Eisensteinの判定法

$R[x]$での分解と$K[x]$での分解のちがいの程度がテーマになる.

例: $R=\mathbb{Z}$, $K=\mathbb{Q}$　$p|ab \Rightarrow p|a$ or $p|b$

準備 UFD Rを整域とし, Kはその商体(分数体)であると仮定する.

$p\in R$, $p\neq 0$ に対して, $(p)=Rp$ がRの素イデアルになるとき, pはRの<u>素元</u>であるという.

$p\in R$ が $p\notin R^\times$ をみたし, $R^\times$の元と$R^\times p$の元以外に約数を持たないとき, pはRの<u>既約元</u>であるという. ($K[x]$の既約元と$K[x]$に含まれる<u>既約多項式</u>は一致する.)

注意 整域の素元は常に既約元になるが一般には逆は成立しない. □

以下の2つの同値な条件のどちらかが成立しているとき, Rは<u>一意分解整域</u>(<u>unique factorization domain</u>, <u>UFD</u>)であるという: (同値性(a)$\Leftrightarrow$(b)は非自明!)

(a) $a\in R$, $a\neq 0$ のとき, $a=p_1\cdots p_n$ (p_iはRの<u>既約元</u>)と書け, $p_1,\dots,p_n$は順序とRの可逆元倍のちがいを除いて一意に定まる.

(b) $a\in R$, $a\neq 0$ のとき, $a=p_1\cdots p_n$ (p_iはRの<u>素元</u>)と書ける.

注意 UFDの既約元は常に素元になるので, UFDにおいて素元と既約元は同じものになる. □

UFDについて色々非自明なことはあるが，素因数分解の存在と(積の順序と可逆元倍のちがいを除いた)一意性が成立している整域のことであり，素元と既約元という2種類の素数の一般化が一致している整域であることを認識していれば，この演習について行くためには十分だと思われる．

以下をみとめて使って良いことにする：

- PID は UFD である．
- たとえば $\mathbb{Z}$ や体 K 上の1変数多項式環 $K[x]$ は PID なので UFD である．
- R が UFD のとき，$R[x]$ や $R[[x]]$ も UFD である．

みとめて使ってよい

我々は特に $\mathbb{Z}$ と $\mathbb{Q}$ の組を例として多用する．

以下，R は UFD であるとし，K はその商体であるとする．　UFD に話を制限

$f(x)=\sum a_i x^i \in R[x]$ の係数 $a_0, a_1, a_2, \ldots$ (有限個を除いて 0) の最大公約数が 1 のとき，
$f(x)$ は R 上の原始多項式であるという．

正確には「R 可逆元」

たとえば $f(x)=6x^2+10x+15$ は $\mathbb{Z}$ 上の原始多項式である．
しかし，$g(x)=2f(x)=12x^2+20x+30$ はそうではない．　R[x] 内の話

$\boxed{f \in K[x] \text{ の内容}}$　→ K[x] も出て来る．

$f(x)=\sum_i a_i x^i \in K[x]$，$f(x) \neq 0$ のとき，a_i の中の分母をまとめることによって，
$f(x)=\frac{1}{b}\sum_i c_i x^i$，$b, c_i \in R$ と書ける．c_i たちの最大公約数を d と書き，
$c_i = dc'_i$，$c'_i \in R$ と表わすとき，$f_0(x)=\sum_i c'_i x^i$ は原始多項式になり，
$c=\frac{d}{b} \in K$ とおくと，$f(x)=c f_0(x)$．　← $f(x)$ は K の元と R 上の原始多項式の積で書ける．

c を $f(x)$ の内容とよぶ

内容 c の一意性

$cf_0(x) = \tilde{c}\tilde{f}_0(x)$, $\tilde{f}_0(x)$ は R上の原始多項式で $\tilde{c} \in K$ と仮定する. $c = \frac{b}{a}$, $\tilde{c} = \frac{\tilde{b}}{\tilde{a}}$,
$a, b, \tilde{a}, \tilde{b} \in R$, a と b は互いに素, $\tilde{a}$ と $\tilde{b}$ は互いに素と書け, $\tilde{a}bf_0(x) = a\tilde{b}\tilde{f}_0(x)$,
両辺の係数の最大公約数はそれぞれ $\tilde{a}b$, $a\tilde{b}$ になる. a と b が互いに素で
$\tilde{a}$ と $\tilde{b}$ が互いに素なことより, $\tilde{a}$, $\tilde{b}$ はそれぞれ a, b の R の可逆元倍になる.

これで, $0 \neq f(x) \in K[x]$ のとき, ある $c \in K^\times$ と R上の原始多項式 $f_0(x)$ で
$f(x) = cf_0(x)$ をみたすものが, R の可逆倍を除いて一意的に定まることが
わかった. このような c を f の内容と呼ぶ.

f の内容の1つを $I(f)$ と書こう. ← $I(f)$ の定義

たとえば $f(x) = \frac{12}{7}x^2 + \frac{20}{7}x + \frac{30}{7} = \frac{2}{7}(6x^2 + 10x + 15)$ より, $I(f) = \frac{2}{7}$ ととれる.

