第13回 代数系

今日 やり残したこと

① UFDについて　R:UFD ⇒ R[X]:UFD

② 円分多項式のモノ性について

⇒ $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

③ PID上の有限生成加群の構造定理（一意性）

→ Jordan, 有限アーベル群

↓

有限体のパリは巡回群

体のパリの有限部分群も巡回群

← 原始根

$\mathbb{F}_{p^n} \supset \mathbb{F}_p$ は単拡大

Recall A: domain かつ UFD

def ⇔ $\forall a \in A \setminus A^\times$ $a = p_1 \cdots p_r$

$r \geq 1$, p_i: 素元

このとき a の分解は

並べかえと $A^\times$ を除いて

一意だった。

($p_i \neq 0$ かつ $(p_i) \in \mathrm{Spec}\, A$)

(同伴元)

Ex $\mathbb{Z}^\times = \{\pm 1\}$ $6 = 2 \cdot 3 = (-3)\cdot(-2)$

記法 A: UFD $a_1 \sim a_n \neq 0$

$\mathrm{GCD}(a_1, \cdots, a_n)$ が $A^\times$ を除いて定まる

(LCM も)

Ex $\mathbb{Q}[\sqrt{-3}] = \{a+b\sqrt{-3} \mid a,b \in \mathbb{Q}\} \subseteq \mathbb{C}$

はUFDでない

$a = 4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$

$b = 2(1+\sqrt{-3})$

$2 \mid a \cdot b \Rightarrow 2 \nmid 1+\sqrt{-3}$

$1+\sqrt{-3} \mid a \cdot b \quad 1+\sqrt{-3} \nmid 2$

(注) $d \mid a, b$ でいうGCD

$d' \mid a, b \Rightarrow d' \mid d$

Lem A : domain $\ni p$: 素元

p は $A[X]$ でも素元

(i) $A[X] \to (A/(p))[X]$ は環準同型

$\sum a_i X^i \mapsto \sum [a_i] X^i$

$$\ker = pA[X] = \{ pf(x) \mid f \in A[X] \}$$

$$= (p)$$

$$\therefore A[X]/pA[X] \simeq (A/pA)[X]$$

R : domain $\Rightarrow R[X]$: domain

(ii) $(A/pA)[X]$ は整域 //

"Cor" (Eisenstein既約判定法)

A: domain $\ni p$: 素元

$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$

条件 ① $1 \leq {}^\forall i \leq n$, $p \mid a_i$

② $p^2 \nmid a_n$

$\Rightarrow$ $f(x)$は既約 in $A[x]$

∵ $(A[x])^\times = A^\times$ に注意。

$f(x) = g(x)h(x)$ $\deg g, \deg h < \deg f$

として矛盾を導く。

$A[x] \twoheadrightarrow (A/pA)[x]$ において

$$f \longmapsto x^n$$
$$\shortparallel \qquad\qquad \shortparallel$$
$$gh \qquad x^m x^{n-m}$$

よって g と h の定数項は p の倍

これは $p^2 \nmid a_n$ に矛盾。//

系 $p \geq 2$ ：素数 $\Phi_p = \prod_{k=1}^{p-1} (x - \zeta_p^k)$

$$= \frac{x^p - 1}{x - 1} \in \mathbb{Q}(x)$$

は既約 in $\mathbb{Q}[x]$

(証) $y = x+1$ $\Phi_p(y) = \frac{(y+1)^p - 1}{y}$ ← 定数項や最高次以外 p で割れる//

$\binom{p}{i} \in p\mathbb{Z}$ $1 \leq i \leq p-1$

Def A : UFD

$f \in A[x]$ について

$\neq 0$ $\quad c(f) := \mathrm{GCD}(\underbrace{a_0, \cdots, a_n}_{\text{"0はとばす"}})$: 容量

