整数係数多項式環$\boldsymbol{Z}[x]$のイデアルについて

大塚美紀生

高校の数学では，多項式は係数を有理数や実数の範囲で考えることで，整数と同じように扱うのがふつうである(→[3])。(**初学者の方々には追って説明**するが，)ここで「同じように」というのは，有理数係数多項式の集合$\boldsymbol{Q}[x]$や実数係数多項式の集合$\boldsymbol{R}[x]$が，有理整数環$\boldsymbol{Z}$と同様「単項イデアル整域」の構造をもつということである。イデアルというのは倍数の集合の概念を一般化したものであり，平たく言えば倍数・約数の議論が同様にできるという意味である。その本質は，有理数や実数は商について閉じているので，どの2つの多項式も割り算ができるということにある。

ところが，係数を整数の範囲に制限すると，いつでも

$$a(x) = b(x)q(x) + r(x), \quad \deg r(x) < \deg b(x)$$

と表せるわけではなくなるので，高校数学のときとは様相が変わってくる。また，大学レベルの代数学の文献においても，一般論的な記述はあるものの，整数係数多項式環$\boldsymbol{Z}[x]$についての具体的記述はあまり見られない。

そこで，整数係数多項式環$\boldsymbol{Z}[x]$のイデアルが，どのような構造をしているかを，本稿では考察していくことにする。有理整数環$\boldsymbol{Z}$を一般の環の場合に広げて考えれば，可換環論における Noether 環や Hilbert Basis Theorem および素イデアルの height などへの手頃な導入書の役割も果たしてくれることであろう。

定理１ 整数係数多項式環$\boldsymbol{Z}[x]$のイデアルは，有限個の整数係数多項式 $f_1(x)$, $f_2(x)$, $\cdots$, $f_n(x)$ で生成され，$f_k(x)$ の最高次係数を a_k，次数を d_k とするとき

$$(a_1) \supsetneqq (a_2) \supsetneqq \cdots \supsetneqq (a_n), \quad d_1 > d_2 > \cdots > d_n$$

となるようにできる。ただし，$n = 1$ の場合や $f_n(x)$ が整数($d_n = 0$)となる場合もあり得る。

定理２ 整数係数多項式環$\boldsymbol{Z}[x]$の素イデアルは

(1) 素数pで生成される単項イデアル (p)

(2) primitive な既約多項式 $f(x) \in \boldsymbol{Z}[x]$ で生成される単項イデアル $(f(x))$

(3) 素数pと $\boldsymbol{Z}/p\boldsymbol{Z}$上既約な多項式 $f(x) \in \boldsymbol{Z}[x]$ により生成されるイデアル $(p,\ f(x))$

のいずれかである。

環についての基本事項

環とイデアルについて用語や概念を知らない人のために，本稿で必要となるものをひと通り述べておこうと思う。代数学を勉強した経験のある人は，予備知識の部分は読み飛ばして，定理の証明へと進んでいただいても差し支えない。

整数全体$\boldsymbol{Z}$のように，和と積が定義された集合を一般化したものは環と呼ばれる。きちんと述べると，集合Rが6条件

(1) 加法と乗法が定義されている；
$$x,\ y \in R \Longrightarrow x+y,\ xy \in R$$
(2) 加法について結合法則が成り立つ；
$$(x+y)+z = x+(y+z) \quad (x,\ y \in R)$$
(3) 加法について交換法則が成り立つ；
$$x+y = y+x \quad (x,\ y \in R)$$
(4) 零元0が存在する；
$$x+0 = 0+x = x \quad (x \in R)$$
(5) $x \in R$に対して加法の逆元$-x \in R$が存在する；
$$x+(-x) = (-x)+x = 0$$
(6) 加法と乗法について分配法則が成り立つ；
$$(x+y)z = xz+yz,\ \ x(y+z) = xy+xz$$

を満たすとき，Rは**環(ring)**であるという。一般には，環の乗法について交換法則は要求されない。(例えば，2次正方行列がなす環)

環Rが，さらに

(7) 乗法について可換；$xy = yx \quad (x,\ y \in R)$
(8) 単位元1が存在；$x\cdot 1 = 1\cdot x = x \quad (x \in R)$

