi i} \int_{C_\varepsilon} \frac{1+u}{e^{nu}u^n} du = \begin{cases} 0 & (n=0) \\ (-n)^{n-1}/n! & (n \geq 1) \end{cases}$$

が従う。よって  $f$  のべき級数展開を  $f(z) = \sum_{n \geq 1} a_n z^n$  とすると  $a_n = (-n)^{n-1}/n!$  であり、 $\lim_{n \rightarrow \infty} |a_{n+1}/a_n| = e$  だから収束半径は  $1/e$  である。



#### 問 4

正則な複素 2 次正方行列のなす群を  $GL_2(\mathbb{C})$  とおく。行列

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

で生成される  $GL_2(\mathbb{C})$  の部分群  $G$  について、以下の問に答えよ。

- (i) 群  $G$  の位数を求めよ。
- (ii) 群  $G$  の中心の位数を求めよ。ただし、 $G$  の中心とは、 $G$  のすべての元と可換な元全体のなす  $G$  の部分群のことである。
- (iii) 群  $G$  に含まれる位数 2 の元の個数を求めよ。

解答.  $I$  は単位行列とする。群の特定の部分集合  $S$  で生成される部分群を  $\langle S \rangle$  で書く。

- (i) 計算により  $\langle A \rangle \cong \mathbb{Z}/6\mathbb{Z}$ ,  $B^2 = I$ ,  $BAB^{-1} = A^{-1}$  がわかる。ゆえに  $BA = (BAB)B = A^5B$  だから、 $G$  の元はすべて  $A^i B^j$  ( $0 \leq i \leq 5, 0 \leq j \leq 1$ ) という形をしている。よって  $\#G \leq 12$  である。  
逆を考察しよう。 $BAB^{-1} = A^{-1}$  より、 $\langle A \rangle \triangleleft G$  である。 $A^3$  は  $\langle A \rangle$  の元で位数が 2 であるような唯一の元なので  $BA^3B = A^3$  である。つまり  $A^3$  は  $G$  の中心  $Z(G)$  の元である。したがって  $\langle A^3, B \rangle = \{I, A^3, B, A^3B\}$  であり  $G$  は位数 4 の部分群を持つ。 $G$  が位数 3 の部分群を持つことは  $A^2$  の位数が 3 であることからあきらかなので、 $\#G \geq 12$  を得る。つまり  $\#G = 12$  ということである。
- (ii)  $Z = A^i B^j$  ( $0 \leq i \leq 5, 0 \leq j \leq 1$ ) が  $Z(G)$  の元だったとする。このとき

$$\begin{aligned} AZA^{-1}Z^{-1} &= A^{i+1}B^jA^{-1}B^{-j}A^{-i} \\ &= A^{i+1}(B^jAB^{-j})^{-1}A^{-i} \\ &= A^{i+1}(A^{1-2j})^{-1}A^{-i} \\ &= A^{2j} \end{aligned}$$

だから  $j = 0$  でなくてはならない。また

$$\begin{aligned} BZBZ^{-1} &= BA^iBA^{-1} \\ &= A^{-i}A^{-i} \\ &= A^{-2i} \end{aligned}$$

より  $i = 0, 3$  でなくてはならない。よって  $Z(G) = \{I, A^3\}$  である。これで  $\#Z(G) = 2$  が示せた。

- (iii) 各々の元の共役類を求めて位数の表を作ると次のようになる。

位数	元	個数
1	$I$	1
2	$B, A^2B, A^4B, A^3, AB, A^3B, A^5B$	7
3	$A^2, A^4$	2
6	$A, A^5$	2

よって位数 2 の元の数 は 7 個。

問 5

3次元微分多様体  $M = \{(x, y, z, w) \in \mathbb{R}^4 \mid xy - z^2 = w\}$  から  $\mathbb{R}^3$  への写像  $f = (f_1, f_2, f_3): M \rightarrow \mathbb{R}^3$  を

$$f(x, y, z, w) = (x + y, z, w)$$

により定める。以下の問に答えよ。

- (i)  $f$  の臨界点の集合  $C$  を求めよ。ただし  $p \in M$  が  $f$  の臨界点であるとは、 $p$  のまわりの  $M$  の座標系  $(u_1, u_2, u_3)$  に関する  $f$  のヤコビ行列

$$\left( \frac{\partial f_i}{\partial u_j} \right)_{1 \leq i, j \leq 3}$$

が正則でないことである。

- (ii)  $C$  が  $M$  の部分多様体になることを証明せよ。

解答.

- (i)  $g: \mathbb{R}^4 \rightarrow \mathbb{R}$  を  $g(x, y, z, w) = xy - z^2 - w$  により定める。このとき  $M = g^{-1}(0)$  であり、 $f$  の微分  $df_p: T_p M \rightarrow \mathbb{R}^3$  は  $f$  の  $\mathbb{R}^4$  への延長のヤコビアン  $Jf_p: \mathbb{R}^4 \rightarrow \mathbb{R}^3$  の  $\text{Ker } Jg_p$  への制限だとみなせる。したがって  $p \in M$  に対して

$$\begin{aligned} p \in C &\iff \text{rank } df_p \leq 2 \\ &\iff \dim \text{Ker } df_p \geq 1 \\ &\iff \dim(\text{Ker } Jf_p \cap \text{Ker } Jg_p) \geq 1 \\ &\iff \dim \text{Ker} \begin{pmatrix} Jg_p \\ JF_p \end{pmatrix} \geq 1 \\ &\iff \text{rank} \begin{pmatrix} Jg_p \\ JF_p \end{pmatrix} \leq 3 \\ &\iff \text{rank} \begin{pmatrix} y & x & -2z & -1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \leq 3 \\ &\iff x = y \end{aligned}$$

だから  $C = \{(x, y, z, w) \in \mathbb{R}^4 \mid xy - z^2 = w, x = y\}$  である。

- (ii)  $h: M \rightarrow \mathbb{R}$  を  $h(x, y, z, w) = x - y$  で定める。任意の点  $p \in h^{-1}(0)$  が正則点であることをいえばよい。計算すると

$$\begin{aligned} \text{rank } dh_p &= 3 - \dim \text{Ker } dh_p \\ &= 3 - \dim \text{Ker} \begin{pmatrix} Jg_p \\ Jh_p \end{pmatrix} \\ &= \text{rank} \begin{pmatrix} Jg_p \\ Jh_p \end{pmatrix} - 1 \\ &= 1 \end{aligned}$$

である。よって 0 は  $h$  の正則値であり、示すべきことがいえた。

問 6

$A(z) = (a_{ij}(z))_{1 \leq j, k \leq N}$  を  $N$  次正方行列、 $D = \{z \in \mathbb{C} \mid |z| < 1\}$  を単位円板、 $m$  を正の整数とし、以下の (A), (B) を仮定する。

(A) 各  $a_{jk}(z)$  は  $D$  上の正則関数である。

(B)  $\det A(z)$  は  $z = 0$  に  $m$  位の零点をもつ。

このとき、十分に小さい正数  $\varepsilon$  に対して、次式が成り立つことを示せ。

$$m = \operatorname{tr} \left( \frac{1}{2\pi i} \int_{C_\varepsilon} A(z)^{-1} \frac{d}{dz} A(z) dz \right)$$

ここで積分路  $C_\varepsilon$  は円周  $C_\varepsilon = \{z \in \mathbb{C} \mid |z| = \varepsilon\}$  を正の向きに一周するものとし、 $\operatorname{tr}(X)$  は行列  $X$  のトレースを表す。

解答. 偏角の原理により、次を示せば十分である。

$$\operatorname{tr} \left( A^{-1} \frac{dA}{dz} \right) = \frac{(\det A)'}{\det A}$$

いま  $A$  の余因子行列を  $B$  とする。つまり  $B$  の  $(i, j)$  成分  $b_{ij}$  を

$$b_{ij} = (-1)^{i+j} \det A_{ji}$$

により定める。ただし  $A_{ji}$  とは  $A$  の  $j$  行目と  $i$  列目を飛ばした  $(N-1)$  次正方行列のことである。このとき  $A^{-1}$  は  $B$  を  $\det A$  で割ったものとなる。そうすると  $C := A^{-1} \frac{dA}{dz}$  の  $(i, j)$  成分  $c_{ij}$  は

$$\begin{aligned} c_{ij} &= \frac{1}{\det A} \sum_{k=1}^N b_{ik} a'_{kj} \\ &= \frac{1}{\det A} \sum_{k=1}^N (-1)^{i+k} \det A_{ki} a'_{kj} \end{aligned}$$

である。したがって  $a_i$  で  $A$  の  $i$  列目を表すことにすると

$$\begin{aligned} (\det A) \operatorname{tr} C &= \sum_{i,k} (-1)^{i+k} \det A_{ki} a'_{ki} \\ &= \sum_k (-1)^{1+k} \det A_{k1} a'_{k1} + \cdots + \sum_k (-1)^{N+k} \det A_{kN} a'_{kN} \\ &= \det(a'_1, a_2, \cdots, a_N) + \cdots + \det(a_1, \cdots, a_{N-1}, a'_N) \\ &= (\det A)' \end{aligned}$$

である。

## ■ 平成 28 年度 専門科目

---

### 問 1

有理数係数の既約多項式  $f(x) = x^3 + ax + b$  を考え、 $K \subset \mathbb{C}$  を  $f(x)$  の最小分解体とする。 $a > 0$  のとき、 $K/\mathbb{Q}$  の Galois 群が 3 次対称群と同型であることを示せ。

解答.  $\lim_{x \rightarrow +\infty} f(x) = +\infty$ ,  $\lim_{x \rightarrow -\infty} f(x) = -\infty$  より、 $f$  は連続なので  $f(\beta_1) = 0$  なる  $\beta_1 \in \mathbb{R}$  がある。 $f'(x) = 3x^2 + a > 0$  より  $f$  は単調増加なので  $f$  の実根は  $\beta_1$  のみである。そこで  $f$  の残りの根を  $\beta_2, \beta_3$  とすると  $\beta_2 = \overline{\beta_3}$  である。いま  $G = \text{Gal}(K/\mathbb{Q})$  を根への作用により 3 次対称群  $S_3$  の部分群とみなす。 $G$  は複素共役をとる写像を含むので、 $\#G$  は偶数でなくてはならない。また  $f$  は既約と仮定したので、 $G$  は集合  $\{1, 2, 3\}$  に推移的に作用するはずであり、とくに  $\#G$  は 3 の倍数である。よって  $\#G$  は 6 の倍数となるが、 $\#S_3 = 6$  なので  $G \cong S_3$  となるしかない。

## 問 2

$K$  を標数が 2 でない代数的閉体とし、 $K$  の元  $a$  に対して、2 変数多項式環  $K[X, Y]$  の剰余環

$$R_a = K[X, Y]/(X^2 - Y^2 - X - Y - a)$$

を考える。以下の問に答えよ。

- (i)  $a = 0$  のとき  $R_a$  の各極大イデアル  $\mathfrak{m}$  に対して  $\dim_K(\mathfrak{m}/\mathfrak{m}^2)$  を求めよ。また  $\mathfrak{m}$  はいつ  $R_a$  の単項イデアルとなるか？理由をつけて答えよ。
- (ii)  $a \neq 0$  のとき  $R_a$  の各極大イデアル  $\mathfrak{m}$  に対して  $\dim_K(\mathfrak{m}/\mathfrak{m}^2)$  を求めよ。また  $\mathfrak{m}$  はいつ  $R_a$  の単項イデアルとなるか？理由をつけて答えよ。

解答. 式を変形すると  $X^2 - Y^2 - X - Y - a = (X + Y)(X - Y - 1) - a$  である。いま  $K$  の標数は 2 ではないと仮定したので

$$\begin{aligned} K[S, T] &\rightarrow K[X, Y] \\ S &\mapsto X + Y \\ T &\mapsto X - Y - 1 \end{aligned}$$

という  $K$  準同型を考えると、これは

$$\begin{aligned} K[X, Y] &\rightarrow K[S, T] \\ X &\mapsto (S + T + 1)/2 \\ Y &\mapsto (S - T - 1)/2 \end{aligned}$$

を逆写像とする同型である。これにより  $R_a$  は

$$U_a := K[S, T]/(ST - a)$$

に対応する。 $U_a$  の極大イデアルを表すのに、記号の濫用だが  $R_a$  の極大イデアルと同じ記号  $\mathfrak{m}$  を使うことにする。いま  $U_a$  の極大イデアル  $\mathfrak{m}$  は、 $E := K[S, T]$  の極大イデアル  $\mathfrak{n}$  であって  $(ST - a)$  を含むものに対応している。Hilbert の零点定理により、 $E/\mathfrak{n}$  は  $K$  の有限次拡大である。 $K$  は代数閉という仮定があったので、 $E/\mathfrak{n} \cong K$  である。この同型による  $S, T$  の像をそれぞれ  $\beta, \gamma \in K$  とする。すると  $(S - \beta, T - \gamma) \subset \mathfrak{n}$  であるが  $(S - \beta, T - \gamma)$  は極大イデアルなので  $(S - \beta, T - \gamma) = \mathfrak{n}$  である。まとめると、 $\mathfrak{n}$  は  $\beta\gamma = a$  なる  $\beta, \gamma$  によって  $\mathfrak{n} = (S - \beta, T - \gamma)$  と表されることがわかった。このことを踏まえて考察をしていく。

- (i)  $a = 0$  のとき  $\beta\gamma = 0$  なので  $\beta = 0$  または  $\gamma = 0$  である。どちらでも同じことなので  $\beta = 0$  とする。 $\gamma = 0$  である場合には

$$\begin{aligned} \mathfrak{m}/\mathfrak{m}^2 &= ((S, T)/ST)/((S^2, ST, T^2)/ST) \\ &\cong (S, T)/(S^2, ST, T^2) \\ &\cong K^2 \end{aligned}$$

だから  $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = 2$  である。もし  $\mathfrak{m}$  が  $U_0$  の単項イデアルなら  $\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{m} \otimes_{U_0} K \cong K$  となるはずだから、 $\mathfrak{m}$  は単項イデアルではない。

$\gamma \neq 0$  のとき。このときには

$$\begin{aligned}(T - \gamma)U_0 &= (T - \gamma, ST)/ST \\ &= (S(T - \gamma), T - \gamma, ST)/ST \\ &= (S, T - \gamma)/ST \\ &= \mathfrak{m}\end{aligned}$$

だから  $\mathfrak{m}$  は単項イデアルである。とくに  $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = 1$  となる。

以上の結果をまとめると

$$\dim_K(\mathfrak{m}/\mathfrak{m}^2) = \begin{cases} 1 & (\beta, \gamma) \neq (0, 0) \text{ のとき。このとき } \mathfrak{m} \text{ は単項イデアル} \\ 2 & (\beta, \gamma) = (0, 0) \text{ のとき} \end{cases}$$

である。 $U_0$  から  $R_0$  に話を戻すと

$$\dim_K(\mathfrak{m}/\mathfrak{m}^2) = \begin{cases} 1 & (b, c) \neq (1/2, 1/2) \text{ のとき。このとき } \mathfrak{m} \text{ は単項イデアル} \\ 2 & (b, c) = (1/2, 1/2) \text{ のとき} \end{cases}$$

がわかったことになる。ただし、 $b, c$  は  $\mathfrak{m} = (X - b, Y - c)/(X^2 - Y^2 - X - Y)$  となるような  $b, c \in K$  である。

(ii) 再び  $U_a$  に話を持っていく。 $a \neq 0$  のとき  $\beta \neq 0$  かつ  $\gamma \neq 0$  である。このとき

$$\begin{aligned}(S - \beta)U_0 &= (S - \beta, ST - a)/(ST - a) \\ &= (T(S - \beta), S - \beta, ST - a)/(ST - a) \\ &= (\beta(T - \gamma), S - \beta, ST - a)/(ST - a) \\ &= (T - \gamma, S - \beta)/(ST - a) \\ &= \mathfrak{m}\end{aligned}$$

だから  $\mathfrak{m}$  は単項イデアルであり、とくに  $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = 1$  がわかる。

### 問 3

位数が奇素数  $p$  である有限体  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  を考え、

$$G = GL_2(\mathbb{F}_p) = \{X \in M_2(\mathbb{F}_p) \mid \det X \neq 0\}$$

とおく。ただし、 $M_2(\mathbb{F}_p)$  は  $\mathbb{F}_p$  の元を成分とする 2 次正方行列全体の集合を表す。以下の問に答えよ。

- (i)  $G$  の元で対角行列と共役でないものの個数を求めよ。
- (ii)  $G$  の 2 つの元  $X, Y$  の最小多項式  $\phi_X(t), \phi_Y(t) \in \mathbb{F}_p[t]$  が一致すれば、 $X$  と  $Y$  は互いに共役であることを示せ。
- (iii) 対角行列を含まない  $G$  の共役類の個数を求めよ。

解答. 以下単位行列を  $E$  で表すことにする。

- (i) まず、行列の正則性と列ベクトルの一次独立性は同値なので  $\#G = (p^2 - 1)(p^2 - p) = p(p - 1)^2(p + 1)$  である。 $G$  の対角行列の全体を  $\Lambda$  とする。 $T \in \Lambda$  は対角成分を入れ替えたものと共役であるので、 $\Lambda$  の共役類は定数行列と、対角成分の入れ替えを無視した定数でない対角行列で代表される。 $G$  の元のうち定数行列全体を  $\Lambda_0$  で、定数でない対角行列の全体を  $\Lambda_1$  であらわすことにする。 $G$  の  $G$  自身への共役による作用を考えると、 $G$  の元のうち対角行列と共役なもの個数は

$$\#\Lambda_0 + \frac{1}{2} \sum_{T \in \Lambda_1} \# \text{Orbit}(T)$$

で求まる。 $\# \text{Orbit}(T) = \#G / \# \text{Stab}(T)$  なので、群  $\text{Stab}(T)$  を決定すればよい。いま  $T \in \Lambda_1$  と  $A \in G$  をとり

$$T = \begin{pmatrix} \beta & 0 \\ 0 & \gamma \end{pmatrix}, \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

とおく。このとき計算すると

$$AT - TA = (\beta - \gamma) \begin{pmatrix} 0 & -b \\ c & 0 \end{pmatrix}$$

なので  $A \in \text{Stab}(T)$  であるということは  $b = c = 0$  を意味する。よって  $T$  に依存せずに  $\# \text{Stab}(T) = \#\Lambda = (p - 1)^2$  であり  $G$  の元のうち対角行列と共役なもの個数は

$$(p - 1) + \frac{1}{2}(p - 1)(p - 2)p(p + 1) = \frac{(p - 1)^2(p^2 - 2)}{2}$$

である。ゆえに求めるべき、対角行列と共役でない元の個数は

$$\#G - \frac{(p - 1)^2(p^2 - 2)}{2} = \frac{1}{2}(p - 1)^2(p^2 + 2p + 2)$$

である。

- (ii)  $X$  と  $Y$  の最小多項式が一致していると仮定し、 $\phi = \phi_X = \phi_Y$  とおく。 $\phi$  がどういう式であるかにより場合分けをする。 $V = \mathbb{F}_p^2$  とおく。

まず  $\phi(t) = t - \lambda$  と表されるとき。このとき  $X$  と  $Y$  は定数行列  $\lambda E$  に一致するので、とくに共役となる。

次に  $\phi(t) = (t - \lambda_1)(t - \lambda_2)$  ( $\lambda_1 \neq \lambda_2$ ) と表されるとき。このとき  $X$  と  $Y$  は  $\mathbb{F}_p$  上対角化可能であり、同じ対角行列と共役である。よって互いに共役となる。

次に  $\phi(t) = (t - \lambda)^2$  という形のとき。このとき  $\dim \text{Ker}(X - \lambda E) = 1$  かつ  $\dim \text{Ker}(X - \lambda E)^2 = 2$  であるので、 $v \in \text{Ker}(X - \lambda E) \setminus \{0\}$  と  $w \in \text{Ker}(X - \lambda E)^2 \setminus \text{Ker}(X - \lambda E)$  をとると  $\{v, w\}$  は  $V$  の基底となる。このとき

$$\begin{aligned} Xv &= \lambda v \\ Xw &= cv + dw \end{aligned}$$

なる  $c, d \in \mathbb{F}_p$  がある。  $c \neq 0$  なので  $w$  を  $c^{-1}w$  で置き換えて  $c = 1$  としてよい。このとき

$$\begin{aligned} (X - dE)w &= v \\ (X - dE)v &= (\lambda - d)v \end{aligned}$$

より  $\det(X - dE) = 0$  だから  $d = \lambda$  である。したがって

$$\begin{aligned} Xv &= \lambda v \\ Xw &= v + \lambda w \end{aligned}$$

だから  $X$  は  $\mathbb{F}_p$  係数の正則行列で共役をとることにより Jordan 標準形に変形できる。これは  $Y$  についても同様なので  $X$  と  $Y$  は共役。

最後に  $\phi$  が  $\mathbb{F}_p[t]$  の 2 次既約多項式であった場合。  $X$  が定める  $R := \mathbb{F}_p[t]$  の  $V$  への作用  $R \times V \rightarrow V$  は作用  $\varphi_A: R/(\phi) \times V \rightarrow V$  を誘導する。  $\phi$  は既約で  $R$  は PID なので、  $(\phi) \subset R$  は極大イデアルである。したがって  $R/(\phi)$  は位数  $p^2$  の有限体  $F := \mathbb{F}_{p^2}$  と同型である。これにより  $V$  を  $F$  ベクトル空間と見なす。  $\#V = \#F$  なので次元は 1 である。よって  $v \in V \setminus \{0\}$  を固定したとき、写像

$$\begin{aligned} F \times \{v\} &\xrightarrow{\varphi_A} V \\ (f, v) &\mapsto f \cdot v = f(A)v \end{aligned}$$

は  $F$  同型である。以上の議論は  $Y$  についても同様に適用できて、  $\varphi_B: F \times \{v\} \rightarrow V$  も  $\varphi_A$  と同様に  $F$  同型となる。よって次の図式

$$\begin{array}{ccc} F \times \{v\} & \xrightarrow{\varphi_A} & V \\ & \searrow \varphi_B & \downarrow T \\ & & V \end{array}$$

を可換にするような  $F$  同型  $T$  が存在する。  $F$  同型は  $\mathbb{F}_p$  同型でもあるので、  $T$  を表現する正則行列  $P \in G$  がある。このとき

$$\forall f \in F \quad Pf(A)v = f(B)v$$

だから、とくに

$$\begin{aligned} PAv &= Bv \\ PA^2v &= B^2v \\ PA^3v &= B^3v \end{aligned}$$



である。よって

$$\begin{aligned}
B^2v &= PA^2v \\
&= PAP^{-1}PAv \\
&= PAP^{-1}Bv \\
B^3v &= PA^3v \\
&= PAP^{-1}PA^2v \\
&= PAP^{-1}B^2v
\end{aligned}$$

だから

$$\begin{aligned}
(PAP^{-1} - B)Bv &= 0 \\
(PAP^{-1} - B)B^2v &= 0
\end{aligned}$$

である。いま  $B$  の最小多項式は 2 次式なので、 $B^2v = aBv + bv$  なる  $a \in \mathbb{F}_p$  と  $b \in \mathbb{F}_p^\times$  がある。よって  $(PAP^{-1} - B)v = 0$  である。 $\phi$  が既約という仮定より  $B$  は固有ベクトルを持たないので、 $\{v, Bv\}$  は  $V$  の  $\mathbb{F}_p$  基底となる。よって  $PAP^{-1} = B$  を得る。これですべての場合を尽くせたので、示すべきことがいえた。

- (iii) 共役ならば最小多項式が同じになることはあきらかなので、(ii) により共役であることと最小多項式が一致することの同値性がいえた。 $G$  の共役類の全体を  $C(G)$  とおくと、最小多項式を対応させる写像

$$\Phi: C(G) \rightarrow \{t^2 + at + b \mid b \neq 0\} \cup \{t + c \mid c \neq 0\}$$

が単射であることがわかったことになる。逆に

$$t^2 + at + b = \det \left( tE - \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} \right)$$

であるから、 $\Phi$  は全射でもある。対角行列を含まない  $G$  の共役類は、 $\Phi$  によって  $(t - \lambda)^2$  という形の式か 2 次既約多項式に対応するので、その個数は

$$(p-1) + \left( p^2 - p - \frac{(p-1)(p-2)}{2} \right) = \frac{(p+2)(p-1)}{2}$$

である。

## ■ 平成 27 年度 基礎科目 I

---

### 問 1

次の広義積分を求めよ。

$$\iint_D \frac{y^2 e^{-xy}}{x^2 + y^2} dx dy$$

ここで、 $D = \{(x, y) \in \mathbb{R}^2 \mid 0 < y \leq x\}$  とする。

解答.  $x = r \cos \theta$ ,  $y = r \sin \theta$  とおくと  $dx dy = r dr d\theta$  であって

$$\begin{aligned} \iint_D \frac{y^2 e^{-xy}}{x^2 + y^2} dx dy &= \int_0^{\pi/4} d\theta \int_0^\infty r \sin^2 \theta e^{-r^2 \sin \theta \cos \theta} dr \\ &= \frac{1}{2} \int_0^{\pi/4} \sin^2 \theta \left( \int_0^\infty e^{-s \sin \theta \cos \theta} ds \right) d\theta \\ &= \frac{1}{2} \int_0^{\pi/4} \frac{\sin \theta}{\cos \theta} d\theta \\ &= -\frac{1}{2} \int_1^{1/\sqrt{2}} \frac{dt}{t} \\ &= \frac{\log 2}{4} \end{aligned}$$

## 問 2

$\mathbb{R}^2$  で定義された関数

$$f(x, y) = \frac{4x^2 + (y+2)^2}{x^2 + y^2 + 1}$$

のとりうる値の範囲を求めよ。

解答.  $f \geq 0$  であり  $f(0, -2) = 0$  なので  $\min f = 0$  はあきらか。最大値を求めよう。  $x = r \cos \theta$ ,  $y = r \sin \theta$  とおくと

$$f(x, y) = 4 + \frac{-3r^2 \sin^2 \theta + 4r \sin \theta}{r^2 + 1}$$

である。  $t = \sin \theta$  とおく。このとき  $-1 \leq t \leq 1$  であって

$$f - 4 = \frac{3r^2}{r^2 + 1} \left( - \left( t - \frac{2}{3r} \right)^2 + \frac{4}{9r^2} \right)$$

である。したがって

$$g = - \left( t - \frac{2}{3r} \right)^2 + \frac{4}{9r^2}$$

としたとき

$$\max(f - 4) = \max_{r \geq 0} \frac{3r^2}{r^2 + 1} \left( \max_{-1 \leq t \leq 1} g(r, t) \right)$$

である。いま

$$\max_{-1 \leq t \leq 1} g(r, t) = \begin{cases} g(2/3r) = 4/(9r^2) & (2/3 \leq r) \\ g(1) = (4 - 3r)/3r & (0 \leq r \leq 2/3) \end{cases}$$

だから

$$\max(f - 4) = \max \left\{ \max_{r \geq 2/3} \frac{4}{3(r^2 + 1)}, \max_{0 \leq r \leq 2/3} \frac{r(4 - 3r)}{r^2 + 1} \right\}$$

が判る。あきらかに

$$\max_{r \geq 2/3} \frac{4}{3(r^2 + 1)} = \frac{12}{13}$$

である。また  $h(r) = r(4 - 3r)/(r^2 + 1)$  とおくと  $h'(r) = -4(r - 1/2)(r + 2)/(r^2 + 1)^2$  だから

$$\max_{0 \leq r \leq 2/3} h(r) = h(1/2) = 1$$

である。すなわち  $\max f = 5$  である。 $f$  は連続関数なのでとりうる値の範囲は区間  $[0, 5]$  ということになる。

### 問 3

$a, b$  を複素数とする。3 次正方行列

$$A = \begin{pmatrix} 2 & a & a \\ b & 2 & 0 \\ -b & 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

について、以下の問に答えよ。

- (i) 行列  $A$  の固有値を求めよ。
- (ii) 行列  $A$  と行列  $B$  が相似となるような複素数  $a, b$  をすべて求めよ。ただし、 $A$  と  $B$  が相似であるとは、複素正則行列  $P$  で  $A = P^{-1}AP$  をみたすものが存在するときをいう。

解答.

