1回目 modular GCD

$\varphi : \mathbb{Z} \to \mathbb{F}_p$

定理 (かんたんなコーナーカット) $f, g \in \mathbb{Z}[x]$.

p 素数. $p \nmid lc(f)$, $p \nmid lc(g)$ とするとき

$$GCD(\varphi(f), \varphi(g)) = 1 \Rightarrow GCD(f, g) = 1 \text{ in } \mathbb{Q}[x].$$

逆に. $GCD(f, g) = 1$ in $\mathbb{Q}[x] \Rightarrow$ 有限個の p をのぞいて.

$GCD(\varphi(f), \varphi(g)) = 1$. ($\Rightarrow$ 有限個の p をのぞいて $\varphi(GCD(f, g)) = GCD(\varphi(f), \varphi(g))$)

これで, 一番大変な場合を排除できる $\Rightarrow$ いくつかの p に対し $GCD(\varphi(f), \varphi(g)) \neq 1$ なるとうすると?

方法1 (中国剰余定理; CRT).

補題 $p_1, \ldots, p_\ell$: 互異なる素数. $h_1, \ldots, h_\ell \in \mathbb{Z}$

$\Rightarrow \exists h \in \mathbb{Z}$ s.t. $h \equiv h_i \bmod p_i$ h は mod $M = p_1 \cdots p_\ell$ で一意.

補題 $a, M \in \mathbb{Z}_{>0}$ に対し. $a \equiv \frac{c}{b} \bmod M$ (すなわち. $ab \equiv c \bmod M$)

$b > 0$, $0 \leq |b|, |c| \leq \sqrt{\frac{M}{2}}$ なる b, c があれば一意的.

これを使って次のように計算.

1. $h_i = GCD(\varphi(f), \varphi(g))$ in $\mathbb{F}_{p_i}[x]$ monic. で次数がすべて同じになるものを求める.

2. $h \equiv h_i \bmod p_i$ となる $h \in \mathbb{Z}[x]$ を求める. $M = p_1 \cdots p_\ell$.

3. h の各係数を $\frac{c}{b}$ $0 \leq |b|, |c| \leq \sqrt{\frac{M}{2}}$ に変換. 全部できたら f, g で割ってみる

☆ f, g の因子のboundを使ってもよいし、incrementalにやってもよい

<u>方法2</u> (Hensel lifting)

<u>定理</u> (Mignotte) $f=\sum_{i=0}^{n} a_i x^i$, $g=\sum_{i=0}^{m} b_i x^i$ $g \mid f$ $(a_i, b_i \in \mathbb{Z})$

$\Rightarrow \|g\|_1 \le \left|\frac{b_m}{a_n}\right| 2^m \|f\|_2$ $\left(\|g\|_1=\sum|b_i|,\ \|f\|_2=\sqrt{\sum|a_i|^2}\right)$

<u>系</u> $lc(f)f$ の因子 g で $lc(g)=lc(f)$ をみたすものについて

$|g_i| \le \|g\|_1 \le 2^m \|f\|_2$

$\left(\because\ \|g\|_1 \le \left|\frac{lc(f)}{lc(f)^2}\right| \cdot 2^m \|lc(f) \cdot f\|_2 = 2^m \|f\|_2\right)$

$p \nmid lc(f)$, $p \nmid lc(g)$ とし $a_1=GCD(\varphi(f), \varphi(g))$, $b_1=\frac{\varphi(f)}{a_1}$ とする

<u>仮定</u> $GCD(a_1, b_1)=1$ in $\mathbb{F}_p[x]$ すると Hensel の補題より

$\forall k$ $\exists a_k, \exists b_k \in \mathbb{Z}[x]$ s.t. $f \equiv a_k b_k \bmod p^k$.

