ALGEBRA II*

Hiroshi SUZUKI†
Department of Mathematics
International Christian University

2004 年度版

目 次

---

*教科書として、永尾汎著「代数学」朝倉書店 を指定。その関係で、証明なども、この教科書に負うところが多い。

†E-mail:hsuzuki@icu.ac.jp

1　環・体・整域

定義 1.1 加法と乗法という二つの演算が定義された集合 R が環 (ring) であるとは、次の R1 $\sim$ R4 を満たすことである。

R1 R は加法に関して加群 (commutative [abelian] group)。

R2 任意の $a, b, c \in R$ に対して、$(ab)c = a(bc)$。（結合律 (associative law)）

R3 任意の $a, b, c \in R$ に対して、$a(b+c) = ab + ac,\ (a+b)c = ac + bc$。（分配律 (distributive law)）

R4 R の 0 （R の加法の単位元）と異なる元 1 で、$1x = x1 = x$ を任意の $x \in R$ に対して満たすものがある。（乗法の単位元）

さらに次の R5 を満たすとき、可換環 (commutative ring) という。

R5 $ab = ba$ for all $a, b \in R$。

注

- R1 $\sim$ R3 のみを満たすものを環と呼び R4 を満たすものを「単位元を持つ環 (unital ring)」と呼び区別することも多い。
- 環 R は乗法に関して R2、R4 を満たすから、モノイドである。従ってその正則元全体 $U(R)$ は群となる。これを単数群という。
- $0x = x0 = 0\ (\neq 1)$ だから、0 は正則元ではない。すなわち、$U(R) \subset R - \{0\}$。$R - \{0\}$ を $R^{\#}$ とも書く。
  (*Pf.*)　$0 = 0x + (-0x) = (0+0)x + (-0x) = 0x + 0x + (-0x) = 0x + 0 = 0x$。

定義 1.2 $U(R) = R - \{0\} = R^{\#}$ となる環を斜体 (skew field) 、可換な（すなわち R5 を満たす）斜体を、体 (field) という。

定義 1.3 環 R の元 a に対し、$b \neq 0$ で $ab = 0$ $[ba = 0]$ となるものが存在するとき、a は左零因子 (left zero divisor) [右零因子 (right zero divisor)] という。可換環の時は単に零因子 (zero divisor) という。0 以外に零因子のない可換環を整域という。すなわち、

R6 $ab = 0 \longrightarrow a = 0$ or $b = 0$。

を満たす可換環、または R1 $\sim$ R6 を満たすもの。

注　体は、整域である。

例 1.1　1. 有理整数環 $\boldsymbol{Z}$ は、整域である。

2. 有理数体 $\boldsymbol{Q}$、実数体 $\boldsymbol{R}$、複素数体 $\boldsymbol{C}$ は、いずれも可換体である。

3. R を環とするとき、R 上の全行列環、$\mathrm{Mat}_n(R)$ は、非可換な環である。

4. n を自然数としたとき、$\boldsymbol{Z}_n = \boldsymbol{Z}/n\boldsymbol{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ に、通常の和、積の n による剰余によって演算を定義すると、元の数が n である可換環になる。

以下では、有理整数環 $\boldsymbol{Z}$ とともに、非常に重要な可換環である多項式環について基本事項を学ぶ。

可換環 R の元を係数とする文字 x の整式

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,\ a_i \in R \text{ for } i = 0, 1, \ldots, n$$

を x を不定元とする R の多項式といい、x を不定元という。また、$R[x]$ で、x を不定元とする R 上の多項式全体を表すものとする。

$$f = f(x) = a_0 + a_1 x + \cdots + a_n x^n,\ g = g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

を $R[x]$ の元とするとき、和および積を以下のように定義する。

$$\begin{aligned} f + g &= \sum_i (a_i + b_i) x^i \\ fg &= \sum_i \Big(\sum_j a_j b_{i-j}\Big) x^i \end{aligned}$$

この演算に関して $R[x]$ は環になる。これを、R 上の多項式環という。

$f = f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x],\ a_n \neq 0$ の時、$n = \deg f$ と書き f の次数という。$f(x) = 0$ の時は、$\deg f = \deg 0 = -\infty$ とする。

命題 1.1 R を整域、$f, g \in R[x]$ とする。このとき、次が成立する。

(1) $\deg(f+g) \leq \max(\deg f, \deg g)$。

(2) $\deg(fg) = \deg f + \deg g$。特に、整域 R 上の多項式環は、また整域である。

証明　(1) (2) ともに明らか。$fg = 0$ とする。(2) を用いると、

$$-\infty = \deg fg = \deg f + \deg g.$$

従って、$\deg f = -\infty$ または $\deg g = -\infty$。すなわち、$f = 0$ または $g = 0$ を得る。 ■

定理 1.2 R を可換環。$f, g \in R[x]$ とし、g の最高次の係数は、R の正則元だとする。このとき、$q, r \in R[x]$、$\deg r < \deg g$ で、$f = gq + r$ となるものが存在する。さらに、R が整域ならば、この様な $q, r \in R[x]$ は、ただ一つに決まる。

証明　$f = a_n x^n + \cdots + a_1 x + a_0$、$a_n \neq 0$、$g = b_m x^m + \cdots + b_1 x + b_0$ とする。まず、$n < m$ の時は、$q = 0$、$r = f$ とすれば良い。

$n \geq m$ と仮定し、$n = \deg f$ に関する帰納法で証明する。b_m は、仮定より正則元だから、逆元が存在する。$h = f - (a_n b_m^{-1}) x^{n-m} g$ とすれば、f の最高次の係数が消えるから、$\deg h < n$。従って、帰納法の仮定より、$R[x]$ の元 q_1, r で、$\deg r < \deg g$ かつ、$h = gq_1 + r$ となるものがある。従って

$$f = g(q_1 + (a_n b_m^{-1}) x^{n-m}) + r$$

と表される。よって、$q = q_1 + (a_n b_m^{-1}) x^{n-m}$ と置けばよい。

R を整域とし、一意性を示す。

$$f = gq + r = gq' + r',\ \deg r, \deg r' < \deg g$$

とする。すると、$g(q - q') = r' - r$。ここで、次数を比べると、

$$\deg g + \deg(q - q') = \deg(g(q - q')) = \deg(r' - r) \leq \max(\deg r', \deg r) < \deg g.$$

$g \neq 0$ より、$q - q' = 0$。従って、$r' - r = 0$。すなわち、$q = q'$、$r = r'$ を得る。 ■

n 変数多項式環は、帰納的に、$R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$ によって定義する。この元は、一般には、次のように書ける。

$$\sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n},\ a_{i_1, \ldots, i_n} \in R.$$

また、$R[x, y] = (R[x])[y] = (R[y])[x]$ と見ることも出来る。

2　イデアルと剰余環

R を環とすると、加法に関しては、加群だから、加法に関する部分群 I は、すべて、正規部分群である。従って、R/I は加群となる。どのような条件のもとで、R/I が環になるであろうか。

$xy \in (x+I)(y+I)$ だから、積が自然に定義できるためには、

$$(x+I)(y+I) \subset xy+I$$

であることが必要である。逆に、上の条件を満たせば、積が定義できる。ここで、$x=0$ または、$y=0$ とおくことによって、$xI \subset I$、$Iy \subset I$ を満たすことが必要であることが分かる。

定義 2.1 環 R の部分集合 $I \neq \emptyset$ が、次の二つの条件、

- $a, b \in I \longrightarrow a+b \in I$
- $a \in I,\ r \in R \longrightarrow ra \in I,\ [ar \in I].$

を満たすとき、I を R の左イデアル [右イデアル] と呼び、左右イデアルを両側イデアルと呼ぶ。

A、B を環 R の部分集合とするとき、これらの和および積を次のように定義する。特に、積の定義に注意。

- $A+B = \{a+b \mid a \in A, b \in B\}.$
- $AB = \{\sum_i a_i b_i \mid a_i \in A,\ b \in B\}.$

練習問題 2.1 以下を示せ。

1. 環 R の左（右、両側）イデアル I, J に対して、$I \cap J$、$I+J$ は共に、左（右、両側）イデアルである。
2. I, J が環 R の両側イデアルならば、IJ も両側イデアルで、$IJ \subset I \cap J$ を満たす。また、等号が成り立たない例をあげよ。

