$J_{x,y} := \{n \in \mathbb{Z} \mid x \le n \le y\}$とおく。

Kを体とする。

$S_n := \{\sigma : J_{1,n} \to J_{1,n} \mid \sigma$は全単射$\}$とおく。

問1　$n \in \mathbb{N}$とする。VをK上のn次元線形空間とし、$\{v_1, \dots, v_n\}$をVの基底とする。

(1) $\lambda_i \in K$ $(i \in J_{1,n})$, $m \in J_{1,n}$, $\lambda_m \neq 0$とする。$w := \sum_{i=1}^{n} \lambda_i v_i$とする。このとき

$\{v_1, \dots, v_{m-1}, w, v_{m+1}, \dots, v_n\}$

がVの基底である事を示せ。

(2) $m \in J_{1,n}$とし$w_1, \dots, w_m$をVの1次独立なm個の元とする。このとき次の「　」を満たす$\sigma \in S_n$が存在する事を示せ。

「各$k \in J_{1,m}$に対して

$\{w_1, \dots, w_k, v_{\sigma(k+1)}, \dots, v_{\sigma(n)}\}$

はVの基底である。」

(3) Vの$n+1$個以上の元は1次従属である事を示せ。

解答 (1) 各自で示せ。

(2) mに関する帰納法。

$m=1$のとき　$w_1 = \sum_{i=1}^{n} \lambda_i v_i$ $(\lambda_i \in K\ (i \in J_{1,n}))$とする。

$w_1 \neq 0$であるのである$z \in J_{1,n}$で$\lambda_z \neq 0$となるものがある。

(1)より$\{v_1, \dots, v_{z-1}, w, v_{z+1}, \dots, v_n\}$は$V$の基底である。$\sigma \in S_n$を

$$\sigma(i) := \begin{cases} z & (i=1\text{のとき}) \\ i-1 & (i \in J_{2,z}\text{のとき}) \\ i & (i \in J_{z+1,n}\text{のとき}) \end{cases}$$

により定義する。このとき

$\{w, v_{\sigma(2)}, \dots, v_{\sigma(n)}\} = \{w, v_1, \dots, v_{z-1}, v_{z+1}, \dots, v_n\}$は$V$の基底である。

<u>$m\in J_{2,n}$のとき</u> 帰納法より次の「 」を満たす$\tau\in S_n$が存在する。

「各$r\in J_{1,m-1}$に対して

$\{w_1,\dots,w_r,v_{\tau(r+1)},\dots,v_{\tau(n)}\}$

はVの基底である。」

$$w_m=\left(\sum_{i=1}^{m-1}\lambda_i w_i\right)+\left(\sum_{j=m}^{n}\lambda_j v_{\tau(j)}\right)$$

$(\lambda_i\in K\ (i\in J_{1,n}))$とする。

$w_1,\dots,w_m$が1次独立であるので$t\in J_{m,n}$で$\lambda_t\neq 0$となるものがある。(1)より

$\{w_1,\dots,w_{m-1},v_{\tau(m)},\dots,v_{\tau(t-1)},w_m,v_{\tau(t+1)},\dots,v_{\tau(n)}\}$

はVの基底である。$\sigma\in S_n$を

$$\sigma(i):=\begin{cases}\tau(i) & (i\in J_{1,m-1})\\ \tau(t) & (i=m)\\ \tau(i-1) & (i\in J_{m+1,t})\\ \tau(i) & (i\in J_{t+1,n})\end{cases}$$

により定義する。σは題意の『 』を満たす。

(3) $d\in\mathbb{N}$を$d\geq n+1$となるものとし$u_1,\dots,u_d$をVのd個の元とする。$u_1,\dots,u_d$は1次独立であると仮定する。このとき$u_1,\dots,u_n$は1次独立であるので(2)より$\{u_1,\dots,u_n\}$はVの基底である。従ってある$\lambda_i\in K$ $(i\in J_{1,n})$で$u_{n+1}=\sum_{i=1}^{n}\lambda_i u_i$となるものがある。

$$(-\lambda_1)u_1+\cdots+(-\lambda_n)u_n+1u_{n+1}+0u_{n+1}+\cdots+0u_d=0$$

であり$1\neq 0$であるので$u_1,\dots,u_d$は1次従属であり矛盾である。従って$u_1,\dots,u_d$は1次従属である。□

次数 xを不定元とし

$K[x] := \{ f(x) = a_n x^n + \cdots + a_1 x + a_0$

$| n \in \mathbb{Z}_{\geq 0}, a_i \in K \ (i \in J_{0,n}) \}$

$= \{ K$上の多項式$\}$

xを不定元とする

とおく。

$n \in \mathbb{Z}_{\geq 0}$, $f(x) = \sum_{i=0}^{n} a_n x^n \in K[x]$

$a_i \in K \ (i \in J_{0,n})$, $a_n \neq 0$,

に対して $\deg(f(x)) := n$ とおく。

$\deg(0) := -\infty$ とおく。$\deg(f(x))$

を$f(x)$の次数という。

$f(x), g(x) \in K[x] \setminus \{0\}$ のとき

$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

が成り立つ。

除法の原理

「 $\forall f(x) \in K[x]$,

$\forall g(x) \in K[x] \setminus \{0\}$,

$\exists h(x) \in K[x]$ (商)

