代数学 II 講義ノート

安藤哲哉

注意: (1) 校正をあまりきちんとしていないので，誤植等に注意して利用して下さい．
(2) 90 分× 15 回で全部の内容を全部証明を付けて講義するのは，時間的にきびしいです．

1. 可換環と加群の定義

定義 1.1.(可換環，整域，体) 集合 R に 2 種類の和 $+$ と積 $\times$ が定義されていて以下 (1) 〜 (3) を満たすとき R を**可換環** (commutative ring) という．ただし，積 $a \times b$ は通号 ab と書き，時に $a \cdot b$ とも書く．
(1) R は和 $+$ について 0 を単位元とするアーベル群である．
(2) R は積について閉じていて，結合法則，交換法則を満たし，1 を単位元とする．つまり，$a, b \in R$ ならば $ab \in R$ で，$(ab)c = a(bc)$, $ab = ba$, $1a = a$ $(\forall a, \forall b, \forall c \in R)$ を満たす．
(3) 分配法則 $(a+b)c = ac + bc$ $(\forall a, \forall b, \forall c \in R)$ を満たす．

以上の定義から，$0a = 0$ (なぜなら $(0a + 0a = (0 + 0)a = 0a)$, $a(b + c) = ab + ac$ が導かれることに注意する．ところで，可換環 R の定義の中で $0 \neq 1$ は仮定しなかったが，もし $0 = 1$ であれば $R = \{0\}$ である．実際，$a \in R$ ならば $a = 1a = 0a = 0$ である．可換環 $\{0\}$ を単に 0 とも書く．

今，R は可換環で $R \neq 0$ とする．$a \in R$ に対し $ab = 1$ を満たす $b \in R$ が存在するとき，この b を $b = a^{-1}$ とか $b = \dfrac{1}{a}$ と書き，a の**逆元**という．a が逆元を持つとき a は**可逆** (invertible) 元であるとか，**単元** (unit) であるという．

また，$a \in R$ に対し，$ab = 0$, $b \neq 0$ を満たす $b \in R$ が存在するとき，a は**零因子**とか**ゼロ因子** (zero dividor) であるという．a が零因子でないとき**非零因子**とか**正則元** (regular) という．

環 R において，$\underbrace{1 + 1 + \cdots + 1}_{n \text{ 個}} = 0$ となることがある (後の例 1.2(3) 参照)．この場合，この条件を満たす最小の自然数 n を R の**標数** (characteristic) という．何個 1 を足しても 0 にならないとき，R の標数は 0 であると約束する．

可換環 R が以下の (4), (5) を満たすとき，R は**整域** (integral domain) であるという．
(4) $0 \neq 1$ である．
(5) 0 以外に零因子は存在しない．つまり，$a, b \in R$, $ab = 0$ ならば $a = 0$ または $b = 0$ である．対偶で書けば，$a \neq 0$, $b \neq 0$ ならば $ab \neq 0$ である．

可換環 R が上の (4) と以下の (6) を満たすとき，R は (可換) **体** (field) であるという．
(6) R の 0 でない元は R の中に逆元を持つ．つまり，$0 \neq a \in R$ ならば，$a^{-1} \in R$.

容易にわかるように，体は整域である．

可換環 R の部分集合 $S \subset R$ が和と積について閉じていて，$a \in S$ であるとき，S は R の**部分環**であるという．S が整域のとき S は R の**部分整域**，S が体のとき S は R の**部分体**であるという．

例 1.2. (1) 整数全体の集合 $\mathbb{Z}$ は体でない整域である．
(2) 有理数全体の集合 $\mathbb{Q}$, 実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$ はいずれも体である．
(3) 自然数 n を法とする剰余系 $\mathbb{Z}/n\mathbb{Z}$ は可換環である．n が合成数 (2 つ以上の素数の積) であるとき $\mathbb{Z}/n\mathbb{Z}$ は整域でない可換環である．実際 $n = pq$ $(p \geqq 2, q \geqq 2)$ のとき，その n を法とする剰余類は，$\overline{0} = \overline{n} = \overline{p}\,\overline{q}$, $\overline{0} \neq \overline{p}$, $\overline{0} \neq \overline{q}$ である．

逆に，n が素数 p の場合，$\mathbb{Z}/p\mathbb{Z}$ は体になる (証明してみよ)．この体 $\mathbb{Z}/p\mathbb{Z}$ を $\mathbb{F}_p$ と書き，標数 p の**素体**という．

定義 1.3.(形式的巾級数環) R を可換環とする．

$$f(X) = \sum_{i=0}^{\infty} a_i X^i \quad (a_0, a_1, \ldots, a_n, \ldots \in R) \qquad ①$$

を X を変数とする R 係数**形式的巾級数** (formal power series) 式といい，こういう形の元全体の集合を $R[[X]]$ と書く.「巾」は「冪」(べき) と書くのが正しいが，画数が多く面倒なので「巾」と略記する．なお，$a \in R$ に対し，$a_0 = a$ で $i \geqq 1$ のとき $a_i = 0$ であるような ① の形の形式的巾級数と同一視することにより，$R \subset R[[X]]$ とみなす．

$g(X)=\sum_{i=0}^{\infty} b_iX^i \in R[[X]]$ に対し，

$$f(X)+g(X)=\sum_{i=0}^{\infty}(a_i+b_i)X^i,\quad f(X)g(X)=\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}a_j+b_{i-j}\right)X^i$$

として和と積を定めると $R[[X]]$ は可換環になり R はその部分環になる．$R[[X]]$ を R 上の (X を変数とする)**1 変数形式的巾級数環**という．

なお，① の形の形式的巾級数 $f(X)$ に対し，$i<n$ ならば $a_i=0$ を満たす最小の非負整数 n を，$\operatorname{ord} f(X)$, $\operatorname{ord}_X f(X)$, $\operatorname{ord} f$ などと書き，f の**オーダー** (order) という．ただし，$f(X)=0$ (すべての a_i が 0) のときは，$\operatorname{ord} f(X)=+\infty$ と約束する．$a_0\neq 0$ のときは $\operatorname{ord} f(X)=0$ である．

$R[[X,Y]]:=(R[[X]])[[Y]]$ を 2 変数形式的巾級数環，$R[[X,Y,Z]]:=(R[[X,Y]])[[Z]]$ を 3 変数形式的巾級数環といい，以下帰納的に，$R[[X_1,X_2,\ldots,X_n]]:=(R[[X_1,\ldots,X_{n-1}]])[[X_n]]$ を n **変数形式的巾級数環**という．$R[[X_1,X_2,\ldots,X_n]]$ の元は，

$$f(X_1,\ldots,X_n)=\sum_{i_1=0}^{\infty}\sum_{i_2=0}^{\infty}\cdots\sum_{i_n=0}^{\infty}a_{i_0,i_1,\cdots,i_n}X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$$

($a_{i_0,i_1,\cdots,i_n}\in R$) という形に書ける．ただ，添え字や指数を書くのが面倒なので，$\overline{\mathbb{N}}=\mathbb{N}\cup\{0\}$, $\mathbf{i}=(i_1, i_2,\ldots, i_n)\in\overline{\mathbb{N}}^n$ とし，$X^{\mathbf{i}}=X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ と略記して，$f(X)=\sum_{\mathbf{i}\in\overline{\mathbb{N}}^n}a_{\mathbf{i}}X^{\mathbf{i}}$ と書くと，すこし簡略化される．こういう書き方を**多重指数表示**という．

定義 1.4.(多項式環) R を可換環とする．

$$f(X)=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_2X^2+a_1X+a_0\quad (n\in\mathbb{N}),\ a_0,\ a_1,\ldots,\ a_n\in R) \qquad ②$$

を X を変数とする R 係数多項式といい，こういう形の元全体の集合を $R[X]$ と書く．$i>n$ のとき $a_i=0$ として，② の $f(X)$ を $\sum_{i=0}^{\infty}a_iX^i\in R[[X]]$ と同一視することにより $R\subset R[X]\subset R[[X]]$ と考えることができる．このとき，$R[X]$ は $R[[X]]$ の部分環になる．$R[X]$ を (X を変数とする) R 上の **1 変数多項式環** (polynomial ring) という．

$a_n\neq 0$ のとき，n を $\deg f(X)$, $\deg_X f(X)$, $\deg f$ などと書き，f の**次数** (degree) という．ただし，$n=0$ で $a_0=0$ のとき，$f(X)$ を**ゼロ多項式**といい，$\deg 0=-\infty$ と約束する．他方，$n=0$ で $a_0\neq 0$ のときは，$f(X)$ を**定数多項式**といい，$\deg f(X)=0$ である．また，最高次の係数 a_n が $a_n=1$ を満たす多項式を**モニック多項式** (monic) という．

帰納的に，$R[X_1,\ldots,X_n]=(R[X_1,\ldots,X_{n-1}])[X_n]$ と定義し，$R[X_1,\ldots,X_n]$ を R 上の n **変数多項式環**という．

問題 1.5. R は整域とする．

(1) $f(X)$, $g(X)\in R[[X]]$ に対し $\operatorname{ord}(f(X)g(X))=\operatorname{ord} f(X)+\operatorname{ord} g(X)$ であることを証明せよ．これともとに，$K[[X]]$ は整域であることを示せ．

(2) $f(X)$, $g(X)\in R[X]$ に対し $\deg(f(X)g(X))=\deg f(X)+\deg g(X)$ であることを証明せよ．

(3) $R[[X_1,\ldots, X_n]]$, $R[X_1,\ldots, X_n]$ は整域であることを証明せよ．

定義 1.6.(R-加群，R-代数) R は可換環とし，R の 0, 1 を一時的に 0_R, 1_R と書く．M は加法 $+$ について 0_M を単元とするアーベル群であるとする．さらに，任意の $a\in R$, $x\in M$ に対して R の**作用**と呼ばれる演算 ax が定義されていて $ax\in M$ であると仮定する．さらに以下の (1) 〜 (3) を満たすとき，M は R-**加群** (R-module) であるという．

(1) (結合法則) $(ab)x=a(bx)$ $(\forall a\in R, \forall b\in R, \forall x\in M)$

(2) (1 の自明な作用) $1_Rx=x$ $(\forall x\in M)$

(3) (分配法則) $(a+b)x=ax+bx$, $a(x+y)=ax+ay$ $(\forall a, \forall b\in R; \forall x, \forall y\in M)$

R が体のとき，R-加群を R-**ベクトル空間**とか R-**線形空間**とも言う．法則 $0_Rx=0_M$, $a0_M=0_M$, $a(-x)=(-a)x$ は上の定義から簡単に導くことができる．

今，R-加群 M が環 (積に関する交換法則は仮定しないこともある) であって，以下の (4) を満たすとき，M は R-**代数** (R-algebra) とか R-**多元環**であるという．

(4) $a(xy) = (ax)y$ ($\forall a \in R$; $\forall x$, $\forall y \in M$)

例えば，多項式環 $R[X_1,\ldots, X_n]$, 形式的巾級数環 $R[[X_1,\ldots, X_n]]$ は R-代数である．一般に，S が R の部分環のとき，R は S-代数である．

M は R-加群とする．部分集合 $N \subset M$ が以下の (5), (6) を満たすとき，N も R-加群になる．このとき，N は M の R-**部分加群**であるとか，部分 R-加群であると言う．

(5) $x, y \in N$ ならば $x + y \in N$.

(6) $a \in R$, $x \in N$ ならば $ax \in N$.

M は R-加群，N は M の R-部分加群とする．このとき剰余加群 M/N は自然に R-加群の構造を持つ．M/N を R-**剰余加群**という．

M は R-加群，$N_i \subset M$ $(i = 1,\ldots, n)$ は R-部分加群とする．

$$N_1 + N_2 + \cdots + N_n = \left\{ \sum_{i=1}^{n} x_i \;\middle|\; x_i \in N_i \right\}$$

も R-部分加群である．これを，$N_1,\ldots, N_r$ の**和**という．$N_1 + N_2 + \cdots + N_n$ は $\displaystyle\sum_{i=1}^{n} N_i$ とも書く．

M は R-加群，$x_1, x_2,\ldots, x_n \in M$ とする．このとき，

$$N = \left\{ \sum_{i=1}^{n} a_i x_n \;\middle|\; a_1, a_2,\ldots, a_n \in R \right\}$$

は M の R-部分加群になる．この N を $Rx_1 + Rx_2 + \cdots + Rx_n$ とか $\displaystyle\sum_{i=1}^{n} Rx_i$ などと書き，$x_1,\ldots, x_n$ によって**生成**される M の R-部分加群という．

逆に，一般に R-部分加群 M に対し，$M = Rx_1 + Rx_2 + \cdots + Rx_n$ となるような $x_1, x_2,\ldots, x_n \in M$ が存在するとき，M は**有限生成** (finitely generated) であるといい，$x_1, x_2,\ldots, x_n$ を M の**生成系** (generator) とか**生成元**という．

定義 1.7.(イデアル) R は可換環とする．R の部分集合 I が R の R-部分加群であるとき，I は R の**イデアル** (idel) であるという．しつこく書くと，次の (1), (2) が成り立つことがイデアルの定義である．

(1) $x, y \in I$ ならば $x + y \in I$.

(2) $a \in R$, $x \in I$ ならば $ax \in I$.

$I_1,\ldots, I_n$ が R のイデアルのとき，$I_1 + \cdots + I_n$ は R-加群だから，R のイデアルになる．

$x_1, x_2,\ldots, x_n \in R$ によって生成される R の R-部分加群 $I = Rx_1 + Rx_2 + \cdots + Rx_n$ は R のイデアルであるが，この I を $(x_1, x_2,\ldots, x_n)$ とか，$x_1R + x_2R + \cdots + x_nR$ とか，$\displaystyle\sum_{i=1}^{n} x_iR$ などとも書き，$x_1,\ldots, x_n$ によって**生成**される R のイデアルという．

一般に，R のイデアル I に対し，$I = (x_1, x_2,\ldots, x_n)$ となるような $x_1, x_2,\ldots, x_n \in R$ が存在するとき，I は**有限生成**であるといい，$x_1,\ldots, x_n \in R$ をその**生成系**とか**生成元**という．特に $n = 1$ のとき，$I = (x) = Rx = xR$ を**単項イデアル** (principal ideal) という．

I が R のイデアルのとき R/I は R-加群であるが，$\overline{a}\overline{b} = \overline{ab}$ ($a, b \in R$ でオーバーラインは I を法とする同値類) によって定義すると，R/I は R-代数の構造を持ち，特に可換環になる．

R をその部分環 S $(S \neq R)$ で割った R/S は環の構造を持たないことを注意する．つまり，$1 \in S$ なので，$\overline{1} = \overline{0}$ となってしまう．

命題 1.8. R は可換環，I は R のイデアル，$x \in R$ は可逆元とする．もし，$x \in I$ ならば $I = R$ である．

証明. $x^{-1} \in R$ である．勝手な $a \in R$ を取ると，$(ax^{-1}) \in R$, $x \in I$ より，$a = (ax^{-1})x \in I$ となる．よって，$R \subset I$ である．$I \subset R$ は明らかなので，$I = R$ である． □

命題 1.9. 可換環 R が体であるための必要十分条件は，R のイデアルが (0) と R の丁度 2 個 $((0) \neq R)$ であることである．

証明. 一般に可換環 R において，$(0) = R0$, $R = R1 = (1)$ はイデアルである (この 2 つを**自明なイデアル**という.)

R は体とし，I はイデアルで $I \neq (0)$ とする．$0 \neq x \in I$ が存在するが，x は可逆元なので，前命題により $I = R$ である．

逆に，R が体でないとすると，R の中に逆元を持たないような $0 \neq x \in R$ が存在する．$I = Rx$ (これはイデアル) とおく．$I \neq (0)$ である．もし，$I = R$ であると，$1 \in R = I = \{ax \mid a \in R\}$ なので，$ax = 1$ を満たす $a \in R$ が存在し，x が可逆元でないことに反する．よって，$I \neq R$ である． □

2. 準同型写像，素イデアル・極大イデアル

定義 2.1.(準同型写像) R, S は可換環とする．写像 $f\colon R \to S$ が以下の (1), (2) を満たすとき，f は (可換環としての) **準同型** (写像) (homomorphism) であるという.

(1) $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ $(a, b \in R)$

(2) $f(1_R) = 1_S$

上の定義から，$f(0_R) = 0_S$ も導かれる．また，$a \in R$ が R の可逆元ならば $f(a^{-1}) = f(a)^{-1}$ なので，$f(a)$ は S の可逆元である．整域や体の準同型写像は可換環の準同型写像のことを言う.

環の準同型写像 $f\colon R \to S$ を 1 つ固定するとき，$a \in R$, $x \in S$ に対して $ax = f(a)x$ と定義することにより，S は R-代数の構造を持つ.

準同型写像 $f\colon R \to S$ が全単射であるとき，$f^{-1}\colon S \to R$ も準同型写像でり，このとき f は**同型** (写像) であるといい，$f\colon R \xrightarrow{\cong} S$ とか $R \cong S$ と書く.

M, N は R-加群とする．写像 $f\colon M \to N$ が以下の (1), (2) を満たすとき，f は (R-加群としての) **準同型** (写像) であるとか，R-**準同型** (写像) であるという.

(1) $f(x+y) = f(x) + f(y)$ $(x, y \in M)$

(2) $f(ax) = af(x)$ $(a \in R, x \in M)$

特に，R が体のとき R-加群としての準同型写像を，**線形写像**とか **1 次変換**とも言う.

準同型写像 $f\colon M \to N$ に対し，

$$\operatorname{Ker} f = f^{-1}(0) = \{a \in R \mid f(a) = 0\}, \quad \operatorname{Im} f = f(M), \quad \operatorname{Coker} f = N/\operatorname{Im} f$$

と書く．$\operatorname{Ker} f$ は M の R-部分加群, $\operatorname{Im} f$ は N の R-部分加群である．f が全単射のとき，f は**同型**写像であるといい，$f\colon M \xrightarrow{\cong} N$ とか $M \cong N$ と書く.

群の準同型定理より，アーベル群として $\operatorname{Coim} f := M/\operatorname{Ker} f \cong \operatorname{Im} f$ であるが，これは R-加群としての同型であるので，$\operatorname{Coim} f$ を用いる必要はない．(次数付き加群などでは，上の同型が成り立たないので $\operatorname{Coim} f$ が必要になる.)

A, B は R-加群とする．写像 $f\colon A \to B$ が可換環としての準同型であって，かつ R-加群としての準同型であるとき，f は R-代数としての**準同型** (写像) であると言う.

定理 2.2.(準同型定理, etc.) R, S は可換環，$f\colon R \to S$ は準同型写像とする．このとき，以下が成り立つ.

(1) $f(R)$ は S の部分環である.

(2) $\operatorname{Ker} f$ は R のイデアルである.

(3) J が S のイデアルならば $f^{-1}(J)$ は R のイデアルである.

(4) f が全射で J が S のイデアルならば，$f\big(f^{-1}(J)\big) = J$ が成り立つ．特に，J_1, J_2 が S のイデアルで $J_1 \subsetneqq J_2$ ならば，$f^{-1}(J_1) \subsetneqq f^{-1}(J_2)$ が成り立つ.

(5) f が全射で I が R のイデアルならば，$f(I)$ は S のイデアルである．(注意．f が全射でないと成立しない.)

(6) f は全射，I_1, I_2 は R のイデアルで，$\operatorname{Ker} f \subset I_1 \subsetneqq I_2$ を満たすとする．すると，$f(I_1) \subsetneqq f(I_2)$ が成り立つ.

(7) $R/(\operatorname{Ker} f) \cong f(R)$ (可換環として同型) である.

証明. (1) 〜 (6) は簡単なので，練習問題とする.

(7) 群の準同型定理から，f から誘導される写像 $\overline{f}\colon R/(\operatorname{Ker} f) \longrightarrow f(R)$ はアーベル群としての同型写像である．これが，積の構造を保つことは容易に確認できるので，可換環としても同型である． □

なお $f(R) = \operatorname{Im} f$ は S の部分環であるが，$R \neq 0$, $S \neq 0$ ならば，$f(R)$ は S のイデアルにはならない．

定義 2.3.(素イデアル，極大イデアル) R は可換環 I はイデアルとする．
(1) $a, b \in R$, $ab \in I$ ならば $a \in I$ または $b \in I$ が成り立つとき，I は R の**素イデアル** (prime ideal) であるという．対偶を書けば，$a, b \notin I$ ならば $ab \notin I$ である．
(2) $I \subsetneqq J \subsetneqq R$ を満たすイデアル J が存在しないとき，I は R の**極大イデアル** (maximal idel) であるという．

命題 2.4. R は可換環，I はイデアルとする．
(1) I が R の素イデアルであるための必要十分条件は，R/I が整域であることである．
(2) I が R の極大イデアルであるための必要十分条件は，R/I が体であることである．
(3) R の極大イデアルは R の素イデアルである．
(4) R が整域であるための必要十分条件は，(0) が R の素イデアルであることである．

証明. 一般に $a \in R$ に対し，I を法とする a の剰余類を $\overline{a} \in R/I$ と書くことにする．
(1) I は R の素イデアルとする．R/I の 0 でない 2 元 $\overline{a}, \overline{b} \in R/I$ $(a, b \in R)$ を取る．$\overline{0}$ でないので $a \notin I, b \notin I$ である．I は素イデアルなので $ab \notin I$ である．よって，$\overline{a}\overline{b} \neq \overline{0}$ で，R/I は整域である．
逆に，イデアル $I \subset R$ が素イデアルでなければ，$a \notin I$, $b \notin I$, $ab \in I$ となる $a, b \in R$ が存在する．R/I の 0 でない 2 元 $\overline{a}, \overline{b} \in R/I$ $(a, b \in R)$ このとき，$\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$, $\overline{a}\overline{b} = \overline{0}$ となり，R/I は 0 でないゼロ因子を持つので R/I は整域でない．

(2) R/I が体であるとする．自然な全射 $f\colon R \to R/I$ を考える．もし，$I \subsetneqq J \subsetneqq R$ となるイデアル J が存在すれば，$f(J)$ は R/I のイデアルである．R/I のイデアルは (0) と R/I しかない．$f(J) = 0$ ならば $J = I$, $f(J) = R/I$ ならば $J = R$ となり矛盾する．
もし，R/I が体でなければ，0 以外の非可逆元 $\overline{a} \in R/I$ $(a \in R)$ が存在する．$J = I + Ra$ は I のイデアルで，$a \notin I$ だから $I \subsetneqq J$ である．しかし，もし $J = R$ ならば $1 = x + ra$ を満たす $x \in I, r \in R$ があり，$\overline{ra} = \overline{1}$ となり，$\overline{a}$ が非可逆元であることに矛盾する．よって，$I \subsetneqq J \subsetneqq R$ で I は極大イデアルでない．

(3) 体は整域であることと，(1), (2) よりわかる．

(4) R は整域とする．$a, b \in R$, $ab \in (0)$ ならば $ab = 0$ であるが，R は整域だから $a = 0$ または $b = 0$ であり，$a \in (0)$ または $b \in (0)$ となる．よって，(0) は素イデアルである．
R が整域でないとすると，$0 \neq a \notin (0)$, $0 \neq b \notin (0)$, $0 = ab \in (0)$ となる $a, b \in R$ があるので，(0) は素イデアルでない． □

定理 2.5. R は可換環，$R \neq I$ はイデアルとする．すると，$I \subset \mathfrak{m}$ を満たす極大イデアル $\mathfrak{m}$ が存在する．(ただし，複数個存在するかもしれない.)

証明. $\mathcal{A} = \left\{ J \,\middle|\, J \text{ は } R \text{ のイデアルで } I \subset J \subsetneqq R \right\}$ とおく．包含関係を順序として $\mathcal{A}$ を (半) 順序集合と考える．(全順序集合 (tatally orderd set) とは限らない順序集合を，全順序集合と区別するために半順序集合 (partially orderd set) ともいう.) $\mathcal{L} \subset \mathcal{A}$ を任意の全順序部分集合とするとき，$\sup \mathcal{L} = \bigcup_{J \in \mathcal{L}} J \in \mathcal{A}$ であることは容易に証明できる．よって，$\mathcal{A}$ は帰納的順序集合であり，Zorn の補題により極大元 $\mathfrak{m}$ が存在する．$\mathfrak{m} \subsetneqq J \subsetneqq R$ となるイデアル J があると，J は $\mathfrak{m}$ より真に大きい $\mathcal{A}$ の元となって矛盾するので．$\mathfrak{m}$ は極大イデアルである． □

命題 2.6. 可換環 $\mathbb{Z}$ において，以下が成り立つ．
(1) $\mathbb{Z}$ のイデアル I は，ある非負整数 n により，$I = (n) = n\mathbb{Z}$ と表すことができる．
(2) (0) 以外の素イデアル I は，ある素数 p により，$I = (p)$ と書ける．また，(p) は極大イデアルである．

証明. (1) I を (0) でない $\mathbb{Z}$ のイデアルとする．$x \in I$ ならば $-x \in I$ だから，I はある自然数を含む．I に含まれる最小の自然数を n とする．$I = (n)$ を示す．勝手な $x \in I$ を取る．x を n で割った商を q,

あまりを r とする．$0 \leqq r < n$, $r = x - nq \in I$ だから，n の最小性から $r = 0$ で，$x = nq \in n\mathbb{Z} = (n)$ となる．よって，$I \subset (n)$ である．$(n) \subset I$ は自明なので，$I = (n)$ である．

(2) p が素数ならば，$\mathbb{Z}/(p) = \mathbb{F}_p$ は体だから，(p) は極大イデアルであり，特に素イデアルである．逆に，n が合成数ならば $\mathbb{Z}/n\mathbb{Z}$ は整域でなかった． □

既約多項式の定義は次節で述べるが，高校までに使っていた「既約」と同じ意味である．

命題 2.7. K を体とし，1 変数多項式環 $K[X]$ を考える．以下が成り立つ．
(1) $K[X]$ の (0) 以外のイデアル I は，あるモニック多項式 $f(X) \in K[X]$ により，$I = (f(X))$ と表すことができる．
(2) (0) 以外の素イデアル I は，ある既約なモニック多項式 $p(X)$ により，$I = (p(X))$ と書ける．また，$(p(X))$ は極大イデアルである．

証明. (1) I を (0) でない $K[X]$ のイデアルとする．I に含まれる次数最小の多項式を $f(X)$ とする．$f(X)$ の最高次の係数を a_n とすると，$a_n^{-1} \in K \subset K[X]$ だから $a_n^{-1} f(X) \in I$ である．よって，はじめから $f(X)$ はモニック多項式であると仮定してよい．

$I = (f(X))$ を示す．勝手な $g(X) \in I$ を取る．$g(X)$ を $f(X)$ で割った商を $q(X)$, あまりを $r(X)$ とする．$\deg r(X) < \deg f(X)$, $r(X) = g(X) - f(X)q(X) \in I$ だから，$\deg f(X)$ の最小性から $r(X) = 0$ で，$g(X) = f(X)g(X) \in (f(X))$ となる．よって，$I = (f(X))$ である．

(2) $\mathbb{Z}$ の場合と同様である． □

命題 2.8. R, S は可換環，$f\colon R \to S$ は準同型写像とする．
(1) $J \subset S$ は素イデアルとする．もし，$f^{-1}(J) \neq R$ ならば $f^{-1}(J)$ は R の素イデアルである．
(2) f は全射，$I \subset R$ は素イデアルで，$I \supset \operatorname{Ker} f$ とする．すると，$f(I)$ も S の素イデアルである．また，I が極大イデアルならば $f(I)$ も極大イデアルである．

証明. (1) 準同型定理より，単射準同型写像 $R/f^{-1}(J) \longrightarrow S/J$ が存在する．この単射準同型写像を通して $R/f^{-1}(J) \subset S/J$ と考える．S/J は整域であって，$R/f^{-1}(J) \neq 0$ なので，$R/f^{-1}(J) \neq 0$ も整域である．または，$R/f^{-1}(J) \cong f(R)/(J \cap f(R)) \subset S/J$ を利用してもよい．

(2) f から誘導される全射 $g\colon R \to S/f(I)$ について，$\operatorname{Ker} g = I$ となるので，準同型定理より $R/I \cong S/f(I)$ である．これより結論を得る． □

3. PID と UFD

定義 3.1.(PID) 可換環 R において，$I = (a) = Ra$ $(a \in R)$ という形のイデアルを**単項イデアル**という．

R が整域であって，R の任意のイデアルが単項イデアルであるとき，R を**単項イデアル整域** (Principal Ideal Domain), 略して **PID** という．

例えば，$\mathbb{Z}$ は命題 2.6 より PID であり，K が体のとき K 上の 1 変数多項式環 $K[X]$ は命題 2.7 より PID である．

定義 3.2.(既約元，素元) R は整域，$0 \neq x \in R$ とする．
(1) x が R で**既約** (irreducible) であるとは,「$y, z \in R$，$x = yz$ ならば y または z が可逆元」が成り立つことを言う．可逆元でない $y, z \in R$ により $x = yz$ と書けるとき，x は**可約** (reducible) であると言う．
(2) x が R の**素元** (prime) であるとは，$x \neq 0$ で，単項イデアル (x) が R の素イデアルであることを言う．
(3) $x, y \in R$ が**同伴**であるとは，ある可逆元 $u \in R$ により $y = ux$ と書けることをいう．
(4) $x = yz$ $(y, z \in R)$ のとき，x は y の**倍数** (multiple) または**倍元**, y は x の**約数** (divisor) または**約元**であると言い，$y|x$ と書く．これは $(x) \subset (y)$ と同値である．
(5) $x = y_1 y_2 \cdots y_n$ (y_1, y_2,..., y_n は既約元) と書けるとき，これを x の**既約元分解**と言う．

(6) $x = y_1y_2\cdots y_n = z_1z_2\cdots z_m$ (y_1,..., y_n, z_1,..., z_m は既約元) と書けるたとする．もし，$m = n$ であって，1, 2,..., n の置換 (並べ替え) i_1, i_2,..., i_n をうまく選ぶと，各 $j = 1, 2, \ldots, n$ に対し x_j と y_{i_j} が同伴になるとき，2 つの既約元分解 $x = y_1y_2\cdots y_n = z_1z_2\cdots z_m$ は**本質的に同じ**であるという．そうでないとき，**本質的に異なる**という．

問 3.3. $R = \mathbb{Z}[\sqrt{5}] = \left\{a + b\sqrt{5} \;\middle|\; a, b \in \mathbb{Z}\right\}$ とおく，R は $\mathbb{Q}$ の部分環なので整域である．

(1) $x = a + b\sqrt{5} \in R$ ($a, b \in \mathbb{Z}$) が R の可逆元であるための必要十分条件は，$a^2 - 5b^2 = \pm 1$ であることを示せ．

(2) 2, $\sqrt{5} + 1$, $\sqrt{5} - 1$ は R の既約元であることを示せ．(ヒント: $x = a + b\sqrt{5}$ ($a, b \in \mathbb{Z}$) に対し，$N(x) = \left|a^2 - 5b^2\right| \in \mathbb{Z}$ と定義し，$N(xy) = N(x)N(y)$ が成り立つことを示して使うと簡単.)

