多項式環の剰余環の性質について

青山学院大学　理工学部　物理・数理学科
学籍番号:15117061　QIN DADI 秦 大地
西山研究室

2021年2月19日

概 要

この論文では主に体上の多項式環の剰余環的性質を調べた．例えば一意分解環であるかどうかやネーターの正規化定理に現れた代数独立な元やそのような代数的独立で生成される多項式環上の加群としての構造などについて考察した．

一般的に，一意分解整域であるかどうかを調べるためには単元群を調べることが重要だから，単元群を決定するこもとこの論文の重要なテーマである．

目 次

1　序論

本研究では可換環論の基本的な定理の一つであるネーターの正規化定理の理解と応用，およびその過程で興味を持った問題として，多項式環の剰余環が一意分解整域 (UFD) であるかどうかを実例によって考える．

ネーターの正規化定理とは次のような定理である．

定理 1 (ネーターの正規化定理)**.** A を体 k 上の有限生成整域とする．このとき，ある $\{y_1, \ldots, y_m\} \subset A$ $(m \geq 0)$ が存在して，次の (1),(2) を満たす．

(1) $\{y_1, \ldots, y_m\}$ は k 上代数的独立．つまり $k[y_1, \ldots, y_m]$ は m 変数多項式環と同型である．

(2) $k[y] = k[y_1, \ldots, y_m]$ と表すと，A は $k[y]$ 上整である．(つまり A は有限生成 $k[y]$ 加群である．)

このとき $m = \dim A$ である．ただし $\dim A$ は A のクルル次元 (環 A における素イデアルの真の増大列の長さの最大値) を表す．

この定理は M.Reid, Undergraduate Algebraic Geometry [Reid] の §3, Theorem 3.13 に述べられている．また，代数多様体上の関数環にも興味があるので，これらを理解することを目標に研究を始めた．

1.1　この論文で考える主な問題

以下 $k[\mathbb{X}] = k[X_1, \ldots, X_n]$ を体 k 上の n 変数多項式環とする．

問題 2. この論文では体 k 上の多項式環の剰余環 $A = k[\mathbb{X}]/I$ に対して次の (1), (2), (3), (4), (5) の問題について考察する．ただし $I \subset k[\mathbb{X}]$ は $k[\mathbb{X}]$ のイデアルである．

(1) I が素イデアルがどうかを判定する．

(2) 剰余環 A の単元群 $A^\times$ を決定する．

(3) 定理 (1) に現れる代数的独立な元の集合 $\{y_1, \ldots, y_m\}$ を決定する．

(4) A の $k[y]$ 加群としての生成元 $\{a_1, \ldots, a_m\}$ を見つける．

(5) A は UFD でないことも多いが，多項式環とは同型ではなく，UFD であるような A の例を探す．

(1) から (5) までの問題を超楕円曲線や超球面の関数環の場合，I が行列式で生成されたイデアルのときなどの場合に考察する．

1.2 主結果

剰余環 $A = k[\mathbb{X}]/I$ ($k[\mathbb{X}]$ は多項式環，I は $k[\mathbb{X}]$ のイデアル) を考える．

1. k を代数閉体とする．$k[\mathbb{X}] = k[X, Y]$ のときに $Q = Y^2 - P(X)$ に対して $I = (Q)$ を考える (§6 参照)．ただし $P(X)$ は X の多項式である．

   (a) $P(X)$ が重根を持たない二次式のとき．

      i. $A^\times$ は巡回群 $\mathbb{Z}$ と $k^\times$ の直積に同型である．

      ii. A は UFD である．

      iii. $A = k[x]y \oplus k[x]$ が成り立つ．(ただし x, y は剰余環 $A = k[X, Y]/I$ における X,Y の像を表す．)

   (b) $P(X)$ が奇数次で一次式の積に分解するとき ($\deg P(X) \geq 3$)．

      i. $A^\times = k^\times$ である．

      ii. A は UFD ではない．

      iii. $A = k[x]y \oplus k[x]$ が成り立つ．

2. $I = (\Delta_n)$ のとき (但し $\Delta_n = \det_n$ は n 次の行列式で $k[\mathbb{X}] = k[X_{ij} \mid 1 \leq i, j \leq n]$)．

   (a) $A^\times = k^\times$ である．

   (b) A は UFD ではない．

   (c) $n = 2$ のとき $A = k[y, z, x - w](x + w) \oplus k[y, z, x - w]$ である．これについては §4 で詳しく説明する．

2 可換環論における基本事項

この節では A は一般の可換環とする．ただし A は常に乗法の単位元 1 を含むとする．

定義 3 (単元と単元群)**.** $a \in A$ が A の**単元**であるとは．$\exists b \in A$ が存在して $ab = 1$ を満たすときに言う．環 A の単元の全体を A の**単元群**と呼ぶ．

$$A^\times = \{a \in A \mid \exists b \in A \ \text{ s.t. } \ ab = 1\}$$

で表す．

例 4. (1) k が体のとき $k^\times = k - \{0\}$ である．

(2) $M_n(k)$ を k 上の n 次正方行列からなる全行列環とするとき $M_n(k)$ の単元群は $M_n(k)^\times = GL_n(k)$ であって n 次正則行列からなる一般線形群に一致する．

定義 5 (零因子)**.** 環 A の元 $a \in A$ に対して $ax = 0$ となる $x \neq 0$ が存在するとき a を**零因子**と呼ぶ.

定義 6 (整域)**.** A が 0 以外の零因子を持たないとき**整域**と呼ぶ.

定義 7 (イデアル)**.** 可換環 A の部分集合 $I \subset A$ が以下の 2 つの条件を満たすとき，I を A の**イデアル**と言う

1. $\forall a, b \in I$ に対して $a + b \in I$ である．(I は加法について閉じている．)
2. $\forall a \in I, r \in A$ に対して $ra \in I$ である．(I は A 加群である．)

定義 8 (素イデアル)**.** 可換環 A のイデアル $J \neq A$ が $a, b \in A$ に対して

$$ab \in J \Longrightarrow a \in J \text{ または } b \in J$$

を満たすとき J を**素イデアル**と言う.

定義 9 (極大イデアル)**.** 可換環 A の真のイデアル $I \subsetneq A$ に対して，$I \subsetneq J \subsetneq A$ になるようなイデアル J が存在しないとき，I を**極大イデアル**と言う.

定義 10 (剰余環)**.** I を A のイデアルとするとき，**剰余環**を A/I で表す．このとき商写像を

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A/I \\ \cup & & \cup \\ a & \longmapsto & \varphi(a) = a + I \end{array}$$

で表す.

命題 11. A を可換環，I をそのイデアルとする．このとき，A/I が整域 $\Longleftrightarrow$ I が素イデアルである.