- (i) 固有多項式  $\Phi_A(\lambda)$  は  $(\lambda - 2)^3$  なので、固有値は 2 のみ。
- (ii)  $A$  の Jordan 標準形が  $B$  になるのはいつかを求めればよい。それは  $\text{rank}(2 - A) = 1$  と同値である。計算すると

$$\text{rank}(2 - A) = \text{rank} \begin{pmatrix} 0 & a & a \\ b & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

だから  $A$  と  $B$  が相似になるのは  $a = 0, b \neq 0$  または  $a \neq 0, b = 0$  のとき。

問 4

$a, b, c, d$  を複素数とする。次の行列の階数を求めよ。

$$\begin{pmatrix} 2 & -3 & 6 & 0 & -6 & a \\ -1 & 2 & -4 & 1 & 8 & b \\ 1 & 0 & 0 & 1 & 6 & c \\ 1 & -1 & 2 & 0 & -1 & d \end{pmatrix}$$

解答. 問題の行列を  $A$  とおく。行基本変形で変形していくと

$$\begin{aligned} A &\sim \begin{pmatrix} 2 & -3 & 6 & 0 & -6 & a \\ -1 & 2 & -4 & 1 & 8 & b \\ 1 & 0 & 0 & 1 & 6 & c \\ 1 & -1 & 2 & 0 & -1 & d \end{pmatrix} \\ &\sim \begin{pmatrix} 0 & -1 & 2 & 0 & -4 & a-2d \\ 0 & 1 & -2 & 1 & 7 & b+d \\ 0 & 1 & -2 & 1 & 7 & c+d \\ 1 & -1 & 2 & 0 & -1 & d \end{pmatrix} \\ &\sim \begin{pmatrix} 0 & -1 & 2 & 0 & -4 & a-2d \\ 0 & 0 & 0 & 1 & 3 & a+b-d \\ 0 & 0 & 0 & 1 & 3 & a+c-3d \\ 1 & 0 & 0 & 0 & 3 & -a+3d \end{pmatrix} \\ &\sim \begin{pmatrix} 0 & -1 & 2 & 0 & -4 & a-2d \\ 0 & 0 & 0 & 1 & 3 & a+b-d \\ 0 & 0 & 0 & 0 & 0 & -b+c-2d \\ 1 & 0 & 0 & 0 & 3 & -a+3d \end{pmatrix} \end{aligned}$$

だから  $-b+c-2d \neq 0$  のとき  $\text{rank } A = 4$  であり、 $-b+c-2d = 0$  のとき  $\text{rank } A = 3$  である。

## ■ 平成 27 年度 基礎科目 II

### 問 1

$f(x), \phi(x)$  は区間  $[0, \infty)$  上の実数値連続関数とし、さらに  $\phi(x)$  は

$$\phi(x) = \phi(x+1) \quad (x \geq 0)$$

$$\int_0^1 \phi(x) dx = 1$$

をみたすとする。このとき、任意の実数  $a > 0$  に対し

$$\lim_{\lambda \rightarrow \infty} \int_0^a f(x) \phi(\lambda x) dx = \int_0^a f(x) dx$$

が成り立つことを示せ。

解答. 示すべきことは

$$\lim_{\lambda \rightarrow \infty} \int_0^a f(x) (\phi(\lambda x) - 1) dx = 0$$

なので  $\psi(x) = \phi(x) - 1$  とおく。  $\varepsilon > 0$  が任意に与えられたとする。

$$I_\lambda = \int_0^a f(x) \psi(\lambda x) dx$$

とおく。すると

$$I_\lambda = \frac{1}{\lambda} \int_0^{a\lambda} f(y/\lambda) \psi(y) dy$$

である。  $a\lambda = n + b$  なる  $n \in \mathbb{Z}$  と  $0 \leq b < 1$  をとると

$$I_\lambda = \frac{1}{\lambda} \sum_{k=0}^{n-1} \int_k^{k+1} f(y/\lambda) \psi(y) dy + \frac{1}{\lambda} \int_n^{n+b} f(y/\lambda) \psi(y) dy$$

となるが、ここで  $M = \int_0^1 |\psi(x)| dx$  とすると

$$\int_n^{n+b} |f(y/\lambda) \psi(y)| dy \leq \sup_{0 \leq x \leq a} |f(x)| M$$

だから  $\lambda \rightarrow \infty$  のとき第 2 項は無視してよい。よって

$$I_\lambda = \frac{1}{\lambda} \sum_{k=0}^{n-1} \int_k^{k+1} f(y/\lambda) \psi(y) dy + O(1/\lambda)$$

であるが、

$$0 = \frac{1}{\lambda} \sum_{k=0}^{n-1} f(k/\lambda) \int_k^{k+1} \psi(y) dy$$

であることから

$$|I_\lambda| \leq \frac{1}{\lambda} \sum_{k=0}^{n-1} \int_k^{k+1} |f(y/\lambda) - f(k/\lambda)| |\psi(y)| dy + O(1/\lambda)$$

である。ここで  $0 \leq y \leq n$  のとき  $0 \leq y/\lambda \leq a$  であることに注意する。 $f$  は  $[0, a]$  上一様連続なので

$$|x - y| < \delta \rightarrow |f(x) - f(y)| < \varepsilon$$

なる  $\delta > 0$  がある。そこで  $\lambda > 1/\delta$  とすると

$$\begin{aligned} |I_\lambda| &\leq \frac{n\varepsilon}{\lambda} M + O(1/\lambda) \\ &\leq aM\varepsilon + O(1/\lambda) \end{aligned}$$

が成り立つ。 $\lambda \rightarrow \infty$  として  $\limsup_{\lambda \rightarrow \infty} |I_\lambda| \leq a\varepsilon M$  を得る。 $\varepsilon > 0$  は任意だったので  $\lim_{\lambda \rightarrow \infty} I_\lambda = 0$  である。

## 問 2

$n$  を正の整数とし、 $A$  を  $n$  次実正方行列で、交代行列であるとする。すなわち  $A$  の転置行列  ${}^tA$  が  $-A$  に一致するとする。このとき、以下の間に答えよ。

- (i) 任意の列ベクトル  $\mathbf{u} \in \mathbb{R}^n$  に対し  $\|(E - A)\mathbf{u}\| \geq \|\mathbf{u}\|$  が成立することを示せ。ただし  $E$  は単位行列であり、 $\mathbf{u}$  はユークリッドノルム  $\sqrt{{}^t\mathbf{u}\mathbf{u}}$  である。
- (ii)  $E - A$  は正則行列であり、 $(E + A)(E - A)^{-1}$  は直行行列となることを示せ。

解答.

- (i)  $A$  は実行列と仮定したので  $A$  の随伴行列は  ${}^tA$  に等しい。よって

$$\begin{aligned}
 \langle (E - A)\mathbf{u}, (E - A)\mathbf{u} \rangle &= \langle \mathbf{u} - A\mathbf{u}, \mathbf{u} - A\mathbf{u} \rangle \\
 &= \langle \mathbf{u}, \mathbf{u} \rangle - \langle \mathbf{u}, A\mathbf{u} \rangle - \langle A\mathbf{u}, \mathbf{u} \rangle + \langle A\mathbf{u}, A\mathbf{u} \rangle \\
 &= \langle \mathbf{u}, \mathbf{u} \rangle - \langle {}^tA\mathbf{u}, \mathbf{u} \rangle - \langle A\mathbf{u}, \mathbf{u} \rangle + \langle A\mathbf{u}, A\mathbf{u} \rangle \\
 &= \langle \mathbf{u}, \mathbf{u} \rangle + \langle A\mathbf{u}, A\mathbf{u} \rangle \\
 &\geq \langle \mathbf{u}, \mathbf{u} \rangle
 \end{aligned}$$

である。

- (ii) (i) より、 $\mathbf{u} \neq 0$  ならば  $(E - A)\mathbf{u} \neq 0$  なので  $E - A$  は正則。  $B = (E - A)^{-1}$  とおく。このとき  $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$  に対して

$$\begin{aligned}
 \langle (E + A)B\mathbf{u}, (E + A)B\mathbf{v} \rangle &= \langle {}^t(E + A)(E + A)B\mathbf{u}, B\mathbf{v} \rangle \\
 &= \langle (E - A)(E + A)B\mathbf{u}, B\mathbf{v} \rangle \\
 &= \langle (E + A)(E - A)B\mathbf{u}, B\mathbf{v} \rangle \\
 &= \langle (E + A)\mathbf{u}, B\mathbf{v} \rangle \\
 &= \langle \mathbf{u}, {}^t(E + A)B\mathbf{v} \rangle \\
 &= \langle \mathbf{u}, \mathbf{v} \rangle
 \end{aligned}$$

であるから  $(E + A)B$  は等長、つまり直行行列である。



### 問 3

$a$  を正の実数とすると、次の広義積分を求めよ。

$$\int_{-\infty}^{\infty} \frac{x \sin x}{(x^2 + a^2)^2} dx$$

解答.  $z \in \mathbb{C}$  に対して

$$f(z) = \frac{ze^{iz}}{(z^2 + a^2)^2}$$

とおく。求める積分は

$$I = \operatorname{Im} \int_{-\infty}^{\infty} f(x) dx$$

である。 $R > 0$  に対して、反時計まわりに半径  $R$  の半円  $\{Re^{i\theta} \mid 0 \leq \theta \leq \pi\}$  を描くような積分路を  $C_R$  とかく。 $S_R = [-R, R] \cup C_R$  とおこう。このとき留数定理から

$$\forall R > 0 \quad \int_{S_R} f(z) dz = 2\pi i \operatorname{Res}(f, ai)$$

が成り立つ。

$R \rightarrow \infty$  のときの  $C_R$  上での積分を評価しよう。 $z = Re^{i\theta}$  において計算すると

$$\begin{aligned} \int_{S_R} |f(z)| dz &\leq \frac{R^2}{(R^2 - a^2)^2} \int_0^\pi e^{-R \sin \theta} d\theta \\ &\leq \frac{R^2 \pi}{(R^2 - a^2)^2} \end{aligned}$$

である。したがって  $R \rightarrow \infty$  のとき左辺は収束して 0 になる。これにより

$$\int_{-\infty}^{\infty} f(x) dx = 2\pi i \operatorname{Res}(f, ai)$$

が判ったことになる。

$b = ai$  とおく。 $f$  の  $b$  での留数を求めたい。

$$g(z) = \frac{ze^{iz}}{(z + b)^2}$$

とすると  $g(z)(z - b)^{-2} = f(z)$  である。 $g$  は  $z = b$  で正則なので、 $g$  の  $z = b$  の周りでの Taylor 展開の一次の係数を求めればよい。つまり

$$\operatorname{Res}(f, ai) = g'(b)$$

である。計算すると

$$g'(z) = \frac{e^{iz}((1 + iz)(z + b) - 2z)}{(z + b)^3}$$

だから代入して

$$g'(b) = \frac{ie^{ib}}{4b} = \frac{e^{-a}}{4a}$$

を得る。よって

$$I = \operatorname{Im} \left( 2\pi i \cdot \frac{e^{-a}}{4a} \right) = \frac{\pi e^{-a}}{2a}$$

である。

#### 問 4

| 1 以上 3500 以下の整数  $x$  のうち、 $x^3 + 3x$  が 3500 で割り切れるものの個数を求めよ。

解答.  $3500 = 2^2 \times 5^3 \times 7$  なので、中国剰余定理より  $\mathbb{Z}/3500\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$  である。いま  $\mathbb{Z}/4\mathbb{Z}$  で  $x$  に値を代入することにより調べると  $x^3 + 3x = 0 \in \mathbb{Z}/4\mathbb{Z} \iff x = 0, \pm 1$  がわかる。

$\mathbb{Z}/7\mathbb{Z}$  で考えると  $x^3 + 3x = x(x^2 + 3) = x(x^2 - 4) = x(x + 2)(x - 2)$  であり、 $\mathbb{Z}/7\mathbb{Z}$  は整域だから  $x^3 + 3x = 0 \in \mathbb{Z}/7\mathbb{Z} \iff x = 0, \pm 2$  が判る。

$\mathbb{Z}/125\mathbb{Z}$  で考える。 $x^3 + 3x = x(x^2 + 3)$  であるが、 $x^2 + 3$  は決して 5 の倍数にならないので  $\mathbb{Z}/125\mathbb{Z}$  において常に単元である。よって  $x^3 + 3x = 0 \in \mathbb{Z}/125\mathbb{Z} \iff x = 0$  が判る。

以上の議論により求める  $x$  の個数は  $3 \times 3 \times 1 = 9$  個である。

問 5

2次元球面

$$S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$$

上の関数

$$f(x, y, z) = xy + yz + zx$$

の臨界点をすべて求め、それらが非退化かどうかを答えよ。

ただし、 $p \in S^2$  が  $f$  の臨界点であるとは、 $S^2$  の  $p$  のまわりの局所座標  $(u, v)$  に関して

$$\frac{\partial f}{\partial u}(p) = \frac{\partial f}{\partial v}(p) = 0$$

となることである。また、 $f$  の臨界点  $p$  は

$$\begin{pmatrix} \frac{\partial^2 f}{\partial u^2}(p) & \frac{\partial^2 f}{\partial u \partial v}(p) \\ \frac{\partial^2 f}{\partial u \partial v}(p) & \frac{\partial^2 f}{\partial v^2}(p) \end{pmatrix}$$

が正則行列であるとき非退化であるという。なおこれらの定義は  $(u, v)$  のとり方によらない。

解答. まず  $f$  の臨界点を求めよう。 $P = (x, y, z) \in S^2$  をとる。 $\tilde{f}$  を  $f$  の  $\mathbb{R}^3$  への延長とし、写像  $g: \mathbb{R}^3 \rightarrow \mathbb{R}$  を  $g(x, y, z) = x^2 + y^2 + z^2 - 1$  で定める。このとき

$$\begin{aligned} p \text{ が } f \text{ の臨界点} &\iff \dim \operatorname{Ker} df_p = 2 \\ &\iff \dim \operatorname{Ker} \begin{pmatrix} J\tilde{f}_p \\ dg_p \end{pmatrix} = 2 \\ &\iff \operatorname{rank} \begin{pmatrix} J\tilde{f}_p \\ dg_p \end{pmatrix} = 1 \\ &\iff \operatorname{rank} \begin{pmatrix} y+z & x+z & x+z \\ 2x & 2y & 2z \end{pmatrix} = 1 \\ &\iff x+y+z=0 \text{ または } x=y=z \end{aligned}$$

である。ゆえに  $f$  の臨界点は  $C = \{(x, y, z) \in S^2 \mid x+y+z=0\}$  の点と、

$$P = \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right), \quad Q = \left(\frac{-1}{\sqrt{3}}, \frac{-1}{\sqrt{3}}, \frac{-1}{\sqrt{3}}\right)$$

である。 $f$  の非退化な臨界点の集合は、 $C \cup \{P\} \cup \{Q\}$  の中で孤立点でなくてはならないはずなので、 $C$  の点はすべて非退化ではない。

北極からの立体射影

$$\varphi(x, y, z) = \left(\frac{x}{1-z}, \frac{y}{1-z}\right) = (s, t)$$

を考える。 $\varphi$  の逆写像は  $K = (1+s^2+t^2)/2$  とおけば

$$\varphi^{-1}(s, t) = \left(\frac{s}{K}, \frac{t}{K}, \frac{K-1}{K}\right)$$

とかける。よって  $f = ((x+y+z)^2 - 1)/2$  により  $T = s+t-1$  とおくと

$$h = f \circ \varphi^{-1}(s, t) = \frac{(2K+T)T}{2K^2}$$

である。したがって面倒極まる計算を実行すると

$$\begin{aligned}
\frac{\partial h}{\partial s} &= \frac{(K - sT)(K - T)}{K^3} \\
\frac{\partial h}{\partial t} &= \frac{(K - tT)(K - T)}{K^3} \\
\frac{\partial^2 h}{\partial s^2} &= \frac{K^2(3s - t) + KT(t - s - 4s^2 - 1) + 3sT^2}{K^4} \\
\frac{\partial^2 h}{\partial t^2} &= \frac{K^2(3t - s) + KT(s - t - 4t^2 - 1) + 3tT^2}{K^4} \\
\frac{\partial^2 h}{\partial s \partial t} &= \frac{-(s + t + 1)K^2 + 2(s + t + st)KT - 3sT^2}{K^4}
\end{aligned}$$

がわかる。ここで

$$\begin{aligned}
\varphi(P) &= \left( \frac{1 + \sqrt{3}}{2}, \frac{1 + \sqrt{3}}{2} \right) \\
\left( \frac{1 + \sqrt{3}}{2} \right)^2 &= \frac{2 + \sqrt{3}}{2} \\
K(P) &= \frac{\sqrt{3}(1 + \sqrt{3})}{2} \\
K(P)^2 &= \frac{3(2 + \sqrt{3})}{2}
\end{aligned}$$

を代入して忍耐強く計算すると

$$\begin{aligned}
\frac{\partial^2 h}{\partial s^2}(\varphi(P)) &= \frac{\partial^2 h}{\partial t^2}(\varphi(P)) = \frac{-7 - 3\sqrt{3}}{2K(P)^4} \\
\frac{\partial^2 h}{\partial s \partial t}(\varphi(P)) &= 0
\end{aligned}$$

を得る。よって  $P$  での Hessian は正則なので  $P$  は非退化。  $\frac{\partial^2 h}{\partial s^2}$  や  $\frac{\partial^2 h}{\partial s \partial t}$  は  $\mathbb{Q}$  係数の有理式なので

$$\begin{aligned}
\frac{\partial^2 h}{\partial s^2}(\varphi(Q)) &= \frac{\partial^2 h}{\partial t^2}(\varphi(Q)) = \frac{-7 + 3\sqrt{3}}{2K(Q)^4} \\
\frac{\partial^2 h}{\partial s \partial t}(\varphi(Q)) &= 0
\end{aligned}$$

であり、 $Q$  も非退化。

問 6

$a$  は実数で  $0 < a < \frac{1}{4}$  とする。このとき、区間  $(0, \infty)$  における常微分方程式

$$\frac{d^2 y}{dx^2} + \frac{a}{x^2} y = 0$$

の任意の解  $y(x)$  は  $\lim_{x \rightarrow +0} y(x) = 0$  をみたすことを示せ。

解答.  $y = x^\beta$  とおくと

$$\frac{d^2 y}{dx^2} = \frac{\beta(\beta-1)}{x^2} y$$

である。ゆえに  $\beta^2 - \beta + a = 0$  なる  $\beta$  に対して  $y = x^\beta$  は特殊解である。 $\beta^2 - \beta + a = 0$  の解は

$$\begin{aligned}\beta_1 &= \frac{1}{2} + \sqrt{\frac{1}{4} - a} \\ \beta_2 &= \frac{1}{2} - \sqrt{\frac{1}{4} - a}\end{aligned}$$

である。 $0 < a < 1/4$  という仮定より  $\beta_1, \beta_2$  はともに正の実数である。係数である  $a/x^2$  は区間  $(0, \infty)$  上で連続なので、常微分方程式の初期値問題の解の存在と一意性定理が適用できて、与えられた微分方程式の解空間は 2 次元ベクトル空間である。よって  $x^{\beta_1}$  と  $x^{\beta_2}$  は一次独立なので任意の解  $y$  は  $x^{\beta_1}$  と  $x^{\beta_2}$  の線形結合で書ける。よって  $\lim_{x \rightarrow +0} y(x) = 0$  である。

問 7

$A$  を実正方行列とする。このとき、ある正の整数  $k$  が存在して  $\operatorname{tr}(A^k) \geq 0$  となることを示せ。ただし  $\operatorname{tr}$  は行列のトレースを表す。

解答. 行列  $A$  のサイズを  $n$  とする。 $A$  の固有多項式の根を重複を込めて

$$\lambda_1, \dots, \lambda_r, \lambda_{r+1}, \overline{\lambda_{r+1}}, \dots, \lambda_{r+s}, \overline{\lambda_{r+s}} \quad (r + 2s = n)$$

とおく。するとトレースは固有値の和なので

$$\operatorname{tr} A^k = \sum_{i=1}^r \lambda_i^k + 2 \sum_{i=1}^s \operatorname{Re} \lambda_{r+i}^k$$

と書ける。ここで  $\lambda_i$  の偏角を考える。 $\arg \lambda_i = 2\pi\alpha_i$  ( $0 \leq \alpha_i < 1$ ) とおく。このとき Dirichlet の近似定理から

$$\exists k \in \mathbb{Z}_{\geq 1} \quad \forall 1 \leq i \leq s+r \quad \exists m_i \in \mathbb{Z} \quad |k\alpha_i - m_i| < \frac{1}{4}$$

が成り立つ。この  $k$  について  $\forall i \quad \arg \lambda_i^k \in [0, \pi/2) \cup (3\pi/2, 2\pi)$  だから  $\operatorname{tr} A^k \geq 0$  が成り立つ。

## 平成 27 年度 専門科目

### 問 1

$G$  は非可換群で次の条件 (\*) を満たすとする。

(\*)  $N_1, N_2 \subset G$  が相異なる自明でない (つまり  $1$  とも  $G$  とも異なる) 正規部分群なら、 $N_1 \not\subset N_2$  である。  
このとき、以下の問に答えよ。

- (i)  $N_1, N_2$  が相異なる  $G$  の自明でない正規部分群なら、 $G = N_1 \times N_2$  であることを証明せよ。
- (ii)  $G$  の自明でない正規部分群の数は高々 2 個であることを証明せよ。

解答.