$f = a_0 x^n + \cdots + a_n$

が原始的 $\underset{\text{def}}{\iff}$ $c(f) = 1$

全て up to $A^\times$

Ex $A = \mathbb{Z}$ $\quad f(x) = 2x \quad c(f) = 2$

$\mathbb{Q}$ $\quad f(x) = 2x \quad c(f) = 1$

Lem (Gauss) $f, g \in A[x]$: 原始的 $\Rightarrow$ fg : 原始的

A : UFD

(∵) otherwise $\exists p$ $p \mid (fg)$ すると $(A/pA)[x]$ で

$[fg] = 0$ すると $[f] = 0$ or $[g] = 0$ //

Lem A : UFD $\hookrightarrow K = \mathrm{Frac}(A)$

$\forall 0 \neq f(x) \in K[x]$

$\exists f_0 \in A[x]$: 原始的

$\exists c \in K$ s.t. $f = f_0 c$

この c は $A^\times$ を除いて一意的で $c_A(f)$ と書く

Ex $x - \frac{1}{2} \in \mathbb{Q}[x]$ $(2x-1)\cdot\frac{1}{2}$

☺ 表示をもつことは明らか

$f = \frac{a}{b} f_0 = \frac{a'}{b'} f_0'$

f_0, f_0' : 原始的

$a, b, a', b' \in A$ s.t.

$\mathrm{GCD} = 1$ $\mathrm{GCD} = 1$

$ab f_0 = a'b f_0'$

$\Rightarrow a \mid a'b \Rightarrow a \mid a'$ 同様 $a' \mid a$, $b \mid b'$, $b' \mid b$ //

Lemma A: UFD, $K = \mathrm{Frac}(A)$

$f, g \in K[X]$

$c_A(fg) = c_A(f)c_A(g)$ up to $A^\times$

$f = c_A(f) f_0$ f_0, g_0: 原始的

$g = c_A(g) g_0$ $c_A(f), c_A(g) \in K$

$fg = c_A(f)c_A(g) f_0 g_0$

原始的 by Gauss

一意性より $c_A(fg) = c_A(f)c_A(g)$

系 A : UFD (2x A:②)

$f(x) \in A[x] \setminus A$: 既約 in $A[x]$
(自動的に原始的)

$\Rightarrow$ $f(x)$ は既約 in $K[x]$

(証) $f = gh$ in $K[x]$

$C_A(f) = C_A(g) C_A(h)$

$\|$

1

$f_0 = C_A(g) C_A(h) g_0 h_0$

$f_0 = f$, $C_A(g) C_A(h) \in A^\times$, $g_0 h_0$: $A(x)$ の原始的

既約性より $g_0 \in A^\times$ or $h_0 \in A^\times$ //

系 同じ設定で $f(x)$ は $A[x]$ の素元

∵ $f \mid gh$ in $A[x] \Rightarrow f \mid g$ or $f \mid h$

f は $K[x]$ の既約元 ⟺ 素元

よって $f \mid g$ in $K[x]$ or $f \mid h$ in $K[x]$

ok!

$fQ = g \quad \exists Q \in K[x]$

$f\, c_A(Q) Q_0 = c_A(g) g_0$

$fQ_0 = \dfrac{c_A(g)}{c_A(Q)} g_0$

fQ_0: 原始的

$\dfrac{c_A(g)}{c_A(Q)} \in A^\times$

よって $f \mid g$ が言えた!!

ようするに A : UFDのとき

A[x]の素元は ・Aの素元

・A[x]の1次以上もつ原始多項式

Thm A : UFD ⇒ A[x]もUFD

(証) $f \in A[x]$ 　$f = c(f) \cdot f_0$

$f \neq 0$

$c(f)$: Aの素元の積　f_0: 原始的

f_0がキヤク ⇒ OK

o.w. $f_0 = g_0 h_0$　$\deg g_0, \deg h_0 < \deg f_0$

このとき g_0, h_0も原始的　これをくり返す //

円分多項式の既約性

$$\Phi_n(X) = \prod_{\substack{0 \le k < n \\ (k,n)=1}} (X - \zeta_n^k) \in \mathbb{C}[X]$$