を満たすとき，**可換環 (commutative ring)** であるという。

環Rにおいて，0でないRの元xがある0でないRの元yに対して$xy = 0$または$yx = 0$となるとき，xをRの**零因子 (zero divisor)** という。(このとき，yも零因子である。) 例えば，2次正方行列がなす環において
$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
であるから，$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$や$\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$は零因子である。これを踏まえて，零因子を持たない可換環を**整域 (integral domain** または **domain)** という。これから考察しようとしている有理整数環$\boldsymbol{Z}$や多項式環$\boldsymbol{Z}[x]$は，もちろん整域である。なお，整域の定義で可換環を前提とするのは，上の行列の例を見てもわかるように，非可換環においては$xy \neq 0$でも$yx = 0$となることが起こり得るからである。

一般の環に対して左イデアル，右イデアルなるものが定義できるが，本稿では可換環だけを対象として定義を述べることにすると，可換環Rの部分集合IがRの**イデアル (ideal)** であるとは，

(i) $a,\ b \in I \Longrightarrow a-b \in I$　　(ii) $r \in R,\ a \in I \Longrightarrow ra \in I$

が成り立つときにいう。イデアルは，整数の集合$\boldsymbol{Z}$における倍数の集合を概念化したものである。いま，可換環Rからn個の要素$a_1,\ a_2,\ \cdots,\ a_n$を選び，集合

$$(a_1,\ a_2,\ \cdots,\ a_n) = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \,|\, r_1,\ r_2,\ \cdots,\ r_n \in R\}$$

を考えると，イデアルになることは容易にわかる。このイデアル $(a_1,\ a_2,\ \cdots,\ a_n)$ を $a_1,\ a_2,\ \cdots,\ a_n$ により**生成される(generated)イデアル**といい，各 $a_k (k = 1,\ 2,\ \cdots,\ n)$ を**生成元(generator)**という。特に，一つの元(要素)から生成されるイデアルを**単項イデアル(principal ideal)**といい，すべてのイデアルが単項イデアルである整域を**単項イデアル整域(principal ideal domain** 略して **PID)**という。あとで示すように，有理整数環 $\boldsymbol{Z}$ は単項イデアル整域であり，定理 1 の文中にある $(a_1),\ (a_2),\ \cdots,\ (a_n)$ はそれぞれ $a_1,\ a_2,\ \cdots,\ a_n$ を生成元とする単項イデアルである。

整数における素数にあたるものを素元，素数の倍数の集合にあたるものを素イデアルという。それらは，素数の性質：

$$p \,|\, ab \implies p \,|\, a \text{ または } p \,|\, b$$

になぞらえて，次のように定義される。環 R のイデアル P が (0) でも R でもなく，

$$ab \in P \text{ ならば “} a \in P \text{ または } b \in P\text{”} \quad (a,\ b \in R)$$

が成り立つとき，P を**素イデアル (prime ideal)** という。環 R の要素 p について，単項イデアル (p) が素イデアルとなるとき，p を**素元 (prime element)** という。

乗法における逆元(いわゆる逆数)をもつ元(要素)を **可逆元**または**単数 (unit)** という。有理整数環 $\boldsymbol{Z}$ においては，± 1 が単数(可逆元)である。(整数もそうであるが，) 環は一般には商について閉じてはいないので，環においては可逆元を考えるということは大変重要になる。0 でないすべての要素が可逆元である環を特に**体 (field)** という。有理数の集合 $\boldsymbol{Q}$ および実数の集合 $\boldsymbol{R}$ は(通常の加法と乗法について)体であり，それぞれ有理数体，実数体と呼ばれる。高校数学流に言えば，体とは四則演算について閉じている数の集合のことである。

補題１ 環 R のイデアル I が可逆元を含めば，$I = R$ である。

(**証明**) I が可逆元 u を含むとすると，u の逆元 $u^{-1} \in R$ が存在するから，イデアルの性質より

$$1 = uu^{-1} \in I$$

任意の $r \in R$ に対して

$$r = r \cdot 1 \in I$$

となるから，$R \subset I$ である。もともと $I \subset R$ であるから，$I = R$ である。

(証明おわり)

x を不定元(変数)として，環 R の要素を係数とする多項式の集合は，環 R から誘導される加法と乗法により環となる。

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad (a_i \in R)$$
$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \quad (b_j \in R)$$

