平成12年度修士論文
非可換多項式環 $k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$ の左単項生成イデアルの共通部分の生成元について

指導教官: 木村俊一 教官

広島大学大学院理学研究科博士課程前期数学専攻
学生番号: M1171023
森島 聖

平成13年2月9日

概要

本論文は, $yx = \alpha xy$ を満たす非可換多項式環 $k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$ の左単項生成イデアルの共通部分の生成元に関して考察したものである. 可換多項式環では, 単項生成イデアルの共通部分は最小公倍多項式によって単項生成されるわけだが, 左 Gröbner 基底アルゴリズムを用いた計算機実験の結果から非可換多項式環 $k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$ の左単項生成イデアルの共通部分は必ずしも単項生成にならないことがわかった. そこで, 単項生成になるいくつかの条件の場合について証明つきで構成し, 単項生成でない場合については具体的構成は出来なかったが, 計算機実験から高々2 元で生成されるのではないかという予想をたてた. この予想や, また, 単項生成になるための必要十分条件に関しては, 今後研究を行っていく上で大変興味深いものとなっている.

目 次

序

k を標数 0 の体とする. 可換多項式環 $k[x_1, \cdots, x_n]$ での Gröbner 基底の応用についてはよく知られており, 消去イデアル, 多項式で表された連立方程式の解, 有理関数で表されたパラメータ表示に対応する陰表示, イデアル商, イデアルの飽和, イデアルの共通部分, イデアルの根基, イデアルの準素分解, シジジー等を計算可能にする ([1][2]).

この論文では Gröbner 基底の概念を非可換多項式環に応用し, 左単項生成イデアルの共通部分の生成元について考察する.

まず 1 章で $k[x_1, \cdots, x_n]$ での Gröbner 基底とその応用, 特に, 消去イデアルの定義 (Definition 1.4) や, 消去イデアルを求めるアルゴリズム (Theorem 1.5), また, それを用いてイデアルの共通部分の生成元を計算するアルゴリズム (Theorem 1.6) を紹介する.

2 章では $x_j x_i = \alpha x_i x_j$ $(j > i)$ を満たす, x_i で生成される非可換多項式環

$$R' = k(\alpha)\langle x_1, \cdots, x_n\rangle / (x_j x_i - \alpha x_i x_j \mid j > i)$$

に Gröbner 基底の概念を適用した左 Gröbner 基底とその応用について議論する. 左 Gröbner 基底 (Definition 2.5) は左除法定理 (Theorem 2.3) と左 S 多項式 (Definition 2.6) を用いて構成することが出来る. このアルゴリズムを用いることにより左消去イデアル (Definition 2.17) と左単項生成イデアルの共通部分の生成元を計算することが出来る (Theorem 2.18,Theorem 2.19).

3 章では, 特に $yx = \alpha xy$ を満たす 2 変数非可換多項式環

$$R = k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$$

に限定し, 左 Gröbner 基底アルゴリズムを用いた左単項生成イデアルの共通部分の生成元の計算及び考察を行う. 可換多項式環では, 単項生成イデアルの共通部分は最小公倍多項式によって単項生成される. しかし, R では左単項生成イデアルの共通部分は必ずしも単項生成にはならない. 例えば,

$$\begin{aligned}(*)\ R\cdot(x+1)\cap R\cdot(y+1) = R\cdot&\left(x^2y + x^2 + \frac{(\alpha+1)}{\alpha}xy + \frac{(\alpha+1)}{\alpha}x + \frac{y}{\alpha} + \frac{1}{\alpha}\right)\\ +R\cdot&\left(xy^2 + \frac{(\alpha+1)}{\alpha}xy + \frac{y^2}{\alpha^2} + \frac{x}{\alpha} + \frac{(\alpha+1)}{\alpha^2}y + \frac{1}{\alpha}\right)\end{aligned}$$

が挙げられる (Example 3.3). この 2 元は左簡約 Gröbner 基底 (Definition 2.12) になっており, その一意性 (Proposition 2.13) から単項生成にはならないことが示される (Lemma 3.4). このように必ずしも左単項生成イデアルの共通部分は単項生成にはならないのだが, 計算機実験の結果 (Example 3.22) から, 左 Gröbner 基底の定義に用いる単項式順序 (Definition 1.1) として辞書式順序 (Example 1.2.1) $x > y$ を取るとき高々2 元からなる左簡約 Gröbner 基底で生成されるのではないかと予想される (Conjecture