(証明). 最初に ($\Longleftarrow$) を示す．そこで $a, b \in A/I$ で $ab = 0$ となったとする．まず，$a' \in A$ であって $\varphi(a') = a$ となるものをとる．$b' \in A$ も同様．すると，$ab = 0$ だから $a'b' \in I$ である．I は素イデアルだから $a' \in I$ としても一般性を失わない．すると $a = \varphi(a') = 0$ となる.

次に ($\Longrightarrow$) を示す．$a, b \in A$ かつ $ab \in I$ となったとする．$ab \in I$ より $\varphi(ab) = \varphi(a)\varphi(b) = 0$ である．A/I は整域だから，$\varphi(a)$ または $\varphi(b) = 0$ ，ここで $\varphi(b) = 0$ としても一般性を失わない．$\varphi(b) = 0$ だから $b \in I$ である．従って I は素イデアルである． □

定義 12 (代数的独立)**.** k を体とする ．k 代数 A の元 $\{y_1, \ldots, y_m\}$ に対して，$k[y] = k[y_1, \ldots, y_m]$ が m 変数多項式環と同型なとき $\{y_1, \ldots, y_m\}$ は k 上**代数的独立**であるという.

定義 13 (加群). 可換環 A 上の**加群** M とは，まず M は加法群であって，A の M への作用

$$\begin{array}{ccc} A \times M & \xrightarrow{f} & M \\ \cup & & \cup \\ (a, x) & \longmapsto & ax \end{array}$$

が与えられているときにいう．また M を A 加群ともいう．

定義 14. B を A の部分環とする．A が B 上**整であるとは**各 $a \in A$ が B 上整であるときにいう．また，元 $a \in A$ が B 上整であるとは $B[a]$ が有限 B 加群のときにいう．(つまりある B 上のモニック多項式 $X^N + b_{N-1}X^{N-1} + \cdots + b_0$ が存在して $a^N + b_{N-1}a^{N-1} + \cdots + b_0 = 0$ を満たす．)

この論文で考察するのは次の定理である．証明については [堀田 1] 定理 4.9 を参照して欲しい．

定理 15 (ネーターの正規化定理). A を体 k 上の有限生成整域とする．このとき，ある $\{y_1, \ldots, y_m\} \subset A$ $(m \geq 0)$ が存在して，次の (1),(2) を満たす．

(1) $\{y_1, \ldots, y_m\}$ は k 上代数的独立．つまり $k[y_1, \ldots, y_m]$ は m 変数多項式環と同型である．

(2) $k[y] = k[y_1, \ldots, y_m]$ と表すと，A は $k[y]$ 上整である．(つまり A は有限生成 $k[y]$ 加群である．)

このとき $m = \dim A$ である．ただし $\dim A$ は A のクルル次元 (環 A における素イデアルの真の増大列の長さの最大値) を表す．

この定理の他に論文で考察したいのは一意分解性であるので，さらに用語を準備する．

定義 16 (素元と既約元). A を可換環とする．$p \in A$ が**素元**とは $p|ab$ ならば $p|a$ または $p|b$ が成り立つときにいう．また $m \in A$ が**既約元**とは $m = ab$ ならば a または b のいずれかが単元であることをいう．

補題 17 (素元は既約元). 整域 A において素元は既約元である．

(証明). $a \in A$ を素元，$a = st$ $(s, t \in A)$ と書けたとすると a が素元なので $a|s$ または $a|t$ である．そこで $a|s$ としても一般性を失わない $s = pa$ と書いて，最初の式に代入すると

$$a = st \implies pa = pst \implies s = pst \implies (1 - pt)s = 0$$

が成り立つ．A は整域で $s \neq 0$ だから $1 - pt = 0$，つまり $pt = 1$ である．つまり t は単元であるから a は既約元であることがわかる． □

定義 18 (UFD)**.** 整域 A の零元でも単元でもない元 a が $a = r_1 r_2 \dots r_n$ のように A の有限個の既約元の積として単元倍を除いて一意に分解できるとき，A は**一意分解整域** (UFD) であると言う．このとき既約元と素元は一致する ([堀田 1, §1.5] 参照)**.**

定義 19 (PID)**.** A を整域とする．A の任意のイデアル I が単項イデアルであるとき A は**単項イデアル整域** (PID) であるという．つまり A の任意のイデアル I に対して，, $\exists a \in A$ が存在して $I = (a) = \{xa \mid x \in A\}$ と表すことができる**.**

補題 20. PID は UFD である．(証明は [川口 1] 定理 5.54 参照)

3 超曲面と関数環

定義 21 (アフィン空間)**.** k を代数閉体とし $k[\mathbb{X}] = k[X_1, \dots, X_n]$ と書く．また，k 上の n 次元**アフィン空間**を $\mathbb{A}_k^n = k^n$ と書く**.**

定義 22 (超曲面)**.** 多項式 $f(X_1, \dots, X_n) \in k[\mathbb{X}]$ で定義された**超曲面** $V(f)$ とは

$$V(f) = \{a \in \mathbb{A}_k^n \mid f(a) = 0\} \subset \mathbb{A}_k^n$$

のことである**.**

定義 23. イデアル $I \subset k[\mathbb{X}]$ に対して

$$V(I) = \{a \in \mathbb{A}_k^n \mid f(a) = 0 \ (f \in I)\}$$

とおいて $V(I)$ を I によって定義された**アフィン代数多様体**と呼ぶ．また $\mathbb{A}_n^k$ の部分集合 V に対して

$$I(V) = \{f \in k[\mathbb{X}] \mid f(a) = 0 \ (a \in V)\}$$

を V の**零化イデアル**という．特に V が代数多様体のとき $I(V)$ を**定義イデアル**ともいう**.**

定義 24 (関数環)**.** アフィン代数多様体 $V \subset \mathbb{A}_k^n$ の定義イデアルをしたとき剰余環 $k[V] = k[\mathbb{X}]/I(V)$ を V の**関数環**と呼ぶ．商写像を

$$\varphi : k[\mathbb{X}] \quad \longrightarrow \quad k[V]$$

とするとき

$$x_i = \varphi(X_i)$$

で V 上の 1 次関数を表す**.**

補題 25. f を斉次既約多項式とする．f で生成された主イデアル (F) に対して $k[\mathbb{X}]/(f)$ への商写像を

$$k[\mathbb{X}] \quad \xrightarrow{\varphi} \quad k[\mathbb{X}]/(f)$$

と書く．このとき $a \in k[\mathbb{X}]$ が既約かつ $\deg(F) > \deg(a)$ ならば $\varphi(a)$ は $k[\mathbb{X}]/(f)$ 上既約である**.**

補題 26. f を斉次既約多項式とする．剰余環 $k[\mathbb{X}]/(f)$ の単元群は $(k[\mathbb{X}]/(f))^\times = k^\times$ である．

補題 25 と 26 は付録で証明する．

4 行列式で定義された関数環

n 次の**行列式多項式**を次のように書く $(n \geq 2)$.