$a_k \equiv a_1 \bmod p$. $b_k \equiv b_1 \bmod p$. $\deg a_k = \deg a_1$, $\deg b_k = \deg b_1$.

a_k, b_k は $lc(a_k), lc(b_k)$ を fix すれば mod p^k で一意

k として $p^k > 2 \cdot B$ $(B=2^{\deg a_1}\|f\|_2)$ をみたすようにする。

$lc(a_1)=lc(b_1)=lc(f)$ に fix し $lc(f)f \equiv a_k b_k \bmod 2^k$

まで上げる。$\Rightarrow$ a_k の係数を $|\ |<\frac{p^k}{2}$ に収めて試し割り

前処理で無平方分解すれば仮定OK

定理 $\mathrm{char}(k)=0$ $f=\prod f_i^{e_i}$ f_i キカク $\Rightarrow \mathrm{GCD}(f,f')=\prod f_i^{e_i-1}$ —(**)

$\mathrm{GCD}\left(\prod f_i^{e_i-1}, \dfrac{f'}{\prod f_i^{e_i-1}}\right)=1$ —(*)

∵ $f'=\sum e_i f_i' f_1^{e_1}\cdots f_{i-1}^{e_{i-1}} f_i^{e_i-1}\cdots f_\ell^{e_\ell}=\left(\prod f_i^{e_i-1}\right)\left(\sum e_i f_1\cdots f_i'\cdots f_\ell\right)$

$\mathrm{GCD}\left(f_i, \sum e_i f_1\cdots f_i'\cdots f_\ell\right)=\mathrm{GCD}\left(f_i, e_i f_1\cdots f_i'\cdots f_\ell\right)$

$e_i\neq 0$ mK より $=\mathrm{GCD}(f_i, f_i')$ $f_i'\neq 0$ より $=1$.

より (*) OK. (**)もOK //

$\dfrac{f}{\mathrm{GCD}(f,f')}=f_1\cdots f_\ell$ で無平方部分. これと GCD をつかえば,

$f=h_1 h_2^2\cdots h_m^m$ (h_iは重複度 m のキカク因子の積).

$\mathrm{GCD}(f,g)=\prod_i \mathrm{GCD}(h_i^i, g)$ ← $\mathrm{GCD}(h_i^i,g)$は $\mathrm{GCD}(h_i,g)$のi乗.

h_i無平方より Hensel OK.

問題点 $\mathrm{GCD}(f,f')$は?

$\Rightarrow \prod f_i^{e_i-1}$ の多項式を作る $\Rightarrow$ (*)より あるpをとれば

$\mathrm{GCD}\left(\varphi(h), \dfrac{\varphi(f')}{\varphi(h)}\right)=1 \Rightarrow$ OK.

2日目 多項式因数分解(1変数)

$\mathbb{Q}[x]$ におけるキャク分解 : $\mathbb{F}_p[x]$ 上の分解を lift する.

1. $\mathbb{F}_p[x]$ におけるキャク分解 (Berlekamp ; Cantor–Zassenhaus)

$f(x) \in \mathbb{F}_p[x]$: 無平方とする. $\pi : \mathbb{F}_p[x] \to \mathbb{F}_p[x]$, $h \mapsto h^p$ は $\mathbb{F}_p$-linear (Frobenius map)

$\left((h_1+h_2)^p = h_1^p + h_2^p \ . \ c \in \mathbb{F}_p \Rightarrow c^p = c \right)$

$\pi : \underbrace{\mathbb{F}_p[x]/\langle f \rangle}_{\text{有限次元 vect. sp.}} \to \mathbb{F}_p[x]/\langle f \rangle$ — $f = \prod_{i=1}^{l} f_i$ (: (f_i キャク).)

$b_i \equiv \begin{cases} 1 & \bmod f_i \\ 0 & \bmod f_j \ \forall (j \neq i) \end{cases}$

$h_i = b f_1 \cdots f_{i-1} f_{i+1} \cdots f_l$

$b_i \bmod f_i \overset{\exists}{=} b F_i \bmod f_i = 1$

とすれば $\mathbb{F}_p[x]/\langle f \rangle \simeq \bigoplus_i \mathbb{F}_p[x]/\langle f_i \rangle$ ("CRT).