$\exists r(x) \in K[x]$

such that

$f(x) = h(x) g(x) + r(x)$,

$\deg(r(x)) < \deg(g(x))$ 」 ―☆

が成り立つ。

問2 $f(x) \in K[x]$, $\deg(f(x)) \geq 1$,

を既約多項式とする。$g(x) \in K[x] \setminus \{0\}$

を $\deg(g(x)) < \deg(f(x))$

となるものとする。このとき

$K[x] f(x) + K[x] g(x) = K[x]$ ―(*)

$\left(\parallel \atop \{ a(x) f(x) + b(x) g(x) \mid a(x), b(x) \in K[x] \} \right)$

が成り立つ事を示せ。

解答

Sを(*)の左辺とする。$h(x)$を

$S \setminus \{0\}$の元で次数が最小の

既約多項式 $f(x) \in K[x]$, $\deg(f(x)) \geq 1$, に対して $g(x), h(x) \in K[x]$, $\deg(g(x)) \geq 1$, $\deg(h(x)) \geq 1$, で $f(x) = g(x) h(x)$ となるものが存在しないとき $f(x)$をK上の既約多項式という。

ものとする。

☆より

$$S = K[x]h(x)$$

が成り立つ。

$f(x) \in S$ であるので

$$f(x) = c(x)h(x)$$

となる $c(x) \in K[x]$ が存在する。

$c(x) \neq 0$, $h(x) \neq 0$, $\deg(f(x)) = \deg(c(x)) + \deg(h(x))$ が成り立つ。

$f(x)$ は既約であるので

$\deg(c(x)) = 0$ または $\deg(h(x)) = 0$

が成り立つ。

$g(x) \in S$ であるので

$$\deg(h(x)) \leq \deg(g(x))$$

が成り立つ。従って $\deg(h(x)) = 0$

である。ゆえに

$$S = K[x]$$

が成り立つ。

問3　$f(x) \in K[x]$, $\deg(f(x)) \geq 1$,

を既約多項式とする。$n := \deg(f(x))$

とおく。L/K を体の拡大とし

$\alpha \in L$ を $f(\alpha) = 0$ となるものとする。

$$K[\alpha] := \left\{ \sum_{i=0}^{m} b_i \alpha^i \,\middle|\, m \in \mathbb{Z}_{\geq 0},\ b_i \in K \ (i \in J_{0,m}) \right\}$$

とおく。

(1) $\{1, \alpha, \cdots, \alpha^{n-1}\}$ が $K[\alpha]$ の

K 上の基底である事を示せ。

(特に $\dim_K K[\alpha] = n$ である。)

(2) $K[\alpha]$ は L の部分体 である事を示せ。

解答 (1)

$f(x) = a_n x^n + \cdots + a_1 x + a_0$,

$a_i \in K \ (i \in J_{0,n})$, $a_n \neq 0$

とする。

No.

Lの元としての等式

$$0 = f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0$$

が成り立つ。

$$\alpha^n = \left(-\frac{a_0}{a_n}\right)1 + \left(-\frac{a_1}{a_n}\right)\alpha + \cdots + \left(-\frac{a_{n-1}}{a_n}\right)\alpha^{n-1}$$

であるので

$$K[\alpha] = \left\{\sum_{i=0}^{n-1} c_i\alpha^i \,\middle|\, c_i \in K\ (i \in J_{0,n-1})\right\}$$

が成り立つ。

$d_i \in K\ (i \in J_{0,n-1})$ を

$$\sum_{i=0}^{n-1} d_i\alpha^i = 0$$

となるものとする。

ある $r \in J_{0,n-1}$ で $d_r \neq 0$ となるものがあるとする。このとき

$k \in J_{1,n-1}$ で $d_k \neq 0$ となるものがある。

$$g(x) := \sum_{i=0}^{n-1} d_i x^i \in K[x]$$

とおく。$g(\alpha) = 0$ が成り立つ。

$$k \leq \deg(g(x)) \leq n-1$$

が成り立つ。問2の(※)より

ある $u(x), v(x) \in K[x]$ で

$$u(x)f(x) + v(x)g(x) = 1$$

となるものがある。

Lの元としての等式

$$1 = u(\alpha)f(\alpha) + v(\alpha)g(\alpha) = u(\alpha)0 + v(\alpha)0 = 0$$

が成り立つ。これは $1 \neq 0$ に矛盾する。

従って $d_0 = d_1 = \cdots = d_{n-1} = 0$ が成り立つ。

従って $1, \alpha, \ldots, \alpha^{n-1}$ は1次独立である。

従って $\{1, \alpha, \ldots, \alpha^{n-1}\}$ は $K[\alpha]$ の基底である。

(2) $\beta \in K[\alpha] \setminus \{0\}$ とおく。
任意の $l \in \mathbb{Z}_{\geq 0}$ に対して $\beta^l \in K[\alpha]$ である。
$\dim_K K[\alpha] = n$ であるので