- (i) 仮定より  $N_1 \cap N_2 \subsetneq N_i \subset G$  かつ  $N_1 \cap N_2 \triangleleft G$  なので  $N_1 \cap N_2 = 1$  である。また  $1 \subsetneq N_i \subsetneq N_1 N_2$  かつ  $N_1 N_2 \triangleleft G$  より  $N_1 N_2 = G$  である。したがって交換子が  $[N_1, N_2] \subset N_1 \cap N_2 = 1$  より自明になるので、 $N_1$  と  $N_2$  の元は互いに可換。よって積をとる写像  $N_1 \times N_2 \rightarrow G$  は準同型でかつ全単射なので同型である。
- (ii) ハイリホーによる。相異なる 3 つの自明でない正規部分群  $N_1, N_2, N_3$  が存在したとしよう。相異なるという仮定から、(i) により  $N_i N_j = G$  ( $i \neq j$ ) であり、 $i \neq j$  である限り  $N_i$  と  $N_j$  の元は互いに可換である。したがって  $G = N_1 N_2$  と  $N_3$  の元は可換なので、とくに  $N_3$  は Abel 群である。同様にして各  $N_i$  が Abel 群であることが判る。よってとくに  $G$  は Abel 群であるが、 $G$  は非可換群であったはずなので矛盾。ゆえに示すべきことがいえた。

## 問 2

$X, Y, T$  を変数とし、 $A = \mathbb{Z}[X, Y]/(Y^2 - 6X^2)$ ,  $B = \mathbb{Z}[X, T]/(T^2 - 6)$  とおく。また、 $A$  における  $X, Y$  の剰余類を  $x, y$ ,  $B$  における  $X, T$  の剰余類を  $x', t$  とする。 $A$  のイデアル  $P_1, P_2$  と  $B$  のイデアル  $Q_1$  を

$$P_1 = xA + yA + 5A, \quad P_2 = (x - y)A + 5A, \quad Q_1 = x'B + (t + 1)B$$

と定めるとき、以下の間に答えよ。

- (i) 単射な環準同型  $\phi: A \rightarrow B$  で  $\phi(x) = x'$ ,  $\phi(y) = x't$  であるものが存在することを証明せよ。
- (ii)  $P_1, P_2$  は  $A$  の素イデアルで  $P_2 \subsetneq P_1$  であることを証明せよ。
- (iii) (i) により  $A$  を  $B$  の部分環とみなすとき、 $Q_1$  は  $B$  の素イデアルで  $Q_1 \cap A = P_1$  であることを証明せよ。
- (iv)  $B$  の素イデアル  $Q_2$  で  $Q_2 \subset Q_1$ ,  $Q_2 \cap A = P_2$  となるものは存在しないことを証明せよ。

解答.

- (i)  $\tilde{\phi}: \mathbb{Z}[X, Y] \rightarrow B$  を  $\tilde{\phi}(X) = x'$ ,  $\tilde{\phi}(Y) = x't$  で定める。このときあきらかに  $(Y^2 - 6X^2) \subset \text{Ker } \tilde{\phi}$  である。逆に  $f \in \text{Ker } \tilde{\phi}$  とする。このとき

$$f(X, Y) = f_0(X) + f_1(X)Y + g(X, Y)(Y^2 - 6X^2)$$

なる  $f_0, f_1 \in \mathbb{Z}[X]$  と  $g \in \mathbb{Z}[X, T]$  がある。よって

$$f_0(X) + f_1(X, T)XT \in (T^2 - 6)$$

であるが、 $T$  についての次数の考察から  $f_0 = f_1 = 0$  でなくてはならない。 $f \in \text{Ker } \tilde{\phi}$  は任意だったから  $\text{Ker } \tilde{\phi} = (Y^2 - 6X^2)$  である。したがってそのような単射  $\phi$  は存在する。

- (ii) 商環を計算すると

$$\begin{aligned} A/P_1 &\cong \mathbb{Z}[X, Y]/(Y^2 - 6X^2, X, Y, 5) \\ &\cong \mathbb{F}_5 \\ A/P_2 &\cong \mathbb{Z}[X, Y]/(Y^2 - 6X^2, X - Y, 5) \\ &\cong \mathbb{F}_5[X] \end{aligned}$$

であり、それぞれ整域なので  $P_1$  と  $P_2$  は素イデアル。 $P_2 \subset P_1$  はあきらかであろう。また商環が異なるので  $P_1 \neq P_2$  である。

- (iii) やはり商環の計算により示す。

$$\begin{aligned} B/Q_1 &\cong \mathbb{Z}[X, T]/(T^2 - 6, X, T + 1) \\ &\cong \mathbb{F}_5 \end{aligned}$$

より  $\mathbb{F}_5$  は整域なので  $Q_1$  は素イデアルである。また

$$\begin{aligned} B/P_1B &\cong \mathbb{Z}[X, T]/(T^2 - 6, X, XT, 5) \\ &\cong \mathbb{Z}[X, T]/(T^2 - 1, X, 5) \\ &\cong \mathbb{F}_5[T]/(T - 1)(T + 1) \\ &\cong \mathbb{F}_5 \times \mathbb{F}_5 \end{aligned}$$



により  $P_1B = (x', t+1)(x', t-1)$  がわかる。よって  $P_1B \subset Q_1$  であり、とくに  $P_1 \subset Q_1 \cap A$  である。  
 $Q_1 \cap A$  は素イデアルで、 $P_1$  は極大イデアルなので  $P_1 = Q_1 \cap A$  でなくてははいけない。

(iv) ハイリホーによる。そのような  $Q_2$  が存在したとする。

$$\begin{aligned} B/P_2B &\cong \mathbb{Z}[X, T]/(T^2 - 6, 5, X - XT) \\ &\cong \mathbb{F}_5[X, T]/(T^2 - 1, 5, X(1 - T)) \\ &\cong \mathbb{F}_5[X, T]/(T - 1)(T + 1, X) \\ &\cong \mathbb{F}_5[X] \times \mathbb{F}_5 \end{aligned}$$

により  $P_2B = (t - 1)(t + 1, x')$  である。 $Q_2$  は素イデアルと仮定したことから、 $P_2B \subset Q_2$  なので  $(t - 1) \subset Q_2$  あるいは  $Q_1 = (t + 1, x') \subset Q_2$  でなくてははいけない。 $P_1 \neq P_2$  なので、 $(t - 1) \subset Q_2$  ということになる。しかしこのとき

$$\begin{aligned} Q_1 &= Q_1 + Q_2 \\ &\supset (t - 1, t + 1, x') \\ &\supset B \end{aligned}$$

となり矛盾。よって示すべきことがいえた。

### 問 3

$\mathbb{C}(t)$  を  $\mathbb{C}$  上の 1 変数有理関数体とする。 $a$  を複素数とし、 $s = t^3 + 3t^2 + at \in \mathbb{C}(t)$  とおく。 $\mathbb{C}$  上  $s$  で生成された  $\mathbb{C}(t)$  の部分体を  $\mathbb{C}(s)$  とするとき、以下の問に答えよ。

- (i) 拡大次数  $[\mathbb{C}(t) : \mathbb{C}(s)]$  を求めよ。
- (ii)  $\mathbb{C}(t)/\mathbb{C}(s)$  がガロア拡大となる複素数  $a$  をすべて求めよ。

解答.

- (i)  $t$  は  $\mathbb{C}(s)$  係数の多項式

$$F := X^3 + 3X^2 + aX - (t^3 + 3t^2 + at)$$

の根である。よって  $[\mathbb{C}(t) : \mathbb{C}(s)] \leq 3$  である。

まず  $[\mathbb{C}(t) : \mathbb{C}(s)] \geq 2$  を示そう。ハイリホーによる。仮に  $t \in \mathbb{C}(s)$  だったとする。 $s$  は  $\mathbb{C}$  上超越的なので  $\mathbb{C}[s]$  は PID であり、とくに整閉である。よって  $t$  は  $\mathbb{C}[s]$  上整なので  $t \in \mathbb{C}[s]$  である。しかし  $s \in \mathbb{C}[t]$  は 3 次式なのでこれは矛盾。よって  $[\mathbb{C}(t) : \mathbb{C}(s)] \geq 2$  である。

次に  $[\mathbb{C}(t) : \mathbb{C}(s)] \geq 3$  を示そう。ハイリホーによる。仮に  $[\mathbb{C}(t) : \mathbb{C}(s)] = 2$  だったとしよう。 $t$  の  $\mathbb{C}(s)$  上の共役を  $\{t, \bar{t}\}$  とする。2 次拡大は正規拡大なので  $\bar{t} \in \mathbb{C}(t)$  であるが、 $\bar{t}$  は  $\mathbb{C}[t]$  上整なので  $\bar{t} \in \mathbb{C}[t]$  である。仮定より  $F$  は  $\mathbb{C}(s)$  係数の多項式として可約な 3 次式なので 1 次式を因数として含む。よって  $F$  の根  $u$  であって  $u \in \mathbb{C}(s)$  なるものがある。むろん  $\mathbb{C}[s]$  の整閉性により実際には  $u \in \mathbb{C}[s]$  である。このとき  $\mathbb{C}[t]$  において

$$ut\bar{t} = t^3 + 3t^2 + at$$

だから  $u\bar{t} = t^2 + 3t + a$  であり、右辺の次数が 2 なので  $u \in \mathbb{C}$  である。よって  $\bar{t}$  は 2 次式ということになるが、これは  $t + \bar{t} \in \mathbb{C}[s]$  に矛盾。以上により  $[\mathbb{C}(t) : \mathbb{C}(s)] = 3$  が結論される。

- (ii)  $\mathbb{C}(t)/\mathbb{C}(s)$  が Galois 拡大であるという命題を (P) であらわすことにする。(P) は次と同値である。

(P1)  $\mathbb{C}(s)$  係数の多項式  $F$  のすべての根は  $\mathbb{C}(t)$  に含まれる。

多項式の根が  $\mathbb{C}(t)$  に入ることと、 $\mathbb{C}(t)$  で因数分解できることは同じなので (P1) は次と同値。

(P2) ある  $f, g, h \in \mathbb{C}(t)$  が存在して  $F(X) = (X - f)(X - g)(X - h)$  が成り立つ。

$F$  は  $\mathbb{C}[t]$  係数のモニック多項式であり、かつ  $\mathbb{C}[t]$  は整閉なので  $f, g, h \in \mathbb{C}[t]$  としてよい。つまり (P2) は次と同値。

(P3) ある  $f, g, h \in \mathbb{C}[t]$  が存在して

$$\begin{aligned} f + g + h &= -3 \\ fg + gh + hf &= a \\ fgh &= t(t - \beta)(t - \gamma) \end{aligned}$$

が成り立つ。ただし  $\beta, \gamma$  は  $t^2 + 3t + a = (t - \beta)(t - \gamma)$  なる  $\mathbb{C}$  の元とする。

$f + g + h$  が定数で  $fgh$  が 3 次式という条件より、 $\deg f = \deg g = \deg h = 1$  でなくてはならない。 $f, g, h$  を適当に並び替えることにより、ある  $b, c, d \in \mathbb{C}$  が存在して  $f(t) = bt$ ,  $g(t) = c(t - \beta)$ ,  $h(t) = d(t - \gamma)$  と表せるとしてよい。このとき計算すると

$$\begin{aligned} f + g + h + 3 &= (b + c + d)t - c\beta - d\gamma + 3 \\ fg + gh + hf - a &= (bc + cd + db)t^2 + (-bc\beta + 3cd - bd\gamma)t + (cd - 1)a \\ fgh &= bcdt(t - \beta)(t - \gamma) \end{aligned}$$

である。よって  $b, c, d$  は次を満たさなくてはならない。

$$\begin{aligned} b + c + d &= 0 \\ bc + cd + db &= 0 \\ bcd &= 1 \\ c\beta + d\gamma - 3 &= 0 \\ -bc\beta + 3cd - bd\gamma &= 0 \\ (cd - 1)a &= 0 \end{aligned}$$

前半の 3 つの条件は、 $b, c, d$  が  $X^3 - 1$  の異なる 3 つの根であることを意味する。残りの条件も使うと

$$3b^2 = b^2(c\beta + d\gamma) = 3bcd = 3$$

より  $b = 1$  が得られる。よって  $c, d$  は  $X^2 + X + 1$  の異なる 2 つの根である。よって、与えられた条件は

$$c\beta + d\gamma = 3$$

と要約できる。つまり (P3) は次と同値である。

**(P4)**  $X^2 + X + 1$  の異なる 2 つの根  $c, d$  をうまく選べば  $c\beta + d\gamma = 3$  が成り立つ。

いま (P4) が成り立つと仮定する。 $-3 = \beta + \gamma$  により  $(1 + c)\beta + (1 + d)\gamma = 0$  であるが、これは  $1 + d + c = 0$  により  $d\beta + c\gamma = 0$  を意味する。よって

$$\begin{aligned} 0 &= (c\beta + d\gamma)(d\beta + c\gamma) \\ &= \beta^2 + \gamma^2 - a \\ &= (\beta + \gamma)^2 - 3a \\ &= 9 - 3a \end{aligned}$$

である。これは  $a = 3$  ということである。逆に  $a = 3$  だと仮定しよう。このとき  $\beta, \gamma$  が

$$\begin{aligned} \beta &= \frac{-3 + \sqrt{-3}}{2} = \sqrt{3}e^{5\pi i/6} \\ \gamma &= \frac{-3 - \sqrt{-3}}{2} = \sqrt{3}e^{7\pi i/6} \end{aligned}$$

と与えられていたとすると、 $d = e^{2\pi i/3}$ ,  $c = e^{4\pi i/3}$  とおけば

$$c\beta + d\gamma = \sqrt{3}(e^{\pi i/6} + e^{11\pi i/6}) = 3$$

となり (P4) が成立する。ゆえに求める条件をみたす  $a$  は  $a = 3$  である。

## 平成 26 年度 基礎科目 I

### 問 1

- (i)  $\{a_n\}_{n=1}^{\infty}$  は実数列で、任意の正整数  $k$  について

$$\lim_{n \rightarrow \infty} (a_{n+k} - a_n) = 0$$

をみたすとする。このとき、この数列  $\{a_n\}_{n=1}^{\infty}$  は収束するか？理由をつけて答えよ。

- (ii) 次の広義積分は収束するか？理由をつけて答えよ：

$$\int_0^{\infty} (1 - e^{-1/x}) dx.$$

解答.

- (i) 収束するとは限らない。反例はたとえば  $a_n = \log n$  とすれば得られる。

- (ii)  $y = 1/x$  とおくと  $dx = -1/y^2 dy$  であって

$$\int_0^{\infty} (1 - e^{-1/x}) dx = \int_0^{\infty} \frac{1 - e^{-y}}{y^2} dy$$

であるはずだから、右辺の収束性を考えればよい。いま Taylor 展開を考えると

$$e^{-y} = 1 - y + O(y^2)$$

だから、 $g(y) = (1 - e^{-y})/y^2$  とおくと  $g(y) = 1/y + h(y)$  なる  $[0, \infty)$  上の連続関数  $h$  がある。 $0 < y$  のとき  $g(y) > 0$  なので、 $0 < \varepsilon < 1$  に対して

$$\begin{aligned} \int_{\varepsilon}^{\infty} g(y) dy &\geq \int_{\varepsilon}^1 g(y) dy \\ &\geq \int_{\varepsilon}^1 \left| \frac{1}{y} + h(y) \right| dy \\ &\geq \int_{\varepsilon}^1 \frac{dy}{y} - \int_{\varepsilon}^1 |h(y)| dy \\ &\geq \log 1/\varepsilon - \int_0^1 |h(y)| dy \end{aligned}$$

が成り立つ。したがって

$$\liminf_{\varepsilon \rightarrow +0} \int_{\varepsilon}^1 g(y) dy = \infty$$

である。よって件の積分は収束しない。

## 問 2

$n$  は 2 以上の整数とする。 $\mathbb{R}^2$  上の関数

$$f(x, y) = x^{2n} + y^{2n} - nx^2 + 2nxy - ny^2$$

について次の問に答えよ：

- (i)  $f$  の最大値・最小値は存在するか？理由をつけて答えよ。
- (ii)  $f$  が極大値・極小値をとる点をすべて求めよ。

解答.

- (i)  $f(x, y) = x^{2n} + y^{2n} - n(x - y)^2$  と書ける。よって  $f(x, x) = 2x^{2n}$  なので  $f$  は最大値を持たない。また  $x = r \cos \theta, y = r \sin \theta$  おいて  $g(r, \theta) = f(r \cos \theta, r \sin \theta)$  とするとき

$$g(r, \theta) = r^{2n}(\cos^{2n} \theta + \sin^{2n} \theta) - nr^2(1 - \sin 2\theta)$$

であるが、

$$\begin{aligned} \cos^{2n} \theta + \sin^{2n} \theta &\geq \max\{\cos^{2n} \theta, \sin^{2n} \theta\} \\ &\geq (1/\sqrt{2})^{2n} \\ &\geq 1/2^n \end{aligned}$$

であるため  $|g(r, \theta)| \geq 2^{-n}r^{2n} - 2nr^2$  と評価できる。したがってある  $R > 0$  が存在して  $g$  は  $\{(r, \theta) \mid r \geq R\}$  上で 0 以上となる。ゆえに  $f(0, 0) = 0$  より

$$\inf_{(x, y) \in \mathbb{R}^2} f(x, y) = \min_{r \leq R} g(r, \theta)$$

だから  $f$  は最小値を持つ。

- (ii)  $x, y$  についてそれぞれ偏微分すると

$$\begin{aligned} \frac{\partial f}{\partial x} &= 2n(x^{2n-1} - x + y) \\ \frac{\partial f}{\partial y} &= 2n(y^{2n-1} - y + x) \end{aligned}$$

である。よって点  $(x, y)$  がもし極値を与えるならば、

$$\begin{aligned} x^{2n-1} - x + y &= 0 \\ y^{2n-1} - y + x &= 0 \end{aligned}$$

である。よって極値を与える点は、 $\alpha = 2^{1/(2n-2)} > 0$  として

$$P = (0, 0), \quad Q_1 = (\alpha, -\alpha), \quad Q_2 = (-\alpha, \alpha)$$

の中にある。これらが実際に極値なのか、そして極値だとすれば極小か極大かを判断するために

Hessian を求める。

$$\begin{aligned}\frac{\partial^2 f}{\partial x^2} &= 2n((2n-1)x^{2n-2} - 1) \\ \frac{\partial^2 f}{\partial y^2} &= 2n((2n-1)y^{2n-2} - 1) \\ \frac{\partial^2 f}{\partial x \partial y} &= 2n\end{aligned}$$

であるから、 $P$  における Hessian は

$$H_P = 2n \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$$

である。 $1/2nH_P$  の固有値は  $0, -2$  であり  $H_P$  は正則でないので、Hessian から  $P$  が極値であるかどうかを判定することはできない。実際、 $f(x, 0) = x^2(x^{2n-2} - n)$  より直線  $y = 0$  上では  $f(P)$  は極大値。 $f(x, x) = 2x^{2n}$  より直線  $y = x$  上では  $f(P)$  は極小値。よって  $P$  は鞍点であり極値を与えない。

$Q_i$  における Hessian は

$$H_{Q_1} = H_{Q_2} = 2n \begin{pmatrix} 4n-3 & 1 \\ 1 & 4n-3 \end{pmatrix}$$

である。 $1/2nH_{Q_i}$  の固有値は  $4n-4, 4n-2$  でありどちらも正。よって Hessian は正定値であるから  $f(Q_1) = f(Q_2) = 4\alpha^2(1-n)$  は極小値。(最小値でもある)

### 問 3

次の 4 次正方行列  $A, B$  は正則か？正則ならば逆行列を求め、正則でないならば階数を求めよ。

$$A = \begin{pmatrix} 2 & 0 & 1 & 3 \\ 0 & 8 & 2 & 4 \\ 2 & 0 & 1 & 4 \\ 0 & 4 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 2 & 0 & 3 \\ 3 & 4 & 2 & 4 \\ 4 & 5 & 3 & 4 \end{pmatrix}$$

解答.  $E$  を単位行列とする。拡大係数行列  $(A \ E)$  を行基本変形すると

$$(A \ E) \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 3/2 & -1/4 & -1 & 1/2 \\ 0 & 1 & 0 & 0 & -1/4 & 0 & 1/4 & 1/4 \\ 0 & 0 & 1 & 0 & 1 & 1/2 & -1 & -1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 1 & 0 \end{pmatrix}$$

を得る。したがって  $A$  は正則で、逆行列は

$$\frac{1}{4} \begin{pmatrix} 6 & -1 & -4 & 2 \\ -1 & 0 & 1 & 1 \\ 4 & 2 & -4 & -4 \\ -4 & 0 & 4 & 0 \end{pmatrix}$$

で与えられる。同様に  $(B \ E)$  を行基本変形していくと  $\text{rank } B = 3$  であることがわかる。とくに  $B$  は正則ではない。



問 4

3 次の複素正方行列

$$A = \begin{pmatrix} 3 & 0 & -1 \\ -2 & 1 & 1 \\ 2 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ -1 & x & 2 \end{pmatrix}$$

に対して、 $A$  と  $B$  が相似になるような複素数  $x$  をすべて求めよ。ただし、行列  $A$  と  $B$  が相似とは、複素正方行列  $P$  で  $A = P^{-1}AP$  を満たすものが存在することをいう。

解答.  $A$  の固有多項式は  $(t-1)^2(t-2)$  なので固有値は  $1, 2$  である。計算すると  $\text{rank}(E-A) = 1$  なので  $\text{Ker}(E-A)$  は 2 次元空間。したがって  $A$  の Jordan 標準形は

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

である。 $B$  の固有多項式も  $(t-1)^2(t-2)$  で、固有値は  $A$  と同じ。しかし

$$\text{rank}(E-B) = \text{rank} \begin{pmatrix} 0 & x & 0 \\ 1 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

なので  $B$  の Jordan 標準形は  $x \neq 0$  のとき対角行列でなく、 $x = 0$  のとき対角行列となる。よって  $A$  と  $B$  が相似となる  $x$  は  $x = 0$  である。

## ■ 平成 26 年度 基礎科目 II

### 問 1

実数値関数  $f(x)$  は  $[0, \infty)$  で連続で  $\lim_{x \rightarrow \infty} f(x) = 1$  とする。このとき

$$\lim_{n \rightarrow \infty} \frac{1}{n!} \int_0^{\infty} f(x) e^{-x} x^n dx = 1$$

であることを証明せよ。

解答. Gamma 関数についてのよく知られた事実として

$$\int_0^{\infty} e^{-x} x^n dx = n!$$

が成り立つことを注意しておく。 $\varepsilon > 0$  が与えられたとする。仮定より

$$x \geq R \rightarrow |f(x) - 1| < \varepsilon$$

なる  $R > 0$  がある。このとき

$$\begin{aligned} \left| \frac{1}{n!} \int_0^{\infty} f(x) e^{-x} x^n dx - 1 \right| &= \frac{1}{n!} \left| \int_0^{\infty} f(x) e^{-x} x^n dx - \int_0^{\infty} e^{-x} x^n dx \right| \\ &\leq \frac{1}{n!} \int_0^{\infty} |f(x) - 1| e^{-x} x^n dx \\ &\leq \varepsilon + \frac{1}{n!} \int_0^R |f(x) - 1| e^{-x} x^n dx \end{aligned}$$

である。よって

$$\limsup_{n \rightarrow \infty} \left| \frac{1}{n!} \int_0^{\infty} f(x) e^{-x} x^n dx - 1 \right| \leq \varepsilon$$

が従う。 $\varepsilon > 0$  は任意だったので、示すべきことがいえた。

## 問 2

$n, m$  を正の整数とする。 $x$  を変数とする  $n$  次以下の  $\mathbb{C}$  係数多項式の全体を  $V_n$  とし、和・差・スカラー倍により  $V_n$  を  $\mathbb{C}$  上のベクトル空間とみなす。 $m$  個の複素数  $\alpha_1, \dots, \alpha_m$  に対し、線形写像  $F: V_n \rightarrow \mathbb{C}^m$  を

$$F(f) = (f(\alpha_1), \dots, f(\alpha_m))$$

で定める。このとき

- (i)  $F$  が単射になるための必要十分条件を  $n, m, \alpha_1, \dots, \alpha_m$  のみを用いて述べよ。
- (ii)  $F$  が全射になるための必要十分条件を  $n, m, \alpha_1, \dots, \alpha_m$  のみを用いて述べよ。

解答.  $\alpha_1, \dots, \alpha_m$  のうち相異なるものの数を  $k$  とする。適当に番号を付けなおすことにより  $\alpha_1, \dots, \alpha_k$  が相異なるとしてよい。 $V_n$  の基底  $\{1, x, \dots, x^n\}$  と  $\mathbb{C}^m$  の標準基底について  $F$  を行列表示すると

$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^n \\ 1 & \alpha_2 & \cdots & \alpha_2^n \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_m & \cdots & \alpha_m^n \end{pmatrix}$$

となる。したがって

$$\text{rank } F = \text{rank} \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^n \\ 1 & \alpha_2 & \cdots & \alpha_2^n \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_k & \cdots & \alpha_k^n \end{pmatrix}$$

である。右辺の行列のサイズが  $s := \min\{k, n+1\}$  の部分正方行列

$$\Delta = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{s-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{s-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_s & \cdots & \alpha_s^{s-1} \end{pmatrix}$$

の行列式は Vandermonde の行列式であって

$$|\det \Delta| = \prod_{i>j} |\alpha_i - \alpha_j| \neq 0$$

である。したがって  $\text{rank } F = \min\{k, n+1\}$  である。ここまでの準備をもってすれば問に答えることはやさしい。

- (i)  $F$  が単射であることは  $\text{rank } F = \dim V_n$  と同値。つまり  $n+1 \leq k$  である。
- (ii)  $F$  が全射であることは  $\text{rank } F = \dim \mathbb{C}^m$  と同値。つまり  $m = k \leq n+1$  である。