(3) $4 = 2 \times 2 = (\sqrt{5} + 1)(\sqrt{5} - 1)$ は本質的に異なる既約元分解であることを示せ．

命題 3.4. 整域 R において，素元は既約元である．

証明. $p \in R$ を素元とし，$p = xy$ ($x, y \in R$) とする．$R/(p)$ での同値類を考えるとき，$\overline{x}\overline{y} = \overline{p} = 0$ である．$R/(p)$ は整域なので，$\overline{x} = 0$ または $\overline{y} = 0$ である．議論は対称なので，$\overline{x} = 0$ とする．すると，$x \in (p)$ であり，$x = pz$ ($\exists z \in R$) と書ける．$p = xy = pyz$ より $p(yz - 1) = 0$ である．p は非零因子なので $yz = 1$ である．よって，y は可逆元であり，p は既約元である． □

定義 3.5.(UFD) R が整域で，次の条件 (1) を満たすとき，R は**素元分解整域** (Uniquely Factorization Domain)，略して **UFD** と言う．

(1) $x \in R$ が可逆元でも 0 でもなければ，ある有限個の素元 p_1, p_2,..., p_n が存在して，$x = p_1p_2\cdots p_n$ と書ける．これを x の**素元分解**という．

前命題により，素元分解は既約元分解である．

補題 3.6. R は可換環，$\mathfrak{p}$ は R の素イデアルとする．a_1,..., $a_n \in R$, $a_1a_2\cdots a_n \in \mathfrak{p}$ であれば，ある $1 \leqq i \leqq n$ が存在して $a_i \in \mathfrak{p}$ である．

証明. n に関する帰納法で簡単に証明できるので，練習問題とする． □

定理 3.7. R は UFD とする．このとき次が成り立つ．

(1) R の既約元は素元である．

(2) p_i, q_j は R の素元，u は可逆元で，$p_1p_2\cdots p_n = uq_1q_2\cdots q_m$ であるとする．すると，$m = n$ であって，1, 2,..., n の置換 i_1, i_2,..., i_n をうまく選ぶと，各 $j = 1, 2, \ldots, n$ に対し p_j と q_{i_j} は同伴になる．

(1), (2) より，R における 2 つの既約元分解 $x = y_1y_2\cdots y_n = z_1z_2\cdots z_m$ は，本質的に同じである．このことを，R において**既約元分解の一意性が成り立つ**という．

証明. (1) x は既約元であるとする．$x = p_1p_2\cdots p_n$ を素元分解とする．もし，$n \geqq 2$ ならば，既約元の定義から p_1 または $(p_2\cdots p_n)$ が可逆元になる．p_1 は素元だから可逆元でない．$p_2\cdots p_n$ が可逆元ならば，$p_2, p_3, \ldots, p_n$ はすべて可逆元となり矛盾する．よって，$x = p_1$ で x は素元である．

(2) $m \geqq n$ と仮定してよい ($m < n$ なら $q_1\cdots q_m = u^{-1}p_1\cdots p_n$)．$n$ に関する帰納法で証明する．

$n = 1$ とする．$uq_1\cdots q_m = p_1 \in (p_1)$ である．(p_1) は素イデアルなので，前補題により $q_i \in (p_1)$ を満たす i がある．q_1,..., q_m を並び変えて添え字を付け替え，$q_1 \in (p_1)$ と仮定してよい．$q_1 = ap_1$ ($\exists a \in R$) と書ける．すると，$p_1 = p_1(auq_2q_3\cdots q_m)$ となる．p_1 は非零因子なので，$auq_2q_3\cdots q_m = 1$ である．もし，$m \geqq 2$ なら q_m は可逆元となり素元でない．よって，$m = 1$ で $au = 1$ である．$q_1 = ap_1$ で a は可逆元なので，p_1 と q_1 は同伴である．

$n \geqq 2$ とし，$n - 1$ までの結果を仮定する．$q_1q_2\cdots q_m = u^{-1}p_1p_2\cdots p_n \in (p_1)$ で，(p_1) は素イデアルなので，前補題により $q_i \in (p_1)$ を満たす i がある．q_1,..., q_m を並び変えて添え字を付け替え，$q_1 \in (p_1)$ と仮定してよい．$q_1 = ap_1$ ($\exists a \in R$) と書ける．$n = 1$ の場合の結果から，p_1 と q_1 は同伴であり，a は可逆元である．また，$p_2p_3\cdots p_n = (au)q_2q_3\cdots q_m$ で (au) は可逆元である．帰納法の仮定から，$m = n$ で q_2,..., q_n を適当に並びかえると，それぞれ p_2,..., p_n と同伴になる． □

定理 3.8. PID は UFD である．

証明. R は PID とし，$0 \neq x_0 \in R$ は可逆元でないとする．x_0 が有限個の素元の積に表せることを証明すればよい．

(x_0) が素イデアルなら $x_0 = x_0$ が素元分解だから，x_0 は素元ないとする．定理 2.5 より，(x_0) を含む極大イデアル $\mathfrak{m}_1$ が存在する．R は PID なので，$\mathfrak{m}_1 = (p_1)$ (p_1 は素元) と書ける．$x_0 \in (x_0) \subset (p_1)$ なので，$x_0 = p_1 x_1$ ($\exists x_1 \in R$) と書ける．x_0 は素元でないから，x_1 は可逆元でも 0 でもない．

もし，x_1 が素元でなければ，同様に，$x_1 = p_2 x_2$ (p_2 は素元で，x_2 は可逆元でも 0 でもい) と書ける．以下，帰納的に，x_{n-1} が素元でなければ，$x_{n-1} = p_n x_n$ (p_n は素元で，x_n は可逆元でも 0 でもい) と書ける．このとき，$x_0 = p_1 p_2 \cdots p_n x_n$ である．x_n が素元なら，これが x_0 の素元分解である．

そこで，任意の $n \in \mathbb{N}$ に対し，x_n は素元でないと仮定して矛盾を導く．$x_{n-1} = p_n x_n \in (x_n)$ だから，$(x_{n-1}) \subset (x_n)$ である．もし，$(x_{n-1}) = (x_n)$ ならば $x_n \in (x_{n-1})$ だから，$x_n = b x_{n-1}$ ($\exists b \in R$) と書け，$x_{n-1} = (bp_n)x_{n-1}$, $p_n = b^{-1}$ となり p_n が可逆元でないことに矛盾する．よって，$(x_{n-1}) \subsetneqq (x_n)$ である．$I = \bigcup_{n=0}^{\infty} (x_n)$ とおく．I がイデアルであることはすぐわかる．$I = (c)$ ($\exists c \in R$) と書ける．I の定義から，ある $n \in \mathbb{N}$ をとれば $c \in (x_n)$ となる．$x_{n+1} \in I = (c) \subset (x_n)$ なので，$x_{n+1} = v x_n$ ($\exists v \in R$) と書ける．すると，$x_n = p_{n+1} x_{n+1} = (v p_{n+1}) x_n$, $p_{n+1} = v^{-1}$ となり p_{n+1} が可逆元でないことに矛盾する． □

定理 3.9. PID においては，(0) でない素イデアルは極大イデアルである．

証明. R は PID で，$(0) \neq \mathfrak{p} \subsetneqq R$ は素イデアルとする．$\mathfrak{p} = (p)$ (p は R の素元) と書ける．$\mathfrak{p}$ を含む R の極大イデアル $\mathfrak{m}$ が存在する．$\mathfrak{m} = (m)$ (m は R の素元) と書ける．$p \in (p) \subset (m)$ なので $p = am$ ($\exists a \in R$) と書ける．R は UFD なので，定理 3.9 より p と m は同伴で a は可逆元である．よって $(p) = (m)$ となり，$\mathfrak{p} = (p)$ は極大イデアルである． □

定義 3.10. R は可換環とする．$\mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_d$ は R の素イデアルで，

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d \qquad ①$$

を満たすとする．① を R の**素イデアル列**といい，d をその**長さ**という．添え字は必ず 0 から始めること．たとえば，1 個だけの素イデアルの列 $\mathfrak{p}_0$ の長さは 0 である (1 ではない)．R のすべての素イデアル列を考えるとき，その長さ d に最大値が存在すれば，その最大値を $\operatorname{Krull\,dim} R$ と書き，R の**クルル次元** (Krull dimension) という．任意の $d \in \mathbb{N}$ に対し，長さ d の素イデアル列が存在する場合は $\operatorname{Krull\,dim} R = \infty$ と約束する．

命題 3.11. (1) K が体ならば $\operatorname{Krull\,dim} K = 0$ である．
(2) R が PID ならば $\operatorname{Krull\,dim} K = 1$ である．

証明. (1) 体 K のイデアルは (0) と K の 2 個しかなく，素イデアルは (0) だけである．よって，長さ 0 の素イデアル列 (0) が，最大の長さを与える．
(2) PID R の (0) でない素イデアル (p) は極大イデアルなので，長さ 1 の素イデアル列 $(0) \subsetneqq (p)$ が長さ最大である． □

参考 3.12. K は体 $R = K[X_1, \ldots, X_n]$, $\mathfrak{p}_i = (X_1, X_2, \ldots, X_i) \subset R$ とする．$R/\mathfrak{p}_i \cong K[X_{i+1}, X_{i+2}, \ldots, X_n]$ でこれは整域なので，$\mathfrak{p}_i$ は R の素イデアルである．よって，長さ n の素イデアル列 $(0) \subsetneqq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ が存在し，$\operatorname{Krull\,dim} K[X_1, \ldots, X_n] \geqq n$ が分かる．実は，$= n$ であるが，その証明には多くの準備が必要で，ずっと後で学習する．

4. 多項式環

体 K 上の多項式環 $K[X_1, \ldots, X_n]$ が UFD であることを証明したいが，少し準備が必要である．

定義 4.1.(最大公約数, 最小公倍数) R は UFD, $x_1, x_2, \ldots, x_n \in R$ はいずれも 0 でないとする．UFD では素元分解の一意性が成立するので，$x_1, \ldots, x_n$ の素元分解に現れる素元を全部集めたものを $p_1, \ldots, p_r$ とする．ただし，$i \neq j$ のとき p_i と p_j は同伴でないとする．

$$x_i = u_i p_1^{e_{i,1}} p_2^{e_{i,2}} \cdots p_r^{e_{i,r}} \quad (u_i \text{ は可逆元で，各 } e_{i,j} \text{ は非負整数})$$

と素元分解する．

$$m_j = \max\{e_{1,j}, e_{2,j}, \ldots, e_{n,j}\}, \quad l_j = \min\{e_{1,j}, e_{2,j}, \ldots, e_{n,j}\}$$

として，

$$\mathrm{LCM}(x_1, \ldots, x_n) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}, \quad \mathrm{GCD}(x_1, \ldots, x_n) = p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$$

と定める．$\mathrm{LCM}(x_1, \ldots, x_n)$ と $\mathrm{GCD}(x_1, \ldots, x_n)$ は同伴を除いて一意的に定まる．$\mathrm{LCM}(x_1, \ldots, x_n)$ を $x_1, \ldots, x_n$) の**最小公倍数**とか**最小公倍元** (Least Common Multiple) という．$\mathrm{GCD}(x_1, \ldots, x_n)$ を $x_1, \ldots, x_n$) の**最大公約数**とか**最大公約元** (Greatest Common Divisor) という．

$R = K[X]$ (K は体) の場合には，最小公倍数，最大公約数は，いずれも最高次の項の係数で割っておいて，モニック多項式になるように選ぶ．

補題 4.2. R は整域とし，$r \in R$ とする．このとき，

$$R[X]/rR[X] \cong (R/rR)[X]$$

が成り立つ．特に，rR が R の素イデアルならば，$rR[X]$ は $R[X]$ の素イデアルである．つまり，r が R の素元ならば r は $R[X]$ の素元である．

証明. $a \in R$ に対し，rR を法とする同値類を $\overline{a} \in R/rR$ と書く．

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in R[X] \qquad ①$$

に対し，$\overline{f}(X) = \overline{a_n} X^n + \overline{a_{n-1}} X^{n-1} + \cdots + \overline{a_1} X + \overline{a_0} \in (R/rR)[X]$ を対応させる写像を $\varphi : R[X] \longrightarrow (R/rR)[X]$ とおく．φ は全射準同型写像である．$\mathrm{Ker}\,\varphi = rR[X]$ を証明すればよい．$f(X) \in rR[X]$ ならば $\overline{f}(X) = 0$ なので，$\mathrm{Ker}\,\varphi \supset rR[X]$ である．

$\mathrm{Ker}\,\varphi \subset rR[X]$ を示す．①のような $f(X)$ に対して $\overline{f}(X) = 0$ ならば $\overline{a_n} = \overline{a_{n-1}} = \cdots \overline{a_1} = \overline{a_0} = 0$ なので，$a_n = rb_n$, $a_{n-1} = rb_{n-1}, \ldots, a_1 = rb_1$, $a_0 = rb_0$ ($b_n, \ldots, b_0 \in R$) と書ける．$g(X) = b_n X^n + \cdots + b_1 X + b_0 \in R[X]$ とおけば，$f(X) = rg(X)$ である．よって，$\mathrm{Ker}\,\varphi \subset rR[X]$ である．したがって，φ は同型写像 $\overline{\varphi} : R[X]/rR[X] \xrightarrow{\cong} (R/rR)[X]$ を誘導する．

rR が R の素イデアル (つまり r が R の素元) のとき，R/pR は整域だから，$R[X]/rR[X] \cong (R/rR)[X]$ も整域である．よって，$rR[X]$ は $R[X]$ の素イデアルで，r は $R[X]$ の素元である． □

R が整域とは限らないときの分数の話は後でするが，さしあたって分数体だけ先に使う．

定義 4.3. R は整域とする．このとき，分数の集合

$$Q(R) := \left\{ \frac{a}{b} \;\middle|\; a, b \in R, b \neq 0 \right\}$$

は，通常の分数の和，積により体になる．$Q(R)$ を R の**分数体**という．R の元 a と $\dfrac{a}{1} \in Q(R)$ を同一視して $R \subset Q(R)$ と考える．

正確な話は，後の局所化のところで話すが，整域でない可換環で分数を考えるためには細心の注意が必要であるが，特に R が UFD の場合の分数は高校までに扱ってきた分数の取り扱いと大差ない．

$Q(R)$ は体なので $Q(R)[X]$ は PID であり UFD である．$R[X] \subset Q(R)[X]$ なので，$Q(R)[X]$ の素元分解を利用して $R[X]$ の既約元分解を考察する．

定理 4.4. R が UFD ならば $R[X]$ も UFD である．

証明. 一般に，$g(X) = \sum_{i=0}^{n} b_i X^i \in R[X]$ の係数が生成するイデアルが $(b_0, \ldots, b_n) = R$ を満たすとき，$g(X)$ は原始多項式であるという．

$g(X)$ は原始多項式で，$f(X) \in R[X]$ とする．$K = Q(R)$ として，ある $h(X) \in K[X]$ により $f(X) = g(X)h(X)$ と書けたと仮定する．このとき，$h(X) \in R[X]$ であることを証明する．

$h(X)$ の係数の分母の最小公倍数を d_1 とする．また $d_1h(X)$ の係数の最大公約数を d_2 とする．このとき，$h_0(X) = (d_1/d_2)h(X)$ とおくと $h_0(X) \in R[X]$ で，$h_0(X)$ は原始多項式である．いま，分数 d_1/d_2 を約分して，d_1 と d_2 は互いに素と仮定してよい．$d_1f(X) = d_2g(X)h_0(X)$ である．もし，d_1 が R の可逆元でないとすると，d_1 の約数であるような R の素元 p が存在する．$pR[X]$ は $R[X]$ の素イデアルで，$d_1f(X) = d_2g(X)h_0(X) \in pR[X]$ なので，d_2, $g(X)$, $h_0(X)$ のいずれかは $pR[X]$ に属する．仮定から d_2 は p の倍数でなく，$g(X)$ と $h_0(X)$ は原始多項式なので p の倍数でない．これは矛盾である．よって，d_1 は R の可逆元である．したがって，$h(X) = (d_2/d_1)h_0(X) \in R[X]$ である．

これを利用して $R[X]$ が UFD であることを証明する．$R[X]$ 内の 0 でも可逆元でもない勝手な元 $f(X)$ をとる．$f(X)$ の次数に関する帰納法で証明する．$f(X)$ が 0 次式ならば $f(X) \in R$ なので，R の中で素元分解すればそれが $R[X]$ での素元分解になる．

$f(X)$ は 1 次以上と仮定する．$K[X]$ は UFD なので，$K[X]$ の中で $f(X) = p_1(X)\cdots p_r(X)$ と素元分解する．$p_1(X)$ の係数の分母の最小公倍数を d_1, 分母の最大公約数を e_1 とし，$q_1(X) = (d_1/e_1)p_i(X)$ とする．$q_1(X)$ は $R[X]$ の原始多項式である．$h(X) = (e_1/d_1)p_2(X)\cdots p_r(X) \in K[X]$ とおけば，$f(X) = q_1(X)h(X)$ である．$q_1(X)$ が原始多項式だから，上に証明したように $h(X) \in R[X]$ となる．$q_1(X)$, $h(X)$ の次数は $f(X)$ の次数より小さいから，帰納法の仮定により $q_1(X)$, $h(X)$ は $R[X]$ の素元の積に因数分解できる． □

系 4.5. R が UFD ならば R 上の n 変数多項式環 $R[X_1,\ldots, X_n]$ も UFD である．

証明. $n = 1$ の時は前定理．$n \geqq 2$ とし，帰納法で $R[X_1,\ldots, X_{n-1}]$ が UFD ならば，$R[X_1,\ldots, X_n] = \big(R[X_1,\ldots, X_{n-1}]\big)[X_n]$ も UFD である． □

系 4.6. K が体ならば $K[X_1,\ldots, X_n]$ は UFD である．

証明. $K[X_1]$ は UFD であった． □

例 4.7. K は体とする．
(1) $f(X) \in K[X]$ が 1 次以上の既約多項式ならば，$K[X]/(f)$ は体である．ここで，$(f) = (f(X)) = f(X)K[X]$ である．
(2) $f(X) = aX + b$, $a \neq 0$ ならば，$K[X]/(f) \cong K$ である．
(3) $f(X)$ が $\mathbb{R}[X]$ の 2 次既約多項式ならば，$\mathbb{R}[X]/(f) \cong \mathbb{C}$ である．

証明. (1) $f(X) \in K[X]$ が既約元なら素元であるので，(f) は素イデアルである．$K[X]$ は PID なので (f) は極大イデアルで，$K[X]/(f)$ は体である．

(2) 写像 $\varphi : K[X] \longrightarrow K$ を $\varphi(g(X)) = g(-b/a) \in K$ $(g(X) \in K[X])$ によって定義する．φ が全射準同型写像であることは，簡単に確認できる．$\varphi(aX + b) = 0$ なので $(aX + b) \subset \mathrm{Ker}\,\varphi$ である．また，$g(X) \in \mathrm{Ker}\,\varphi$ ならば，高校の数学 II で習った因数定理より，$g(X)$ は $(aX + b)$ の倍数であるので，$g(X) \in (aX + b)$ である．よって，$\mathrm{Ker}\,\varphi = (aX + b)$ である．準同型定理より，$K[X]/(aX + b) \cong K$ である．

(3) 2 次方程式 $f(X) = 0$ の 2 つの複素数解を $X = p \pm q\sqrt{-1}$ $(p, q \in \mathbb{R})$ とする．ここで $q \neq 0$ である．
一般に $g(X) \in K[X]$ に対し $g(X)$ を $f(X)$ で割った商を $g(X)$, あまりを $r(X) = aX + b$ とする．$\varphi(g(X)) = g(a + b\sqrt{-1}) = a(p + q\sqrt{-1}) + b \in \mathbb{C}$ により，写像 $\varphi : \mathbb{R}[X] \longrightarrow \mathbb{C}$ を定める．φ が全射準同型写像であることは，簡単に確認できる．
$\mathrm{Ker}\,\varphi = (f)$ を示せばよい．$\varphi(f) = 0$ だから $\mathrm{Ker}\,\varphi \supset (f)$ である．また，$\varphi(g(X)) = 0$ ならば $ap + b = 0$, $aq = 0$, $q \neq 0$ より，$a = 0$, $b = 0$ となり，$g(X) \in (f)$ となる，よって，$\mathrm{Ker}\,\varphi = (f)$ で，$\mathbb{R}[X]/(f) \cong \mathbb{C}$ である． □

5. 中国剰余定理

定義 5.1.(直和) R_1, R_2,..., R_n は可換環とする．直積集合 $R_1 \times R_2 \times \cdots \times R_n$ を (圏論の一般論に合わせるために) $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ と書く．$R_1 \oplus R_2 \oplus \cdots \oplus R_n$ の元は，$\mathbf{a} = (a_1, a_2,\ldots, a_n)$ $(a_1 \in R_1,$

$a_2 \in R_2, \ldots, a_n \in R_n$) と表すことができる．また，$\mathbf{b} = (b_1, b_2, \ldots, b_n)$ ($b_1 \in R_1, \ldots, b_n \in R_n$) に対し，和と積を

$$\mathbf{a} + \mathbf{b} = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$
$$\mathbf{ab} = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

と定める．すると，$R_1 \oplus R_2 \oplus \cdots \oplus R_n$ は，$(0, 0, \ldots, 0)$ をゼロ，$(1, 1, \ldots, 1)$ を単位元とする可換環になる．$R_1 \oplus R_2 \oplus \cdots \oplus R_n$ を $R_1, \ldots, R_n$ の**直和**という．$R_1 \oplus \cdots \oplus R_n$ は $\bigoplus_{i=1}^{n} R_i$ とも書く．

R を可換環，$M_1, M_2, \ldots, M_n$ を R-加群とする．直積集合 $M_1 \times M_2 \times \cdots \times M_n$ を $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ と書き，和と R の作用を，

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$
$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$$

($(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in M_1 \oplus \cdots \oplus M_n$, $a \in R$) で定めると $M_1 \oplus \cdots \oplus M_n$ は R-加群になる．これを $M_1, \ldots, M_n$ の**直和**といい，$\bigoplus_{i=1}^{n} M_i$ とも書く．

R, S が整域であっても $R \oplus S$ は整域に決してならない．実際，$(1,0), (0,1) \in R \oplus S$ はゼロでないが，$(1,0)(0,1) = (0,0)$ となり，ゼロでない零因子を持つ．

定義 5.2.(イデアルの積) R は可換環，I, J は R のイデアルとする．

$$IJ = \left\{ \sum_{i=1}^{r} a_i b_i \;\middle|\; r \in \mathbb{N} \text{ で } a_i \in I, b_i \in J \ (i = 1, \ldots, r) \right\}$$

とおく．IJ が R のイデアルになることは容易にわかる．ここで，$\{ab \mid a \in I, b \in J\}$ は R のイデアルになるとは限らず，これは IJ とは必ずしも一致しないことに注意する．

$I_1, I_2, \ldots, I_n$ が R のイデアルのとき，n に関する帰納的定義により，

$$I_1 I_2 \cdots I_n = (I_1 I_2 \cdots I_{n-1}) I_n$$

として，イデアルの積 $I_1 I_2 \cdots I_n$ を定義する．

$I_2 I_1 = I_1 I_2$ は自明で，$(I_1 I_2) I_3 = I_1 (I_2 I_3)$ も簡単に証明できるので，帰納法で，$I_1 I_2 \cdots I_n$ は上の定義で括弧をつける位置や，積の順序に依存しないことがわかる．

問 5.3. R は可換環，$I_1, I_2, \ldots, I_n$ は R のイデアルとする．
(1) $I_1 \cap I_2 \cap \cdots \cap I_n$ は R のイデアルであることを示せ．
(2) $I_1 I_2 \cdots I_n \subset I_1 \cap I_2 \cap \cdots \cap I_n$ であることを示せ．
(3) $R = \mathbb{Z}$ において $I = (6)$, $J = (8)$ とおく．$IJ = (48)$, $I \cap J = (24)$ であることを示せ．この場合，$IJ \subsetneqq I \cap J$ である．

定理 5.4.(中国剰余定理など) R は可換環，$I_1, I_2, \ldots, I_n$ が R のイデアルとする．今，任意の $1 \leqq i < j \leqq n$ に対し $I_i + I_j = R$ が成り立つと仮定する．このとき $I_1, I_2, \ldots, I_n$ は**互いに素**であると言う．このとき，以下が成り立つ．
(1) $I_1 + (I_2 \cap I_3 \cap \cdots \cap I_n) = R$ である．
(2) $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$ が成り立つ．
(3) $R/(I_1 I_2 \cdots I_n) \cong (R/I_1) \oplus (R/I_2) \oplus \cdots \oplus (R/I_n)$ が成り立つ．

証明. (1) $2 \leqq j \leqq n$ に対し $I_1 + I_j = R \ni 1$ だから，$a_j + b_j = 1$ を満たす $a_j \in I_1, b_j \in I_j$ が存在する．適当に $c_j \in R$ を取れば，

$$1 = \prod_{j=2}^{n} (a_j + b_j) = b_2 b_3 \cdots b_n + \sum_{j=2}^{n} a_j c_j$$

という形に展開できる．ここで，$b_2 b_2 \cdots b_n \in I_2 \cap I_3 \cap \cdots \cap I_n$, $\sum_{j=2}^{n} a_j c_j \in I_1$ なので，$1 \in I_1 + (I_2 \cap I_3 \cap \cdots \cap I_n)$ であり，命題 1.8 より (1) が得られる．