$h \bmod f \longleftrightarrow (h \bmod f_i)$

$\mathrm{Ker}(\pi - \mathrm{Id})$ も分解して. $\mathrm{Ker}(\pi - \mathrm{Id}) \simeq \bigoplus_i \mathrm{Ker}(\pi_i - \mathrm{Id})$ $\left(\pi_i : \mathbb{F}_p[x]/\langle f_i \rangle \to \mathbb{F}_p[x]/\langle f_i \rangle, \ h \mapsto h^p \right)$

ここで. $\mathbb{F}_p[x]/\langle f_i \rangle \simeq \mathbb{F}_{p^{d_i}}$ ($\because$ f_i キャク $\deg f_i = d_i$)

で. $\mathrm{Ker}(\pi_i - \mathrm{Id}) = \{ \alpha \in \mathbb{F}_{p^{d_i}} \mid \alpha^p = \alpha \} = \mathbb{F}_p$. $\therefore$ $\mathrm{Ker}(\pi - \mathrm{Id}) = \bigoplus_i \mathbb{F}_p$ (l 個の直和)

$\therefore$ $\mathrm{Ker}(\pi - \mathrm{Id})$ は具体的に計算でき. $\dim_{\mathbb{F}_p} \mathrm{Ker}(\pi - \mathrm{Id}) = f$ のキャク因子の個数

また. $\forall g \in \mathrm{Ker}(\pi - \mathrm{Id})$. $\exists s_1, \ldots, s_l$. $g \equiv s_i \bmod f_i$

$\forall (s_1, \ldots, s_l) \in \mathbb{F}_d^{\,l}$, $\exists g \in \mathrm{Ker}(\pi - \mathrm{Id})$. $g \equiv s_i \bmod f_i$

よって. $g \in \mathrm{Ker}(\pi - \mathrm{Id})$ に対し. $g - s$ ($s \in \mathbb{F}_d$) のいずれかは f_i のいくつかを因子にもつ

実際には $\mathrm{Ker}(\pi - \mathrm{Id})$ の基底 $\{ g_1 = 1, g_2, \ldots, g_l \}$ をとり.

$\mathrm{GCD}(g_i - s, f)$ を $s \in \mathbb{F}_p$ に対して計算すれば しまいにはすべての f_i を得る

pが小 ⇒ これでOK　pが大 ⇒ コストが大きすぎ ⇒ 確率的アルゴリズム
(2ケタくらい)

<u>定理</u>　p : odd prime ⇒ $\#\{g \in \mathrm{Ker}(\pi - \mathrm{Id}) \mid \mathrm{GCD}(g^{\frac{p-1}{2}}-1, f) \neq 1, f\}$

$$= p^l - \left(\frac{p-1}{2}\right)^l - \left(\frac{p+1}{2}\right)^l$$

$f \mid g^p - g = g(g^{\frac{p-1}{2}}-1)(g^{\frac{p+1}{2}}+1)$

$s^{\frac{p-1}{2}} = \begin{cases} 1 \\ -1 \\ 0 \end{cases}$　$g \equiv s_i \bmod f_i$　$g^{\frac{p-1}{2}} \equiv \begin{cases} 1 \\ -1 \\ 0 \end{cases}$

<u>意味</u>　$g \in \mathrm{Ker}(\pi - \mathrm{Id})$をランダムにとると $\mathrm{GCD}(g^{\frac{p-1}{2}}-1, f)$により$f$の非自明因子を得る確率が　$1 - \left(\frac{p-1}{2p}\right)^l - \left(\frac{p+1}{2p}\right)^l \simeq 1 - \frac{1}{2^l} - \frac{1}{2^l} = 1 - \frac{1}{2^{l-1}}$

$l > 2 \Rightarrow \geq \frac{1}{2}$

2) $\mathbb{Q}$上でのキカク分解

<u>Berlekamp-Hensel アルゴリズム</u>

$f(x) \in \mathbb{Z}[x]$ 無平方

$f(x) \equiv c \prod_{i=1}^{l} f_i(x) \bmod p$　f_i : monic と分解, k : $p^k > 2^{n+1}\|f\|_2$ みたすk

$F \leftarrow f$

for $i = 1$ to $l-1$ do

　$a_1 \leftarrow f_i$　$b_1 \leftarrow \prod_{j=i+1}^{l} f_j$.　($\Rightarrow F \equiv lc(f)\, a_1 b_1 \bmod p$.)

　$F \equiv lc(f)\, a_k b_k \bmod p^k$ まで lifting.