$1, \beta, \ldots, \beta^n$ は1次従属である。

従って $d_i \in K\ (i \in J_{0,n})$ と

$k \in J_{1,n}$ で $\sum_{i=0}^{n} d_i \beta^i = 0$

かつ $d_k \neq 0,\ d_j = 0\ (j \in J_{0,k-1})$

となるものが存在する。

$$\beta^{-1} = \frac{\beta^k}{\beta^{k+1}}$$

$$= \frac{\frac{1}{d_k}(-d_{k+1}\beta^{k+1} - \cdots - d_n\beta^n)}{\beta^{k+1}}$$

$$= \left(-\frac{d_{k+1}}{d_k}\right) + \left(-\frac{d_{k+2}}{d_k}\right)\beta + \cdots$$

$$+ \left(-\frac{d_n}{d_k}\right)\beta^{n-k-1} \in K[\alpha]$$

従って $K[\alpha]$ は L の部分体

である。 □

<u>問4</u> $f(x) \in K[x],\ \deg(f(x)) \geq 1$

を既約多項式とする。L/K を

体の拡大とし $\alpha \in L$ を $f(\alpha) = 0$

となるものとする。M/L を体の

拡大とし $\beta \in M$ を $f(\beta) = 0$

となるものとする。このとき体

の同型写像

$$\Phi : K[\alpha] \longrightarrow K[\beta]$$

で $\Phi(c) = c\ \ (c \in K)$,

$\Phi(\alpha) = \beta$ となるものが一意的

に存在する事を示せ。

<u>解答</u>

$n := \deg(f(x))$,

$f(x) = a_n x^n + \cdots + a_1 x + a_0$

$a_i \in K\ (i \in J_{0,n}),\ a_n \neq 0$,

とする。

$$\dim_K K[\alpha] = \dim_K K[\beta] = n$$

である。$\{1, \alpha, \cdots, \alpha^{n-1}\}$ は $K[\alpha]$

の K 上の基底である。

$\{1, \beta, \cdots, \beta^{n-1}\}$ は $K[\beta]$ の K 上

の基底である。

全単射 $\Phi : K[\alpha] \longrightarrow K[\beta]$

を

$$\Phi\left(\sum_{i=0}^{n-1} b_i \alpha^i\right) = \sum_{i=0}^{n-1} b_i \beta^i$$

$$\left(b_i \in K \ \left(i \in J_{0,n-1}\right)\right)$$

により定義する。このとき

$$\Phi(cu+dv) = c\,\Phi(u) + d\,\Phi(v)$$

$$(u, v \in K[\alpha],\ c, d \in K)$$

が成り立つ。(特に $\Phi(u+v) = \Phi(u)+\Phi(v)$ が成り立つ。)

$$\alpha^n = \left(-\frac{a_0}{a_n}\right)\cdot 1 + \left(-\frac{a_1}{a_n}\right)\alpha + \cdots + \left(-\frac{a_{n-1}}{a_n}\right)\alpha^{n-1},$$

$$\beta^n = \left(-\frac{a_0}{a_n}\right) 1 + \left(-\frac{a_1}{a_n}\right)\beta + \cdots + \left(-\frac{a_{n-1}}{a_n}\right)\beta^{n-1}$$

であるので

$$\forall m, \forall k \in \mathbb{Z}_{\geq 0},\ \exists l_i \in K\ (i \in J_{0,n-1})$$

$$\alpha^m \cdot \alpha^k = \sum_{i=0}^{n-1} l_i \alpha^i, \text{ および}$$

$$\beta^m \cdot \beta^k = \sum_{i=0}^{n-1} l_i \beta^i$$

が成り立つ。

従って

$$\Phi(uv) = \Phi(u)\Phi(v) \quad (u, v \in K[\alpha])$$

が成り立つ。

$u \in K[\alpha] \setminus \{0\}$ とする。

$$\begin{aligned}
\Phi(u^{-1}) &= \Phi(u^{-1})\cdot 1 \\
&= \Phi(u^{-1})\left(\Phi(u)\Phi(u)^{-1}\right) \\
&= \left(\Phi(u^{-1})\Phi(u)\right)\Phi(u)^{-1} \\
&= \Phi(u^{-1}u)\Phi(u)^{-1} \\
&= \Phi(1)\Phi(u)^{-1} \\
&= 1\cdot\Phi(u)^{-1} \\
&= \Phi(u)^{-1}
\end{aligned}$$

従って Φ は体の同型写像であり $\Phi(c) = c\ (c \in K)$ を満たす。

Φ の一意性は明らかである。