3.25). 一方, 単項生成になる場合については, いくつかの構成方法 (Proposition 3.16, Proposition 3.21) を与える. ここで, この構成方法に関連して, 高橋宣能氏による予想 (Conjecture 3.24) が提起されている. 最後に残るのは単項生成になる必要十分条件は何かという問題 (Problem 3.23) である. これらの予想や問題は, 今後研究を行っていく上で大変興味深いものとなっている.

本文における記号の説明： R' は $x_jx_i = \alpha x_ix_j$ $(i < j)$ を満たす多変数非可換多項式環, R は $yx = \alpha xy$ を満たす 2 変数非可換多項式環を表し, R' の多項式はすべて $x_jx_i = \alpha x_ix_j$ $(i < j)$ を用いて各項を $x_1, \cdots, x_n$ の順の積で表すことにする. R の多項式についても同様である. これにより, 非可換多項式環上で可換の積を考えることが出来るので, これを『$*$』によって表す. また, 特に断わらない限り単項生成元は零多項式でないと仮定する.

謝辞： 本論文作成と研究にあたり, 木村俊一先生には多大な御指導と助言をいただきました. 木村俊一先生の海外出張時には, 高橋宣能先生にも御指導と助言をいただきました. 2 年間で様々な面においてお世話になった他の諸先生方や友人達, また, 6 年間, 勉学に励む上での素晴しい環境を私に与えて下さった広島大学も含めて, この場を借りて感謝の意を表します.

第1章　多項式環とGröbner基底

1.1　多項式環とGröbner基底

Gröbner 基底という概念は廣中平祐と B. Buchberger によって発見されたものであるが, この概念は, 計算代数, 特に多項式環における様々な代数的対象の具体量の計算への応用を多く持つ. この節では,(可換) 多項式環 $k[x_1, \cdots, x_n]$ における Gröbner 基底とその応用について簡単に説明する. なお, この節での定義の細密な部分や証明については [1],[2] を参照するとよいが, 同様の議論を 2 章で非可換多項式環について詳しく述べる.

まず単項式に順序づけを行う.

Definition 1.1 M を単項式全体の集合とする. M 上の関係 $>$ が

1. $>$ は, 全順序である.
2. $>$ は, 整列順序である.
3. $\forall a, b, c \in M$ に対し, $a > b \quad \Longrightarrow \quad ac > bc$

を満たすとき, $>$ を M 上の**単項式順序**という.

単項式順序は, $x^\alpha > x^\beta$ のとき, $\alpha > \beta$ と表すこともある. ただし, $\alpha = (\alpha_1, \cdots, \alpha_n)$ で, $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ とする. β についても同様である.

以下に単項式順序の例をいくつか挙げる.

Example 1.2

1. **辞書式順序** (*lex order*) $\alpha >_{lex} \beta \Longleftrightarrow$
   $\alpha - \beta$ の 0 でない一番左にくる要素が正の数.
2. **総次数辞書式順序** (*grlex order*) $\alpha >_{grlex} \beta \Longleftrightarrow$
   $\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$ または, $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ かつ $\alpha >_{lex} \beta$
3. **総次数逆辞書式順序** (*grevlex order*) $\alpha >_{grevlex} \beta \Longleftrightarrow$
   $\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$ または, $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ かつ $\alpha - \beta$ の 0 でない一番右にくる要素が負の数.

4. l **番目消去順序** (*l-th elimination order*) $\alpha >_l \beta \Longleftrightarrow$

$\sum_{i=1}^{l}\alpha_i > \sum_{i=1}^{l}\beta_i$ または, $\sum_{i=1}^{l}\alpha_i = \sum_{i=1}^{l}\beta_i$ かつ $\alpha >_{grevlex} \beta$

この単項式順序に関しては, [3] を参考にするとよい.