$$\Delta_n(\mathbb{X}) = \sum_{\sigma \in S_n} (\mathrm{sgn}\ \sigma) X_{1,\sigma(1)} \dots X_{n,\sigma(n)} = \begin{vmatrix} X_{1,1} & X_{2,1} & \dots & X_{n,1} \\ X_{1,2} & X_{2,2} & \dots & X_{n,2} \\ \dots & \dots & \dots & \dots \\ X_{1,n} & X_{2,n} & \dots & X_{n,n} \end{vmatrix} \tag{1}$$

n 次の行列式 $\Delta_n(\mathbb{X})$ は n^2 変数であることに注意する．

4.1 $\Delta_n(\mathbb{X})$ の既約性

まず行列式多項式が既約であることを示そう．簡単な $n = 2$ の場合から証明を始める．

4.1.1 $n = 2$ のとき

命題 27. $\Delta_2(\mathbb{X})$ は既約多項式である．

(証明). 2 次の行列式が

$$\begin{vmatrix} X & Y \\ Z & W \end{vmatrix} = fg \qquad (f, g \in k[X, Y, Z, W]) \tag{2}$$

と分解したとすると $\deg(f) + \deg(g) = \deg(\Delta_2) = 2$ である．このとき $\deg(f)$ または $\deg(g) = 0$ ならば f または g が単元となる．そこで $\deg(f) = \deg(g) = 1$ のときを考え，

$$f = \alpha_1 X + \beta_1 Y + \gamma_1 Z + \delta_1 W$$

$$g = \alpha_2 X + \beta_2 Y + \gamma_2 Z + \delta_2 W$$

と表す．ここで $\alpha_1, \beta_1, \dots$ などは定数である．すると

$$\begin{aligned} fg &= (\alpha_2 X + \beta_2 Y + \gamma_2 Z + \delta_2 W)(\alpha_1 X + \beta_1 Y + \gamma_1 Z + \delta_1 W) \\ &= \alpha_1 \alpha_2 X^2 + \dots \end{aligned} \tag{3}$$

だが $\Delta_2 = XW - YZ = fg$ なので，$\alpha_1\alpha_2 = 0$ である．そこで $\alpha_2 = 0$ としても一般性を失わない．このとき $\alpha_1 \neq 0$ だから $\beta_2 = 0$ である．同様にして $\gamma_2 = 0$ を示すことができる．これを上の式に代入すると

$$\begin{aligned}\Delta_2 = fg &= (\alpha_1 X + \beta_1 Y + \gamma_1 Z + \delta_1 W)\delta_2 W \\ &= \alpha_1\delta_2 XW + \beta_1\delta_2 WY + \gamma_1\delta_2 WZ + \delta_1\delta_2 W^2\end{aligned}$$

だから $W|\Delta_2$ だがこれは矛盾．$\therefore \deg f = \deg g = 1$ は起こらない．以上より Δ_2 は既約多項式であることがわがった． □

4.1.2 一般の $n \geq 2$ の場合

命題 28. $\Delta_n(\mathbb{X})$ は既約多項式である．

(証明). Δ_n が

$$\Delta_n(\mathbb{X}) = \begin{vmatrix} X_{1,1} & X_{2,1} & \dots & X_{n,1} \\ X_{1,2} & X_{2,2} & \dots & X_{n,2} \\ \dots & \dots & \dots & \dots \\ X_{1,n} & X_{2,n} & \dots & X_{n,n} \end{vmatrix} = fg$$

と分解したとする．

まず $X_{1,1}$ を考える．もし $X_{1,1}$ が f の単項式の因子に現れるとすると，

$$f = X_{1,1}f_1 + f_2 \quad (f_1 \neq 0)$$

と書ける．ここで f_2 は $X_{1,1}$ を含まない単項式の和である．Δ_n は $X_{1,1}$ の一次式だから g の単項式には $X_{1,1}$ は現れない．次に Δ_n を 1 列目に関して余因子展開する．

$$\Delta_n = X_{1,1}\begin{vmatrix} X_{2,2} & \dots & X_{n,2} \\ \dots & \dots & \dots \\ X_{2,n} & \dots & X_{n,n} \end{vmatrix} - X_{1,2}\begin{vmatrix} X_{2,1} & \dots & X_{n,1} \\ \dots & \dots & \dots \\ X_{2,n} & \dots & X_{n,n} \end{vmatrix} + \dots$$

この式を見ると Δ_n ので単項式の因子は積 $X_{1,1}X_{1,2}$ を含まない．つまり，もし $X_{1,1}$ が f の単項式に現れるので g の単項式の因子は $X_{1,2}$ を含まない．同じ方法で g の単項式の因子は $X_{1,i}$ $(1 \leq i \leq n)$ を含まない．第 2 列目について余因子展開すると

$$\Delta_n = -X_{2,1}\begin{vmatrix} X_{1,2} & \dots & X_{n,2} \\ \dots & \dots & \dots \\ X_{1,n} & \dots & X_{n,n} \end{vmatrix} + X_{2,2}\begin{vmatrix} X_{1,1} & \dots & X_{n,1} \\ \dots & \dots & \dots \\ X_{1,n} & \dots & X_{n,n} \end{vmatrix} + \dots$$

2 列目の変数 $X_{2,j}$ $(1 \leq j \leq n)$ は全て f の単項式の因子に現れ g の単項式の因子には含まれない．

最後に，行列式の性質より，列を入れ替えると (± 1) 倍される．前の結果を使って，全ての変数 $X_{i,j}$ は f の単項式の因子に含まれることがわかる．従って g は変数をまったく含まない定数である．以上より Δ_n は既約である． □

4.2 $k[\mathbb{X}]/(\Delta_n)$ が一意分解整域かどうかの判定

$\Delta_n = \Delta_n(\mathbb{X})$ は既約斉次多項式なので補題 26 より $(k[\mathbb{X}]/(\Delta_n))^\times = k^\times$ である．これで剰余環 $k[\mathbb{X}]/(\Delta_n)$ の場合の単元群の問題 (3) が解決した．

$k[\mathbb{X}]$ が UFD だから Δ_n は素元であって (Δ_n) は素イデアルである．従って，剰余環 $k[\mathbb{X}]/(\Delta_n)$ は整域である．商写像を

$$\varphi : k[\mathbb{X}] \longrightarrow k[\mathbb{X}]/(\Delta_n)$$

で表す．

4.2.1 $k[\mathbb{X}]/(\Delta_2)$ が一意分解整域ではないこと

剰余環 $k[\mathbb{X}]/(\Delta_2) = k[X,Y,Z,W]/(XW - YZ)$ が一意分解整域ではないことを次の 2 つの主張 (1),(2) によって示す．

(1) $k[X,Y,Z,W]/(XW-YZ) = k[x,y,z,w]$ の元 x,y,z,w は既約である．ただし $x = \varphi(X), y = \varphi(Y), z = \varphi(Z), w = \varphi(W)$ と書いた．