(2) n に関する帰納法で証明する．$I_1I_2 = I_1 \cap I_2$ を示す．$\supset$ を示せばよい．$a_2 + b_2 = 1$, $a_2 \in I_1$, $b_2 \in I_2$ であった．勝手な $x \in I_1 \cap I_2$ を取る．$a_2 \in I_1$, $x \in I_2$ なので $a_2x \in I_1I_2$ である．また，$x \in I_1$, $b_2 \in I_2$ なので $xb_2 \in I_1I_2$ である．よって，$x = a_2x + xb_2 \in I_1I_2$ である．よって，$I_1 \cap I_2 \subset I_1I_2$ である．

$n \geqq 3$ とする．帰納法の仮定から，$I_2I_3 \cdots I_n = I_2 \cap I_3 \cap \cdots \cap I_n$ である．(1) より，$I_1 + I_2I_3 \cdots I_n = R$ である．$n = 2$ の場合の結果から，

$$I_1I_2 \cdots I_{n-1}I_n = I_1(I_2 \cdots I_{n-1}I_n) = I_1 \cap (I_2 \cdots I_n) = I_1 \cap (I_2 \cap \cdots \cap I_n)$$

となり，(2) を得る．

(3) $I = I_1I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$ とおく．$a \in R$ に対し，I_j を法とする同値類を $[a]_j \in R/I_j$ と書き，I を法とする同値類を $\overline{a} \in R/I$ と書くことにする．$a \in R$ に対し $\varphi(a) = \big([a]_1, [a]_2, \ldots, [a]_n\big) \in (R/I_1) \oplus (R/I_2) \oplus \cdots \oplus (R/I_n)$ として，写像 $\varphi : R \longrightarrow ((R/I_1) \oplus \cdots \oplus (R/I_n))$ を定める．φ が環の準同型写像であることは容易にわかる．

φ が全射であることを示す．勝手な $(x_1, \ldots, x_n) \in ((R/I_1) \oplus \cdots \oplus (R/I_n))$ を取る．ある $r_j \in R$ により $x_j = [r_j]_j$ と書ける．

I_k 以外の $I_1, \ldots, I_n$ の共通部分を $J_k = \bigcap_{j \neq k} I_j$ とおく．(1) より，$c_k + d_k = 1$ を満たす $c_k \in I_k$, $d_k \in J_k$ が存在する．$[c_k]_k = 0$ なので $[d_k]_k = 1$ である．他方，$j \neq k$ のとき $J_k \subset I_j$ なので，$[d_k]_j = 0$ である．$r = r_1d_1 + r_2d_2 + \cdots + r_nd_n$ とおく．$j \neq k$ のとき $[r_jd_j]_k = 0$ なので，今の考察から，$[r]_k = [r_kd_k]_k = [r_k]_k = x_k$ となる．よって，$\varphi(r) = (x_1, \ldots, x_n)$ であり，φ は全射である．

$\mathrm{Ker}\,\varphi = I$ を示す．$r \in I$ ならば $[r]_j = 0$ なので $\varphi(r) = 0$ であり，$I \subset \mathrm{Ker}\,\varphi$ である．

逆に，$b \in R$ が $\varphi(r) = 0$ を満たすとすると，$[r]_k = 0$ より $r \in I_k$ である．よって，$r \in I_1 \cap \cdots \cap I_n = I$ であり，$\mathrm{Ker}\,\varphi \subset I$ である．よって，$\mathrm{Ker}\,\varphi = I$ であり，準同型定理から，(3) を得る． □

系 5.5. R は PID で，$p_1, p_2, \ldots, p_n$ はどの 2 つも互いに同伴でない素元とする．$e_1, e_2, \ldots, e_n \in \mathbb{N}$ とし，$a = p_1^{e_1}p_2^{e_2} \cdots p_n^{e_n}$ とする．すると，

$$R/(a) \cong (R/(p_1^{e_1})) \oplus (R/(p_2^{e_2})) \oplus \cdots \oplus (R/(p_n^{e_n}))$$

が成り立つ．

証明. $I_k = (p_k^{e_k})$ とおく．$i \neq j$ のとき $I_i + I_j = R$ であることを示せば，前定理から結論を得る．もし，$I_i + I_j \subsetneqq R$ ならば，$I_i + I_j$ を含む極大イデアル (q) (q は素元) が存在する．$p_i^{e_i} \in (q)$ で p_i が素元なので $p_i = q$ となる．同様に $p_j = q$ となり，p_i と p_j が同伴でないことに矛盾する． □

例 5.6. (1) $\mathbb{R}[X]/(X^2 - 1) \cong \mathbb{R}[X]/(X + 1) \oplus \mathbb{R}[X]/(X - 1) \cong \mathbb{R} \oplus \mathbb{R}$
(2) $\mathbb{C}[X]/(X^2 + 1) \cong \mathbb{C}[X]/(X + \sqrt{-1}) \oplus \mathbb{C}[X]/(X - \sqrt{-1}) \cong \mathbb{C} \oplus \mathbb{C}$

問題 5.7.($\mathbb{Q}$ 上の 2 次体) $f(X) = X^2 + aX + b \in \mathbb{Q}[X]$ が $\mathbb{Q}[X]$ の元として既約であるとする．(f) は $\mathbb{Q}[X]$ の極大イデアルであり，$K = \mathbb{Q}[X]/(f)$ は体になる．ところで，包含写像 $\mathbb{Q} \subset \mathbb{Q}[X]$ と自然な全射 $\mathbb{Q}[X] \to K$ の合成写像 $\varphi{:}\,\mathbb{Q} \to K$ は単射であり，φ を通して $\mathbb{Q} \subset K$ と考えることができる．

$f(X) = 0$ の $\mathbb{C}$ における解の 1 つは $X = \dfrac{a}{2} + \dfrac{\sqrt{a^2 - 4b}}{2}$ であるが，$\dfrac{\sqrt{a^2 - 4b}}{2} = \dfrac{k}{l}\sqrt{m}$ (k と l は互いに素な整数，m は素数の 2 乗で割り切れないような整数) と表わしておく．このとき，

$$K \cong \mathbb{Q}[\sqrt{m}] := \left\{x + y\sqrt{m} \;\middle|\; x, y \in \mathbb{Q}\right\}$$

であることを証明せよ．このような K を $\mathbb{Q}$ 上の 2 次体という．

本題からそれるが，形式的巾級数環について補足をしておく．R が整域ならば $R[[X]]$ は整域である．しかし，R が UFD でも $R[[X]]$ が UFD かどうかはわかならい．K が体のとき $K[[X]]$ が PID であることは，以下の定理を使うと簡単に証明できる．

定理 5.8. R は可換環とし，$f(X) = \sum_{k=0}^{\infty} a_kX^k \in R[[X]]$ ($a_k \in R$) とする．$f(X)$ が $R[[X]]$ の可逆元であるための必要十分条件は，a_0 が R の可逆元であることである．

証明. $g(X)=\sum_{k=0}^{\infty}b_kX^k\in R[[X]]$, $f(X)g(X)=1$ であると仮定する．両辺の定数項を比較すると，$a_0b_0=1$ なので，a_0 は R の可逆元である．

逆に，a_0 が R の可逆元であると仮定する．$b_0=a_0^{-1}$ とおく．帰納的に，$b_0,\ldots,b_n\in R$ まで定まったとき漸化式 $b_{n+1}=-\dfrac{1}{a_0}\sum_{k=0}^{n}a_kb_k$ によって $b_{n+1}\in R$ を定める．このようにして得られた無限数列 $\{b_n\}$ を利用して，$g(X)=\sum_{k=0}^{\infty}b_kX^k\in R[[X]]$ を定めると，$f(X)g(X)=1$ が成り立つ．よって，$f(X)$ は $R[[X]]$ の可逆元である． □

系 5.9. K は体，$S_n=K[[X_1,\ldots,X_n]]$ とする．$f(X_1,\ldots,X_n)\in S_n$ の定数項を $a\in K$ とする．$f(X_1,\ldots,X_n)$ が S_n の可逆元であるための必要十分条件は，$a\neq0$ である．

証明. $S_0=K$, $S_n=S_{n-1}[[X_n]]$ $(n\in\mathbb{N})$ とする．前定理を利用して，n に関する帰納法ですぐ証明できる． □

系 5.10. K が体ならば $K[[X]]$ は PID である．また，I が (0) でも $K[[X]]$ でもない $K[[X]]$ のイデアルならば，ある自然数 n により $I=(X^n)$ と書ける．

証明. I は (0) でも $K[[X]]$ でもない $K[[X]]$ のイデアルとする．$f(X)=\sum_{n=0}^{\infty}a_nX^n\in K[[X]]$, $f(X)\neq0$ に対し，$a_n\neq0$ となる最小の n の値を $\operatorname{ord}_X f(X)$ と表わし，$f(X)$ の**オーダー**という．ただし，$\operatorname{ord}_X 0=+\infty$ と約束しておく．I の元の中でオーダーが最小のものの 1 つを $f(X)$ とし，$\operatorname{ord}_X f(X)=n$ とおく．以下，$I=(X^n)$ であることをを証明する．

$f(X)=X^nf_1(X)$ $(f_1(X)\in K[[X]])$ と書け，$f_1(X)$ の定数項は 0 でないから，$f_1(X)f_2(X)=1$ を満たす $f_2(X)\in K[[X]]$ が存在する．すると，$X^n=f(X)f_2(X)\in I$ なので，$(X^n)\subset I$ である．

$I\subset(X^n)$ を示す．I の 0 以外の任意の元 $g(X)$ は $\operatorname{ord}_X g(X)\geqq n$ を満たすから，$g(X)=X^nh(X)$ $(h(X)\in K[[X]])$ と書ける．よって，$I\subset(X^n)$ である． □

6. 局所化と局所環

R が整域のとき分数体 $Q(R)$ の定義をきちんと書いてみよう．$\dfrac{a}{b}=\dfrac{c}{d}$ $(a,b,c,d\in R,\ b\neq0,\ d\neq0$ であることは $ad=bc$ によって定義されていた (書かなかったが高校まではそうであった)．さらに，$\dfrac{c}{d}=\dfrac{e}{f}$ $(e,f\in R,\ f\neq0)$ のとき，$\dfrac{a}{b}=\dfrac{e}{f}$ であることを証明しよう (高校までは，証明せずに自明の事実として使っていた)．

$\dfrac{c}{d}=\dfrac{e}{f}$ より $cf=de$ である．$ad=bc$ より $(af)d=(ad)f=(bc)f=(cf)b=(de)b=(be)d$ である．よって，$(af-be)d=0$ である．R は整域で $d\neq0$ だから $af-be=0$ で $af=be$ となる．よって，$\dfrac{a}{b}=\dfrac{e}{f}$ である．

R が整域でない可換環で，d が零因子だと，最後の段階で $af-be=0$ が導けない．そこで，以下のように，慎重な考察をしないといけない．

定義 6.1.(積閉集合 S と $S^{-1}R$) R は可換環とし，$S\subset R$ は部分集合とする．S が次の (1), (2) を満たすとき，S は**積閉集合**であるという．

(1) $x,y\in S$ ならば $xy\in S$.

(2) $1\in S$ かつ $0\notin S$.

ただし，条件 (2) が成立しなくても，命題 6.2 まで問題は生じない．

集合 $S\times R$ 上に関係 $\sim$ を，

$$「(s_1, r_1) \sim (s_2, r_2) \iff \text{ある } t \in S \text{ が存在して } (s_1r_2 - s_2r_2)t = 0」$$

によって定義する．ここで，$s_1, s_2 \in S$; $r_1, r_2 \in R$ である．この関係 $\sim$ が同値関係であることは，命題 6.2 で証明する．$S^{-1}R = (S \times R)/\sim$ とおく．(s, r) の関係 $\sim$ による同値類を $\dfrac{r}{s} \in S^{-1}R$ と書くことにする．しつこいようだが，$S^{-1}R$ における $\dfrac{r_1}{s_1} = \dfrac{r_2}{s_2}$ の定義は $(s_1r_2 - s_2r_1)t = 0$ $(\exists t \in S)$ であって，$s_1r_2 = s_2r_1$ ではない．だから，約分も勝手にできるわけではない．$S^{-1}R$ における和と積を次のように定める．

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_2r_1 + s_1r_2}{s_1s_2}, \quad \frac{r_1}{s_1}\frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}$$

この定義が well defined であることは次の命題で証明する．すると，$S^{-1}R$ は可換環になる．$S^{-1}R$ を S による R の**局所化** (localization) とか**商環**という．

命題 6.2. (1) 上の定義において $\sim$ は同値関係である．
(2) 上の定義の和と積は，矛盾なく定議されている．

証明. (1) 対称律「$(s_1, r_1) \sim (s_2, r_2) \Longrightarrow (s_2, r_2) \sim (s_1, r_1)$」と，反射律「$(s, r) \sim (s, r)$」を満たすことは自明である．推移律を示す．$(s_1, r_1) \sim (s_2, r_2)$, $(s_2, r_2) \sim (s_3, r_3)$ とする．ある $t_1, t_2 \in S$ により，$(s_1r_2 - s_2r_1)t_1 = 0$, $(s_2r_3 - s_3r_2)t_2 = 0$ となる．つまり，$s_1r_2t_1 = s_2r_1t_1$, $s_2r_3t_2 = s_3r_2t_2$ である．

$$(s_1r_3)(s_2t_1t_2) = (s_2r_3t_2)(s_1t_1) = (s_3r_2t_2)(s_1t_1) = (s_1r_2t_1)(s_3t_2) = (s_2r_1t_1)(s_3t_2) = (s_3r_1)(s_2t_1t_2)$$

であり，$(s_1r_3 - s_3r_1)(s_2t_1t_2) = 0$ を得る．$(s_2t_1t_2) \in S$ だから，$(s_1, r_1) \sim (s_3, r_3)$ である．よって，$\sim$ は同値関係である．

(2) $\dfrac{r_1}{s_1} = \dfrac{r_1'}{s_1'}$, $\dfrac{r_2}{s_2} = \dfrac{r_2'}{s_2'}$ のとき，$\dfrac{s_2r_1 + s_1r_2}{s_1s_2} = \dfrac{s_2'r_1' + s_1'r_2'}{s_1's_2'}$, $\dfrac{r_1r_2}{s_1s_2} = \dfrac{r_1'r_2'}{s_1's_2'}$ を示せばよい．和のほうを示す．ある $t_1, t_2 \in S$ により，$r_1s_1't_1 = r_1's_1t_1$, $r_2s_2't_2 = r_2's_2t_2$ となる．

$$\begin{aligned}(s_2r_1 + s_1r_2)(s_1's_2')(t_1t_2) &= (r_1s_1't_1)(s_2s_2't_2) + (r_2s_2't_2)(s_1s_1't_1)\\ &= (r_1's_1t_1)(s_2s_2't_2) + (r_2's_2t_2)(s_1s_1't_1)\\ &= (s_2'r_1' + s_1'r_2')(s_1s_2)(t_1t_2)\end{aligned}$$

なので，$\dfrac{s_2r_1 + s_1r_2}{s_1s_2} = \dfrac{s_2'r_1' + s_1'r_2'}{s_1's_2'}$ である．

積 $\dfrac{r_1r_2}{s_1s_2} = \dfrac{r_1'r_2'}{s_1's_2'}$ の証明は簡単なので，練習問題とする． □

ここまで，積閉集合の定義の条件 (2) はまったく使っていないことに注意する．

実は，$0 \in S$ ならば $S^{-1}R = 0$ となる．実際，任意の r/s と $0/s \in S^{-1}R$ に対し，$0 \in S$ をとれば $(rs - 0s)0 = 0$ だから，$r/s = 0/s = 0$ であり，$S^{-1}R = \{0\}$ である．それを気にしなければ $0 \in S$ でも構わない．

$1 \in S$ という条件は，実際は不要である．もし $1 \in S$ ならば，$\varphi\colon R \longrightarrow S^{-1}R$ を $\varphi(a) = \dfrac{a}{1} \in S^{-1}R$ によって定義することができる．φ は環の準同型写像であるが，R が整域の場合と異なり，一般の可換環では φ は単射とは限らない．

しかし，$1 \notin S$ でも，勝手な $s \in S$ を取り，$\varphi(a) = \dfrac{sa}{s} \in S^{-1}R$ によって $\varphi\colon R \longrightarrow S^{-1}R$ を定義すれば，前の φ と同じ写像になる．

要するに，$1 \in S$ という条件は，$\dfrac{a}{1}$ という簡明な分数が定義できるように付けただけの条件で，代わりに $\dfrac{as}{s}$ という分数で我慢すれば，特になくてもよい条件である．

定義 6.3. R は可換環，S は R の非零因子全体の集合とする．S は積閉集合なので $S^{-1}R$ が定義できる．この $S^{-1}R$ を $Q(R)$ と書き，R の**全商環**という．(R が整域の場合は，前に定義した分数体 $Q(R)$ と一致する.)

定義 6.4. R は可換環，$\mathfrak{p}$ は R の素イデアルとし，$S = R - \mathfrak{p}$ (差集合) とする．$x, y \in S$ ならば，$x, y \notin \mathfrak{p}$ であるが，$\mathfrak{p}$ は素イデアルなので $xy \notin \mathfrak{p}$ となり，$xy \in S$ となる．$0 \in \mathfrak{p}$ なので $0 \notin S$, $1 \notin \mathfrak{p}$ なので $1 \in S$ である．よって，S は積閉集合である．$S^{-1}R$ を $R_{\mathfrak{p}}$ と書き，$\mathfrak{p}$ による R の**局所化**という．

定義 6.5. R は可換環で体でも 0 でもないとする．R がちょうど 1 個だけ極大イデアルを持つとき，R は**局所環** (local ring) であるという．R の唯一の極大イデアルを $\mathfrak{m}$ とし，$k = R/\mathfrak{m}$ とする．このとき，$(R, \mathfrak{m})$ は局所環である，とか，$(R, \mathfrak{m}, k)$ は局所環である，という書き方をする．

定理 6.6. R は体でない可換環で，$\mathfrak{p}$ は R の素イデアルとする．このとき，$R_{\mathfrak{p}}$ は，

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

を唯一の極大イデアルとする局所環である．

証明. $\mathfrak{p}R_{\mathfrak{p}}$ が $R_{\mathfrak{p}}$ のイデアルであることの証明は簡単なので省略する (練習問題として解いてみよ)．$S = R - \mathfrak{p}$ とおく．

$r/s \in R_{\mathfrak{p}} - \mathfrak{p}R_{\mathfrak{p}}$ とする．定義から，$r, s \in S$ と仮定してよい．すると，$s/r \in R_{\mathfrak{p}}$ であり，$(r/s)(s/r) = 1$ となる．よって，r/s は $R_{\mathfrak{p}}$ の可逆元である．

さて，もし，$\mathfrak{p}R_{\mathfrak{p}} \subsetneqq I \subsetneqq R_{\mathfrak{p}}$ を満たす $R_{\mathfrak{p}}$ にイデアル I が存在すれば，上の考察から I は $R_{\mathfrak{p}}$ の可逆元を 1 個以上含む．すると，命題 1.8 より，$I = R_{\mathfrak{p}}$ となり矛盾する．よって，$\mathfrak{p}R_{\mathfrak{p}}$ は $R_{\mathfrak{p}}$ の極大イデアルである．

また，$\mathfrak{p}R_{\mathfrak{p}}$ 以外の極大イデアル $\mathfrak{m}$ が存在したと仮定すると，同様に，$\mathfrak{m}$ は $R_{\mathfrak{p}}$ の可逆元を 1 個以上含み，$\mathfrak{m} = R_{\mathfrak{p}}$ となり矛盾する． □

定理 6.7. A は体でない可換環で，$S \subset A$ は積閉集合，$B = S^{-1}A$ とおく．$\varphi\colon A \to B$ を $\varphi(a) = a/1$ で定める．φ は準同型写像で，以下の性質を満たす．

(1) I が A のイデアルならば，$IB = \left\{ a/s \in B \;\middle|\; a \in I,\, s \in S \right\}$ も B のイデアルである．このとき，$IB \neq B$ であるための必要十分条件は，$I \cap S = \emptyset$ である．
(2) I が A の素イデアルで $I \cap S = \emptyset$ ならば，IB も B の素イデアルである．さらに，$\varphi^{-1}(IB) = I$ が成り立ち，φ から誘導される準同型写像 $\overline{\varphi}: A/I \longrightarrow B/IB$ は単射である．
(3) B のイデアル J について，$I = \varphi^{-1}(J)$ とおくと，$J = IB$ である．
(4) J が B の素イデアルならば，$I = \varphi^{-1}(J)$ は A の素イデアルである．
(5) I, J が A の素イデアルで $J \subsetneqq I$, $I \cap S = \emptyset$ ならば，$JB \subsetneqq IB$ である．
(6) I, J が B のイデアルで $J \subsetneqq I$ ならば，$\varphi^{-1}(J) \subsetneqq \varphi^{-1}(I)$ である．

証明. (1) $a, b \in I$; $s, t \in S$ ならば，$at + bs \in I$, $st \in S$ なので，$a/s + b/t = (at + bs)/(st) \in IB$ である．また，$c \in A$ のとき，$cb \in I$ なので，$(c/s)(b/t) = (cb)/(st) \in IB$ である．よって，IB は B のイデアルである．

$J = IB$ とする．$\exists x \in I \cap S \neq \emptyset$ とすると，$1/x \in B$ より，$J = B$ となってしまう．したがって，$J \subsetneqq B$ となるためには，$I \cap S = \emptyset$ が必要である．

逆に，$I \cap S = \emptyset$ と仮定する．もし $IB = B$ ならば，ある $s \in S$ が存在して $1 = s/s \in IB$ である．よって，$IB \subsetneqq B$ である．

(2) I は A の素イデアルとする．$a, b \in A$; $s, t \in S$, $(a/s)(b/t) \in IB$ とする．ある $c \in I$; $u, v \in S$ が存在して $(a/s)(b/t) = c/u$, つまり，$(abu - cst)v = 0$ となる．$0 \in I$, $v \notin I$ だから $abu - cst \in I$ である．$cst \in I$ だから，$abu \in I$ である．$u \notin I$ だから $ab \in I$ である．よって，$a \in I$ または $b \in I$ となる，$a/s \in IB$ または $b/y \in IB$ である．よって，IB は B の素イデアルである．

$\varphi^{-1}(IB) = I$ を示す．勝手な $a \in \varphi^{-1}(IB)$ を取る．$\varphi(a) = r/s \in IB \cap \varphi(A)$ $(\exists r \in I, \exists s \in S)$ と書ける．ある $t \in S$ により $(as - r)t = 0$ となる．$0 \in I$, $t \notin I$ で I が素イデアルなので，$as - r \in I$ である．$r \in I$ なので $as \in I$ で，$s \notin I$ なので $a \in I$ である．よって，$\varphi^{-1}(IB) \subset I$ である．

$\varphi^{-1}(IB) \supset I$ の証明は簡単 (各自考えよ)．よって，$\varphi^{-1}(IB) = I$ である．

$\overline{\varphi}$ が単射であることを示す．$\psi\colon A \to B/J$ を自然な写像とするとき，$\operatorname{Ker}\psi = \varphi^{-1}(J) = I$ であるので，準同型定理より，$\overline{\varphi}\colon A/I \to B/J$ は単射である．

(3) $\varphi(I) \subset J$ だから，$IB = \varphi(I)B \subset JB = J$ である．逆に，$x \in J$ は $x = r/s$ $(r \in A, s \in S)$ と書け，ある $t \in S$ により，$rt/1 = rt = xst \in J$ となる．$\varphi(rt) = rt/1 \in J$ だから $rt \in \varphi^{-1}(J) = I$ である．すると，$x = r/s = rt/st \in IB$ となり，$J \subset IB$ である．よって $J = IB$ である．

(4) J が素イデアルのとき I が素イデアルであることを示す．$x, y \in A$, $xy \in I$ のとき，$\varphi(xy) \in J$ で，J は素イデアルだから $\varphi(x) \in J$ または $\varphi(y) \in J$ である．つまり，$x \in \varphi^{-1}(J)$ または $y \in \varphi^{-1}(J)$ であり，I は素イデアルである．

(5) $I \cap S = \emptyset$ であるような A の素イデアル I と，B の素イデアル J が，$J = IB$, $I = \varphi^{-1}(J)$ という対応によって 1 対 1 に対応することからわかる．

(6) は (3) からすぐわかる． □

定義 6.8. 環 R の素イデアル I に対し，

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \subsetneqq \cdots \subsetneqq \mathfrak{p}_{h-1} \subsetneqq \mathfrak{p}_h = I$$

を満たす素イデアル列の長さ h の最大値を $\operatorname{ht} I$ と書き，I の**高さ** (height) と言う．また，

$$\mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \mathfrak{p}_2 \supsetneqq \cdots \supsetneqq \mathfrak{p}_{c-1} \supsetneqq \mathfrak{p}_c = I$$

を満たす素イデアル列の長さ c の最大値を $\operatorname{coht} I$ と書き **coheight** と言う．

定理 6.9. R は体でない可換環で，$\mathfrak{p}$ は R の素イデアルとする．このとき，以下が成り立つ．
(1) $\operatorname{Krull\,dim} R \geqq \operatorname{ht}\mathfrak{p} + \operatorname{coht}\mathfrak{p}$.
(2) $\operatorname{ht}\mathfrak{p} = \operatorname{Krull\,dim} R_{\mathfrak{p}}$
(3) $\operatorname{coht}\mathfrak{p} = \operatorname{Krull\,dim} R/\mathfrak{p}$

証明. (1) 定義から明らか．

(2) $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_h = \mathfrak{p}$ は R の素イデアル列とする．$\mathfrak{q}_i = \mathfrak{p}_i R_{\mathfrak{p}}$ とおくと，前定理の (2), (6) より，$\mathfrak{q}_0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_h = \mathfrak{p}R_{\mathfrak{p}}$ で，これは $R_{\mathfrak{p}}$ の素イデアル列になる．
逆に，$\mathfrak{q}_0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_m = \mathfrak{p}R_{\mathfrak{p}}$ が $R_{\mathfrak{p}}$ の素イデアル列であるとする．$\mathfrak{p}_i = \varphi^{-1}(\mathfrak{q}_i)$ とおくと，前定理の (3), (7) より，$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_m = \mathfrak{p}$ は R の素イデアル列になる．これより，結論を得る．

(3) $\psi\colon R \to R/\mathfrak{p}$ を自然な全射とする．$\mathfrak{p} = \mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_h$ は R の素イデアル列とする．$\mathfrak{q}_i = \psi(\mathfrak{p}_i)$ とおくと，$\mathfrak{q}_0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_h = \mathfrak{p}R_{\mathfrak{p}}$ で，これは $R/\mathfrak{p}$ の素イデアル列になる．
逆に．$(0) = \mathfrak{q}_0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_m$ を $R/\mathfrak{p}$ の素イデアル列とする．$\mathfrak{p}_i = \varphi^{-1}(\mathfrak{q})_{\mathrm{i}}$ とおくと，
$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_m = \mathfrak{p}$ であり，これは R の素イデアル列である．$\mathfrak{p}_{m+i} = \psi^{-1}(\mathfrak{r}_i)$ とおくと，$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_m = \mathfrak{p}$ は R の素イデアル列になる．これより，結論を得る． □

定理 6.10. K は体とする．このとき，n 変数形式的巾級数環 $K[[X_1,\ldots, X_n]]$ は $\mathfrak{m} = (X_1, X_2,\ldots, X_n)$ を唯一の極大イデアルとする局所環である．

証明. $S = K[[X_1,\ldots, X_n]]$ とおく．$S/\mathfrak{m} \cong K$ なので，$\mathfrak{m}$ は極大イデアルである．
今，$\mathfrak{m}$ 以外の極大イデアル I が存在したと仮定して矛盾を導く．$f = f(X_1,\ldots, X_n) \in I$, $f \notin \mathfrak{m}$ を満たす f の定数項 a を考える．もし，$a = 0$ ならば $\mathfrak{m}$ の定義から $f \in \mathfrak{m}$ となるので，$a \neq 0$ である．$a \in K$ だから，a^{-1} が存在する．上の系から f は S の可逆元である．すると $I = S$ となり，I が極大イデアルであることに矛盾する． □

命題 6.11. R は可換環，$S \subset R$ は積閉集合とする．
(1) R が UFD ならば，$S^{-1}R$ も UFD である．
(2) R が PID ならば，$S^{-1}R$ も PID である．