### 問 3

$L_R (R > 0)$  は複素平面において  $-R + 2i$  を始点、 $R + 2i$  を終点とする線分を表す。このとき

$$\lim_{R \rightarrow \infty} \int_{L_R} \frac{\cos z}{z^2 + 1} dz$$

の値を求めよ。

解答.  $z = t + 2i$  と変数変換して整理すると

$$\int_{L_R} \frac{\cos z}{z^2 + 1} dz = \frac{e^{-2}}{2} \int_{-R}^R \frac{e^{it}}{(t+3i)(t+i)} dt + \frac{e^2}{2} \int_{-R}^R \frac{e^{-it}}{(t+3i)(t+i)} dt$$

である。そこで

$$f(z) = \frac{e^{iz}}{(z+3i)(z+i)}$$

$$g(z) = \frac{e^{-iz}}{(z+3i)(z+i)}$$

とおく。上半平面を反時計回りにまわる半円を  $C_R = \{Re^{i\theta} \mid 0 \leq \theta \leq \pi\}$  とし、下半平面を反時計回りにまわる半円を  $D_R = \{Re^{i\theta} \mid \pi \leq \theta \leq 2\pi\}$  とする。留数定理により任意の  $R > 3$  について

$$\begin{aligned} \int_{-R}^R f(t) dt + \int_{C_R} f(z) dz &= 0 \\ - \int_{-R}^R g(t) dt + \int_{D_R} g(z) dz &= 2\pi i (\text{Res}(g, -3i) + \text{Res}(g, -i)) \end{aligned}$$

である。計算すると

$$\lim_{R \rightarrow \infty} \int_{C_R} f(z) dz = \lim_{R \rightarrow \infty} \int_{D_R} g(z) dz = 0$$

であるから、ゆえに

$$\begin{aligned} \int_{-\infty}^{\infty} f(t) dt &= 0 \\ - \int_{-\infty}^{\infty} g(t) dt &= 2\pi i (\text{Res}(g, -3i) + \text{Res}(g, -i)) \end{aligned}$$

である。 $g$  の  $z = -3i$  および  $z = -i$  における極は一位なので

$$\text{Res}(g, -3i) = \frac{i}{2e^3}$$

$$\text{Res}(g, -i) = -\frac{i}{2e}$$

である。ゆえに

$$\int_{-\infty}^{\infty} g(t) dt = \pi(e^{-3} - e^{-1})$$

であることが判ったので

$$\lim_{R \rightarrow \infty} \int_{L_R} \frac{\cos z}{z^2 + 1} dz = \frac{\pi(1 - e^2)}{2e}$$

が結論される。

#### 問 4

| 群  $G = (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z})$  の指数 3 の部分群の個数を求めよ。

解答.  $3G = \{3g \mid g \in G\}$  とする。  $G$  の指数 3 の部分群  $H$  は  $3G \subset H$  を満たすので、  $G/3G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  の位数 3 の部分群と対応する。位数 3 の群は巡回群なので、位数 3 の部分群の数は位数 3 の元の数のちょうど半分である。よって求める部分群の数は  $(9 - 1)/2 = 4$  個である。

問 5

$f: S^2 \rightarrow S^1$  を  $C^\infty$  級写像とする。ただし、 $S^n$  は  $n$  次元球面

$$\left\{ (x_0, \dots, x_n) \in \mathbb{R}^{n+1} \mid \sum_{i=0}^n x_i^2 = 1 \right\}$$

を表す。このとき  $S^2$  上の少なくとも 2 点において  $f$  の微分は零写像になることを示せ。

解答. 被覆写像  $p: \mathbb{R} \rightarrow S^1$  をとる。これは普遍被覆である。 $q \in S^2, r \in \mathbb{R}$  とし  $f(q) = p(r)$  であるものとする。このとき  $\pi_1(S^2, q) = 1$  だから

$$f_*(\pi_1(S^2, q)) \subset p_*(\pi_1(\mathbb{R}, r))$$

である。よって  $f$  の  $p$  に関するリフト  $g: S^2 \rightarrow \mathbb{R}$  が存在して次を可換にする。

$$\begin{array}{ccc} & & \mathbb{R} \\ & \nearrow g & \downarrow p \\ S^2 & \xrightarrow{f} & S^1 \end{array}$$

$p$  は局所的に微分同相なので  $g$  も  $C^\infty$  級である。ここで  $S^2$  はコンパクトなので  $g$  は最大値と最小値を持つ。したがって  $g$  は少なくとも 2 つの臨界点を持つ。任意の  $x \in S^2$  に対して  $df_x = dp_{g(x)} \circ dg_x$  だから、 $f$  も少なくとも 2 つの臨界点を持つことになる。

## 問 6

$a$  は 0 でない実数、 $p(t)$  は  $\mathbb{R}$  上の連続な周期関数で周期  $T$  ( $T > 0$ ) をもつとする。このとき常微分方程式

$$\frac{d}{dt}x(t) = ax(t) + p(t)$$

の解  $x(t)$  で、周期  $T$  を持つ周期関数となるものが唯一つ存在すること証明せよ。

解答.  $p$  は連続なので常微分方程式の初期値問題の解の存在と一意性定理が適用できる。よって周期  $T$  の解が唯一存在するということは、 $x(t+T) - x(t)$  が恒等的にゼロになるような初期値  $x(0)$  が唯一つ存在することと同じことである。いま与えられた関数  $p$  の周期性から解  $x$  は

$$\frac{d}{dt}(x(t+T) - x(t)) = a(x(t+T) - x(t))$$

を満たす。よって  $x(t+T) - x(t) = Ce^{at}$  を満たすような定数  $C$  が存在する。 $C = x(T) - x(0)$  であるから、問題は  $x(T) - x(0) = 0$  となるような初期値  $x(0)$  の存在と一意性を示すことに帰着する。

与えられた微分方程式は線形非斉次なので  $x(t) = e^{at}y(t)$  と変数変換すれば解くことができ、解は

$$x(t) = e^{at} \int_0^t e^{-as} p(s) ds + e^{at} x(0)$$

である。ゆえに  $M = \int_0^T e^{-as} p(s) ds$  とおけば

$$x(T) - x(0) = e^{aT} M + (e^{aT} - 1)x(0)$$

である。ゆえに求める周期解は初期値

$$x(0) = -\frac{e^{aT} M}{e^{aT} - 1}$$

に対応しているわけで、これで存在と一意性がいえた。

問 7

$n$  を正の整数とし、 $n$  次実正方行列  $A = (a_{ij})_{1 \leq i, j \leq n}$  において、不等式

$$|a_{ii}| > \sum_{1 \leq j \leq n, j \neq i} |a_{ij}|$$

がすべての  $i = 1, \dots, n$  に対して成立しているとする。ただし、右辺の和は 1 から  $n$  までの整数  $j$  で  $i$  以外のものにわたる。このとき、 $A$  は正則であることを示せ。

解答.  $Av = 0$  なる  $v \in \mathbb{R}^n$  が与えられたとする。

$$|v_m| = \max_i |v_i|$$

とおく。このとき

$$\begin{aligned} |a_{mm}v_m| &= \left| a_{mm}v_m - \sum_{j=1}^n a_{mj}v_j \right| \\ &= \left| \sum_{j \neq m} a_{mj}v_j \right| \\ &\leq \sum_{j \neq m} |a_{mj}| |v_j| \\ &\leq |v_m| \sum_{j \neq m} |a_{mj}| \end{aligned}$$

だから

$$|v_m| (|a_{mm}| - \sum_{j \neq m} |a_{mj}|) \leq 0$$

であり、仮定から  $|v_m| = 0$  でなくてはならない。これは  $A$  が正則であることを意味する。



## 平成 26 年度 専門科目

### 問 1

$\mathbb{C}[X, Y]$  を複素数係数の 2 変数多項式環、 $A = \mathbb{C}[X, Y]/(X^2 + Y^3 - 1)$  とし、 $X, Y \in \mathbb{C}[X, Y]$  の  $A$  での類をそれぞれ  $x, y$  とおく。

- (i)  $A$  が整域であり、 $A$  の商体  $L$  が  $\mathbb{C}(y)$  の 2 次拡大であることを証明せよ。
- (ii)  $A$  が  $\mathbb{C}[y]$  の  $L$  における整閉包であることを証明せよ。
- (iii)  $y$  が  $A$  の既約元であることを証明せよ。
- (iv)  $A$  が UFD (一意分解整域) であるかどうか理由をつけて決定せよ。

解答.

- (i)  $B := \mathbb{C}[Y]$ ,  $K := \mathbb{C}(Y)$  とし、 $A$  は  $B$  代数として  $A = B[X]/(X^2 + Y^3 - 1)$  ととらえなおす。 $B$  は PID なので  $B[X]$  は UFD である。このとき  $X^2 + Y^3 - 1$  は  $\mathfrak{p} = (Y - 1)$  に関する Eisenstein 多項式であるため  $K[X]$  の元として既約かつ素元である。ゆえに  $A$  は整域。  
 $A$  を  $B$  代数として捉えたのと同様  $L$  も  $K$  代数として  $L = K[X]/(X^2 + Y^3 - 1)$  と捉えなおす。

$$\begin{array}{ccc} K & \longrightarrow & L \\ \uparrow & & \uparrow \\ B & \longrightarrow & A \end{array}$$

$X \in K[X]$  の  $L$  での像を  $x$  と書くことにする。 $L$  は  $K$  上  $x$  で生成されていて  $x$  の  $K$  上の最小多項式は  $T^2 + Y^3 - 1 \in K[T]$  なので  $[L : K] = 2$  であることが判る。

- (ii)  $x \in L$  は  $B$  上整なので  $A/B$  は整拡大。逆に  $z \in L$  が  $B$  上整だったと仮定する。 $[L : K] = 2$  なので  $z = ax + b$  なる  $a, b \in K$  がある。ここで  $L/K$  は分離拡大なので、 $G := \text{Hom}_K^{\text{al}}(L, \bar{K}) = \{\sigma_1, \sigma_2\}$  とするとトレース  $\text{Tr}_{L/K}: L \rightarrow K$  とノルム  $N_{L/K}: L \rightarrow K$  は

$$\text{Tr}_{L/K}(s) = \sum_{\sigma \in G} \sigma(s)$$

$$N_{L/K}(s) = \prod_{\sigma \in G} \sigma(s)$$

と計算できる。 $B$  は PID なのでとくに整閉であり、 $s \in L$  が  $B$  上整ならば  $s$  のトレースとノルムも  $B$  の元となる。したがって

$$\begin{aligned} \text{Tr}_{L/K}(z) &= 2b \in B \\ N_{L/K}(z - b) &= a^2(Y^3 - 1) \in B \end{aligned}$$

が得られる。 $Y^3 - 1$  は平方因子を持たないので  $a \in B$  でなくてはならない。よって  $z \in A$  である。 $z$  は任意だったから、これで  $A$  が  $L$  における  $B$  の整閉包であることがいえた。

- (iii) ハイリホーによる。 $Y \in A$  が可約だったとする。このとき非単元  $\alpha, \beta \in A$  があって  $Y = \alpha\beta$  を満たす。ノルムをとって  $Y^2 = N_{L/K}(\alpha)N_{L/K}(\beta)$  を得る。 $B$  は UFD なので素元  $Y \in B$  によるオーダー

を考えることができる。(ii)により  $A$  は  $L$  における  $B$  の整閉包であったので、各  $\sigma \in G$  は  $\sigma(A) \subset A$  を満たす。 $\alpha, \beta$  は  $A$  の単元ではないので、よって  $N_{L/K}(\alpha), N_{L/K}(\beta)$  も  $B$  の単元ではない。以上により  $N_{L/K}(\alpha), N_{L/K}(\beta)$  の素元  $Y \in B$  に関するオーダーは 1 である。よって  $N_{L/K}(\alpha) = uY$  なる単元  $u \in B^\times = \mathbb{C}^\times$  がある。 $\alpha = cx + d$  ( $c, d \in B$ ) とおくと

$$u^{-1}Y = c^2(Y^3 - 1) + d^2$$

が得られる。ここで  $\deg(c^2(Y^3 - 1)) = 2\deg c + 3$  は奇数で  $\deg d^2 = 2\deg d$  は偶数なので

$$\begin{aligned} 1 &= \deg(u^{-1}Y) \\ &= \deg(c^2(Y^3 - 1) + d^2) \\ &= \max\{2\deg c + 3, 2\deg d\} \\ &\geq 3 \end{aligned}$$

となって矛盾。よって  $Y \in A$  は既約元である。

(iv) 計算すると

$$\begin{aligned} A/(Y) &\cong B[X]/(X^2 + Y^3 - 1, Y) \\ &\cong \mathbb{C}[X, Y]/(X^2 - 1, Y) \\ &\cong \mathbb{C}[X]/(X - 1)(X + 1) \\ &\cong \mathbb{C}^2 \end{aligned}$$

なので  $Y \in A$  は素元ではない。もしも  $A$  が UFD なら既約元はすべて素元であるはずなので、 $A$  は UFD ではない。

## 問 2

$K \subset \mathbb{C}$  を部分体、 $p$  を素数とする。 $\mathbb{C}$  に含まれる任意の有限次拡大  $L/K$  に対し、 $L = K$  でなければ  $[L : K]$  は  $p$  で割り切れると仮定する。このとき、 $\mathbb{C}$  に含まれる任意の有限次拡大  $L/K$  に対し、 $[L : K]$  は  $p$  のべき (1 を含む) であることを証明せよ。

解答.  $K$  の有限次拡大  $L \subset \mathbb{C}$  が与えられたとする。 $L$  の  $K$  上の Galois 閉包を  $\tilde{L}$  とする。 $G := \text{Gal}(\tilde{L}/K)$  とおく。 $G$  の Sylow- $p$  部分群を  $H$  とし、 $H$  の不変体

$$\tilde{L}^H = \left\{ x \in \tilde{L} \mid \forall \sigma \in H \quad \sigma(x) = x \right\}$$

を考える。Galois の基本定理により  $[\tilde{L} : \tilde{L}^H] = \#H$  だから、 $[\tilde{L}^H : K] = \#(G/H)$  であり  $[\tilde{L}^H : K]$  は  $p$  で割り切れない。よって仮定により  $\tilde{L}^H = K$  であるから  $H = G$  であり、とくに  $[\tilde{L} : K]$  は  $p$  のべきである。 $[L : K]$  は  $[\tilde{L} : K]$  を割り切るので、 $[L : K]$  も  $p$  のべき (1 を含む) である。

### 問 3

$\zeta$  を 1 の原始 7 乗根  $e^{2\pi\sqrt{-1}/7}$  とし、 $\mathbb{C}$  の部分集合

$$A = \{a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5 + a_6\zeta^6 \mid a_1, a_2, a_3, a_4, a_5, a_6 \in \{0, 1\}\}$$

を考える。このとき  $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$  となる  $\alpha \in A$  となる  $\alpha \in A$  の個数を求めよ。

解答.  $\mathbb{Q}(\zeta)$  は  $\mathbb{Q}$  の Galois 拡大であり、円分体論により  $G := \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  は  $(\mathbb{Z}/7\mathbb{Z})^\times$  と同型である。ここで次が成り立つ。

補題. 次は同値。

- (i)  $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$
- (ii)  $\forall \sigma \in G \setminus \{1\} \quad \sigma(\alpha) \neq \alpha$

証明.

(i) $\Rightarrow$ (ii) 対偶を示す。ある  $\sigma \in G \setminus \{1\}$  に対し  $\sigma(\alpha) = \alpha$  だとする。このとき  $\mathbb{Q}(\alpha)$  は  $\langle \sigma \rangle$  の不変体に含まれ、 $\mathbb{Q}(\zeta)$  より真に小さい。

(i) $\Rightarrow$ (ii) 仮定より単射  $G \rightarrow \text{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \overline{\mathbb{Q}})$  があるので

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \# \text{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \overline{\mathbb{Q}}) \geq \#G = [\mathbb{Q}(\zeta) : \mathbb{Q}]$$

が得られる。よって  $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$  である。

□

したがって  $\#\{\alpha \in A \mid \forall \sigma \in G \setminus \{1\} \quad \sigma(\alpha) \neq \alpha\}$  を求めればよい。 $(\mathbb{Z}/7\mathbb{Z})^\times$  は 3 を生成元とする巡回群である。対応する  $G$  の生成元を  $\tau$  とする。 $I := \{0, 1\}$  とおく。 $a_i$  の番号を付け替えて

$$A = \{a_1\zeta + a_2\zeta^3 + a_3\zeta^2 + a_4\zeta^6 + a_5\zeta^4 + a_6\zeta^5 \mid (a_1, \dots, a_6) \in I^6\}$$

とみなす。このとき  $A$  の元に対する  $\tau$  の作用は  $I^6$  の元に対する  $s := (123456) \in \mathfrak{S}_6$  の作用と解釈できる。ただし

$$\begin{aligned} \langle s \rangle \times I^6 &\rightarrow I^6 \\ (\sigma, (a_i)_i) &\mapsto (a_{\sigma(i)})_i \end{aligned}$$

として作用を定めるものとする。したがって求めるべきものは、集合

$$B := \{a \in I^6 \mid \forall \sigma \in \langle s \rangle \setminus \{1\} \quad \sigma(a) \neq a\}$$

の位数である。ここで条件  $\forall \sigma \in \langle s \rangle \setminus \{1\} \quad \sigma(a) \neq a$  は  $\# \text{Orbit}(a) = 6$  つまり  $\# \text{Stab}(a) = 1$  を意味する。

したがって

$$\begin{aligned}\#B &= \{a \in I^6 \mid \#\text{Stab}(a) = 1\} \\ &= 64 - \{a \in I^6 \mid \#\text{Stab}(a) \geq 2\} \\ &= 64 - \{a \in I^6 \mid \text{Stab}(a) = \langle s^2 \rangle\} - \{a \in I^6 \mid \text{Stab}(a) = \langle s^3 \rangle\} - \{a \in I^6 \mid \text{Stab}(a) = \langle s \rangle\}\end{aligned}$$

である。いま  $\text{Stab}(a) = \langle s \rangle$  となる  $a \in I^6$  は

$$(0, 0, 0, 0, 0, 0) \quad (1, 1, 1, 1, 1, 1)$$

の 2 個。  $\text{Stab}(a) = \langle s^2 \rangle$  となる  $a \in I^6$  は

$$(0, 1, 0, 1, 0, 1) \quad (1, 0, 1, 0, 1, 0)$$

の 2 個。  $\text{Stab}(a) = \langle s^3 \rangle$  となる  $a \in I^6$  は

$$\begin{aligned}(0, 0, 1, 0, 0, 1) & \quad (0, 1, 0, 0, 1, 0) \\ (0, 1, 1, 0, 1, 1) & \quad (1, 0, 0, 1, 0, 0) \\ (1, 0, 1, 1, 0, 1) & \quad (1, 1, 0, 1, 1, 0)\end{aligned}$$

の 6 個。ゆえに  $\#B = 64 - (2 + 2 + 6) = 54$  が求める答えである。

## ■ 平成 25 年度 基礎数学

---

### 問 1

$\mathbb{R}^4$  に標準的な内積を入れる。 $V$  を

$$\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

で生成される  $\mathbb{R}^4$  の部分ベクトル空間とする。このとき  $V$  の  $\mathbb{R}^4$  における直交補空間  $W$  の基底を 1 組求めよ。

解答. 計算すると

$$W = \text{Ker} \begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

の基底としてたとえば

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

がとれることがわかる。

## 問 2

3 次の複素正方行列

$$A = \begin{pmatrix} -4 & -1 & -1 \\ 1 & -2 & 1 \\ 0 & 0 & -3 \end{pmatrix}, \quad B = \begin{pmatrix} -2 & 1 & 0 \\ -1 & -4 & 1 \\ 0 & 0 & -3 \end{pmatrix}$$

を考える。行列  $A$  と  $B$  は相似かどうか理由を答えよ。ただし、行列  $A$  と  $B$  が相似とは、複素正方行列  $P$  で  $A = P^{-1}BP$  をみたすものが存在することをいう。

解答. 固有多項式は  $A$  も  $B$  も  $(t+3)^3$  になるが、

$$\text{rank}((-3)E - A) = 1$$

$$\text{rank}((-3)E - B) = 2$$

なので固有空間の次元が異なる。よって  $A$  と  $B$  は相似ではない。

### 問 3

|  $\mathbb{R}^2$  上の関数  $f(x, y) = (3xy + 1)e^{-(x^2+y^2)}$  の最大値が存在することを示し、その最大値を求めよ。

解答.  $x = r \cos \theta$ ,  $y = r \sin \theta$  と変数変換して  $g(r, \theta) = f(x, y)$  とおく。このとき  $\theta$  に関係なく一様に

$$\lim_{r \rightarrow \infty} |g(r, \theta)| \leq \lim_{r \rightarrow \infty} \left( \frac{3}{2}r^2 + 1 \right) e^{-r^2} = 0$$

だから、ある  $R > 0$  があって、 $r \geq R$  のとき  $|g(r, \theta)| \leq 1 = f(0, 0)$  である。 $g$  は連続なので  $[0, R] \times [0, 2\pi]$  上で最大値を持っており、それが  $g$  および  $f$  の最大値となる。よって最大値の存在がいえた。

$g$  の停留点をすべて求めよう。方程式

$$\begin{aligned} \frac{\partial g}{\partial r} &= (3(1 - r^2) \sin 2\theta - 2)re^{-r^2} = 0 \\ \frac{\partial g}{\partial \theta} &= (3r^2 \cos 2\theta)e^{-r^2} = 0 \end{aligned}$$

を考える。これを解いて次の解を得る。

- (1)  $r = 0$
- (2)  $r = 1/\sqrt{3}$ ,  $\sin 2\theta = 1$
- (3)  $r = \sqrt{5/3}$ ,  $\sin 2\theta = -1$

それぞれの場合に  $g$  の値を求めると (1) のとき  $g = 1$ , (2) のとき  $g = \frac{3}{2}e^{-1/3}$  で、(3) のとき  $g = -\frac{3}{2}e^{-5/3}$  である。最大値は停留値のなかにあるので、このうち最大のもの、つまり  $\frac{3}{2}e^{-1/3}$  が  $g$  そして  $f$  の最大値である。



問 4

$\alpha, \beta$  を実数とする。広義積分

$$\int_1^{\infty} \frac{x^{\alpha} \log x}{(1+x)^{\beta}} dx$$

が収束するような  $\alpha, \beta$  の範囲を求めよ。

解答.  $F(x) = x^{\alpha}(1+x)^{-\beta} \log x$ ,  $G = x^{\alpha-\beta} \log x$  とおいたとき

$$\lim_{x \rightarrow \infty} \frac{F}{G} = \left( \frac{x}{1+x} \right)^{\beta} = 1$$

なので  $\int_1^{\infty} F dx$  と  $\int_1^{\infty} G dx$  の収束は同値。そこで  $\gamma = \alpha - \beta$  とおいて

$$I = \int_1^{\infty} x^{\gamma} \log x dx$$

の収束を考えればよい。いま  $\gamma \geq -1$  とすると

$$\begin{aligned} I &\geq \int_e^{\infty} x^{\gamma} \log x dx \\ &\geq \int_e^{\infty} x^{\gamma} dx \end{aligned}$$

より  $I$  は発散する。逆に  $\gamma < -1$  としよう。このとき

$$\begin{aligned} I &= \frac{1}{\gamma+1} \int_e^{\infty} (x^{\gamma+1})' \log x dx \\ &= -\frac{1}{\gamma+1} \int_e^{\infty} x^{\gamma+1} dx \end{aligned}$$

より  $I$  は収束する。まとめると、 $\gamma = \alpha - \beta$  としたとき、 $\gamma \geq -1$  なら発散で  $\gamma < -1$  なら収束。

## ■ 平成 25 年度 数学 I

### 問 1

複素数を成分とする 2 次正方行列全体の集合を  $M_2(\mathbb{C})$  で表す。 $A \in M_2(\mathbb{C})$  は単位行列のスカラー倍ではないとし、 $S = \{B \in M_2(\mathbb{C}) \mid AB = BA\}$  とおく。このとき、 $X, Y \in S$  なら  $XY = YX$  であることを示せ。

解答. この解答では、単に環といったとき可換とは限らないものとする。 $X \in M_n(\mathbb{C})$  に対して部分環  $Z(X)$  を

$$Z(X) = \{B \in M_2(\mathbb{C}) \mid XB = BX\}$$

により定める。 $Y \in M_2(\mathbb{C})$  と  $X$  が共役で、 $Y = PXP^{-1}$  なる  $P \in GL_2(\mathbb{C})$  が存在するとき、 $B \in Z(X)$  に対して  $(PBP^{-1})Y = PBXP^{-1} = PXBP^{-1} = Y(PBP^{-1})$  であるから  $PBP^{-1} \in Z(Y)$  である。つまり写像

$$\begin{aligned} Z(X) &\rightarrow Z(Y) \\ B &\mapsto PBP^{-1} \end{aligned}$$

が存在する。これは全単射であり、環としての同型である。

$A$  の Jordan 標準形を考えることにより

$$\Lambda := PAP^{-1} = \begin{pmatrix} \beta & \gamma \\ 0 & \delta \end{pmatrix}$$

となるような正則行列  $P$  の存在がいえる。ただし  $\gamma = 0$  または  $\beta = \delta$  であるものとする。スカラー行列でないという仮定から、 $\gamma = 0$  のとき  $\beta \neq \delta$  であり  $\beta = \delta$  のときでも  $\gamma \neq 0$  である。 $Z(\Lambda)$  を特定しよう。 $B \in M_2(\mathbb{C})$  が与えられたとし

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \Lambda = \begin{pmatrix} \beta & \gamma \\ 0 & \delta \end{pmatrix}$$

と表されていたとする。このとき計算すると

$$B\Lambda - \Lambda B = \begin{cases} \gamma \begin{pmatrix} -c & a-d \\ 0 & c \end{pmatrix} & (\beta = \delta, \gamma \neq 0) \\ (\beta - \gamma) \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} & (\beta \neq \delta, \gamma = 0) \end{cases}$$

だから  $Z(\Lambda)$  は次のように求まる。

(1)  $\beta = \delta, \gamma \neq 0$  のとき

$$Z(\Lambda) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$$

(2)  $\beta \neq \delta, \gamma = 0$  のとき

$$Z(\Lambda) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{C} \right\}$$

したがっていずれにせよ  $Z(\Lambda)$  は可換環である。よってそれと同型な  $Z(A)$  も可換環。

問 2

$b > a > 0$  を実数、 $f: [0, \infty) \rightarrow \mathbb{R}$  を連続関数とする。このとき以下を示せ。

(i)

$$\lim_{\varepsilon \rightarrow +0} \int_{a\varepsilon}^{a\varepsilon} \frac{f(x)}{x} dx = f(0) \log \frac{b}{a}$$

(ii) 広義積分  $\int_1^\infty \frac{f(x)}{x} dx$  が収束するなら

$$\int_1^\infty \frac{f(bx) - f(ax)}{x} dx = f(0) \log \frac{a}{b}$$

が成り立つ。

解答.