に対して，$i > n$ のときは $a_i = 0$，$j > m$ のときは $b_j = 0$ と表すことにすると，

$$f(x)+g(x)=\sum_{k=0}^{M}(a_k+b_k)x^k \quad (M=\max\{n,\ m\})$$
$$f(x)g(x)=\sum_{k=0}^{n+m}c_kx^k,\ \ c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0$$

により和と積が(R の演算法則だけで)定義される。この多項式からなる環を(x を変数とする)R 上の**多項式環 (polynomial ring)** といい，$R[x]$ で表す。

$\boldsymbol{Z}$, $\boldsymbol{Z[x]}$ に関する予備知識

整数全体の集合$\boldsymbol{Z}$は，通常の加法と乗法により環をなす。この環は**有理整数環(the ring of rational integers)**と呼ばれる。「有理」とつけるのは，代数的整数(環)と区別するためと代数的整数と有理数のちょうど共通部分となることに起因するが，本稿では代数的整数について深入りしないことにする。

補題２　有理整数環 Z は，単項イデアル整域である。

(**証明**)　$\boldsymbol{Z}$の任意のイデアルを I とし，I に属する正で最小の整数を a とする。I に属する任意の整数 b に対して，整数の性質より

$$b=aq+r,\ \ 0\leqq r<a$$

を満たす整数 $q,\ r$ がただ一つ存在する。イデアルの性質より

$$r=b-aq\in I$$

であるが，a は I に属する正の最小整数であるから

$$r=0$$

となる。よって，

$$b=aq\in(a)$$

であり，b は任意であったから $I\subset(a)$ となるが，$a\in I$ より $(a)\subset I$ であるから

$$I=(a)$$ (証明おわり)

体を係数とする多項式環であれば，補題２と同様の性質が成り立つ。証明も補題２と同様の手法が通用する。このことは，高校数学で「整式(多項式)が整数と同様に扱える」ことの本質的な部分を物語っている。

補題３　体 K を係数とする多項式環 $K[x]$ は，単項イデアル整域である。

(**証明**)　$K[x]$ の任意のイデアルを I とし，I に属する 0 でない最小次数の多項式を $A(x)$ とする。$A(x)$ の最高次係数が 0 でないことと 0 でない K の元(要素)は可逆元であるから，整数と同様に必ず $A(x)$ で割ることができる。したがって，任意の I に属する多項式 $B(x)$ に対して

$$B(x)=A(x)Q(x)+R(x),\ \ \deg R(x)<\deg A(x)$$

を満たす多項式 $Q(x),\ R(x) \in K[x]$ が(0でない)定数倍の違いを除いてただ一つに定まる。ここで，degは次数を表す記号である。イデアルの性質より

$$R(x) = B(x) - A(x)Q(x) \in K[x]$$

であるが，$A(x)$ は I に属する 0でない最小次数の多項式であるから

$$R(x) \equiv 0 \quad (\text{恒等的に } 0,\ R(x)\text{そのものが定数 } 0)$$

となる。よって，

$$B(x) = A(x)Q(x) \qquad \therefore\ I = (A(x)) \qquad (\text{証明おわり})$$

イデアルがすべて単項イデアルであるということは，公約数が考えられるということである。そこで，次の基本性質が成り立つ。

補題４ a と bが互いに素な整数であるとき，

$$am + bn = 1$$

を満たす整数 $m,\ n$ が存在する。

(**証明**) 補題２より $\boldsymbol{Z}$は単項イデアル整域であるから，

$$(a,\ b) = (d)$$

を満たす整数 d が存在する。$a \in (d),\ b \in (d)$ より

$$a = rd,\ \ b = sd \quad (r,\ s \in \boldsymbol{Z})$$

と表される。a と b は互いに素であるから $d = \pm 1$ であり，

$$(a,\ b) = (1)$$

特に，$1 \in (a,\ b)$ であるから

$$am + bn = 1$$

を満たす整数 $m,\ n$ が存在する。 (証明おわり)