証明. どちらも簡単なので，練習問題にする．

7. 完全系列

定義 7.1. R は環で，I は $\mathbb{Z}$ 内の連続する整数からなる部分集合とし，各 $i \in I$ に対し M_i は R-加群で，$i, i+1 \in I$ のときに $f_i\colon M_i \to M_{i+1}$ は R-準同型写像であるとする．このとき，

$$\cdots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \xrightarrow{f_{i+2}} \cdots \qquad (*)$$

などと書き，**系列** (sequence) という．さらに，各 $i, i+1, i+2 \in I$ に対し $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$ が成り立つとき，上の系列 $(*)$ は**完全系列** (exact sequence) であるという．

なお，$M_i = 0$ のとき，R-準同型写像 $f_i\colon 0 \to M_{i+1}$ はゼロ写像しか存在しないので，f_i を省略して単に $0 \to M_{i+1}$ と書く．同様に，準同型写像 $f_i\colon M_i \to 0$ もゼロ写像しか存在しないので，単に $M_i \to 0$ と書く．

完全系列の中で，

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

という形のものが基本になる．この形の完全系列を**短完全系列** (short exact sequence) という．

命題 7.2. R-加群 M, N に対し，以下が成り立つ．

(1) $0 \longrightarrow M \xrightarrow{f} N$ が完全 $\iff$ f は単射．

(2) $M \xrightarrow{f} N \longrightarrow 0$ が完全 $\iff$ f は全射．

(3) $0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$ が完全 $\iff$ f は同型写像．

証明. 簡単なので練習問題とする． □

定理 7.3. K は体，M は有限次元 K-ベクトル空間とする．完全系列

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

が存在するならば，$\dim_K M = \dim_K L + \dim_K N$ が成り立つ．

証明. L と $f(L)$ は同型で，$f(L)$ は有限次元ベクトル空間 M の部分空間だから，$f(L)$ も有限次元で，L も有限次元である．$\dim_K L = l$ とし，$x_1,\ldots, x_l$ を L の基底とする．$y_1 = f(x_1),\ldots, y_l = f(x_l)$ とおく．f は単射だから，$y_1,\ldots, y_l$ は 1 次独立である．$\dim_K M = m$ とし，$m - l$ 個の元 $y_{l+1},\ldots, y_m \in M$ をうまく選んで，$y_1,\ldots, y_l, y_{l+1},\ldots, y_m$ が M の基底になるようにできる．g は全射だから，$g(y_1),\ldots, g(y_m)$ は N の生成系になる．ところが，$1 \leqq i \leqq l$ のとき $g(y_i) = g(f(x_i)) = 0$ だから，$g(y_{l+1}),\ldots, g(y_m)$ が N の生成系になる．もし，これらの間に線形関係 $\sum_{j=l+1}^{m} a_j g(y_j) = 0$ $(a_i \in K)$ があれば，$\sum_{j=l+1}^{m} a_j y_j \in \operatorname{Ker} g = \operatorname{Im} f$ だから，$\sum_{j=l+1}^{m} a_j y_j = f\left(\sum_{i=1}^{l} a_i x_i\right)$ $(\exists a_i \in K)$ と書ける．しかし，$y_1,\ldots, y_m$ は 1 次独立だから，$a_1 = \cdots = a_m = 0$ でなければならない．したがって，$g(y_{l+1}),\ldots, g(y_m)$ は N の基底になり，$\dim_K N = m - l$ が得られる． □

系 7.4. K は体で，$M_1,\ldots, M_n$ は有限次元 K-ベクトル空間で，完全系列

$$0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-2}} M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} 0$$

が存在すると仮定する．このとき，$\sum_{i=1}^{n} (-1)^i \dim_K M_i = 0$ が成り立つ．

証明. $0 \to \operatorname{Ker} f_i \xrightarrow{\subset} M_i \xrightarrow{f_i} \operatorname{Im} f_i \to 0$ は完全系列だから，$\dim_K M_i = \dim_K \operatorname{Ker} f_i + \dim_K \operatorname{Im} f_i$ が成り立つ．$\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$ だから，

$$\sum_{i=1}^{n} (-1)^i \dim_K M_i = \dim_K \operatorname{Im} f_0 + (-1)^n \dim_K \operatorname{Im} f_n = 0$$

が成り立つ． □

定理 7.5. R-加群の完全系列

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

に対し，次の (1) 〜 (3) は同値である．

(1) ある R-準同型 $h\colon M \to L$ が存在し，$h \circ f = \mathrm{id}_L$ を満たす．

(2) ある R-準同型 $i\colon N \to M$ が存在し，$i \circ g = \mathrm{id}_N$ を満たす．

(3) N と同型な部分 R-加群 $N' \subset M$ が存在し，$M = f(L) \oplus N'$, $g(N') = N$ が成り立つ．このとき，$g|_{N'}\colon N' \to N$ は同型写像である．

上のいずれかの条件が成立するとき，完全系列 $0 \to L \to M \to N \to 0$ は**分解**するとか**分裂**するとか **split** するという．

証明. (1) $\Longrightarrow$ (3) は，$N' = \operatorname{Ker} h$ とすれば容易に証明できる．(3) $\Longrightarrow$ (1) は，正射影 $f(L) \oplus N' \twoheadrightarrow f(L)$ と $f^{-1}\colon f(L) \to L$ の合成を h とすればよい．(2) $\Longrightarrow$ (3) は，$N' = \operatorname{Im} j$ とすれば証明でき，(3) $\Longrightarrow$ (2) は，$g\colon N' \to N$ の逆写像から $j\colon N \to N' \xrightarrow{\subset} M$ を作ればよい． □

問 7.6. R は可換環，$f\colon L \to M$ が R-加群の準同型写像のとする．このとき，以下の完全系列が存在することを示せ．

$$0 \longrightarrow \operatorname{Ker} f \xrightarrow{\subset} L \xrightarrow{f} \operatorname{Im} f \longrightarrow 0$$
$$0 \longrightarrow \operatorname{Im} f \xrightarrow{\subset} M \longrightarrow \operatorname{Coker} f \longrightarrow 0$$
$$0 \longrightarrow \operatorname{Ker} f \xrightarrow{\subset} L \xrightarrow{f} M \longrightarrow \operatorname{Coker} f \longrightarrow 0$$

定義 7.7. R が環，M, N が R-加群のとき，M から N への R-準同型写像全体の集合を

$$\operatorname{Hom}_R(M, N) = \{ f\colon M \to N \mid f \text{ は } R\text{-準同型写像} \}$$

と書く．$f, g \in \operatorname{Hom}_R(M, N)$ に対し，写像 $f+g : M \to N$ を，$(f+g)(x) = f(x) + g(x)$ $(x \in M)$ と定めると $f+g$ も R-準同型写像になり，$f+g \in \operatorname{Hom}_R(M, N)$ となる．また，定数 $a \in R$ に対し，写像 $af : M \to N$ を，$(af)(x) = a(f(x))$ $(x \in M)$ と定めると，af も R-準同型写像になり，$af \in \operatorname{Hom}_R(M, N)$ となる．このように，$\operatorname{Hom}_R(M, N)$ に和と R の作用 (スカラー倍) を定めると，$\operatorname{Hom}_R(M, N)$ も R-加群になる．

$\varphi\colon L \to M$ が R-準同型写像のとき，$h \in \operatorname{Hom}_R(M, N)$ に対し，$h \circ \varphi \in \operatorname{Hom}_R(L, N)$ を対応させる写像を，

$$\varphi^*\colon \operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_R(L, N)$$

と書くことにする．また，$g \in \operatorname{Hom}_R(N, L)$ に対し，$\varphi \circ g \in \operatorname{Hom}_R(N, M)$ を対応させる写像を，

$$\varphi_*\colon \operatorname{Hom}_R(N, L) \longrightarrow \operatorname{Hom}_R(N, M)$$

と書く．

問 7.8. R は環，L, M, N, A は R-加群で，$f\colon L \to M$, $g\colon M \to N$ は R-線形写像とする．このとき，次が成り立つことを示せ．

$$(g \circ f)^* = f^* \circ g^* : \operatorname{Hom}_R(N, A) \longrightarrow \operatorname{Hom}(L, A)$$
$$(g \circ f)_* = g_* \circ f_* : \operatorname{Hom}_R(A, L) \longrightarrow \operatorname{Hom}(A, N)$$

定理 7.9. R は環で，L, M, N, A は R-加群とする．

(1) $L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ が完全系列ならば，

$$0 \longrightarrow \operatorname{Hom}_R(N, A) \xrightarrow{g^*} \operatorname{Hom}_R(M, A) \xrightarrow{f^*} \operatorname{Hom}_R(L, A)$$

は完全系列である．

(2) $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N$ が完全系列ならば，

$$0 \longrightarrow \operatorname{Hom}_R(A, L) \xrightarrow{f_*} \operatorname{Hom}_R(A, M) \xrightarrow{g_*} \operatorname{Hom}_R(A, N)$$

は完全系列である．

証明. (1) g^* が単射であることを示す．$h \in \operatorname{Hom}_R(N, A)$ に対し，$g^*(h) = h \circ g = 0$ であると仮定する．$z \in N$ を勝手な元とするとき，$g(y) = z$ を満たす $y \in M$ が存在する．$h(y) = (h \circ g)(z) = 0$ だから，h は 0 写像である．したがって，$\operatorname{Ker} g^* = 0$ で，g^* は単射である．

$\operatorname{Im} g^* = \operatorname{Ker} f^*$ を示す．$f^* \circ g^* = (g \circ f)^* = 0^* = 0$ より，$\operatorname{Im} g^* \subset \operatorname{Ker} f^*$ である．逆に，$h \in \operatorname{Ker} f^*$ をとる．任意の $x \in L$ に対し，$h(f(x)) = 0$ である．$\operatorname{Im} f = \operatorname{Ker} g$ だから，$h(\operatorname{Ker} g) = 0$ である．したがって，$h\colon M \to A$ から，$\overline{h}\colon M/\operatorname{Ker} g \longrightarrow A$ が誘導されるが，$M/\operatorname{Ker} g \cong N$ なので，$\overline{h} \in \operatorname{Hom}_R(N, A)$ とみなせる．このとき，$h = \overline{h} \circ g$ が成り立つので，$\operatorname{Im} g^* = \operatorname{Ker} f^*$ である．

(2) f_* が単射であることを示す．$h \in \mathrm{Hom}_R(A, L)$ に対し，$f_*(h) = f \circ h = 0$ ならば，任意の $x \in A$ に対し，$f(h(x)) = 0$ であるが，f は単射なので，$h(x) = 0$ で $h = 0$ となる．

$\mathrm{Im}\, f_* = \mathrm{Ker}\, g_*$ を示す．$g_* \circ f_* = (g \circ f)_* = 0$ より，$\mathrm{Im}\, f_* \subset \mathrm{Ker}\, g_*$ である．逆に，勝手な $h \in \mathrm{Ker}\, g_*$ をとる．任意の $a \in A$ に対し，$g(h(a)) = 0$ で，$h(a) \in \mathrm{Ker}\, g$ である．$\mathrm{Im}\, f = \mathrm{Ker}\, g$ より，ある $x \in L$ により，$h(a) = f(x)$ と書ける．f は単射なので，この x は a から一意的に定まる．そこで，$h'(a) = x$ によって，$h' \in \mathrm{Hom}_R(A, L)$ を定めることができ，$h = f_*(h')$ となる． □

注意 7.10. $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ が完全系列であっても，

$$0 \longrightarrow \mathrm{Hom}_R(N, A) \xrightarrow{g^*} \mathrm{Hom}_R(M, A) \xrightarrow{f^*} \mathrm{Hom}_R(L, A) \longrightarrow 0 \qquad ①$$

$$0 \longrightarrow \mathrm{Hom}_R(A, L) \xrightarrow{f_*} \mathrm{Hom}_R(A, M) \xrightarrow{g_*} \mathrm{Hom}_R(A, N) \longrightarrow 0 \qquad ②$$

はいずれも完全系列であるとは**限らない**．例えば，$R = \mathbb{Z}$ とし，$\mathbb{Z}$-加群の完全系列

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \quad (\text{ただし，} f(x) = 2x)$$

に対し，$A = \mathbb{Z}/2\mathbb{Z}$ とすると，① の f^* は全射でないし，② の g_* は全射でない．

命題 7.11. R は環，M は R-加群とする．このとき，次が成り立つ．

$$\mathrm{Hom}_R(R, M) \cong M$$

証明. $f \in \mathrm{Hom}_R(R, M)$ に対し $f(1) \in M$ を対応させ，逆に $x \in M$ に対し $f(a) = ax$ で定まる $f \in \mathrm{Hom}_R(R, M)$ を対応させればよい． □

定理 7.12.(蛇の補題, snake lemma) L_1, M_1, N_1, L_2, M_2, N_2 は R-加群で，以下の図式は可換 (つまり，$g \circ \varphi_1 = \varphi_2 \circ f$, $h \circ \psi_1 = \psi_2 \circ g$) であり，横の 2 つの列 $L_1 \to M_1 \to N_1 \to 0$ と $0 \to L_2 \to M_2 \to N_2$ は完全系列であるとする．

$$\begin{array}{ccccccccc} & & L_1 & \xrightarrow{\varphi_1} & M_1 & \xrightarrow{\psi_1} & N_1 & \longrightarrow & 0 \\ & & {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L_2 & \xrightarrow{\varphi_2} & M_2 & \xrightarrow{\psi_2} & N_2 & & \end{array}$$

このとき，以下の完全系列が存在する．

$$\mathrm{Ker}\, f \xrightarrow{\varphi_0} \mathrm{Ker}\, g \xrightarrow{\psi_0} \mathrm{Ker}\, h \xrightarrow{\delta} \mathrm{Coker}\, f \xrightarrow{\varphi_3} \mathrm{Coker}\, g \xrightarrow{\psi_3} \mathrm{Coker}\, h$$

ここで，φ_0, ψ_0 は φ_1, ψ_1 の定義域と終域を制限して得られる写像であり，φ_3 と ψ_3 はそれぞれ φ_2, ψ_2 から自然に誘導される写像である．δ を**連結写像**という．

さらに，もし φ_1 が単射であれば φ_0 も単射であり，もし ψ_2 が全射であれば ψ_3 も全射である．

証明. (1) $\varphi_1(\mathrm{Ker}\, f) \subset \mathrm{Ker}\, g$ だから，$\varphi_0 = \varphi_1|_{\mathrm{Ker}\, f} : \mathrm{Ker}\, f \longrightarrow \mathrm{Ker}\, g$ は矛盾なく定義できる．$\psi_0 = \psi_1|_{\mathrm{Ker}\, g} : \mathrm{Ker}\, g \longrightarrow \mathrm{Ker}\, h$ も同様である．

$\mathrm{Im}\, \varphi_0 = \varphi_1(\mathrm{Ker}\, f) = \mathrm{Im}\, \varphi_1 \cap \mathrm{Ker}\, g = \mathrm{Ker}\, \psi_1 \cap \mathrm{Ker}\, g = \mathrm{Ker}\, \psi_0$ なので，$\mathrm{Ker}\, f \xrightarrow{\varphi_0} \mathrm{Ker}\, g \xrightarrow{\psi_0} \mathrm{Ker}\, h$ は完全である．また，φ_0 の定義から，φ_1 が単射ならば φ_0 も単射である．

(2) $\pi_L : L_2 \twoheadrightarrow \mathrm{Coker}\, f$, $\pi_M : M_2 \twoheadrightarrow \mathrm{Coker}\, g$, $\pi_N : N_2 \twoheadrightarrow \mathrm{Coker}\, h$ を自然な全射とする．φ_3, ψ_3 の定義から，$\pi_M \circ \varphi_2 = \varphi_3 \circ \pi_L$, $\pi_N \circ \psi_2 = \psi_3 \circ \pi_M$ である．

$\mathrm{Im}\, \varphi_3 = \varphi_3(\pi_L(L_2)) = \pi_M(\varphi_2(L_2)) = \pi_M(\mathrm{Im}\, \varphi_2) = \mathrm{Im}\, \varphi_2 / \mathrm{Im}\, g = \mathrm{Ker}\, \psi_2 / \mathrm{Im}\, g = \mathrm{Ker}\, \psi_3$ なので，$\mathrm{Coker}\, f \xrightarrow{\varphi_3} \mathrm{Coker}\, g \xrightarrow{\psi_3} \mathrm{Coker}\, h$ は完全である．また，ψ_2 が全射ならば，それから誘導される ψ_3 も全射である．

(3) 連結写像 (connecting mophism) とよばれる写像 $\delta : \mathrm{Ker}\, h \longrightarrow \mathrm{Coker}\, f$ を構成する．

勝手な元 $z \in \mathrm{Ker}\, h \subset N_1$ をとる．このとき，$\psi_1(y) = z$ を満たす $y \in M_1$ が存在する．$\psi_2(g(y)) = h(\psi_1(y)) = h(z) = 0$ だから，$g(y) \in \mathrm{Ker}\, \psi_2 = \mathrm{Im}\, \varphi_2$ である．そこで，この y に対し $\varphi_2(x) = g(y)$ を満たす $x \in L_2$ が一意的に存在する．

$\pi_L(x)$ が y の選び方に依存しないことを示す．$\psi_1(y')=z$ を満たす他の $y'\in M_1$ と，$\varphi_2(x')=y'$ を満たす $x'\in L_2$ をとる．このとき，$y-y'\in\operatorname{Ker}\psi_1=\operatorname{Im}\varphi_1$ なので，$y-y'=\varphi_1(x_1)$ を満たす $x_1\in L_1$ が存在する．すると，φ_2 の単射性から $x-x'=f(x_1)$ となる．したがって，$\pi_L(x)=\pi_L(x'+f(x_1))=\pi_L(x)+\pi_L(f(x_1))=\pi_L(x')$ となる．

そこで，$\delta(z)=\pi_L(x)$ と定義することができる．

(4) 上の記号において，もし，ある $y_0\in\operatorname{Ker}g$ が存在して $z=\psi_0(y_0)$ と書けているとすると，$y=y_0$ と選ぶことができるので，$\varphi_2(x)=g(y)=0$ であり，$x=0$ となる．よって，$\delta(z)=\pi_L(x)=0$ である．したがって，$\operatorname{Im}\psi_0\subset\operatorname{Ker}\delta$ である．

逆に，$z\in\operatorname{Ker}\delta$ とすると，$\pi_L(x)=0$ だから，$f(x_1)=x$ を満たす $x_1\in L_1$ が存在する．$g(y-\varphi_1(x_1))=\varphi_2(x-x)=0$ だから，$y-\varphi_1(x_1)\in\operatorname{Ker}g$ であり，$z=\psi_1(y)=\psi_1(y-\varphi_1(x_1))=\psi_0(y-\varphi_1(x_1))$ なので，$z\in\operatorname{Im}\psi_0$ となる．したがって，$\operatorname{Ker}\delta\subset\operatorname{Im}\psi_0$ で，$\operatorname{Ker}g\xrightarrow{\psi_0}\operatorname{Ker}h\xrightarrow{\delta}\operatorname{Coker}f$ は完全である．

(5) 記号は (3) と同じとする．

$$\varphi_3(\delta(z))=\varphi_3(\pi_L(x))=\pi_M(\varphi_2(x))=\pi_M(g(y))=0$$

より，$\operatorname{Im}\delta\subset\operatorname{Ker}\varphi_3$ である．

逆に，$\pi_L(x)\in\operatorname{Coker}f$ が $\varphi_3(\pi_L(x))=0$ を満たしたとする．すると，$\varphi_2(x)\in\operatorname{Ker}\pi_M=\operatorname{Im}g$ だから，$g(y)=\varphi_2(x)$ を満たす $y\in M_1$ が存在する．$h(\psi_1(y))=\psi_2(g(y))=0$ だから，$\psi_1(y)\in\operatorname{Ker}h$ である．このとき，$\delta(\psi_1(y))=\pi_L(x)$ となるので，$\operatorname{Ker}\varphi_3\subset\operatorname{Im}\delta$ である．したがって，$\operatorname{Ker}h\xrightarrow{\delta}\operatorname{Coker}f\xrightarrow{\varphi_3}\operatorname{Coker}g$ は完全である． □

定理 7.13.(ファイブ・レンマ, 5-lemma) 下の図式は R-加群の可換図式で，横の 2 行はいずれも完全系列であるとする．

$$\begin{array}{ccccccccc} L_1 & \xrightarrow{f_1} & L_2 & \xrightarrow{f_2} & L_3 & \xrightarrow{f_3} & L_4 & \xrightarrow{f_4} & L_5 \\ {\scriptstyle h_1}\downarrow & & {\scriptstyle h_2}\downarrow & & \downarrow{\scriptstyle h_3} & & \downarrow{\scriptstyle h_4} & & \downarrow{\scriptstyle h_5} \\ M_1 & \xrightarrow{g_1} & M_2 & \xrightarrow{g_2} & M_3 & \xrightarrow{g_3} & M_4 & \xrightarrow{g_4} & M_5 \end{array}$$

このとき，以下が成立する．
(1) h_1 が全射，h_2 と h_4 が単射ならば，h_3 も単射である．
(2) h_5 が単射，h_2 と h_4 が全射ならば，h_3 も全射である．

証明. (1) $K_i=\operatorname{Ker}h_i$ とおく．$i\leqq 4$ に対し，$h_{i+1}(f_i(K_i))=f_{i+1}(h_i(K_i))=f_{i+1}(0)=0$ だから，$f_i(K_i)\subset K_{i+1}$ であり，$f_i'=f_i|_{K_i}:K_i\to K_{i+1}$ が定義できる．$2\leqq i\leqq 4$ に対し $f_i\circ f_{i-1}=0$ だから，$f_i'\circ f_{i-1}'=0$ で，$\operatorname{Im}f_{i-1}'\subset\operatorname{Ker}f_i'$ である．

$\operatorname{Ker}f_3'=0$ を示す．$x_3\in\operatorname{Ker}f_3'\subset\operatorname{Ker}f_3=\operatorname{Im}f_2\subset L_3$ をとる．ある $x_2\in L_2$ により，$x_3=f_2(x_2)$ と書ける．$g_2(h_2(x_2))=h_3(f_2(x_2))=h_3(x_3)=0$ だから，ある $y_1\in M_1$ により，$h_2(x_2)=g_1(y_1)$ と書ける．h_1 は全射だから，ある $x_1\in L_1$ により，$y_1=h_1(x_1)$ とかける．すると，

$$h_2(f_1(x_1))=g_1(h_1(x_1))=g_1(y_1)=h_2(x_2)$$

であるが，h_2 は単射なので，$x_2=f_1(x_1)$ であり，$x_3=f_2(f_1(x_1))=0$ となる．すると，$f_3'\colon K_3\xrightarrow{\subset}K_4=0$ だから，$K_3=0$ で f_3 は単射である．

(2) 上と同じ要領で証明できる． □

8. テンソル積

定義 8.1.(無限個の加群の直積と直和) R は可換環，Λ は集合とし，各 $\lambda\in\Lambda$ に対し R-加群 M_λ が与えられているとする．直積集合 $M=\prod_{\lambda\in\Lambda}M_\lambda$ を考える．M の元を $(x_\lambda)_{\lambda\in\Lambda}$ とか，略して $(x_\lambda)\in M$ と書くことにする．ここで，$(x_\lambda)_{\lambda\in\Lambda}$ は各 $\lambda\in\Lambda$ に対し，M_λ の元 $x_\lambda\in M_\lambda$ を 1 個ずつ選んだものを表す．$(x_\lambda)_{\lambda\in\Lambda}\in M$, $(y_\lambda)_{\lambda\in\Lambda}\in M$, と $a\in R$ に対し，和と R の作用を，

$$(x_\lambda)_{\lambda\in\Lambda}+(y_\lambda)_{\lambda\in\Lambda}=(x_\lambda+y_\lambda)_{\lambda\in\Lambda}\in M,\quad a(x_\lambda)_{\lambda\in\Lambda}=(ax_\lambda)_{\lambda\in\Lambda}\in M$$

によって定義すれば，M は R-加群になる．この $M = \prod_{\lambda\in\Lambda} M_\lambda$ を M_λ $(\lambda \in \Lambda)$ の**直積** (direct product) と言う．また，

$$\bigoplus_{\lambda\in\Lambda} M_\lambda = \left\{ (x_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda \;\middle|\; x_\lambda \neq 0 \text{ となる } \lambda \in \Lambda \text{ は有限個しか存在しない} \right\}$$

とおくと，$N := \bigoplus_{\lambda\in\Lambda} M_\lambda$ は M の R-部分加群になる．N を M_λ $(\lambda \in \Lambda)$ の**直和** (direct sum) と言う．

L を R-加群とし，任意の $\lambda \in \Lambda$ に対し $M_\lambda = L$ である場合，直積 $M = \prod_{\lambda\in\Lambda} M_\lambda$ を L^Λ とも書き，直和 $N = \bigoplus_{\lambda\in\Lambda} M_\lambda$ を $L^{\oplus\Lambda}$ とも書く．

一般に，R-加群 L に対し，ある部分集合 $X \subset L$ が存在し，$\varphi : R^{\oplus X} \longrightarrow L$ を，$(a_x)_{x\in X} \in R^{\oplus X}$ に対し $\varphi((a_x)_{x\in X}) = \sum_{x\in X} a_x x \in L$ で定める．φ が単射ならば X は R 上 **1 次独立**とか**線形独立**であるといい，φ が全射ならば X は L の**生成系**であるという．φ が同型写像ならば，X は L の R 上の**基底** (base) であるといい，L は R-**自由加群** (free module) であるといい，

問 8.2. X が有限集合の場合，上の，1 次独立，生成系，基底の定義は，ベクトル空間の場合の定義と一致することを確かめよ．

定理 8.3. K が体のとき，任意の K-加群 (K-ベクトル空間) $M \neq 0$ は，K-自由加群である．

証明. $\mathcal{A} = \{ X \subset M \mid X \text{ は } R \text{ 上線形独立} \}$ とおく．$0 \in x \in M$ を取るとき，$\{x\} \in \mathcal{A}$ だから，$\mathcal{A} \neq \emptyset$ である．$\mathcal{A}$ は集合の包含関係を順序として帰納的順序集合である．実際 $\mathcal{L}$ が $\mathcal{A}$ の全順序部分集合ならば，$\sup \mathcal{L} = \bigcup_{X\in\mathcal{L}} X$ である．

Zorn の補題により $\mathcal{A}$ の極大元 X が存在する．X は線形独立である．もし，X が M の生成系でなければ，X を含む M の最小の K-部分加群を N とするとき，$N \subsetneqq M$ である．そこで，$y \in M - N$ を取り，$Y = X \cup \{y\} \supsetneqq X$ とすると，K が体であることから $Y \in \mathcal{A}$ が簡単に証明できて，X の極大性に矛盾する．よって，X は M の基底で，M は K-自由加群である． □

定義 8.4. R は可換環，L, M は R-加群とする．以下，$L \otimes_R M$ を構成していく．
直積集合 $L \times M$ を基底とする自由 R-加群

$$U = R^{\oplus L\times M} = \bigoplus_{(x,y)\in L\times M} R \cdot (x, y)$$

を考える．以下の U の部分集合 X, Y を考える．

$$X = \{ (ax_1 + bx_2, y) - a(x_1, y) - b(x_2, y) \mid x_1, x_2 \in L;\ y \in M;\ a, b \in R \}$$
$$Y = \{ (x, ay_1 + by_2) - a(x, y_1) - b(x, y_2) \mid x \in L;\ y_1, y_2 \in M;\ a, b \in R \}$$

$X \cup Y$ を含む最小の U の R-部分加群を V とし，

$$L \otimes_R M = U/V$$

と定義し，これを L と M の R 上の**テンソル積** (tensor product) という．また，$(x, y) \in U$ の $U/V = L \otimes_R M$ における同値類を $x \otimes y$ と書く．
上の定義から，

$$L \otimes_R M = \left\{ \sum_{i=1}^{n} x_i \otimes y_i \;\middle|\; n \in \mathbb{N},\ x_i \in L,\ y_i \in M \right\}$$

であり，V が X, Y を含むので，以下の関係式が成り立つ．

$$(ax_1 + bx_2) \otimes y = a(x_1 \otimes y) + b(x_2 \otimes y)$$
$$x \otimes (ay_1 + by_2) = a(x \otimes y_1) + b(x \otimes y_2)$$
$$(\text{ただし，}\ a, b \in R;\ x, x_1, x_2 \in L;\ y, y_1, y_2 \in M)$$