この節の始めに見たように、I を環 R の両側イデアルで $I \neq R$ とすると、R/I は、

$$(a+I)+(b+I) = (a+b)+I,\ (a+I)\cdot(b+I) = (ab)+I$$

と、和と積を定義する事により、R/I は環になる。この環を剰余環 (quotient ring) と言う。

- $a \in R$ のとき、Ra $[aR]$ は、左イデアル [右イデアル] になるが、これを単項 (principal) 左 [右] イデアルと言う。R が可換環の時は、$Ra = aR$ を (a) ともかく。

- $0=\{0\}$、R は、R の両側イデアルであるが、これらを、R の自明なイデアルという。
- I を R の左 [右] イデアルとする。このとき、

  $$I = R \Leftrightarrow U(R) \cap I \neq \emptyset.$$

  (*Pf.*) $I=R$ とすると、$1 \in I \cap U(R)$ より、$U(R) \cap I \neq \emptyset$。逆に、$u \in U(R) \cap I$ とする。このとき、$r \in R$ とすと、

  $$r = r(u^{-1}u) = (ru^{-1})u \in RI \subset I.$$

  従って、$R \subset I$。よって、$I=R$。

命題 2.1 R を環としたとき、次は、同値。
R は、斜体 $\Leftrightarrow$ R の左 [右] イデアルは、0 と R のみ。

証明 ($\Rightarrow$) I を 0 とは異なる R の左イデアルとする。$a \in I - \{0\}$ とすると、$a \in U(R)$。従って、上の注より $I=R$。

($\Leftarrow$) $a \neq 0$ とすると、$a \in Ra$ より、Ra は 0 でない左イデアルだから、仮定より $1 \in R = Ra$。従って、R の元 b で、$ba=1$ となるものがある。特に、$b \neq 0$ だから、同様にして、$R=Rb$。特に、R の元 c で、$cb=1$ となるものがある。すると、

$$c = c1 = c(ba) = (cb)a = 1a = a$$

だから、$ab=ba=1$。よって、R の 0 以外の元は、すべて、単元である。従って、R は斜体である。 ■

順序集合 X が、任意の空でない部分集合に最小元を持つとき、整列集合 (well-ordered set) という。

定義 2.2
1. 任意のイデアルが、単項である整域を単項イデアル整域 (PID : principal ideal domain) と言う。
2. 整域 R から、整列集合 (well-ordered set) X への写像 $\rho : R \to X$ があって、次の二つの条件を満たすとき、R はユークリッド整域 (Euclidean domain) であると言う。
   (a) $0 \neq a \in R \Rightarrow \rho(0) < \rho(a)$.
   (b) $a, b \in R$ $(a \neq 0) \Rightarrow b = aq + r,\ \rho(r) < \rho(a)$ となる $q, r \in R$ がある。

定理 2.2 ユークリッド整域は、単項イデアル整域である。

証明 R をユークリッド整域、I を R の イデアルとする。$I=0$ ならば、明らかに、単項イデアルだから、$I \neq 0$ とする。

$$\emptyset \neq \{\rho(x) \mid 0 \neq x \in I\} \subset X$$

の最小元を、$\rho(a)$ $a \in I$ とする。ここで、$b \in I$ とすると、$b = aq + r$、$\rho(r) < \rho(a)$ となる、$q, r \in R$ がある。$r = b - aq \in I$ だから、a の取り方から、$r=0$ を得、$b \in Ra$。b は任意だから、$I = Ra$、すなわち、すべてのイデアルは単項である。 ■

例 2.1

1. $\rho : \boldsymbol{Z} \to \{0\} \cup \boldsymbol{N}$ を $\rho(a) = |a|$ によって定義すると、$\boldsymbol{Z}$ はユークリッド整域になる。特に、定理 2.2 より、$\boldsymbol{Z}$ は、単項イデアル整域である。実は、$\boldsymbol{Z}$ においては、イデアルであることと、部分加群であることは同じであるから、単項イデアル整域であることは、単に、$\boldsymbol{Z}$ の部分群が巡回群であることを主張しているに過ぎない。

2. K を体とする。$\rho : K[x] \to \{-\infty, 0\} \cup \boldsymbol{N}$ を $\rho(f) = \deg f$ によって定義すると、定理 1.2 により、$K[x]$ はユークリッド整域になる。特に、定理 2.2 より、$K[x]$ は単項イデアル整域である。

3　準同型定理

定義 3.1 環 R から、R' への写像 $f : R \to R'$ が、

$$f(a+b) = f(a) + f(b),\ f(ab) = f(a)f(b),\ f(1_R) = f_{R'}$$

を満たすとき、f を R から、R' への（環）準同型 ((ring) homomorophism) と言う。f が全単射の時同型と言い、$R \simeq R'$ と書く。

例 3.1 I を、環 R の両側イデアルで、$(R \neq I)$ とするとき、

$$f : R \longrightarrow R/I,\ (a \mapsto a+I)$$

は、環準同型で、全射である。

定義 3.2 環 R の部分集合 S が次の条件

$$a, b \in S \Rightarrow a - b \in S,\ ab \in S,\ 1_R \in S$$

を満たすとき、S は、R の部分環 (subring) であるという。また、R は、S の拡大環 (extension ring) であるという。

練習問題 3.1 部分環は、環である。

命題 3.1 $f : R \to R'$ を環準同型とする。

(1) $\mathrm{Ker} f = \{a \in R \mid f(a) = 0\}$ は、両側イデアル。

(2) $\mathrm{Im} f = \{f(a) \mid a \in R\}$ は、R' の部分環。

証明　練習問題 3.2. ■

定理 3.2 （準同型定理）R、R' を環、$f : R \to R'$ を環準同型とすると、

$$R/\mathrm{Ker} f \simeq \mathrm{Im} f.$$

証明　命題 3.1 より、$R/\mathrm{Ker} f$ も、$\mathrm{Im} f$ も、環。群の準同型定理より、

$$\bar{f} : R/\mathrm{Ker} f \to \mathrm{Im} f,\ (a + \mathrm{Ker} f \mapsto f(a))$$

は、well-defined で、加群としての同型写像。

$$\bar{f}((a+\mathrm{Ker} f)(b+\mathrm{Ker} f)) = \bar{f}(ab+\mathrm{Ker} f) = f(ab) = f(a)f(b) = \bar{f}(a+\mathrm{Ker} f)\bar{f}(b+\mathrm{Ker} f)$$

$$\bar{f}(1_{R/\mathrm{Ker} f}) = \bar{f}(1+\mathrm{Ker} f) = f(1_R) = 1_{R'}.$$

よって、$\bar{f}$ は、環として同型。 ■

上の証明で、群の準同型定理を用いたが、そこでの鍵は、以下の同値であった。

$$f(a) = f(b) \Leftrightarrow f(a-b) = 0 \Leftrightarrow a - b \in \mathrm{Ker} f \Leftrightarrow a + \mathrm{Ker} f = b + \mathrm{Ker} f$$

これは、上で定義された $\bar{f}$ が、well-defined かつ全単射であることを示している。

例 3.2 $K \subset L$ を体、$\alpha \in L$ とする。$\phi : K[x] \to L$ $(f(x) \mapsto f(\alpha))$ を環準同型とする。$\mathrm{Im}\phi$ を $K[\alpha]$ と書く。すなわち、$K[\alpha] = \{f(\alpha) \mid f(x) \in K[x]\}$。すると、準同型定理により、$K[x]/\mathrm{Ker}\phi \simeq K[\alpha]$ となるが、$\mathrm{Ker}\phi$ は、単項イデアル整域 $K[x]$ のイデアルだから、ある $p(x) \in K[x]$ によって、$\mathrm{Ker}\phi = K[x]p(x) = (p(x))$ と書ける。$p(x) = 0$ すなわち $\mathrm{Ker}\phi = 0$ の時、α を K 上超越的な元と呼ぶ。$p(x) \neq 0$ の時は、$p(x)$ として、モニック（最高次の係数が 1 のもの）をとる事が出来る。実は、$p(x)$ は、$\mathrm{Ker}\phi$ の 0 でない多項式の内で、次数が最小で、モニックなものとして、一意的に決まる。定理 2.2 の証明参照。このとき、α を K 上代数的な元、$p(x)$ を α の K 上の最小多項式という。