補題５ $A(x)$ と $B(x)$ が 1 次以上の共通因数をもたない体 K 上の 0でない多項式であるとき，

$$A(x)M(x) + B(x)N(x) = 1$$

を満たす体 K 上の多項式 $M(x),\ N(x)$ が存在する。

(**証明**) 補題３より $K[x]$ は単項イデアル整域であるから，

$$(A(x),\ B(x)) = (D(x))$$

を満たす体 K 上の多項式 $D(x)$ が存在する。$A(x) \in (D(x)),\ B(x) \in (D(x))$ より

$$A(x) = R(x)D(x),\ \ B(x) = S(x)D(x) \quad (R(x),\ S(x) \in K[x])$$

と表される。$A(x)$ と $B(x)$ は 1 次以上の共通因数をもたず，零多項式でないから

$$D(x) = k \in K,\ \ k \neq 0$$

であり，$k^{-1} \in K$ より

$$(A(x),\ B(x)) = (k) = (1)$$

特に，$1 \in (A(x),\ B(x))$ であるから

$$A(x)M(x)+B(x)N(x)=1$$

を満たす体 K 上の多項式 $M(x),\ N(x)$ が存在する。　　(証明おわり)

有理整数環$\boldsymbol{Z}$においては，素数で生成されるイデアルが素イデアルとなるが，その素イデアルは極大イデアルとなる。一般の可換環 R においては，素イデアルが極大イデアルとは限らない。まだ証明はしていないが，定理２の結果を認めるならば，p を素数とすると $\boldsymbol{Z}[x]$ において (p) は素イデアルであるが，

$$(p)\subsetneqq(p,\ f(x))\subsetneqq\boldsymbol{Z}[x]$$

であるから，(p) は$\boldsymbol{Z}[x]$ においては極大イデアルではない。

補題６　有理整数環$\boldsymbol{Z}$において

$$p\text{が素数}\iff(p)\text{が}\boldsymbol{Z}\text{の素イデアル}$$

であり，素イデアル(p)を含む$\boldsymbol{Z}$のイデアルは (p)または(1)だけである。

(**証明**) 前半部分は，素数の性質そのものである。

I を $(p)\subsetneqq I\subset\boldsymbol{Z}$ であるイデアルとすると，

$$q\notin(p),\ q\in I$$

を満たす整数 q が存在する。p は素数で $q\notin(p)$であるから，p と q は互いに素であり，補題４より

$$pm+qn=1$$

を満たす整数 $m,\ n$ が存在する。よって，

$$1\in(p,\ q)\subset I$$

であるから，補題１より $I=(1)=\boldsymbol{Z}$ である。　　(証明おわり)

整数を自然数 n で割った余りで分類して

$$a\equiv b\pmod n\iff n\,|\,a-b$$

により関係 $\equiv$ を定めると，$\equiv$ は同値関係となる。この同値関係 $\equiv$ により同値類別するとき，その各同値類は **nを法とする剰余類 (residue class modulo n)** または剰余合同類と呼ばれる。剰余類の集合は $\boldsymbol{Z}$ から誘導される演算により環をなす。実際，

$$\begin{aligned}&a\equiv\alpha\pmod n,\quad b\equiv\beta\pmod n\\ \iff\ &n\,|\,a-\alpha,\quad n\,|\,b-\beta\\ \Longrightarrow\ &(a+b)-(\alpha-\beta)=(a-\alpha)+(b-\beta)\equiv0\pmod n\\ &ab-\alpha\beta=(a-\alpha)b+\alpha(b-\beta)\equiv0\pmod n\\ \iff\ &a+b\equiv\alpha+\beta\pmod n,\quad ab\equiv\alpha\beta\pmod n\end{aligned}$$

により和と積が矛盾なく定義され，それ以外の環の条件が成り立つことは明らかである。n を法とする剰余類がなす環を**剰余環(residue ring)**といい，$\boldsymbol{Z}/n\boldsymbol{Z}$ または $\boldsymbol{Z}/(n)$ で表す。可換環論の立場では，イデアル(n)による**商環(quotient ring)**という。