上の例では $x_1 > \cdots > x_n$ となっているが, 変数に任意の順序を定めても同様に単項式順序を定めることが出来る. また, *1* や *4* のような

$$\exists l \quad s.t. \quad \forall p = x_1^{\alpha_1}\cdots x_l^{\alpha_l}(\neq 1), \forall q = x_{l+1}^{\alpha_{l+1}}\cdots x_n^{\alpha_n} \text{ に対し}, \ p > q$$

を満たすような単項式順序を l **番目消去型順序**という.

すべての単項式順序は加重行列によって行列表示出来ることが知られている. 上から順に行ベクトルと比較したいそれぞれの単項式の指数の内積の大小を調べるやり方である.

例えば, 総次数辞書順序なら,

$$\underbrace{\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ \vdots & \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}}_{n}$$

l 番目消去イデアルなら,

$$\underbrace{\begin{pmatrix} \overbrace{1 & \ldots & 1}^{l} & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 1 & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 & 0 \\ 1 & 1 & \ldots & 1 & 0 & 1 \\ \vdots & & & \ddots & \vdots & \vdots \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & \ddots & & & \vdots & \vdots \\ 0 & 1 & \ldots & 1 & 1 & 1 \end{pmatrix}}_{n}$$

のように行列表示する. 詳細は [4] を参照のこと.

単項式順序を固定したとき, 多項式 f の項の中で最も大きいものを f の**先導項**といい $\mathrm{LT}(f)$ と表す. また, その単項式を $\mathrm{LM}(f)$, 係数を $\mathrm{LC}(f)$, $\mathrm{LT}(f)$ の指数部分を $\mathrm{multideg}(f)$ と表す. さらに $G \subset k[x_1, \cdots, x_n]$ に対し, $\mathrm{LT}(G)$ を, G の元の先導項の集合とする.

以後, 特に断わらない限り $x_1 > \cdots > x_n$ であるような, ある単項式順序を固定し議論を進めていく.

Definition 1.3 $I \subset k[x_1, \cdots, x_n]$ をイデアル, $G \subset I$ を I の有限生成系とし , 単項式順序 $>$ を固定する.

$$(\mathrm{LT}(I)) = (\mathrm{LT}(G))$$

が満たされるとき, G を I の $>$ に関する **Gröbner 基底**という. ただし, 有限集合 A に対し, (A) は, A のすべての元で生成されるイデアルを表す.

実際, $I=(f_1,\cdots,f_s)$ のように具体的に生成元が与えられた場合,Gröbner 基底を計算するアルゴリズム (Buchberger のアルゴリズム) が知られている. 特に簡約 Gröbner 基底と呼ばれるものは一意に定まるので, 以後, Gröbner 基底は簡約化されたものを扱うことにする.

多項式を複数の多項式で割りたいとき, 多変数型の除法定理アルゴリズムを適用することによりそれぞれの商多項式と剰余多項式を計算することが出来るが, 一般に, 単項式順序や多項式で割る順番を変えて計算するとこれらは一意ではない. しかし,Gröbner 基底で割ると, 単項式順序や割る順番にかかわらず剰余多項式は一意に定まる. このことから, 具体的に多項式とイデアルの生成元が与えられたときに, イデアルの Gröbner 基底を用いることにより, 多項式がイデアルに所属しているかどうかの判定が可能になる.

この他にも Gröbner 基底の応用例は多いが, ここでは消去イデアルを計算するアルゴリズムとイデアルの共通部分を計算するアルゴリズムについて述べておく.

Definition 1.4 $I \subset k[x_1,\cdots,x_n]$ をイデアルとするとき,

$$I_l := I \cap k[x_{l+1},\cdots,x_n]$$

を l **番目消去イデアル**という.

より一般に $R'=k[x_{i_1},\cdots,x_{i_s}]$ $(\{x_{i_1},\cdots,x_{i_s}\}\subset\{x_1,\cdots,x_n\})$ に対して, $I'=I\bigcap R'$ を $\{x_{i_1},\cdots,x_{i_s}\}$ に関する**消去イデアル**ということもあるが, 変数を並べかえることにより以下と同じ議論が出来る. 次の定理が, l 番目消去イデアルの生成元 (Gröbner 基底) の計算アルゴリズムを与える.