以下 $K = \boldsymbol{Q}$、$L = \boldsymbol{C}$ とする。e、π は、$\boldsymbol{Q}$ 上超越的な元である。($\boldsymbol{Q}$ 上超越的な元を超越数 (transcendental number) と呼ぶ。一般的には、超越数であることを証明することは、とても難しい。

$\alpha = \sqrt{-1}$ とすると、$\mathrm{Ker}\phi = (x^2 + 1)$ であり、$\boldsymbol{Q}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \boldsymbol{Q}\}$ が環であることもこれより分かった。次回には、これが体になることも分かる。

$\alpha = \sqrt[3]{2}$ とすると、$\mathrm{Ker}\phi = (x^3 - 2)$ であり、$\boldsymbol{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b \in \boldsymbol{Q}\}$ となる。

例 3.3 $A \in \mathrm{Mat}_n(\boldsymbol{C})$、$\psi : \boldsymbol{C}[x] \to \mathrm{Mat}_n(\boldsymbol{C})$ $(f(x) \mapsto f(A))$ とする。Hamilton-Cayley の定理により、$\mathrm{Ker}\psi \supset (\det(xI - A)) \neq 0$。よって、monic な多項式によって、$\mathrm{Ker}\psi = p_A(x)$ と書ける。この $p_A(x)$ を最小多項式という。上の事から $p_A \mid \det(xI - A)$ である。例えば、

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ -4 & 4 \end{pmatrix},\ C = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

としたとき、それぞれの最小多項式は、

$$p_A(x) = (x-1)(x+2),\ p_B(x) = (x-2)^2,\ p_C(x) = x - 2$$

である。

4　素イデアルと極大イデアル

R を可換環、I をイデアルとする。このとき、剰余環 R/I が、整域や体となるイデアル I の満たすべき条件を考える。

定義 4.1　(1) 可換環 R のイデアル $I(\neq R)$ について、

$$ab \in I \longrightarrow a \in I \text{ または } b \in I$$

が成立するとき、I を素イデアル (prime ideal) という。

(2) 可換環 R のイデアル $I(\neq R)$ について、

$$I \subset J:\ R \text{ のイデアル} \longrightarrow I = J \text{ または } J = R$$

が成立するとき、I を極大イデアル (maximal ideal) という。

定理 4.1　R を可換環、I をそのイデアルとする。

(1) R/I は整域 $\Leftrightarrow$ I は素イデアル。

(2) R/I は体 $\Leftrightarrow$ I は極大イデアル。

(3) 極大イデアルは、素イデアル。

証明　(1) R/I が整域であることは、以下のことと同値である。

$$\begin{aligned}
&\bar{a}, \bar{b} \in R/I,\ \bar{a}\bar{b} = \bar{0} \to \bar{a} = \bar{0} \text{ または } \bar{b} = \bar{0} \\
&\quad \Leftrightarrow\quad a, b \in R,\ (a+I)(b+I) = ab + I = I \to a + I = I \text{ または } b + I = I \\
&\quad \Leftrightarrow\quad a, b \in R,\ ab \in I \to a \in I \text{ または } b \in I \\
&\qquad\qquad (x + I = y + I \leftrightarrow x - y \in I \text{ に注意})
\end{aligned}$$

(2) 命題 2.1 により、R/I が体であることと、R/I の 0 でないイデアルは、R/I のみであることは同値である。これは、言い換えると、R のイデアル J で I を真に含むものは、R に限られるということと同値であるから（練習問題参照)、I が R の極大イデアルであることと同値である。

(3) I：極大イデアル $\Leftrightarrow$ R/I：体 $\Rightarrow$ R/I：整域 $\Leftrightarrow$ I：素イデアル。 ■

注　R を可換環とすると、上の定理から、零イデアル (0) が素イデアルであることと、R が整域であることが同値であり、また、(0) が極大イデアルであることと、R が体であることが同値である。

命題 4.2　R を単項イデアル整域 (PID)、I を R のイデアルで $I \neq (0)$ なるものとする。このとき、次は同値。

$$I\text{：素イデアル} \Leftrightarrow I\text{：極大イデアル}$$

証明　定理 4.1 により、極大イデアルは、常に素イデアルだから、$I = (a) \neq (0)$ を素イデアルとして、I が極大イデアルであることを示す。J を I を真に含む R のイデアルとする。R は、単項イデアル整域だから、$J = (b)$ とおける。$a \in (a) = I \subset J = (b)$ だから、$a = bc$ となる $c \in R$ が存在する。$I = (a)$ は、素イデアルだから $b \in I$ または $c \in I$。$b \in I$ とすると、$J = (b) \subset (a) = I$ となり J が I を真に含むイデアルであることに反するから、$c \in I = (a)$。すなわち、$c = ad$ となる $d \in R$ が存在する。これより、

$$a = bc = bad = abd \to a(bd - 1) = 0$$

を得る。$a \neq 0$ だったから $bd = 1$ すなわち $R = (1) \subset (b) = J$ となり $J = R$ となるから、I は極大イデアルである。 ■

命題 4.3 n を有理整数環 $\boldsymbol{Z}$ の零でない元とする。ことのき、次は同値。

$$(n)\text{：極大イデアル} \Leftrightarrow (n)\text{：素イデアル} \Leftrightarrow n \text{ は素数}$$

証明　まず、$(n) \subset (m)$ は、$m \mid n$ と同値であることに注意する。これより、$(m) = (n)$ であることと、$m = \pm n$ は同値であることが分かる。さて、「(m) が極大であること」と、「$(m) \subset (n)$ ならば、$(n) = (m)$ または $(n) = (1)$ であること」とは、同値である。これより、n の約数は、$\pm n$ であるか、または ± 1 であるかのどちらかであることを得る。極大イデアルは、$(1) = \boldsymbol{Z}$ とは異なるから、

$$(n)\text{：極大イデアル} \Leftrightarrow n \text{ は素数}$$

$\boldsymbol{Z}$ は、単項イデアル整域であるから、命題 4.2 より、零でないイデアルが極大イデアルであることと、素イデアルであることは、同値であることが分かる。 ■

注　この命題により、$\boldsymbol{Z}_n = \boldsymbol{Z}/(n)$ が体であることと、整域であることと、n が素数であることは、全て同値であることもわかった。

定義 4.2 整域 R 上の次数が 1 以上の多項式 $f(x)$ は、$R[x]$ において、$f(x) = g(x)h(x)$ $\deg g > 0$、$\deg h > 0$ と分解されるとき（R 上）可約、そうでないとき、（R 上）既約であるという。

命題 4.4 K を体とし、$f(x) \in K[x]$ を零でない多項式とする。このとき、次は同値。

$$(f(x))\text{：極大イデアル} \Leftrightarrow (f(x))\text{：素イデアル} \Leftrightarrow f(x) \text{ は既約}$$

証明　$f(x)$ が定数の時は、上の 3 つのどの条件も満たさないから考えなくて良い。そこで、$\deg f(x) \geq 1$ とする。$K[x]$ は、単項イデアル整域であるから、$(f(x))$ が極大イデアルであることと、素イデアルであることは、同値である。このことと、$f(x)$ が既約であることが同値であることを示す。

$f(x)$ を可約とする。すなわち、$f(x)=g(x)h(x)$、$\deg g(x)>1$、$\deg h(x)>1$ とする。すると、

$$(f(x))\subset(g(x))\subset K[x]$$

でどちらも等号は成り立たない。$U(K[x])=U(K)=K^*$ だから、練習問題より以下が同値であることから明か。

$$(f_1(x))=(f_2(x))\Leftrightarrow f_1(x)=cf_2(x)\ (c\in K^*).$$

逆に、$(f(x))$ は極大イデアルではないとする。$(g(x))$ を $(f(x))$ を真に含みかつ $K[x]$ とは異なるイデアルとする。すると、$f(x)=g(x)h(x)$ とかけ、条件から、$f(x)$ は、可約であることが分かる。 ■