定義 8.5. R を環，L, M, N を R-加群とする．写像 $f\colon L\times M\longrightarrow N$ が，
(1) 任意の $x_1, x_2\in L$; $a_1, a_2\in R$; $y\in M$ に対し，

$$f(a_1x_1+a_2x_2,\, y)=a_1f(x_1,\, y)+a_2f(x_2,\, y)$$

(2) 任意の $x\in L$; $y_1, y_2\in M$; $b_1, b_2\in R$ に対し，

$$f(x,\, b_1y_1+b_2y_2)=b_1f(x,\, y_1)+b_2f(x,\, y_2)$$

を満たすとき，f は**双線形写像** (bilinear map) であるという．

定理 8.6.(普遍性による特徴づけ) R を環，L, M, N を R-加群，$f\colon L\times M\longrightarrow N$ は双線形写像とする．また，$\varphi\colon L\times M\longrightarrow L\otimes_R M$ は，$\varphi(x,\, y)=x\otimes y$ $(x\in L,\, y\in M)$ で定まる写像とする．このとき，R-準同型写像 $g\colon L\otimes_R M\longrightarrow N$ で，$f=g\circ\varphi$ を満たすものが存在する．

$$\begin{array}{ccc} L\times M & \xrightarrow{\ f\ } & N \\ {\scriptstyle\iota}\downarrow & \overset{\Phi}{\nearrow} & \uparrow{\scriptstyle g} \\ U & \xrightarrow[\ \pi\ ]{} & U/V=L\otimes_R M \end{array}$$

証明. 定義 8.3 の記号を用いる．$(x,\, y)\in L\times N$ $(x\in L,\, y\in M)$ に対し，$(x,\, y)\in U$ を対応させる自然な単射を $\iota\colon L\times M\hookrightarrow U$ とする．また，$(x,\, y)\in U$ $(x\in L,\, y\in M)$ に対し，$\Phi(x,\, y)=f(x,\, y)$ と定め，これを線形に拡張することによって，$\Phi\colon U\longrightarrow N$ を定義する．このとき，$f=\Phi\circ\iota$ が成り立つ．

$\pi\colon U\twoheadrightarrow U/V=L\otimes_R M$ を自然な全射とする．f は双線形写像だから，$f(X)=0$ を満たす．同様に $f(Y)=0$ で，V は $X\cup Y$ で生成されるから，$f(V)=0$ である．したがって $V\subset\operatorname{Ker}\Phi$ で，これより，ある R-準同型写像 $g\colon L\otimes_R M\longrightarrow N$ で，$\Phi=g\circ\pi$ を満たすものが存在する．このとき，$f=\Phi\circ\iota=g\circ\pi\circ\iota=g\circ\varphi$ である． □

上の定理は，任意の $x\in L$ と $y\in M$ に対し，$g(x\otimes y)\in N$ を双線形性の条件を満たすように定めれば，

$$g\left(\sum_{i=1}^{n}a_i(x_i\otimes y_i)\right)=\sum_{i=1}^{n}a_ig(x_i\otimes y_i)$$

を満たすような R-準同型写像 $g\colon(L\otimes_R M)\longrightarrow N$ が，矛盾なく (一意的に) 定まることを保証してくれる．

定理 8.7. R は環，L, M, L', M' は R-加群，$f\colon L\to L'$, $g\colon M\to M'$ は R-準同型写像とする．このとき，f と g の**テンソル積**

$$f\otimes g\colon(L\otimes_R M)\longrightarrow(L'\otimes_R M')$$

を $\sum_{i=1}^{n}x_i\otimes y_i$ $(x_i\in L,\, y_i\in M)$ に対し，

$$(f\otimes g)\left(\sum_{i=1}^{n}x_i\otimes y_i\right)=\sum_{i=1}^{n}f(x_i)\otimes g(y_i)$$

が成立するように矛盾なく定めることができる．

証明. L, M, U, V, X, Y の記号は今までと同様とする．また，L', M' から同様の方法で，U', V', X', Y' を定める．U の生成元 $(x,\, y)$ $(x\in L,\, y\in M)$ に対し，$\Phi(x,\, y)=\big(f(x),\, g(y)\big)$ とし，これを線形に拡張して，$\Phi\colon U\to U'$ を定める．Φ と自然な全射 $U'\twoheadrightarrow U'/V'=L'\otimes_R M'$ を合成して，$\varphi\colon U\longrightarrow L'\otimes_R M'$ を作る．

$\Phi(X)\subset X'$, $\Phi(Y)\subset Y'$ は容易にわかるから，$\Phi(V)\subset V'$ で，$V\subset\operatorname{Ker}\varphi$ となる．これより，φ から命題のような f が定義できる． □

定理 8.8. R は環，L, M, N は R-加群とすると，次が成り立つ．
(1) $R\otimes_R M\cong M\otimes_R R\cong R$
(2) $L\otimes_R M\cong M\otimes_R L$

(3) $(L \otimes_R M) \otimes_R N \cong L \otimes_R (M \otimes_R N)$

証明. (1) $R \otimes_R M$ の元は，$\sum_{i=1}^{r} a_i(b_i \otimes x_i)$ $(a_i, b_i \in R, x_i \in M)$ と書ける．$x = \sum_{i=1}^{r} a_i b_i x_i \in M$ とおけば，

$$\sum_{i=1}^{r} a_i(b_i \otimes x_i) = 1 \otimes \left(\sum_{i=1}^{r} a_i b_i \otimes x_i \right) = 1 \otimes x$$

である．よって，$R \otimes_R M$ の元は，$1 \otimes x$ $(x \in M)$ という形に書ける．

$\varphi\colon R \times M \longrightarrow R \otimes_R M$ を $\varphi(a, x) = a \otimes x$ で定まる写像とし，$f\colon R \times M \longrightarrow M$ は $f(a, x) = ax$ で定まる双線形写像とする．定理 11.4 より，R-準同型写像 $g\colon R \otimes_M R \longrightarrow M$ で，$f = g \circ \varphi$ を満たすものが存在する．構成法から，$g(1 \otimes x) = x$ である．

$h\colon M \longrightarrow (R \otimes_R M)$ を $h(x) = 1 \otimes x$ で定めれば，これらは R-準同型写像で，$h \circ g = \mathrm{id}$, $g \circ h = \mathrm{id}$ である．よって，g, h は同型写像で $R \otimes_R M \cong M$ である．

$M \otimes_R R \cong R$ も同様.

(2) $f(\sum x_i \otimes y_i) = \sum y_i \otimes x_i$ で定まる $f\colon L \otimes_R M \longrightarrow M \otimes_R L$ は同型写像である．

(3) $(L \otimes_R M) \otimes_R N$ は $(x \otimes y) \otimes z$, $L \otimes (M \otimes_R N)$ は $x \otimes (y \otimes z)$ $(x \in L, y \in M, z \in N)$ という形の元で生成され，

$$f((x \otimes y) \otimes z) = x \otimes (y \otimes z)$$

を線形に拡張して得られる写像 $f\colon (L \otimes_R M) \otimes_R N \longrightarrow L \otimes (M \otimes_R N)$ は同型写像である． □

定理 8.9. R は環，M_λ $(\lambda \in \Lambda)$, N は R-加群とする．このとき次が成り立つ．

$$\left(\bigoplus_{\lambda \in \Lambda} M_\lambda \right) \otimes_R N \cong \bigoplus_{\lambda \in \Lambda} (M_\lambda \otimes_R N)$$

証明. $M = \bigoplus_{\lambda \in \Lambda} M_\lambda$ とし，$\iota_\lambda\colon M_\lambda \hookrightarrow M$ を埋入写像，$\pi_\lambda\colon M \twoheadrightarrow M_\lambda$ を正射影とする．

$$(\pi_\lambda \otimes \mathrm{id}_N) \circ (\iota_\lambda \otimes \mathrm{id}_N)\colon (M_\lambda \otimes_R N) \longrightarrow (M \otimes_R N) \longrightarrow (M_\lambda \otimes_R N)$$

は恒等写像であるから，$\iota_\lambda \otimes \mathrm{id}_N$ は単射，$\pi_\lambda \otimes \mathrm{id}_N$ は全射である．これらの写像から，

$$\iota\colon \bigoplus_{\lambda \in \Lambda} (M_\lambda \otimes_R N) \longrightarrow M \otimes_R N, \quad \pi\colon M \otimes_R N \longrightarrow \bigoplus_{\lambda \in \Lambda} (M_\lambda \otimes_R N)$$

を自然に定めると，$\pi \circ \iota$, $\iota \circ \pi$ は恒等写像になるので，これらは同型写像になる． □

系 8.10. K は体，$L = K^m$, $M = K^n$ のとき，$L \times_K M \cong K^{mn}$ である．

定理 8.11. (右半完全性) R は環，$L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ は R-加群の完全系列，A は R-加群とすると，

$$(L \otimes_R A) \xrightarrow{f'} (M \otimes_R A) \xrightarrow{g'} (N \otimes_R A) \longrightarrow 0$$

(ただし，$f' = f \otimes \mathrm{id}_A$, $g' = g \otimes \mathrm{id}_A$) は完全系列である．($f$ が単射でも f' は単射とは限らない．)

証明. (1) g' が全射であることを示す．$N \otimes_R A$ の元は，$z' = \sum_i z_i \otimes a_i$ $(z_i \in N, a_i \in A)$ という形をしている．g は全射だから，$g(y_i) = z_i$ を満たす $y_i \in M$ が存在する．このとき，$g'\left(\sum_i y_i \otimes a_i \right) = z'$ となる．

(2) $\mathrm{Im}\, f' = \mathrm{Ker}\, g'$ を示す．$g \circ f = 0$ より $g' \circ f' = (g \circ f) \otimes \mathrm{id}_A = 0$ であり，$\mathrm{Im}\, f' \subset \mathrm{Ker}\, g'$ である．

$Q = (M \otimes_R A)/\mathrm{Im}\, f'$ とし，$\pi\colon M \otimes_R A \twoheadrightarrow Q$ を自然な全射とする．$N \otimes_R A$ は $z \otimes a$ $(z \in N, a \in A)$ という形の元で生成される．この z, a をしばらく固定する．

$g(y) = z$ となる $y \in M$ をとる．$g(y) = g(y') = z$ のとき，$y - y' \in \mathrm{Ker}\, g = \mathrm{Im}\, f$ なので，$y - y' = f(x)$ を満たす $x \in L$ が存在する．このとき，$f'(x \otimes a) = y \otimes a - y' \otimes a$ だから，$\pi(y \otimes a) = \pi(y' \otimes a)$ とな

る．そこで，$h\colon N\otimes_R A\longrightarrow Q$ を，$h(z\otimes a)=\pi(y\otimes a)$ で定まる写像を線形に拡張することによって定義できる．

h の定義から，$\pi=h\circ g'$ を満たす．すると，$\operatorname{Ker}g'\subset\operatorname{Ker}(h\circ g')=\operatorname{Ker}\pi=\operatorname{Im}f'$ となる． □

定理 8.12. R は環，L, M は R-加群で，L_0 は L の部分 R-加群，M_0 は M の部分 R-加群とする．包含写像 $\iota_L\colon L_0\xrightarrow{\subset}L$ に $\otimes_R M$ して作った写像 $\iota_L\otimes\mathrm{id}_M\colon(L_0\otimes_R M)\longrightarrow(L\otimes_R M)$ (これは単射とは限らない) の像を

$$N_1=\operatorname{Im}\left(\iota_L\otimes\mathrm{id}_M\colon(L_0\otimes_R M)\longrightarrow(L\otimes_R M)\right)$$

とおく．同様に，$\iota_M\colon M_0\xrightarrow{\subset}M$ をとり，

$$N_2=\operatorname{Im}\left(\mathrm{id}_L\otimes\iota_M\colon(L\otimes_R M_0)\longrightarrow(L\otimes_R M)\right)$$

とおく．このとき，

$$(L/L_0)\otimes_R(M/M_0)\cong(L\otimes_R M)/(N_1+N_2)$$

が成り立つ．

証明. $0\to L_0\xrightarrow{\subset}L\twoheadrightarrow L/L_0\to 0$ に $\otimes_R M$ すると，完全系列

$$L_0\otimes_R M\xrightarrow{f}L\otimes_R M\longrightarrow(L/L_0)\otimes_R M\longrightarrow 0$$

($f=\iota_L\otimes\mathrm{id}_M$) が得られるので，

$$L/L_0\otimes_R M\cong(L\otimes_R M)/\operatorname{Im}f=(L\otimes_R M)/N_1$$

である．

$$N_2'=\operatorname{Im}\left(\mathrm{id}_{L/L_0}\otimes\iota_M:(L/L_0\otimes_R M_0)\longrightarrow(L/L_0\otimes_R M)\right)$$

とおく．上の結果から，

$$\frac{L}{L_0}\otimes_R\frac{M}{M_0}\cong\frac{L/L_0\otimes_R M}{N_2'}\cong\frac{(L\otimes_R M)/N_1}{N_2'}$$

である．自然な全射

$$g\colon(L\otimes_R M)\twoheadrightarrow(L\otimes_R M)/N_1\cong L/L_0\otimes_R M$$
$$h\colon(L\otimes_R M)/N_1\twoheadrightarrow\frac{(L\otimes_R M)/N_1}{N_2'}\cong L/L_0\otimes_R M/M_0$$

を考える．$g(N_2)=N_2'$ だから，準同型定理より，

$$g^{-1}(N_2')=N_2+\operatorname{Ker}g=N_2+N_1$$

が成り立つ．よって，$\operatorname{Ker}(h\circ g)=N_1+N_2$ で，

$$L/L_0\otimes_R M/M_0\cong(L\otimes_R M)/(N_1+N_2)$$

が成り立つ． □

例 8.13. m, $n\in\mathbb{N}$ で，m と n の最大公約数が d のとき，

$$(\mathbb{Z}/m\mathbb{Z})\otimes_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})\cong\mathbb{Z}/d\mathbb{Z}$$

である．これを使うと，$0\longrightarrow L\xrightarrow{f}M\xrightarrow{g}N\longrightarrow 0$ が完全系列であっても，$0\longrightarrow(L\otimes_R A)\xrightarrow{f'}(M\otimes_R A)\xrightarrow{g'}(N\otimes_R A)\longrightarrow 0$ が完全系列にならない例が構成できる．例えば，

$$0\longrightarrow\mathbb{Z}\xrightarrow{f}\mathbb{Z}\longrightarrow\mathbb{Z}/2\mathbb{Z}\longrightarrow 0\quad(\text{ただし，}f(x)=2x)$$

に $\otimes_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ すると，完全系列 $\mathbb{Z}/2\mathbb{Z}\xrightarrow{f'}\mathbb{Z}/2\mathbb{Z}\longrightarrow\mathbb{Z}/2\mathbb{Z}\longrightarrow 0$ が得られるが，f' は 0 写像であって，単射ではない．

定義 8.14.(係数拡大) R は可換環，S は R-代数，M は R-加群とする．S は R-加群なので，R-加群として $S\otimes_R M$ が定義できる．勝手な $t\in S$, $x\in S\otimes_R M$ を取る．ある $n\in\mathbb{N}$; $s_i\in S$, $m_i\in M$ により，$x=\sum_{i=1}^{m}s_i\otimes m_i$ と書ける．そこで，$tx=\sum_{i=1}^{m}(ts_i)\otimes m_i\in S\otimes_R M$ によって S の $S\otimes_R M$ への作用を定めると，$S\otimes_R M$ は S-加群になる．$S\otimes_R M$ を R-加群 M の S への**係数拡大**という．

例 8.15. R, S は体で $R \subset S$ (部分環)，$M = R^n$ (R 上のランク n の自由加群) とする．このとき，$S \otimes_R M \cong S^n$ である．

実際，$M_1 = \cdots = M_n = R$ として，$M = R^n = \bigoplus_{i=1}^{n} M_i$ であるので，

$$S \otimes_R M = S \otimes_R \left(\bigoplus_{i=1}^{n} M_i \right) \cong \bigoplus_{i=1}^{n} S \otimes_R M_i \cong \bigoplus_{i=1}^{n} S \otimes_R R \cong \bigoplus_{i=1}^{n} S = S^n$$

である．

定義 8.16.(R-代数のテンソル積) R は可換環，S_1, S_2 は R-多元環とする．S_1, S_2 は R-加群であるので，R-加群として $S_1 \otimes_R S_2$ が定義できる．勝手な元 x, $y \in S_1 \otimes_R S_2$ を取る．ある m, $n \in \mathbb{N}$; a_i, $a'_j \in S_1$, b_i, $b'_j \in S_2$ により，$x = \sum_{i=1}^{m} a_i \otimes b_i$, $y = \sum_{j=1}^{n} a'_j \otimes b'_j$ と書ける．そのとき，

$$xy = \sum_{i=1}^{m} \sum_{j=1}^{n} (a_i a'_j) \otimes (b_i b'_j) \in S_1 \otimes_R S_2$$

によって，$S_1 \otimes_R S_2$ に積を矛盾なく定義できる (証明が必要だが，難しくないので省略)．すると，$S_1 \otimes_R S_2$ も可換環になる (定義を確認するだけなので証明省略)．単位元は $1 \otimes 1$, ゼロ元は $0 \otimes 0$ である．$S_1 \otimes_R S_2$ を R-代数 S_1, S_2 の**テンソル積**という．$S_1 \otimes_R S_2$ は R-代数，S_1-代数，S_2-代数の構造も持つ．

問 8.17. R は可換環，$S_1 = R[X_1, \ldots, X_m]$, $S_2 = R[Y_1, \ldots, Y_n]$ とする．すると，

$$S_1 \otimes_R S_2 \cong R[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$$

であることを証明せよ．

ヒント: S_1 は $\left\{ X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m} \;\middle|\; i_1, \ldots, i_m \in \mathbb{N} \cup \{0\} \right\}$ を基底とする自由加群であることと，定理 8.9 を用いよ．

9. ネーター環

定義 9.1. R-加群 M が**ネーター加群** (Noetherian module) であるとは，M の部分 R-加群 N_i の列 $N_1 \subset N_2 \subset N_3 \subset \cdots$ があれば，ある $n \in \mathbb{N}$ が存在して，$i \geqq n$ ならば $N_i = N_n$ となることをいう．

環 R が**ネーター環**であるとは，R を R-加群を考えたときネーター加群であることをいう．つまり，R のイデアルの列 $I_1 \subset I_2 \subset I_3 \subset \cdots$ があれば，ある $n \in \mathbb{N}$ が存在して，$I_n = I_{n+1} = I_{n+2} = \cdots$ となることをいう．

R は可換環，S は R-代数とする．S が R-加群として有限生成であるとき，**有限** R-多元環であると言う．他方，$S \cong R[X_1, \ldots, X_n]/I$ (I は $R[X_1, \ldots, X_n]$ のあるイデアル) と書けるとき，S は**有限生成** R-多元環であるとか，R 上有限生成な環であると言う．有限 R-多元環は有限生成 R-多元環であるが，逆は一般には正しくなく，例えば，多項式環 $R[X]$ は有限生成 R-多元環であるが，有限 R-多元環ではない．

R-多元環の間の写像 $f\colon S_1 \to S_2$ は，f が環の準同型写像であって，かつ R-加群の準同型写像であるとき，R-多元環の準同型写像であると言う．

定理 9.2. R-加群 M がネーター加群であるための必要十分条件は，M の任意の部分 R-加群が R 上有限生成であることである．特に，R がネーター環であるための必要十分条件は，R の任意のイデアルが有限生成であることである．

証明. M はネーター加群で，N は M の部分 R-加群とする．$N_0 = \{0\}$ とし，帰納的に R-加群の列が $N_0 \subset N_1 \subset \cdots \subset N_i \subset N$ まで定まったとき，$N_i \neq N$ であれば $x_{i+1} \in N - N_i$ を選んで，$N_{i+1} = N_i + Rx_i$ とおく．M はネーター加群だから，ある $n \in \mathbb{N}$ が存在し $N = N_n = Rx_1 + \cdots + Rx_n$ となる．よって，N は有限生成である．

逆に，M の任意の部分 R-加群 N が有限生成であるとする．M の部分 R-加群 N_i の列 $N_1 \subset N_2 \subset N_3 \subset \cdots$ があるとする．$\bigcup_{i=1}^{\infty} N_i$ は M の有限生成部分加群だから，その生成元を $x_1, \ldots, x_m$ とすれば，

ある $n \in \mathbb{N}$ が存在して，$x_1,\ldots, x_m \in N_n$ となる．よって，$\bigcup_{i=1}^{\infty} N_i = N_n$ であり，$i \geqq n$ のとき $N_i = N_n$ となる． □

定理 9.3. R がネーター環のとき，有限生成 R-加群はネーター加群である．

証明. $M = Rx_1 + \cdots + Rx_r$ $(x_i \in M)$ とし，生成元の個数 r に関する帰納法で証明する．$r = 1$ のときは，$\varphi\colon R \to Rx_1 = M$ を $\varphi(a) = ax_1$ で定義される写像とする．R-部分加群の列が $N_0 \subset N_1 \subset \cdots \subset M$ があると，R のイデアルの列 $\varphi^{-1}(N_0) \subset \varphi^{-1}(N_1) \subset \cdots$ ができるが，R はネーター環なので，ある $n_0 \in \mathbb{N}$ が存在して任意の $n \geqq n_0$ に対し $\varphi^{-1}(N_n) = \varphi^{-1}(N_{n_0})$ となる．したがって，$N_n = N_{n_0}$ であり，M はネーター加群である．

$r \geqq 2$ とし，$r-1$ 個以下の元で生成される R-加群については定理は正しいと仮定する．$M_1 = Rx_r$, $M_2 = M/M_1$ とすると，M_1, M_2 は $r-1$ 個以下の元で生成されるのでネーター加群である．$\varphi\colon M \twoheadrightarrow M_1$ を自然な全射とする．R-部分加群の列が $N_0 \subset N_1 \subset \cdots \subset M$ があると，M_1 はネーター加群だから，ある $n_1 \in \mathbb{N}$ が存在して任意の $n \geqq n_1$ に対し $N_n \cap M_1 = N_{n_1} \cap M_1$ となり，M_2 はネーター加群だから，ある $n_2 \in \mathbb{N}$ が存在して任意の $n \geqq n_2$ に対し，$\varphi(N_n) = \varphi(N_{n_2})$ となる．したがって，$n \geqq n_0 = \max\{n_1, n_2\}$ のとき，$N_n = N_{n_0}$ となる． □

系 9.4. (1) R がネーター環，M が有限生成 R-加群，N が M の部分 R-加群ならば，N は有限生成なネーター加群である．

(2) R がネーター環，M が有限生成 R-加群，N が M の部分 R-加群ならば，M/N もネーター加群である．

(3) R がネーター環のとき，R/I もネーター環である．

定理 9.5. R がネーター環ならな， $R[X]$ もネーター環である．

証明. $R[X]$ のイデアル I を取る．自然数 n に対し，I に属する n 次多項式の最高次 (n 次) の係数全体の集合と $\{0\}$ の合併集合を J_n とする．また，$J_0 = I \cap R$ とする．J_n は R のイデアルで，$J_0 \subset J_1 \subset J_2 \subset \cdots$ である．R はネーター環だから，ある $n \in \mathbb{N}$ が存在して，$J_n = J_{n+1} = J_{n+2} = \cdots$ となる．今，J_k は有限生成イデアルだから，$J_k = (a_{k,1},\ldots, a_{k,r_k})$ とし，$a_{k,i}$ を最高次 (k 次) の項の係数とする I に属する多項式を 1 つ選んで，それを $f_{k,i} \in R[X]$ とする．

$F_k = \{f_{k,1},\ldots, f_{k,r_k}\}$ とし，$F_0 \cup F_1 \cup \cdots \cup F_n$ で生成される $R[X]$ のイデアルを I' とする．定義から，$I' \subset I$ である．

逆に，任意の $g \in I$ に対し，$g \in I'$ となることを，$k = \deg_X g$ に関する帰納法で証明する．$k = 0$ なら，$g \in R \cap I = J_0 = (f_{0,1},\ldots, f_{0,r_0})$ より，$g \in I'$ である．

$1 \leqq k \leqq n$ とする．g の最高次の項の係数 b は J_k に属するから，ある $b_1,\ldots, b_{r_k} \in R$ が存在し，$b = b_1a_{k,1} + \cdots + b_{r_k}a_{k,r_k}$ となる．したがって，$h = g - (b_1f_{k,1} + \cdots + b_{r_k}f_{k,r_k})$ とおけば，$\deg_X h \leqq k-1$, $h \in I$ となる．帰納法の仮定から，$h \in I'$ なので，$g \in I'$ である．

$k > n$ の場合は，$J_k = J_n$ だから，同様に，ある $b_1,\ldots, b_{r_n} \in R$ が存在し，$h = g - X^{k-n} \cdot (b_1f_{n,1} + \cdots + b_{r_n}f_{n,r_n})$ とおけば，$\deg_X h \leqq k-1$ となり，帰納法の仮定から，$h \in I'$ なので，$g \in I'$ となる．したがって，$I = I'$ で I は有限生成である．すなわち，$R[X]$ はネーター環である． □

定理 9.6.(ヒルベルト (Hilbert) の基底定理) R はネーター環とする．このとき，$R[X_1,\ldots, X_n]$ はネーター環であり，そのイデアル I による剰余環 $R[X_1,\ldots, X_n]/I$ もネーター環である．したがって，ネーター環 R 上の有限生成多元環はネーター環である．

証明. $R[X_1,\ldots, X_n] = (R[X_1,\ldots, X_{n-1}])[X_n]$ より，R がネーター環ならば，$R[X_1,\ldots, X_n]$ もネーター環である．また，$R[X_1,\ldots, X_n]$ の任意のイデアル I に対し，$R[X_1,\ldots, X_n]/I$ もネーター環である． □

上の定理から，K が体のとき，$K[X_1,\ldots, X_n]$ や $K[X_1,\ldots, X_n]/I$ はネーター環である．

定理 9.7. R はネーター環，$S \subset R$ は積閉集合とする．このとき，$S^{-1}R$ はネーター環である．

証明. 定理 6.7 の証明を思い出そう．S^{-1} のイデアルの列 $J_1 \subset J_2 \subset J_3 \subset \cdots$ に対し，$I_k = \varphi^{-1}(J_k)$ とおくと，$I_1 \subset I_2 \subset I_3 \subset \cdots$ は R のイデアル列である．R はネーター環だから，ある $n \in \mathbb{N}$ が存在して，$k > n$ のとき $I_k = I_n$ となる．すると，$J_k = I_k(S^{-1}R) = I_n(S^{-1}R) = J_n$ となる． □

10. 準素イデアル

定理 10.1. R は可換環，R のイデアル $I \subsetneqq R$ に対し，

$$\sqrt{I} := \left\{ a \in R \;\middle|\; \text{ある } n \in \mathbb{N} \text{ に対して } x^n \in I \right\}$$

とおく．すると，$\sqrt{I}$ は R のイデアルである．さらに，以下が成り立つ．
(1) $\sqrt{I}$ は I を含む R のすべての素イデアルの共通部分に等しい．
(2) I, J が R のイデアルのとき，$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ である．

証明. $\sqrt{I}$ がイデアルであることを示す．$x, y \in \sqrt{I}$ とすると，ある $n \in \mathbb{N}$ が存在し，$x^n \in I, y^n \in I$ となる．このとき，二項定理により，$(x+y)^{2n} = x^n f(x,y) + y^n g(x,y)$ という形に表せるので，$x+y \in \sqrt{I}$ である．

また，$a \in R$ に対し，$(ax)^n \in I$ なので，$ax \in \sqrt{I}$ である．

(1) I を含む R のすべての素イデアルの共通部分を J とする．$\mathfrak{p}$ が素イデアルで $I \subset \mathfrak{p}$ ならば，$\sqrt{I} \subset \mathfrak{p}$ であることはすぐわかる．よって，$\sqrt{I} \subset J$ である．

逆に，$x \in J$, $x \notin \sqrt{I}$ を取る．$S = \left\{ x^n \;\middle|\; n \in \mathbb{N} \right\}$ は積閉集合である．$I(S^{-1}R)$ を含む $S^{-1}R$ の極大イデアルの R への引き戻しを $\mathfrak{p}$ とする．$\mathfrak{p}$ は I を含み，S と交わらない極大なイデアルである．また，定理 6.7(4) より $\mathfrak{p}$ は素イデアルである．$x \notin \mathfrak{p}$ なので，$x \notin J$ である．

