1　はじめに

環というときは単位元を持つ可換環を意味するものとします．また，**部分環**というときはもとの環と単位元 1 を共有するものとします．したがってイデアルは部分環と考えません．**環準同型**というときは，環準同型写像であって，単位元の像が単位元であるものとします．環の上の**加群**を考えるときは，環の単位元は恒等写像として加群に作用するものとします．

環 R のイデアル $\mathfrak{a}, \mathfrak{b}$ に対して，$\mathfrak{a} \cap \mathfrak{b}$ は R のイデアルです．また，

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a},\, b \in \mathfrak{b}\},$$
$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{j=1}^{r} a_j b_j \,\middle|\, a_j \in \mathfrak{a},\, b_j \in \mathfrak{b},\, r = 1, 2, \ldots \right\},$$
$$\mathfrak{a} : \mathfrak{b} = \{x \in R \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$$

とおきます．これらは R のイデアルです．それぞれ $\mathfrak{a}, \mathfrak{b}$ の**和**，**積**，**商**といいます．

R のイデアルからなる集合族 $\{\mathfrak{a}_\lambda\}$ に対して，$\bigcup_\lambda \mathfrak{a}$ より生成されるイデアルを $\sum_\lambda \mathfrak{a}_\lambda$ と書きます．有限個のイデアル $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ について，$\mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_n$ で生成されるイデアルと $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ とは一致します．

2　素イデアル

R を環とします．

定理 2.1.　R のイデアル $\mathfrak{p} \neq R$ について次の条件はすべて同値である：

(i)　R の元 a, b について，$ab \in \mathfrak{p}$ ならば，$a \in \mathfrak{p}$ または $b \in \mathfrak{p}$ である．

(ii)　R のイデアル $\mathfrak{a}, \mathfrak{b}$ について，$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ ならば，$\mathfrak{a} \subseteq \mathfrak{p}$ または $\mathfrak{b} \subseteq \mathfrak{p}$ である．

(iii)　剰余環 $R/\mathfrak{p}$ は整域である．

定義 2.2.　上の定理の条件を満たす R のイデアル $\mathfrak{p} \neq R$ を**素イデアル** (prime ideal) という．

- R の零イデアルが素イデアル $\Longleftrightarrow$ R が整域.

命題 2.3.　Q を環とし，R を Q の部分環とする．$\mathfrak{p}$ が Q の素イデアルであるとき，$\mathfrak{p} \cap R$ は R に等しいか，または R の素イデアルである．

命題 2.4.　$f : R \longrightarrow R'$ を環準同型とする．$\mathfrak{p}$ が R' の素イデアルならば，$f^{-1}(\mathfrak{p})$ は R の素イデアルである．

命題 2.5.　$f : R \longrightarrow R'$ を全射環準同型とする．$\mathfrak{p}$ が R の素イデアルであって，$\mathrm{Ker}\, f \subseteq \mathfrak{p}$ ならば，$f(\mathfrak{p})$ は R' の素イデアルである．

命題 2.6. $\mathfrak{a}$ を R のイデアルとし，$\pi : R \longrightarrow R/\mathfrak{a}$ を自然な全射準同型とする．$\mathfrak{a}$ を含む R の素イデアル全体を $\mathcal{P}$ とし，剰余環 $R/\mathfrak{a}$ の素イデアル全体 $\mathcal{P}'$ とすれば，写像

$$\Phi : \mathcal{P} \longrightarrow \mathcal{P}', \quad \mathfrak{p} \longmapsto \pi(\mathfrak{p})$$

は全単射である．逆写像は

$$\Psi : \mathcal{P}' \longrightarrow \mathcal{P}, \quad \mathfrak{p}' \longmapsto \pi^{-1}(\mathfrak{p}')$$

である．さらに，R の素イデアル $\mathfrak{p}_1, \mathfrak{p}_2$ に対して，

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \Longleftrightarrow \Phi(\mathfrak{p}_1) \subseteq \Phi(\mathfrak{p}_2)$$

が成り立つ．

3 極大イデアル

R を環とします．

定理 3.1. R のイデアル $\mathfrak{m} \neq R$ について次の条件は同値である：

(i) R のイデアル $\mathfrak{a}$ について，$\mathfrak{m} \subseteq \mathfrak{a} \subsetneq R$ ならば $\mathfrak{m} = \mathfrak{a}$ である．

(ii) 剰余環 $R/\mathfrak{m}$ は体である．

定義 3.2. 上の定理の条件を満たす R のイデアル $\mathfrak{m} \neq R$ を**極大イデアル** (maximal ideal) という．

- R の極大イデアル $\mathfrak{m}$ は素イデアルである．

命題 3.3. $f : R \longrightarrow R'$ を全射環準同型とする．$\mathfrak{m}$ が R の極大イデアルならば，$f^{-1}(\mathfrak{m})$ は R の極大イデアルである．

定理 3.4. $\mathfrak{a}$ を R のイデアルとし，S を R の部分集合で

- $S \neq \phi$,
- $a, b \in S \Longrightarrow ab \in S$,
- $\mathfrak{a} \cap S = \phi$

なる条件を満たすものとする．このとき R のイデアルの集合

$$\mathcal{F} = \{\mathfrak{b} \mid \mathfrak{a} \subseteq \mathfrak{b} \subsetneq R, \, \mathfrak{b} \cap S = \phi\}$$

について次のことが成り立つ：

(i) $\mathcal{F}$ には包含関係に関する極大元が存在する．

(ii) $\mathcal{F}$ の極大元の任意の 1 つを $\mathfrak{p}$ とすれば，$\mathfrak{p}$ は R の素イデアルである．

証明.

(i) 少なくとも $\mathfrak{a} \in \mathcal{F}$ であるから $\mathcal{F}$ は空でない．また，イデアルの包含関係による順序により $\mathcal{F}$ は順序集合になる．$\mathcal{F}$ が帰納的集合であることを示すために，$\{K_\lambda \mid \lambda \in \Lambda\}$ を $\mathcal{F}$ の空でない任意の全順序集合とする．$K = \bigcup_{\lambda\in\Lambda} K_\lambda$ とおくと，K は $\{K_\lambda \mid \lambda \in \Lambda\}$ の $\mathcal{F}$ における上界である．なぜなら K は $\mathfrak{a}$ を含む R のイデアルであり，

$$K_\lambda \cap S = \phi\ (\forall\lambda \in \Lambda) \Longrightarrow K \cap S = \phi$$

より $K \in \mathcal{F}$ だからである．これで $\mathcal{F}$ が帰納的集合であることが示された．したがって Zorn の補題により $\mathcal{F}$ の極大元が存在する．

(ii) まず

$$\mathfrak{a} \subseteq \mathfrak{p} \subsetneq R, \qquad \mathfrak{p} \cap S = \phi$$

であることに注意する．いま仮に，$b \notin \mathfrak{p}$, $c \notin \mathfrak{p}$, $bc \in \mathfrak{p}$ であるとする．$\mathfrak{b} = (b)+\mathfrak{p}$, $K = (c)+\mathfrak{p}$ とすれば，$\mathfrak{p} \subsetneq \mathfrak{b}$, $\mathfrak{p} \subsetneq K$ であるから $\mathfrak{p}$ の極大性により $\mathfrak{b} \cap S \neq \phi$, $K \cap S \neq \phi$ でなければならない．よって S の元 s_1, s_2 が存在して

$$s_1 = r_1 b + u_1, \qquad s_2 = r_2 c + u_2 \qquad (\exists r_1, \exists r_2 \in R,\ \exists u_1, \exists u_2 \in \mathfrak{p})$$

と表される．このとき

$$s_1 s_2 = r_1 r_2 bc + r_1 b u_2 + r_2 c u_1 + u_1 u_2 \in \mathfrak{p}.$$

ゆえに $s_1 s_2 \in \mathfrak{p} \cap S$．これは $\mathfrak{p} \cap S = \phi$ に反する．

□

系 3.4.1. 任意のイデアル $\mathfrak{a} \neq R$ に対して，$\mathfrak{a}$ を含む R の極大イデアル $\mathfrak{m}$ が存在する．

証明. $S = \{1\}$ とすれば，R のイデアル $\mathfrak{b}$ について

$$\mathfrak{b} \cap S = \phi \Longleftrightarrow 1 \notin \mathfrak{b} \Longleftrightarrow \mathfrak{b} \neq R.$$

したがって $\mathcal{F} = \{\mathfrak{b} \mid \mathfrak{a} \subseteq \mathfrak{b} \subsetneq R\}$ に極大元 $\mathfrak{m}$ が存在する．$\mathfrak{m}$ は $\mathfrak{a}$ を含む R の極大イデアルである． □

系 3.4.2. 任意の環 R に対して，R の極大イデアル $\mathfrak{m}$ は少なくとも一つ存在する．

証明. $\mathfrak{a} = (0)$ として系 3.4.1 を適用すればよい． □

4　商環

定義 4.1.　R の部分集合 S が**積閉** (multiplicatively closed) であるとは

(i)　$1 \in S$,

(ii)　$x, y \in S \Longrightarrow xy \in S$

が成り立つことをいう．

例 4.2.　R の元 $x \neq 0$ に対して，$S = \{x^n \mid n = 0, 1, 2, \ldots\}$ とおけば，S は積閉集合である．

例 4.3.　S を R から零元と零因子を除いた集合とすると，S は積閉である．特に，R が整域ならば，$S = R\backslash\{0\}$ は積閉集合である．