例 4.1 x^2+1、x^2-2 が $\boldsymbol{Q}$ 上既約であることは簡単に確かめられるから、(x^2+1)、(x^2-2) は、$\boldsymbol{Q}[x]$ の極大イデアルであり、従って、$\boldsymbol{Q}[\sqrt{-1}]\simeq\boldsymbol{Q}[x]/(x^2+1)$、$\boldsymbol{Q}[\sqrt{2}]\simeq\boldsymbol{Q}[x]/(x^2-2)$ は、体であることが分かる。

次数の高い多項式について、既約かどうかはどのように判定すればよいのだろうか。実は、一般には非常に難しい。しかし、次の判定法は有効である。

命題 4.5 [Eisenstein の既約性判定法] p を素数、$f(x)=a_nx^n+\cdots+a_1x+a_0\in\boldsymbol{Z}[x]$ で以下の条件を満たすとする。

$$a_n\not\equiv 0\ (\mathrm{mod}\ p),\ a_{n-1}\equiv\cdots\equiv a_1\equiv a_0\equiv 0\ (\mathrm{mod}\ p),\ a_0\not\equiv 0\ (\mathrm{mod}\ p^2)$$

このとき、$f(x)$ は、$\boldsymbol{Z}$ 上既約である。

証明　可約として矛盾を導く。

$$f(x)=g(x)h(x),\ r=\deg g>0,\ s=\deg h>0,$$

$$g(x)=b_rx^r+\cdots+b_0,\ h(x)=c_sx^s+\cdots+c_0$$

とする。$a_0=b_0c_0$ は仮定より p で割り切れるが、p^2 では割り切れない。従って、p は、b_0 は割らないが、c_0 は割ると仮定する。一方、$a_n=b_rc_s$ は仮定から p で割れないから、c_s も p で割れない。c_0 は p で割れるとしているから、今 i を c_i が p で割り切れない最小の整数とする。従って、

$$c_0\equiv c_1\equiv\cdots\equiv c_{i-1}\equiv 0\not\equiv c_i\ (\mathrm{mod}\ p).$$

すると、

$$a_i=b_0c_i+b_1c_{i-1}+\cdots+b_ic_0\equiv b_0c_i\not\equiv 0\ (\mathrm{mod}\ p).$$

である。仮定から $n=i<s=\deg h$ となり、これは、矛盾である。従って、$f(x)$ は既約である。 ■

注　この命題は、$\boldsymbol{Z}$ 上既約かどうかの判定法であるが、実は、練習問題にもあるように、ガウスの補題（命題 7.7）といわれるものにより $\boldsymbol{Q}$ 上既約であることも分かる。

例えば、x^n-2、x^3-3x^2-9x-6 は、$\boldsymbol{Z}$ 上（そして、$\boldsymbol{Q}$ 上）既約である。

5　環の直和

定義 5.1 環 $R_1, R_2, \ldots, R_n$ が与えられたとき、直積

$$R = R_1 \times R_2 \times \cdots \times R_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R_i,\ i = 1, \ldots, n\}$$

に加法と乗法を次のように定義する。

加法：$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$

乗法：$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n)$

このとき、R は環になる。R を $R_1, \ldots, R_n$ の直和といい、以下のように書く。

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_n.$$

注　$1_R = (1_{R_1}, 1_{R_2}, \ldots, 1_{R_n})$、$0_R = (0_{R_1}, 0_{R_2}, \ldots, 0_{R_n})$ である。
　また、$R_i^* = \{(0, \ldots, 0, a, 0, \ldots, 0) \mid a \in R_i\}$（第 i 成分以外は、0）とすると、R_i^* は、R の両側イデアルである。

　可換環 R の二つのイデアル I, J が $I + J = R$ を満たすとき、I は J と互いに素であるという。すなわち次の同値条件を満たすことである。

$$I + J = R \Leftrightarrow x + y = 1 \text{ となる } x \in I,\ y \in J \text{ が存在する。}$$

　$\boldsymbol{Z}$ においては、(m) と (n) が互いに素な事と、$(m, n) = 1$ すなわち、m と n の最大公約数が 1 であることは同値である。実際、$x + y = 1$ となる $x \in (m),\ y \in (n)$ が存在するということは、$am + bn = 1$ となる $a, b \in \boldsymbol{Z}$ が存在することであり、このことは、$(m, n) = 1$ と同値であるからである。

　「3 で割って 1 余り、10 で割って 3 余り、7 では割り切れ、13 で割ると 11 余るような数はあるだろうか。またあるならばそれをすべて求めることが出来るか。」という種類の問題は、古くからいろいろと考えられていたようで孫子の「兵法」に軍隊の編成の問題から議論されていることなどから、この問題を取り扱った次の定理は中国剰余定理 (Chinise Remainer's Theorem) と呼ばれているとのことである。

定理 5.1 [中国剰余定理] R を可換環、$I_1, I_2, \ldots, I_n$ をどの二つも互いに素なイデアル（すなわち、$i \neq j$ のとき、$I_i + I_j = R$）とする。$a_1, a_2, \ldots, a_n \in R$ を任意の元とするとき、$x \equiv a_i \pmod{I_i}$ がすべての $i = 1, 2, \ldots, n$ に対して、成り立つ元 $x \in R$ が存在する。

証明　<u>$n = 2$ のとき</u>　仮定より、$1 = c_1 + c_2$ となる $c_1 \in I_1,\ c_2 \in I_2$ がある。そこで、$x = a_1c_2 + a_2c_1$ とおくと、$(\mathrm{mod}\ I_1)$ で、

$$x \equiv a_1c_2 + a_2c_1 \equiv a_1c_2 \equiv a_1(1 - c_1) \equiv a_1 - a_1c_1 \equiv a_1$$

となる。$x \equiv a_2 \pmod{I_2}$ も同様にして得る。

<u>$n > 2$ のとき</u>　まず、各 i について、次の性質を満たす $x_i \in R$ が存在することを示す。

$$x_i \equiv 1 \pmod{I_i},\ j \neq i \text{ の時は } x_i \equiv 0 \pmod{I_j}.$$

記号を見やすくするため、$i = 1$ のときを考える。$j \geq 2$ については、$I_1 + I_j = R$ だから、$c_1^{(j)} + c_j = 1$ となる、$c_1^{(j)} \in I_1$、$c_j \in I_j$ がある。すべてを掛け合わせると、

$$1 = \prod_{j=2}^{n}(c_1^{(j)} + c_j) \equiv c_2 \cdots c_n \pmod{I_1}$$

だから、$1 - c_2 \cdots c_n = c_1$ とおくと、$c_1 \in I_1$ である。とくに、$R = I_1 + I_2 \cdots I_n$ すなわち、二つのイデアル I_1、$I_2 \cdots I_n$ は互いに素であることが分かる。上記 $n = 2$ の時は、既に示してあるから、$x_1 \in R$ で、

$$x_1 \equiv 1 \pmod{I_1},\ x_1 \equiv 0 \pmod{I_2 \cdots I_n}$$

を満たすものが存在することが分かる。ところが、$j \geq 2$ に対して、$I_2 \cdots I_n \subset I_j$ であるから、$x_1 \equiv 0 \pmod{I_j}$ でもある。これで最初の主張が示された。

今、各 i について、x_i をとり、$x = a_1x_1 + \cdots + a_nx_n$ とおくと、

$$\begin{aligned} x &\equiv a_1x_1 + \cdots + a_nx_n \pmod{I_i} \\ &\equiv a_ix_i \pmod{I_i} \\ &\equiv a_i \pmod{I_i} \end{aligned}$$

となり、求めるものが得られた。 ■

6 商環

この節では、可換環に逆元をつけ加えてどれぐらい体に近く出来るかを考える。

定義 6.1 可換環 R の部分集合 S が次の条件

$$(i)\ a, b \in S \to ab \in S \qquad (ii)\ 1 \in S, 0 \notin S$$

を満たすとき、S は R の乗法的部分集合、積閉集合 (multiplicative subset) と言う。

例 6.1

1. R の非零因子全体（零因子以外の元すべて）は、乗法的部分集合である。
2. P を R の素イデアルとしたとき、$R - P$ は、乗法的部分集合である。

R を可換環 S を乗法的部分集合とする。
$R \times S$ に次のような関係を定義する。

$$(a, s) \sim (a', s') \Leftrightarrow (as' - a's)t = 0 \text{ となる } t \in S \text{ が存在する。}$$