　$F_i \leftarrow a_k$, $c \leftarrow lc(f)\, b_k$

end for

($f \equiv lc(f) \prod_{i=1}^{l} F_i \bmod p^k$).

loop

　$G \leftarrow (lc(f) \times F_{i_1} \cdots F_{i_t})$ の係数を $\left(-\frac{p^k}{2}, \frac{p^k}{2}\right)$にひきもどし.

　$G \mid lc(f) f \Rightarrow G$ が因子.

endloop

<u>問題点</u>　真の因子 $\ll l \Rightarrow$ 組み合せパックパック <u>対策</u> knapsack アルゴリズム.

3) 代数拡大 ($k(\alpha)$) 上のキヤク分解

準備：終結式

定義 $f(x) = a_n x^n + \cdots + a_0 = a_n(x-\alpha_1)\cdots(x-\alpha_n)$ $a_n \neq 0$

$g(x) = b_m x^m + \cdots + b_0 = b_m(x-\beta_1)\cdots(x-\beta_m)$ $b_m \neq 0$ に対し、

$$\mathrm{res}_x(f,g) \underset{\mathrm{def}}{=} a_n^n b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\beta_j)$$

を f, g の終結式 (resultant) と呼ぶ。

定義 f, g 上と同じ。 $\mathrm{Syl}_x(f,g) = \begin{array}{c} \left(\begin{array}{ccccc} a_n & \cdots & a_0 & & \\ & \ddots & & \ddots & \\ & & a_n & \cdots & a_0 \\ b_m & \cdots & b_0 & & \\ & \ddots & & \ddots & \\ & & b_m & \cdots & b_0 \end{array}\right) \begin{array}{l} \}\, m \\ \\ \}\, n \end{array} \\ \underbrace{\qquad\qquad\qquad}_{m+n} \end{array}$

を f, g の Sylvester 行列という。

定理 $\mathrm{res}_x(f,g) = \det(\mathrm{Syl}_x(f,g))$ 特に $\mathrm{res}_x(f,g) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$

定理 $\mathrm{GCD}_x(f,g) \neq 1 \iff \mathrm{res}_x(f,g) = 0$

$\mathrm{res}_x(f,g) \in \langle f, g \rangle$ より詳しく、 $\exists u, v \in \mathbb{Z}[a, b]$

$uf + vg = \mathrm{res}_x(f,g)$ — (*)

例 判別式 $f(x) = \prod(x-\alpha_i)$. $f(x) = \sum_i \frac{f(x)}{x-\alpha_i}$

$$\mathrm{res}_x(f, f') = \prod f'(\alpha_i) = \prod_i (\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{i<j}(\alpha_i-\alpha_j)^2$$

$\mathrm{res}_x(f, f') = 0 \iff f$ が重根をもつ。

系. $\mathrm{Norm}(f) = f_1^{e_1} \cdots f_\ell^{e_\ell}$ f_i キカクとすると.

$\mathrm{GCD}(f, \bar{f}_i)$ は f のいくつかのキカク因子の積 とくに. $e_i = 1 \Rightarrow$

$\mathrm{GCD}(f, \bar{f}_i)$ は f のキカク因子.

定理. f 無平方 $\Rightarrow$ $\mathrm{Norm}(f(x+s\alpha))$ が無平方でない $s \in \mathbb{Z}$ は有限個

以上により次のアルゴリズムを得る.

$f(x)$ の根 $= \beta_1 \cdots \beta_n$ とすると $f(\alpha, x)$

$f(x+s\alpha)$ の根 $= \beta_1 - s\alpha_i, \cdots, \beta_n - s\alpha_i$ $f(\alpha, x+s\alpha)$

$f(\alpha_i, x+s\alpha_i)$

アルゴリズム afactor

入力: $f(\alpha, x)$ 無平方, $s \in \mathbb{N}$ 出力: f のキカク分解

$H \leftarrow \mathrm{Norm}(f(\alpha, x+s\alpha))$ $H = h_1^{e_1} \cdots h_r^{e_r}$ h_i キカク/K.

$F \leftarrow \emptyset$

for $i = 1$ 和 r do

$f_i \leftarrow \mathrm{GCD}(f(\alpha, x+s\alpha), h_i)$

if $e_i = 1$ then $F \leftarrow F \cup \{f_i\}$

else $F \leftarrow F \cup \mathrm{afactor}(f_i(x-s\alpha), s+1)$

endfor.