例 4.4.　$\mathfrak{p}$ を R の素イデアルとするとき，$S = R\backslash\mathfrak{p}$ は積閉集合である．

R の積閉部分集合 S が与えられたとき，直積集合 $R \times S$ における関係 $\sim$ を

$$(x, s) \sim (y, t) \Longleftrightarrow \exists u \in S \;\; s.t. \;\; u(xt - ys) = 0$$

と定義します．$\sim$ は同値関係になります．$\sim$ による商集合 $R \times S/\sim$ を $S^{-1}R$ で表します．また，(x, s) を代表元とする同値類を x/s と書きます．

$S^{-1}R$ の二つの元 $x/s, y/t$ の和および積を

$$\frac{x}{s} + \frac{y}{t} = \frac{xt + ys}{st},$$
$$\frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st}$$

によって定義します．これらの定義は同値類の代表元の取り方によりません．この和と積に対して，$S^{-1}R$ は $0/1$ を零元，$1/1$ を単位元とする可換環になります．

定義 4.5.　$S^{-1}R$ を，R の S による**商環**あるいは**分数環** (quotient ring) という．

- $x \in R$ と $s \in S$ について，$x/s = 0/1 \Longleftrightarrow \exists t \in S \;\; s.t. \;\; tx = 0$.
- $S^{-1}R = \{0/1\} \Longleftrightarrow 0 \in S$.
- $\mathfrak{a}$ が R のイデアルであるとき，$\mathfrak{a}S^{-1}R = \{x/s \mid x \in \mathfrak{a}, s \in S\}$ は $S^{-1}R$ のイデアルである．

S, T を R の積閉部分集合とし，$S \subseteq T$ とします．このとき，写像

$$S^{-1}R \longrightarrow T^{-1}R, \quad \frac{x}{s} \longmapsto \frac{x}{s}$$

は単射準同型です．したがって $S^{-1}R \subseteq T^{-1}R$ とみなすことができます．

定義 4.6. S を R から 0 と零因子を除いた集合とする．このとき商環 $S^{-1}R$ を，R の**全商環** (total quotient ring) と呼ぶ.

- R が整域のとき，R の全商環は体になる.

定義 4.7. 整域 R の全商環を**商体** (quotient field) と呼ぶ.

例 4.8. 有理整数環 $\mathbb{Z}$ の商体は有理数体 $\mathbb{Q}$ である.

例 4.9. 体 K 上の n 変数多項式環 $K[X_1, \ldots, X_n]$ は整域である．その商体を $K(X_1, \ldots, X_n)$ と書き，体 K 上の n 変数の**有理関数体** (rational function field) と呼ぶ.

写像

$$f_S : R \longrightarrow S^{-1}R, \quad x \longmapsto \frac{x}{1}$$

は環準同型であり，

$$\mathrm{Ker}\, f_S = \{x \in R \mid \exists s \in S \ \ s.t. \ \ sx = 0\}.$$

特に，$S^{-1}R$ が全商環のとき，$\mathrm{Ker}\, f_S = \{0\}$ なので f_S は単射になり，R を $S^{-1}R$ の部分環とみなすことができます.

命題 4.10. 整域 R の商体は，R を部分環として持つ体のうちで最小のものである.

命題 4.11. S を R の積閉集合とするとき，$f_S(S) \subseteq (S^{-1}R)^{\times}$.

定理 4.12 (普遍性). S を R の積閉集合とし，f_S を上で定めた単射環準同型とする．環 R' と，$f(S) \subseteq (R')^{\times}$ なる環準同型 $f : R \longrightarrow R'$ に対して，環準同型 $g : S^{-1}R \longrightarrow R'$ がただ一つ存在して，$f = g \circ f_S$ を満たす.

命題 4.13. S を R の積閉部分集合とし，$f_S : R \longrightarrow S^{-1}R$ を上で定義した単射環準同型とする．S との共通部分が空であるような R の素イデアル全体を $\mathcal{P}$ とし，$S^{-1}R$ の素イデアル全体を $\mathcal{P}'$ とすれば，写像

$$\Phi : \mathcal{P} \longrightarrow \mathcal{P}', \quad \mathfrak{p} \longmapsto f_S(\mathfrak{p})\, S^{-1}R$$

は全単射である．逆写像は

$$\Psi : \mathcal{P}' \longrightarrow \mathcal{P}, \quad \mathfrak{p}' \longmapsto f_S^{-1}(\mathfrak{p}')$$

である．さらに，R の素イデアル $\mathfrak{p}_1, \mathfrak{p}_2$ に対して，

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \Longleftrightarrow \Phi(\mathfrak{p}_1) \subseteq \Phi(\mathfrak{p}_2)$$

が成り立つ.

5　局所環

R を環とします.

定義 5.1.　極大イデアルが有限個しかない環を**半局所環** (semi-local ring) という．とくに，極大イデアルがただ一つしかない環を**局所環** (local ring) という.

命題 5.2.　環 R について，次の二つの条件は同値である：

(i)　R は局所環である.

(ii)　R と異なる R のイデアルの中に最大のものが存在する.

証明.

(i)⇒(ii)　環 R の R 以外の任意のイデアルに対して，そのイデアルを含む極大イデアルが必ず存在する．極大イデアルがたた一つということから R 以外のすべてのイデアルはその極大イデアルに含まれることになる．よってその極大イデアルが R と異なるイデアルのうちで最大のものとなる.

(ii)⇒(i)　R と一致しない最大のイデアルは，たた一つの極大イデアルである.　□

注意 5.3.　証明中に用いた「環 R の R 以外の任意のイデアルに対して，そのイデアルを含む極大イデアルが必ず存在する」という命題を示すためには Zorn の補題を必要とする.

命題 5.4.　R を局所環とし，$\mathfrak{m}$ を R の極大イデアルとする．このとき $\mathfrak{m}$ は単元以外のすべての R の元からなる.

証明.　もし仮に $\mathfrak{m}$ が単元を含むならば $\mathfrak{m}$ は R と一致する．これは仮定に矛盾する．よって $\mathfrak{m}$ は単元を含まない．したがって $\mathfrak{m}$ の元はすべて単元ではない.

逆に，R の単元ではない任意の元を a とする．a の生成する単項イデアル (a) は R と一致しない．ゆえに (a) は $\mathfrak{m}$ に包まれる．よって a は $\mathfrak{m}$ に含まれる.　□

命題 5.5.　環 R の単元でない元の全体が R のイデアルならば，それは R と一致しない R のイデアルのうちで最大のものである．特に，R は局所環である.

証明.　単元でない元の全体を R_0 とする．仮定により R_0 は R のイデアルであり，少なくとも単位元は R_0 に属さないから $R_0 \subsetneq R$ である.

いま仮に R のイデアル $\mathfrak{a}$ で $\mathfrak{a} \not\subseteq R_0$ となるものが存在したとする．このとき $\mathfrak{a}$ は単元 a を含むから，$\mathfrak{a}$ は R に一致する．ゆえに，R 自身を除く R のイデアルはすべて R_0 に包まれる．すなわち R_0 は R と一致しない R のイデアルの中で最大のものである.　□

例 5.6.　体 K は局所環である．K と一致しない最大のイデアルは零イデアル (0) である.

例 5.7. p を素数とする．p 進整数環 $\mathbb{Z}_p$ は局所環である．$\mathbb{Z}_p$ を除くイデアルのうちで最大のものは $p\mathbb{Z}_p$ である．

例 5.8. 体 K を係数とする一変数の形式的冪級数

$$f(X) = \sum_{n=0}^{\infty} a_n X^n, \quad a_n \in K$$

の全体 $R = K[[X]]$ は局所環であり，R と一致しない最大のイデアルは X により生成される単項イデアル (X) である．実際，

$$f(X) \text{ が } R \text{ の単元} \iff a_0 \text{ が } K \text{ の単元}$$

である．K は体だから，0 以外の K の元はすべて単元である．ゆえに，(X) は R の単元でない元の全体である．ゆえに命題 5.5 から R が局所環であることがわかる．

例 5.9. K を体とし，$R = K[[X_1, \ldots, X_n]]$ を n 変数の形式的冪級数環とする．
$R = (K[[X_1, \ldots, X_{n-1}]])[[X_n]]$ であることを用いると，$f \in R$ について，

$$\begin{aligned}
f \text{ が } R \text{ の単元} &\iff f \text{ の } X_n \text{ を含まない項からなる部分が } K[[X_1, \ldots, X_{n-1}]] \text{ の単元} \\
&\iff f \text{ の } X_{n-1}, X_n \text{ を含まない項からなる部分が } K[[X_1, \ldots, X_{n-2}]] \text{ の単元} \\
&\iff \cdots\cdots \\
&\iff f \text{ の定数項が } K \text{ の単元}
\end{aligned}$$

である．K は体だから，0 以外の K の元はすべて単元である．ゆえに，$X_1, \ldots, X_n$ で生成されるイデアル $(X_1, \ldots, X_n)$ は定数項を持たない R の元の全体であるから，単元ではない R の元の全体である．ゆえに R は局所環であり，$(X_1, \ldots, X_n)$ がただ一つの極大イデアルである．

R を環とし，$\mathfrak{p}$ を R の素イデアルとします．$S = R \backslash \mathfrak{p}$ は積閉集合になります．このとき，R の S による商環

$$R_{\mathfrak{p}} = S^{-1}R = \left\{ \frac{x}{s} \;\middle|\; x \in R, \, s \in R \backslash \mathfrak{p} \right\}$$

は局所環になります．$R_{\mathfrak{p}}$ のたた一つの極大イデアルは

$$\mathfrak{p}R_{\mathfrak{p}} = \left\{ \frac{x}{s} \;\middle|\; x \in \mathfrak{p}, \, s \in R \backslash \mathfrak{p} \right\}$$

です．

定義 5.10. $R_{\mathfrak{p}}$ を素イデアル $\mathfrak{p}$ による R の**局所化** (localization) という．

例 5.11. 有理整数環 $\mathbb{Z}$ の (2) による局所化は

$$\mathbb{Z}_{(2)} = \left\{ \frac{b}{a} \in \mathbb{Q} \;\middle|\; a, b \in \mathbb{Z}, \; a \text{ は奇数} \right\}$$

である．

6　一意分解整域

この節では，R は整域であると仮定します．

定義 6.1.　R の元 a, b に対して，R のある元 c が存在して $a = bc$ と表されるとき，a を b の**倍元** (multiple)，b を a の**約元**あるいは**因子** (divisor) であるといい，このことを $a \mid b$ という記号で表す.