(2) $rx \neq y, z$ $(r \in (k[\mathbb{X}]/(\Delta_2))^\times)$ である．つまり，$xw = yz$ は本質的に異なる 2 通りの既約元分解を与える．

(証明). 主張 (1) の証明: $x = fg$ $(f, g \in k[\mathbb{X}]/(\Delta_2))$ と書くと $k[\mathbb{X}]/(\Delta_2)$ は次数付き環だから，

$$\deg x = 1 = \deg f + \deg g \implies 0 \leq \deg f, \deg g \leq 1$$

が成り立つ．ここで $\deg f = 0$ としても一般性を失わない．$\deg g = 0$，これは $f \in k^\times$ が単元であることを意味している．同じ方法を使って y, z, w は既約元であることがわがる．

主張 (2) の証明: 背理法を使う．$rx = y$ と仮定する．

$$rx = y \implies rX - Y \in (XW - ZY) \subset k[X,Y,Z,W]$$

だが $XW - ZY$ は斉次二次式なので $rX - Y = 0$ でなければならず，矛盾である．

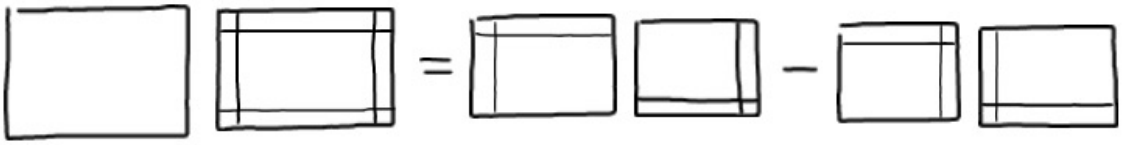
以上より剰余環 $k[\mathbb{X}]/(\Delta_2)$ は一意分解整域ではないことが示された． □

4.2.2 $k[\mathbb{X}]/(\Delta_n)$ $(n \geq 2)$ が一意分解整域ではないこと

$n \geq 3$ に対しても $k[\mathbb{X}]/(\Delta_n)$ は UFD でないが，その証明に必要な定理を準備する．

定理 29 (Desnanot-Jacobi 恒等式). $M = (X_{i,j})_{0 \leq i,j \leq n}$ が n 次正方行列のとき，次の等式が成り立つ．

$$|M||M^{1,n}_{1,n}| = |M^1_1||M^n_n| - |M^1_n||M^n_1| \qquad \text{(下図参照)} \tag{4}$$



ただし，$|M|$ は M の行列式，$|M_i^j|$ は M から i 行目と j 列目を除いた $(n-1)\times(n-1)$ 小行列の行列式を表す．この定理の証明は付録で行う．

定理 30. 剰余環 $k[\mathbb{X}]/(\Delta_n)$ は UFD でない．

(証明). Desnanot-Jacobi 恒等式より

$$(\Delta_n)(\Delta_n)^{1,n}_{1,n} = (\Delta_n)^1_1(\Delta_n)^n_n - (\Delta_n)^1_n(\Delta_n)^n_1$$

であるが，剰余環においては $\Delta_n = 0$ であるから $(\Delta_n)^1_1(\Delta_n)^n_n = (\Delta_n)^1_n(\Delta_n)^n_1$ が成り立つ．

$n = 2$ の場合と同じように次の 2 つの主張 (1),(2) を示せば良い．

(1) $k[\mathbb{X}]/(\Delta_n)$ において $(\Delta_n)^1_1, (\Delta_n)^n_n, (\Delta_n)^1_n, (\Delta_n)^n_1$ は既約である．

(2) $r \in (k[\mathbb{X}]/(\Delta_n))^\times$ を単元とするとき $r(\Delta_n)^1_1 \neq (\Delta_n)^1_n, (\Delta_n)^n_1$ である．

この (1), (2) が証明できれば $(\Delta_n)^1_1(\Delta_n)^n_n = (\Delta_n)^1_n(\Delta_n)^n_1$ は 2 通りの本質的に異なる既約元分解を与えることがわかり，従って $k[\mathbb{X}]/(\Delta_n)$ は UFD でないことがわかる．

主張 (1) は補題 25 を使えばよい．

主張 (2) も補題 26 を使いて，$n = 2$ のときと同様に示すことができる． □

4.3 剰余環 $k[\mathbb{X}]/(\Delta_2)$ とネーターの正規化定理

$n = 2$ のとき

$$k[X, Y, Z, W]/(XW - ZY) = k[x, y, z, w] \tag{5}$$
$$\varphi(X) = x,\ \varphi(Y) = y,\ \varphi(Z) = z,\ \varphi(W) = w$$

とおく．ネーター正規化定理の主張の (1), (2) を具体的に書くと，今の場合には次の (1), (2) になる．

(1) $\{x - w, y, z\}$ は k 上代数的独立である．($\because f(x - w, y, z) = 0), w = 0$ とすると $f(x, y, z) = 0 \implies f \equiv 0$)

(2) $k[x, y, z, w]$ は $B = k[x - w, y, z]$ 上整あって B 加群としての生成元として $\{1, x + w\}$ をとることができる．つまり

$$k[x, y, z, w] = k[x + w, y, z, x - w] = k[y, z, x - w](x + w) \oplus k[y, z, x - w]$$

が成り立つ．($\because (x + w)^2 - (x - w)^2 - 4zy = 4xw - 4zy = 0$)

5　楕円曲線と超楕円曲線

定義 31 (楕円曲線と超楕円曲線). $P(X)$ を X の多項式で重根を持たないものとする．このとき

$$Y^2 = P(X) \qquad (P(X)\text{ は X の多項式，重根を持たない})$$

で定義された曲線は $\deg P(X) = 3, 4$ のとき**楕円曲線**と呼ばれる．また $\deg P(X) \geq 5$ のときは**超楕円曲線**と言う．

5.1　奇数次の (超) 楕円曲線の関数環

$\deg P(X) = 2n+1$ $(n \in \mathbb{N})$ を奇数として，イデアル $I = (Y^2 - P(X))$ を考える．また

$$\begin{array}{ccc} k[X,Y] & \xrightarrow{\varphi} & k[X,Y]/(Y^2 - P(X)) \\ \cup & & \cup \\ a & \longmapsto & \varphi(a) = a + I \end{array}$$

を商写像，X,Y の φ による像を

$$x = \varphi(X)\ ,\quad y = \varphi(Y) \tag{6}$$

と書く．従って

$$k[X,Y]/(Y^2 - P(X)) = k[x,y] \tag{7}$$

である．

5.2　$k[x,y]$ の単元群

命題 32. 奇数次楕円曲線と超楕円曲線の関数環 $k[x,y]$ の単元群は $k^\times$ である．

(証明). $f, g \in k[x,y]$ に対して $fg = 1$ となったとする．$f = yf_1 + f_1,\quad g = yg_2 + g_2$ $(f_1, g_1, f_2, g_2 \in k[x])$ と表しておくと $fg = (yf_2 + g_2)(yf_1 + g_1) = 1$ だから $y^2 f_1 f_2 + (f_1 g_2 + f_2 g_1)y + g_1 g_2 = 1$，$y^2 = P(x)$ に代入して

$$(P(x))f_1 f_2 + g_1 g_2 + (f_1 g_2 + f_2 g_1)y = 1$$

$$\begin{cases} P(x)f_1 f_2 + g_1 g_2 = 1 \\ f_1 g_2 + f_2 g_1 = 0 \end{cases} \tag{8}$$