応用 最小分解体. $L = K(\alpha_1, \ldots, \alpha_n)$ α_i: $f(x)$ の根

$f(x) \in K[x]$ キカクとする. $\alpha_1 \leftarrow f(x)$ の1根とし. f を $K(\alpha_1)$ 上でキカク分解.

$f = \prod f_i$ f_i が1つ次ならば, その根を α_2 とする.

各 f_i を $K(\alpha_1, \alpha_2)$ 上分解 ... 1次因子はかりになるまでつづける

得られる結果 $L = K(\alpha_\ell, \alpha_{\ell-1}, \ldots, \alpha_1)$

$L = K[t_\ell, \ldots, t_1] / \langle h_\ell(t_\ell, \ldots, t_1), h_{\ell-1}(t_{\ell-1}, \ldots, t_1), h_1(t_1) \rangle$

および $f = (x - t_1) \cdots (x - t_\ell)(x - a_1(t_1, \ldots, t_\ell)) \cdots (x - a_{n-\ell}(t_1, \ldots, t_\ell))$

これから $\mathrm{Gal}(f)$ も強引に計算可能

$\mathbb{Q}(\alpha_\ell, \ldots, \alpha_1)$ 上の計算: $\mathbb{Q}[\alpha_\ell, \ldots, \alpha_1, x_1, \ldots, x_n] / \langle h_\ell, \ldots, h_1 \rangle$ として実現できる.

実際には, 簡単化, 逆元計算ちょっと大へん. ⇒ グレブナー基底の観点から.

後計算するのもよい

グレブナー基底

1. 項順序. 単項約化. グレブナー基底

K: 体. $R = K[X] = K[x_1, \dots, x_n]$

$T = \{ x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_i \in \mathbb{Z}_{\geq 0} \}$ ここでは項(term)と呼ぶ.

定義 Tの全順序 $<$ で

1. $\forall t.\ 1 \leq t$
2. $t \leq s \quad u \in T \Rightarrow ut \leq us$.

を満たすものを項順序(term order)と呼ぶ.

例 $<_{lex}$ (辞書式順序) $x^\alpha <_{lex} x^\beta \iff \exists i.\ \alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}.\ \alpha_i < \beta_i$

$<_{grevlex}$ $<_{drl}$ (全次数逆辞書式順序) $x^\alpha <_{grevlex} x^\beta \iff$

$$\begin{cases} |\alpha| < |\beta| & (|\alpha| = \alpha_1 + \dots + \alpha_n \text{ 全次数}) \\ \text{または} & \\ |\alpha| = |\beta| \text{ かつ} & \exists i.\ \alpha_n = \beta_n, \dots, \alpha_{i+1} = \beta_{i+1}\ \alpha_i > \beta_i \end{cases}$$

より一般に $w = (w_1, \dots, w_n) \in \mathbb{Z}^n_{>0}$ に対し $|\alpha|$ を $|\alpha|_w = w_1\alpha_1 + \dots + w_n\alpha_n$ にした weight つき順序も有効.

他に 半積順序 ($X = X_1 \sqcup X_2$ として X_1 に対して O_1 で比較. $\Rightarrow X_2$ に対して O_2 で比較) など.

定義 $f \in R$ を $f = \sum_{i=1}^{m} c_i t_i \quad c_i \neq 0 \quad t_1 > t_2 > \dots > t_m \quad (c_i \in K, t_i \in T)$

と書くとき $HT(f) = t_1,\ HC(f) = c_1,\ HM(f) = c_1 t_1$

(Becker–Weispfenning) $HT(S) = \{ HT(s) \mid s \in S \}$. $T(f) = \{ t_1, \dots, t_m \}$ (サポート)