定義 6.2.　また，R のある単元 u が存在して $a = bu$ となるとき，a と b とは**同伴** (associate) であるという.

命題 6.3.　同伴は同値関係である.

証明.　a, b, c を R の元とし，u, v を R の単元とする.

反射法則：R の単位元 1 は単元であり，$a = a \cdot 1$.

対称法則：$a = bu$ ならば $b = au^{-1}$.

推移法則：$a = bu, b = cv$ とすれば $a = cvu$，vu は単元.　□

命題 6.4.　整域 R の二つの元 a, b について，次の二つの条件は同値である.

(i)　a と b とは同伴である.

(ii)　$a \mid b$ かつ $b \mid a$ が成り立つ.

証明.

(i)⇒(ii)　a, b が同伴ならば，ある単元 u によって $a = bu$．よって $b \mid a$．またこのとき $b = au^{-1}$ であるから $a \mid b$.

(ii)⇒(i)　$a \mid b$ かつ $b \mid a$ ならば，R の元 x, y が存在して $a = bx, b = ay$ となる．よって

$$b = bxy \qquad \therefore b(1 - xy) = 0.$$

$b = 0$ のときは $a = 0$ であるから a と b とは同伴である．$b \neq 0$ のときは $xy = 1$ となり，x, y ともに単元である．よってこの場合も a と b とは同伴である.　□

定義 6.5.　整域 R の 0 でも単元でもない元 a について，分解 $a = bc$ があれば，b または c が単元になるとき，a は**既約元** (irreducible element) であるという.

命題 6.6.　整域 R の二つの元 p, q について，p と q とが同伴ならば

$$p \text{ は既約元である} \iff q \text{ は既約元である}$$

証明． p が既約元ならば，p は 0 でも単元でもない．よって p と同伴な q もまた 0 でも単元でもない．

p の元 a について $a \mid q$ ならば $a \mid p$．p は既約だから a は単元であるか，または p と同伴である．a と p とが同伴ならば，p と q とが同伴だから a と q も同伴である．ゆえに q は既約元である．逆も同様． □

定義 6.7. 整域 R の 0 でも単元でもない元 a について

$$a \mid bc \Longrightarrow a \mid b \text{ または } a \mid c$$

が成り立つとき，a を**素元** (prime element) という．

命題 6.8. 整域 R の素元はすべて既約元である．

証明． p を素元とする．R の元 a について $a \mid p$ とすると，R の元 b が存在して $p = ab$ と書ける．p は素元だから $p \mid a$ または $p \mid b$ である．R が整域であれば，$a \mid p$ かつ $p \mid a$ のとき a と p とは同伴である．$p \mid b$ ならば，R の元 c が存在して $b = pc$ と書けるから，$p = pac$．$p \neq 0$ かつ R は整域だから $1 = ac$．ゆえに a は単元である．したがって p は既約元である． □

命題 6.9. 整域 R の二つの元 p, q について，p と q とが同伴ならば

$$p \text{ は素元である} \Longleftrightarrow q \text{ は素元である}$$

証明． p が素元ならば p は 0 でも単元でもない．よって p と同伴な q もまた 0 でも単元でもない．

R の元 a, b について，$q \mid ab$ ならば $p \mid ab$ である．p は素元だから $p \mid a$ または $p \mid b$．したがって $q \mid a$ または $q \mid b$．ゆえに q は素元である．逆も同様． □

定義 6.10. 整域 R の元 $a_1, \ldots, a_n$ が与えられたとき，すべての a_i の約元になる元を $a_1, \ldots, a_n$ の**公約元** (common divisor) という．公約元であって，すべての公約元の倍元になるものを**最大公約元** (greatest common divisor) という．

定義 6.11. 整域 R の元 $a_1, \ldots, a_n$ が与えられたとき，すべての a_i の倍元になる元を $a_1, \ldots, a_n$ の**公倍元** (common multiple) という．公倍元であって，すべての公倍元の約元になるものを**最小公倍元** (least common multiple) という．

定義 6.12. 整域 R の元 a, b について，それらの最大公約元が R の単位元であるとき，a と b とは**互いに素** (relatively prime) であるという．

定義 6.13. 整域 R が次の性質を満たすとき，R は**一意分解整域** (unique factorization domain) であるという．

(i) 0 でも単元でもない任意の元 a に対して，有限個の既約元 $p_1, \dots, p_r$ が存在して $a = p_1 \cdots p_r$ と表される．

(ii) (i) のような分解は一意的である．すなわち，既約元 $p_1, \dots, p_r$ と既約元 $q_1, \dots, q_s$ について，$p_1 \cdots p_r = q_1 \cdots q_s$ であれば $r = s$ であり，番号をつけかえれば，すべての i について p_i と q_i とは互いに同伴になる．

注意 6.14. 一意分解整域のことを，素元分解整域あるいは素元分解環などと呼ぶこともある．また，一意分解整域を UFD と呼ぶこともある．UFD は unique factorization domain の略である．

注意 6.15. 一意分解整域の定義における条件 (i)，(ii) は，次のように述べても同じである．

(i$'$) 0 でない任意の元 a は，単元 u と有限個の既約元 $p_1, \dots, p_r$ $(r \geq 0)$ によって $a = up_1 \cdots p_r$ と表される．

(ii$'$) 単元 u, v，既約元 $p_1, \dots, p_r$ と既約元 $q_1, \dots, q_s$ について，$up_1 \cdots p_r = vq_1 \cdots q_s$ であれば $r = s$ であり，$r \geq 1$ のとき，番号をつけかえれば，すべての i について p_i と q_i とは互いに同伴である．

定理 6.16. R が一意分解整域であるための必要十分条件は，次の二つの条件を満たすことである．

(i) R の 0 でも単元でもない元 x はすべて，有限個の既約元 $p_1, \dots, p_r$ によって

$$x = p_1 p_2 \cdots p_r$$

と表される．

(ii) R の既約元は素元である．

例 6.17. 有理整数環 $\mathbb{Z}$ は一意分解整域である．単元は ± 1 である．既約元と素元とは一致し，$\pm p$ (p は素数) なるものが既約元のすべてである．

命題 6.18. 一意分解整域においては，最大公約元，最小公倍元は必ず存在する．

7 一意分解整域上の多項式環

定義 7.1. 一意分解整域 R 上の多項式

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

の係数 $a_0, \dots, a_n$ の最大公約元を f の**内容** (content) といい，$c(f)$ で表す.

定義 7.2. $c(f)$ が単元であるような多項式 $f \in R[X]$ を**原始多項式** (primitive polynomial) という．

命題 7.3. R を一意分解整域とし，$f(X)$ を $R[X]$ の 0 でない多項式とする．

(i) $f(X)$ は $c(f)$ と原始多項式との積として表される．

(ii) $f(X)$ が $R[X]$ の既約元で $\deg f \geq 1$ ならば $f(X)$ は原始多項式である．

証明.

(i) $f(X) = a_0 + a_1X + \cdots + a_nX^n$ とする．$a_i = c(f)b_i$, $b_i \in R$ とおくと，$b_0, b_1, \ldots, b_n$ は互いに素だから，$f_1(X) := b_0 + b_1X + \cdots + b_nX^n$ は原始多項式であって，$f(X) = c(f)f_1(X)$.

(ii) $f(X)$ が $R[X]$ の既約元で $\deg f \geq 1$ であるとする．$c(f) \mid f(x)$ で，$\deg c(f) = 0$ だから $c(f)$ と $f(X)$ とは同伴ではない．ゆえに $c(f)$ は単元である．よって $f(X)$ は原始的である．

□

定義 7.4. K が体のとき，K の 0 でない元はすべて $K[X_1, \ldots, X_n]$ の単元である．したがって，$f \in K[X_1, \ldots, X_n]$ が既約元であることと f が次数の低い多項式の積に分解しないこととは同値である．この場合，既約元は**既約多項式** (irreducible polynomial) と呼ばれる．

定理 7.5 (Gauss). 一意分解整域 R 上の多項式環 $R[X]$ において，二つの原始多項式の積は原始多項式である．

証明. $f(X) = a_0 + a_1X + \cdots + a_mX^m$, $g(X) = b_0 + b_1X + \cdots + b_nX^n$ が原始多項式であって，

$$f(X)g(X) = c_0 + c_1X + \cdots + c_{m+n}X^{m+n}, \qquad c_k = \sum_{k=i+j} a_ib_j$$

が原始多項式ではないとして矛盾を導く．

$f(X)g(X)$ が原始多項式でなければ，$c_0, \ldots, c_{m+n}$ をすべて割る既約元 p が存在する．$f(X)$, $g(X)$ は原始多項式であるから，ある番号 s, t ($0 \leq s \leq m$, $0 \leq t \leq n$) が存在して

$$p \mid a_0, \quad \ldots, \quad p \mid a_{s-1}, \quad p \nmid a_s, \quad p \mid b_0, \quad \ldots, \quad p \mid b_{t-1}, \quad p \nmid b_t$$