が成り立つ．この式より

$$\begin{cases} P \\ f_1 \\ f_2 \end{cases} \text{と} \begin{cases} g_1 \\ g_2 \end{cases} \text{は互い素} \implies \begin{cases} f_1 | f_2 \text{かつ } f_2 | f_1 \\ g_2 | g_1 \text{かつ } g_1 | g_2 \end{cases} \text{つまり} \begin{cases} f_1 = r f_2 \\ g_1 = t g_2 \end{cases} \quad (r, t \in k)$$

と表されている．一方

$$f_1g_2 = -f_2g_1 \implies rf_2g_2 + tf_2g_2 = 0 \quad \therefore (r+t)f_2g_2 = 0$$

従って $(r+t) = 0$ または $f_2g_2 = 0$ である．

(i) $f_2g_2 = 0$ のとき，f_2 または $g_2 = 0$ である ($f_2 = g_2 = 0$ はありえない)．$f_2 = 0,\ g_2 \neq 0$ のときは

$$fg = (yf_1 + g_1)g_2 = yf_1g_2 + g_1g_2 = 1 \tag{9}$$

これから $f_1 = 0$ かつ $g_1,\ g_2 \in k[x]^\times = k^\times$ である．

$$f_2 \neq 0,\ g_2 = 0$$

のときは

$$1 = (yf_1 + g_1)yf_2 = y^2f_1f_2 + g_1yf_2$$

だから $g_1 = 0$ かつ $1 = P(x)f_1f_2$ となり矛盾 ($\because$ 1 は $P(x)$ で割り切れない)．

(ii) $(r+t) = 0$ のとき．$t = -r$ になる．つまり

$$yf_1 + g_1 = (yrf_2 - rg_2) = r(yf_2 - g_2)$$

である．これを最初の式に代入すると，

$$\begin{aligned} fg &= (f_1y + g_1)(f_2y + g_2) = r(f_2y + g_2)(f_2y - g_2) \\ &= r(y^2f_2^2 - g_2^2) = r(P(x)f_2^2 - g_2^2) = 1 \end{aligned}$$

である．次数を比較すると $\deg P + 2\deg f_2 = \deg(1 + g_2^2)$ となるが左辺の次数は奇数で，右辺は偶数なので矛盾する．

(i), (ii) より $f = f_2, g = g_2 \in k^\times$ であることがわかる． □

5.3 奇数次の (超) 楕円曲線の関数環と一意分解性

k は代数閉体とする．ここでは $P(X)$ が奇数モニック多項式，つまり $\deg P(X) = 2n + 1\ (n \in \mathbb{N})$ の場合を考える．k は代数閉体だから

$$P(X) = (X - a_1)(X - a_2)(X - a_3)\dots(X - a_{2n+1})$$

と因数分解できる．ここで $a_i \in k\ (i = 1, 2, 3\dots, 2n+1)$ は相異なる根である．

楕円曲線の関数環が **UFD ではない**ことを次の 2 つの主張 (1),(2) によって示そう．剰余環を $k[x,y] = k[X,Y]/(Y^2 - P(X))$ と書くのであった．

(1) $k[x,y]$ の元 $y, x - a\ (a \in k)$ は既約である．

(2) $y^2 = (x - a_1)(x - a_2)(x - a_3)\dots(x - a_{2n+1})$ は $k[x,y]$ において本質的に異なる 2 通りの既約分解である．つまり単元 $r \in k^\times$ に対して $ry \neq x - a$ である．

5.3.1 y が既約であることの証明

(証明). $y = fg$ と分解したとする.

$$f = f_1 + yf_2,\ \ g = g_1 + yg_2 \quad (f_i, g_i \in k[x], i = 1, 2)$$

とおく，このとき，

$$\begin{aligned} y = fg &= (f_1 + yf_2)(g_1 + yg_2) = f_1g_1 + y(f_1g_2 + f_2g_1) + y^2f_2g_2 \\ &= P(x)f_2g_2 + f_1g_1 + y(f_1g_2 + f_2g_1) \end{aligned}$$

なので，係数を比較して

$$\begin{cases} P(x)f_2g_2 + f_1g_1 = 0 \\ f_1g_2 + f_2g_1 = 1 \end{cases} \iff \begin{cases} P(x)f_2g_2 = -g_1f_1 \\ f_1g_2 = 1 - f_2g_1 \end{cases}$$

である．両辺の次数を比較して

$$\begin{cases} 2n + 1 + \deg(f_2g_2) = \deg(g_1f_1) \\ \deg(f_1g_2) = \deg(1 - f_2g_1) \end{cases} \tag{10}$$

(i) f_2g_1 が定数のとき.このときは $f_1g_2 = 1 - f_2g_1$ も定数で f_i, g_i は全て定数となる．また $P(X)f_1f_2 = -g_1g_2$ より $f_1f_2 = g_1g_2 = 0$ がわかる．従って f_1, f_2 のうち一方は 0，g_1, g_2 も一方は 0 である.

$f_1 = 0$ なら，$f_2g_1 = 1$ より $g_1 \neq 0$．従って $g_2 = 0$ である．これより $f = yf_2, g = g_1$ であって，$g \in k_\times$ は単元.

$f_2 = 0$ なら．同様にして $f_1 \in k^\times$ は単元である.

(ii) f_2g_1 が定数でないとき.このときは

$$\deg(f_1g_2) = deg(f_2g_1 - 1) = deg(f_2g_1)$$

だから，式 (10) より

$$\begin{cases} 2n + 1 + \deg f_1 + \deg f_2 = \deg g_1 + \deg g_2 \\ \deg f_1 + \deg g_2 = \deg f_2 + \deg g_1 \end{cases}$$

辺々を引き算して整理すると，

$$2n + 1 + 2\deg f_2 = 2\deg g_2$$

だが，左辺は奇数で右辺は偶数でから矛盾．従って (ii) の場合は起こりえない.

(i) (ii) より f または g は単元となるので，y は既約である. □

5.3.2　$x-a\ (a\in k)$ が既約であることの証明

(証明). $x-a=fg$ とする.

$$f=f_1+yf_2,\ \ g=g_1+yg_2\quad (f_i,g_i\in k[x],i=1,2)$$

とおく. このとき,

$$x-a=fg=(f_1+yf_2)(g_1+yg_2)=f_1g_1+y(f_1g_2+f_2g_1)+P(x)f_2g_2$$

なので, 係数を比較して

$$\begin{cases} P(x)g_2f_2+g_1f_1=x-a \\ f_1g_2+f_2g_1=0 \end{cases} \tag{11}$$

である.