(2) $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$ は自明である．勝手な $x \in \sqrt{I} \cap \sqrt{J}$ を取る．ある $n \in \mathbb{N}$ が存在して，$x^n \in I$, $x^n \in J$ となるので，$x^n \in I \cap J$ となり，$x \in \sqrt{I \cap J}$ がわかる． □

定理 10.2(中山の補題) R は可換環，M は有限生成 R-加群，N は M の部分 R-加群とする．また，R のすべての極大イデアルの共通部分を J とする (J は **Jacobson 根基**とよばれる)．このとき，もし，

$$JM + N = M$$

が成り立つならば，$M = N$ である．

証明. $L = M/N$ とおく．$L \neq 0$ と仮定して矛盾を導く．$JM + N = M$ より，$JL = L$ となる．L も有限生成 R-加群なので，生成元を $x_1, \ldots, x_n \in L$ とする．$JL = L$ より，各 $1 \leqq i \leqq n$ に対し，

$$x_i = \sum_{j=1}^{n} a_{ij} x_j, \quad (\exists a_{ij} \in J)$$

と書ける．a_{ij} を第 i 行第 j 列の成分とする n 次正方行列を A とする．また，$x_1, \ldots, x_n$ を縦に並べてできる列ベクトルを $\mathbf{x}$，n 次の単位行列を I_n とすると，$(I_n - A)\mathbf{x} = \mathbf{0}$ (0-ベクトル) なので，$(I_n - A)$ の余因子行列を B とし $a = \det(I_n - A)$ とおけば，$a\mathbf{x} = B(I_n - A)\mathbf{x} = \mathbf{0}$ である．他方，$a_{ij} \in J$ なので，ある $m \in J$ が存在して，$a = \det(I_n - A) = 1 + m \notin J$ である．もし，a が可逆元でないとすると $(a) \subsetneqq R$ だから，$(a) \subset \mathfrak{m} \subsetneqq R$ を満たす極大イデアルが存在する．$m \in J \subset \mathfrak{m}$ だから $1 = a - m \in \mathfrak{m}$. よって，$\mathfrak{m} = R$ となり矛盾する．よって，$a^{-1} \in R$ で，$\mathbf{x} = a^{-1}\mathbf{0} = \mathbf{0}$ となり矛盾する．したがって，$L = 0$ で，$M = N$ である． □

系 10.3.(Krull の共通部分定理)
(1) $(R, \mathfrak{m})$ がネーター局所環ならば，$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0)$ である．
(2) R がネーター整域で，$I \neq R$ がそのイデアルのとき，$\bigcap_{n=1}^{\infty} I^n = (0)$ である．

証明. (1) $M = \bigcap_{n=1}^{\infty} \mathfrak{m}^n$ とする．$\mathfrak{m}M \supset M$ を示す．$\mathfrak{m} = (a_1, \ldots, a_r)$ と書ける．多項式環 $S = R[X_1, \ldots, X_r]$ を考え，自然な準同型写像 $\varphi\colon S \to R$ を $\varphi(X_i) = a_i$ で定める．

$$S_n = \{f \in S \mid f \text{ は } n \text{ 次斉次多項式}\} \cup \{0\},$$
$$J_n := \{f \in S_n \mid \varphi(f) \in M\}$$

とし，$\bigcup_{n\in\mathbb{N}} J_n$ で生成される S のイデアルを J とする．$J = (f_1, \ldots, f_s)$ と書ける．J の定義から，各 f_i は斉次元であると仮定してよい．$d_i = \deg f_i$, $n_0 = \max\{d_1, \ldots, d_s\}$ とする．$\varphi(S_n) = \mathfrak{m}^n$ に注意する．

勝手な $b \in M$ を取る．$n = n_0 + 1$ とすると，$b \in \mathfrak{m}^n$ なので，$\varphi(g) = b$ となる $g \in S_n$ が存在する．$g = h_1 f_1 + \cdots + h_s f_s$ ($h_i \in S$ はある $(n - d_i)$ 次斉次式) と書ける．

$$b = \varphi(g) = \sum_{i=1}^{s} \varphi(h_i)\varphi(f_i) \in \sum_{i=1}^{s} \mathfrak{m}^{n-d_i} M \subset \mathfrak{m}^{n-n_0} M \subset \mathfrak{m}M$$

となる．よって，$\mathfrak{m}M \supset M$ を示す．$\subset$ は自明なので，$\mathfrak{m}M = M$ である．

$\mathfrak{m}M = M$ である．そこで，$N = 0$ として中山の補題を使うと，$M = 0$ が得られる．

(2) I を含む極大イデアル $\mathfrak{m}$ を取る．$S = R_{\mathfrak{m}}$, $\mathfrak{n} = \mathfrak{m}R_{\mathfrak{m}}$ とおく．$R \subset S$ とみなしたとき，$I^n \subset \mathfrak{n}^n$ である．(1) より，$\bigcap_{n=1}^{\infty} I^n \subset \bigcap_{n=1}^{\infty} \mathfrak{n}^n = (0)$ である． □

定義 10.4. R のイデアル $I \subsetneqq R$ が「$a, b \in R$, $ab \in I$, $b \notin I \Longrightarrow \exists n \in \mathbb{N}$, $a^n \in I$」を満たすとき，I は**準素イデアル** (primary ideal) であると言う．

例 10.5. $R = \mathbb{Z}$ において，p が素数で $n \in \mathbb{N}$ のとき，(p^n) は準素イデアルである．一般に R が UFD で $p \in R$ が素元のとき，(p^n) は準素イデアルである．

問 10.6. R は可換環とする．
(1) $I \subset R$ が準素イデアルならば，$\sqrt{I}$ は R の素イデアルであることを示せ．
(2) $\mathfrak{m} \subset R$ が極大イデアルのとき，$\sqrt{(\mathfrak{m}^n)} = \mathfrak{m}$ で，$\mathfrak{m}^n$ は準素イデアルであることを示せ．

注意 10.7. $\mathfrak{p}$ が極大ではない R の素イデアルのとき，$\sqrt{(\mathfrak{p}^n)} = \mathfrak{p}$ は成り立つが，$\mathfrak{p}^n$ が準素イデアルになるとは限らない．例えば, $R = \mathbb{C}[X, Y, Z]/(X^2 - YZ)$ において，$\mathfrak{p} = (X, Y)$ は R の素イデアルであるが，$\mathfrak{p}^2$ は準素イデアルにならない．

定理 10.8. R がネーター環で，$I \subsetneqq R$ が R のイデアルのとき，有限個の準素イデアル $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ で，以下の条件を満たすものがある．
(1) $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$.
(2) $i \neq j$ ならば $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$.
(3) $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ から $\mathfrak{q}_i$ を除いた $n-1$ 個のイデアルの共通部分を $\mathfrak{r}_i = \bigcap_{j\neq i} \mathfrak{q}_j$ とおくとき，$I \subsetneqq \mathfrak{r}_i$.

このような準素イデアル $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ を用いて，I を (1) のように表すことを，I の**準素イデアル分解**と言う．また，素イデアル $\sqrt{\mathfrak{q}_i}$ を I の**素因子**と言う．I の準素イデアル分解 (1) において，素因子 $\mathfrak{p}$ に対し，$\mathfrak{q} \subsetneqq \mathfrak{p}$ を満たす I の素因子 $\mathfrak{q}$ が存在する場合，$\mathfrak{p}$ を**埋没素因子** (embeded prime) とか**非孤立素因子**と言う，このような素因子 $\mathfrak{q}$ が存在しない場合，$\mathfrak{p}$ を**極小素因子**と言う，

極小素因子全体の集合は，準素イデアル分解 (1) の取り方に依存せずに I から一意的に定まる．

証明. R のイデアル J が既約であるとは，R のイデアル J_1, J_2 が $J = J_1 \cap J_2$ を満たせば，$J = J_1$ または $J = J_2$ が成り立つことをいう．

もし，I が既約でなければ，あるイデアル $I_1 \neq I$, $I_2 \neq I$ により，$I = I_1 \cap I_2$ と表せる．I_1 や I_2 が既約でなければ，I_1 あるいは I_2 をこのように分解する．この操作を繰り返して，$I = I_1 \cap \cdots \cap I_n$ ($I_k \neq I$) ができる．R では真に増大する無限イデアル列は存在しないから，このような分解はどこかで終わって，すべての I_k は既約イデアルになる．

Claim. 既約イデアルは準素イデアルである．

I は既約イデアルとする．I が準素イデアルでないと仮定すると，ある $x, y \in R$ で，$xy \in I$, $y \notin I$, $x^i \notin I$ $(\forall i \in \mathbb{N})$ となるものが存在する．

$J_n = \left\{ a \in R \;\middle|\; ax^n \in I \right\}$ とすると，$J_1 \subset J_2 \subset \cdots$ だから，ネーター環の性質より，ある $n \in \mathbb{N}$ が存在して，$J_n = J_{n+1} = \cdots$ となる．$I_1 = I + x^n R$, $I_2 = I + yR$ とおくと，$I_1 \neq I$, $I_2 \neq I$, $I \subset I_1 \cap I_2$ である．逆に，$a \in I_1 \cap I_2$ を取ると，$a = b_1 + c_1 x^n = b_2 + c_2 y$ $(b_i \in I,\ c_i \in R)$ と書ける．すると，$c_1 x^{n+1} = c_2 xy + (b_2 - b_1)x \in I$ となるので，$c_1 \in J_{n+1} = J_n$ であり，$a \in I$ となり，$I = I_1 \cap I_2$ が得られる．これは I が既約であることと矛盾するので，I は準素イデアルである．

以上より，I は (1) のように準素イデアルの共通部分として表せる．このとき，もし (3) が成立せず，$I = \mathfrak{r}_i$ となる i があったら，$\mathfrak{q}_i$ を取り除いても (1) が成立するから，このような無駄な $\mathfrak{q}_i$ をすべて取り除いて，(3) が成立するようにできる．

また，(2) が成立しないとする．例えば，$\sqrt{\mathfrak{q}_1} = \sqrt{\mathfrak{q}_2}$ であるとする．すると，$\mathfrak{q} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ も準素イデアル (簡単なので証明してみよ) だから，(2) の表示から $\mathfrak{q}_1$, $\mathfrak{q}_2$ を取り除いて $\mathfrak{q}$ を付け加える．このような操作を繰り返すと (2) が成り立つようになる．

最後に，極小素因子の一意性を証明する．$\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ を準素イデアル分解 (1) の極小素因子全体の集合とする．また，$I = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_m$ を別の準素イデアル分解とし，$\mathfrak{p}'_1, \ldots, \mathfrak{p}'_s$ をその極小素因子全体の集合とする．

$$\mathfrak{p}_i \supset \sqrt{I} = \sqrt{\mathfrak{q}'_1} \cap \cdots \cap \sqrt{\mathfrak{q}'_m} = \mathfrak{p}'_1 \cap \cdots \cap \mathfrak{p}'_s$$

より，ある j が存在し，$\mathfrak{p}_i \supset \mathfrak{p}'_j$ となる．逆に，k が存在し，$\mathfrak{p}'_j \supset \mathfrak{p}_k$ となるが，$\mathfrak{p}_i$, $\mathfrak{p}_k$ は極小なので，$i = k$ となる． □

注意 10.9. 上の準素イデアル分解は一意的とは限らない．

例 10.10. $R = \mathbb{Z}$ とし，n は 2 以上の整数，$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ をその素因数分解とする．定理 5.4(2) より，

$$(n) = (p_1^{e_1})(p_2^{e_2}) \cdots (p_r^{e_r}) = (p_1^{e_1}) \cap (p_2^{e_2}) \cap \cdots \cap (p_r^{e_r})$$

であるが，これがイデアル $(n) = n\mathbb{Z}$ の準素イデアル分解である (この場合は，この 1 通りしかない)．

もともと，準素イデアル分解というのは，$\mathbb{Z}$ における素因数分解の一般化として考えられたものである．

11. 完備化と p 進整数環

射影的極限 (逆極限) の定義は，簡単のため添え字集合 I が (半) 順序集合の場合についてのみ述べるが，定義をかなり変更することにより I が有向グラフの場合 (例えば，サイクルを含んだり，写像 $M_i \to M_j$ が複数存在する場合) にも定義することができる．ただ,「十分先で一致する」という余計な条件をつけて議論しないといけないので，この授業では扱わない．

定義 11.1. R は環，$(\Lambda, \leqq)$ は半順序集合とし，各 $\lambda \in \Lambda$ に対し，R-加群 M_λ が与えられているとする．さらに，$\lambda, \mu \in \Lambda$ が $\lambda \leqq \mu$ を満たす場合には R-準同型写像 $f_{\mu\lambda} \colon M_\mu \to M_\lambda$ が与えられていると仮定する．これが，次の条件 (1), (2) を満たすとき，$\{M_\lambda, f_{\mu\lambda}\}$ は**射影系**とか**逆系**であるという．

(1) $f_{\lambda\lambda} \colon M_\lambda \to M_\lambda$ は恒等写像である $(\forall \lambda \in \Lambda)$.

(2) $\lambda, \mu, \nu \in \Lambda$ が $\lambda \leqq \mu \leqq \nu$ を満たせば，$f_{\nu\lambda} = f_{\mu\lambda} \circ f_{\nu\mu}$ が成り立つ．

なお，$\Lambda = \mathbb{N}$ の場合には，各 $n \in \Lambda$ に対し $f_{n+1,n} \colon M_{n+1} \to M_n$ を与えれば，それから自然に帰納系が定まることに注意する．

上のような射影系 $\{M_\lambda, f_{\mu\lambda}\}$ に対し，その**射影的極限** (**逆極限**) $\varprojlim_\lambda M_\lambda = \varprojlim M_\lambda$ を以下のように定義する．

$$\varprojlim M_\lambda = \left\{ (x_\lambda)_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} M_\lambda \;\middle|\; \lambda, \mu \in \Lambda,\ \lambda \leqq \mu \text{ ならば } x_\lambda = f_{\mu\lambda}(x_\mu) \right\}$$

また，包含写像 $\varprojlim M_\lambda \xrightarrow{\subset} \prod_{\lambda \in \Lambda} M_\lambda$ と正射影 $\pi_\mu \colon \prod_{\lambda \in \Lambda} M_\lambda \twoheadrightarrow M_\mu$ を合成して得られる写像を $f_{\infty\mu} \colon \varprojlim M_\lambda \longrightarrow M_\mu$ と書く．

$x \in \varprojlim M_\lambda$ に対し $x_\lambda = f_{\infty\lambda}(x) \in M_\lambda$ $(\lambda \in \Lambda)$ とするとき，$x = \varprojlim x_\lambda$ と書き，x は Λ-列 $\{x_\lambda\}$ の**極限**であるという．

この講義では帰納的極限は使わないので，以下は授業では話さないが，一応紹介しておく．

定義 11.2. R は環，$(\Lambda, \leqq)$ は半順序集合とし，各 $\lambda \in \Lambda$ に対し，R-加群 M_λ が与えられているとする．さらに，$\lambda, \mu \in \Lambda$ が $\lambda \leqq \mu$ を満たす場合には R-準同型写像 $f_{\lambda\mu}\colon M_\lambda \to M_\mu$ が与えられていると仮定する．これが，次の条件 (1), (2) を満たすとき，$\{M_\lambda, f_{\lambda\mu}\}$ は**帰納系**とか**直系**とか**順系**であるという．
(1) $f_{\lambda\lambda}\colon M_\lambda \to M_\lambda$ は恒等写像である $(\forall \lambda \in \Lambda)$.
(2) $\lambda, \mu, \nu \in \Lambda$ が $\lambda \leqq \mu \leqq \nu$ を満たせば，$f_{\lambda\nu} = f_{\mu\nu} \circ f_{\lambda\mu}$ が成り立つ．

上のような帰納系 $\{M_\lambda, f_{\lambda\mu}\}$ に対し，その**帰納的極限** (**直極限**, **順極限**) $\varinjlim M_\lambda$ を次のように定義する．

$U = \bigoplus_{\lambda\in\Lambda} M_\lambda$ とし，$\iota_\mu\colon M_\mu \hookrightarrow U$ を埋入写像とする．さらに，

$$X = \left\{ \iota_\lambda(x) - \iota_\mu(f_{\lambda\mu}(x)) \in U \;\middle|\; \lambda, \mu \in \Lambda,\ \lambda \leqq \mu,\ x \in M_\lambda \right\}$$

とし，X で生成される U の部分 R-加群を V とおく．そして，

$$\varinjlim M_\lambda = U/V$$

定義する．$\varinjlim M_\lambda$ を $\varinjlim_\lambda M_\lambda$ などとも書く．

また，$\iota_\mu\colon M_\mu \to U$ と自然な全射 $U \twoheadrightarrow U/V$ を合成して得られる写像を，$f_{\mu\infty}\colon M_\mu \longrightarrow \varinjlim M_\lambda$ と書くことにする．X の定義から，$\lambda, \mu \in \Lambda, \lambda \leqq \mu$ であるとき，$f_{\mu\infty} \circ f_{\lambda\mu} = f_{\lambda\infty}$ が成り立つ．

$x \in \varinjlim M_\lambda$ を任意に選ぶとき，ある $r \in \mathbb{N}$ とある $\lambda_1, \ldots, \lambda_r \in \Lambda$ により，$x = f_{\lambda_1\infty}(x_{\lambda_1}) + \cdots + f_{\lambda_r\infty}(x_{\lambda_r})$ と表すことができる．さらに，Λ が有向集合であれば，ある $\lambda \in \Lambda$ とある $x_\lambda \in M_\lambda$ により，$x = f_{\lambda\infty}(x_\lambda)$ と表すことができる．なお，Λ が**有向集合**であるとは，任意の $\lambda, \mu \in \Lambda$ に対し，$\lambda \leqq \nu$, $\mu \leqq \nu$ を満たす $\nu \in \Lambda$ が存在することをいう．この場合，$x = f_{\lambda_1\infty}(x_{\lambda_1}) + \cdots + f_{\lambda_r\infty}(x_{\lambda_r})$ に対し，$\lambda_i \leqq \mu$ $(\forall i)$ となるような μ をとり $y_i = f_{\lambda_i\mu}(x_{\lambda_i})$, $y = y_1 + \cdots + y_r$ とおけば，$x = f_{\mu\infty}(y)$ となる．

帰納的極限, 射影的極限の定義からわかるように，もし，添え字集合 Λ が無順序集合 (任意の $\lambda \neq \mu \in \Lambda$ が比較不可能である半順序集合) であれば，射影的極限は直積と一致し，帰納的極限は直和に一致する．

また, 射影系や，有向集合による帰納系において，もし，各 M_λ が R-多元環で $f_{\lambda\mu}$ が R-多元環の準同型写像であるならば，$\varinjlim M_\lambda$ も $\varprojlim M_\lambda$ も R-多元環になる．

実際，$1 = (1_\lambda)_{\lambda\in\Lambda} \in \varprojlim M_\lambda$ なので，$\varprojlim M_\lambda$ は $\prod_{\lambda\in\Lambda} M_\lambda$ の部分環になる．また，Λ が有向集合の場合は，$\lambda, \mu \in \Lambda$ に対し，$\lambda \leqq \nu$, $\mu \leqq \nu$ を満たす $\nu \in \Lambda$ を取ると，$f_{\lambda\infty}(1_\lambda) = f_{\lambda\infty}(1_\nu) = f_{\mu\infty}(1_\mu)$ なので，これが $\varinjlim M_\lambda$ の単位元になり，$\varinjlim M_\lambda$ も環になる．

定義 11.3. R は可換環，$\mathfrak{a}$ は R のイデアルとし，$\Lambda = \mathbb{N}$ を自然な順序で順序集合とする．$n \in \mathbb{N}$ に対し，$M_n = R/\mathfrak{a}^n$ とおく．$m \leqq n$ のとき $f_{nm}\colon R/\mathfrak{a}^n \twoheadrightarrow R/\mathfrak{a}^m$ は自然な全射とする．すると，$\{R/\mathfrak{a}^n, f_{nm}\}$ は $\mathbb{N}$ を添え字集合とする射影系になる．このとき，射影的極限 $\varprojlim_n R/\mathfrak{a}^n$ を $\widehat{R}$ などと書き，$\mathfrak{a}$ による R の**完備化**という．

特に，$R = \mathbb{Z}$ で $\mathfrak{a} = (p) = p\mathbb{Z}$ (p は素数) のとき，イデアル (p) による $\mathbb{Z}$ の完備化を $\mathbb{Z}_p$ と書き，$\mathbb{Z}_p$ を p-**進整数環**という．

$\varprojlim_n R/(0)^n \cong R$ であることに注意する．

命題 11.4. $\{M_\lambda, f_{\mu\lambda}\}, \{N_\lambda, g_{\mu\lambda}\}$ は同じ半順序集合 Λ で添え字づけられた射影系とし，各 $\lambda \in \Lambda$ に対し R-準同型写像 $h_\lambda\colon M_\lambda \to N_\lambda$ が存在して，$\lambda \leqq \mu$ $(\in \Lambda)$ ならば $h_\lambda \circ f_{\mu\lambda} = g_{\mu\lambda} \circ h_\mu$ が成り立つと仮定する．すると，$h_\infty\colon \varprojlim M_\lambda \longrightarrow \varprojlim N_\lambda$ が一意的に存在して，任意の $\lambda \in \Lambda$ に対し $g_{\infty\lambda} \circ h_\infty = h_\lambda \circ f_{\infty\lambda}$

が成り立つ．この h_∞ を $\{h_\lambda\}$ の**射影的極限**といい，$h_\infty = \varprojlim h_\lambda$ と書く．

$$\begin{array}{ccc} M_\mu & \xrightarrow{h_\mu} & N_\mu \\ {\scriptstyle f_{\mu\lambda}}\downarrow & & \downarrow{\scriptstyle g_{\mu\lambda}} \\ M_\lambda & \xrightarrow{h_\lambda} & N_\lambda \end{array} \qquad \begin{array}{ccc} \varprojlim M_\lambda & \xrightarrow{h_\infty} & \varprojlim N_\lambda \\ \downarrow{\scriptstyle f_\lambda} & & \downarrow{\scriptstyle g_\lambda} \\ M_\lambda & \xrightarrow{h_\lambda} & N_\lambda \end{array}$$

証明. $h_\lambda\colon M_\lambda \to N_\lambda$ から，$h : \prod_{\lambda\in\Lambda} M_\lambda \longrightarrow \prod_{\lambda\in\Lambda} N_\lambda$ が誘導される．

$$\varprojlim M_\lambda = \left\{ (x_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda \;\middle|\; \lambda,\, \mu \in \Lambda,\, \lambda \leqq \mu \text{ ならば } x_\lambda = f_{\mu\lambda}(x_\mu) \right\},$$

$$\varprojlim N_\lambda = \left\{ (y_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} N_\lambda \;\middle|\; \lambda,\, \mu \in \Lambda,\, \lambda \leqq \mu \text{ ならば } y_\lambda = g_{\mu\lambda}(y_\mu) \right\}$$

なので，h の定義域を制限することによって，求める h_∞ が得られる． □

$I \subset J \subset R$ がイデアルのとき，上の命題から，自然な全射 $\varprojlim_n R/I^n \longrightarrow \varprojlim_n R/J^n$ が存在する．

命題 11.5. R はネーター環，$\mathfrak{m}$ は R の極大イデアルとし，$\widehat{R} = \varprojlim_n R/\mathfrak{m}^n$ とおく．今，R は整域であるか，または，局所環であると仮定する．
(1) 自然な単射 $\iota\colon R \to \widehat{R}$ が存在する．
(2) $\widehat{R}$ は $\mathfrak{m}\widehat{R}$ を唯一の極大イデアルとする局所環である．

証明. (1) $h_n\colon R \to R/\mathfrak{m}^n$ を自然な全射とする．前命題を，$\Lambda = \mathbb{N}$, $M_n = R$, $f_{mn} = \mathrm{id}_R$, $N_n = R/\mathfrak{m}^n$, $g_{mn}\colon R/\mathfrak{m}^m \longrightarrow R/\mathfrak{m}^n$ を自然な全射として適用すると，$\iota = h_\infty\colon R \to \widehat{R}$ が構成できる．構成方法から，$\operatorname{Ker}\iota = \bigcap_{n=1}^{\infty} \mathfrak{m}^n$ であるが，Krull の共通部分定理より $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0)$ であり，ι は単射である．

(2) $K = R/\mathfrak{m}$, $R_n = R/\mathfrak{m}^n$ と置く．$R_n/\mathfrak{m}R_n \cong R/\mathfrak{m} = K$ なので，$\widehat{R}/\mathfrak{m}\widehat{R} = \varprojlim R_n/\mathfrak{m}R_n = K$ である．よって，$\mathfrak{m}\widehat{R}$ は $\widehat{R}$ の極大イデアルである．

次に，I は $\widehat{R}$ の極大イデアルとする．$J = I \cap R$ とおくと，準同型定理より $R/J \subset \widehat{R}/I$ である．$1 \notin J$ より $R/J \neq 0$ で R/J は整域で，$J \neq R$ は R のイデアルである．よって，$J \subset \mathfrak{m}$ で，$I \subset \mathfrak{m}$ となる．I は極大だから，$I = \mathfrak{m}$ となる． □

命題 11.6. K は体，$R = K[X_1,\ldots, X_r]$, $\mathfrak{m} = (X_1,\ldots, X_r)$ とする．このとき，

$$\varprojlim_n R/\mathfrak{m}^n \cong K[[X_1, \ldots, X_r]]$$

である．

証明. $\widehat{R} = \varprojlim_n R/\mathfrak{m}^n$, $S = K[[X_1, \ldots, X_r]]$, $\mathfrak{n} = \mathfrak{m}S$ とする．$S/\mathfrak{n}^n \cong R/\mathfrak{m}^n$ である．$S/\mathfrak{n}^n$ の元は巾級数 $f = \sum_{i_1=1}^{\infty} \cdots \sum_{i_r=1}^{\infty} a_{i_1\cdots i_r} X_1^{i_1} \cdots X_r^{i_r}$ に対し，その n 次以上の項を $\mathfrak{n}^n$ を法とすることにより無視したものであるから，$n-1$ 次以下の多項式 $f_n = \sum_{i_1+\cdots+i_r<n} a_{i_1\cdots i_r} X_1^{i_1} \cdots X_r^{i_r}$ と同一視できる．よって，$\widehat{S} = \varprojlim_n S/\mathfrak{n}^n$ の元は f と同一視でき，自然な単射 $S \to \widehat{S}$ は全射であり，同型写像になる．そこで，$S = \widehat{S}$ と考える．

命題 11.3 より，$\{h_n\}$ から $h\colon S \to \widehat{R}$ が誘導される．各 h_n が全射なので，h は全射である．また，$\operatorname{Ker} h = \bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0)$ なので，h は単射で，同型写像である． □

命題 11.7. R がネーター環ならば，$R[[X_1, \ldots, X_n]]$ もネーター環である．

証明. $R[[X_1, \ldots, X_n]] = (R[[X_1, \ldots, X_{n-1}]])[[X_n]]$ なので，R をネーター環として $R[[X]]$ もネーター環であることを示せばよい．$f(X) = \sum_{k=d}^{\infty} a_k X^k$, $a_d \neq 0$ に対し，$a_d X^d$ を $f(X)$ の**先導項**という．

I は $R[[X]]$ のイデアルとする．I の元の先導項全体を I_0 とし，I_0 で生成される $R[X]$ のイデアルを J とする．$R[X]$ はネーター環なので，J は有限個の元で生成される．その生成元は I_0 の元から選べる．つまり，$J = (b_1 X^{d_1}, \ldots, b_r X^{d_r})$ $(b_i \in R)$ と書ける．$b_j X^{d_j} \in J$ を先導項とする I の元の 1 つを f_j とする．

$I = (f_i, \ldots, f_r)$ であることを確かめる．$\supset$ は自明なので，$\subset$ を示す．勝手な $f(X) \in I$ を取る．$d = \operatorname{ord} f(X)$, $k = \max\{d_1, \ldots, d_r\}$ とおく．