(*) モニック $\mathbb{Q}[X]$ の元 次数 $\varphi(n)$

Thm $\forall n \ge 1$, $\Phi_n(X)$ はモニック in $\mathbb{Q}[X]$

$f(X) = f_W(\Phi_k ; \zeta_n)$

$\forall p \nmid n$: 素数, $f(\zeta_n^p) = 0$ を言う

(このとき $\forall k$ s.t. $(k,n)=1$, $f(\zeta_n^k)=0$

k の素因数についての帰納法で示せる)

Ex $k = 6 = 2 \cdot 3$ $f(\zeta_n^2) = 0$ $f((\zeta_n^2)^3) = 0$

$$\Delta := \prod_{0 \le i < j < n} (\zeta_n^i - \zeta_n^j)^2$$

$$= \pm n^n \text{ は有理的}$$

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

$f(x) \mid \Phi_n(x)$ in $\mathbb{Q}[X]$

$f(x) \in \mathbb{Z}[X]$ が分かる

$$\left(\begin{aligned} \Phi_n(x) &= f(x)\, g(x) \\ &= c_{\mathbb{Z}}(f)\, f_0\, c_{\mathbb{Z}}(g)\, g_0 \\ &= f_0\, g_0 \end{aligned} \right)$$

$$f(x) = (x - \zeta_n)(x - \zeta_n^{◎}) \cdots (x - \zeta_n^{*})$$

$f(\zeta_n^p) \neq 0$ $\quad f(\zeta_n^p) \in \overline{\mathbb{Z}}$ 代数的整数

$f(x) \in \mathbb{Q}[X]$ より

$$f(x^p) \equiv f(x)^p \mod p$$

(より正確に $f(x^p) - f(x)^p = p\,g(x)$

$\exists g(x) \in \mathbb{Q}[X]$)

$\Leftarrow \binom{p}{i} \in p\mathbb{Z} \quad 1 \leq i \leq p$

よって $f(\zeta_N^p) \in p\overline{\mathbb{Z}}$

一方で $\exists \chi \in \overline{\mathbb{Q}} \quad p\chi = \pm n^n$

つまり $\chi \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ これは矛盾//

初等的の部分

$$\Delta = \pm \prod_{0 \le i < j < n} \left(\zeta_n^i - \zeta_n^j \right) \qquad x^n - 1$$

$$= \pm \prod_{i,j} \zeta_n^i \left(1 - \zeta_n^{j-i} \right)$$

$$= \pm \prod_{i} \zeta_n^i \boxed{\prod_{k=1}^{n-1} \left(1 - \zeta_n^k \right)} = \pm n^n$$

n

□ の proof

$$f_n(x) = \prod_{k=1}^{n-1} \left(x - \zeta_n^k \right) = \frac{x^n - 1}{x - 1} = 1 + \cdots + x^{n-1}$$

$x = 1$ を代入する

みとめたこと

$$\overline{\mathbb{Z}} = \{ \theta \in \mathbb{C} \mid \exists f(x) \in \mathbb{Z}[x] \ (\text{モニック}),\ f(\theta) = 0 \} \text{ は環}$$

意外と非自明

Ex $\sqrt{2}, \sqrt{3} \in \overline{\mathbb{Q}}$

$x^2-2 \quad x^2-3$

$\sqrt{2}+\sqrt{3}$

x^4-10x^2+1

みとめたこと $\overline{\mathbb{Q}} \cap \mathbb{Q} = \mathbb{Q}$

(;) $x^n + a_1 x^{n-1} + \cdots + a_n = 0 \quad a_i \in \mathbb{Q}$

は $x = \frac{q}{p}$ $p \geq 2$ を解にもたない

もったとすると $x^n + \cdots + a_n = \left(x - \frac{q}{p}\right) Q(x)$

in $\mathbb{Q}[x]$

$= (px - q) Q_0(x)$ $\frac{1}{p} \mathbb{Q}(\mathbb{Q})$

PID上のf.g. moduleの構造定理(お話)