Theorem 1.5 G を イデアル $I \subset k[x_1,\cdots,x_n]$ の l 番目消去型順序に関する (簡約)Gröbner 基底とする. このとき $0 \le l \le n$ に対し,

$$G_l := G \cap k[x_{l+1},\cdots,x_n]$$

は l 番目消去イデアル I_l の (簡約)Gröbner 基底である.

上で述べた通り l 番目消去型順序には, 辞書式順序や l 番目消去順序があるのだが, 実際に計算する場合には, 辞書式順序よりも l 番目消去順序のほうが計算スピードが速い傾向があることが計算機実験からわかった. ちなみに, l 番目消去順序で計算した l 番目消去イデアルの生成元は, 総次数逆辞書式順序に関する Gröbner 基底となる. なお, 辞書式順序や l 番目消去順序が l 番目消去型順序といわれる所以は, この定理から明らかであろう.

次の定理はイデアルの共通部分の生成元を計算するアルゴリズムを与える.

Theorem 1.6 $I, J \subset k[x_1,\cdots,x_n]$ をイデアルとする. このとき,

$$I \cap J = (tI + (1-t)J) \cap k[x_1,\cdots,x_n].$$

この定理からイデアル $tI+(1-t)J \subset k[t,x_1,\cdots,x_n]$ の $\{t\}$ に関する 1 番目消去イデアルを計算すれば, $I \cap J$ の生成元 (Gröbner 基底) が求まる.

第2章　左Gröbner基底のアルゴリズムと応用

1 章では Gröbner 基底とその応用について簡単にふれたが, この章では, $x_j x_i = \alpha x_i x_j$ を満たす x_i で生成される非可換多項式環

$$R' = k(\alpha)\langle x_1, \cdots, x_n\rangle / (x_j x_i - \alpha x_i x_j \mid j > i)$$

に Gröbner 基底の概念を導入した左 Gröbner 基底アルゴリズムとその応用について議論していく. なお, R' の多項式はすべて $x_j x_i = \alpha x_i x_j$ $(i < j)$ を用いて各項を $x_1, \cdots, x_n$ の順の積で表すことにする. このように表したとき, 非可換多項式環上で可換の積を表したい場合には『$*$』の記号を用いることにする. また, このとき, 単項式順序が可換の場合と同様に定義できるので, 以後, 特に断らない限り単項式順序を固定して議論を進める.

2.1　左除法定理と左Gröbner基底

まず初めに, 非可換の場合の除法定理アルゴリズムを紹介する.

Lemma 2.1 $s = cx^a, t = dx^b \in R'$　$c, d \in k(\alpha)$　$a = (a_1, \cdots, a_n)$　$b = (b_1, \cdots, b_n)$ とする. このとき,

$$st = \alpha^e (s * t) \quad ただし, \ e = \sum_{i=1}^{n-1}\left(b_i \sum_{j=i+1}^{n} a_j\right).$$

証明は容易なので省略する.

Definition 2.2 前補題での α^e は, s と t によって決まるので, これを $\mathrm{sig}(s,t)$ とおく. すなわち, $st = \mathrm{sig}(s,t)(s*t)$ と表せる.

次の定理が左除法定理とそのアルゴリズムである.

Theorem 2.3 $f, f_1, \cdots, f_s \in R'$　($f_i \neq 0$) に対し,

$$f = a_1 f_1 + \cdots + a_s f_s + r \quad (r = 0 \quad または \quad \mathrm{LT}(f_i) \text{ は } r \text{ のどの項も右から割り切らない })$$

を満たす $a_1, \cdots, a_s, r \in R'$ が存在する (以下に述べる通り計算方法がある).

(Proof)
コンピュータの言語をまねた疑似コードを用いて表示する. ただし, 疑似コードと証明での除法演算記号『A/B』及び, 『$\frac{A}{B}$』は, 可換の除法を意味する. この論文において以下この演算記号は特に断わらない限り同様のものとする.