$\boxed{\text{Gaussの補題}}$ RはUFDであるとし，Kはその商体であると仮定する．

このとき，R上の原始多項式の積はR上の原始多項式になり，

$f, g \in K[x]$, $f \neq 0$, $g \neq 0$ に対して，$I(fg)$ と $I(f)I(g)$ はRの可逆元倍のちがいを除いて等しい．

$\boxed{\text{証明}}$ 内容のRの可逆元倍を除いた一意性と $fg = I(f)I(g)f_0 g_0$ (f_0, g_0 はR上の原始多項式) より，$f_0 g_0$ もR上の原始多項式ならば $I(fg)$ は $I(f)I(g)$ のRの可逆元倍になる．

$f, g \in R[x]$ は原始多項式であるとする．$f(x) = \sum_i a_i x^i$, $g(x) = \sum_j b_j x^j$, $a_i, b_j \in R$ と書く，

pはRの任意の素元であるとする． ← ポイント（"mod p" で考える！）

f, g は原始多項式なのである s, t が存在して，a_s, b_t は p で割り切れない．

s, t として，そのようなものの中で最小のものをとると，

$$(fg\text{の } x^{s+t} \text{ の係数}) = \underbrace{a_0 b_{s+t} + \cdots + a_{s-1} b_{t+1}}_{\substack{a_0, \dots, a_{s-1}\text{ が}\\ p\text{で割り切れる}}} + \underbrace{a_s b_t}_{\substack{p\text{で割り}\\ \text{切れない．}}} + \underbrace{a_{s+1} b_{t-1} + \cdots + a_{s+t} b_0}_{\substack{b_0, \dots, b_{t-1}\text{ が}\\ p\text{で割り切れる}}}$$

pで割り切れない．

となるので，fg の係数で p で割り切れないものが存在する．

これより，fg がR上の原始多項式であることがわかる． $\boxed{\text{q.e.d.}}$

(注) 自然な射影 $\pi_p : R[x] \to R[x]/(p) = (R/(p))[x]$ を使えばもっとわかりやすくなる．

準備したかった結果 R は UFD であり，K はその商体であると仮定する．

$R[x]$ に含まれる多項式で1次以上の2つの $R[x]$ の元の積に分解されないものは，$K[x]$ における既約多項式になる．

たとえば，$\mathbb{Z}$ 係数多項式で1次以上の2つの $\mathbb{Z}$ 係数多項式の積に分解されないものは1次以上の2つの $\mathbb{Q}$ 係数多項式の積にも分解されない．

証明 $h \in R[x]$ が $h = fg$, $f, g \in K[x]$, $\deg f \geqq 1$, $\deg g \geqq 1$ と分解されると仮定する．
$f = I(f) f_0$, $g = I(g) g_0$, $h = I(h) h_0$, f_0, g_0, h_0 は R 上の原始多項式と書ける．
$h \in R[x]$ より，$I(h) \in R$ であることに注意せよ．

Gauss の補題より，$I(h) = a I(f) I(g)$, $a \in R^\times$ と書けるので

$$I(f) I(g) f_0 g_0 = fg = h = I(h) h_0 = a I(f) I(g) h_0,$$

$$\therefore\ h_0 = a^{-1} f_0 g_0, \quad h = I(h) a^{-1} f_0 g_0.$$ ← これは h の $R[x]$ 内での分解

したがって，h は $R[x]$ でも1次以上の多項式の積に分解される．
以上の対偶をとれば上の結果が得られる　□

勉強の仕方 $R = \mathbb{Z}$, $K = \mathbb{Q}$ の場合に上の証明を書き直してみよ．□

$\boxed{\text{Eisensteinの判定法}}$ RはUFDであるとし，Kはその商体であるとする．

"mod p"で見る！

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$，$a_i \in R$ とRの素元 p について，

$p \nmid a_n$，$p \mid a_{n-1}$，…，$p \mid a_1$，$p \mid a_0$，$p^2 \nmid a_0$ $\Longrightarrow$ $f(x)$ は K上 既約．

$\boxed{\text{証明}}$ 前ページの結果より，K上既約であることを示すためには，
1次以上の $R[x]$ の2つの元の積に $f(x)$ が分解されないことを示せばよい．

非自明なポイント

結局，次を示せばよい：

$p \nmid a_n$，$p \mid a_{n-1}$，…，$p \mid a_1$，$p \mid a_0$ かつ
$f(x)$ が1次以上の $R[x]$ の2つの元の積に分解される $\Longrightarrow$ $p^2 \mid a_0$．

$p \nmid a_n$，$p \mid a_{n-1}$，…，$p \mid a_0$ でかつ $f = gh$，$g, h \in R[x]$，$\deg g \geqq 1$，$\deg h \geqq 1$
と仮定する．このとき，自然な射影 $\pi_p : R[x] \to R[x]/(p) = (R/(p))[x]$ について，

$$\pi_p(f) = \overline{a_n} x^n = \pi_p(g)\pi_p(h), \quad 0 \neq \overline{a_n} \in R/(p).$$

係数を mod p で
$R/(p)$ にうつす

ゆえに，$\pi_p(g)$，$\pi_p(h)$ の定数項は $R/(p)$ の中で0になる．
すなわち，g と h の定数項はどちらも p で割り切れる．
このことから $f = gh$ の定数項 a_0 が p^2 で割り切れることがわかる． □

易しい部分