すると、これは同値関係になる。(a, s) を含む同値類を a/s で表し、同値類全体を $S^{-1}R$ で表す。$S^{-1}R$ に加法と、乗法を次のように定義する。

加法：$(a_1/s_1) + (a_2/s_2) = (a_1s_2 + a_2s_1)/s_1s_2$

乗法：$(a_1/s_1)(a_2/s_2) = (a_1a_2/s_1s_2)$

これらの和・積は、$S^{-1}R$ の表し方によらず、一意的に定まり、可換環になる。これを R の S による商環 (quotient ring) という。

注

1. $0_{S^{-1}R} = 0/1$、$1_{S^{-1}R} = 1/1$、$-(a/s) = (-a)/s$ であり、$s \in S$ ならば、$s/1 \in U(S^{-1}R)$ である。
2. S が零因子を含まないときは、$a/s = a'/s' \Leftrightarrow as' - a's = 0$。
3. $\phi_S : R \to S^{-1}R\ (a \mapsto a/1)$ を自然な準同型という。
   ϕ_S：単射 $\Leftrightarrow$ S は、零因子を含まない。

例 6.2

1. S を R の非零因子全体の時、$S^{-1}R$ を R の全商環 (ring of total quotients) という。
2. R が整域のときは、R の全商環は体になる。これを商体 (quotient field) と呼び、$\mathcal{Q}(R)$ とかく。
   (a) $\mathcal{Q}(\boldsymbol{Z}) = \boldsymbol{Q}$、有理整数環の商体は、有理数体である。

(b) $\mathcal{Q}(K[x_1,\ldots,x_n]) = K(x_1,\ldots,x_n) = \{f/g \mid f,g \in K[x_1,\ldots x_n],\ g \neq 0\}$ であり、これを有理関数体という。

(c) P を可換環 R の素イデアル、$(R-P)^{-1}R$ を R_P と書き、R の P による局所化 (localization) と呼ぶ。

定義 6.2 可換環 R がただ一つの極大イデアル M を持つとき、R は、局所環 (local ring) であるという。

注　体は、(0) がただ一つの極大イデアルであるから、局所環である。

R を局所環、M をその極大イデアルとする。I を R とは異なるイデアルとすると、Zorn の補題を用いることにより、I を含む極大イデアルが一つ存在する。R は、局所環であるから $I \subset M$ であることが分かる。すなわち、M は、R の真のイデアルをすべて含む。

命題 6.1 可換環 R について、次の二つは、同値。[(1) $\Rightarrow$ (2) には、選択公理が必要]

(1) R は局所環。

(2) $R-U(R)$ は、R のイデアル。

証明　(1) $\Rightarrow$ (2)　M を R のただ一つの極大イデアルとする。$M \neq R$ だから、$M \cap U(R) = \emptyset$ すなわち、$M \subset R-U(R)$。ここで、$a \in R-U(R)$ とすると、$Ra \neq R$ だから、$a \in Ra \subset M$。よって、$R-U(R) \subset M$。従って、$M = R-U(R)$ であり、これはイデアルである。

(2) $\Rightarrow$ (1)　J を $R \neq J$ なる R のイデアル、$I = R-U(R)$ とする。このとき、$J \cap U(R) = \emptyset$ だから、$J \subset I$。よって I は R のただ一つの極大イデアルである。 ■

命題 6.2 P を可換環 R の素イデアルとすると、局所化 R_P は局所環で、

$$P' = \{a/s \mid a \in P,\ s \notin P\}$$

がそのただ一つの極大イデアルである。

証明　<u>P' は、R_P のイデアルである。</u>

(*Pf.*)　$(a/s)+(b/t) = (at+bs)/st$、$a,b \in P,\ s,t \notin P$ とすると、$at+bs \in P$、$st \notin P$ だから、$(at+bs)/st \in P'$。同様に、$r \in R$ の時、$(r/t)(a/s) = ar/ts \in P'$。従って、$P'$ は R_P のイデアルである。

<u>$a/s \in P' \Leftrightarrow a \notin P.$</u>

(*Pf.*)　($\Rightarrow$) $a \in P$ ならば、$a/s \in P'$ だから、明らか。

($\Leftarrow$) $a/s \in P'$ とすると、$a/s = a'/s'$ となる $a' \in P$、$s' \notin P$ が存在する。従って、$(as'-a's)t = 0$ を満たす $t \notin P$ が存在する。これより、$as't = a'st \in P$ だから、仮定より $a \in P$ を得る。

$\underline{R_P - P' = U(R_P)}$
(*Pf.*) ('$\subset$' であること。) $a/s \notin P'$ とすると、$a \notin P$ だから、$s/a \in R_P$。すなわち、$a/s \in U(R_P)$。
('$\supset$' であること。) $1 \notin P$ だから、$1/1 \notin P'$。$a/s \in U(R_P) \cap P'$ とすると、$a \in P$ であり、かつ、$(a/s)(b/t) = 1/1$ となる、$b \in R$、$t \notin P$ が存在する。これより、ある $t' \notin P$ により、$abt' = stt'$ となるが、この式の右辺は、P に属さず、左辺は、P に属することになり矛盾。従って、$U(R_P) \cap P' = \emptyset$。これより、$R_P - P' = U(R_P)$ を得る。 ■

7　一意分解整域

7.1　一意分解整域と単項イデアル整域

R を整域、$a, b \in R$ とする。

- $(a) \subset (b) \Leftrightarrow a = bc$ となる $c \in R$ がある。このとき、$b \mid a$ と書く。
- $(a) = (b) \Leftrightarrow a = bu$ となる $u \in U(R)$ がある。このとき、$a \approx b$ と書き同伴という。
- R の元 $p \neq 0$ が正則元でなくかつ、$p = uv \to u \in U(R)$ 又は、$v \in U(R)$ の時、p を素元という。

定義 7.1 整域 R が次の二つの条件を満たすとき、R を一意分解整域 (UFD = Unique Factorization Domain) であるという。

(i) $a \in R$ を零でない単元でもない元とする。$a = p_1 p_2 \cdots p_r$ (p_i は素元) と書ける。

(ii) $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ (p_i, q_j は素元）ならば $r = s$ で番号を付け替えれば $p_i \approx q_i$。

命題 7.1 R を整域、$0 \neq p \in R$ とする。

(1) (p) が素イデアル ならば、 p は素元。

(2) R が UFD ならば (p) が素イデアルことと、p は素元であることは同値。

証明　(1) $p = ab$ とする。仮定より、$a \in (p)$ または $b \in (p)$。$a \in (p)$ とする。$(a) \subset (p) = (ab) \subset (a)$ だから、$a \approx p$ で $p = au$、$u \in U(R)$ と書ける。$a(b-u) = p - p = 0$ で、R は整域だから $b = u \in U(R)$。

(2) p を素数とする。$ab \in (p)$ とすると、a または $b \in U(R)$ のときは明らか。$ab = pc$、$a = p_1 \cdots p_r$、$b = q_1 \cdots q_s$、$c = v_1 \cdots v_t$ を素元分解とする。

$$p_1 \cdots p_r q_1 \cdots q_s = p v_1 \cdots v_t$$

素元分解の一意性より $p \approx p_i$ 又は $p \approx q_j$。そこで、$p \approx p_i$ とすると、$a = p_1 \cdots p_r \in (p_i) = (p)$。$p \approx q_j$ とすると、$b = q_1 \cdots q_s \in (q_j) = (p)$。 ■

注　この命題は、ある環 R が一意分解整域ではないことを示すためにも用いられる。すなわち、素元ではあるが、それで生成されたイデアルが、素イデアルではない元の存在が示されればそれで良い。

命題 7.2 R を単項イデアル整域、$p \neq 0$ とすると次は同値。

(1) p は素元。

(2) (p) は素イデアル。

(3) (p) は極大イデアル。

証明　命題 4.2 により (2) $\Leftrightarrow$ (3)、また、命題 7.1 により (2) $\Rightarrow$ (1) も示してあるから、(1) $\Rightarrow$ (3) を示せばよい。$(p) \subset I = (q) \subset R$ とすると、$p = qa$ と書ける。仮定より、q が単元か、a が単元。それぞれ、$(q) = R$ または、$(p) = (q)$ となる。従って、(p) は極大イデアルである。 ■