Input: $f_1, \cdots, f_s, f$
Output: $a_1, \cdots, a_s, r$

$a_1 := 0;\ \cdots;\ a_s := 0;\ r := 0$
$p := f$
WHILE $p \neq 0$ DO
    $i := 1$
    divisionoccurred := false
    WHILE $i \leq s$ AND divisionoccurred = false Do
        IF $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ THEN
            $a_i := a_i + \mathrm{LT}(p)/(\mathrm{LT}(f_i)\mathrm{sig}(\mathrm{LT}(p)/\mathrm{LT}(f_i), \mathrm{LT}(f_i)))$
            $p := p - (\mathrm{LT}(p)/(\mathrm{LT}(f_i)\mathrm{sig}(\mathrm{LT}(p)/\mathrm{LT}(f_i), \mathrm{LT}(f_i))))f_i$
            divisionoccurred := true
        ELSE
            $i := i + 1$
    IF divisionoccurred = false THEN
        $r := r + \mathrm{LT}(p)$
        $p := p - \mathrm{LT}(p)$

これが, 計算方法であることを示す.

この計算方法には, 各計算段階において, $\mathrm{LT}(p)$ を割り切るような $\mathrm{LT}(f_i)$ が存在する場合の段階 (除法段階とする) と, $\mathrm{LT}(p)$ を割り切るような $\mathrm{LT}(f_i)$ が存在しない場合の段階 (余り段階とする) の 2 通りがある. まず, $a_1, \cdots, a_s, r, p$ の初期値を, $a_{1(0)}, \cdots, a_{s(0)}, r_{(0)}, p_{(0)}$ とおき, m 回目の計算段階における $a_1, \cdots, a_s, r, p$ の値を, $a_{1(m)}, \cdots, a_{s(m)}, r_{(m)}, p_{(m)}$ とおく.

まず, 各計算段階において

$$f = a_1 f_1 + \cdots + a_s f_s + p + r$$

を満たすことを示す.
$m = 0$ のとき,

$$a_{1(0)} f_1 + \cdots + a_{s(0)} f_s + p_{(0)} + r_{(0)} = 0 \cdot f_1 + \cdots + 0 \cdot f_s + f + 0 = f.$$

m 回目の計算段階に進む前に,

$$f = a_{1(m-1)} f_1 + \cdots + a_{s(m-1)} f_s + p_{(m-1)} + r_{(m-1)}$$

が成り立っていると仮定する. m 回目の計算段階が除法段階のとき, 値が変わる変数は, a_i, p で

$$\begin{aligned} a_{i(m)} f_i + p_{(m)} &= \left\{ a_{i(m-1)} + \frac{\mathrm{LT}(p_{(m-1)})}{\mathrm{LT}(f_i)\mathrm{sig}(\mathrm{LT}(p_{(m-1)})/\mathrm{LT}(f_i), \mathrm{LT}(f_i))} \right\} f_i \\ &\quad + \left\{ p_{(m-1)} - \frac{\mathrm{LT}(p_{(m-1)})}{\mathrm{LT}(f_i)\mathrm{sig}(\mathrm{LT}(p_{(m-1)})/\mathrm{LT}(f_i), \mathrm{LT}(f_i))} f_i \right\} \\ &= a_{i(m-1)} f_i + p_{(m-1)} \end{aligned}$$

より

$$f = a_{1(m)}f_1 + \cdots + a_{s(m)}f_s + p_{(m)} + r_{(m)}.$$

m 回目の計算段階が余り段階のとき, 値が変わる変数は, p, r で

$$p_{(m)} + r_{(m)} = \{p_{(m-1)} - \mathrm{LT}(p_{(m-1)})\} + \{r_{(m-1)} + \mathrm{LT}(p_{(m-1)})\} = p_{(m-1)} + r_{(m-1)}$$

より

$$f = a_{1(m)}f_1 + \cdots + a_{s(m)}f_s + p_{(m)} + r_{(m)}.$$

以上により, 各計算段階において

$$f = a_1f_1 + \cdots + a_sf_s + p + r$$

を満たす.

次に, $p = 0$ のときに計算が終わるので, 出力結果が

$$f = a_1f_1 + \cdots + a_sf_s + r$$

となることは明らかである.

さらに, 出力結果が, $r = 0$ または $\forall\mathrm{LT}(f_i)$ は r のすべての項を割り切らないという条件を満たすことは, r の初期値 ($r_{(0)} = 0$) と, 余り段階に進む条件 (LT(p) を割り切るような LT(f_i) は存在しない) と, 余り段階における計算 ($r_{(m)} = r_{(m-1)} + \mathrm{LT}(p_{(m-1)})$) より明らかである.