補題７　pを素数とするとき，$\boldsymbol{Z}/p\boldsymbol{Z}$は体である。

(**証明**) 環であることはわかっているので，任意の 0 でない元(要素)が可逆元(単数)であることだけ示せばよい。

整数 a と同値な類を $\overline{a}$で表すことにして，$\overline{a}$が$\boldsymbol{Z}/p\boldsymbol{Z}$の 0 でない元であるとすれば，

$$a \not\equiv 0 \pmod{p}$$

であるから，a と p は互いに素である。補題４より

$$ab + pq = 1$$

を満たす整数 $b,\ q$ が存在するから

$$ab \equiv 1 \pmod{p} \qquad \therefore\ \overline{a}\,\overline{b} = 1$$

となって，0でない$\overline{a}$は$\boldsymbol{Z}/p\boldsymbol{Z}$における可逆元である。　　(証明おわり)

多項式

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \boldsymbol{Z}[x]$$

の係数の最大公約数$gcd(a_0,\ a_1,\ \cdots,\ a_n)$を$f(x)$の**content**といい，$f(x)$の contentが１であるとき，$f(x)$は**primitive**であるという。primitiveは「原始的」とも訳されるが，そのニュアンスはここでの意味とはマッチしないので，本稿ではそのままprimitiveと表すことにする。なお，contentの(代数学の用語としての)和訳を筆者は知らない。

高校数学において $f(x)$が既約多項式であるとは，$f(x)$ より次数が低い１次以上の因数を持たない多項式のことであるが，それは暗に係数が実数や複素数などの体であることを前提としている。係数が体でない多項式環やさらに一般の可換環 Rにおいては，因数を持たないという既約の意味をもう少し精密に定義する必要がある。

一般の可換環 Rにおいて，Rの元(要素) aが**既約(irreducible)**であるとは，aは 0 でも可逆元でもなく，$a = bc\ (b,\ c \in R)$ ならば b または cが可逆元になるときにいう。

$\boldsymbol{Z}[x]$において可逆元(単数)は± 1であるから，$\boldsymbol{Z}[x]$における既約元は素数であるか，または定数でない低い次数の因数を持たない primitive な多項式である。

補題８　pを素数とする。$\boldsymbol{Z}[x]$において

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$
$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

がともに pで割り切れないならば，$f(x)g(x)$ も pで割り切れない。

(**証明**) $f(x),\ g(x)$がともに pで割り切れないとすれば，それぞれ pで割り切れない係数が少なくとも一つ存在する。pで割り切れない$f(x)$の最低次係数をa_i，pで割り切れない$g(x)$の最低次係数をb_jとすると，$f(x)g(x)$のx^{i+j}の係数

$$\begin{aligned} c_{i+j} = {} & (a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_{i-1}b_{j+1}) \\ & + a_ib_j + (a_{i+1}b_{j-1} + \cdots + a_{i+j-1}b_1 + a_{i+j}b_0) \end{aligned}$$

において，a_ib_j 以外は pで割り切れ，a_ib_j は pで割り切れないから，c_{i+j} は pで割り切れない。よって，$f(x)g(x)$ は pで割り切れない。　　(証明おわり)

補題９　$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ が $\boldsymbol{Z}[x]$ において既約ならば，$\boldsymbol{Q}[x]$ においても既約である。

(**証明**)　$f(x)$ より次数が低い $g(x),\ h(x)\in\boldsymbol{Q}[x]$ を用いて

$$f(x)=g(x)h(x)$$

と表されるとする。$g(x),\ h(x)$ の係数(を既約分数で表したとき)の分母の最小公倍数をそれぞれ $b,\ c$ とすると，

$$b\cdot g(x),\ \ c\cdot h(x)\in\boldsymbol{Z}[x]\ \text{はともに primitive}$$

となるから，補題８(の対偶)より

$$bc\cdot f(x)=\{b\cdot g(x)\}\{c\cdot h(x)\}\ \text{は primitive}$$

であり，

$$bc=\pm1\qquad\therefore\ \ b=\pm1,\ \ c=\pm1\ \text{（複号任意）}$$

である。ゆえに，

$$g(x),\ \ h(x)\in\boldsymbol{Z}[x]$$

となって，$f(x)$ は $\boldsymbol{Z}[x]$ においても既約ではない。

以上の対偶をとると，$\boldsymbol{Z}[x]$ において既約ならば，$\boldsymbol{Q}[x]$ においても既約である。

(証明おわり)