定理 7.3 単項イデアル整域は一意分解整域である。

証明　R を単項イデアル整域とし、$0 \neq a \in R - U(R)$ とする。このとき、$(a) \neq R$ だから (a) を含む極大イデアル (p_1) が存在する。命題 7.2 より p_1 は素元である。$(a) \subset (p_1)$ より、$a = p_1 a_1$ と表すことが出来、$p_1 \notin U(R)$ より、(a_1) は、(a) を真に含む。$a_1 \notin U(R)$ ならば素元 p_2 が存在して、$a_1 = p_2 a_2$、$(a = p_1 p_2 a_2)$ と書くことが出来る。この様にして順に a_i を取っていくとき、正則元でない限りにおいて、真に増加する列

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_i) \subset \cdots$$

がつくれる。$\bigcup_{i=1}^{\infty}(a_i)$ は R のイデアルだから、$\bigcup_{i=1}^{\infty}(a_i) = (d)$ と書ける。従って、ある i について、$d \in (a_i)$ となるから、$(a_i) = (a_{i+1})$ となり真に増加することはない。よってある r について a_r は正則元、すなわち、$p_r a_r$ は素元で、$a = p_1 p_2 \cdots (p_r a_r)$。

一意性:$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$、$r \leq s$ とし、r に関する帰納法を用いる。$q_1 q_2 \cdots q_s = a \in (p_1)$ で、(p_1) は素イデアルだから、$q_i \in (p_1)$ となる i がある。しかし、$(q_i) \subset (p_1)$ で、どちらも極大イデアルであるから、$q_i \approx p_1$ である。番号を付け替え、$q_1 = p_1 u$、$u \in U(R)$ とすると、

$$p_1 p_2 \cdots p_r = p_1 u q_2 \cdots q_s$$

を得るから、$p_2 \cdots p_r = u q_2 \cdots q_s$。帰納法により、$r = s$ かつ、番号の付け替えにより、$p_i \approx q_i$ となることが分かる。 ■

これにより、ユークリッド整域は、単項イデアル整域であり、単項イデアル整域は、一意分解整域であることが分かった。しかし、これだけでは、$\boldsymbol{Z}[x]$ や、$\boldsymbol{Q}[x_1, \cdots, x_n]$ が一意分解整域かどうかは分からない。

例 7.1 $\boldsymbol{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \boldsymbol{Z}\}$ は一意分解整域ではない事を示す。上でも注意したように、2 は素元であるが、(2) は素イデアルではないことを示す。

- $\alpha = a + b\sqrt{-5}$ のとき、$N(\alpha) = \alpha\bar{\alpha} = a^2 + 5b^2$ とすると、

$$\alpha \in U(\boldsymbol{Z}[\sqrt{-5}]) \Leftrightarrow N(\alpha) = 1 \Leftrightarrow \alpha = \pm 1.$$

(*Pf.*)　$\pm 1 \in U(\boldsymbol{Z}[\sqrt{-5}])$ は明らか。逆に $\alpha\beta = 1$ とすると、

$$1 = N(\alpha\beta) = N(\alpha)N(\beta)$$

だから、$a^2 + 5b^2 = N(\alpha) = 1$。これを満たす $a, b \in \boldsymbol{Z}$ を考えると、$b = 0$、$a = \pm 1$ であることが分かる。

- 2 は素元。

  (*Pf.*)　$2 = \alpha\beta$、$N(\alpha) \neq 1$、$N(\beta) \neq 1$、$\alpha = a + b\sqrt{-5}$ とする。

  $$4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$$

  だから、$a^2 + 5b^2 = N(\alpha) = 2$。しかしこれは不可能である。従って、$N(\alpha) = 1$ 又は、$N(\beta) = 1$ すなわち、α, β のうちどちらかは、単元である。

- (2) は、素イデアルではない。

  (*Pf.*)　$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 \in (2)$。ここで、$1 \pm \sqrt{-5}$ のどちらかが、(2) に入るとすると、$1 \pm \sqrt{-5} = 2\gamma$ と書いたとき、

  $$6 = N(1 \pm \sqrt{-5}) = 4N(\gamma)$$

  となり、これは不可能である。従って、$1 \pm \sqrt{-5}$ どちらも (2) に入らない。これは、(2) が素イデアルではないことを示す。

7.2 一意分解整域上の多項式環

ここでは、R を一意分解整域、$K = Q(R)$ を商体とする。

- d が、$a_1, \ldots, a_n \in R$ の最大公約元であるとは、以下の２条件を満たすことである。
  1. $d \mid a_i,\ i = 1, 2, \ldots, n$。
  2. $c \mid a_i,\ i = 1, 2, \ldots, n$ ならば、$c \mid d$。
- l が、$a_1, \ldots, a_n \in R$ の最小公倍元であるとは、以下の２条件を満たすことである。
  1. $a_i \mid l,\ i = 1, 2, \ldots, n$。
  2. $a_i \mid m,\ i = 1, 2, \ldots, n$ ならば、$l \mid m$。
- $a_1, a_2, \ldots, a_n$ の最大公約元が 1 であるとき、$a_1, a_2, \ldots, a_n$ は、互いに素 (coprime) であるという。
- $a_0, a_1, \ldots, a_n$ が互いに素である時、$f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ を原始多項式 (primitive polynomial) という。

練習問題にもあるように、R が一意分解整域ならば最大公約元、最小公倍元は存在し、R の正則元倍をのぞいて一意的に決まる。$R = \boldsymbol{Z}$ のときは、たとえば 4 と 6 の最大公約元は上の定義のもとでは、± 2 となります。

定理 7.4 一意分解整域 R 上の多項式環 $R[x_1, x_2, \ldots, x_n]$ は、一意分解整域である。

補題 7.5 $f(x) \in K[x]$ とすると、$c \in K$ と、原始多項式 $f_0(x) \in R[x]$ で、$f(x) = cf_0(x)$ となるものがある。この c は R の正則元倍をのぞいて一意的に決まる。これを $I(f)$ と書く。

証明　$f(x) = (b_0/a_0) + (b_1/a_1)x + \cdots + (b_n/a_n)x^n$、$0 \neq a_i, b_j \in R$。$m$ を $a_0, a_1, \ldots, a_n$ の最小公倍元、$m = a_ic_i$、d を $b_0c_0, b_1c_1, \ldots, b_nc_n$ の最大公約元、$de_i = b_ic_i$ とする。$e_0, e_1, \ldots, e_n$ は互いに素である。さらに、

$$\begin{aligned} f(x) &= (b_0/a_0) + (b_1/a_1)x + \cdots + (b_n/a_n)x^n \\ &= \frac{1}{m}(b_0c_0 + b_1c_1x + \cdots + b_nc_nx^n) \\ &= \frac{d}{m}(e_0 + e_1x + \cdots + e_nx^n) \end{aligned}$$

ここで、$c = d/m$、$f_0(x) = e_0 + e_1x + \cdots + e_nx^n$ とおけばよい。

$f(x) = cf_0(x) = c'f_0'(x)$、$f_0(x)$、$f_0'(x)$ は、R 上の原始多項式、$c = b/a$、$c' = b'/a'$、a と b、a' と b' は互いに素な R の元とする。$a'bf_0(x) = ab'f_0'(x)$ だから、それぞれの係数の最大公約元を考えると、最大公約元は、正則元倍をのぞいて、一意に決まり、

$f_0(x)$、$f_0'(x)$ はともに原始多項式だから、$a'b = ab'u$ となる $u \in U(R)$ がある。従って、$c = b/a = (b'/a')u = c'u$。 ■

K の 2 元 c, c' について、$c' = cu$ となる $u \in U(R)$ が存在するとき、$c \approx c'$ と書く。このとき、$f(x) \in K[x]$ について、

- $f(x) \in R[x] \Leftrightarrow I(f) \in R$。
- $f(x)$ が原始多項式 $\Leftrightarrow I(f) \approx 1$。