(i) $f_2g_2\neq 0$ の時, $\deg P(x)=2n+1\geq 3$ なので, 式 (11) の最高次の係数を比較して

$$\begin{cases} 2n+1+\deg(g_2f_2)-\deg(g_1f_1)=0 \\ \deg(f_1g_2)-\deg(f_2g_1)=0 \end{cases} \tag{12}$$

となるが, §5.3.1 の証明と同様に考えると, これは $\deg P(x)=2n+1$ が奇数であることに矛盾する. つまり (i) は起こり得ない.

(ii) $f_2g_2=0$ の時, $f_2=0$ ならば $f_1\neq 0$ なので (11) の第二式より $g_2=0$ である. 従って $x-a=f_1g_1$ だが, $f_1,\ g_1\in k[x]$ なので $f_1\in k^\times$ または $g_1\in k^\times$ である.

(i) (ii) より f または g は単元となるので. $x-a$ は既約である. □

定理 33. 奇数次の超楕円曲線の関数環は UFD ではない.

(証明). $y^2=(x-a_1)(x-a_2)(x-a_3)\dots(x-a_{2n+1})$ が異なる既約元分解であることを示せばよい. つまり, $r\in k^\times$ を単元とする時, $ry\neq x-a$ であることを示す. 元の $k[X,Y]$ で考えるよう.

実際 $m(Y^2-P(X))\in I\ (m\in k[X,Y])$ の元は 0 でなければ常に $(2n+1)$ 次以上なので $rY-(X-a)$ に一致することはない.

つまり $y^2=(x-a_1)\dots(x-a_{2n+1})$ は異なる既約元分解である. □

6　円 $(X^2+Y^2=1)$ 上の関数環

$\mathrm{char}(k)\neq 2$ のとき X^2+Y^2-1 は既約多項式である. 従って剰余環 $k[X,Y]/(X^2+Y^2-1)$ は整域である. 商写像を

$$\varphi : k[X,Y]\longrightarrow k[X,Y]/(X^2+Y^2-1) \tag{13}$$

と書く. またいつものように

$$\varphi(X)=x,\qquad \varphi(Y)=y$$

$k[X,Y]/(X^2+Y^2-1)=k[x,y]$ と表す.

6.1 複素数体上の円

$k = \mathbb{C}$ のとき考える．$x^2 + y^2 = (x + iy)(x - iy)$ より，座標変換

$$\begin{cases} x - iy = u \\ x + iy = v \end{cases} \iff \begin{cases} u + v = 2x \\ u - v = -2iy \end{cases}$$

と行うと，$uv = 1$ であって $v = u^{-1}$ が成り立つ．従って，

$$k[X, Y]/(X^2 + Y^2 - 1) = k[x, y] \cong k[u, u^{-1}]$$

である．

補題 34. 環 $k[u, u^{-1}]$ は PID である．(従って UFD である．)

(証明). $k[u, u^{-1}]$ はネーターである[1]．だからイデアル $I \subset k[u, u^{-1}]$ に対して，有限個の $\{f_1, f_2, \ldots, f_n\}$ $(f_i \in k[u, u^{-1}])$ が存在して $(f_1, f_2, \ldots, f_n) = I$ が成り立つ．$f_i = g_i/u_i^m$ $(g_i \in k[u],\ m_i \in \mathbb{N})$ とすると u^{-1} は単元だから

$$I = (f_1, \ldots, f_n) = (g_1, \ldots, g_n)$$

である．$k[u]$ は UFD だから $\{g_1, \ldots, g_n\}$ を $k[u]$ で考えると $(g_1, \ldots, g_n) = (d)$ となる多項式 $d \in k[u]$ が存在する．これを $k[u, u^{-1}]$ で考えると，$(d) = I$ であることがわかる．つまり $k[u, u^{-1}]$ は PID である． □

補題 35. $k[u, u^{-1}]^\times$ は巡回群 $\mathbb{Z}$ と $\mathbb{C}^\times$ の直積に同型である．

(証明). $f, g \in k[x, y]$ に対して $fg = 1$ となったとする．

$$f = \frac{f_1}{u^{m_f}},\ \ g = \frac{g_1}{u^{m_g}},\ \ (f_1, g_1 \in k[u],\ m_f, m_g \in \mathbb{N})$$

と表しておくと

$$fg = \frac{f_1}{u^{m_f}} \frac{g_1}{u^{m_g}} = 1 \implies \frac{f_1}{u^{m_f}} \frac{g_1}{u^{m_g}} = \frac{f_1 g_1}{u^{m_f + m_g}} = 1$$

である．つまり $f_1 g_1 = u^{m_f + m_g}$ が成り立つ．$f_1 g_1 = u^{m_f + m_g}$ を $k[u]$ の中で考えて $k[u]$ が UFD であることに注意すると $f_1 = u^d,\ g_1 = u^{m_g + m_f - d}$ となる (定数倍はうまく調整すればよい)．だから $k[u, u^{-1}]^\times$ は巡回群 $\mathbb{Z}$ と $\mathbb{C}^\times$ の直積に同型である． □

[1] 付録 A.3 を参考

6.2 超球面の場合

超球面上の関数環

$$A_n = k[X_1, \ldots, X_n]/(X_1^2 + \cdots + X_n^2 - 1) \quad (n \geq 2)$$

を $k = \mathbb{R}$ または $k = \mathbb{C}$ の場合に考える．次の定理が Swan によって得られている．

定理 36 (Theorem 5(2)[Swan]). 関数環 A_n を $k = \mathbb{C}$ 上で考えるときは $A_{n,\mathbb{C}}$, $\mathbb{R}$ で考えるときは $A_{n,\mathbb{R}}$ と書く．

(1) $k = \mathbb{C}$ のとき

(a) $n = 3$ のとき $A_{3,\mathbb{C}}$ は UFD ではない．

(b) $n \geq 2, n \neq 3$ のとき $A_{n,\mathbb{C}}$ は UFD である．

(2) $k = \mathbb{R}$ のとき

(a) $n = 2$ のとき $A_{2,\mathbb{R}}$ は UFD ではない．

(b) $n \geq 3$ のとき $A_{n,\mathbb{R}}$ は UFD である．

$n = 2$ のとき $A_{2,\mathbb{C}}$ が UFD で $A_{2,\mathbb{R}}$ が UFD でないことは永田によって代数的な議論で証明させた．

7 将来の展望

今後は $A = k[\mathbb{X}]/(Y^2 - P(X))$ が $\deg P(X) = 2n(n \geq 2)$ のときにまず A の単元群と UFD かどうかを判定する (例えば $A = k[\mathbb{X}]/(Y^2 - X^4 - 1)$)。超楕円曲線上の関数環の単元群と超幾何関数の関係についても研究中である。その後の勉強は，代数学と複素解析で手に入れると思います．機会があれば，楕円曲線論も勉強してみます．