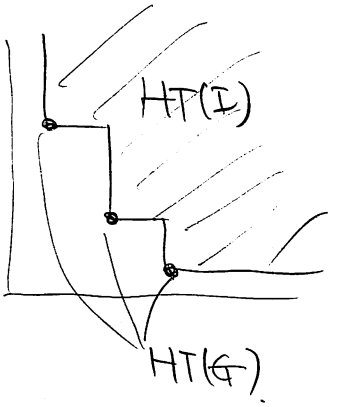
$M = \{ ct \mid c \in K, t \in T \}$

定義（グレブナー基底）$I \subset R$ イデアル，$<$ 項順序とする．

有限集合 $G \subset I$ が I の $<$ に関するグレブナー基底（Gröbner basis; GB）

$\underset{def}{\Longleftrightarrow}$ $\langle HT(G) \rangle = \langle HT(I) \rangle$

$\Longleftrightarrow$ $\forall f \in I \setminus \{0\}$ $\exists g \in G$ s.t. $HT(g) \mid HT(f)$



例 $R = k[x]$ $I \subset R$ イデアル $\Rightarrow$ $\exists f \in I$, $I = \langle f \rangle$

このとき $\{f\}$ は I の GB

例 $A = (a_{ij})_{m \times n}$ $A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}$ $I = \langle f_1, \dots, f_m \rangle$

A の行基本変形による階段形 $B = \begin{pmatrix} 1 & & & * \\ & 1 & & * \\ & & 1 & * \\ 0 & & & \end{pmatrix} = (b_{ij})$ とする．

$B\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} g_1 \\ \vdots \\ g_\ell \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ とすれば $G = \{g_1, \dots, g_\ell\}$ は I の GB

例 $G = \{x_1 - f_1(x_n), \dots, x_{n-1} - f_{n-1}(x_n), f_n(x_n)\}$ $I = \langle G \rangle$ とすれば

G は I の GB．（fact: I が 0 次元 $\Rightarrow$ 線形変数変換後 $\sqrt{I}$ はこの形の G をもつ）

定義（単項簡約）$f \xrightarrow[G]{} h$ $\Longleftrightarrow$ $\exists t \in T(f)$, c を t の係数，$\exists g \in G$ s.t. $HT(g) \mid t$.

$h = f - \dfrac{ct}{HM(g)} g$.（$ct$ が消去された）

f を 0 回以上単項簡約して h を得るとき $f \xrightarrow[G]{*} h$ と書く．

h がそれ以上簡約できないとき h は G について normal form という．

定理 term order は well order（すなわち $\forall S \subset T$ $S \neq \emptyset \Rightarrow S$ は最小元をもつ）

（通常は単独で証明．ここでは Hilbert の基底定理を引用）

系 $<$ に関する無限降下列はない。

(証明 [illegible])

系 $\forall f \in R \setminus \{0\}$ $f \xrightarrow[G]{} h_1 \xrightarrow[G]{} h_2 \to \cdots$ は有限回で normal form r に到達する

このとき r を f の G による剰余(の一つ)という

定理 イデアル I の GB G は存在して $I = \langle G \rangle$ さらに $f \in I \iff f \xrightarrow[G]{*} 0$

∵) $\langle HT(I) \rangle = \langle t_1, \ldots, t_\ell \rangle$ $(t_i \in T)$ (by Hilbertの基底定理)

$HT(g_i) = t_i$ となる $g_i \in I$ をとれる このとき G は I の GB.

$f \in I$ とする $f \xrightarrow[G]{*} r$. r を正規形とする. $r = f - m_1 g_{i_1} - \cdots - m_N g_{i_N}$ より

$r \in I$. もし $r \neq 0$ とすれば $HT(r) \in \langle HT(G) \rangle$ より. r が normal form であることに矛盾 ∴ $r = 0$. ∴ $f \in \langle G \rangle$. ∴ $\langle G \rangle = I$ //

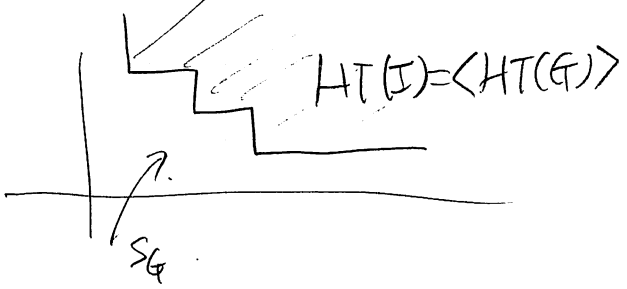
定理 G が I の GB. $f \xrightarrow[G]{*} h_1$, $f \xrightarrow[G]{*} h_2 \Rightarrow h_1 = h_2$

定義 $NF_G : R \to R$. $f \mapsto f$ の G による剰余 h_1, h_2 が正規形

定理 $S_G = \{ t \in T \mid t$ はどの $HT(g)$ $g \in G$ でも割れない$\}$ とおくと.