最後に, 有限回の計算で $p = 0$ になる, つまり, 計算が有限回で終わることを示す.
m 回目の計算段階が除法段階のとき

$$p_{(m)} = p_{(m-1)} - \frac{\mathrm{LT}(p_{(m-1)})}{\mathrm{LT}(f_i)\mathrm{sig}(\mathrm{LT}(p_{(m-1)})/\mathrm{LT}(f_i), \mathrm{LT}(f_i))}f_i$$

$$\mathrm{LT}\left(\frac{\mathrm{LT}(p_{(m-1)})}{\mathrm{LT}(f_i)sig(\mathrm{LT}(p_{(m-1)})/\mathrm{LT}(f_i), \mathrm{LT}(f_i))}f_i\right) = \frac{\mathrm{LT}(p_{(m-1)})}{\mathrm{LT}(f_i)\mathrm{sig}(\mathrm{LT}(p_{(m-1)})/\mathrm{LT}(f_i), \mathrm{LT}(f_i))}\mathrm{LT}(f_i)$$
$$= \mathrm{sig}(\mathrm{LT}(p_{(m-1)})/\mathrm{LT}(f_i), \mathrm{LT}(f_i))\frac{\mathrm{LT}(p_{(m-1)}) * \mathrm{LT}(f_i)}{\mathrm{LT}(f_i)\mathrm{sig}(\mathrm{LT}(p_{(m-1)})/\mathrm{LT}(f_i), \mathrm{LT}(f_i))} = \mathrm{LT}(p_{(m-1)})$$

より, $\mathrm{multideg}(p_{(m)}) < \mathrm{multideg}(p_{(m-1)})$ または $p_{(m)} = 0$ になる.
m 回目の計算段階が余り段階のとき

$$p_{(m)} = p_{(m-1)} - \mathrm{LT}(p_{(m-1)})$$

より, 明らかに $\mathrm{multideg}(p_{(m)}) < \mathrm{multideg}(p_{(m-1)})$ または $p_{(m)} = 0$ になる. 単項式順序は整列順序なので, 以上により, 有限回の計算で $p = 0$ になる.
(証明終わり)

左除法定理アルゴリズムにより求まる商多項式と剰余多項式は f_i で割る順番や単項式順序に依存する.

左除法定理アルゴリズムを数式処理ソフト *Mathematica* 用にリスト処理計算を用いて実装したプログラム `NCPolyDiv` を用いて具体例を計算する. なお, プログラムと説明については, 付録 A を参照のこと.

Example 2.4

1. $k(\alpha)\langle x,y\rangle/(yx-\alpha xy)$ において

$$\begin{cases} f = x^2y^3+1 \\ f_1 = xy-y \\ f_2 = y^2+1 \end{cases}$$

とする.

```
In[2]:=f=x^2*y^3+1;f1=xy-y;f2=y^2+1
```

f を右から総次数逆辞書式順序 $x>y$ に関して $\{f_1,f_2\}$ で割る. なお, t はダミー変数である (付録 A 参照).

```
In[3]:=NCPolyDiv[f,{f1,f2},grevlex,{x,y,t}]
```

Out[3]= $\left\{\left\{\frac{y^2}{\alpha^4}+\frac{xy^2}{\alpha^2},\frac{y}{\alpha^4}\right\},1-\frac{y}{\alpha^4}\right\}$

よって,

$$x^2y^3+1=\left(\frac{y^2}{\alpha^4}+\frac{xy^2}{\alpha^2}\right)(xy-y)+\frac{y}{\alpha^4}\left(y^2+1\right)+1-\frac{y}{\alpha^4}$$

である.