8 謝辞

最後に本卒業研究にて，一年間ご指導をして下さった西山先生に御礼申し上げ たいと思います．多忙である中，論文添削と証明のヒントをしてくれて，誠にありがとうございました．また後期代数学 III の寺田先生と解析学 V の時弘先生も感謝します．卒業研究発表会において助言をいただき，増田先生，谷口先生に感謝致します. 半年間を共に過ごした須永君と中川君に感謝します. 文法の問題をたくさん指摘してくれてありがどうございます．この四年間を一緒に過ごした物理数理の皆様，ありがとうございました．

A　付録

A.1　Desnanot-Jacobi 恒等式の証明

定義 37. X は $n \times n$ 行列，$|X|$ は X の行列式．$|X_i^j|$ は X から i 行目と j 列目を除いた $(n-1) \times (n-1)$ 行列の行列式．

定理 38.

$$|X||X_{1,n}^{1,n}| = |X_1^1||X_n^n| - |X_n^1||X_1^n| \tag{14}$$

(証明). (by D. M. Bressoud [Bressoud])

$X = (x_{i,j})_{i,j=1}^n$，$a_{i,j} = (-1)^{i+j}\det(X_i^j)$ とする．

$$X' = \begin{vmatrix} a_{1,1} & 0 & 0 & ... & 0 & 0 & a_{n,1} \\ a_{1,2} & 1 & 0 & ... & 0 & 0 & a_{n,2} \\ a_{1,3} & 0 & 1 & 0 & ... & 0 & a_{n,3} \\ ... & ... & ... & ... & ... & ... & ... \\ a_{1,n-1} & 0 & ... & 0 & 1 & 0 & a_{n,n-2} \\ a_{1,n-1} & 0 & 0 & ... & 0 & 1 & a_{n,n-1} \\ a_{1,n} & 0 & 0 & ... & 0 & 0 & a_{n,n} \end{vmatrix} \tag{15}$$

$det(X') = a_{1,1}a_{n,n} - a_{n,1}a_{1,n} = |X_1^1||X_n^n| - |X_n^1||X_1^n|$

$$XX' = \begin{vmatrix} det(X) & x_{1,2} & x_{1,3} & ... & x_{1,k-2} & x_{1,k-1} & 0 \\ 0 & x_{2,2} & x_{2,3} & ... & x_{2,k-2} & x_{2,k-1} & 0 \\ 0 & x_{3,2} & x_{3,3} & ... & x_{3,k-2} & x_{3,k-1} & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & x_{k-2,2} & x_{k-2,3} & ... & x_{k-2,k-2} & x_{k-2,k-1} & 0 \\ 0 & x_{k-1,2} & x_{k-1,3} & ... & x_{k-1,k-2} & x_{k-1,k-1} & 0 \\ 0 & x_{k,2} & x_{k,3} & ... & x_{k,k-2} & x_{k,k-1} & det(X) \end{vmatrix} \tag{16}$$

この式より

$$det(XX') = det(X)det(X') \Longrightarrow |X|^2|X_{1,n}^{1,n}| = |X|(|X_1^1||X_n^n| - |X_n^1||X_1^n|) \tag{17}$$

両辺の $|X|$ を消して，$|X||X_{1,n}^{1,n}| = |X_1^1||X_n^n| - |X_n^1||X_1^n|$ である． □

A.2　次数環の定義と性質

定義 39. A が環であり，$\mathbb{Z}$ 加群として $A = \oplus_{n=0}^{\infty} A_n$ と部分加群の直和になっていて，$A_nA_m \subset A_{n+m}$ となるとき，A を次数環という．

定義 40. 次数環 A 上の加群 M が $M = \oplus_{n=0}^{\infty} M_n$ と部分 $\mathbb{Z}$ 加群の直和になっていて，$A_n M_m \subset M_{n+m}$ となるとき，M を次数 A 加群という．

定義 41. 上の定義の状況で M の部分 A 加群 N が $N = \oplus_{n\in\mathbb{Z}}(N \cap M_n)$ となるとき，斉次部分加群という．A のイデアル I が A の斉次部分加群であるとき，I を斉次イデアルという．

定義 42. $B = \oplus_{n=0}^{\infty} B_n$ が次数環，A が B の部分環で，$A = \oplus_{0\leq}(A \cap B_n)$ となるとき，A を斉次部分環と言う．

定義 43. 最初の定義で $a_i \in A_i$ $(i = 0, \ldots, d), a = a_0 + \cdots + a_d$ で $a_d \neq 0$ なら，d のことを a の次数といい $\deg a$，あるいは $\deg_A a$ と書く．

補題 44. $A = \oplus_{n=0}^{\infty} A_n$ が次数環で，$I = \oplus_{n=0}^{\infty} I_n$ が斉次イデアルであるとき，A/I も A_n/I_n を n 次成分とする次数環になる．

(証明). A/I は次のように表す

$$A \quad \xrightarrow{\varphi} \quad A/I$$

$\mathrm{Ker}\varphi = \oplus_{n=0}^{\infty} I_n = I$,$\mathrm{Im}\varphi = A/I \Longrightarrow A/I \cong \oplus_{n=0}^{\infty} A_n/I_n$
$a_i + I_i \in A_i/I_i, a_j + I_j \in A_j/I_j$

$$(A_i/I_i)(A_j/I_j) = (a_i + I_i)(a_j + I_j) = a_i a_j + a_i I_j + I_i a_j + I_i I_j$$

$a_i a_j \in a_{i+j}, a_i I_j + I_i a_j + I_i I_j \in I_{i+j} \Longrightarrow a_i I_j + I_i a_j + I_i I_j \in A_{i+j}/I_{i+j}$ 上の定義より A/I も A_n/I_n を n 次成分とする次数環である．

□

A.3 補題の証明

補題 45 (2)**.** f が斉次既約多項式とする，(f) は f で生成された主イデアル．$k[\mathbb{X}]/(f)$ の単元群 $(k[\mathbb{X}]/(f))^{\times} = k^{\times}$

(証明). f は斉次多項式だから，$k[\mathbb{X}]/(f)$ は次数付き環になる．a を単元とすると．$ab = 1$ となる b がある．このとき，両辺の次数を比較すると $\deg(a)+\deg(b)=\deg(1)=0 \Rightarrow \deg(a)=\deg(b)=0$, つまり $a \in k^{\times}$ がわかる． □

補題 46 (1)**.** F が斉次既約多項式とする，(F) は F で生成された主イデアル．$k[\mathbb{X}]/(F)$ は次のように定義する．

$$k[\mathbb{X}] \quad \xrightarrow{\varphi} \quad k[\mathbb{X}]/(F)$$

このとき $a \in k[\mathbb{X}]$ が既約かつ $\deg(F) > \deg(a) \Longrightarrow \varphi(a)$ は $k[\mathbb{X}]/(F)$ 上既約.