(i) 任意に  $c > 0$  が与えられたとする。仮定より

$$0 \leq x < \delta \rightarrow |f(x) - f(0)| < c$$

なる  $\delta > 0$  がある。そこで  $\varepsilon < b^{-1}\delta$  とおけば

$$\begin{aligned} \left| \int_{a\varepsilon}^{a\varepsilon} \frac{f(x)}{x} dx - f(0) \log \frac{b}{a} \right| &\leq \left| \int_{a\varepsilon}^{a\varepsilon} \frac{f(x) - f(0)}{x} dx \right| \\ &\leq \int_{a\varepsilon}^{a\varepsilon} \frac{|f(x) - f(0)|}{x} dx \\ &\leq c \int_{a\varepsilon}^{a\varepsilon} \frac{dx}{x} \\ &\leq c \log \frac{b}{a} \end{aligned}$$

である。 $c > 0$  は任意だったので、示すべきことがいえた。

(ii)  $\varepsilon > 0$  をとる。このとき

$$\begin{aligned} \int_\varepsilon^\infty \frac{f(bx) - f(ax)}{x} dx - f(0) \log \frac{a}{b} &= \int_{b\varepsilon}^\infty \frac{f(x)}{x} dx - \int_{a\varepsilon}^\infty \frac{f(x)}{x} dx + f(0) \log \frac{b}{a} \\ &= - \int_{a\varepsilon}^{b\varepsilon} \frac{f(x)}{x} dx + f(0) \log \frac{b}{a} \end{aligned}$$

であるから (i) より従う。

### 問 3

$p$  を素数とする。アーベル群  $A$  は位数  $p^4$  であり、位数  $p$  の部分群  $N$  で  $A/N \cong \mathbb{Z}/p^3\mathbb{Z}$  となるものをもつとする。このような  $A$  を同型を除いてすべて求めよ。

解答. 有限生成 Abel 群の基本定理により  $A$  は次のいずれかに同型である。

- (1)  $\mathbb{Z}/p^4\mathbb{Z}$
- (2)  $\mathbb{Z}/p^3\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$
- (3)  $\mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}$
- (4)  $\mathbb{Z}/p^2\mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})^2$
- (5)  $(\mathbb{Z}/p\mathbb{Z})^4$

一方で仮定により  $A/N \cong \mathbb{Z}/p^3\mathbb{Z}$  である。よって  $A/N$  には位数が  $p^3$  以上であるような元が存在する。したがって (3), (4), (5) はありえないと判る。逆に (1) ならば  $N = \langle p^3 \rangle$ , (2) ならば  $N = \langle (0, 1) \rangle$  とおけば条件を満たす。よって  $A$  は  $\mathbb{Z}/p^4\mathbb{Z}$  または  $\mathbb{Z}/p^3\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$  に同型である。

問 4

写像  $F: \mathbb{R}^4 \rightarrow \mathbb{R}^4$  を  $F(x, y, z, w) = (xy, y, z, w)$  と定め、写像  $f: S^3 \rightarrow \mathbb{R}^4$  を  $F$  の 3 次元球面

$$S^3 = \{(x, y, z, w) \in \mathbb{R}^4 \mid x^2 + y^2 + z^2 + w^2 = 1\}$$

への制限とする。 $S^3$  の各点  $p$  における  $f$  の微分  $df_p$  の階数を求めよ。

解答.  $g: \mathbb{R}^4 \rightarrow \mathbb{R}$  を  $g(x, y, z, w) = x^2 + y^2 + z^2 + w^2 - 1$  で定める。 $df_p$  は  $F$  のヤコビアン  $JF_p$  を  $\text{Ker } dg_p$  に制限したものと等しい。よって

$$\text{Ker } df_p = \text{Ker} \begin{pmatrix} JF_p \\ dg_p \end{pmatrix}$$

であるので

$$\text{rank } df_p = \text{rank} \begin{pmatrix} JF_p \\ dg_p \end{pmatrix} - 1$$

である。ここで  $p = (x, y, z, w)$  とおくと

$$\text{rank} \begin{pmatrix} JF_p \\ dg_p \end{pmatrix} = \text{rank} \begin{pmatrix} y & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ x & 0 & 0 & 0 \end{pmatrix}$$

なので

$$\text{rank } df_p = \begin{cases} 2 & (x = y = 0) \\ 3 & (x \neq 0 \text{ または } y \neq 0) \end{cases}$$

問 5

$a, b > 0$  を実数、 $n \geq 2$  を整数とすると、次の広義積分を求めよ。

$$I_n = \int_{-\infty}^{\infty} \frac{\exp(ia(x - ib))}{(x - ib)^n} dx$$

解答.  $R > 0$  とし、半径  $R$  の半円  $C_R = \{Re^{i\theta} \mid 0 \leq \theta \leq \pi\}$  を考える。 $C_R$  には  $\theta$  が増加する向きに向きが入っているものとする。

$$f(z) = \frac{\exp(ia(z - ib))}{(z - ib)^n}$$

とおくと、留数定理により、任意の  $R > b$  に対して

$$\int_{-R}^R f(x) dx + \int_{C_R} f(z) dz = 2\pi i \operatorname{Res}(f, ib)$$

である。いま計算すると

$$\int_{C_R} |f(z)| dz \leq \frac{Re^{ab}\pi}{(R - b)^n}$$

だから  $n \geq 2$  という仮定により  $\lim_{R \rightarrow \infty} \int_{C_R} |f(z)| dz = 0$  である。よって  $I_n = 2\pi i \operatorname{Res}(f, ib)$  である。

$$f(z) = \frac{1}{(z - ib)^n} \sum_{k=0}^{\infty} \frac{(ia)^k}{k!} (z - ib)^k$$

だから

$$I_n = \frac{2\pi i (ia)^{n-1}}{(n-1)!}$$

と求まる。

## ■ 平成 25 年度 数学 II

### 問 1

体  $K = \mathbb{Q}(\sqrt{N}, \sqrt{i+1})$  が  $\mathbb{Q}$  上の Galois 拡大となるような最小の正の整数  $N$  と、そのときの Galois 群  $\text{Gal}(K/\mathbb{Q})$  を求めよ。ただし  $i = \sqrt{-1}$  とする。

解答. 以下この解答では  $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$  は認めて使う。

$\sqrt{i+1}$  は  $(T^2 - 1)^2 + 1 = T^4 - 2T^2 + 2$  の根のひとつである。 $T^4 - 2T^2 + 2 \in \mathbb{Z}[T]$  は  $p = 2$  について Eisenstein 多項式なので  $T^4 - 2T^2 + 2 \in \mathbb{Q}[T]$  は既約元である。とくに  $[\mathbb{Q}(\sqrt{i+1}) : \mathbb{Q}] = 4$  がわかる。さらに

$$\begin{aligned} T^4 - 2T^2 + 2 &= (T^2 - 1)^2 + 1 \\ &= (T^2 - 1 + i)(T^2 - 1 - i) \\ &= (T^2 - \sqrt{2}e^{-\pi i/4})(T^2 - \sqrt{2}e^{\pi i/4}) \\ &= (T - \sqrt[4]{2}e^{-\pi i/8})(T + \sqrt[4]{2}e^{-\pi i/8})(T - \sqrt[4]{2}e^{\pi i/8})(T + \sqrt[4]{2}e^{\pi i/8}) \end{aligned}$$

であるから、 $\alpha = \sqrt[4]{2}e^{\pi i/8}$  とおいたとき  $\sqrt{i+1}$  の共役は  $\alpha, \bar{\alpha}, -\alpha, -\bar{\alpha}$  である。したがって  $K$  の  $\mathbb{Q}$  上の Galois 閉包を  $\tilde{K}$  とすると  $\alpha\bar{\alpha} = \sqrt{2}$  より  $\tilde{K} = \mathbb{Q}(\sqrt{N}, \sqrt{2}, \alpha)$  である。だから  $N = 2$  とおけば  $K/\mathbb{Q}$  は Galois 拡大である。

$N = 2$  が最小であることを示すには、 $\mathbb{Q}(\alpha)/\mathbb{Q}$  が Galois 拡大でないことを言わねばならない。ハイリホーで示す。 $\mathbb{Q}(\alpha)/\mathbb{Q}$  が Galois 拡大だと仮定する。このとき  $\bar{\alpha} \in \mathbb{Q}(\alpha)$  なので  $\sqrt{2} \in \mathbb{Q}(\alpha)$  である。 $i \in \mathbb{Q}(\alpha)$  はあきらかなので  $\mathbb{Q}(i, \sqrt{2}) \subset \mathbb{Q}(\alpha)$  であり、 $\mathbb{Q}$  上の拡大次数が同じだから  $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\alpha)$  である。 $G := \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$  とする。このとき  $\sigma \in G$  を

$$\begin{cases} \sigma(\sqrt{2}) = -\sqrt{2} \\ \sigma(i) = i \end{cases}$$

により定め、 $\tau \in G$  を複素共役とすると  $G = \{1, \sigma, \tau, \tau\sigma\}$  である。このとき  $\sigma(\alpha)$  は何になるか、ということを考える。 $\sigma(\alpha) = \alpha$  とすると  $\sigma$  が恒等写像となってしまうのでおかしい。 $\sigma(\alpha) = \bar{\alpha}$  とすると、 $\sigma$  と  $\tau$  が一致してしまうことになりおかしい。 $\sigma(\alpha) = -\alpha$  なら、

$$-\sqrt{2} = \sigma(\sqrt{2}) = \sigma(\alpha\bar{\alpha}) = -\alpha\sigma(\bar{\alpha})$$

より  $\sigma(\bar{\alpha}) = \bar{\alpha}$  である。これは  $\bar{\alpha}$  が  $\langle \sigma \rangle$  の不変体  $\mathbb{Q}(i)$  に属することを意味しており、 $[\mathbb{Q}(\alpha) : \mathbb{Q}] > [\mathbb{Q}(i) : \mathbb{Q}]$  に矛盾。もしも  $\sigma(\alpha) = -\bar{\alpha}$  なら、

$$-\sqrt{2} = -\bar{\alpha}\sigma(\bar{\alpha})$$

より  $\sigma(\bar{\alpha}) = \alpha$  である。これは  $\sigma^2(\alpha) = -\sigma(\bar{\alpha}) = -\alpha$  を意味し、 $\sigma^2 = 1$  であることに矛盾。いずれにせよ矛盾が得られたので、 $\mathbb{Q}(\alpha)/\mathbb{Q}$  は Galois 拡大ではない。とくに  $\sqrt{2}$  は  $\mathbb{Q}(\alpha)$  の元ではなく、 $K/\mathbb{Q}(\alpha)$  が 2 次拡大であることも従う。

あとは  $K = \mathbb{Q}(\sqrt{2}, \alpha)$  として Galois 群  $G := \text{Gal}(K/\mathbb{Q})$  を求めよう。 $K$  は中間体  $N := \mathbb{Q}(\sqrt{2})$  と  $M := \mathbb{Q}(\alpha)$  の合成体として得られるので、 $G$  の部分群として  $\text{Gal}(K/N) \cap \text{Gal}(K/M) = 1$  である。

$[K : \mathbb{Q}] = 8$  より  $[K : N] = 4$  であり、積をとる写像 (準同型とはいっていない)

$$\mathrm{Gal}(K/N) \times \mathrm{Gal}(K/M) \rightarrow G$$

は全単射である。 $N/\mathbb{Q}$  が Galois 拡大であることにより  $\mathrm{Gal}(K/N) \triangleleft G$  であることも含めると、 $G$  が次の半直積で表されることがわかる。

$$G \cong \mathrm{Gal}(K/N) \rtimes \mathrm{Gal}(K/M)$$

しかし半直積で表された、で済ますわけにはいかない。次に  $\mathrm{Gal}(K/N)$  の元を決定しよう。 $\alpha \in K$  は  $N$  上の多項式  $T^4 - 2T^2 + 2 \in N[T]$  の根である。 $[K : N] = 4$  なのでこれは既約多項式。したがって  $K$  は既約多項式  $T^4 - 2T^2 + 2 \in N[T]$  の  $N$  上の最小分解体だから、 $\mathrm{Gal}(K/N)$  は根の集合  $\{\alpha, \bar{\alpha}, -\alpha, -\bar{\alpha}\}$  に推移的に作用する。

$$\alpha_1 = \alpha, \quad \alpha_2 = \bar{\alpha}, \quad \alpha_3 = -\alpha, \quad \alpha_4 = -\bar{\alpha}$$

と添え字付けることにより、 $\mathrm{Gal}(K/N) \subset G \subset \mathfrak{S}_4$  とみなす。複素共役を  $\tau \in \mathrm{Gal}(K/N)$  とおくと、 $\tau = (12)(34)$  である。推移性により、ある  $\sigma \in \mathrm{Gal}(K/N)$  であって  $\sigma(\alpha) = -\alpha$  なるものがある。このとき

$$\sqrt{2} = \sigma(\alpha\bar{\alpha}) = -\alpha\sigma(\bar{\alpha})$$

より  $\sigma(\bar{\alpha}) = -\bar{\alpha}$  であることが判る。つまり  $\sigma = (13)(24)$  である。 $\sigma, \tau \in \mathfrak{S}_4$  は互いに可換であり、これで  $\mathrm{Gal}(K/N) = \langle (12)(34), (13)(24) \rangle = \{1, (13)(24), (14)(23), (12)(34)\}$  であることがいえた。

次に  $\mathrm{Gal}(K/M)$  の元を決定する。 $k \in \mathrm{Gal}(K/M)$  を  $k(\sqrt{2}) = -\sqrt{2}$  なる元とする。このとき

$$-\sqrt{2} = k(\alpha\bar{\alpha}) = \alpha k(\bar{\alpha})$$

より  $k(\bar{\alpha}) = -\bar{\alpha}$  であって、 $k = (24)$  であることがわかった。まとめると

$$G = \langle (13)(24), (12)(34), (24) \rangle \subset \mathfrak{S}_4$$

である。 $(12)(34)(24) = (1234)$  なので、これは

$$G = \langle (1234), (24) \rangle \cong D_4$$

であることを意味している。なお位数 8 の有限群であって、正規でない部分群を持つのは  $D_4$  だけであることを知っているなら、それを使ってもよい。



## 問 2

$A = \mathbb{C}[x, y]$  を  $\mathbb{C}$  上の 2 変数多項式環とし、 $A$  の部分環  $B$  を

$$B = \{f(x, y) \in A \mid f(-x, -y) = f(x, y)\}$$

と定める。このとき、次の問 (1), (2) に答えよ。

- (1)  $A$  の極大イデアル  $m_0 = (x, y)$ ,  $m_1 = (x - 1, y)$  に対し、 $n_0 = m_0 \cap B$ ,  $n_1 = m_1 \cap B$  とおく。このとき、剰余環  $A/n_0A$ ,  $A/n_1A$  の  $\mathbb{C}$  上のベクトル空間としての次元を求めよ。
- (2)  $A$  が  $B$  加群として自由加群ではないことを証明せよ。

解答.

- (1)  $B$  は偶数次の項だけからなる  $A$  の元全体と一致するので、

$$B = \mathbb{C}[x^2, xy, y^2]$$

である。いま  $(x^2, xy, y^2)B \subset n_0$  であるが、 $(x^2, xy, y^2)B$  は極大イデアルで  $n_0$  は素イデアルなので  $(x^2, xy, y^2)B = n_0$  であり、

$$\begin{aligned} A/n_0A &\cong \mathbb{C}[x, y]/(x^2, xy, y^2) \\ &\cong \mathbb{C}^3 \end{aligned}$$

と求まる。また  $(x^2 - 1, xy, y^2)B \subset n_1$  であるが、 $(x^2 - 1, xy, y^2)B$  が極大イデアルであることと  $n_1$  が素イデアルであることにより  $(x^2 - 1, xy, y^2)B = n_1$  である。よって

$$\begin{aligned} A/n_1A &\cong \mathbb{C}[x, y]/(x^2 - 1, xy, y^2) \\ &\cong \mathbb{C}[x, y]/(x - 1, xy, y^2)(x + 1, xy, y^2) \\ &\cong \mathbb{C}[x, y]/(x - 1, y)(x + 1, y) \\ &\cong \mathbb{C}^2 \end{aligned}$$

である。

- (2) ハイリホーによる。仮に  $A$  が自由  $B$  加群だったと仮定すると、 $A \cong B^{\oplus k}$  なる  $k$  がある。このとき  $i$  によらずに

$$A/n_iA \cong A \otimes_B B/n_i \cong (B/n_i)^{\oplus k} \cong \mathbb{C}^{\oplus k}$$

となるはずなので、矛盾。よって  $A$  は自由  $B$  加群ではない。

問 1

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \quad v_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad v_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$w_1 = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} \quad w_2 = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} \quad w_3 = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

とおく。\$V\$ を \$v\_1, v\_2, v\_3\$ で生成される \$\mathbb{R}^4\$ の部分ベクトル空間とし、\$W\$ を \$w\_1, w\_2, w\_3\$ で生成される \$\mathbb{R}^4\$ の部分ベクトル空間とする。このとき、\$V \cap W\$ の基底をひとつ求めよ。

解答. \$V \cap W = (V^\perp + W^\perp)^\perp\$ を用いて求める。計算すると

$$V^\perp = \left\{ x \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}$$

$$W^\perp = \left\{ x \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}$$

であるから

$$V \cap W = \left\{ x \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$$

であることが判る。

## 問 2

複素数体  $\mathbb{C}$  の元を成分とする  $n$  次正方行列全体のなす集合を  $M_n(\mathbb{C})$  とする。

- (1)  $M_n(\mathbb{C})$  の元  $N$  が、ある自然数  $k$  に対して  $N^k$  が零行列になるとする。このとき、 $N$  の固有値がすべて 0 であることを示せ。
- (2)  $M_n(\mathbb{C})$  の元  $A$  をひとつ決めて、写像  $f_A: M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$  を  $f_A(X) = XA - AX$  によって定義する。 $M_n(\mathbb{C})$  は複素数体  $\mathbb{C}$  上の  $n^2$  次元のベクトル空間であり、 $f_A$  は  $M_n(\mathbb{C})$  の線形変換である。このとき、ある自然数  $m$  に対して  $A^m$  が零行列になるとすると、線形変換  $f_A$  の固有値がすべて 0 となることを示せ。

解答.  $E(\lambda, T)$  で  $T$  の  $\lambda$  に属する固有空間を表すことにする。

- (1)  $\lambda$  を  $N$  の固有値とし、 $v \in E(\lambda, N) \setminus \{0\}$  とする。すると  $N^k v = \lambda^k v$  である。 $N^k = 0$  であるから、 $\lambda = 0$  でなくてはならない。
- (2)  $f_A$  の  $k$  回合成を  $f_A^k$  と書くことにする。このときあきらかに

$$f_A^k(X) = \sum_{i+j=k} a_{i,j}(k) A^i X A^j$$

が成り立つような  $a_{i,j}(k) \in \mathbb{C}$  が存在する。よって  $f_A^{2m} = 0$  なので  $f_A$  はべき零であり、(1) よりとくに固有値はすべて 0 である。

コメント. 読者は (2) の解答をどう思われたであろうか。Lie 環のブラケットのごとき豊富な構造をもつものを題材としながら、かくも自明であろうとは無礼千万、到底許すべからざることだ……との感想を持たれたとしたら、ご意見全く同感である。実際  $A$  がべき零であるという仮定を外して、(2) の主張を次のように一般化することができる。

**命題.**  $A \in M_n(\mathbb{C})$  に対して  $f_A: M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$  を  $f_A(X) = [X, A] = XA - AX$  によって定義する。このとき  $A$  の固有値の重複度を込めた全体、つまり  $A$  のスペクトラムを  $\{\mu_1, \dots, \mu_n\}$  とすると  $f_A$  のスペクトラムは  $\{\mu_i - \mu_j \mid 1 \leq i, j \leq n\}$  である。

証明.  $A$  が対角化可能であるときにまず示す。双線形形式

$$\begin{aligned} \mathbb{C}^n \times \mathbb{C}^n &\rightarrow M_n(\mathbb{C}) \\ (u, v) &\rightarrow uv^T \end{aligned}$$

が誘導する線形写像  $s: \mathbb{C}^n \otimes \mathbb{C}^n \rightarrow M_n(\mathbb{C})$  を考える。 $\mathbb{C}^n$  の標準基底を  $\{e_i\}$  としたとき  $\{e_i \otimes e_j\}_{i,j}$  は  $\mathbb{C}^n \otimes \mathbb{C}^n$  の基底になるが、 $s$  はこれをどう写すだろうか？ある  $c_{ij} \in \mathbb{C}$  があり

$$\sum_{i,j} c_{ij} s(e_i \otimes e_j) = 0$$

だったとする。このとき任意の  $k$  について

$$\begin{aligned} 0 &= \left( \sum_{i,j} c_{ij} e_i e_j^T \right) e_k \\ &= \sum_{i,j} c_{ij} \delta_{jk} e_i \\ &= \sum_i c_{ik} e_i \end{aligned}$$

であるから  $c_{ik} = 0$  である。 $k$  は任意だったから、 $s$  が単射であることがわかる。 $\mathbb{C}^n \otimes \mathbb{C}^n$  の  $\mathbb{C}$  ベクトル空間としての次元は  $n^2$  で、 $M_n(\mathbb{C})$  と同じなので  $s$  は同型でもある。

いま  $A$  は対角化可能と仮定したので  $A^T$  も対角化可能である。 $A$  と  $A^T$  の特性多項式は同じなのでスペクトラムも同一であり、

$$\mathbb{C}^n \otimes \mathbb{C}^n = \bigoplus_{i,j} E(\mu_i, A) \otimes E(\mu_j, A^T)$$

と書ける。同型  $s$  による  $E(\mu_i, A) \otimes E(\mu_j, A^T)$  の像を考えよう。 $u \in E(\mu_i, A)$  と  $v \in E(\mu_j, A^T)$  が与えられたとする。このとき

$$\begin{aligned} [uv^T, A] &= uv^T A - Auv^T \\ &= u(A^T v)^T - (Au)v^T \\ &= (\mu_j - \mu_i)uv^T \end{aligned}$$

であるから  $s(u \otimes v) \in E(\mu_j - \mu_i, f_A)$  である。 $s$  は線形なので  $s$  による  $E(\mu_i, A) \otimes E(\mu_j, A^T)$  の像は  $E(\mu_j - \mu_i, f_A)$  に含まれる。 $s$  は同型なので、これにより  $f_A$  も対角化可能であって、そのスペクトラムが  $\{\mu_i - \mu_j \mid 1 \leq i, j \leq n\}$  となることがいえた。

対角化可能とは限らない一般の  $A$  の場合。このとき  $A$  に収束する対角化可能な行列の列  $\{A_m\} \subset M_n(\mathbb{C})$  がとれる。 $A$  のスペクトラムを  $\{\mu_i\}$ 、 $A_m$  のスペクトラムを  $\{\mu_i^{(m)}\}$  とすると、固有値は係数に連続的に依存するので  $\lim_{m \rightarrow \infty} \mu_i^{(m)} = \mu_i$  である。(そうなるように番号を対応させる) したがって  $f_A$  のスペクトラムは  $f_{A_m}$  のスペクトラム  $\left\{ \mu_i^{(m)} - \mu_j^{(m)} \mid 1 \leq i, j \leq n \right\}$  の極限であるので、 $\{\mu_i - \mu_j \mid 1 \leq i, j \leq n\}$  となる。□

### 問 3

$x > 0$  で定義された次の関数項級数は各点収束するが  $(0, \infty)$  上で一様収束しないことを示せ。

$$\sum_{n=0}^{\infty} \frac{x^2}{n^2 x + 1}$$

解答.  $n \rightarrow \infty$  の極限での振る舞いを単純化しよう。

$$f_n(x) = \frac{x^2}{n^2 x + 1}, \quad g_n(x) = \frac{x}{n^2}$$

として、 $E = [1, \infty)$  とおく。 $E$  上では  $x$  によらずに

$$\left| \frac{f_n(x)}{g_n(x)} - 1 \right| \leq \frac{1}{n^2 x + 1} \leq \frac{1}{n^2}$$

だから、 $E$  上で  $f_n/g_n$  は 1 に一様収束する。したがって

$$n \geq R \rightarrow \forall x \in E \quad \frac{1}{2} g_n(x) \leq f_n(x) \leq \frac{3}{2} g_n(x)$$

なる  $R > 0$  がある。いま任意に自然数  $L > 0$  が与えられたとする。このとき  $L' = \max\{L+1, R\}$  とすると  $E$  上において

$$\begin{aligned} \sum_{n=0}^{\infty} f_n(x) - \sum_{n=0}^L f_n(x) &= \sum_{n=L+1}^{\infty} f_n(x) \\ &\geq \sum_{n=L'}^{\infty} f_n(x) \\ &\geq \frac{1}{2} \sum_{n=L'}^{\infty} g_n(x) \\ &\geq \frac{x}{2} \sum_{n=L'}^{\infty} \frac{1}{n^2} \end{aligned}$$

と評価できる。ここで

$$\left\| \frac{x}{2} \sum_{n=L'}^{\infty} \frac{1}{n^2} \right\|_E \geq \frac{(L')^2}{2} \sum_{n=L'}^{\infty} \frac{1}{n^2} \geq 1$$

であることより

$$\left\| \sum_{n=0}^{\infty} f_n(x) - \sum_{n=0}^L f_n(x) \right\|_{(0, \infty)} \geq 1$$

となる。 $L$  は任意にとっていたはずだから、これで一様収束しないことがいえた。

問 4

次の広義積分が収束するような実数  $s$  の範囲を求めよ。またそのときの積分値を計算せよ。

$$\iint_{\mathbb{R}^2} \frac{dxdy}{(x^2 - xy + y^2 + 1)^s}$$

解答.  $x^2 - xy + y^2 = (x - y/2)^2 + (\sqrt{3}y/2)^2$  であるから

$$\begin{aligned} x - \frac{y}{2} &= \zeta = r \cos \theta \\ \frac{\sqrt{3}}{2}y &= \eta = r \sin \theta \end{aligned}$$

とおくと

$$d\zeta d\eta = \left| \det \begin{pmatrix} 1 & -1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix} \right| dxdy = \frac{\sqrt{3}}{2} dxdy$$

より  $dxdy = 2/\sqrt{3} d\zeta d\eta = 2r/\sqrt{3} dr d\theta$  である。よって

$$\begin{aligned} \iint_{\mathbb{R}^2} \frac{dxdy}{(x^2 - xy + y^2 + 1)^s} &= \frac{2}{\sqrt{3}} \int_0^{2\pi} \int_0^\infty \frac{r}{(r^2 + 1)^s} dr \\ &= \frac{1}{\sqrt{3}} \int_0^{2\pi} \int_0^\infty \frac{1}{(r + 1)^s} dr \end{aligned}$$

である。ゆえにこの積分は  $s > 1$  のとき、かつそのときに限って収束する。そして  $s > 1$  であるとき積分値は

$$\frac{2\pi}{\sqrt{3}(s-1)}$$

である。

## ■ 平成 24 年度 数学 I

---

### 問 1

$A, B$  は複素数係数の  $n$  行  $m$  列行列、 $f(X)$  は複素数係数の多項式とする。

$$Af(B) = B$$

が成り立っているとする。次を証明せよ。

- (1)  $f(B)$  が正則ならば  $A$  と  $B$  は可換である。
- (2)  $f(B)$  が正則でなければ  $f(0) = 0$  である。

解答.