Thm A: PID

M: f.g. A-module

$\left(\text{i.e. } \exists v_1, \dots, \exists v_n \in M \text{ s.t. } \forall m \in M \ \exists \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in A^n,\ m = \sum_{i=1}^{n} a_i v_i \right)$

as A-modules

$$M \cong A/I_1 \times \cdots \times A/I_s \times \underbrace{A \times \cdots \times A}_{t}$$

ここで $A \supsetneq I_1 \supsetneq \cdots \supsetneq I_s \supsetneq \{0\}$ ideal

(注) M, N: A-module のとき $M \times N$ は A-module

(注) ふつう $\times$ は $\oplus$ と書く (になる $(M \oplus N$ とかく)

(注) A/I は $a[x] = (ax)$ で A-module

Cor (有限アーベル群の構造定理)

$A = \mathbb{Z}$ とすると G: finite $\mathbb{Z}$-module

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

$$\| $$

$$C_{n_1} \times \cdots \times C_{n_s}$$

$\exists\, n_1 \mid \cdots \mid n_s$

Rk Abel群と $\mathbb{Z}$-moduleと(ほぼ)同じ概念

"Ma分" $\longleftrightarrow$ M

$G \rightsquigarrow \mathbb{Z} \times G \longrightarrow G$

$$(n, g) = \begin{cases} \underbrace{g + \cdots + g}_{n} & n > 0 \\ 0 & n = 0 \end{cases}$$

$n < 0$ も定義

Jordan標準形への応用

$A \in M_n(\mathbb{F})$, $\mathbb{F}$：体：固定

(注) $\mathbb{F}^n$ は $\mathbb{F}[x]$-module via

$$\left(\sum_{i=0}^{n} a_i x^i, v \right) \longmapsto \sum_{i=0}^{n} a_i A^i v$$

$\uparrow$ $\mathbb{F}[x]$　$\uparrow$ $\mathbb{F}^n$　$\in \mathbb{F}^n$

"Cor" M：$\mathbb{F}[x]$-module $\dim_{\mathbb{F}} M < +\infty$

$$M \simeq \bigoplus_{i=1}^{r} \mathbb{F}[x]/(f_i(x))$$

本当は自で書く

Def $f(x) = x^m + a_1 x^{m-1} + \cdots + a_m \in F[x]$

$$C(f) = \begin{pmatrix} 0 & & & -a_m \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \vdots \\ & & 1 & -a_1 \end{pmatrix} \in M_m(F)$$

$[x^0]$ (x^{m-1})

fのコンパニオン行列

$x^m = -a_1 x^{m-1} - \cdots - a_m$ in $F[x]/(f(x))$

Eg $f(x) = x^3 + 3x^2 + 2x + 1$

$$C(f) = \begin{pmatrix} 0 & & -1 \\ 1 & 0 & -2 \\ & 1 & -3 \end{pmatrix}$$

上の設定で

Prop $F[x]/(f(x)) = V$ は $\dim_F V = m$ かつ

xの作用の$[x^0], \cdots, [x^{m-1}]$に関する

表現行列は$C(f)$

明らか

系 $\exists R \in GL_n(F)$ s.t.

$$R^{-1}AR = \bigoplus_{i=1}^{r} C(f_i)$$

Propの設定で

$F = \mathbb{C}$ ならOK

$$f(x) = (x-r_1)^{\delta_1} \cdots (x-r_m)^{\delta_m}$$

$r_1 \sim r_m \in F$: 異なる $\forall \delta_\delta \geq 1$

CRT as ring

$$F[x]/(f(x)) \cong \bigoplus_{i=1}^{r} F[x]/(x-r_i)^{\delta_i}$$

これは $F[x]$-module としてそう

prop $W = \mathbb{F}[x]/((x-\alpha)^m)$ $\alpha \in \mathbb{F}$ について

$[(x-\alpha)^0], \cdots, [(x-\alpha)^{m-1}]$ が基底で,

$x-\alpha$ の表現行列は

$$J(0;m) = \begin{pmatrix} [(x-\alpha)^{m-1}] & & & [(x-\alpha)^0] \\ 0 & 1 & & \\ & \ddots & \ddots & \\ & & 1 & \\ & & 0 & \end{pmatrix}$$