まず，$g_{d-1}(X) = 0$ とおき，$g_d(X), g_{d+1}(X), \ldots$ を $\operatorname{ord}_X \big(f(X) - g_j(X)\big) > j$ を満たすように，以下のように帰納的に構成する．

$g_{j-1}(X)$ が $\operatorname{ord}_X \big(f(X) - g_{j-1}(X)\big) \geqq j$ を満たすように構成できたとする．ある $c_{j,1}, \ldots, c_{j,r} \in R$ により，

$$\operatorname{ord}_X \big(f(X) - g_{j-1}(X) - \big(c_{j,1} b_1 X^j + \cdots + c_{j,r} b_r X^j\big)\big) > j$$

となるようにできる．そこで，$g_j(X) := g_j(X) + \sum_{i=1}^{r} c_{j,i} X^{j-d_i} f_i(X)$ とおくと，$\operatorname{ord}_X \big(f(X) - g_j(X)\big) > \operatorname{ord}_X \big(f(X) - g_{j-1}(X)\big) \geqq j$ となる．この操作を繰り返して $c_{j,i} \in R$ を定め，$h_i(X) := \sum_{j=d}^{\infty} c_{j,i} X^{j-k}$ とおけば，$f(X) := \sum_{i=1}^{r} h_i(X) f_i(X)$ となる． □

参考. R が UFD ならば $R[[X]]$ も UFD である，という命題は，証明されていないし，恐らく正しくない (例えば，R が体上の無限変数多項式環の場合)．しかし，K が体のとき $K[[X_1, \ldots, X_n]]$ は UFD である，という命題は正しい．これは，正則局所環は UFD である，という定理を経由して証明するのが簡明であるが，この講義の範囲を超えている．

命題 11.8. $(R, \mathfrak{m})$ がネーター局所環ならば，$\widehat{R} = \varprojlim_n R/\mathfrak{m}^n$ もネーター局所環である．

証明. $\mathfrak{m} = (a_1, \ldots, a_r)$ と書ける．$S = R[X_1, \ldots, X_r]$, $T = R[[X_1, \ldots, X_r]]$, $\mathfrak{a} = (X_1 - a_1, \ldots, X_r - a_r) \subset S$, $\mathfrak{b} = (X_1 - a_1, \ldots, X_r - a_r) \subset T$ とおく．$S/\mathfrak{a} \cong R$ である．$\mathfrak{n} = (X_1, \ldots, X_r) \subset S$ とするとき，$S/\mathfrak{n}^n \twoheadrightarrow S/(\mathfrak{n}^n + \mathfrak{a}) \cong R/\mathfrak{m}^n$ だから，自然な全射 $\varphi : \varprojlim_n S/\mathfrak{n}^n \longrightarrow \varprojlim_n R/\mathfrak{m}^n$ が存在する．つまり，全射 $\varphi\colon T \to \widehat{R}$ が存在する．T がネーター環なので，$\widehat{R}$ もネーター環である．なお，$\operatorname{Ker} \varphi = \mathfrak{b}$ である． □

$\mathbb{Z}_p$ の元を具体的に表示する方法を考える．$f_{\infty n}\colon \mathbb{Z}_p \longrightarrow \mathbb{Z}/(p^n)$ は自然な全射とする．$x \in \mathbb{Z}_p$ を取る．$x_n = f_{\infty n}(x)$ とおく．x_n は $y_n = \sum_{i=0}^{n-1} a_{n,i} p^i \in \mathbb{Z}$ $(a_{n,i} \in \{0, 1, \ldots, p-1\})$ の p^n を法とする同値類であるとする．$m > n$ のとき $f_{mn}(x_m) = x_n$ だから，$m > n > i$ のとき，$a_{m,i} = a_{n,i}$ である．そこで，$a_i = a_{n,i}$ $(n > i)$ とおく．この $a_i \in \{0, 1, \ldots, p-1\}$ は x から一意的に定まる．そこで $x = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ と表示する．

例えば，$x=-1\in Z\subset\mathbb{Z}_p$ のとき，$a_0=a_1=a_2=\cdots=p-1$ であり，$-1=\sum_{i=0}^{\infty}(p-1)p^i$ である．このことから，$\mathbb{Z}_p$ では「正負」の概念は定義できないことがわかる．

R が整域でも $\widehat{R}$ は整域とは限らない．(例えば，$R=\mathbb{C}[X,Y]/(Y^2-X^2(X+1))$, $\mathfrak{m}=(X,Y)$.) 特に，R が UFD でも $\widehat{R}$ は UFD とは限らない．

命題 11.9. (1) $\mathbb{Z}_p$ は $p\mathbb{Z}_p$ を唯一の極大イデアルとする局所環である．
(2) $\mathbb{Z}_p$ は整域である．
(3) $\mathbb{Z}_p$ は PID である．

証明. (1) $\mathfrak{p}=p\mathbb{Z}$ とし $\mathfrak{p}$ による $\mathbb{Z}$ の局所化を $S=\mathbb{Z}_{\mathfrak{p}}$ とおく．$\mathbb{Z}/p^n\mathbb{Z}\cong S/p^nS$ なので，$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}\cong\varprojlim_n S/p^nS$ である．よって，前命題より，$\mathbb{Z}_p$ はネーター局所環である．

(2) 系 10.3 より，$\bigcap_{n\in\mathbb{N}} p^n\mathbb{Z}_p=(0)$ である．よって，$0\neq x\in\mathbb{Z}_p$ に対し，$x\in p^n\mathbb{Z}_p$, $x\notin p^{n+1}\mathbb{Z}_p$ を満たす $n\in\mathbb{N}\cup\{0\}$ が存在する．この n を $n=\mathrm{ord}_p\,x$ と書く．これは，$\mathbb{Z}$ の元についての ord_p の定義と一致する．

$\mathbb{Z}_p$ は $p\mathbb{Z}_p$ を唯一の極大イデアルとする局所環だから，$\mathrm{ord}_p\,x=0$ ならば $x^{-1}\in\mathbb{Z}_p$ が存在する．$\mathrm{ord}_p\,x=n$ のとき，$x\in p^n\mathbb{Z}_p$ だから $x=p^ny$ を満たす $y\in\mathbb{Z}_p$ が存在し，$\mathrm{ord}_p\,y=0$ である．よって，$p^n=y^{-1}x$ である．これより，$x\mathbb{Z}_p=p^n\mathbb{Z}_p$ である．特に，$x,\,y\in\mathbb{Z}_p-\{0\}$ に対し $\mathrm{ord}_p(xy)=\mathrm{ord}_p\,x+\mathrm{ord}_p\,y$ が成り立ち，$xy\neq0$ である．

(3) 上の議論から，$\mathbb{Z}_p$ のイデアルは，(0), $\mathbb{Z}_p$ 以外には，$p^n\mathbb{Z}$ $(n\in\mathbb{N})$ しか存在しない．これらは，すべて単項イデアルである． □

$p,\,q\in\mathbb{N}$ を相異なる素数とし，$a=pq$ とする．このとき，射影的極限 $\varprojlim_n \mathbb{Z}/a^n\mathbb{Z}$ は整域にならない．

定義 11.10. $\mathbb{Z}_p$ の分数体を

$$\mathbb{Q}_p=Q(\mathbb{Z}_p)=\left\{\frac{x}{y}\;\middle|\;x,\,y\in\mathbb{Z}_p,\,y\neq0\right\}$$

と書き，p-**進数体**という．$\mathbb{Z}\subset\mathbb{Z}_p$ だから，$\mathbb{Q}\subset\mathbb{Q}_p$ である．ただし，$\mathbb{Z}_p\not\subset\mathbb{C}$ だから $\mathbb{Q}_p\not\subset\mathbb{C}$ である．

$\mathbb{Q}_p$ の元を具体的に表示する方法を考える．$x=a/b\in\mathbb{Q}_p$ $(a,\,b\in\mathbb{Z}_p)$ を取る．上の (2) の証明のように，$\mathrm{ord}_p\,b=n$ とすると，$\mathrm{ord}_p\,c=0$ であるような $c\in\mathbb{Z}_p$ が存在して，$b=p^nc$ と書ける．$c^{-1}\in\mathbb{Z}_p$ が存在するから，$x=(ac^{-1})/p^n$ と書ける．$ac^{-1}\in\mathbb{Z}_p$ だから，$x=\sum_{i=-n}^{\infty}a_ip^i$, $a_i\in\{0,\,1,\ldots,\,p-1\}$ と一意的に表すことができる．

命題 11.11. p を素数とし，$\mathbb{Z}$ の極大イデアル $(p)=p\mathbb{Z}$ による局所化を $\mathbb{Z}_{(p)}$ とする．すると
(1) 自然な単射 $\iota\colon\mathbb{Z}_{(p)}\to\mathbb{Z}_p$ が存在する．
(2) $\mathbb{Z}_{(p)}$ の $p\mathbb{Z}_{(p)}$ による完備化は $\mathbb{Z}_p$ と同型である．
(3) ι を通して $\mathbb{Z}\subset\mathbb{Z}_{(p)}\subset\mathbb{Z}_p\subset\mathbb{Q}_p$ と考えるとき，$\mathbb{Z}_p\cap\mathbb{Q}=\mathbb{Z}_{(p)}$ である．

証明. (1) $\mathbb{Z}_{(p)}$ の 0 でない元は y/x $(x,\,y\in\mathbb{Z}$ で，$\mathrm{GCD}(x,\,y)=1$, $\mathrm{GCD}(x,\,p)=1)$ と書ける．$\mathrm{GCD}(x,\,p^n)=1$ だから，x の $\mathbb{Z}/p^n\mathbb{Z}$ における像 x_n は逆元 y_n を持つ．

$m\leqq n$ のとき，自然な全射を $f_{nm}\colon\mathbb{Z}/p^n\mathbb{Z}\longrightarrow\mathbb{Z}/p^n\mathbb{Z}$ とするとき $f_{nm}(x_n)=x_m$ である．よって，$x_\infty=\varprojlim x_n\in\mathbb{Z}_p$ と $y_\infty=\varprojlim y_n\in\mathbb{Z}_p$ が存在する．$x_ny_n=1$ なので，$x_\infty y_\infty=1$ である．なお，$\mathbb{Z}\subset\mathbb{Z}_p$ と考えるとき，$x_\infty=x$ である．つまり，x は $\mathbb{Z}_p$ で可逆である．よって，$y/x\in\mathbb{Z}_p$ である．$y/x\in\mathbb{Z}_{(p)}$ に $y/x\in\mathbb{Z}_p$ を対応させることにより，自然な単射 $\iota\colon\mathbb{Z}_{(p)}\to\mathbb{Z}_p$ が得られる．

(2) $\mathbb{Z}/p^n\mathbb{Z}\cong\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ だから，$\mathbb{Z}_{(p)}$ に $p\mathbb{Z}_{(p)}$ による完備化は $\mathbb{Z}$ の $p\mathbb{Z}$ による完備化と一致する．

(3) $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p \cap \mathbb{Q}$ は (1) からわかる．$\mathbb{Z}_{(p)} \supset \mathbb{Z}_p \cap \mathbb{Q}$ を示す．$z \in \mathbb{Z}_p \cap \mathbb{Q}$ は $\mathbb{Q}$ の元だから $z = y/x$ (x, $y \in \mathbb{Z}$, $\mathrm{GCD}(x, y) = 1$) と書ける．$z \in \mathbb{Z}_p$ だから $0 \leqq \mathrm{ord}_p\, z = \mathrm{ord}_p\, y - \mathrm{ord}_p\, x$ である．もし $\mathrm{ord}_p\, x > 0$ だと $\mathrm{GCD}(x, y) = 1$ だから $\mathrm{ord}_p\, y = 0$ で，$\mathrm{ord}_p\, z < 0$ となってしまう．よって，$\mathrm{ord}_p\, x = 0$ である．$x \notin p\mathbb{Z}$ だから $y/x \in \mathbb{Z}_{(p)}$ である．よって，$\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)}$ である． □

12. アルティン環

定義 12.1. R は可換環とする．R-加群 M が**アルティン加群** (Artinian module) であるとは，M の部分 R-加群 N_i の列 $N_1 \supset N_2 \supset N_3 \supset \cdots$ があれば，ある $n \in \mathbb{N}$ が存在して，$i \geqq n$ ならば $N_i = N_n$ となることをいう．

環 R が**アルティン環**であるとは，R を R-加群を考えたときアルティン加群であることをいう．つまり，R のイデアルの列 $I_1 \supset I_2 \supset I_3 \supset \cdots$ があれば，ある $n \in \mathbb{N}$ が存在して，$I_n = I_{n+1} = I_{n+2} = \cdots$ となることをいう．

補題 12.2. K は体，M は K-ベクトル空間とする．このとき，次の (1) 〜 (3) は同値．
(1) M は有限次元．
(2) M はネーター K-加群．
(3) M はアルティン K-加群．

証明. (1) $\Longrightarrow$ (2), (3) は自明．ネーター環上のネーター加群は有限生成なので，(2) $\Longrightarrow$ (1) が成り立つ．

(3) $\Longrightarrow$ (1) を示す．$\dim_K M = \infty$ と仮定し，X を M の基底とする．x_1, x_2,$\cdots \in X$ を取り，$X_n = X - \{x_1, \ldots, x_n\}$ とおく．X_n を基底とする M の部分ベクトル空間を M_n とすれば，$M_1 \supsetneqq M_2 \supsetneqq \cdots$ となる． □

定理 12.3. R はアルティン環とする．
(1) R が整域ならば R は体である．
(2) $\mathrm{Krull}\dim R = 0$ である．
(3) R は有限個の極大イデアルしか持たない．
(4) J を R のすべての極大イデアルの共通部分をとする．すると，ある $n \in \mathbb{N}$ が存在して $J^n = (0)$ となる．
(5) R はネーター環である．

証明. (1) $0 \neq a \in R$ を取る．$(a^n) \supset (a^{n+1}) \supset \cdots$ なので，ある $n \in \mathbb{N}$ が存在して，$(a^n) = (a^{n+1})$ となる．よって，$a^n \in (a^{n+1})$ なので，ある $b \in R$ により，$a^n = a^{n+1}b$ と書ける．R は整域なので，$1 = ab$ である．よって，$b = a^{-1} \in R$ となる．

(2) $\mathfrak{p} \subset R$ は素イデアルとする．$R/\mathfrak{p}$ もアルティン環であることは容易にわかる．(1) より $R/\mathfrak{p}$ は体で，$\mathfrak{p}$ は極大イデアルである．

(3) R が無限個の相異なる極大イデアル $\mathfrak{m}_1$, $\mathfrak{m}_2$,... を持ったとすると，$\mathfrak{m}_1 \supsetneqq \mathfrak{m}_1\mathfrak{m}_2 \supsetneqq \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supsetneqq \cdots$ という無限降鎖ができ，矛盾する．

(4) ある $n_0 \in \mathbb{N}$ が存在して $n \geqq n_0$ ならば $J^n = J^{n_0}$ となる．$J_0 = J^{n_0}$ とおく．$J_0 \neq (0)$ と仮定して矛盾を導く．$IJ_0 \neq (0)$ を満たす R のイデアル I 全体の集合 Λ を考える．R はアルティン環だから Λ には包含関係に関する極小元 I_0 が存在する．$I_0J_0 \neq (0)$ なので $aJ_0 \neq (0)$ を満たす $a \in I_0$ が存在する．$aJ_0^2 = aJ_0 \neq (0)$ なので，$abJ_0 \neq (0)$ となる $b \in J_0$ が存在する．I_0 の極小性から $(ab) = I_0 = (a)$ でなければならない．すると，$a = abc$ を満たす $c \in R$ が存在する．$x = bc$ とおくと $x \in J_0$ である．$a = ax = (ax)x = ax^2 = \cdots = ax^m$ $(\forall m \in \mathbb{N})$ である．ところで，$\sqrt{0} = J$ であるので，ある $m \in \mathbb{N}$ が存在して $x^m = 0$ となる．よって，$a = 0$ となり，矛盾する．

(5) $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_r$ は，相異なるとは限らない R の極大イデアルとし，$M_i = \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_{i-1}$ $(M_1 = R)$ とおく．(4) より，$M_r = 0$ となるように極大イデアルを選んでおくことができる．$M_i \supset M_{i+1}$ で，M_i はアルティン R-加群である．よって，M_i/M_{i+i} もアルティン R-加群である．$\mathfrak{m}_i(M_i/M_{i+1}) = (\mathfrak{m}_iM_i)/M_{i+1} = 0$ だから，M_i/M_{i+i} もアルティン $R/\mathfrak{m}_i$-加群である．$K_i := R/\mathfrak{m}_i$ は体だから，補題より M_i/M_{i+i} はネーター R-加群である．したがって，$R = M_1/M_r$ もネーター R-加群である． □

定理 12.4. R がネーター環で $\operatorname{Krull\,dim} R = 0$ であることと，R がアルティン環であることは，同値である．

証明. 前定理から，アルティン環はクルル次元 0 のネーター環である．

今，R はクルル次元 0 のネーター環とする．イデアル $(0) \subset R$ の準素イデアル分解 $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ を取る．$\mathfrak{m}_i = \sqrt{\mathfrak{q}_i}$ とおくと，$\operatorname{Krull\,dim} R = 0$ より素イデアル $\mathfrak{m}_i$ は極大イデアルである．$\mathfrak{m}_i$ は有限生成だから，ある $n \in \mathbb{N}$ に対して $\mathfrak{m}_i^n \subset \mathfrak{q}_i$ となる．$\operatorname{Krull\,dim} R = 0$ より，$i \neq j$ のとき $\mathfrak{m}_i^n + \mathfrak{m}_j^n = R$ となる．よって，$i \neq j$ のとき $\mathfrak{q}_i + \mathfrak{q}_j = R$ である．中国剰余定理より，$R = R/(0) \cong R/\mathfrak{q}_1 \oplus \cdots \oplus R/\mathfrak{q}_r$ となる．各 $R/\mathfrak{q}_i$ がアルティン環ならば R もアルティン環である．それには，$R/\mathfrak{m}_i^n$ がアルティン環であればよい．$S = R/\mathfrak{m}_i^n$, $\mathfrak{n} = \mathfrak{m}_i S$, $M_j = \mathfrak{n}^{j-1}/\mathfrak{n}^j$ (ただし $\mathfrak{n}^0 = S$) とおく．$M_n = 0$ である．$K = R/\mathfrak{m}_i$ とおくと，各 M_j はネーター K-加群なので，アルティン K-加群である．よって，S はアルティン環である． □

13. 整拡大

定義 13.1. R は整域，$K = Q(R)$ は R の分数体, L は K を含む体とする．$z \in L$ に対し，ある自然数 n と $a_0, a_1, \ldots, a_{n-1} \in R$ が存在して

$$z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \cdots + a_2 z^2 + a_1 z + a_0 = 0 \qquad ①$$

を満たすとき，z は R 上**整** (integral) であると言う．$z \in R$ ならば z は R 上整である ($n = 1, a_0 = -z \in R$ とすればよい)．特に，R が体のとき，R 上整な元を R 上**代数的** (algebraic) と言い，R 上代数的でない元を R 上**超越的** (transcendental) と言う．R 上整な元 z に対し，① を満たす R 上のモニック多項式のうち，2 つの 1 次以上の R 上のモニック多項式の積に表せない多項式を x の R 上の**最小多項式**と呼ぶことにする．例えば，R が UFD であれば z の最小多項式は一意的に定まるが，一般の整域 R では z の最小多項式は必ずしも一意的でないことに注意する．

R を含む整域 S の各元が R 上整であるとき，S は R 上**整**であるとか，S は R の**整拡大** (integral extension) である言う．特に，R, S が体で，S が R 上整のとき，S は R 上**代数的**であるとか，S は R の**代数拡大**であると言う．S が R 上代数的でないとき，S は R 上**超越的**であるとか，S は R の**超越拡大**であると言う．

$x_1, \ldots, x_n \in S$ に対し，R-多元環として $R[X_1, \ldots, X_n] \cong R[x_1, \ldots, x_n]$ (左辺は多項式環) であるとき，$x_1, \ldots, x_n$ は R 上**代数的独立**であると言い，代数的独立でないとき**代数的従属**であると言う．

命題 13.2. 上の定義と同じ記号を用いる．$z \in L$ とする．
(1) $M \neq 0$ が $R[z]$-加群で，R-加群として有限生成ならば，z は R 上整である．
(2) z が R 上整であるための必要十分条件は，$R[z]$ が有限生成 R-加群であることである．

証明. (1) $M = Rx_1 + \cdots + Rx_n$ とする．M は $R[z]$-加群だから，$zx_i \in M$ であり

$$zx_i = \sum_{j=1}^{n} a_{ij} x_j \quad (a_{ij} \in R)$$

と書ける．a_{ij} を (i, j)-成分とする n 次正方行列を A, n 次の単位行列を I, $f(z) = \det(zI - A)$ とおくと，体 $Q(R[z])$ の元を成分とする行列とベクトルとして，連立方程式 $(zI - A)\mathbf{x} = \mathbf{0}$ がゼロベクトル以外の解を持つから，$f(z) = 0$ である．$f(z)$ は z^n の係数が 1 の，z についての n 次多項式だから，z は R 上整である．

(2) z が R 上整ならば ① を満たすから，逆に，$R[z]$ が有限生成 R-加群ならば，(1) を $M = R[z]$ として用いれば z は R 上整となる． □

命題 13.3. 定義 13.1 と同じ記号を用いる．
(1) $z \in L$ が R 上整で，$w \in L$ が $R[z]$ 上整ならば，w は R 上整である．
(2) $x, y \in L$ が R 上整ならば，$x + y$, xy も R 上整である．
(3) R が体で，$0 \neq x \in L$ が R 上代数的ならば，$1/x$ は R 上代数的である．
(4) S が R の整拡大ならば，$Q(S)$ は $Q(R)$ の代数拡大である．

(5) 整域 S が体 R 上整ならば S は体である．

証明. (1) $w \in L$ が $R[z]$ 上整ならば，$(R[z])[w] = R[z, w]$ も有限生成 R-加群だから，w は R 上整である．

(2) $R[x, y]$ は有限生成 R-加群だから，$x + y$, xy は R 上整である．

(3) x が R 上代数的ならば，$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ $(a_i \in R)$ と書ける．$a_0 \neq 0$ と仮定してよい．すると，

$$\frac{1}{x^n} + \frac{a_1}{a_0} \cdot \frac{1}{x^{n-1}} + \cdots + \frac{a_{n-1}}{a_0} \cdot \frac{1}{x} + \frac{1}{a_0} = 0$$

なので，$1/x$ は R 上代数的である．

(4) は明らかである．

(5) $x \in S$ が (3) の証明のように表せるとき，

$$\frac{1}{x} = -\frac{1}{a_0}(x^{n-1} + a_{n-1}x^{n-1} + \cdots + a_2x + a_1) \in S$$

なので，S は体である． □

定義 13.4. 定義 13.1 と同じ記号を使う．前命題より，

$$R'_L := \left\{ x \in L \;\middle|\; x \text{ は } R \text{ 上整} \right\}$$

とおくと，R'_L は整域になる．R'_L を L における R の**整閉包**という．$R'_K = R$ が成り立つとき，R は**整閉** (integrally closed) であるという．R がネーター整域であって整閉であるとき，R は**正規環**であるという．

補題 13.5. R, S は可換環で，$R \subset S$ とする．このとき，S の素イデアル $\mathfrak{q}$ に対し，$\mathfrak{p} = \mathfrak{q} \cap R$ は R の素イデアルである．

証明. $x, y \in R$, $xy \in \mathfrak{p} \subset \mathfrak{q}$ ならば，$x \in \mathfrak{q}$ または $y \in \mathfrak{q}$ だから，$x \in \mathfrak{p}$ または $y \in \mathfrak{p}$ となる． □

定理 13.6.(Lying-over Theorem) R, S はネーター整域で，$R \subset S$ かつ S は R 上整とする．このとき，R の素イデアル $\mathfrak{p}$ に対し，$\mathfrak{q} \cap R = \mathfrak{p}$ となる S の素イデアル $\mathfrak{q}$ が存在する．また，R の素イデアル列 $\mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_r$ に対し，S の素イデアル列 $\mathfrak{q}_0 \supsetneqq \mathfrak{q}_1 \supsetneqq \cdots \supsetneqq \mathfrak{q}_r$ で，$\mathfrak{q}_i \cap R = \mathfrak{p}_i$ を満たすものが存在する．

特に，$\operatorname{Krull\,dim} S = \operatorname{Krull\,dim} R$ である．

証明. まず，$\mathfrak{p}$ が R の極大イデアルの場合を考える．$\mathfrak{p}S \neq S$ であることを示す．もし $\mathfrak{p}S = S$ ならば，$1 = p_1s_1 + \cdots + p_ks_k$ $(p_i \in \mathfrak{p},\ s_i \in S)$ と書ける．$S' = R[s_1, \ldots, s_k]$ は有限生成 R-加群で，$S' = Rx_1 + \cdots + Rx_n$ $(x_1 = 1)$ と表せば，$S' = \mathfrak{p}S'$ より，$x_i = \sum_{j=1}^{n} a_{ij}x_j$ $(a_{ij} \in \mathfrak{p})$ と表せる．a_{ij} を (i, j)-成分とする n 次正方行列を A とし，I を単位行列として，$b = \det(I - A) \in 1 + \mathfrak{p}$ とすれば，$bx_i = 0$ より $b = 0$ となり矛盾する．したがって，$\mathfrak{p}S \neq S$ である．

S における $\mathfrak{p}S$ の準素イデアル分解 $\mathfrak{p}S = J_1 \cap \cdots \cap J_m$ を取る．$I = \sqrt{J_1} \cap R$ とおけば，I は R の素イデアルで，$I \supset \mathfrak{p}$ である．$\mathfrak{p}$ は極大イデアルだから，$I = \mathfrak{p}$ である．そこで，$\mathfrak{q} = \sqrt{J_1}$ とおく．$S/\mathfrak{q}$ は $R/\mathfrak{p}$ 上整なので体であり，$\mathfrak{q}$ は極大イデアルである．そして，$\mathfrak{q} \cap R = \mathfrak{p}$ を満たす．

$\mathfrak{p}$ が R の素イデアルの場合は，$S_{\mathfrak{p}} = \{x/y \in Q(S) \mid x \in S, y \in R - \mathfrak{p}\}$ とおくと，$S_{\mathfrak{p}}$ は $R_{\mathfrak{p}}$ の整拡大である．$\mathfrak{p}R_{\mathfrak{p}}$ は $R_{\mathfrak{p}}$ の極大イデアルなので，上の議論から $S_{\mathfrak{p}}$ の極大イデアル $\tilde{\mathfrak{q}}$ で $\tilde{\mathfrak{q}} \cap R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ を満たすものが存在する．そこで，$\mathfrak{q} = \tilde{\mathfrak{q}} \cap S$ とおけば，$\mathfrak{q} \cap R = \mathfrak{p}R_{\mathfrak{p}} \cap R = \mathfrak{p}$ である．

さて，R の素イデアル列 $\mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_r$ に対し，S の素イデアル列 $\mathfrak{q}_1 \supsetneqq \mathfrak{q}_2 \supsetneqq \cdots \supsetneqq \mathfrak{q}_r$ で $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ $(1 \leqq i \leqq r)$ を満たすものが存在することを帰納法の仮定として，$\mathfrak{q}_0$ の存在を証明する．$\overline{S} = S/\mathfrak{q}_1$ は $\overline{R} = R/\mathfrak{p}_1$ の整拡大である．上の議論から，$\overline{S}$ の素イデアル $\overline{\mathfrak{q}}$ で，$\overline{\mathfrak{q}} \cap \overline{R} = \mathfrak{p}_0/\mathfrak{p}_1$ を満たすものが存在する．そこで，自然な全射 $S \to \overline{S}$ による $\overline{\mathfrak{q}}$ の原像を $\mathfrak{q}_0 \subset S$ とすれば，$\mathfrak{q}_0 \cap R = \mathfrak{p}_0$, $\mathfrak{q}_0 \supsetneqq \mathfrak{q}_1$ となる．これより，$\operatorname{Krull\,dim} R \leqq \operatorname{Krull\,dim} S$ がわかる．

また，$\mathfrak{q}_0 \supsetneqq \mathfrak{q}_1 \supsetneqq \cdots \supsetneqq \mathfrak{q}_r$ が S の素イデアル列のとき，$\mathfrak{q}_0 \cap R \supset \mathfrak{q}_1 \cap R \supset \cdots \supset \mathfrak{q}_r \cap R$ は R の素イデアル列であり，上の議論から，もし $\mathfrak{q}_i \cap R = \mathfrak{q}_{i+1} \cap R$ ならば $\mathfrak{q}_i = \mathfrak{q}_{i+1}$ である．よって，$\operatorname{Krull\,dim} S \leqq \operatorname{Krull\,dim} R$ である． □

補題 13.7. (1) K は体で無限個の要素を持つとする．$f \in K[X_1,\ldots, X_n] - K$ ならば，$c_2,\ldots, c_n \in K$ をうまく選んで，$Y_i = X_i + c_iX_1$ $(2 \leqq i \leqq n)$ とおくと，$K[X_1,\ldots, X_n]$ は $K[f, Y_2,\ldots, Y_n]$ 上整になる．

(2) K は標数 p の有限体とする．$f \in K[X_1,\ldots, X_n] - K$ ならば，$m_2,\ldots, m_n \in \mathbb{N}$ をうまく選んで，$Y_i = X_i + X_1^{pm_i}$ $(2 \leqq i \leqq n)$ とおくと，$K[X_1,\ldots, X_n]$ は $K[f, Y_2,\ldots, Y_n]$ 上整になる．

証明. (1) f の $X_1,\ldots, X_n$ について i 次の部分を f_i として，$f = f_d + f_{d-1} + \cdots + f_0$ $(f_d \neq 0)$ とする．今，$f_d(1, -c_2, -c_3,\ldots, -c_n) \neq 0$ となるように，$c_2,\ldots, c_n \in K$ を選んでおく．すると，f を X_1, $Y_2,\ldots, Y_n$ $(Y_i = X_i + c_iX_1)$ の多項式で表し，

$$f = \sum_{i=0}^{d} g_i(Y_2,\ldots,Y_n)\cdot X_1^i$$

としたとき，$g_d \in K$ かつ $g_d = f_d(1, -c_2,\ldots, -c_n) \neq 0$ となる．上の等式を定数 g_d で割ると

$$X_1^d + \sum_{i=0}^{d-1} \frac{g_i(Y_2,\ldots,Y_n)}{g_d}\cdot X^i - \frac{f}{g_d} = 0$$

という $K[f, Y_2,\ldots, Y_n]$ 上の X_1 に関するモニック多項式が得られるので，X_1 は $K[f, Y_2,\ldots, Y_n]$ 上整である．

$2 \leqq i \leqq n$ に対し，$X_i = Y_i - c_iX_1$ も $K[f, Y_2,\ldots, Y_n]$ 上整であるから，$K[X_1,\ldots, X_n]$ は $K[f, Y_2,\ldots, Y_n]$ 上整である．

(2) の証明は，永田雅宜「可換環論」p.104 を見よ． □

定理 13.8. K は体，I は多項式環 $S = K[X_1,\ldots, X_n]$ の高さ r の素イデアルとする．すると，ある K 上代数的独立な $f_1,\ldots, f_n \in S$ が存在し，

(1) S は $R = K[f_1,\ldots, f_n]$ 上整．

(2) $I \cap R = \sum_{i=1}^{r} Rf_i$.