- (1)  $f(B)$  は  $B$  と可換なので

$$(BA - AB)f(B) = BAf(B) - Af(B)B = B^2 - B^2 = 0$$

である。 $f(B)$  は正則だったから  $BA = AB$  が従う。

- (2)  $f(B)$  が正則でないので、ある  $v \in \mathbb{C}^n \setminus \{0\}$  であって  $f(B)v = 0$  なるものがある。よって  $Bv = Af(B)v = 0$  だから  $f(0)v = 0$  である。 $v \neq 0$  より  $f(0) = 0$  でなくてはならない。

## 問 2

$p \geq 3$  を奇素数、 $n$  を自然数とする。行列の乗法を演算とする群

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{Z}/p^n\mathbb{Z}, ad = 1 \right\}$$

には位数  $p^{2n-1}$  の部分群がただ一つ存在することを示せ。

解答. まず  $G$  の位数を求めると、 $\#G = p^n \times \#(\mathbb{Z}/p^n\mathbb{Z})^\times = p^{2n-1}(p-1)$  である。したがって、 $G$  の Sylow- $p$  部分群が正規部分群であることを示せば十分。いま  $H \subset G$  を  $G$  の Sylow- $p$  部分群とする。このとき  $H$  の共役の数を  $s$  とすると、 $s$  は  $\#(G/H) = p-1$  の約数であってかつ  $s \equiv 1 \pmod{p}$  を満たす。よって  $s = 1$  である。つまり  $H \triangleleft G$  なので、示すべきことがいえた。



### 問 3

$f(x)$  は  $[0, \infty)$  上の非負実数値連続関数で単調非増加であり、かつ  $f(x)/\sqrt{x}$  は  $[0, \infty)$  上広義積分をもつと仮定する。このとき、以下の間に答えよ。

(1)  $\lim_{x \rightarrow \infty} \sqrt{x}f(x) = 0$  を示せ。

(2) 任意の  $0 < \varepsilon < 1$  に対し

$$\lim_{x \rightarrow \infty} \int_{\varepsilon x}^x \frac{f(y)}{\sqrt{x-y}} dy = 0$$

を示せ。

解答.

(1) 計算すると

$$\begin{aligned} \int_x^{2x} \frac{f(t)}{\sqrt{t}} dt &\geq f(2x) \int_x^{2x} \frac{dt}{\sqrt{t}} \\ &\geq 2f(2x)(\sqrt{2x} - \sqrt{x}) \\ &\geq (2 - \sqrt{2})\sqrt{2x}f(2x) \end{aligned}$$

であることより、あきらか。

(2) 計算すると

$$\begin{aligned} \int_{\varepsilon x}^x \frac{f(y)}{\sqrt{x-y}} dy &\leq f(\varepsilon x) \int_{\varepsilon x}^x \frac{dy}{\sqrt{x-y}} \\ &\leq 2\sqrt{1-\varepsilon}\sqrt{x}f(\varepsilon x) \\ &\leq 2\sqrt{(1-\varepsilon)/\varepsilon}\sqrt{\varepsilon x}f(\varepsilon x) \end{aligned}$$

である。よって (1) よりあきらか。

#### 問 4

$n$  を正の整数とし、 $\mathbb{T}^n$  を  $\mathbb{C}^n$  に標準的に埋め込まれた  $n$  次元トーラス、すなわち

$$\mathbb{T}^n = \{(z_1, \dots, z_n) \in \mathbb{C}^n \mid |z_1| = \dots = |z_n| = 1\}$$

とする。 $f: \mathbb{T}^n \rightarrow \mathbb{T}^n$  を、連続写像ですべての  $(z_1, \dots, z_n) \in \mathbb{T}^n$  について

$$f(z_1, \dots, z_n) = f(\bar{z}_1, \dots, \bar{z}_n)$$

をみたすものとする。 $(\bar{z}$  は  $z \in \mathbb{C}$  の複素共役を表す)

- (1)  $S^1$  を単位円  $\{z \in \mathbb{C} \mid |z| = 1\}$  とし、写像  $\gamma: S^1 \rightarrow \mathbb{T}^n$  を  $\gamma(z) = (z, 1, \dots, 1)$  で定める、このとき  $f \circ \gamma$  は定値写像とホモトピックであることを示せ。
- (2)  $f$  が誘導する基本群の間の写像  $f_*: \pi_1(\mathbb{T}^n) \rightarrow \pi_1(\mathbb{T}^n)$  は零写像であることを示せ。
- (3)  $f$  は定値写像とホモトピックであることを示せ。

(注) 位相空間  $X, Y$  とその間の連続写像  $F: X \rightarrow Y$  について、 $F$  が定値写像とホモトピックであるとは、連続写像  $H: X \times [0, 1] \rightarrow Y$  と  $q_* \in Y$  で、すべての  $p \in X$  について  $H(p, 0) = q_*$  と  $H(p, 1) = F(p)$  が成り立つものが存在することをいう。

注意. (1) においてホモトピー  $H: S^1 \times [0, 1] \rightarrow \mathbb{T}^n$  を

$$H(e^{i\theta}, t) = f(e^{i\theta t}, 1, \dots, 1)$$

とすればいいというのは誤りである。 $\theta$  には  $2\pi$  の整数倍分のあいまいさがあるので、この  $H$  は well-defined にならない。

解答.

- (1)  $e^{i\theta} = z$  という対応により  $\gamma: S^1 \rightarrow \mathbb{T}^n$  を  $\mathbb{R}/2\pi\mathbb{Z}$  上の写像とみなす。 $f$  についての仮定により  $f \circ \gamma$  は  $P := f \circ \gamma(0) = f(1, \dots, 1)$  を出発して  $Q := f \circ \gamma(\pi) = f(-1, 1, \dots, 1)$  まで行き、その後来た道を引き返して  $P$  に戻っていくようなパスである。つまり

$$f \circ \gamma(\theta) = f(e^{i(\pi - |\pi - \theta|)}, 1, \dots, 1)$$

と表せる。したがって  $H: \mathbb{R}/2\pi\mathbb{Z} \times [0, 1] \rightarrow \mathbb{T}^n$  を

$$H(\theta, t) = f(e^{it(\pi - |\pi - \theta|)}, 1, \dots, 1)$$

とおけば、これは  $f \circ \gamma$  と定値写像の間のホモトピーである。

- (2)  $\pi_1(\mathbb{T}^n) = \pi_1(S^1 \times \dots \times S^1) = \pi_1(S^1) \times \dots \times \pi_1(S^1)$  だから、 $f_*: \pi_1(\mathbb{T}^n) \rightarrow \pi_1(\mathbb{T}^n)$  が零写像であることを示すには、 $\pi_1(S^1) \cong \mathbb{Z}$  の生成元を  $a$  として  $f_*(a, 1, \dots, 1) = 0$  を示せばよい。ところが  $f_*(a, 1, \dots, 1) = [f \circ \gamma]$  なので (1) により、示すべきことがいえた。
- (3) (2) により  $f_*(\pi_1(\mathbb{T}^n)) = 0$  なので、次を可換にするリフト  $g$  が存在することがわかる。

$$\begin{array}{ccc} & & \mathbb{R}^n \\ & \nearrow g & \downarrow p \\ \mathbb{T}^n & \xrightarrow{f} & \mathbb{T}^n \end{array}$$

ただし  $p: \mathbb{R}^n \rightarrow \mathbb{T}^n$  は普遍被覆である。そこで  $H: \mathbb{T}^n \times [0, 1] \rightarrow \mathbb{T}^n$  を

$$H(w, t) = p(tg(w))$$

とすると、これは  $f$  と定値写像の間のホモトピーになっている。

問 5

関数  $f$  を

$$f(z) = \frac{1}{2\pi i} \int_{-\infty}^{\infty} \frac{e^{-|x|}}{x-z} dx$$

と定める。このとき  $f(z)$  は  $z \in \mathbb{C} \setminus \mathbb{R} = \{z \in \mathbb{C} \mid z \notin \mathbb{R}\}$  で正則であることを示せ。また、極限

$$\lim_{\varepsilon \rightarrow +0} (f(i\varepsilon) - f(-i\varepsilon))$$

を求めよ。

解答. 微分と積分が交換するだろうという楽観的な予想が正しければ、

$$f'(z) = \frac{1}{2\pi i} \int_{-\infty}^{\infty} \frac{e^{-|x|}}{(x-z)^2} dx$$

となっているはずである。これが正しいことを確かめればよい。つまり与えられた開集合  $U := \mathbb{C} \setminus \mathbb{R}$  上で

$$\lim_{w \rightarrow 0} \left| \frac{f(z+w) - f(z)}{w} - \frac{1}{2\pi i} \int_{-\infty}^{\infty} \frac{e^{-|x|}}{(x-z)^2} dx \right| = 0$$

となることを示そうというのである。そうすれば  $f$  が  $U$  上で正則であることがいえる。(ある点  $z$  での正則性とは、 $z$  のある開近傍上で微分可能であるということであって、 $z$  における微分可能性より強い性質だが、 $U$  が開集合なので問題ない)

$z \in U$  とする。計算すると

$$\left| \frac{f(z+w) - f(z)}{w} - \frac{1}{2\pi i} \int_{-\infty}^{\infty} \frac{e^{-|x|}}{(x-z)^2} dx \right| \leq \frac{|w|}{2\pi} \int_{-\infty}^{\infty} \frac{e^{-|x|}}{|(x-z)^2(x-z-w)|} dx$$

であることが判る。 $|w|$  が十分小さいとき、 $|\operatorname{Im}(z+w)| \geq |\operatorname{Im}(z)|/2$  としてよい。よって  $y := |\operatorname{Im}(z)|$  とおけば  $z \in U$  より  $y > 0$  であって

$$\begin{aligned} \frac{|w|}{2\pi} \int_{-\infty}^{\infty} \frac{e^{-|x|}}{|(x-z)^2(x-z-w)|} dx &\leq \frac{|w|}{2\pi} \left(\frac{y}{2}\right)^{-3} \int_{-\infty}^{\infty} e^{-|x|} dx \\ &\leq \frac{8|w|}{y^3\pi} \end{aligned}$$

である。よって  $w \rightarrow 0$  のときこの積分はゼロになる。これで  $f$  が  $U$  上で正則であることがいえた。

また、愚直に計算すると

$$f(i\varepsilon) - f(-i\varepsilon) = \frac{2\varepsilon}{\pi} \int_0^{\infty} \frac{e^{-x}}{x^2 + \varepsilon^2} dx$$

である。 $x = \varepsilon \tan \theta$  において変数変換すると

$$f(i\varepsilon) - f(-i\varepsilon) = \frac{2}{\pi} \int_0^{\pi/2} e^{-\varepsilon \tan \theta} d\theta$$

と表せる。ここで  $\varepsilon_n \rightarrow 0$  なる点列  $\varepsilon_n > 0$  が任意に与えられたとする。 $n$  によらず一様に

$$|e^{-\varepsilon_n \tan \theta}| \leq 1$$

であって  $1$  は区間  $[0, \pi/2)$  上可積分なので、Lebesgue の収束定理により

$$\lim_{n \rightarrow \infty} (f(i\varepsilon_n) - f(-i\varepsilon_n)) = \frac{2}{\pi} \int_0^{\pi/2} d\theta = 1$$

である。 $\varepsilon_n$  は任意だったから、求める極限は  $1$  である。

## ■ 平成 24 年度 数学 II

### 問 1

1 以上の整数  $a$  に対して  $K = \mathbb{Q}(\sqrt{3+a\sqrt{5}})$  が  $\mathbb{Q}$  の Galois 拡大体となるものを求め、そのような  $a$  に対して Galois 群  $\text{Gal}(K/\mathbb{Q})$  を求めよ。

解答. 以下、この解答では  $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = 4$  は認めて使う。

$\beta = \sqrt{3+a\sqrt{5}}$  とおく。 $\beta$  は  $f(X) = X^4 - 6X^2 + 9 - 5a^2 \in \mathbb{Z}[X]$  の根である。 $\beta$  の共役元を調べたいので、 $f$  の既約性をいいたい。そのために  $[K : \mathbb{Q}] = 4$  を示そう。 $M := \mathbb{Q}(\sqrt{5})$  とおく。 $[K : M] = 2$  を示せば十分である。

ハイリホーで  $[K : M] = 2$  を示そう。仮にそうでないとする。このとき  $\beta \in M$  である。 $\beta^2 = 3 + a\sqrt{5}$  より、

$$N_{M/\mathbb{Q}}(\beta)^2 = 9 - 5a^2$$

である。 $\beta \in M$  は  $\mathbb{Z}$  上整なので、 $N_{M/\mathbb{Q}}(\beta) \in \mathbb{Z}$  であり、したがって  $9 - 5a^2 \in \mathbb{Z}$  は平方数である。これは  $a = 1$  でなくてはならないことを意味する。このとき、そもそも

$$\beta = \sqrt{3 + \sqrt{5}} = \frac{1 + \sqrt{5}}{\sqrt{2}}$$

だから  $\sqrt{2} \in M$  ということになる。これは矛盾。したがって  $[K : M] = 2$  であり、とくに  $f \in \mathbb{Q}[X]$  は既約多項式である。

よって  $\gamma := \sqrt{3-a\sqrt{5}}$  としたとき  $\beta$  の  $\mathbb{Q}$  上の共役元は  $\{\pm\beta, \pm\gamma\}$  である。ゆえに  $K$  の  $\mathbb{Q}$  上の Galois 閉包を  $L$  とおくと  $L = \mathbb{Q}(\beta, \gamma) = K(\sqrt{9-5a^2})$  である。これにより  $a \geq 2$  のとき  $K \neq L$  なので  $K/\mathbb{Q}$  は Galois 拡大ではない。よって  $K/\mathbb{Q}$  が Galois 拡大になるのは  $a = 1$  のときである。

$a = 1$  とすると先述のように  $\beta = (1 + \sqrt{5})/\sqrt{2}$  なので  $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \subset K$  である。 $\mathbb{Q}$  上の拡大次数が同じなので  $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = K$  であり、Galois 拡大の推進定理から  $\text{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  であることが判る。

問 2

- (1)  $n$  は 2 以上の整数とし、 $\zeta_n$  を 1 の原始  $n$  乗根とする。 $\mathbb{C}[[x, y]]$  は変数  $x, y$  についての  $\mathbb{C}$  上の二変数形式的べき級数環とする。

$$R = \{f(x, y) \in \mathbb{C}[[x, y]] \mid f(\zeta_n x, \zeta_n^{-1} y) = f(x, y)\}$$

とおく。環  $R$  は  $\mathbb{C}$  上の二変数形式的べき級数環に  $\mathbb{C}$  代数として同型ではないことを示せ。

- (2) 環

$$S = \{f(x, y) \in \mathbb{C}[[x, y]] \mid f(\zeta_n x, \zeta_n y) = f(x, y)\}$$

は  $n > 2$  のとき、 $\mathbb{C}$  代数として  $R$  に同型ではないことを示せ。

解答.

- (1)  $R$  の元は  $x^i y^j$  ( $i - j \in n\mathbb{Z}$ ) という形の元の形式和なので  $R = \mathbb{C}[[x^n, xy, y^n]]$  であって、 $R$  は  $\mathfrak{m}_R = (x^n, xy, y^n)$  を極大イデアルとする局所環である。 $\mathbb{C}$  ベクトル空間  $\mathfrak{m}_R/\mathfrak{m}_R^2$  の次元を求めよう。

$$\mathfrak{m}_R/\mathfrak{m}_R^2 = (x^n, xy, y^n)/(x^{2n}, x^2 y^2, y^{2n}, x^{n+1} y, x^n y^n, xy^{n+1})$$

である。 $x^n, xy, y^n$  は  $\mathfrak{m}_R/\mathfrak{m}_R^2$  において線形独立なので次元は 3 以上。また  $\mathfrak{m}_R/\mathfrak{m}_R^2$  は 3 つの元で生成されているので次元は 3 以下であることもいえる。よって  $\dim_{\mathbb{C}} \mathfrak{m}_R/\mathfrak{m}_R^2 = 3$  であることが判った。一方で局所環  $\mathbb{C}[[x, y]]$  の極大イデアルを  $\mathfrak{m} = (x, y)$  とすると

$$\mathfrak{m}/\mathfrak{m}^2 = (x, y)/(x^2, xy, y^2)$$

であるから  $\dim_{\mathbb{C}} \mathfrak{m}/\mathfrak{m}^2 = 2$  なので同型ではない。

- (2)  $S$  の元は  $x^i y^j$  ( $i + j \in n\mathbb{Z}$ ) という形の元の形式和なので

$$S = \mathbb{C}[[x^n, x^{n-1} y, \dots, xy^{n-1}, y^n]]$$

と表せる。局所環  $S$  の極大イデアル  $\mathfrak{m}_S$  は

$$\mathfrak{m}_S = (x^n, x^{n-1} y, \dots, xy^{n-1}, y^n)$$

と表される。 $\mathfrak{m}_S^2$  は次数が  $2n$  であるような元で生成されるので、 $\mathfrak{m}_S/\mathfrak{m}_S^2$  において

$$\{x^n, x^{n-1} y, \dots, xy^{n-1}, y^n\}$$

は線形独立である。よって  $\dim_{\mathbb{C}}(\mathfrak{m}_S/\mathfrak{m}_S^2) \geq n + 1$  である。いま  $n \geq 3$  と仮定したので、これで示すべきことがいえたことになる。

## ■ 平成 23 年度 基礎数学

---

### 問 1

$x$  を複素数とする。4 次複素正方行列

$$\begin{pmatrix} x & 1 & -1 & 1 \\ 1 & x & 1 & -1 \\ -1 & 1 & x & 1 \\ 1 & -1 & 1 & x \end{pmatrix}$$

の階数を求めよ。

解答. 与えられた行列を  $A$  とする。基本変形を繰り返して

$$\text{rank } A = \begin{cases} 1 & (x = -1) \\ 3 & (x = 3) \\ 4 & (x \neq 3, -1) \end{cases}$$

を得る。



## 問 2

3 次複素正方行列

$$A = \begin{pmatrix} 6 & -3 & -2 \\ 4 & -1 & -2 \\ 3 & -2 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 & -1 \\ 1 & 3 & 1 \\ -1 & -1 & 1 \end{pmatrix}$$

を考える。

- (1)  $A, B$  の固有値 2 に属する固有空間の基底を一組ずつ求めよ。
- (2)  $A$  と  $B$  は相似かどうか理由をつけて答えよ。ただし、2 つの 3 次複素正方行列  $A, B$  が相似とは、 $A = P^{-1}BP$  をみたす正則な 3 次複素正方行列  $P$  が存在することをいう。

解答. 以下単位行列を  $E$  で表すことにする。

- (1) 計算すると

$$\begin{aligned} \text{Ker}(2E - A) &= \left\{ z \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix} \in \mathbb{C}^3 \mid z \in \mathbb{C} \right\} \\ \text{Ker}(2E - B) &= \left\{ y \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + z \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \in \mathbb{C}^3 \mid y, z \in \mathbb{C} \right\} \end{aligned}$$

である。

- (2) 固有値 2 に属する固有空間の次元が異なるので、 $A$  と  $B$  は相似ではない。

### 問 3

函数項級数

$$\sum_{n=1}^{\infty} \frac{x}{(1+x)^n}$$

が区間  $[0, 1]$  上で一様収束するかどうかを、理由を付けて答えよ。

解答. 与えられた級数を  $f(x)$  で表す。計算すると  $f(0) = 0$  かつ  $f(x) = 1$  ( $x > 0$ ) であることがわかる。よって  $f$  は連続ではないが、もし一様収束するならば連続であるはずなので、一様収束しない。

問 4

$a < b$  とし区間  $[a, b]$  上の実数値連続関数  $f(x), \varphi(x)$  は共に狭義単調増加とする。

$$\int_a^b f(x) dx = 0$$

ならば、 $\int_a^b \varphi(x)f(x) dx > 0$  となることを証明せよ。

解答. 仮定より  $(b-a)f(a) < 0 < (b-a)f(b)$  である。よって  $f(a) < 0$  かつ  $f(b) > 0$  であることがわかる。  
 $f$  は連続であるから、 $f(c) = 0$  なる  $a < c < b$  が存在することになる。このとき

$$\begin{aligned} \int_a^b \varphi(x)f(x) dx &= \int_a^b \varphi(x)f(x) dx - \varphi(c) \int_a^b f(x) dx \\ &= \int_a^b (\varphi(x) - \varphi(c))f(x) dx \\ &= \int_a^c (\varphi(x) - \varphi(c))f(x) dx + \int_c^b (\varphi(x) - \varphi(c))f(x) dx \\ &> 0 \end{aligned}$$

という評価ができる。

## ■ 平成 23 年度 数学 I

### 問 1

$V$  を  $\mathbb{C}$  上の有限次元ベクトル空間とし、 $f: V \rightarrow V$  を一次変換とする。 $W_1, W_2$  を  $V$  の部分空間で  $V = W_1 + W_2$ ,  $f(W_1) \subset W_1$ ,  $f(W_2) \subset W_2$  を満たすとする。 $f$  の  $W_1$  への制限を  $f|_{W_1}: W_1 \rightarrow W_1$  とおき、 $f$  の  $W_2$  への制限を  $f|_{W_2}: W_2 \rightarrow W_2$  とおく。

- (1)  $f|_{W_1}$  の最小多項式を  $P_1(x)$ ,  $f|_{W_2}$  の最小多項式を  $P_2(x)$  とおく。 $f$  の最小多項式は  $P_1(x), P_2(x)$  の最小公倍元であることを示せ。
- (2)  $f|_{W_1}, f|_{W_2}$  が対角化可能であるとき、 $f$  も対角化可能であることを示せ。

ただし、 $P(x), Q(x) \in \mathbb{C}[x]$  に対し、 $P(x)$  が  $Q(x)$  で割り切れるとき、 $P(x)$  は  $Q(x)$  の倍元であるという。また  $P(x), Q(x)$  の最小公倍元とは  $P(x), Q(x)$  の倍元のうち次数が最小のモノニック多項式のことをいう。

解答.