であり，$p \nmid a_sb_t$ である．

$$c_{s+t} = \cdots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \cdots$$

だから $p \nmid c_{s+t}$．これは仮定に反する．したがって $f(X)g(X)$ は原始的である． □

定理 7.6. 一意分解整域 R の商体を K とする．R の元を係数とする多項式 $f(X)$ が $K[X]$ において

$$f(X) = g_1(X)h_1(X) \qquad g_1,\ h_1 \in K[X]$$

のように二つの多項式の積に分解すれば，$f(X)$ は $R[X]$ において次のように二つの多項式の積に分解する：

$$\begin{aligned} &f(X) = g(X)h(X) \qquad g,\ h \in R[X], \\ &\deg g = \deg g_1, \quad \deg h = \deg h_1. \end{aligned}$$

定理 7.7. 一意分解整域 R 上の多項式環 $R[X]$ の元 f について次の条件は同値である．

(1) f は $R[X]$ の素元である．

(2) f は R の素元または原始多項式である．

定理 7.8. R を一意分解整域とすれば，$R[X]$ も一意分解整域である．

定理 7.9. R を一意分解整域，K を R の商体, $Q = R[X_1, \ldots, X_n]$ を n 変数の多項式環とする．

(1) Q は一意分解整域である．

(2) Q の素元は R の素元 p または $K[X_1, \ldots, X_n]$ において既約な Q の原始多項式である．

定理 7.10. 一意分解整域 R の商体を K とする．R の元を係数とする n 変数の多項式 $f(X_1, \ldots, X_n)$ が $K[X_1, \ldots, X_n]$ において

$$f(X_1, \ldots, X_n) = g_1(X_1, \ldots, X_n)h_1(X_1, \ldots, X_n) \qquad g_1,\ h_1 \in F[X_1, \ldots, X_n]$$

のように二つの多項式の積に分解するならば，$f(X_1, \ldots, X_n)$ は $R[X_1, \ldots, X_n]$ において二つの多項式の積に分解する：

$$\begin{aligned} &f(X_1, \ldots, X_n) = g(X_1, \ldots, X_n)h(X_1, \ldots, X_n) \qquad g,\ h \in R[X_1, \ldots, X_n], \\ &\deg g = \deg g_1, \quad \deg h = \deg h_1. \end{aligned}$$

定理 7.11 (Eisenstein). R を一意分解整域とし，K を R の商体とする．$R[X]$ の元

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$$

について，R の既約元 p で

$$p \nmid a_0, \qquad p \mid a_i,\ (i = 1, \ldots, n), \quad p^2 \nmid a_n$$

となるものが存在すると仮定する．このとき，$f(X)$ は $K[X]$ における既約多項式である．

証明. R 係数の多項式 $f(X)$ について

$$\begin{aligned} f(X) &= g(X)h(X), \qquad g(X),\, h(X) \in R[X], \\ g(X) &= b_0X^n + b_1X^{n-1} + \cdots + b_n, \qquad b_i \in R, \\ h(X) &= c_0X^n + c_1X^{n-1} + \cdots + c_n, \qquad c_i \in R \end{aligned}$$

とおく．$a_n = b_nc_n$, $p \mid a_n$, $p^2 \nmid a_n$ であるから，b_n, c_n はどちらか一方だけが p で割り切れる．

そこで $p \mid b_n$, $p \nmid c_n$ とすれば，$a_{n-1} = b_nc_{n-1} + b_{n-1}c_n$, $p \mid a_{n-1}$ から $p \mid b_{n-1}$ がいえる．一般に

$$a_k = b_nc_k + b_{n-1}c_{k+1} + \cdots + b_kc_n \quad (0 \leq k \leq n)$$

と書けるから，$1 \leq j \leq n$ に対して，$p \mid b_j$ がいえる．

いま仮に $b_0 = 0$ とすれば，$a_0 = b_nc_0 + b_{n-1}c_1 + \cdots + b_1c_{n-1}$ の右辺は p で割り切れるから，$p \mid a_0$ である．しかしながらこれは仮定に反する．よって $b_0 \neq 0$．すなわち $\deg g = n$ となり，$f(X)$ は $n-1$ 次以下の多項式の積にはならない．ゆえに $f(X)$ は $R[X]$ において既約になる．したがって $f(X)$ は $K[X]$ においても既約になる． □

命題 7.12. R を一意分解整域とし，K を R の商体とする．R 係数の多項式 $f(X)$ と R の元 a に対して

$$f(X) \text{ が既約} \iff f(X+a) \text{ が既約}$$

が成り立つ．

証明. $f(X) = g(X)h(X)$, $\deg g > 0$, $\deg h > 0$ とすれば，R の任意の元 a に対して

$$f(X+a) = g(X+a)h(X+a)$$

である．よって $f(X)$ が可約であれば，$f(X+a)$ も可約である．同様にして，$f(X-a)$ が可約であれば，$f(X)$ も可約である．よって a の代わりに $-a$ とみれば，逆も示されたことになる． □

例 7.13. p が素数のとき

$$X^{p-1} + X^{p-2} + \cdots + X + 1$$

は $\mathbb{Q}[X]$ における既約多項式である．

証明. $f(X) = X^{p-1} + \cdots + X + 1$ とおく．

$$f(X) = \frac{X^p - 1}{X - 1}$$

であるから

$$\begin{aligned} f(X+1) &= \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + pX^{p-2} + \cdots + \binom{p}{r} X^{p-r-1} + \cdots + p \end{aligned}$$

一方

$$\binom{p}{r} = \frac{p!}{r!(p-r)!} \in \mathbb{Z}, \qquad p \nmid r!(p-r)! \qquad \therefore\ p \mid \binom{p}{r}$$

よって Eisenstein の定理から $f(X+1)$ が既約，したがって $f(X)$ も既約である． □

8　Noether 環

R を環とします.

定義 8.1.　$(A, \leq)$ を順序集合とする．A の元 a が**極大元**であるとは,

$$a < x \text{ となるような } A \text{ の元 } x \text{ が存在しない}$$

という条件を満たすことをいう.

命題 8.2.　環 R について，次の 3 つの条件は同値である：

(i)　任意のイデアルの単調増加列

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots$$

に対して，ある番号 n_0 があって

$$n \geq n_0 \Longrightarrow \mathfrak{a}_n = \mathfrak{a}_{n_0}.$$

(ii)　$\mathfrak{A} \neq \phi$ を R のイデアルからなる任意の集合とするとき，$\mathfrak{A}$ は包含関係 $\subseteq$ に関して極大元をもつ．すなわち，あるイデアル $\mathfrak{a}_0 \in \mathfrak{A}$ があって，$\mathfrak{a} \in \mathfrak{A}$ に対して，もし $\mathfrak{a}_0 \subseteq \mathfrak{a}$ ならば $\mathfrak{a} = \mathfrak{a}_0$ となる.

(iii)　R の任意のイデアルは有限生成である．すなわち，R の任意のイデアル $\mathfrak{a}$ は，R の有限個の元 $a_1, a_2, \ldots, a_n$ によって $\mathfrak{a} = Ra_1 + \cdots + Ra_n$ と表される.

証明.

(i)⇒(ii)　もし仮に (ii) が成り立たないとすると，R のイデアルからなる空でない集合で極大元をもたないものが存在する．それを $\mathfrak{A}$ とする．$\mathfrak{A}$ の元を 1 つとり，それを $\mathfrak{a}_1$ とする．$\mathfrak{a}_1$ は $\mathfrak{A}$ の極大元ではないので，$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$ なる $\mathfrak{a}_2 \in \mathfrak{A}$ が存在する．$\mathfrak{a}_2$ もまた $\mathfrak{A}$ の極大元ではないので，$\mathfrak{a}_2 \subsetneq \mathfrak{a}_3$ なる $\mathfrak{a}_3 \in \mathfrak{A}$ が存在する．以下同様に繰り返せば，R のイデアルの無限列

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_n \subsetneq \cdots$$

が存在することになり，(i) に矛盾する.

(ii)⇒(iii)　$\mathfrak{a}$ を R の任意のイデアルとする．$\mathfrak{a}$ に含まれる有限生成イデアル全体からなる集合を $\mathfrak{A}$ とする．$\mathfrak{A} \ni (0)$ だから $\mathfrak{A} \neq \phi$ である．ゆえに (ii) から $\mathfrak{A}$ は極大元 $\mathfrak{a}_0$ をもつ．もし，$\mathfrak{a}_0 \subsetneq \mathfrak{a}$ ならば，$a \in \mathfrak{a} - \mathfrak{a}_0$ をとり，イデアル $Ra + \mathfrak{a}_0$ を $\mathfrak{a}_1$ と書くと，$\mathfrak{a}_0$ は有限生成だから $\mathfrak{a}_1$ も有限生成であり，$\mathfrak{a}_1 \subseteq \mathfrak{a}$ だから $\mathfrak{a}_1 \in \mathfrak{A}$ である．一方，$\mathfrak{a}_0 \subsetneq \mathfrak{a}_1$ だから，これは $\mathfrak{a}_0$ の定め方に矛盾する．ゆえに $\mathfrak{a} = \mathfrak{a}_0$ であり，$\mathfrak{a}$ は有限生成である.