補題 7.6 (1) 原始多項式の積は原始多項式。

(2) $f(x), g(x) \in K[x]$ ならば、$I(fg) \approx I(f)I(g)$。

証明 (1) $f(x) = a_0 + a_1x + \cdots + a_lx^l$、$g(x) = b_0 + b_1x + \cdots + b_mx^m$ を原始多項式、

$$h(x) = f(x)g(x) = c_0 + c_1x + \cdots + c_nx^n,\ p \mid c_i, ; i = 0, 1, \ldots, n$$

p は素元、とする。a_i のうち、p で割れない最小の i を i_0 とする。また、b_j のうち、p で割れない最小の j を j_0 とする。すると、

$$\begin{aligned} c_{i_0+j_0} &= a_0b_{i_0+j_0} + \cdots + a_{i_0-1}b_{j_0+1} + a_{i_0}b_{j_0} + a_{i_0+1}b_{j_0-1} + \cdots + a_{i_0+j_0}b_0 \\ &\equiv a_{i_0}b_{j_0} \ (\mathrm{mod}\ (p)) \\ &\not\equiv 0 \ (\mathrm{mod}\ (p)) \end{aligned}$$

(2) $f(x) = I(f)f_0(x)$、$g(x) = I(g)g_0(x)$ で、$f_0(x)$、$g_0(x)$ は原始多項式と書く。すると、$f(x)g(x) = I(f)I(g)f_0(x)g_0(x)$ で、$f_0(x)g_0(x)$ は、(1) より、原始多項式だから、$I(f)I(g) \approx I(fg)$。 ■

命題 7.7 $f(x) \in R[x]$ に対して、$f(x)$ が $R[x]$ の元として既約であることと、$K[x]$ の元として既約であることは同値である。

証明 $f(x)$ が $K[x]$ の元として既約ならば、$R[x]$ の元として既約であることは明らか。$K[x]$ において、$f(x) = g(x)h(x)$、$g(x), h(x) \in K[x]$ とする。ここで、$g(x) = I(g)g_0(x)$、$h(x) = I(h)h_0(x)$、$f_0(x), g_0(x)$ は原始多項式とすると、$f(x) = I(g)I(h)g_0(x)h_0(x)$、$f(x) \in R[x]$ より、$I(g)I(h) \approx I(gh) \in R$。従って、$\deg g_0 = \deg g = 0$ 又は、$\deg h_0 = \deg h = 0$。従って、$K[x]$ においても既約である。 ■

補題 7.8 $f(x)$ を $R[x]$ の素元とすると、次のいずれかが成立。

(i) $\deg f = 0$ で、f は R の素元。

(ii) $\deg f > 0$ で、f は既約な原始多項式。

証明　$U(R[x]) = U(R)$ である事に注意すると、かつ上の $(i), (ii)$ が素元であることは明か。

逆に $f(x)$ を素元とする。$f = gh$ とすると、g, h のいずれかは、$U(R[x]) = U(R)$ の元だから、$f \in R$ 又は、同じことだが $\deg f = 0$ ならば、f は、R の素元である。$\deg f > 0$ ならば、f は既約で、かつ $f = I(f)f_0$ より $I(f) \in U(R)$ となり f は原始多項式。従って、この場合は、(ii) が成立する。 ■

定理 7.4 の証明　$R[x_1, \ldots, x_{n-1}, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$ だから、$n = 1$ の場合、すなわち、R が一意分解整域の時、$R[x]$ が一意分解整域であることを示せばよい。

$0 \neq f(x) \in R[x]$ が素元分解可能であることを $\deg f$ に関する帰納法で示す。$\deg f = 0$ の時は、R が一意分解整域であるから、補題 7.8 (i) に注意すれば $R[x]$ の素元に分解できることが分かる。$\deg f > 0$ かつ可約の時は、$f = gh$、$\deg g > 0, \deg h > 0$ と表すと、$\deg g < \deg f$、$\deg h < \deg f$ だから、帰納法の仮定により、g、h ともに素元分解できる。従って、f も素元分解できる。そこで既約とする。すると、$f = I(f)f_0$、f_0 は原始多項式と書くと、f_0 は既約でもあるから、補題 7.8 (ii) により素元、後は、$I(f)$ に R における素元分解を適用すれば $R[x]$ における素元分解が得られる。

<u>一意性：</u>　$f = p_1 \cdots p_k f_1 \cdots f_l = q_1 \cdots q_m g_1 \cdots g_n$ を f の素元分解とし、$p_1, \ldots, p_k, q_1, \ldots, q_m \in R$、$f_1, \ldots, f_l, g_1, \ldots, g_n$ は次数が 1 以上の既約原始多項式とする。すると、$f_1 \cdots f_l$、$g_1 \cdots g_n$ は 補題 7.6 により、ともに原始多項式だから、

$$I(f) \approx p_1 \cdots p_k \approx q_1 \cdots q_m$$

を得、ある $u \in U(R)$ によって、$up_1 \cdots p_k = q_1 \cdots q_m$ と書けるから、R が一意分解整域であることより、この部分の一意性は得られる。一方、$K[x]$ は、体上の多項式環だからユークリッド整域、とくに一意分解整域で $uf_1 \cdots f_l = g_1 \cdots g_n$ に一意性を適用すると、適当に順番を入れ替えると、$c_i f_i = g_i$、$c_i \in K$ と書くことが出来る。$I(g_i) = 1$ だから $c_i \in R$ を得、g_i が原始多項式であることより、$c_i \in U(R)$ を得る。従って、分解は一意的である。 ■

8 加群

定義 8.1 R を環、M を加群とし、写像、

$$R \times M \to M,\ (r, m) \mapsto rm$$

が与えられ、次の条件を満たすとき、M を R-左加群（または単に R-加群）という。

$$r(x+y) = rx + ry,\ (r+s)x = rx + ry,\ (rs)x = r(sx),\ 1x = x$$

$(x, y \in M,\ r, s \in R)$。

- R-右加群も同様に定義される。R が可換の時は、単に R-加群と呼ぶ。
- $N \subset M$ が R-部分加群であるとは、N が 部分加群で、かつ、$rx \in N$ がすべての、$r \in R$、$x \in N$ について成り立つことを言う。$RN \subset N$ なる条件を N が R の作用で閉じているとか安定であるとも言う。
- $f : M \to M'$ が R-加群の準同型であるとは、

  $$f(a+b) = f(a) + f(b),\ f(ra) = rf(a),\ (r \in R,\ a, b \in M)$$

  を満たす時を言う。$f(ra) = rf(a)$ なる条件を、f は、R の作用と可換などとも言う。

例 8.1

1. 加群は、$\boldsymbol{Z}$-加群である。
2. 環 R は、R-加群であり、I が R-加群 R の部分加群であることと、I が R の左イデアルであることは同値である。
3. K を体としたとき、K-加群は、K-ベクトル空間の事である。

定義 8.2

1. M を R-加群、$S \subset M$ とするとき、

   $$< U > = \left\{ \sum_i r_i u_i \mid r_i \in R,\ u_i \in U \right\}$$

   を U で生成される R-部分加群という。
2. $|U| < \infty$ なる U について、$M = < U >$ となるとき、M を R-有限生成という。このときは、その生成元を $u_1, u_2, \ldots, u_n$ とすると、$M = Ru_1 + Ru_2 + \cdots + Ru_n$。
3. $r_1 u_1 + r_2 u_2 + \cdots + r_n u_n = 0$、$(r_i \in R)$ ならば、$r_1 = r_2 = \cdots = r_n = 0$ が成り立つとき、$u_1, u_2, \ldots, u_n$ は、R-自由であるという。M を生成する部分集合 U が R-自由（すなわち U の任意の有限部分集合が R-自由）であるとき、M は、U を基とする R-自由加群であるという。

- V を体 K 上の K-有限生成なベクトル空間とすると、V は K-自由加群で、その基に属する元の個数は基の解き方によらず一定である。

定義 8.3 R を 可換環とする。R-加群でかつ環である A が次の条件を満たすとき A は R 上の多元環（R-代数）であるという。

$$a, b \in A,\ r \in R \text{ に対し } (ra)b = a(rb) = r(ab).$$

例 8.2 1. R 上の全行列環は、R 多元環である。

2. $G = \{1 = u_1, u_2, \ldots, u_n\}$ を有限群とし、G の元を基とする R-自由加群 $R[G] = Ru_1 \oplus \cdots \oplus Ru_n$ に次のように積を定義したものを群環という。

$$\left(\sum_{i=1}^{n} \alpha_i u_i\right)\left(\sum_{j=1}^{n} \beta_j u_j\right) = \sum_{i,j=1}^{n} \alpha_i \beta_j u_i u_j.$$