(証明). まず $\deg F = n$ $(n \geq 1)$ とする．ここで背理法を使う，$a = fg + P(X,Y)F$ を仮定する．ここで f, g, P の次数を考える．ここで f, g, P の次数を考える．

$$f = f_0 + f_1 + \cdots + f_v (degf_i = i, i = 0, 1, \ldots, v)$$

$$g = g_0 + g_1 + \cdots + g_w (degf_i = i, i = 0, 1, \ldots, w)$$

$$P = P_0 + P_1 + \cdots + P_u (degf_i = i, i = 0, 1, \ldots, u)$$

つまり

$$fg = (f_0 g_0 + 1 \text{ 次以上})$$

$$PF = P_0 F + P_1 F + P_2 F + \cdots + P_u F$$

$\deg(P_0 F) = n$ より

$$fg = (F + \text{n 次以上})$$

つまり

$$f_0 g_0 = 0, f_1 g_0 + f_0 g_1 = 0, f_2 g_0 + f_0 g_2 + f_1 g_1 = 0, \ldots$$

ここで，$g_0 = 0$ としてもよい．$f_1 g_0 + f_0 g_1 = 0$ ので，$g_1 = 0$．同様にして

$$g_0 = 0, g_1 = 0, g_2 = 0, \ldots, g_{n-2} = 0$$

$-f_v g_w = P_u F \Longrightarrow F | f_v$ または $F | g_w$．$Fa = f_v$ または $Fb = g_w$，ここで $Fb = g_w$ としても一般性を失わない．

$$gf = (g_0 + g_1 + \cdots + g_w)(f_0 + f_1 + \cdots + f_v) = (g_0 + g_1 + \cdots + Fb)(f_0 + f_1 + \cdots + f_v)$$

$$(g_0+g_1+\cdots+Fb)(f_0+f_1+\cdots+f_v) = (g_0+g_1+\cdots+g_{w-1})(f_0+f_1+\cdots+f_v)+Fb(f_0+f_1+\cdots+f_v)$$

$$(g_0 + g_1 + \cdots + g_{w-1})(f_0 + f_1 + \cdots + f_v) + Fb(f_0 + f_1 + \cdots + f_v) = (P_0 + \cdots + P_u)F$$

$$(g_0+g_1+\cdots+g_{w-1})(f_0+f_1+\cdots+f_v)+\Delta B(f_0+f_1+\cdots+f_v) = (P_0+\cdots+P_u-Bf_0-\ldots Bf_v)\Delta$$

　すると，初めから $g = g_0 + g_1 + \cdots + g_{w-1}$ としてよい，$\deg f + \deg g$ に関する帰納法を使う証明すれば良い．　□

A.4　ネーター環の定義と応用

定義 47. 環 A について，次の条件は同値である．

(1) 任意のイデアル $I \subset A$ は有限生成である．すなわち，任意のイデアル $I \subset A$ に対して，$f_1, \ldots, f_k \in I$ が存在して，$I = (f_1, \ldots, f_k)$ となる．

(2) A のイデアルの任意の増加列

$$I_1 \subset \cdots \subset I_m \subset \ldots$$

は途中から一定となる．すなわち，$I_N = I_{N+1} = \ldots$ となる N がある．(これを昇鎖条件を満たす)

(3) 空でないイデアルの族の中に極大元が存在する．

これらの条件が成り立つとき，A をネーター環という．

(証明). (1) $\Longrightarrow$ (2) を示す．イデアルの列 $I_1 \subset \cdots \subset I_m \subset \ldots$ が与えられたとする．$I = \cup I_m$ とおくと，明らかに I もイデアルであるから，(1) より $f_1, \ldots, f_k$ をとって $I = (f_1, \ldots, f_k)$ とできる．各 i に対して，$f_i \in I_{m_i}$ となる m_i があるから，$N = \max\{m_i\}$ とおけば $I = I_N$ となり，I_N から先では列は一定となる．

(2) $\Longrightarrow$ (3) ツォルンの補題より明らか．

(3) $\Longrightarrow$ (1) I を任意のイデアルとする．$\Sigma = \{J \subset I \mid J$ は有限生成イデアル $\}$ とおくと．(3) より Σ には極大元がある．それを J_0 とする．このとき，$J_0 = I$ となる．($\because$ もしそうでないとすると $\forall f \in I - J_0$ をとり，イデアル $Af + J_0$ を作ると，これも有限生成で I に含まれ，しかも J_0 より真に大きくなるからである．) つまり任意のイデアル $I \subset A$ は有限生成である． □

命題 48. A をネーター環とし，$I \subset A$ をイデアルとする．このとき，剰余環 $B = A/I$ もネーターとなる．

命題 49. A をネーター整域 (すなわち，ネーター環で 0 以外の元は零因子を持たない環) とし，K を A の商体とする．A の 0 を含まない部分集合 S に対して，

$$B = A[S^{-1}] = \{\frac{a}{b} \in K \mid a \in A, b \text{ は } 1 \text{ または } S \text{ の元の積}\}$$

とおくと，B もネーター環となる．

参考文献

[Reid] Miles Reid, Undergraduate Algebraic Geometry，Cambridge University Press 1988

[Silverman] Joseph H. Silverman, Rational Points on Elliptic Curves, New York, Springer-Verlag, 1992

[雪江 1] 雪江 明彦，代数学 2 環と体とガロワ理論，日本評論社，2010/12/7

[雪江 2] 雪江 明彦，代数学 3 代数学のひろがり，日本評論社，2011/3/16

[堀田 1] 堀田 良之，現代数学の基礎 11 環と体 1，岩波書店，1997/10/29

[堀田 2] 堀田 良之，加群十話，朝倉書店，1988/10/1

[堀田 3] 堀田 良之，代数入門: 群と加群，裳華房，1987/9/20

[原岡 1] 原岡 喜重，超幾何関数，朝倉書店，2002/10/1

[成田 1] 成田 正雄，イデアル論入門，共立出版 復刊版，2009/7/9

[川口 1] 川口周，代数学入門，日本評論社，2017/9/25

[Nagata] Masayoshi Nagata, A remark on the unique factorization theorem, 1957

[Bressoud] D. M. Bressoud, Proofs and Confirmations: The Story of the Alternating Sign Matrix Conjecture, MAA Spectrum, Mathematical Associations of America, Washington, D.C., 1999

[Swan] Richard G. Swan, Vector Bundles and Projective Modules, American Mathematical Society, Vol. 105, No. 2 (Nov., 1962)

[Stack1] Georges Elencwajg, URL:https://mathoverflow.net/questions/5591/are-quotients-of-polynomial-rings-almost-ufds

[Stack2] URL:https://math.stackexchange.com/questions/536624/is-the-localization-of-a-pid-a-pid