(iii)⇒(i)　R のイデアルの増加列

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots$$

を任意にとる．このとき，$\mathfrak{a} = \bigcup_{n=1}^{\infty} \mathfrak{a}_n$ は R のイデアルである．実際，$\alpha, \beta \in \mathfrak{a}$ ならば，ある番号 n_1, n_2 があって $\alpha \in \mathfrak{a}_{n_1}$, $\beta \in \mathfrak{a}_{n_2}$ である．$n = \max\{n_1, n_2\}$ とすれば，$\alpha, \beta \in \mathfrak{a}_n$ であるから，$\alpha - \beta \in \mathfrak{a}_n \subseteq \mathfrak{a}$ となる．ゆえに I は加法群として R の部分群である.

また，任意の $r \in R,\ \alpha \in \mathfrak{a}$ に対して，ある番号 n があって，$\alpha \in \mathfrak{a}_n$ であるから，$r\alpha \in \mathfrak{a}_n \subseteq \mathfrak{a}$ である．ゆえに $\mathfrak{a}$ は R のイデアルである．

(iii) より $\mathfrak{a}$ は有限生成である．そこで $a_1, \cdots, a_r \in R$ を $\mathfrak{a}$ の生成元とすると，各 i について，ある番号 n_i がとれて $a_i \in \mathfrak{a}_{n_i}$ である．$n_0 = \max\{n_1, \ldots, n_r\}$ とおけば，$a_1, \cdots, a_r \in \mathfrak{a}_n$ であるから $\mathfrak{a} = \mathfrak{a}_n$ である．ゆえに $n \geq n_0$ なる任意の番号 n について，$\mathfrak{a}_n = \mathfrak{a} = \mathfrak{a}_{n_0}$ である． □

定義 8.3. 環 R が上の定理の条件 (i)〜(iii) をみたすとき，R を **Noether 環**という[1]．条件 (i) を**昇鎖条件**，条件 (ii) を**極大条件**という．

例 8.4. 単項イデアル環は Noether 環である．よって例えば，体，有理整数環 $\mathbb{Z}$，p 進整数環 $\mathbb{Z}_p$ などは Noether 環である．

定理 8.5 (Cohen). 環 R が Noether 環であるための必要十分条件は，R のすべての素イデアルが有限生成であることである．

命題 8.6. R, R' を環，$f : R \longrightarrow R'$ を準同型写像とする．このとき，R が Noether 環ならば，f の像 $f(R)$ も Noether 環である．

証明. $f(R)$ の任意のイデアルを $\mathfrak{a}$ とする．$\mathfrak{a}$ の逆像 $f^{-1}(\mathfrak{a})$ は R のイデアルであるから，ある有限個の元 $a_1, a_2, \ldots, a_n$ で生成されている．このとき $\mathfrak{a} = f(f^{-1}(\mathfrak{a}))$ は $f(a_1), \cdots, f(a_n)$ で生成される． □

例 8.7. R を Noether 環，$\mathfrak{a}$ を R のイデアルとする．自然な準同型 $f : R \longrightarrow R/\mathfrak{a},\ x \longmapsto x + \mathfrak{a}$ を考えれば，命題 8.6 により剰余環 $R/\mathfrak{a}$ も Noether 環であることがわかる．さらに，命題 8.6 の証明を見ればわかるように R が単項イデアル環ならば $R/\mathfrak{a}$ も単項イデアル環である．

命題 8.8. R を環とし，$\mathfrak{a}$ を R のイデアルとする．$\mathfrak{a}$ に含まれる R のイデアルがすべて有限生成であり，かつ $R/\mathfrak{a}$ が Noether 環ならば，R は Noether 環である．

証明. R の任意のイデアル $\mathfrak{b}$ が有限生成であることを示せばよい．$\mathfrak{b} \subseteq \mathfrak{a}$ のときは明らかなので，$\mathfrak{b} \not\subseteq \mathfrak{a}$ とする．

自然な準同型 $\pi : R \longrightarrow R/\mathfrak{a}$ を考えると，$\pi(\mathfrak{a} + \mathfrak{b})$ は $R/\mathfrak{a}$ のイデアルだから有限生成である．よって

$$\pi(\mathfrak{a} + \mathfrak{b}) = (\pi(a_1), \ldots, \pi(a_n)), \quad a_i \in \mathfrak{a} + \mathfrak{b}$$

と書け，さらに

$$a_i = b_i + c_i, \quad b_i \in \mathfrak{a}, \quad c_i \in \mathfrak{b}$$

[1] Noether はネーターと読みます．人名です．

と書ける．また，$\mathfrak{a}\cap\mathfrak{b}$ は $\mathfrak{a}$ に含まれる R のイデアルだから有限生成である．よって

$$\mathfrak{a}\cap\mathfrak{b}=(d_1,\dots,d_m),\quad d_i\in\mathfrak{a},\quad c_i\in\mathfrak{b}$$

と書ける．このとき

$$\mathfrak{b}=(c_1,\dots,c_n,d_1,\dots,d_m)$$

が成り立つ．実際，$\supseteq$ は明らかである．$\subseteq$ は

$$\begin{aligned}
x\in\mathfrak{b} &\Longrightarrow \pi(x)\in\pi(\mathfrak{a}+\mathfrak{b})\\
&\Longrightarrow \pi(x)=\sum_{i=1}^{n}\pi(x_i)\pi(a_i)=\sum_{i=1}^{n}\pi(x_i)\pi(b_i+c_i),\quad x_i\in R\\
&\Longrightarrow \pi(x-\sum_{i=1}^{n}x_ib_i-\sum_{i=1}^{n}x_ic_i)=0\quad (0\text{ は }R/\mathfrak{a}\text{ の零元})\\
&\Longrightarrow x-\sum_{i=1}^{n}x_ib_i-\sum_{i=1}^{n}x_ic_i\in\mathfrak{a}\\
&\Longrightarrow x-\sum_{i=1}^{n}x_ic_i\in\mathfrak{a}\cap\mathfrak{b}\\
&\Longrightarrow x-\sum_{i=1}^{n}x_ic_i=\sum_{i=1}^{n}y_id_i,\quad y_i\in R\\
&\Longrightarrow x\in(c_1,\dots,c_n,d_1,\dots,d_m)
\end{aligned}$$

よりわかる．したがって，$\mathfrak{b}$ は有限生成である． □

命題 8.9. R_1, …, R_n が Noether 環ならば，環の直和 $R_1\oplus\cdots\oplus R_n$ も Noether 環である．

証明． $n=2$ のとき，$R=R_1\oplus R_2$, $\mathfrak{a}=\{(x,0)\in R\mid x\in R_1\}$ とおく．$\mathfrak{a}$ は R のイデアルであり，$\mathfrak{a}\cong R_1$, $R/\mathfrak{a}\cong R_2$ である．

$\mathfrak{a}$ に含まれる R のイデアルは，R_1 のイデアルと 1 対 1 に対応するから，有限生成である．また，R_2 は Noether 環だから，$R/\mathfrak{a}$ も Noether 環である．ゆえに命題 8.8 により，R も Noether 環である．

$n\geq 3$ のときは，

$$R_1\oplus\cdots\oplus R_n=(R_1\oplus\cdots\oplus R_{n-1})\oplus R_n$$

に注意すれば，n に関する帰納法によって命題が示せる． □

定理 8.10 (Hilbert の基底定理). R が Noether 環であれば，n 変数多項式環 $R[X_1,X_2,\dots,X_n]$ も Noether 環である．

証明． まず，1 変数のときを証明する．

$R[X]$ に有限生成でないイデアル $\mathfrak{a}\neq(0)$ が存在したとして矛盾を導く．$\mathfrak{a}$ の 0 でない元の中で次数が最小のものを f_1 とする．$\mathfrak{a}$ は有限生成ではないので，$\mathfrak{a}\backslash(f_1)\neq\phi$ である．そこで，$\mathfrak{a}\backslash(f_1)$ の元の中で次数が最小のものを f_2 とする．一般に，f_1, …, f_{k-1} まで定まったとして，$f_k\in\mathfrak{a}$ を $\mathfrak{a}\backslash(f_1,\dots,f_{k-1})$ の元の中で次数が最小のものとする．このとき

$$\deg f_j\leq\deg f_{j+1}\quad(j=1,2,\dots)$$

である．各 f_j の最高次の係数を a_j とおくと，R のイデアルの増加列

$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots \subseteq (a_1, \ldots, a_k) \subseteq \cdots$$

が得られる．R は Noether 環であるから，ある N が存在して

$$(a_1, \ldots, a_N) = (a_1, \ldots, a_{N+1}) = (a_1, \ldots, a_{N+2}) = \cdots$$

とくに，$a_{N+1} \in (a_1, \ldots, a_N)$ より

$$a_{N+1} = c_1 a_1 + \cdots + c_N a_N, \quad c_j \in R$$

と表される．このとき

$$f^* = f_{N+1} - \sum_{j=1}^{N} \left(c_j X^{\deg f_{N+1} - \deg f_j} f_j \right)$$

とおくと，$f^* \in \mathfrak{a}$, $f^* \notin (f_1, \ldots, f_N)$ かつ $\deg f^* < \deg f_{N+1}$ となり，f_{N+1} のとり方に矛盾する．ゆえに，1 変数のとき定理は正しい．

$n \geq 2$ のとき，n 変数多項式については

$$R[X_1, X_2, \ldots, X_n] = (R[X_1, X_2, \ldots, X_{n-1}])[X_n]$$

に注意すれば，n についての帰納法を使って証明できる． □

例 8.11. 有理数係数の n 変数多項式環 $\mathbb{Z}[X_1, X_2, \ldots, X_n]$ は Noether 環である．

例 8.12. K を体とすれば，$K[X_1, X_2, \ldots, X_n]$ は Noether 環である．

命題 8.13. R を環，S を R の部分環とする．S が Noether 環であるとき，S に R の有限個の元 a_1, a_2, …, a_n を添加した環 $S[a_1, a_2, \ldots, a_n]$ は Noether 環である．