Cor 上の設定で x の表現行列は $J(\alpha;m)$

これから $\forall A \in M_n(\mathbb{C}) \exists P \in GL_n(\mathbb{C})$

s.t. $P^{-1}AP =$ Jordan 細胞の直和

が分かる

構造 thm の単因子論による説明(2)いい

Recall Rank 標準形 $\mathbb{F}$:体 (お話)

$$\forall M \in M_{a,b}(\mathbb{F})\ \exists! r\ \exists P \in GL_a(\mathbb{F})\ \exists Q \in GL_b(\mathbb{F})$$

$$PMQ = \begin{pmatrix} E_r & O \\ O & O \end{pmatrix}$$

Fact $\mathbb{F}$:PID (単因子標準形)

$$\forall M \in M_{a,b}(\mathbb{F})\ \exists I_1 \supseteq \cdots \supseteq I_s \supsetneq \{0\}$$

$I_1 = (d_1)$, $I_s = (d_s)$

$$\exists P \in GL_a(\mathbb{F})$$

$$\exists Q \in GL_b(\mathbb{F})\quad PMQ = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & O \\ & & d_s & \\ \hline & O & & O \end{array}\right)$$

注) F: 可換環

$$P \in GL_n(F) \iff \det P \in F^\times$$

⇒ $PQ = QP = E_n$ で det をとる

⇐ $P^{-1} = \frac{1}{\det P} \tilde{P}$

注) 単因子標準形を用いて

構造 thm を示すことができる

逆に構造 thm から単因子

標準形を示すこともできる

例

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

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

"ツルカメ算"

↑ 単因子行列

↑ $\det = 1$

unimodular

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

"sketch of proof" (お話)

A : PID はネーター環

M : f.g. A-module (A : ネーター) のとき

$^{\forall}N \subseteq M$: sub A-module も f.g.

$$
\begin{array}{ccccc}
A^n & \xrightarrow{F} & A^m & \overset{G}{\twoheadrightarrow} & M \\
\wr\!\! & \circlearrowleft\ \text{有限表示} & \wr\!\! & & \\
A^n & \xrightarrow{\text{単因子論}} & A^m & &
\end{array}
$$

$$
\left(\begin{array}{ccc|c}
d_1 & & & \\
& \ddots & & \\
& & d_s & \\
\hline
& & &
\end{array}\right)
$$

e_i

$G(e_i) = m_i$

有限生成

$\mathrm{Im}\, G = \sum_{i=1}^{m} A m_i$

$\mathrm{Ker}\, G \subseteq$ U も f.g.

$\shortparallel$

$\mathrm{Im}\, F$

即 $M \simeq A^m / \mathrm{Ker}\, G = A^m / \mathrm{Im}\, F$

$\simeq A/(d_1) \times \cdots \times A/(d_s) \times A^{m-s}$

なので構造thmの形はすぐに出る

注

$$\begin{array}{ccc} M_1 & \xrightarrow{f} & M_2 \\ \alpha \wr \downarrow & \circlearrowleft & \downarrow \wr \beta \\ N_1 & \xrightarrow[g]{} & N_2 \end{array}$$

のとき

fのCoker

$$M_2/\mathrm{Im}\, f \overset{\text{自然}}{\simeq} N_2/\mathrm{Im}\, g$$

∵

$$\begin{array}{ccccc} M_2 & \xrightarrow{\beta} & N_2 & \twoheadrightarrow & N_2/\mathrm{Im}\, g \\ \downarrow & & & & \\ M_2/\mathrm{Im}\, f & & & & \end{array}$$

$[x] \mapsto [\beta(x)] \in$?

$\beta(\mathrm{Im} f) \subseteq \mathrm{Im}\, g$

同様に

$$N_2/\mathrm{Im}\, g \to M_2/\mathrm{Im}\, f$$

$$[y] \mapsto [\beta^{-1}(y)]$$

これらは互いに逆