定理１の証明

I を $\boldsymbol{Z}[x]$ のイデアルとし，I に属するすべての多項式(定数も含む)の最高次係数から成る集合を J_1 とする。

$a,\ b\in J_1$ とすると，ある I に属する多項式

$$f(x)=ax^n+\cdots,\ \ g(x)=bx^m+\cdots$$

が存在する。I はイデアルであるから，$n\geqq m$ のときは

$$f(x)-x^{n-m}g(x)=(a-b)x^n+\cdots\in I,$$

$n\leqq m$ のときは

$$x^{m-n}f(x)-g(x)=(a-b)x^m+\cdots\in I$$

であり，J_1 の定め方より

$$a-b\in J_1$$

である。

$a\in J_1$ に対して，a を最高次係数とする I の多項式 $f(x)=ax^n+\cdots$ が存在し，$c\in\boldsymbol{Z}$とすると，I は $\boldsymbol{Z}[x]$ のイデアルであるから

$$cf(x)=cax^n+\cdots\in I$$

J_1 の定め方より

$$ca\in J_1$$

よって，J_1 は $\boldsymbol{Z}$ のイデアルとなるから，補題２より

$$J_1=(a_1)$$

となる整数 a_1 が存在する。J_1 の定め方より，a_1 を最高次係数とする I の多項式が存

在するが，その中で最低次のものを $f_1(x)$ とし，その次数を d_1 とする。

ここで，

$$I = (f_1(x))$$

が成り立てば定理１の証明は終わるので，

$$I \supsetneqq (f_1(x))$$

のときを考える。このとき，J_1 の定め方より，I に属するすべての多項式の最高次係数は a_1 で割り切れるので，I に属する d_1 次以上の任意の多項式 $f(x)$ は $f_1(x)$ で割ることができて，

$$f(x) = f_1(x)q_1(x) + r_1(x), \quad \deg r_1(x) < d_1 = \deg f_1(x)$$

と表す $q_1(x),\ r_1(x) \in \boldsymbol{Z}[x]$ が存在する。ここで，$\deg$ は次数を表す記号である。

I はイデアルであるから

$$r_1(x) = f(x) - f_1(x)q_1(x) \in I$$

であり，$d_1 = \deg f_1$ の最小性より

$$r_1(x) \equiv 0 \ \text{ または } \ r_1(x) \text{ の最高次係数が } a_1 \text{と単数でない整数との積}$$

であることがわかる。

そこで，I に属する d_1 より低次の多項式($(f_1) \subsetneqq I$ より実際に存在)の最高次係数から成る集合を J_2 とすると，J_1 と同様にして，

$$J_2 = (a_2)$$

を満たす整数 a_2 が存在し，a_2 を最高次係数とする I の多項式の中で最低次のものを $f_2(x)$ とする。$f_2(x)$の次数を d_2 とすると，

$$J_1 = (a_1) \supsetneqq J_2 = (a_2), \quad d_1 > d_2$$

である。

$I = (f_1(x),\ f_2(x))$ でなければ，同様にして $\boldsymbol{Z}$のイデアル $J_3 = (a_3)$ と最高次係数を a_3 とする最低次の多項式 $f_3(x)$ を定め，以下この作業を繰り返していく。ところが，次数は 0 以上の整数であるからこの作業は有限回で終了し，ある自然数 n が存在して

$$I = (f_1(x),\ f_2(x),\ \cdots,\ f_n(x)), \quad (a_1) \supsetneqq (a_2 \supsetneqq \cdots \supsetneqq (a_n),$$
$$d_1 = \deg f_1(x) > d_2 = \deg f_2(x) > \cdots > d_n = \deg f_n(x)$$

となる。　　(定理１の証明おわり)

定理２の証明

$\boldsymbol{Z}[x]$ の素イデアルを P とする。定理１より

$$P = (f_1(x),\ f_2(x),\ \cdots,\ f_n(x)),$$
$$\text{ただし，}\ f_k(x) = a_k x^{d_k} + (d_k - 1 \text{ 次以下}) \in \boldsymbol{Z}[x],$$
$$(a_1) \supsetneqq (a_2) \supsetneqq \cdots \supsetneqq (a_n), \quad d_1 > d_2 > \cdots > d_n$$