証明. 写像

$$\Phi : S[X_1, X_2, \ldots, X_n] \longrightarrow S[a_1, a_2, \ldots, a_n], \quad f \longmapsto f(a_1, a_2, \ldots, a_n)$$

を考えると，Φ は環の全準同型である．Hilbert の基底定理により，$S[X_1, X_2, \ldots, X_n]$ は Noether 環である．ゆえに，命題 8.6 により $S[a_1, a_2, \ldots, a_n]$ も Noether 環である． □

定理 8.14. R が Noether 環ならば，R 上の n 変数形式的冪級数環 $R[[X_1, X_2, \ldots, X_n]]$ は Noether 環である．

注意 8.15. Hilbert の基底定理と同じようにして証明できる．ただし，最高次の項を考える代わりに最低次の項を考える．

証明. まず，1 変数のときを証明する．

$R[X]$ に有限生成でないイデアル $\mathfrak{a} \neq (0)$ が存在したとして矛盾を導く．

$f \in R[X]$ について，f の最低次の項の次数を $\deg^* f$ とおく．もし $f \neq 0$ かつ $\deg^* f = 0$ ならば，f は単元である．$\mathfrak{a}$ がそのような元を含めば $\mathfrak{a} = (1)$ である．したがって以下，$\mathfrak{a}$ は $f \neq 0$ かつ $\deg^* f = 0$ なる元 f を持たないと仮定する．

$\mathfrak{a}$ の 0 でない元の中で最低次の項の次数が最小のものを f_1 とする．$\mathfrak{a}$ は有限生成ではないので，$\mathfrak{a} \backslash (f_1) \neq \phi$ である．そこで，$\mathfrak{a} \backslash (f_1)$ の元の中で最低次の項の次数が最小のものを f_2 とする．一般に，$f_1, \ldots, f_{k-1}$ まで定まったとして，$f_k \in \mathfrak{a}$ を $\mathfrak{a} \backslash (f_1, \ldots, f_{k-1})$ の元の中で最低次の項の次数が最小のものとする．このとき

$$\deg^* f_j \leq \deg^* f_{j+1} \quad (j = 1, 2, \ldots)$$

である．各 f_j の最低次の項の係数を a_j とおくと，R のイデアルの増加列

$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots \subseteq (a_1, \ldots, a_k) \subseteq \cdots$$

が得られる．R は Noether 環であるから，ある N が存在して

$$(a_1, \ldots, a_N) = (a_1, \ldots, a_{N+1}) = (a_1, \ldots, a_{N+2}) = \cdots$$

とくに，$a_{N+1} \in (a_1, \ldots, a_N)$ より

$$a_{N+1} = c_1 a_1 + \cdots + c_N a_N, \quad c_j \in R$$

と表される．このとき

$$f^* = f_{N+1} + \sum_{j=1}^{N} \left(c_j X^{\deg f_{N+1} - \deg f_j - 1} f_j \right)$$

とおくと，$f^* \in \mathfrak{a}$, $f^* \notin (f_1, \ldots, f_N)$ かつ $\deg^* f^* < \deg f_{N+1}$ となり，f_{N+1} のとり方に矛盾する．ゆえに，1 変数のとき定理は正しい．

$n \geq 2$ のとき，n 変数形式的冪級数については

$$R[[X_1, X_2, \ldots, X_n]] = (R[[X_1, X_2, \ldots, X_{n-1}]])[[X_n]]$$

に注意すれば，n についての帰納法を使って証明できる． □

命題 8.16. R を Noether 環とし，S を R の積閉部分集合とする．$0 \neq S$ ならば，商環 $S^{-1}R$ も Noether 環である．

定理 8.17 (Artin-Rees の補題). R を Noether 環とし，$\mathfrak{a}$ を R のイデアルとする．L を有限生成 R 加群とし，M, N を L の部分 R 加群とする．このとき，ある正の整数 r が存在して，任意の整数 $n \geq r$ に対して

$$\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap N)$$

が成り立つ．

定理 8.18 (Krull の共通部分定理). R を Noether 環とし，M を有限生成 R 加群，$\mathfrak{a}$ を R のイデアルとする．このとき

$$\bigcap_{n=1}^{\infty} \mathfrak{a}^n M = \{x \in M \mid \exists a \in \mathfrak{a} \ \ s.t. \ \ ax = x\}$$

が成り立つ．

9 根基

R を環とします.

定義 9.1. R のイデアル $\mathfrak{a}$ に対して，

$$\sqrt{\mathfrak{a}} = \{x \in R \mid \exists n \in \mathbb{N} \ \ s.t. \ \ x^n \in \mathfrak{a}\}$$

を $\mathfrak{a}$ の**根基** (radical) という.

- $\sqrt{\mathfrak{a}}$ は R のイデアルである.
- $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$.
- $\mathfrak{a} \subseteq \mathfrak{b} \Longrightarrow \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}}$.
- $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.
- $\sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$.
- $\sqrt{\mathfrak{a}^n} = \sqrt{\mathfrak{a}} \ \ (n > 0)$.

例 9.2. R を一意分解整域とする．$x \in R$ とし，$x = p_1^{e_1} \cdots p_r^{e_r}$ を x の素元分解とする．$\mathfrak{a} = (x)$ を，x を生成元とする R の単項イデアルとすれば，$\sqrt{\mathfrak{a}} = (p_1 \cdots p_r)$ となる．

定義 9.3. R のイデアル $\mathfrak{a}$ で，$\sqrt{\mathfrak{a}} = \mathfrak{a}$ であるものを**根基イデアル** (radical ideal) と呼ぶ.

例 9.4. 素イデアルは根基イデアルである．すなわち，素イデアル $\mathfrak{p}$ の根基は $\mathfrak{p}$ 自身である．

定義 9.5. R の元 x が**冪零** (nilpotent) であるとは

$$\exists n \in \mathbb{N} \ \ s.t. \ \ x^n = 0$$

が成り立つことをいう.

- 零イデアルの根基は，R の冪零な元の全体と一致する．

定義 9.6. 零イデアルの根基を**冪零根基** (nilradical) という[2].

命題 9.7.

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p} \quad (\mathfrak{p} \text{ は } R \text{ の素イデアル}).$$

系 9.7.1. R の冪零根基，すなわち R の冪零な元の全体は，R のすべての素イデアルの共通部分と一致する．

命題 9.8. R のイデアル $\mathfrak{a}$ に対し，$\pi : R \longrightarrow R/\mathfrak{a}$ を自然な全射準同型とする．このとき，$R/\mathfrak{a}$ の冪零根基の π による逆像は $\mathfrak{a}$ の根基 $\sqrt{\mathfrak{a}}$ に一致する．

定義 9.9. R のすべての極大イデアルの共通部分を R の **Jacobson 根基**といい[3]，$\mathrm{Jac}\, R$ で表す．

例 9.10. 局所環 R はただ一つの極大イデアル $\mathfrak{m}$ を持つ．したがって局所環の Jacobson 根基はそのただ一つの極大イデアル $\mathfrak{m}$ である．

定理 9.11 (Krull-東屋の補題). M を有限生成 R 加群，N を M の部分 R 加群とする．このとき

$$(\mathrm{Jac\ R})M + N = M \Longrightarrow M = N$$

が成り立つ．

注意 9.12. Krull-東屋の補題は，中山の補題と呼ばれることもある．

10 準素イデアル

R を環とします.

定義 10.1. R のイデアル $\mathfrak{a}$ が**準素** (primary) であるとは

$$xy \in \mathfrak{a} \Longrightarrow x \in \mathfrak{a} \text{ または } y \in \sqrt{\mathfrak{a}}$$

が成り立つことをいう．

- 素イデアルは準素イデアルである．

[2]冪零根基のことを根基と呼ぶ本もあります．
[3]Jacobson はジェイコブソンと読みます．人名です．

命題 10.2. R のイデアル $\mathfrak{a}$ が準素であるための必要十分条件は，剰余環 $R/\mathfrak{a}$ がもし零因子を持てば，それらがすべて冪零であることである．

例 10.3. $R = \mathbb{Z}, p$ を素数とし，$\mathfrak{q} = (p^n)$ とする．このとき，$\mathfrak{q}$ は $n = 1$ のとき素イデアル，$n \geq 2$ のとき準素イデアルである．

例 10.4. K を体とし，$R = K[X], \mathfrak{q} = (X^n)$ とする．このとき，$\mathfrak{q}$ は $n = 1$ のとき素イデアル，$n \geq 2$ のとき準素イデアルである．

例 10.5. R を一意分解整域とし，p を R における素元とする．$\mathfrak{q} = (p^n)$ とする．このとき，$\mathfrak{q}$ は $n = 1$ のとき素イデアル，$n \geq 2$ のとき準素イデアルである．逆に，$x \in R$ がある一つの素元の冪として分解されないならば，(x) は準素イデアルではない．

命題 10.6. R のイデアル $\mathfrak{a}$ について，$\sqrt{\mathfrak{a}}$ が極大イデアルならば，$\mathfrak{a}$ は準素イデアルである．

命題 10.7. 準素イデアル $\mathfrak{q}$ の根基 $\sqrt{\mathfrak{q}}$ は素イデアルである．しかも，$\mathfrak{q}$ を含む素イデアルのうちで最小のものである．

定義 10.8. $\mathfrak{p}$ を R の素イデアルとする．R のイデアル $\mathfrak{a}$ が **$\mathfrak{p}$-準素** ($\mathfrak{p}$-primary) であるとは，$\mathfrak{a}$ が準素イデアルであって，$\sqrt{\mathfrak{a}} = \mathfrak{p}$ が成り立つときにいう．