が成り立つようにできる．

証明. r に関する帰納法で証明する．$r = 0$ のときは $I = (0)$ だから主張は自明である．

$r \geqq 1$ とし，高さが r 未満のイデアルについては主張は正しいと仮定する．$J \subset I$ で $\operatorname{ht} J = r-1$ を満たす素イデアル J を取る．帰納法の仮定から，代数的独立な $Y_1,\ldots, Y_n \in S$ が存在し，S は $R' = K[Y_1,\ldots, Y_n]$ 上整，かつ，$J \cap R' = \sum_{i=1}^{r-1} R'Y_i$ を満たす．

Lying-over Theorem より $\operatorname{ht}(I \cap R') = r$ である．$Y_1,\ldots, Y_{r-1} \in J \cap R' \subset I$ に注意する．$0 \neq f_r \in I \cap K[Y_r, Y_{r+1},\ldots, Y_n]$ を取る．前補題から，ある $f_i = Y_i + c_iY_r$ または $f_i = Y_i + Y_r^{pm_i}$ $(r+1 \leqq i \leqq n)$ が存在し，$K[Y_r,\ldots, Y_n]$ は $K[f_r, f_{r+1},\ldots, f_n]$ 上整になる．$f_1 = Y_1,\ldots, f_{r-1} = Y_{r-1}$ とおけば，S は R' 上整，R' は $R = K[f_1,\ldots, f_n]$ 上整だから，S は R 上整になる．

また，$I \cap R$, $(f_1,\ldots, f_r) \subset R$ はいずれも素イデアルで，$\operatorname{ht}(I \cap R) = r = \operatorname{ht}(f_1,\ldots, f_r)$ だから，$I \cap R = (f_1,\ldots, f_r)$ である．構成の方法から，$f_{r+1},\ldots, f_n$ は $K(Y_1,\ldots, Y_r)$ 上代数的独立だから，$f_1,\ldots, f_n \in S$ は K 上代数的独立である． □

定理 13.9.(正規化定理) R が体 K 上有限生成な整域ならば，K 上代数的独立なある $x_1,\ldots, x_m \in R$ を選んで，R が $K[x_1,\ldots, x_m]$ 上整であるようにできる．

証明. $R = S/I$ のとき，前の定理の $f_{r+1},\ldots, f_n$ の I を法とする同値類を $x_1,\ldots, x_m$ とおけばよい． □

定義 13.10.(超越次数) 体 K を含む体 L が，K 上代数的に独立な d 個の超越元を含み，L 内のどの $d+1$ 個の元も代数的従属のとき，$d = \mathrm{tr.deg}_K L$ と書き，K 上の**超越次数**と言う．また，$d = \mathrm{tr.deg}_K L < +\infty$ で，K 上代数的独立なある元 $x_1,\ldots, x_d \in L$ が存在し，L が有理関数体 $K(x_1,\ldots, x_d)$ の有限次代数拡大体である場合，L は K 上**有限生成**な体であると言う．正規化定理により，これは，L が K 上有限生成なある整域の分数体であることと同値である．

定理 13.11. R が体 K 上有限生成な整域で，

$$\mathfrak{p}_d \supsetneqq \mathfrak{p}_{d-1} \supsetneqq \mathfrak{p}_{d-2} \supsetneqq \cdots \supsetneqq \mathfrak{p}_1 \supsetneqq \mathfrak{p}_0 = (0)$$

が細分できない R の素イデアル列で，$\mathfrak{p}_d$ が極大イデアルであれば，

$$\mathrm{Krull\,dim}\, R = \mathrm{tr.deg}_K Q(R) = d$$

である．

証明. $\mathrm{tr.deg}_K Q(R) = d$ を d に関する帰納法で証明する．$d = 0$ のとき，(0) が極大イデアルだから R は体で，$R = Q(R)$ は K の代数拡大で，$\mathrm{tr.deg}_K Q(R) = 0$ である．

$d \geqq 1$ とする．前の系と定理 13.8 より，K 上代数的独立な $x_1,\ldots, x_m \in R$ を選んで，R が $S = K[x_1,\ldots, x_m]$ 上整かつ，$\mathfrak{p}_1 \cap S = Sx_1$ となるようにできる．

$S' = S/(\mathfrak{p}_1 \cap S) \cong K[x_2, x_3,\ldots, x_m]$ とおく．準同型定理より，$S' = S/(\mathfrak{p}_1 \cap S) \subset R/\mathfrak{p}_1$ とみなせ，$R/\mathfrak{p}_1$ は S' 上整である．

$R/\mathfrak{p}_1$ と S' に対して帰納法の仮定を適用して，$\mathrm{tr.deg}_K Q(S') = d-1$ を得る．これより，$\mathrm{tr.deg}_K Q(R) = \mathrm{tr.deg}_K Q(S) = 1 + \mathrm{tr.deg}_K Q(S') = d$ を得る．

長さ d の素イデアル列が存在するから，$\mathrm{Krull\,dim}\, R \geqq d$ であるが，もし，$\mathrm{Krull\,dim}\, R > d$ とすると，長さ $d+1$ 以上の素イデアル列が存在し，上の結果から，$\mathrm{tr.deg}_K Q(R) \geqq d+1$ となって矛盾する．したがって，$\mathrm{Krull\,dim}\, R = d$ である． □

系 13.12. R が体 K 上有限生成な整域，I が R の素イデアルのとき，

$$\mathrm{ht}\, I + \mathrm{coht}\, I = \mathrm{Krull\,dim}\, R$$

である．

系 13.13. K が体のとき，$\mathrm{Krull\,dim}\, K[X_1,\ldots, X_n] = n$ である．

証明. $\mathrm{Krull\,dim}\, K[X_1,\ldots, X_n] = \mathrm{tr.deg}_K K(X_1,\ldots, X_n) = n$ である． □

問 13.14. UFD は整閉であることを示せ．

問 13.15. $\mathbb{C}[X,Y]/(X^2 - Y^3) \cong \mathbb{C}[T^2, T^3]$ で，これは整閉でない整域であることを示せ．

14. 離散付値環

定義 14.1. R は可換環，M は R-加群，$X \subset M$ とする．

$$\mathrm{ann}(X) = \left\{ a \in R \;\middle|\; \text{任意の } x \in X \text{ に対して } ax = 0 \right\}$$

と書き，$\mathrm{ann}(X)$ を X の **annihilator** という．$X = \{x\}$ のときは，$\mathrm{ann}(X)$ を $\mathrm{ann}(x)$ とも書く．

R の素イデアル $\mathfrak{p}$ が，ある $x \in M$ により $\mathfrak{p} = \mathrm{ann}(x)$ と表せるとき，$\mathfrak{p}$ は M の**素因子**であるという．M の素因子全体の集合を $\mathrm{Ass}\, M$ とか $\mathrm{Ass}_R M$ と書く．

命題 14.2. R はネーター環，$M \neq 0$ は R-加群とする．このとき，$\mathrm{Ass}_R M \neq \emptyset$ である．

証明. $\mathcal{A} = \left\{ \mathrm{ann}(x) \;\middle|\; 0 \neq n \in M \right\}$ とおく．包含関係について $\mathcal{A}$ は帰納的順序集合になるので，極大元 $I = \mathrm{ann}(x_0) \in \mathcal{A}$ が存在する．もし，I が素イデアルでなければ，$a, b \notin I, ab \in I$ となる $a, b \in R$ が存在する．$a \notin I$ より，$ax_0 \neq 0$ である．ann の定義から $\mathrm{ann}(ax_0) \supset \mathrm{ann}(x_0)$ であるが，$b \in \mathrm{ann}(ax_0)$ な

ので，$\mathrm{ann}(ax_0) \supsetneqq \mathrm{ann}(x_0)$ となり，$\mathrm{ann}(x_0)$ の極大性に反する．よって，I は素イデアルで，$I \in \mathrm{Ass}_R M$ である． □

問 14.3. R は可換環とする．以下を示せ．
(1) $0 \to L \to M \to N \to 0$ が R-加群の完全系列のとき，$\mathrm{Ass}_R L \subset \mathrm{Ass}_R M \subset \mathrm{Ass}_R L \cup \mathrm{Ass}_R N$.
(2) M が有限生成 R-加群ならば，$\mathrm{Ass}_R M$ は有限集合である．

定義 14.4. $(R, \mathfrak{m})$ がクルル次元 1 の整閉なネーター局所整域のとき，**離散付値環** (Discrete Valuation Ring) と言い，略して **DVR** と言う.「付値」は「附値」とも書く．

定理 14.5. $(R, \mathfrak{m})$ は DVR とする．このとき，以下が成り立つ．
(1) R は PID である．
(2) I が R のイデアルで $I \neq (0)$ ならば，ある $n \in \mathbb{N}$ が存在して $I = \mathfrak{m}^n$ と書ける．

証明. (1-i) $\mathfrak{m}$ が単項であることを示す．勝手な $0 \neq a \in \mathfrak{m}$ を取る．$R/aR \neq 0$ なので，$\mathrm{Ass}_R(R/aR) \neq \emptyset$ である．任意の $y \in R/aR$ に対し $a \in \mathrm{ann}(y)$ なので，$(0) \notin \mathrm{Ass}_R(R/aR)$ である．R の素イデアルは (0) と $\mathfrak{m}$ しか存在しないので，$\mathrm{Ass}_R(R/aR) = \{\mathfrak{m}\}$ である．よって，ある $b \in R - aR$ により $\mathfrak{m} = \mathrm{ann}(\overline{b})$ と書ける．ここで，$\overline{b} \in R/aR$ は b の aR を法とする剰余類である．このとき，$b\mathfrak{m} \subset aR$ である．
$\mathfrak{m}$ が単項でないと仮定してみる．すると，$b\mathfrak{m} \neq aR$ である．$I \subsetneqq aR$ を満たすイデアル I は，あるイデアル J により $I = aJ$ と書け，$J \subsetneqq R$ を満たす．$\mathfrak{m}$ は極大イデアルだから，$J \subset \mathfrak{m}$ となり，$I \subset a\mathfrak{m}$ となる．このことと $b\mathfrak{m} \subsetneqq aR$ より，$b\mathfrak{m} \subset a\mathfrak{m}$ となる．よって，$\dfrac{b}{a}\mathfrak{m} \subset \mathfrak{m} \subset Q(R)$ で，命題 13.2(1) より，b/a は R 上整である．R は整閉なので，$b/a \in R$ となり，$b \in aR$ となって矛盾する．よって，$\mathfrak{m}$ は単項である．以下，$\mathfrak{m} = pR$ とする．
(2) $(0) \neq I \subsetneqq R$ をイデアルとする．$I \subset pR$ である．$I \subset p^{n_1}R$, $I \subset p^{n_1+1}R$ となる $n_1 \in \mathbb{N}$ を取る．
I の準素イデアル分解 $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ を取る．(0) でない R の素イデアルは $\mathfrak{m} = pR$ しか存在しないので，$\sqrt{\mathfrak{q}_i} = pR$ である．$\mathfrak{q}_i$ は準素イデアルなので，ある $n_i \in \mathbb{N}$ を取ると，$p^{n_i} \in \mathfrak{q}_i$ となる．よって，ある $n \in \mathbb{N}$ をとると $p^n \in I$ となる．$p^{n_2} \in I$, $p^{n_2-1} \notin I$ となる $n_2 \in \mathbb{N}$ を取る．
$p^{n_2}R \subset I \subset p^{n_1}R$. $n_2 \geqq n_1$ であるが，$n_2 > n_1$ と仮定してみる．I 元はすべて p^{n_1} の倍数なので，$J = (1/p^{n_1})I$ も R のイデアルになる．$p^{n_2-n_1} \in J$ なので $J \neq (0)$ である．$J \not\subset pR$ で R は局所環なので，$J = R$ となる．よって，$I = p^{n_1}R$ である．
(1-ii) R のイデアルは，(0) と (p^n) $(n \in \mathbb{N})$ しかなく，PID である． □

定義 14.6. $(R, \mathfrak{m})$ は DVR とする．$\mathfrak{m} = pR$ と書ける．$0 \neq a \in R$ に対し，$a \in \mathfrak{m}^n$, $a \notin \mathfrak{m}^{n+1}$ (ただし $\mathfrak{m}^0 = R$ とする) を満たす $n \in \mathbb{N} \cup \{0\}$ が一意的に定まる．この n を $\mathrm{ord}_p a$ とか $\mathrm{ord}_{\mathfrak{m}} a$ と書く．便宜的に，$\mathrm{ord}_p 0 = +\infty$ と約束する．
次に，$K = Q(R)$, $x = a/b \in K$ $(a, b \in R)$ とする．このとき，$\mathrm{ord}_p x = \mathrm{ord}_p a - \mathrm{ord}_p b$ により，分数 $x = a/b$ の選び方に依存せずに矛盾なく $\mathrm{ord}_p x$ の値が定まる (簡単なので，証明してみよ).
$\mathrm{ord}_p x$ を K, あるいは R の**付値**と言う．
多くの教科書では，付値 $\mathrm{ord}_p(x) = \nu(x)$ の存在から，付値体や付値環を定義するが，長くなるので，この講義では最短コースで話す．

例 14.7. (1) p 進整数環 $\mathbb{Z}_p$ は DVR である．
(2) p を素数，$\mathfrak{p} = p\mathbb{Z}$ とするとき，$\mathbb{Z}$ の $\mathfrak{p}$ による局所化 $\mathbb{Z}_{\mathfrak{p}}$ は DVR である．

例 14.8. K は体，$\mathfrak{p}$ は 1 変数多項式環 $S = K[X]$ の素イデアル，$R = S_{\mathfrak{p}}$ とおくと，R は DVR である．

参考 14.9. N が M の R-部分加群のとき．N が M の**準素部分加群**であるとは,「$a \in R$ に対し，$ax = 0$ を満たす $0 \neq x \in (M/N)$ が存在すれば，$a \in \sqrt{\mathrm{ann}(M/N)}$」が成り立つことをいう．$R$ のイデアル $\mathfrak{q}$ が，R の準素部分加群であるとき，$\mathfrak{q}$ は R の**準素イデアル**であるという．準素イデアル分解の一般化として，次の準素加群分解が成立する．ただし，本講義の範囲を超えるので，証明はしない．

定理 14.10.(準素加群分解) R はネーター可換環，$0 \neq M$ は有限生成 R-加群，$N \subsetneqq M$ は R-部分加群とする．

(1) $\mathrm{Ass}(M/N)$ は空でない有限集合であって，$\mathrm{Ass}(M/N)$ の極小元全体の集合は，

$$\mathrm{Supp}(M/N) := \left\{ \mathfrak{p} \;\middle|\; \mathfrak{p} \text{ は } R \text{ の素イデアルで，} R_{\mathfrak{p}} \otimes_R M \neq 0 \right\}$$

の極小元全体の集合と一致する．

(2) $\mathrm{Ass}(M/N) = \left\{ \mathfrak{p}_1, \ldots, \mathfrak{p}_r \right\}$ とおくとき，M の準素部分加群 $N_1, \ldots, N_r$ が存在して，

$$N = N_1 \cap \cdots \cap N_r, \quad \mathrm{ann}(M/N_i) = \mathfrak{p}_i, \quad \mathrm{Ass}(M/N_i) = \left\{ \mathfrak{p}_i \right\}$$

$(i = 1, \ldots, r)$ を満たす．これを N の**準素 (加群) 分解**という．ただし，$N_1, \ldots, N_r$ は一意的とは限らない．

15. デデキンド 環と幾何学的環

定義 15.1.(分数イデアル) R は整域，$K = Q(R)$ とする．$I \subset K$ が R-部分加群で，ある $0 \neq a \in R$ により $aI \subset R$ となるとき，I は**分数イデアル**であるという．

$I, J \subset K$ が分数イデアルのとき，$\left\{ xy \in K \;\middle|\; x \in I, y \in J \right\}$ を含む最小の分数イデアルを IJ と書き，I と J の**積**という．

定義 15.2.(デデキンド 環) クルル次元 1 の整閉なネーター環を**デデキンド 環**とか **Dedekind 環**という．

定理 15.3. R はデデキンド 環，$(0) \neq I$ は R の分数イデアルとする．すると，$IJ = R$ となるような分数イデアル J が存在する．したがって，(0) でない R の分数イデアル全体の集合は，積に関して群になる．

証明. $J = \left\{ y \in Q(R) \;\middle|\; yI \subset R \right\}$ とおく．定義から，$IJ \subset R$ である．もし，$IJ \subsetneqq R$ ならば IJ を含む極大イデアル $\mathfrak{m} \subset R$ が存在する．$R_{\mathfrak{m}}$ は DVR である．$\mathfrak{m} = pR_{\mathfrak{m}}$ と書けるので，$IR_{\mathfrak{m}} = p^n R_{\mathfrak{m}}$ $(\exists n \in \mathbb{Z})$ と書ける．

$p^n = q/s$ $(q \in R,\ s \in R - \mathfrak{m})$ と書ける．適当に $s \in R - \mathfrak{m}$ を選び直せば，$q = p^n s \in I$ である．$p^{-n} q^n = s^n \in R$ なので，$p^{-n} \in J$ である．よって，$IJR_{\mathfrak{m}} = R_{\mathfrak{m}}$ である．これは，$IJR_{\mathfrak{m}} \subset \mathfrak{m}R_{\mathfrak{m}}$ と矛盾する．よって，$IJ = R$ である． □

問 15.4. R がデデキンド 環ならば，R の (0) でも R でもないイデアル I は，有限個の極大イデアルイデアルの積に表せることを証明せよ．

参考 15.5. K は $\mathbb{Q}$ の有限次代数拡大体とする．$\mathbb{Z}$ 上整な K の元全体の集合を R をする．すると，R はデデキンド 環になる．この R を K の**整数環**という．

この命題は，R がネーター環であることの証明が少し面倒である．R がネーター環であることを認めると，定理 13.5 より，$\mathrm{Krull\,dim}\, R = \mathrm{Krull\,dim}\, \mathbb{Z} = 1$ であり，定義から R は整閉だからデデキンド 環であることがわかる．

定義 15.6. 体 K の代数拡大体が K 以外に存在しないとき，K は**代数閉体**であるという．K が代数閉体であることとと，1 次以上の任意の多項式 $f(X) \in K[X]$ が，$K[X]$ において 1 次式の積に因数分解できることは同値である．

代数学続論か複素関数論で学習すると思うが，$\mathbb{C}$ は代数閉体であることが知られている．

K を代数閉体とし，$S = K[X_1, X_2, \ldots, X_n]$ とする．S のイデアル I により $R = S/I$ と表せる環を，K 上の**幾何学的環**という．

定理 15.7. K は代数閉体とし，$S = K[X_1, X_2, \ldots, X_n]$ とする．すると，S の勝手な極大イデアル $\mathfrak{m}$ は，ある $a_1, a_2, \ldots, a_n \in K$ によって，

$$\mathfrak{m} = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$$

と表せる．

証明. $L = S/\mathfrak{m}$, $\psi\colon S \twoheadrightarrow S/\mathfrak{m} = L$ を自然な全射とする．定理 6.9 より，$\operatorname{coht}\mathfrak{m} = \operatorname{Krull\,dim} S/\mathfrak{m} = 0$ である．L は K 上 $\psi(X_1)$,..., $\psi(X_n)$ で生成される有限生成な整域である．定理 13.10 より，$0 = \operatorname{Krull\,dim} S/\mathfrak{m} = \operatorname{tr.deg}_K L$ なので，L は K の代数拡大体である．K は代数閉体なので $L = K$ である．

$a_i = \psi(X_i)$ とおき $\mathfrak{M} = (X_1 - a_1,\ldots, X_n - a_n)$ とおく．$\psi(X_i - a_i) = 0$ だから，$\mathfrak{M} \subset \operatorname{Ker}\psi = \mathfrak{m}$ である．$\mathfrak{M}$ は S の極大イデアルだから，$\mathfrak{M} = \mathfrak{m}$ である． □

定義 15.8. K は体，$S = K[X_1,\ldots, X_n]$, I は S のイデアルとする．このとき，

$$V(I) = \bigl\{(a_1,\ldots,a_n) \in K^n \bigm| \text{任意の } f \in I \text{ に対し } f(a_1,\ldots, a_n) = 0\bigr\}$$

と書くことにし，$V(I)$ を I を**定義イデアル**とする K^n 内の**代数的集合**という．

例えば，単項イデアル $I = (f)$ に対しては，$V(I)$ は $f(a_1,\ldots, a_n) = 0$ で定まる K^n の部分集合である．

定理 15.9. K は代数閉体とし，$S = K[X_1, X_2,\ldots, X_n]$, $R = S/I$ とする．$\psi\colon S \to R$ を自然な全射とし，$x_i = \psi(X_i)$ とおく．すると，R の勝手な極大イデアル $\mathfrak{m}$ は，ある $(a_1, a_2,\ldots, a_n) \in V(I)$ によって，

$$\mathfrak{m} = (x_1 - a_1,\, x_2 - a_2,\ldots,\, x_n - a_n)$$

と表せる．逆に $(a_1, a_2,\ldots, a_n) \in V(I)$ ならば，$(x_1 - a_1,\, x_2 - a_2,\ldots,\, x_n - a_n)$ は R の極大イデアルである．

証明. $\pi\colon S \to R$ を自然な全射とし，$\mathfrak{M} = \pi^{-1}\mathfrak{m}$ とする．準同型定理より，$R/\mathfrak{m} \cong S/\mathfrak{M} \cong K$ である．前定理より，ある $a_1,\ldots, a_n \in K$ により，$\mathfrak{M} = (X_1 - a_1,\ldots, X_n - a_n)$ と書ける．$\psi(\mathfrak{M}) = \mathfrak{m}$ で，$\psi(X_i) = x_i$, $\psi(a_i) = a_i$ だから，$\mathfrak{m} = (x_1 - a_1,\ldots, x_n - a_n)$ である．

$\mathbf{a} = (a_1,\ldots, a_n) \in K^n$ とする．$f \in \mathfrak{M}$ ならば $f(\mathbf{a}) = 0$ であることに注意する．もし，$\mathbf{a} \notin V(I)$ ならば，$f(\mathbf{a}) \neq 0$ を満たす $f \in I$ が存在し，$R \neq \mathfrak{M} \supsetneq I$ と矛盾する．よって，$\mathbf{a} \in V(I)$ である．

逆に，$\mathbf{a} \in V(I)$ ならば，$\mathfrak{m} = (x_1 - a_1,\ldots, x_n - a_n)$ とするとき，$\psi^{-1}(\mathfrak{m}) = (X_1 - a_1,\ldots, X_n - a_n)$ だから，$\mathfrak{m}$ は R の極大イデアルである． □

定理 15.10.(ヒルベルトの零点定理) K は代数閉体，$S = K[X_1,\ldots, X_n]$, I は S のイデアルとする．さらに，S/I は 0 以外の巾零元 (何乗かすると 0 になる元) を持たないと仮定する．このとき，もし，$f(X_1,\ldots, X_n) \in S$ が任意の $(a_1,\ldots, a_n) \in V(I)$ に対し $f(a_1,\ldots, a_n) = 0$ を満たせば，$f \in I$ である．

証明. $f \in S$ が任意の $(a_1,\ldots, a_n) \in V$ に対し $f(a_1,\ldots, a_n) = 0$ を満たすとする．$I = (f_1,\ldots, f_m)$ としておく．

$h = 1 - X_0 f \in S' = K[X_0,\, X_1,\ldots,\, X_n]$ とする．自然に $S = K[X_1,\, X_2,\ldots,\, X_n] \subset S'$ と考え，$J = IS' + hS$ とする．$V(J) = \emptyset$ を示す．

$(a_0, a_1,\ldots, a_n) \in V(J)$ であると仮定する．$V(J)$ の定義より，$1 - a_0 f(a_1,\ldots,a_n) = 0$ である．また，$I \subset J$ より，$(a_1,\ldots, a_n) \in V(I)$ である．したがって，$f(a_1,\ldots, a_n) = 0$ であるが，$0 = 1 - a_0 f(a_1,\ldots, a_n) = 1$ となり矛盾する．よって，$V(J) = \emptyset$ である．

もし $J \neq S'$ ならば，J を含む S' の極大イデアル $\mathfrak{m} = (X_0 - a_0,\, X_1 - a_1,\ldots, X_n - a_n)$ が存在する．このとき，$(a_0,\ldots, a_n) \subset V(J)$ である．したがって，$J = S'$ でなければならない．

特に，$1 \in J$ で，J は S' 上 h と $f_1,\ldots, f_m$ で生成されていたから，ある $g_0,\ldots, g_m \in S'$ を取り，

$$\begin{aligned} 1 =& g_0(X_0,\ldots,X_n)\bigl(1 - X_0 f(X_1,\ldots,X_n)\bigr) \\ &+ \sum_{i=1}^{m} g_i(X_0,\ldots,X_n) f_i(X_1,\ldots,X_n) \end{aligned}$$

と書ける．この等式に $X_0 = 1/f(X_1,\ldots,X_n)$ を代入し，両辺に f の何乗かを掛けて両辺が多項式になるようにすると，

$$f^k = \sum_{i=1}^{m} h_i(X_1,\ldots,X_n) f_i(X_1,\ldots,X_n)$$

という形に表すことができる．したがって，$f^k \in I$ である．

ところで，S/I は 0 以外の巾零元を持たなかったから，$f \in I$ である． □