2. $k(\alpha)\langle x,y,z\rangle/(yx-\alpha xy, zy-\alpha yz, zx-\alpha xz)$ において

$$\begin{cases} f = xyz+yz^3 \\ f_1 = x-y^2 \\ f_2 = y^2+z \\ f_3 = z-1 \\ f_4 = y \end{cases}$$

とする.

```
In[4]:=f=x*y*z+y*z^3;f1=x-y^2;f2=y^2+z;f3=z-1;f1=y
```

f を右から辞書式順序 $x>y>z$ に関して $\{f_1,f_2,f_3,f_4\}$ で割る.

```
In[5]:=NCPolyDiv[f,{f1,f2,f3,f4},lex,{x,y,z,t}]
```

`Out[5]=`$\left\{\left\{\frac{yz}{\alpha^2}, \frac{yz}{\alpha^2}, y+yz+yz^2-\frac{y}{\alpha^2}-\frac{yz}{\alpha^2}, 1-\frac{1}{\alpha^2}\right\}, 0\right\}$

よって,

$$xyz+yz^3=\frac{yz}{\alpha^2}\left(x-y^2\right)+\frac{yz}{\alpha^2}\left(y^2+z\right)+\left(y+yz+yz^2-\frac{y}{\alpha^2}-\frac{yz}{\alpha^2}\right)(z-1)+\left(1-\frac{1}{\alpha^2}\right)y$$

である.

次に, 左 Gröbner 基底を定義する.

Definition 2.5 $I \subset R'$ を左イデアル, $G \subset I$ を I の有限生成系とし, 単項式順序 $>$ を固定する.

$$I_L\left(\mathrm{LT}(I)\right)=I_L\left(\mathrm{LT}(G)\right)$$

を満たすとき, G を I の $>$ に関する**左 Gröbner 基底**という. ただし, $I_L(A)$ は, A を生成系とする左イデアルを表わす.

左除法定理アルゴリズムを用いて, 左 Gröbner 基底アルゴリズムを構成する. そのためには, 次の左 S 多項式という概念が必要になる.

Definition 2.6 $f, g \in R'$ を零でない多項式とし, $m=\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$ を可換の意味での最大公約多項式 (ここでは単項式) とする. このとき,

$$S_L(f,g)=\frac{\mathrm{sig}\left(\frac{m}{\mathrm{LT}(g)}, \mathrm{LT}(g)\right)}{\mathrm{sig}\left(\frac{m}{\mathrm{LT}(f)}, \mathrm{LT}(f)\right)}\cdot\frac{m}{\mathrm{LT}(f)}\cdot f-\frac{m}{\mathrm{LT}(g)}\cdot g$$

を f と g の**左 S 多項式**という.

左 S 多項式という概念は, 定義からわかるように各々の先導項を消去するものである.

Definition 2.7 $f, f_1, \cdots, f_s \in R'$ ($\forall f_i \neq 0$) とし, $F=\{f_1, \cdots, f_s\}$ を順序付き集合とする. 左除法定理アルゴリズムを用いて

$$f=a_1f_1+\cdots+a_sf_s+r \quad (r=0 \quad \text{または} \quad \mathrm{LT}(f_i) \text{ は } r \text{ のどの項も右から割り切らない})$$

と表したときの剰余多項式 r を, $\overline{f}^F$ と表す.

左 S 多項式を用いることにより, 左 Gröbner 基底であるかどうかの判定ができる.

Theorem 2.8 $I=I_L(G) \subset R'$ を左イデアルとしする. このとき,

$$G \text{ が } I \text{ の左 Gröbner 基底} \iff \forall p, q \in G \text{ に対し}, \overline{S_L(p,q)}^G=0.$$

証明は省略する. [5] の *Theorem* 3.11 を参照のこと.

左 S 多項式を用いて左 Gröbner 基底アルゴリズムを構成する.

Theorem 2.9 $I = I_L(f_1, \cdots, f_s)(\neq \{0\}) \subset R'$ を左イデアルとする. このとき, 次のアルゴリズムが I の左 Gröbner 基底 G を求めるものである.

Input: $F = (f_1, \cdots, f_s)$
Output: $F \subset G$ を満たす I の左 Gröbner 基底 $G = (g_1, \cdots, g_t)$

$G := F$
REPEAT
  $G' := G$
  FOR $p \neq q$ を満たす G' の 元の組 $\{p, q\}$ *DO*
    $S := \overline{S_L(p,q)}^{G'}$
    IF $S \neq 0$ *THEN* $G := G \bigcup \{S\}$
UNTIL $G = G'$