$R/I \simeq \mathrm{span}_K(S_G)$ (K-線形)

$[f] \mapsto NF_G(f)$



$\{ [s] \mid s \in S_G \}$ は一次独立. mR/I

2. 応用

① サポートを指定したメンバーシップ

問 $T(f)=\{t_0,\dots,t_l\}$ なる $f\in I$ を求めよ.

解 $f=a_0t_0+\cdots+a_lt_l$ とすると. $f\in I \iff NF_G(f)=0$

$\iff a_0NF_G(t_0)+\cdots+a_lNF_G(t_l)=0$ これは. $NF_G(t_i)$ にあらわれる

S_G の元について整理すると. $C_0(a_0,\dots,a_l)s_0+\cdots+C_m(a_0,\dots,a_l)s_m=0$ $(s_i\in S_G)$

$\iff \begin{cases} C_0=0 \\ \vdots \\ C_m=0 \end{cases}$ この線形方程式を解けばよい

例 最小多項式.

$\dim_K R/I<\infty \iff |S_G|<\infty \iff \forall i\ \exists g$ s.t. $HT(g)=x_i^{m_i}$

(0次元イデアル) このとき. $\forall x_i\in X$ $\{[1],[x_i],[x_i^2],\dots,[x_i^N]\}$ はすべて一次従属

N ではじめてなったとする: $c_N[x_i^N]+\cdots+c_0[1]=0$ $(c_1\neq 0)$

$m_{x_i}(t)=\sum c_it^i$ を x_i の最小多項式とよぶ.

$u=(u_1,\dots,u_n)\in V(I)$ とすれば $m_{x_i}(u_i)=0$ より u_i が確定する.

② 消去理論.

定義 $X=Y\sqcup Z$ $<$ が (Y,Z) に関する消去順序とは

$\alpha\neq(0,\dots,0)\Rightarrow y^\alpha z^\beta > z^\gamma$ $(\forall\beta,\forall\gamma)$ をみたすこと.

(例: 辞書順序, lex) $Y>>Z$ と書く.

定理 $<$ が (Y,Z) に関する消去順序 G が $<$ に関するこの G は

$\Rightarrow I\cap K[Z]=\langle G\cap K[Z]\rangle$, $G\cap K[Z]$ は $I\cap K[Z]$ の G 基

$\because$ $f\in I\cap K[Z]\Rightarrow f\in I$ より $\exists g\in G$ $HT(g)\mid HT(f)$ $f\in K[Z]$ より $HT(g)\in K[Z]$

$g\in K[Z]$

応用は大変多い

a). $I \cap J$, $I = \langle f_1, \dots, f_m \rangle$ $J = \langle h_1, \dots h_\ell \rangle$

$\Rightarrow I \cap J = \langle tf_1, \dots, tf_m, (1-t)h_1, \dots, (1-t)h_\ell \rangle \cap k[X]$

(かんたん) 消去 >> X で計算

b). $I : f = \{ h \in R \mid hf \in I \}$ (イデアル商)

$I : f = \dfrac{I \cap \langle f \rangle}{f} = \langle \frac{g_1}{f}, \dots, \frac{g_\ell}{f} \rangle$ ($\{g_1, \dots, g_\ell\}$: $I \cap \langle f \rangle$ の基底)

$J = \langle h_1, \dots, h_\ell \rangle \Rightarrow I : J = \{ h \in R \mid hJ \subset I \} = \bigcap (I : \{h_i\})$ も計算できる.

c) $I : f^\infty = \bigcup_{s=1}^{\infty} (I : f^s) = I : f^{s_0}$ (saturation)

$I : f^\infty = (k[t]I + \langle tf - 1 \rangle) \cap R$

(∵) $h \in$ 右辺 とすれば $h(x) = \sum \tilde{a}_i(x,t) f_i + \tilde{a}(x,t)(tf-1)$ ($f_i \in I$)

$Q(R)$ 上で $t = \frac{1}{f}$ として $h(x) = \sum a_i(x, \frac{1}{f}) f_i$ ∴ ある $f^s h = \sum \tilde{a}_i(x) f_i \in$ 右辺.