と表される。P は素イデアルであるから，定理１の条件を考慮しなければ，各 $f_k(x)$ は素元，すなわち

$f_k(x)$ は素数(0 次多項式)または(primitive な)既約多項式

にとることができるが，定理 1 の条件が付加できることを示す。

$f_1(x)$ の content を c_1 とすると，

$$f_1(x) = c_1 g_1(x) \quad (c_1 \in \boldsymbol{Z},\ g_1(x) \in \boldsymbol{Z}[x] \text{ は primitive})$$

と表される。P は素イデアルであるから，$f_1(x) \in P$ より

$$c_1 \in P \ \text{ または } \ g_1(x) \in P$$

$c_1 \in P$ のとき $c_1 \in (a_n) \subset (a_1)$ である。一方，a_1 は $f_1(x)$ の最高次係数であるから $c_1 \,|\, a_1$ であり，$(a_1) \subset (c_1)$ となるから

$$(c_1) = (a_n) = (a_1) \qquad \therefore \ P = (a_1)$$

となる。このとき，$a_1 = st\ (s,\ t \in \boldsymbol{Z})$ とすると，$P = (a_1)$ は素イデアルであるから，$s \in (a_1)$ または $t \in (a_1)$ であり，a_1 (または $-a_1$)は素数である。

$g_1(x) \in P$ のとき，イデアル (a_1) の定め方より $g_1(x)$ の最高次係数は $\pm a_1$ であるから，$f_1(x) = g_1(x)$ としてよい。$f_1(x)$ が $\boldsymbol{Z}[x]$ における因数を持つとすれば，a_1 の約数を最高次係数とする多項式であるから，$f_1(x)$ の次数の最小性より，$f_1(x)$ は単数(± 1)倍の違いを除いて 1 と $f_1(x)$ 以外に因数を持たない。したがって，$f_1(x)$ は(primitive な)既約多項式である。このとき，イデアル (a_k) の最大性と次数 d_k の最小性より，$f_n(x)$ まで同じ議論が続けられる。

以上により，素イデアル P は

$$P = (f_1(x),\ f_2(x),\ \cdots,\ f_n(x)),$$

$f_k(x) = a_k x^{d_k} + (d_k - 1 \text{ 次以下})$ は

素数(0 次多項式)または(primitive な)既約多項式,

$$(a_1) \supsetneqq (a_2) \supsetneqq \cdots \supsetneqq (a_n),\quad d_1 > d_2 > \cdots > d_n$$

と表されることを前提として，定理 2 の証明を行なうことができる。

まず，$d_1 > d_2 \geqq 1$ と仮定して矛盾を導く。$f_1(x)$ と $f_2(x)$ は次数が異なる(primitive な)既約多項式であるから，補題 9 より $\boldsymbol{Q}[x]$ においても既約多項式であり，次数が異なることより互いに素である。補題 5 より

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

を満たす $g_1(x),\ g_2(x) \in \boldsymbol{Q}[x]$ が存在する。

このとき，ある整数 b に対して $bg_1(x),\ bg_2(x)$ は整数係数となって，

$$f_1(x)\cdot bg_1(x) + f_2(x)\cdot bg_2(x) = b \quad (bg_1(x),\ bg_2(x) \in \boldsymbol{Z}[x])$$

と表されるから $b \in (f_1(x),\ f_2(x)) \subset P$ であり，

$$d_n = 0,\quad a_n = f_n(x) \text{ は素数 } \ (n \geqq 3)$$

となる。

$$(a_1) \supsetneqq (a_2) \supsetneqq (a_n)$$

であるから，補題 6 より a_2 は単数で $(a_2) = \boldsymbol{Z}$ となり，$(a_1) \supsetneqq (a_2)$ は成り立たない。