また，準素イデアル $\mathfrak{q}$ が $\mathfrak{p}$-準素であることを，準素イデアル $\mathfrak{q}$ が $\mathfrak{p}$ に**属する**という．

例 10.9. $R = \mathbb{Z}, p$ を素数とし，$\mathfrak{q} = (p^n)$ とする．このとき，$\sqrt{\mathfrak{q}} = (p)$ である．

例 10.10. K を体とし，$R = K[X], \mathfrak{q} = (x^n)$ とする．このとき，$\sqrt{\mathfrak{q}} = (x)$ である．

命題 10.11. $\mathfrak{a}$ を R のイデアルで R とは異なるものとし，$\mathfrak{p}$ を素イデアルとする．$\mathfrak{a}$ が $\mathfrak{p}$-準素であるためには，

(i) $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{a}}$,

(ii) $xy \in \mathfrak{a} \Longrightarrow x \in \mathfrak{a}$ または $y \in \mathfrak{p}$

であることが必要十分である．

命題 10.12. $\mathfrak{p}$ を素イデアルとする．$\mathfrak{q}_1, \mathfrak{q}_2$ がともに $\mathfrak{p}$-準素イデアルならば，$\mathfrak{q}_1 \cap \mathfrak{q}_2$ もまた $\mathfrak{p}$-準素イデアルである．

注意 10.13. $\mathfrak{q}_1$, $\mathfrak{q}_2$ が互いに包含関係を持たない素イデアルに属する準素イデアルであるとき，$\mathfrak{q}_1 \cap \mathfrak{q}_2$ は準素イデアルではない．

命題 10.14. $\mathfrak{q}$ を素イデアル $\mathfrak{p}$ に属する準素イデアルとし，$a \in R \backslash \mathfrak{q}$ とする．このとき，$\mathfrak{q} : (a) = \{x \in R \mid xa \in \mathfrak{q}\}$ もまた $\mathfrak{p}$ に属する準素イデアルである．

11 Noether 環における準素分解

定義 11.1. 環 R のイデアル $\mathfrak{a}$ が，二つのイデアル $\mathfrak{b}, \mathfrak{c}$ によって

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}, \quad \mathfrak{a} \subsetneq \mathfrak{b}, \quad \mathfrak{a} \subsetneq \mathfrak{c}$$

と書けるとき，$\mathfrak{a}$ は**可約** (reducible) であるといい，そうでないとき，すなわち，

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Longrightarrow \mathfrak{a} = \mathfrak{b} \text{ または } \mathfrak{a} = \mathfrak{c}$$

であるとき，$\mathfrak{a}$ は**既約** (irreducible)，あるいは**直既約** (indecomposable) であるという．

命題 11.2. 環 R の素イデアルは既約である．

命題 11.3. Noether 環 R の既約イデアルは準素イデアルである．

命題 11.4. Noether 環 R の任意のイデアルは，ある有限個の既約イデアルの共通部分として表される．

系 11.4.1. Noether 環 R のイデアル $\mathfrak{a}$ に対して，ある有限個の準素イデアル $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ が存在して

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

と書ける．

Noether 環 R のイデアル $\mathfrak{a}$ が上の系のように有限個の準素イデアルの共通部分として表されているとき，ある $\mathfrak{q}_i$ で $\cap_{j \neq i} \mathfrak{q}_j$ を含むものがあれば，$\mathfrak{q}_i$ を除く他の準素イデアルの共通部分で $\mathfrak{a}$ を表すことができます．よって，どの $\mathfrak{q}_i$ も他のものの共通部分を含まないようにすることができます．

定義 11.5. R を Noether 環，$\mathfrak{a}$ を R のイデアル，$\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ を有限個の準素イデアルとし，

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

と表されているとする．どの $\mathfrak{q}_i$ も他のものの共通部分 $\cap_{j \neq i} \mathfrak{q}_j$ を含まないとき，この等式を，$\mathfrak{a}$ の**準素分解** (primary decomposition) という．あるいは，準素イデアルによる $\mathfrak{a}$ の**無駄のない表示**ということもある．

またこのとき，$\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ を $\mathfrak{a}$ の**準素成分** (primary component) という．

注意 11.6. 準素分解は一意的とは限らない．

命題 11.7. Noether 環 R のイデアル $\mathfrak{a}$ の二つの準素分解

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_m$$

を考える．このとき，各根基の集合について

$$\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\} = \{\sqrt{\mathfrak{q}'_1}, \ldots, \sqrt{\mathfrak{q}'_m}\}$$

が成り立つ．したがって，集合 $\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$ は $\mathfrak{a}$ に対して一意的に定まる．

定義 11.8. 上の定理の $\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}$ を $\mathfrak{a}$ の**素因子** (prime divisor) という．

$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ を準素分解とします．同じ素因子に属する準素イデアルの共通部分は，その素因子に属する準素イデアルです．したがって，$\mathfrak{a}$ の異なる素因子の個数を r とするとき，$\mathfrak{a} = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_r$ なる準素分解が得られます．しかも，$\mathfrak{a}$ の準素成分全体と素因子全体とが $\mathfrak{q} \longmapsto \sqrt{\mathfrak{q}}$ なる対応で一対一に対応しています．

定義 11.9. イデアル $\mathfrak{a}$ の準素分解が**最短** (shortest) であるとは，$\mathfrak{a}$ の準素成分全体と素因子全体とが $\mathfrak{q} \longmapsto \sqrt{\mathfrak{q}}$ なる対応で一対一に対応していることをいう．

また，最短の準素分解を，準素イデアルによる**最短表示**ということもある．

12 Krull 次元

R を環とします．この節で登場するイデアルはすべて R のイデアルとします．

定義 12.1. R の素イデアルからなる全順序集合を素イデアルの**鎖** (chain) と呼ぶ[4]．

以下，登場する素イデアルの鎖は高々可算個の元からなるものに限ります．

定義 12.2. 素イデアルの鎖 $\mathcal{C}$ の**長さ** (length) を

$$\operatorname{length} \mathcal{C} = \begin{cases} |\mathcal{C}| - 1, & \mathcal{C} \text{ が有限集合のとき} \\ \infty, & \mathcal{C} \text{ が無限集合のとき} \end{cases}$$

と定める．ただし $|\mathcal{C}|$ は $\mathcal{C}$ の濃度である．$|\mathcal{C}|$ が有限でないとき，$\mathcal{C}$ の長さは無限であるという．

定義 12.3. 素イデアル $\mathfrak{p}$ に対して，$\mathfrak{p}$ の**高さ** (height) を，$\max \mathcal{C} = \mathfrak{p}$ であるような素イデアルの鎖 $\mathcal{C}$ の長さの上限として定義する．すなわち

$$\operatorname{ht} \mathfrak{p} = \sup\{ \operatorname{length} \mathcal{C} \mid \mathcal{C} \text{ は } \mathfrak{p} \text{ を最大元としてもつ素イデアルの鎖} \}.$$

[4]鎖は「さ」と読みます．

例 12.4. R が整域のとき，零イデアル (0) は素イデアルになる．R の素イデアル $\mathfrak{p}$ について，次のことが成り立つ：

- $\mathrm{ht}\ \mathfrak{p} = 0 \Longleftrightarrow \mathfrak{p} = (0)$.
- $\mathrm{ht}\ \mathfrak{p} = 1$ であるための必要十分条件は，$\mathfrak{p} \neq (0)$ であり，かつ $\mathfrak{p}$ に含まれる素イデアルが $\mathfrak{p}$ 自身と零イデアル (0) のみであることである．

定義 12.5. 一般のイデアル $\mathfrak{a}\,(\neq R)$ に対して，$\mathfrak{a}$ の**高さ**を

$$\mathrm{ht}\ \mathfrak{a} = \min\{\, \mathrm{ht}\ \mathfrak{p} \mid \mathfrak{p} \text{ は } \mathfrak{a} \subseteq \mathfrak{p} \text{ なる素イデアル} \,\}$$

と定義する．

定義 12.6. 環 R の **Krull 次元** (Krull dimension) を

$$\mathrm{Krull\ dim}\ R = \sup\{\, \mathrm{ht}\ \mathfrak{p} \mid \mathfrak{p} \text{ は素イデアル} \,\}$$

によって定義する．

注意 12.7. 素イデアル $\mathfrak{a}$ の高さを $\mathfrak{a}$ の**階数** (rank)，$R/\mathfrak{a}$ の Krull 次元を $\mathfrak{a}$ の**相対階数** (corank) と呼ぶこともある．

命題 12.8. 素イデアル $\mathfrak{p}$ による R の局所化を $R_{\mathfrak{p}}$ とするとき，

$$\mathrm{ht}\ \mathfrak{p} = \mathrm{Krull\ dim}\ R_{\mathfrak{p}}$$

が成り立つ．

命題 12.9. $\mathfrak{p}$ を R の素イデアル，S を R の積閉部分集合，$S^{-1}R$ を S による R の商環とする．このとき，

$$\mathfrak{p} \cap S = \phi \Longrightarrow \mathrm{ht}\ \mathfrak{p} = \mathrm{ht}\ (\mathfrak{p}S^{-1}R)$$

が成り立つ．

命題 12.10. R の任意のイデアル $\mathfrak{a}$ に対して

$$\mathrm{ht}\ \mathfrak{a} + \mathrm{Krull\ dim}\ R/\mathfrak{a} \leq \mathrm{Krull\ dim}\ R$$