G を有限群、$A = \boldsymbol{C}[G]$、V を A-加群とする。$g \in G$ のとき $\phi(g) : V \to V,\ (v \mapsto gv)$ とすると、$\phi(g) \in \mathrm{GL}(V)$、また、$\phi : G \to \mathrm{GL}(V),\ (g \mapsto \phi(g))$ は、群としての準同型である。逆に、群の準同型 $\phi : G \to GL(V)$ が与えられると、V は、A 加群となる。

M を R-加群とする。M が 0 と M 以外に部分加群を持たないとき、M を既約と言う。既約でないとき、可約と言う。

定理 8.1 (Schur's Lemma) M、N を共に既約 R-加群とする。

(1) $f : M \to N$ を R-準同型で恒等的に 0 でなければ、f は同型である。

(2) $End_R(M)$ で $M \to M$ なる準同型全体とすると、$End_R(M)$ は斜体となる。

証明　f を R-準同型とすると、$\mathrm{Ker}f$、$\mathrm{Im}f$ は、共に R-部分加群である。

(1) $f \neq 0$ とすると、$\mathrm{Ker}f \neq M$、$\mathrm{Im}f \neq 0$ だから $\mathrm{Ker}f = 0$、$\mathrm{Im}f = N$ となる。これは、f が同型写像であることを意味する。

(2) (1) より明か。 ■

9　ヒルベルトの基定理

定義 9.1　1. R-(左) 加群 M に対して、その R-部分加群の任意の空でない集合に極大 [極小] なものが存在するとき、M は、ネーター [アルチン] 加群であると言う。

2. 環 R が R-(左) 加群として、ネーター [アルチン] 環であるとき R は (左)-ネーター [アルチン] 環であるという。

3. M の R-部分加群の任意の列

$$M_1 \subset M_2 \subset \cdots \subset M_i \subset \cdots \ (M_1 \supset M_2 \supset \cdots \supset M_i \supset \cdots)$$

に対して、ある n が存在して、$M_n = M_{n+1} = \cdots$ となるとき、M は昇鎖律 [降鎖律] を満たすという。

命題 9.1 R-加群 M がネーター [アルチン] 加群であるという事と、M が昇鎖律 [降鎖律] を満たすことは同値である。

証明　R-加群 M がネーター加群だとする。$M_1 \subset M_2 \subset \cdots$ を部分加群の列とすると、$\{M_i \mid i \in \boldsymbol{N}\}$ の中に極大なもの M_n が存在するから、$M_n = M_{n+1} = \cdots$。逆に、空でない部分加群の族 S に極大なものが無ければ、$M_1 \subset M_2 \subset \cdots \subset M_i$ を真に増大する鎖として取る。すると、M_i は S の中で極大ではないから、$M_i \subset M_{i+1},\ M_i \neq M_{i+1}$ となるものを含む、これを続けていくと、真に増大する部分加群の無限列がとれるので昇鎖律を満たさない。アルチン加群であることと、降鎖律を満たすことが同値であることの証明も同様。 ■

命題 9.2 R-加群 M について、次は同値。

(i) M はネーター加群。

(ii) M の任意の R-部分加群は R-有限生成。

証明　$(i) \Rightarrow (ii)$　N を M の部分 R-加群、S を N の R-部分加群で、R-有限生成なもの全体とする。仮定から、S に極大元 N_0 が存在する。$N \neq N_0$ ならば、$x \in N - N_0$ とすると、$Rx + N_0$ は、有限生成でかつ N_0 を真に含むことになり N_0 の極大性に反するから $N = N_0$、すなわち、N も有限生成である。

$(ii) \Rightarrow (i)$ $M_1 \subset M_2 \subset \cdots$ を M の部分加群の列とする。$N = \bigcup_i M_i$ は、R-加群だから、仮定より有限生成で、$N =< u_1, u_2, \ldots, u_n >$ となる生成元があり、N の仮定よりある M_m にすべての $u_1, u_2, \ldots, u_n$ が入る。従って、

$$N \subset M_m \subset M_{m+1} \subset \cdots \subset N.$$

よって、M は昇鎖律を満たす。命題 9.1 により M はネーター加群である。 ■

系 9.3 単項イデアル整域は、ネーター環である。

証明　任意のイデアルは、1 個の元で生成されるから、明らか。 ■

定理 9.4 可換ネーター環 R 上の多項式環 $R[x_1, x_2, \ldots, x_n]$ はネーター環である。

証明　$n = 1$ の時を示せばよい。I を $R[x]$ のイデアルとする。

$$I_i = \{r \in R \mid f(x) = a_i x^i + \cdots + a_1 x + a_0 \in I \text{ で } a_i = r \text{ となるものがる。}\}$$

とおくと、これは R のイデアルである。また、$f(x) = a_i x^i + \cdots + a_1 x + a_0 \in I$ ならば、$xf(x) = a_i x^{i+1} + \cdots + a_1 x^2 + a_0 x \in I$ だから、$I_0 \subset I_1 \subset I_2 \subset \cdots$ である。仮定より、R はネーター環で、命題 9.1 より昇鎖律を満たすから $I_r = I_{r+1} = \cdots$ となる r が存在する。命題 9.2 により、各 $I_0, I_1, \ldots, I_r$ は有限生成だから、$a_{i_1}, \ldots, a_{i_{s_i}}$ を I_i $(i = 0, 1, \ldots, r)$ の R 上の生成元とする。f_{i_j} を最高次の係数が、a_{i_j} となる I の i 次多項式とする。このとき、これらが I を生成すること、すなわち次が成立することを示す。

$$I = \sum_{i=0}^{r} \sum_{j=1}^{s_i} R[x] f_{i_j}(x).$$

$f = a_m x^m + \cdots + a_1 x + a_0 \in I$ とし、$m = \deg f$ に関する帰納法で示す。

$m = 0$ ならば、$f = a_0 \in I_0 = \sum_{j=1}^{s_0} Ra_{0_j} = \sum_{j=1}^{s_0} Rf_{0_j}$ だから、この場合は良い。

$m > 0$ とする。$r < m$ の時は、$e = m - r$、$r \geq m$ の時は、$e = 0$ と置くことにすると、

$$a_m \in I_m = I_{m-e} = \sum_{j=1}^{s_{m-e}} Ra_{(m-e)_j}$$

だから、$a_m = \sum_{j=1}^{s_{m-e}} c_j a_{(m-e)_j}$ とすると、

$$\deg(f(x) - x^e \sum_{j=1}^{s_{m-e}} c_j f_{(m-e)_j}(x)) < \deg f(x)$$

だから、帰納法により、$f \in \sum_{i=0}^{r} \sum_{j=1}^{s_i} R[x] f_{i_j}(x)$ であることが分かった。

$R[x]$ の任意のイデアルが、有限生成だから、命題 9.2 より、$R[x]$ はネーター環である。
■

ネーター加群の剰余加群はネーター加群であることは簡単に分かるから、ネーター環の剰余環はネーター環である。可換環 S が 可換環 R を部分環として含み、さらに $s_1, \ldots, s_n \in S$ に対して、R と、$\{s_1, \ldots, s_n\}$ を含む S の部分環は、S であるとする。(このとき、$\{s_1, \ldots, s_n\}$ は、R-上 S を環として生成するという。例えば、$\boldsymbol{Z}[x]$ において、x は、$\boldsymbol{Z}$-上 $\boldsymbol{Z}[x]$ を環として生成するが、$\boldsymbol{Z}$-加群としては、$\boldsymbol{Z} + \boldsymbol{Z}x$ すなわち 1 次以下の多項式全体が生成されるものである。

系 9.5 可換ネーター環上有限生成な可換環はネーター環である。

証明　R を可換ネーター環とする。R-上有限生成な可換環は、R 上の多項式環の準同型像であるから、R 上の多項式環の剰余環と同型である。従って、ネーター環である。 ■