$h \in$ 右辺. $f^s h \in I$. $h = \underbrace{h(1 - t^s f^s)}_{\in \langle tf-1 \rangle} + \underbrace{h t^s f^s}_{\in k[t]I} \in$ 右辺)

<u>イデアルの分解の基本</u>

$I = (I : f^\infty) \cap (I + \langle f^{s_0} \rangle)$ ($I : f^\infty = I : f^{s_0}$)

⊃) $I \subset$ 右辺はOK $g \in$ 右辺とすると $f^{s_0} g \in I$. かつ $g = h + uf^{s_0}$

($\exists h \in I$) $\underset{I \ni}{f^{s_0} g} = \underset{I \ni}{f^{s_0} h} + uf^{2s_0}$ より $uf^{2s_0} \in I$ ∴ $u \in I : f^{2s_0} = I : f^{s_0}$

∴ $uf^{s_0} \in I$ ∴ $g \in I$.

d) 根基. $\mathrm{Char}(k)=0$ I が0次元ならやさしい.

$\sqrt{I}=\{f\in R \mid \exists m\in\mathbb{Z}_{\geq 0},\ f^m\in I\}$ これも代数.

$V(I)=V(\sqrt{I})$

I が0次元 $\Rightarrow$ $\forall x_i\in X$ $\exists m_i(x_i)\in I$ ($m_i(x_i)$: x_iの最小多項式)

このとき $\sqrt{I}=I+\langle sf(m_1),\dots,sf(m_n)\rangle$

一般次元: 複雑. (分解してから求める)

$\sqrt{I}=\bigcap P_i$ (P_i: 素イデアル)

4回目 補遺

定理 (Buchberger) $I=\langle G\rangle$ $G=\{g_1,\dots,g_l\}$ が I の GB

$\iff \forall g_i, g_j \in G$. $\mathrm{Spoly}(g_i, g_j) \xrightarrow[G]{*} 0$

∵) $\Rightarrow$ OK. $\Leftarrow$ を示す. g_i は monic としてよい. $t_i = HT(g_i)$.

$t_{ij} = LCM(t_i, t_j)$ と書く. $\mathrm{Spoly}(g_i, g_j) = s_i g_i - s_j g_j$.

$s_i = \dfrac{t_{ij}}{t_i}$ と書ける. $\mathrm{Spoly}(g_i, g_j) \xrightarrow[G]{*} 0$ より

$$s_i g_i = s_j g_j + \underbrace{\sum^{\exists} u_k g_k}_{(*)} \quad HT(u_k g_k) < t_{ij}.$$

$f \in I \setminus \{0\}$. を. $f = h_1 g_1 + \cdots + h_l g_l$ $\underbrace{}_{(**)}$ と書くとき. $HT(f) = \max_i HT(h_i g_i)$

なら $\exists g_i$ $HT(g_i) \mid HT(f)$. $HT(f) < \max_i HT(h_i g_i) \equiv t$ とすると.

$\exists i, \exists j$. $i \neq j$. $HT(h_i g_i) = HT(h_j g_j) = t$. このとき. $(*)$ より

$$HT(h_i) g_i = HT(h_j) g_j + \sum \frac{t}{t_{ij}} u_k g_k \quad \left(\text{両辺に } \frac{t}{t_{ij}} \text{ をかけた}\right)$$

これより $h_i g_i + h_j g_j = {}^{\exists}c\, HT(h_j) g_j + \sum^{\exists} v_k g_k$ $(HT(v_k g_k) < t)$

と書ける. よって $(**)$ の係数をとりかえて. 共に $i \mid HT(h_i g_i) = t$ をへらせる. $\underbrace{}_{(***)}$

これを繰り返すと $(***) = 0$ となり. $\max HT(h_i g_i)$ が下がる.

∴ これを有限回繰り返すと. 無限降下列の非存在により

$HT(f) = \max_i HT(h_i g_i)$ となる //