- (1)  $f$  の最小多項式を  $P \in \mathbb{C}[x]$  とする。 $P(f): V \rightarrow V$  は零写像なので、とくに  $W_i$  上でも零。よって  $P$  は  $P_1$  でも  $P_2$  でも割り切れる。逆にある  $Q \in \mathbb{C}[x]$  があって  $Q$  が  $P_1, P_2$  の倍元だとすると  $Q(f): V \rightarrow V$  は零。よって  $Q$  は  $P$  で割り切れる。以上により  $P$  は  $P_1, P_2$  の最小公倍元である。
- (2)  $f|_{W_1}, f|_{W_2}$  が対角化可能なら、 $P_1$  と  $P_2$  は重根を持たない。よって (1) より  $P$  も重根を持たない。ゆえに  $f$  は対角化可能。

## 問 2

区間  $[0, 1]$  上の実数値連続関数  $f(x)$  は  $f(0) = 0, f(1) = 1$  をみたしている。このとき、極限值

$$\lim_{n \rightarrow \infty} n \int_0^1 f(x) x^{2n} dx$$

を求めよ。

注意.  $f(0) = 0$  という仮定は不要である。

解答.  $\varepsilon > 0$  が任意に与えられたとする。  $f$  は連続なので

$$|1 - x| < \delta \rightarrow |1 - f(x)| < \varepsilon$$

なる  $\delta > 0$  が存在する。したがって

$$\begin{aligned} \left| n \int_0^1 f(x) x^{2n} dx - n \int_0^1 x^{2n} dx \right| &\leq n \int_0^1 |f(x) - 1| x^{2n} dx \\ &\leq n \int_{1-\delta}^1 |f(x) - 1| x^{2n} dx + n \int_0^{1-\delta} |f(x) - 1| x^{2n} dx \\ &\leq n\varepsilon \int_{1-\delta}^1 x^{2n} dx + n(1-\delta)^{2n} \int_0^{1-\delta} |f(x) - 1| dx \\ &\leq \frac{n(1 - (1-\delta)^{2n+1})}{2n+1} \varepsilon + n(1-\delta)^{2n} \int_0^{1-\delta} |f(x) - 1| dx \end{aligned}$$

という評価ができる。  $n \rightarrow \infty$  としたとき  $(1-\delta)^n \rightarrow 0$  なので

$$\limsup_{n \rightarrow \infty} \left| n \int_0^1 f(x) x^{2n} dx - n \int_0^1 x^{2n} dx \right| \leq \varepsilon/2$$

であることがわかる。  $\varepsilon > 0$  は任意だったから

$$\lim_{n \rightarrow \infty} n \int_0^1 f(x) x^{2n} dx = \lim_{n \rightarrow \infty} n \int_0^1 x^{2n} dx = \frac{1}{2}$$

であることがいえた。

コメント. Lebesgue の収束定理を用いた別解がある。多項式近似定理により、連続関数  $f$  は  $[0, 1]$  上  $C^\infty$  級関数で一様近似できる。  $n \int_0^1 x^{2n} dx$  は定数で抑えられるので、  $f \in C^1[0, 1]$  として良い。そうすると部分積分が使えて

$$n \int_0^1 f(x) x^{2n} dx = \frac{n}{2n+1} - \int_0^1 f'(x) \left( \frac{nx^{2n+1}}{2n+1} \right) dx$$

である。ここで  $[0, 1]$  上では  $n$  によらず一様に

$$\left| f'(x) \left( \frac{nx^{2n+1}}{2n+1} \right) \right| \leq |f'(x)|$$

であって  $f'$  は可積分関数なので、Lebesgue の収束定理により

$$\lim_{n \rightarrow \infty} \int_0^1 f'(x) \left( \frac{nx^{2n+1}}{2n+1} \right) dx = 0$$

であることが言える。よって求める積分の値は  $1/2$  である。

### 問 3

$L$  を階数 2 の自由アーベル群  $\mathbb{Z}^2$  の部分群で  $(a, b), (c, d) \in \mathbb{Z}^2$  により生成されるものとする。このとき、以下の間に答えよ。

- (1) 商群  $\mathbb{Z}^2/L$  の位数が有限になるための必要十分条件を  $a, b, c, d$  を用いて表せ。
- (2)  $abcd \neq 0$  をみたし、かつ  $\mathbb{Z}^2/L$  の位数が有限となるもののうちから、
  - (i)  $\mathbb{Z}^2/L = \{0\}$  となる例
  - (ii)  $\mathbb{Z}^2/L$  が非自明な巡回群になる例
  - (iii)  $\mathbb{Z}^2/L$  が巡回群にならない例
 を各々 1 つずつ与えよ。

解答.

- (1)  $A \in M_2(\mathbb{Z})$  を

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

により定めると、 $L$  は  $A$  の像  $A(\mathbb{Z}^2)$  と一致することに注意する。有限生成 Abel 群の基本定理により  $\#(\mathbb{Z}^2/L) < \infty$  と  $\mathbb{Z}^2/L$  が位数  $\infty$  の元を持たないことは同値である。よって、 $\mathbb{Z}^2/L$  のすべての元の位数が有限になるための条件を求めれば十分である。

さて  $\mathbb{Z}^2/L$  のすべての元の位数が有限と仮定しよう。このとき任意に与えられた  $p \in \mathbb{Z}^2$  の  $\mathbb{Z}^2/L$  における像の位数は有限であり、よって  $np \in L$  なる 0 でない整数  $n$  がある。ゆえに  $np \in A(\mathbb{Z}^2)$  であるから、とくに  $p \in A(\mathbb{Q}^2)$  である。 $p \in \mathbb{Z}^2$  は任意にとっていたから、 $\mathbb{Z}^2 \subset A(\mathbb{Q}^2)$  ということだが、 $\mathbb{Q}^2$  の元は適当に 0 でない整数を乗ずれば  $\mathbb{Z}^2$  の元にすることができるので  $\mathbb{Q}^2 = A(\mathbb{Q}^2)$  である。つまり  $A \in GL_2(\mathbb{Q})$  であるから、 $ad - bc \neq 0$  ということになる。

逆に  $ad - bc \neq 0$  とする。任意に  $p \in \mathbb{Z}^2$  が与えられたとしよう。 $A \in GL_2(\mathbb{Q})$  なので、 $p = Ax$  なる  $x \in \mathbb{Q}^2$  が存在する。 $mx \in \mathbb{Z}^2$  なる 0 でない整数  $m$  をとると、 $mp = A(mx) \in L$  なので  $p$  の  $\mathbb{Z}^2/L$  における像の位数は有限であることがわかる。よって任意の  $\mathbb{Z}^2/L$  の元の位数は有限となることが従う。以上により、求める必要十分条件は  $ad - bc \neq 0$  である。

- (2) (i)  $A \in GL_2(\mathbb{Z})$  であって、どの成分も 0 でなければなんでもいい。たとえば

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

など。

- (ii) たとえば

$$A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

とおくと  $L = \{(x, y)^T \mid x - y \in 2\mathbb{Z}\}$  である。よって  $\mathbb{Z}^2/L$  の各元は 0 か  $(1, 0)^T$  で代表されるので  $\#(\mathbb{Z}^2/L) = 2$  であり、 $\mathbb{Z}^2/L \cong \mathbb{Z}/2\mathbb{Z}$  であるということになる。

- (iii) たとえば (i) で与えた行列の各成分を 2 倍して

$$A = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}$$

とすれば

$$L = \begin{pmatrix} 2 \\ 0 \end{pmatrix} \mathbb{Z} \oplus \begin{pmatrix} 0 \\ 2 \end{pmatrix} \mathbb{Z}$$

なので  $\mathbb{Z}^2/L \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  であることが判る。

#### 問 4

$n$  を 2 以上の自然数とする。

- (1)  $n$  次元実射影空間  $\mathbb{R}P^n$  の基本群  $\pi_1(\mathbb{R}P^n)$  を計算せよ。ただし、 $n$  次元単位球面  $S^n$  が単連結であることを用いてよい。
- (2)  $\mathbb{R}P^n$  から単位円  $S^1$  への連続写像は、常に定値写像とホモトピックであることを示せ。

解答.

- (1) 普遍被覆  $p: S^n \rightarrow \mathbb{R}P^n$  をとる。このとき  $\pi_1(\mathbb{R}P^n)$  は deck 変換群

$$D_n := \{f: S^n \rightarrow S^n \mid f \text{ は } p \circ f = p \text{ なる連続写像}\}$$

と同型であることが知られている。

そして  $S^n$  の連結性から、 $D_n \cong \mathbb{Z}/2\mathbb{Z}$  である。なぜならば!  $f \in D_n$  が与えられたとしよう。任意の  $x \in S^n$  に対して  $f(x) \in \{x, -x\}$  なので

$$\begin{aligned} V_1 &= \{x \in S^n \mid f(x) = x\} \\ V_2 &= \{x \in S^n \mid f(x) = -x\} \end{aligned}$$

とおくと  $S^n = V_1 \cup V_2$  である。さらに  $V_1, V_2$  は  $f$  の連続性から閉集合であってなおかつ  $V_1 \cap V_2 = \emptyset$  であるので、 $S^n$  の連結性より  $V_1$  と  $V_2$  のどちらかが  $S^n$  全体と一致しなくてはならない。ゆえにかくのごとし。したがって  $\pi_1(\mathbb{R}P^n) \cong \mathbb{Z}/2\mathbb{Z}$  であることが言えた。

- (2)  $f: \mathbb{R}P^n \rightarrow S^1$  が与えられたとする。 $f_*: \pi_1(\mathbb{R}P^n) \rightarrow \pi_1(S^1)$  は  $\pi_1(\mathbb{R}P^n) \cong \mathbb{Z}/2\mathbb{Z}$  と  $\pi_1(S^1) \cong \mathbb{Z}$  より零写像なので、次の図式

$$\begin{array}{ccc} & & \mathbb{R} \\ & \nearrow g & \downarrow \pi \\ \mathbb{R}P^n & \xrightarrow{f} & S^1 \end{array}$$

を可換にするようなリフト  $g$  がある。ただし  $\pi: \mathbb{R} \rightarrow S^1$  は普遍被覆である。よってホモトピー  $H: \mathbb{R}P^n \times [0, 1] \rightarrow S^1$  を

$$H(x, t) = \pi(tg(x))$$

として定めることができ、 $f$  が定値写像とホモトピックであることが判る。



問 5

函数

$$f(z) = \frac{e^{(1+i)z}}{(e^z + 1)^2} \quad (z \in \mathbb{C})$$

に関する以下の問に答えよ。

- (1)  $L > 0$  とし、複素平面上の 4 点  $L, L + 2\pi i, -L + 2\pi i, -L$  を頂点とする長方形の内部にある  $f(z) dz$  の極と留数を求めよ。
- (2) 広義積分  $\int_{-\infty}^{\infty} f(x) dx$  を計算せよ。

解答.

- (1) 与えられた長方形の内部に極があるとすれば、それは  $z = i\pi$  であることはすぐにわかる。位数と留数を求めよう。

$$e^z + 1 = - \sum_{k=1}^{\infty} \frac{(z - i\pi)^k}{k!}$$

であることから、

$$g(z) := \frac{e^z + 1}{z - i\pi} = - \sum_{k=1}^{\infty} \frac{(z - i\pi)^{k-1}}{k!}$$

と計算できる。よって  $g$  は  $\mathbb{C}$  上正則であって  $g(i\pi) = -1$  である。 $g$  を使うと  $f$  は

$$f(z) = \frac{1}{(z - i\pi)^2} \frac{e^{(1+i)z}}{g(z)^2}$$

と表せる。 $h(z) = e^{(1+i)z} g(z)^{-2}$  とおく。 $h$  は正則で  $h(i\pi) = -e^{-\pi}$  なので、 $f$  が  $z = i\pi$  に持つ極の位数は 2 である。

留数は  $\text{Res}(f, i\pi) = h'(i\pi)$  から求めることができる。計算すると

$$h'(z) = \frac{e^{(1+i)z}((1+i)g(z) - 2g'(z))}{g(z)^3}$$

$$g'(z) = - \sum_{k=2}^{\infty} \frac{(k-1)}{k!} (z - i\pi)^{k-2}$$

だから  $\text{Res}(f, i\pi) = h'(i\pi) = -ie^{-\pi}$  である。

- (2) 与えられた長方形と実軸の共有部分を  $L_1$  とし、残り 3 つの辺を正の向きに回る順に  $L_2, L_3, L_4$  とする。つまるところ  $L_1$  は  $-L$  から  $L$  を、 $L_2$  は  $L$  から  $L + 2\pi i$  を、 $L_3$  は  $L + 2\pi i$  から  $-L + 2\pi i$  を、 $L_4$  は  $-L + 2\pi i$  から  $-L$  をそれぞれつなぐ線分とする。留数定理により、すべての  $L > 0$  に対して

$$\int_{L_1 \cup \dots \cup L_4} f(z) dz = 2\pi i \text{Res}(f, i\pi) = 2\pi e^{-\pi}$$

が成り立つ。このとき

$$\int_{L_3} f(z) dz = -e^{-2\pi} \int_{L_1} f(z) dz$$

であることに注意する。また  $L \rightarrow \infty$  のとき

$$\left| \int_{L_2} f(z) dz \right| \leq \frac{2\pi e^L}{(e^L - 1)^2}$$
$$\left| \int_{L_4} f(z) dz \right| \leq \frac{2\pi e^{-L}}{(1 - e^{-L})^2}$$

という評価ができるので  $L_2, L_4$  上の積分はゼロに収束する。ゆえに留数定理の式より

$$\int_{-\infty}^{\infty} f(x) dx = \frac{2\pi e^{\pi}}{e^{2\pi} - 1}$$

であることがわかる。

## 平成 23 年度 数学 II

### 問 1

$p \geq 3$  を奇素数、 $\mathbb{F}_p$  を  $p$  個の元からなる有限体とする。 $\mathbb{F}_p$  の元を成分とする正則な 2 次元正方行列全体のなす群を  $GL_2(\mathbb{F}_p)$  とおく。

- (1)  $GL_2(\mathbb{F}_p)$  の元で固有値がすべて 1 となるものの個数を求めよ。
- (2)  $GL_2(\mathbb{F}_p)$  の半単純でない元の個数を求めよ。ただし、 $A \in GL_2(\mathbb{F}_p)$  が半単純とは、 $\mathbb{F}_p$  の代数的閉包  $\overline{\mathbb{F}_p}$  の元を成分とする正則な 2 次正方行列  $P$  が存在して  $P^{-1}AP$  が対角行列となることである。

解答. 以下  $G := GL_2(\mathbb{F}_p)$  とおく。単位行列は  $E$  で表す。

- (1) 平成 28 年度専門科目問 3(ii) で「最小多項式が同じならば共役」ということを示した。その証明と同様にして、固有値がすべて 1 であるような  $G$  の元は  $E$  または 2 次の Jordan 細胞

$$\Lambda = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

と共役であることが言える。そこで、 $E$  と  $\Lambda$  の共役類の位数を求めればよい。 $E$  の共役類はあきらかに  $\{E\}$  だから気にしなくてよい。問題は  $\Lambda$  である。

$G$  の  $G$  自身への共役による作用を考える。すると求めるべき値は  $1 + \# \text{Orbit}(\Lambda)$  と表される。

$$\# \text{Orbit}(\Lambda) = \#G / \# \text{Stab}(\Lambda)$$

であることと  $\#G = p(p-1)^2(p+1)$  であることより、 $\# \text{Stab}(\Lambda)$  が判ればよい。

計算すると

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

と表されている元  $A \in G$  に対して

$$A\Lambda - \Lambda A = \begin{pmatrix} -c & a-d \\ 0 & c \end{pmatrix}$$

だから

$$\text{Stab}(\Lambda) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{F}_p, a \neq 0 \right\}$$

と求まる。よって  $\# \text{Stab}(\Lambda) = p(p-1)$  なので  $\# \text{Orbit}(\Lambda) = p^2 - 1$  であって、求める「固有値がすべて 1 の  $G$  の元の個数」は  $1 + (p^2 - 1) = p^2$  である。

- (2)  $L := GL_2(\overline{\mathbb{F}_p})$  とおく。代数閉体上であれば Jordan 標準形が存在することを利用すると、半単純でない  $G$  の元全体とは、

$$X := \{A \in G \mid \text{ある } P \in L \text{ が存在して } P^{-1}AP \text{ が 2 次の Jordan 細胞に等しい}\}$$

であることが言える。このとき  $A \in X$  の固有値は  $\mathbb{F}_p$  の元である。なぜならば！  $\beta \in \overline{\mathbb{F}_p}$  に対して

$$\Lambda_\beta = \begin{pmatrix} \beta & 1 \\ 0 & \beta \end{pmatrix}$$

とおこう。 $A \in X$  とし、 $P^{-1}AP = \Lambda_\beta$  なる  $\beta \in \overline{\mathbb{F}_p}$  と  $P \in L$  をとる。特性多項式を考えると、これは  $L$  上で共役をとっても変化しないので  $\Phi_A(t) = (t - \beta)^2 \in \mathbb{F}_p[t]$  である。よって  $2\beta \in \mathbb{F}_p$  ということになるが、 $p$  は奇素数と仮定していたのだった。ゆえにかくのごとし。

ということは実は  $\Lambda_\beta \in G$  だったのである。すると次に気になるのは 2 つの  $G$  の元が  $L$  上で共役ならば  $G$  上でも共役だろうか？ということだが、これはすでに平成 28 年度専門科目問 3(ii) の証明で肯定的に解決済みであった。すなわち  $X$  の元とは  $G$  において 2 次の Jordan 細胞と共役なもの全体である。つまり

$$\#X = \sum_{\beta \in \mathbb{F}_p^\times} \# \text{Orbit}(\Lambda_\beta)$$

と計算できることになる。(1) と同様に  $\# \text{Orbit}(\Lambda_\beta) = p^2 - 1$  なので、

$$\#X = (p - 1)^2(p + 1)$$

である。

## 問 2

複素数体の部分体  $K$  を  $K = \mathbb{Q}(i\sqrt{17+4\sqrt{17}})$  によって定める。

- (1)  $K$  は  $\mathbb{Q}$  の 4 次の Galois 拡大であることを示せ。
- (2)  $K$  の  $\mathbb{Q}$  上の Galois 群  $\text{Gal}(K/\mathbb{Q})$  を求めよ。

解答.

- (1)  $\alpha = i\sqrt{17+4\sqrt{17}}$  とおく。計算すると  $\alpha$  は  $f(X) = X^4 + 34X^2 + 17 \in \mathbb{Z}[X]$  の根である。 $f$  は  $p = 17$  に関する Eisenstein 多項式だから  $\mathbb{Q}[X]$  の元として既約で、よって  $[K : \mathbb{Q}] = 4$  である。

$$f(X) = (X^2 + 17 - 4\sqrt{17})(X^2 + 17 + 4\sqrt{17})$$

より  $\alpha$  の  $\mathbb{Q}$  上の共役は  $\beta := i\sqrt{17-4\sqrt{17}}$  とおいたとき  $\{\pm\alpha, \pm\beta\}$  である。ゆえに  $K$  の  $\mathbb{Q}$  上の Galois 閉包を  $\tilde{K}$  とすると  $\tilde{K} = \mathbb{Q}(\alpha, \beta) = K(\sqrt{17})$  である。ここで

$$\sqrt{17} = -\frac{\alpha^2 + 17}{4}$$

だから  $\sqrt{17} \in K$  であって、ゆえに  $K = \tilde{K}$  と結論できる。つまり  $K/\mathbb{Q}$  は Galois 拡大である。

- (2)  $G := \text{Gal}(K/\mathbb{Q})$  とおく。 $K$  は既約多項式  $f$  の最小分解体なので  $G$  は根の集合  $\{\pm\alpha, \pm\beta\}$  に推移的に作用する。

$$\gamma_1 = \alpha, \quad \gamma_2 = -\alpha, \quad \gamma_3 = \beta, \quad \gamma_4 = -\beta$$

と添え字付けることにより  $G \subset \mathfrak{S}_4$  とみなす。

$K$  は実数でない元を含むので、 $G$  の元の中には複素共役がある。 $\tau \in G$  を複素共役とすると、この同一視により  $\tau = (12)(34)$  である。また推移性により  $\sigma(\alpha) = \beta$  なる  $\sigma \in G$  の存在がわかる。このとき

$$\sigma(\sqrt{17}) = \sigma\left(-\frac{\alpha^2 + 17}{4}\right) = -\frac{\beta^2 + 17}{4} = -\sqrt{17}$$

であることから

$$-\alpha\beta = \sqrt{17} = -\sigma(\sqrt{17}) = \sigma(\alpha\beta) = \beta\sigma(\beta)$$

より  $\sigma(\beta) = -\alpha$  であり、 $\sigma = (1324)$  である。とくに  $\sigma \in G$  は位数 4 の元なので  $G$  は巡回群であって  $G \cong \mathbb{Z}/4\mathbb{Z}$  であることが結論される。

## ■ 平成 22 年度 基礎数学

---

### 問 1

実正方行列  $A, B$  を次のように定める。

$$A = \begin{pmatrix} 3 & 2 & -1 & -1 \\ 6 & 3 & 4 & 1 \\ 5 & 1 & 5 & 1 \\ 1 & -1 & 3 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 2 & -1 & -1 & 3 \\ -1 & 2 & 3 & 3 \\ -1 & 2 & 1 & -2 \end{pmatrix}$$

$A$  の行列式  $|A|$  と  $B$  の逆行列  $B^{-1}$  を求めよ。

解答. 計算すると  $|A| = 6$  であることがわかる。 $B^{-1}$  は

$$B^{-1} = \begin{pmatrix} -13 & 5 & -2 & -2 \\ 7 & -2 & 1 & 2 \\ -15 & 5 & -2 & -3 \\ 6 & -2 & 1 & 1 \end{pmatrix}$$

と求まる。計算過程など頭脳明晰な読者諸賢には必要ないだろう。

## 問 2

$n$  行  $m$  列の実行列  $A$  の階数が  $m$  であるとする。このとき、 $m$  行  $l$  列の実行列  $B, C$  が

$$AB = BC$$

を満たせば

$$B = C$$

であることを示せ。

解答.  $\text{rank } A = m$  ということは  $n \geq m$  かつ  $A$  は単射でなくてはならない。一方で  $A(B - C) = 0$  より  $\mathbb{R}^l$  の標準基底  $\{e_i\}$  をとると、すべての  $i$  について  $A(B - C)e_i = 0$  である。 $A$  は単射なので  $(B - C)e_i = 0$  が従う。 $i$  は任意だったから  $B = C$  である。

### 問 3

次の重積分を求めよ。

$$\iint_D \frac{dxdy}{1+(x+y)^4}$$

ただし  $D = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0, y \geq 0, x + y \leq 1\}$  とする。

解答.  $s = x, t = x + y$  と変数変換する。  $dt ds = dxdy$  である。積分領域  $D$  は

$$E = \{(s, t) \in \mathbb{R}^2 \mid 0 \leq t \leq 1, 0 \leq s \leq t\}$$

に対応する。これで計算すると

$$\begin{aligned} \iint_D \frac{dxdy}{1+(x+y)^4} &= \int_0^1 dt \int_0^t \frac{ds}{1+t^4} \\ &= \int_0^1 \frac{t}{1+t^4} dt \\ &= \frac{1}{2} \int_0^1 \frac{dt}{1+t^2} \\ &= \frac{1}{2} \int_0^{\pi/4} d\theta \\ &= \frac{\pi}{8} \end{aligned}$$

がわかる。



問 4

- (1) ある定数  $C$  が存在し、 $-1 \leq x \leq 1$  のとき

$$|e^x - 1 - x| \leq Cx^2$$

となることを示せ。

- (2) 級数

$$\sum_{n=1}^{\infty} \left( e^{x/n} - 1 - \frac{x}{n} \right)$$

は  $x$  が  $[-1, 1]$  を動くとき一様収束することを示せ。

解答.