が成り立つ．

命題 12.11. $\mathcal{P}$ を，イデアル $\mathfrak{a} \neq R$ を含む素イデアル全体とする．このとき，任意の $\mathfrak{p} \in \mathcal{P}$ に対して，包含関係に関する $\mathcal{P}$ の極小元で $\mathfrak{p}$ に含まれるものが存在する．

定義 12.12. $\mathcal{P}$ を，イデアル $\mathfrak{a} \neq R$ を含む素イデアル全体とする．$\mathcal{P}$ の包含関係に関する極小元を $\mathfrak{a}$ の**極小素因子** (minimal prime divisor) あるいは**極小付随素イデアル** (minimal associate prime) という．

- イデアル $\mathfrak{a} \neq R$ の極小素因子は $\mathfrak{a}$ の素因子である．逆は一般には成立しない．

定理 12.13 (Krull の標高定理). R を Noether 環とし，$a_1, \ldots, a_n \in R$ とする．$\mathfrak{p}$ が $(a_1, \ldots, a_n)$ の極小素因子ならば，$\operatorname{ht} \mathfrak{p} \leq n$ である．

13　次数付き環

定義 13.1. 環 R が次の条件を満たすとき，R を**次数付き環** (graded ring) と呼ぶ：整数 $n \geq 0$ に対して，R の部分加法群 R_n が定まっていて

(i) $1 \in R_0$,

(ii) $R_i R_j \subseteq R_{i+j} \quad (\forall i, \forall j \in \mathbb{Z}, i \geq 0, j \geq 0)$,

(iii) $R = \displaystyle\bigoplus_{n=0}^{\infty} R_n$ 　(R 加群として)

が成り立つ．

各 R_n を R の n 次**斉次成分** (homogeneous part) という．

$R = \bigoplus_{n=0}^{\infty} R_n$ が次数付き環のとき，次のことが成り立ちます：

- R_0 は R の部分環である．
- 各 R_i は R 加群である．
- $R_+ = \bigoplus_{n=1}^{\infty} R_n$ は R のイデアルである．

定義 13.2. 環 R が与えられたとき，次数付き環の定義における条件 (i), (ii), (iii) を満たすような R の部分加法群 R_n $(n \geq 0)$ を与えることを，R に**次数を付ける** (grade) という．

注意 13.3. 同じ環に異なる次数付けをした場合，次数付き環としては別のものと考える．

例 13.4. 任意の環 R に対して，$R_0 = R$, $R_n = \{0\}$ $(n \geq 1)$ として R に次数を付けることができる．これを**自明な次数付け**という．

例 13.5. 環 R のイデアル $\mathfrak{a}$ に対して,

$$Q = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n \quad \text{ただし} \quad \mathfrak{a}^0 = R$$

とおけば,Q は $\mathfrak{a}^n$ を n 次斉次成分とする次数付き環になる.

例 13.6. 環 R 上の多項式環 $R[X_1, \ldots, X_n]$ は,$R_0 = R$ とし,$R_d\ (d \geq 1)$ を d 次の同次多項式の全体とすることによって次数付き環になる.

例 13.7. R を環とし,M を R 加群とする.M の R 上のテンソル代数 $T(M)$ は,$T^p(M) = M \otimes \cdots \otimes M$ (n 個の M のテンソル積) を n 次斉次成分とする次数付き環である.

定義 13.8. 次数付き環 $R = \bigoplus_{n=0}^{\infty} R_n$ の元 x について,ある整数 $n \geq 0$ が存在して $x \in R_n$ であるとき,x は次数 n の**斉次元** (homogeneous element) であるという.

例 13.9. 環 R 上の多項式環 $R[X_1, \ldots, X_n]$ において,d 次の同次多項式は次数 d の斉次元である.

定義 13.10. 次数付き環 $R = \bigoplus_{n=0}^{\infty} R_n$ のイデアル $\mathfrak{a}$ が**斉次イデアル** (homogeneous ideal) あるいは**次数付きイデアル** (graded ideal) であるとは,$\mathfrak{a} = \bigoplus_{n=0}^{\infty}(R_n \cap \mathfrak{a})$ が成り立つことをいう.

命題 13.11. $R = \bigoplus_{n=0}^{\infty} R_n$ を次数付き環とする.このとき,次の三つの条件は同値である:

(i) R は Noether 環である.

(ii) R_0 は Noether 環であり,$R_+ = \bigoplus_{n=1}^{\infty} R_n$ は R の有限生成イデアルである.

(iii) R_0 は Noether 環であり,R は R_0 上有限個の元で生成される.

命題 13.12. 次数付き環の斉次イデアル $\mathfrak{a}$ の根基 $\sqrt{\mathfrak{a}}$ は斉次イデアルである.

命題 13.13. 次数付き Noether 環 R の斉次イデアル $\mathfrak{a}$ に対して,ある有限個の斉次準素イデアル $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ が存在して $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ と書ける.

14 正規環

Q を環とし,R を Q の部分環とします.

定義 14.1. 多項式 $f \in Q[X]$ が**モニック** (monic) であるとは,f の最高次係数が 1 であることをいう.また,モニックな多項式を**単多項式**と呼ぶ.

定義 14.2. $x \in Q$ が R 上**整** (integral) であるとは，x がモニックな多項式 $f(x) \in R[X]$ の根であるときにいう．

定義 14.3. Q のすべての元が R 上整であるとき，Q は R 上**整** (integral) であるといい，Q のことを R の**整拡大** (integral extension) と呼ぶ．

例 14.4. R 自身は R 上整である．なぜなら，任意の $a \in R$ に対して，$f(X) = X - a$ とおけば，$f(X) \in R[X]$ かつ $f(a) = 0$ となるからである．

定義 14.5. $\overline{R} = \{x \in Q \mid x \text{ は } R \text{ 上整 }\}$ とおく．これを Q における R の**整閉包** (integral closure) という．

定義 14.6. $\overline{R} = R$ のとき，R は Q において**整閉** (integrally closed) であるという．

定義 14.7. R を整域とする．R が商体において整閉であるとき，R を**正規環** (normal ring) あるいは**整閉整域** (integraly closed domain) と呼ぶ．

例 14.8. 有理整数環 $\mathbb{Z}$ は正規環である．

例 14.9. 一意分解整域は正規環である．

例 14.10. 体 K 上の n 変数多項式環 $K[X_1, \ldots, X_n]$ は正規環である．

例 14.11. 有限次代数体 K の整数環 $\mathfrak{o}_K$ は正規環である．

定理 14.12 (Krull-秋月). R を Krull 次元が 1 以下の Noether 整域とし，K を R の商体とする．K の有限次拡大体 L の部分環 Q が R を含むならば，Q もまた Krull 次元が 1 以下の Noether 整域である．

定義 14.13. Q の元 $x_1, \ldots, x_n$ が R 上**代数的独立** (algebraically independent) であるとは，多項式 $f \in R[X_1, \ldots, X_n]$ について

$$f(x_1, \ldots, x_n) = 0 \Longrightarrow f = 0$$

が成り立つことをいう．

定理 14.14 (多項式環の正規化定理). $\mathfrak{a}$ を体 K 上の多項式環 $K[X_1, \ldots, X_n]$ のイデアルとし，r を $\mathfrak{a}$ の高さとする：$r = \mathrm{ht}\,\mathfrak{a}$. このとき，$K[X_1, \ldots, X_n]$ の元 $f_1, \ldots, f_n$ で，次の条件を満たすものが存在する：

(i) $K[X_1, \ldots, X_n]$ は $K[f_1, \ldots, f_n]$ 上整である.

(ii) $\mathfrak{a} \cap K[f_1, \ldots, f_n]$ は $f_1, \ldots, f_n$ で生成される.

(iii) $f_{r+i} = X_{r+i} + g_i$ $(\exists g_i \in K[X_1, \ldots, X_n],\ i = 1, \ldots, n-r)$.

定理 14.15 (Noether の正規化定理). 体 K 上有限生成な環 R に対して，K 上代数的独立な元 $a_1, \ldots, a_n$ を適当にとれば，R は $K[a_1, \ldots, a_n]$ 上整になる.

定義 14.16. $\mathfrak{p}$ を R の素イデアルとし，$\mathfrak{P}$ を Q の素イデアルとする．$\mathfrak{P} \cap R = \mathfrak{p}$ であるとき，$\mathfrak{P}$ は $\mathfrak{p}$ の**上に乗っている** (lies over) という.

命題 14.17. Q が R 上整であると仮定する．$\mathfrak{p}$ を R の素イデアルとする.

(i) $\mathfrak{p}$ の上に乗っている Q の素イデアルが存在する．すなわち，Q の素イデアル $\mathfrak{P}$ で $\mathfrak{P} \cap R = \mathfrak{p}$ となるものが存在する.

(ii) $\mathfrak{p}$ の上に乗っている二つの Q の素イデアルについて，一方が他方に含まれることはない.

定理 14.18 (上昇定理 (going-up theorem)). Q が R 上整であると仮定する．$\mathfrak{p}_1, \mathfrak{p}_2$ を R の二つの素イデアルとする．$\mathfrak{P}_1$ を $\mathfrak{p}_1$ の上に乗っている Q の素イデアルとする．このとき，$\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ ならば，Q の素イデアル $\mathfrak{P}_2$ で，

$$\mathfrak{P}_1 \subseteq \mathfrak{P}_2, \qquad \mathfrak{P}_2 \cap R = \mathfrak{p}_2$$

を満たすものが存在する.

参考文献

[1] 永田雅宜: 可換環論, 紀伊国屋書店, 1974

[2] 堀田良之: 代数入門 —群と加群—, 裳華房, 1987

[3] 桂利行: 代数幾何入門, 共立出版, 1998

[4] 石田正典: 代数幾何学の基礎, 培風館, 2000