よって，

$$n = 1 \ \text{ または } \ d_1 > d_2 = 0$$

が成り立ち，$n=1$ のときは (1) または (2) となり，$d_1 > d_2 = 0$ のとき

$$P = (f_1(x),\ p) \quad (p \text{ は素数})$$

と表される。ここで，$f_1(x)$ より低い次数で定数でない $g(x),\ h(x) \in \boldsymbol{Z}[x]$ を用いて

$$f_1(x) \equiv g(x)h(x) \pmod{p}$$

と表されるとすれば，$g(x)$ も $h(x)$ も $P = (f_1(x),\ p)$ に属さないから P が素イデアルであることに反する。よって，$f_1(x)$ は $\boldsymbol{Z}/p\boldsymbol{Z}$ 上でも既約であり，$d_1 > d_2 = 0$ のときは (3)の形になる。以上により，必要条件が示された。

以下，(1), (2), (3)の形のイデアルが実際素イデアルになること(十分条件)を示す。

(1) 補題８より，素数 p で生成される $\boldsymbol{Z}[x]$ のイデアルは素イデアルである。

(2) $\boldsymbol{Z}[x]$において $f(x) \mid g(x)h(x),\ f(x) \nmid g(x)$ $(g(x),\ h(x) \in \boldsymbol{Z}[x])$であるとする。

$g(x)$が定数ならば，$f(x)$が primitiveであることより $f(x) \mid h(x)$ となるから，$g(x)$が(1 次以上の)多項式である場合を考える。

補題９より，$f(x)$ は $\boldsymbol{Q}[x]$ においても既約であるから，$f(x)$ と $g(x)$ は $\boldsymbol{Q}[x]$ において互いに素である。補題５より

$$f(x)s(x) + g(x)t(x) = 1$$

を満たす $s(x),\ t(x) \in \boldsymbol{Q}[x]$ が存在する。ある整数 c が存在して

$$a(x) = c\cdot s(x),\ \ b(x) = c\cdot t(x) \in \boldsymbol{Z}[x],$$
$$f(x)a(x) + g(x)b(x) = c$$

と表されるから，

$$c\cdot h(x) = f(x)a(x)h(x) + g(x)h(x)\cdot b(x)$$

である。$\boldsymbol{Z}[x]$ において $f(x) \mid g(x)h(x)$ であるから

$$f(x) \mid c\cdot h(x)$$

であり，$f(x)$ は primitiveであるから

$$f(x) \mid h(x)$$

となる。よって，$\boldsymbol{Z}[x]$ において $P = (f(x))$ は素イデアルである。

(3) 多項式 $y(x) \in \boldsymbol{Z}[x]$ を $(\boldsymbol{Z}/p\boldsymbol{Z})[x]$ において考えるときは $\overline{y}\,(x)$ と表すことにする。

$g(x)h(x) \in (p,\ f(x)),\ g(x) \notin (p,\ f(x))$ とすると，$(\boldsymbol{Z}/p\boldsymbol{Z})[x]$ において

$$\overline{g}\,(x)\,\overline{h}\,(x) \in (\overline{f}\,(x))$$

である。補題７より $\boldsymbol{Z}/p\boldsymbol{Z}$ は体であり，$\overline{f}\,(x)$ は $\boldsymbol{Z}/p\boldsymbol{Z}[x]$ において既約であるから，$\overline{f}\,(x) \nmid \overline{g}\,(x)$ より $\overline{f}\,(x)$ と $\overline{g}\,(x)$ は互いに素である。よって，補題５より

$$\overline{f}\,(x)\,\overline{u}\,(x) + \overline{g}\,(x)\,\overline{v}\,(x) = 1$$

を満たす $u(x),\ v(x) \in \boldsymbol{Z}[x]$ が存在し，

$$\overline{h}\,(x) = \overline{f}\,(x)\,\overline{u}\,(x)\,\overline{h}\,(x) + \overline{g}\,(x)\,\overline{h}\,(x)\cdot\overline{v}\,(x) \in (\overline{f}\,(x))$$
$$\therefore\ \ h(x) \in (p,\ f(x))$$

よって，$\boldsymbol{Z}[x]$ において $P = (p,\ f(x))$ は素イデアルである。

(定理２の証明おわり)

参考文献

[1] J.J.Watkins, *Topics in commutative ring theory*,
Princeton University Press (2007)

[2] 藤崎源二郎, 体とガロア理論, 岩波書店(1991).

[3] 大塚美紀生, 定数倍はなぜ無視されるのか？, 早稲田数学フォーラム.
(http://homepage2.nifty.com/wasmath/constant=unit.pdf)

2008.2.16