- (1)  $e^x$  の  $x = 0$  の周りでの Taylor 展開を考えると

$$\lim_{x \rightarrow 0} \frac{e^x - 1 - x}{x^2} = \frac{1}{2}$$

である。よって  $h(x) = (e^x - 1 - x)/x^2$  は  $[-1, 1]$  上の連続関数である。よってとくに有界であり  $C = \max_{x \in [-1, 1]} |h(x)|$  が存在する。この  $C$  が与えられた条件を満たす。

- (2) (1) を使うと

$$\begin{aligned} \sum_{n=1}^{\infty} \left( e^{x/n} - 1 - \frac{x}{n} \right) &\leq C \sum_{n=1}^{\infty} \left( \frac{|x|}{n} \right)^2 \\ &\leq C \sum_{n=1}^{\infty} \frac{1}{n^2} \end{aligned}$$

であることが判る。よって一様収束する。

## ■ 平成 22 年度 数学 I

### 問 1

$A^5 = 2E_n$  を満たす  $n$  次正方行列で成分がすべて有理数のものが存在するための、 $n$  に関する必要十分条件を求めよ。(ただし、 $E_n$  は  $n$  次単位行列である)

解答.  $A^5 = 2E_n$  なる  $A \in M_n(\mathbb{Q})$  が存在したとする。このとき  $(\det A)^5 = 2^n$  より  $\det A \in \mathbb{Q}$  は  $\mathbb{Z}$  上整である。よって  $\mathbb{Z}$  が整閉であることから  $\det A \in \mathbb{Z}$  であり、 $n$  は 5 の倍数である。

逆に  $n$  が 5 の倍数だと仮定する。 $A^5 = 2E_n$  となるような  $A$  を構成したいが、ブロック分けすることにより  $n = 5$  の場合に帰着できる。だから  $n = 5$  としよう。固有多項式を  $\Phi$  で表すことにする。このとき  $A^5 = 2E_5$  であることと  $\Phi_A(t) = t^5 - 2$  であることは同値である。なぜならば!  $\Phi_A(t) = t^5 - 2$  ならば Cay-Hamilton の定理より  $A^5 = 2E_5$  であることが直ちにわかる。逆に  $A^5 = 2E_5$  とする。このとき  $A$  の  $\mathbb{Q}$  上の最小多項式は  $t^5 - 2$  を割り切るはずだが、 $t^5 - 2 \in \mathbb{Q}[t]$  は既約多項式なので、 $t^5 - 2$  が最小多項式である。ゆえに再び Cay-Hamilton の定理より  $t^5 - 2$  は  $\Phi_A(t)$  を割り切ることがわかるが、どちらも 5 次モニック多項式なので両者は一致していなくてはならない。よって  $\Phi_A(t) = t^5 - 2$  が従う。ゆえにかくのごとし。そこで  $\Phi_A(t) = t^5 - 2$  となるような  $A$  を構成すればいいことになるが、それは

$$t^5 - 2 = \det \begin{pmatrix} t & -1 & 0 & 0 & 0 \\ 0 & t & -1 & 0 & 0 \\ 0 & 0 & t & -1 & 0 \\ 0 & 0 & 0 & t & -1 \\ -2 & 0 & 0 & 0 & t \end{pmatrix}$$

なので

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 0 \end{pmatrix}$$

とおけば  $\Phi_A(t) = t^5 - 2$  となる。以上により求める必要十分条件は、 $n$  が 5 の倍数であることである。

問 2

$f$  を、点  $0$  を含む開区間で  $C^1$  級の函数とすると、極限

$$\lim_{h \rightarrow +0} \frac{1}{h^2} \left\{ \int_0^h f(x) \, dx - hf(0) \right\}$$

を求めよ。

問 3

|(  $(\mathbb{Z}/525\mathbb{Z})^\times$  の元で位数が 4 であるものの個数を求めよ。ただし  $(\mathbb{Z}/525\mathbb{Z})^\times$  は可換環  $\mathbb{Z}/525\mathbb{Z}$  の可逆な元全体の作る群である。)

問 4

$X$  を位相空間、 $e \in X$  とし

$$\Omega = \{\alpha: [0, 1] \rightarrow X \mid \alpha \text{ は連続写像、} \alpha(0) = \alpha(1) = e\}$$

とする。 $\Omega$  の同値関係  $\simeq$  を次で定義する。

$\alpha, \beta \in \Omega$  に対して、連続写像  $F: [0, 1] \times [0, 1] \rightarrow X$  で

$$F(t, 0) = \alpha(t) \quad (0 \leq t \leq 1)$$

$$F(t, 1) = \beta(t) \quad (0 \leq t \leq 1)$$

$$F(0, s) = F(1, s) = e \quad (0 \leq s \leq 1)$$

を満たすものが存在するとき、 $\alpha \simeq \beta$  と定める。また、位相空間  $X$  は

$$\mu(x, e) = \mu(e, x) = x \quad (x \in X)$$

を満たす連続写像  $\mu: X \rightarrow X \rightarrow X$  をもつものとする。 $\alpha, \beta \in \Omega$  に対して  $\Omega$  の元  $\alpha * \beta$  と  $\alpha \# \beta$  を次で定義する。

$$(\alpha * \beta)(t) = \begin{cases} \alpha(2t) & (0 \leq t \leq 1/2) \\ \beta(2t - 1) & (1/2 \leq t \leq 1) \end{cases}$$

$$(\alpha \# \beta)(t) = \mu(\alpha(t), \beta(t)) \quad (0 \leq t \leq 1)$$

このとき、次の命題 (1), (2), (3) を示せ。

- (1)  $\alpha, \beta, \alpha', \beta' \in \Omega$  に対して  $\alpha \simeq \beta, \alpha' \simeq \beta'$  ならば  $\alpha \# \alpha' \simeq \beta \# \beta'$  である。
- (2)  $\alpha, \beta \in \Omega$  に対して  $\alpha \# \beta \simeq \alpha * \beta$  である。
- (3)  $\alpha, \beta \in \Omega$  に対して  $\alpha \# \beta \simeq \beta * \alpha$  である。

問 5

次の積分を求めよ。

$$\int_{-\infty}^{\infty} \frac{e^{ix} - 1}{x(x^2 + 1)} dx$$

## Appendix 1. 半直積と Galois 群

平成 30 年度の院試専門科目の問 3 を解いているときに補題として準備したものです。

有限次 Galois 拡大の合成であるような体拡大があるとき、その Galois 群が直積で表されるという定理がありました。この仮定を少し緩めても、直積を半直積に代えて同様のことが成り立つというのがここでの主張です。半直積の形のままで積がどうなっているかがやや判りにくく、元の位数や共役類を調べるのに不都合ですが、幸いにして有限巡回拡大の合成であるような場合なら Galois 群の表示が容易にわかります。ついでに、半直積についてまとめた事実を紹介している文献がなかなか見つからなかったので主要と思われるものを簡単にまとめておきました。

結果的にこの補題を使っても件の院試の問題はそんなに楽にはならなくてガッカリしましたが、半直積が自然に出てくる状況をひとつ見つけられたことは嬉しいです。

**命題.** (直積の特徴づけ)

群  $G$  とその部分群  $N, H$  があるとする。このとき次は同値。

- (1)  $G$  と直積  $N \times H$  は自然に同型である。つまり積をとる写像  $\varphi: N \times H \rightarrow G$  は群の準同型であつて、かつ同型になる。次の図式

$$\begin{array}{ccc} & N \times H & \\ \nearrow & \downarrow \varphi & \nwarrow \\ N & \longrightarrow G \longleftarrow & H \end{array}$$

を可換にするような同型  $\varphi$  があるといってもよい。

- (2)  $N \triangleleft G$  かつ  $H \triangleleft G$  であり、かつ  $N \cap H = 1$  で  $NH = G$  である。

**証明.**

- (1)  $\Rightarrow$  (2)  $q \in N, g \in G$  が与えられたとする。 $(n \in N$  としないのは、 $n$  と  $h$  の形が似ていて間違えやすいため)  $\varphi$  の逆写像  $\psi$  をとっておく。すると、 $\psi(g) = (g_N, g_H)$  と表せる。ゆえに

$$\begin{aligned} \psi(gqg^{-1}) &= \psi(g)(q, 1)\psi(g)^{-1} \\ &= (g_N, g_H)(q, 1)(g_N^{-1}, g_H^{-1}) \\ &= (g_N q g_N^{-1}, 1) \end{aligned}$$

である。したがって  $gqg^{-1} = \varphi(g_N q g_N^{-1}, 1) \in N$  であるから、 $N \triangleleft G$  である。同様にして  $H \triangleleft G$  もいえる。また、 $x \in N \cap H$  とすると、 $\psi(x) \in N \times H$  は  $(1, 1)$  でなくてはならない。したがって、 $x \in \text{Ker } \psi$  である。 $\psi$  は同型だから  $x = 1$  であつて、 $N \cap H = 1$  がいえた。さらに、 $G = NH$  であることはあきらかであろう。

- (2)  $\Rightarrow$  (1)  $N, H$  は  $G$  の部分群なので、積をとる写像  $\varphi: N \times H \rightarrow G$  が定義できる。 $N \triangleleft G, H \triangleleft G$  なので交換子  $[N, H]$  は  $N \cap H$  の部分群であるが、 $N \cap H = 1$  なので  $[N, H] = 1$  である。よって  $N$  の元と  $H$  の元は可換であり、 $\varphi$  は群準同型になる。 $N \cap H = 1$  より  $\varphi$  は単射であり、 $NH = G$  より  $\varphi$  は全

射である。

□

**補題.** (半直積の基本的な性質)

群  $N, H$  と群作用  $\Phi: H \rightarrow \text{Aut } N$  があって、半直積  $N \rtimes_{\Phi} H$  を考えているとする。  $q \in N, h \in H$  とする。このとき次が成り立つ。

- (1) 作用成分への射影  $N \rtimes_{\Phi} H \rightarrow H$  s.t.  $(q, h) \mapsto h$  は準同型である。
- (2) 正規成分への入射  $N \rightarrow N \rtimes_{\Phi} H$  s.t.  $q \mapsto (q, 1)$  は準同型である。
- (3) 作用成分への入射  $H \rightarrow N \rtimes_{\Phi} H$  s.t.  $h \mapsto (1, h)$  は準同型である。
- (4)  $h \in \text{Ker } \Phi$  ならば  $(q, h) = (1, h)(q, 1)$  である。
- (5) 常に  $(q, h) = (q, 1)(1, h)$  が成り立つ。
- (6) 自然な入射と射影は、分裂する短完全列

$$\begin{array}{ccccccc} 1 & \longrightarrow & N & \longrightarrow & N \rtimes_{\Phi} H & \longrightarrow & H \longrightarrow 1 \\ & & & & \uparrow & \nearrow & \\ & & & & H & & \end{array}$$

(The arrow from  $H$  to  $N \rtimes_{\Phi} H$  is labeled 1)

をなす。

**証明.** あきらか。

□

**命題.** (半直積の特徴づけ)

群  $G$  の部分群  $N, H$  が与えられているとする。このとき次は同値。

- (1) ある群作用  $\Phi: H \rightarrow \text{Aut } N$  が存在して、  $G$  は半直積  $N \rtimes_{\Phi} H$  と自然に同型である。つまり積をとる写像  $\varphi: N \rtimes_{\Phi} H \rightarrow G$  s.t.  $(q, h) \mapsto qh$  は群準同型で、かつ同型である。次の図式

$$\begin{array}{ccccc} & & N \rtimes_{\Phi} H & & \\ & \nearrow & \downarrow \varphi & \nwarrow & \\ N & \longrightarrow & G & \longleftarrow & H \end{array}$$

を可換にするような同型  $\varphi$  があるといってもよい。

- (2)  $N \triangleleft G$  かつ  $NH = G$  かつ  $N \cap H = 1$  が成り立つ。

**証明.**

- (1) $\Rightarrow$ (2)  $NH = G$  はあきらか。  $x \in N \cap H$  とすると  $(x, x^{-1}) \in \text{Ker } \varphi$  だから  $x = 1$  でなくてはならない。よって  $N \cap H = 1$  である。  $N \triangleleft G$  を示そう。  $g \in G$  と  $q \in N$  が与えられたとする。  $p: N \rtimes_{\Phi} H \rightarrow H$



を射影とし、 $\psi$  を  $\varphi$  の逆写像とする。このとき  $\psi(g) = (g_N, g_H)$  と表せる。ゆえに

$$\begin{aligned} p \circ \psi(gqg^{-1}) &= p((g_N, g_H)(q, 1)(g_N^{-1}, g_H^{-1})) \\ &= 1 \end{aligned}$$

である。したがって  $gqg^{-1} \in \varphi(\text{Ker } p) = N$  である。よって  $N \triangleleft G$  がわかった。

(2) $\Rightarrow$ (1)  $N \triangleleft G$  より、群作用  $\Phi: H \rightarrow \text{Aut } N$  を  $\Phi_h(q) = hqh^{-1}$  により定めることができる。(順序を逆に  
して  $\Phi_h(q) = h^{-1}qh$  とするとうまくいかないことに注意) このとき  $q_1, q_2 \in N$  と  $h_1, h_2 \in H$  が与え  
られたとすれば

$$\begin{aligned} \varphi((q_1, h_1)(q_2, h_2)) &= \varphi(q_1 \Phi_{h_1}(q_2), h_1 h_2) \\ &= \varphi(q_1 h_1 q_2 h_1^{-1}, h_1 h_2) \\ &= q_1 h_1 q_2 h_2 \\ &= \varphi(q_1, h_1) \varphi(q_2, h_2) \end{aligned}$$

だから  $\varphi$  は群準同型になる。 $\varphi$  が単射であることは  $N \cap H = 1$  より従い、全射であることは  $NH = G$  より従う。

□

**命題.** (半直積の関手性 その 1)

$N_1, N_2, H$  が群で群作用  $\Phi: H \rightarrow \text{Aut } N_1$  が与えられていたとする。このとき同型  $g: N_1 \rightarrow N_2$  に対して  ${}_g\Phi: H \rightarrow \text{Aut } N_2$  を  ${}_g\Phi(h) = g \circ \Phi_h \circ g^{-1}$  で定めると、写像  $g_*: N_1 \rtimes_{\Phi} H \rightarrow N_2 \rtimes_{{}_g\Phi} H$  s.t.  $g_*(q, h) = (g(q), h)$  は群の準同型である。

**証明.** 計算すればわかる。実際に行ってみると

$$\begin{aligned} g_*((q, h_1)(q', h_2)) &= g_*(q \Phi_{h_1}(q'), h_1 h_2) \\ &= (g(q)g(\Phi_{h_1}(q')), h_1 h_2) \\ (g(q), h_1)(g(q'), h_2) &= (g(q)g(\Phi_{h_1}(q')), h_1 h_2) \\ &= (g(q)g(\Phi_{h_1}(q')), h_1 h_2) \end{aligned}$$

であるから一致する。

□

**命題.** (半直積の関手性 その 2)

$N, H_1, H_2$  が群で群作用  $\Phi: H_2 \rightarrow \text{Aut } N$  が与えられていたとする。このとき群準同型  $f: H_1 \rightarrow H_2$  に対して  $\Phi_f: H_1 \rightarrow \text{Aut } N$  を  $(\Phi_f)_h = \Phi_{f(h)}$  により定める。そうすると写像  $f_*: N \rtimes_{\Phi_f} H_1 \rightarrow N \rtimes_{\Phi} H_2$  s.t.  $f_*(q, h) = (q, f(h))$  は群の準同型である。

証明. 計算すればわかる。実際に行ってみると

$$\begin{aligned} f_*((q_1, h)(q_2, h')) &= f_*(q_1 \Phi_{f(h)}(q_2), hh') \\ &= (q_1 \Phi_{f(h)}(q_2), f(h)f(h')) \\ &= f_*(q_1, h)f_*(q_2, h') \end{aligned}$$

であるから一致。 □

**命題.** (分裂する完全列からの半直積の構成)

群  $G, H, N$  と準同型  $i, j, p$  からなる分裂する短完全列

$$\begin{array}{ccccccc} 1 & \longrightarrow & N & \xrightarrow{j} & G & \xrightarrow{p} & H \longrightarrow 1 \\ & & & & \uparrow i & \nearrow 1 & \\ & & & & H & & \end{array}$$

が与えられたとする。このとき、ある群作用  $\Psi: H \rightarrow \text{Aut } N$  が存在して、自然な同型  $G \cong N \rtimes_{\Psi} H$  がある。すなわち、ある同型  $\psi$  が存在して次の図式

$$\begin{array}{ccccc} & & N \rtimes_{\Psi} H & & \\ & \nearrow & \downarrow \psi & \nwarrow & \\ N & \xrightarrow{j} & G & \xleftarrow{i} & H \end{array}$$

が可換になる。

証明.  $N' = j(N)$ ,  $H' = i(H)$  とおく。このとき  $N' = \text{Ker } p$  より  $N' \triangleleft G$  である。 $x \in N' \cap H'$  とすると  $x = j(q) = i(h)$  なる  $q \in N, h \in H$  があるが、 $p(x) = 1 = h$  より  $x = 1$  でなくてはならない。よって  $N' \cap H' = 1$  である。また  $g \in G$  とすると  $g(i \circ p)(g^{-1}) \in \text{Ker } p$  なので  $g(i \circ p)(g^{-1}) = j(q)$  なる  $q \in N$  がある。したがって  $g = j(q)(i \circ p)(g) \in N'H'$  だから  $G = N'H'$  が成り立つ。よって、ある同型  $\varphi$  と群作用  $\Phi: H' \rightarrow \text{Aut } N'$  であって、次の図式

$$\begin{array}{ccccc} & & N' \rtimes_{\Phi} H' & & \\ & \nearrow & \downarrow \varphi & \nwarrow & \\ N' & \longrightarrow & G & \longleftarrow & H' \end{array}$$

を可換にするようなものがある。ここで  $i, j$  は単射であるので、同型  $I: H \rightarrow H'$  と  $K: N' \rightarrow N$  が存在し

て、次の図式

$$\begin{array}{ccccc}
N & \longrightarrow & N \rtimes_{K\Phi_I} H & \longleftarrow & H \\
\downarrow K^{-1} & & \downarrow K_*^{-1} & & \parallel \\
N' & \longrightarrow & N' \rtimes_{\Phi_I} H & \longleftarrow & H \\
\parallel & & \downarrow I_* & & \downarrow I \\
N' & \longrightarrow & N' \rtimes_{\Phi} H' & \longleftarrow & H' \\
\parallel & & \downarrow \varphi & & \parallel \\
N' & \longrightarrow & G & \longleftarrow & H' \\
\downarrow K & & \parallel & & \downarrow I^{-1} \\
N & \xrightarrow{j} & G & \xleftarrow{i} & H
\end{array}$$

は可換になる。これで示すべきことがいえた。  $\square$

**命題.** (有限巡回群の半直積の表示)

群  $N, H$  は有限巡回群であり群作用  $\Phi: H \rightarrow \text{Aut } N$  が存在して半直積  $N \rtimes_{\Phi} H$  を考えているとする。 $N, H$  の生成元  $q, h$  をそれぞれとって固定し  $\Phi_h(q) = q^t$  となる  $t \in \mathbb{Z}$  をとることができる。このとき

$$N \rtimes_{\Phi} H \cong \{q, h \mid q^{\#N} = h^{\#H} = 1, hqh^{-1} = q^t\}$$

が成り立つ。

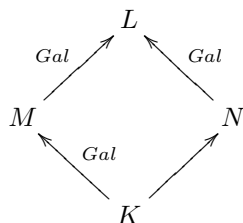
**証明.** 右辺の群を  $G$  とおく。自由群の普遍性により、自由群  $F_2$  から  $N \rtimes_{\Phi} H$  への準同型  $\varphi$  であって  $\varphi(q) = (q, 1)$  かつ  $\varphi(h) = (1, h)$  なるものがある。なお、ここで  $q \in F_2$  と  $q \in N$  は本来別の記号で書くべきだが、かえって煩雑になるので同じ記号とした。 $\varphi$  は全射である。このとき  $q^{\#N}, h^{\#H} \in \text{Ker } \varphi$  はあきらか。また

$$\begin{aligned}
\varphi(hqh^{-1}) &= (1, h)(q, 1)(1, h^{-1}) \\
&= (\Phi_h(q), 1) \\
&= (q^t, 1) \\
&= \varphi(q)^t
\end{aligned}$$

だから  $hqh^{-1}q^{-t} \in \text{Ker } \varphi$  である。したがって、全射  $\psi: G \rightarrow N \rtimes_{\Phi} H$  が誘導される。ここで  $N \rtimes_{\Phi} H$  の位数は  $\#(N \times H)$  であるので  $\#G \geq \#(N \times H)$  である。一方で  $\#G \leq \#(N \times H)$  はあきらかなので結局  $\#G = \#(N \times H)$  であり、 $\psi$  は同型でなくてはならない。  $\square$

**命題.** (半直積と Galois 群)

有限次 Galois 拡大  $L/K$  があり、その中間体  $M, N$  があって  $L = M \cdot N$  かつ  $K = M \cap N$  を満たすとする。



さらに  $M/K$  は Galois 拡大であるとする。このとき

$$\text{Gal}(L/K) \cong \text{Gal}(L/M) \rtimes \text{Gal}(L/N)$$

が成り立つ。

**証明.**  $M/K$  は Galois 拡大なので  $\text{Gal}(L/M) \triangleleft \text{Gal}(L/K)$  である。 $L$  は  $M$  と  $N$  の合成なので  $\text{Gal}(L/M) \cap \text{Gal}(L/N) = 1$  である。また Galois 拡大の推進定理 (雪江 [2] 定理 4.6.1) により  $\text{Gal}(L/N) \cong \text{Gal}(M/K)$  なのでとくに  $[L : N] = [M : K]$  であり、したがって  $[L : N][L : M] = [L : K]$  である。ゆえに、 $\text{Gal}(L/K) \cong \text{Gal}(L/M) \rtimes \text{Gal}(L/N)$  がわかる。  $\square$

## Appendix 2. Dirichlet の Diophantus 近似定理

平成 27 年度基礎科目 II の問 7 のための補足です。あの問題は Dirichlet の近似定理を認めてしまえばほぼ当たり前ののですが、しかし Dirichlet の近似定理ってあんまり本に載ってませんからね。見たことないひとも多いと思います。そこで、Dirichlet の近似定理の内容とその証明をここで補うことにしました。鳩の巣論法を使った証明もあります。それについては Dirichlet の Diophantus 近似定理で調べてください。

**定義.**  $\mathbb{R}^n$  の部分集合  $S$  があるとする。このとき  $S$  が点対称 (centrally symmetric) であるとは、任意の  $x \in S$  に対して  $-x \in S$  であることをいう。また  $S$  が凸 (convex) であるとは、任意の  $x, y \in S$  に対し、 $x$  と  $y$  を結ぶ線分が  $S$  に含まれるということである。つまり任意の  $0 \leq t \leq 1$  に対して  $tx + (1-t)y \in S$  であることを指す。

**命題.** (Minkowski の定理)

$\mu$  は Lebesgue 測度とする。 $S \subset \mathbb{R}^n$  が点対称かつ凸な可測集合で、 $\mu(S) > 2^n$  ならば  $S \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset$  である。

**証明.** ハイリホーによる。 $S \cap \mathbb{Z}^n = \{0\}$  と仮定しよう。 $I$  を  $\mathbb{R}^n$  の標準基底が張る超立方体とする。このとき

$$\begin{aligned} \frac{1}{2^n} \mu(S) &= \mu\left(\frac{S}{2}\right) \\ &= \mu\left(\frac{S}{2} \cap \prod_{d \in \mathbb{Z}^n} (I + d)\right) \\ &= \mu\left(\prod_{d \in \mathbb{Z}^n} \frac{S}{2} \cap (I + d)\right) \\ &= \sum_{d \in \mathbb{Z}^n} \mu\left(\frac{S}{2} \cap (I + d)\right) \\ &= \sum_{d \in \mathbb{Z}^n} \mu\left(\left(\frac{S}{2} - d\right) \cap I\right) \end{aligned}$$

である。ここで  $S$  が凸かつ点対称という仮定により  $d \neq d'$  のとき  $(S/2 + d) \cap (S/2 + d') = \emptyset$  である。したがって

$$\begin{aligned} \frac{1}{2^n} \mu(S) &= \mu\left(\prod_{d \in \mathbb{Z}^n} \left(\frac{S}{2} - d\right) \cap I\right) \\ &\leq \mu(I) \\ &= 1 \end{aligned}$$

となって矛盾。よって示すべきことが言えた。

□

命題. (Dirichlet の近似定理)

$d \geq 1$  とする。実数  $\alpha_1, \dots, \alpha_d$  と  $N \in \mathbb{N}$  が与えられたとき次が成り立つ。

$$\exists q, p_i \in \mathbb{Z} \text{ s.t. } 1 \leq q \leq N \quad \text{and} \quad \forall i \quad |q\alpha_i - p_i| \leq \frac{1}{N^{1/d}}$$

証明. 次のような  $\mathbb{R}^{1+d}$  の部分集合  $S$  を考える。

$$S = \left\{ (x, y_1, \dots, y_d) \in \mathbb{R}^{1+d} \mid -N - 1/2 \leq x \leq N + 1/2, \forall i \quad |x\alpha_i - y_i| \leq \frac{1}{N^{1/d}} \right\}$$

このとき  $S$  は明らかに凸かつ点対称な可測集合なので、あとは  $\mu(S) > 2^{d+1}$  がいえれば Minkowski の定理から主張が従う。計算すると  $M = \frac{1}{N^{1/d}}$  として

$$\begin{aligned} \mu(S) &= \int_{-N-1/2}^{N+1/2} dx \int_{\alpha_d x - M}^{\alpha_d x + M} dy_d \cdots \int_{\alpha_1 x - M}^{\alpha_1 x + M} dy_1 \\ &= (2M)^d (2N + 1) \\ &= \frac{2^d (2N + 1)}{N} \\ &> 2^{d+1} \end{aligned}$$

である。よって示すべきことがいえた。 □

## 参考文献

- [1] 雪江明彦『代数学 1 群論入門』(日本評論社, 2010)
- [2] 雪江明彦『代数学 2 環と体とガロア理論』(日本評論社, 2010)