(Proof)
まず始めに, すべての計算段階において, $G \subset I$ であることを示す. 初期値は, $G = F$ より, $G \subset I$. $G' \subset I$ と仮定する. 各計算段階において, G には, ある $p, q \in G'$ に対して, $S = \overline{S_L(p,q)}^{G'} \neq \{0\}$ なら, S が加わる. $p, q \in G' \subset I$ より, $S_L(p,q) \in I$ となる. よって, $(I \supset)G' = \{g_1, \cdots, g_s\}$ とすると左除法定理より,

$$S = S_L(p,q) - a_1 g_1 -, \cdots, -a_s g_s \quad (\forall i \quad a_i \in R')$$

となり, $S \in I$. よって, $G \bigcup \{S\} \subset I$ より, すべての計算段階において $G \subset I$ である.
次に, すべての計算段階において $I_L(G) = I$ を示す. しかしこのことは, F が I の生成系であることと, すべての計算段階において $F \subset G$ より明らかである.
計算が終了するのは, 最終行において $G = G'$ となるとき, すなわち $\forall p, q \in G$ に対し, $\overline{S_L(p,q)}^{G'} = 0$ となるときである. よって, 前定理より, G は I の左 Gröbner 基底である.
最後に, 計算が有限回の計算段階で終了することを示す. $G' \subset G$ より $I_L(\mathrm{LT}(G')) \subset I_L(\mathrm{LT}(G))$. まず 最終行において $G' \neq G$ のとき, $I_L(\mathrm{LT}(G')) \neq I_L(\mathrm{LT}(G))$ であることを示す. $G' \neq G$ であるということは, ある $p, q \in G'$ に対して, $S = \overline{S_L(p,q)}^{G'}$ が G に加わるということである. S は $S_L(p,q)$ を右から G' で割った剰余多項式より, $\mathrm{LT}(S) \notin I_L(\mathrm{LT}(G'))$. 一方で $\mathrm{LT}(S) \in I_L(\mathrm{LT}(G))$ より, $G' \neq G$ ならば, $I_L(\mathrm{LT}(G')) \neq I_L(\mathrm{LT}(G))$ である. よって, 計算段階を繰り返すことにより, 左イデアルの昇鎖が出来る. 非可換多項式環 R' はネーター環より, 有限回で $I_L(\mathrm{LT}(G')) = I_L(\mathrm{LT}(G))$ になる. このとき $G' = G$ となるので, 計算は有限回で終了する.
(証明終わり)
このアルゴリズムは, S 多項式を可換の場合で定義し,(可換) 除法定理アルゴリズムを用いることにより, 同様に, (可換)Gröbner 基底を計算するものでもある. 可換の場合, Buchberger のアルゴリズムといわれており, Gröbner 基底アルゴリズムの基本になっている. 現在では Gröbner 基底アルゴリズムの様々な改良によって計算がより効率よく出来るようになっている. しかし, すべての場合に最適なアルゴリズムはなく, 計算する対象によって, 効率のよいアルゴリズムは違うものになる. アルゴリズムの改良に関しては [1], Gröbner 基底アルゴリズムにまつわる話は [6] を参照するとよい. なお,(非可換) 左 Gröbner 基底アルゴリズムに関しても可換の場合の改良が幾つか応用できる.
前定理のアルゴリズムによって出力される左 Gröbner 基底は, 必要以上の元を出力する場合がある. 次の補題により, どの元が不必要かがわかる.

Lemma 2.10 G を左イデアル $I \subset R'$ の左 Gröbner 基底, $p \in G$ を $\mathrm{LT}(p) \in I_L(\mathrm{LT}(G - \{p\}))$ を満たす多項式とする. このとき, $G - \{p\}$ は I の左 Gröbner 基底である.

(Proof)
G は I の左 Gröbner 基底より, $I_L(\mathrm{LT}(I)) = I_L(\mathrm{LT}(G))$ を満たす.仮定より, $\mathrm{LT}(p) \in I_L(\mathrm{LT}(G - \{p\}))$ から, $I_L(\mathrm{LT}(G - \{p\})) = I_L(\mathrm{LT}(G))$. よって, $G - \{p\}$ は I の左 Gröbner 基底である.
(証明終わり)
このことにより, 不必要な元を除去し, 元の数を極小にすることが出来る.

Definition 2.11 左イデアル $I \subset R'$ の左 Gröbner 基底 G が,

1. $\forall p \in G$ に対し, $\mathrm{LC}(p) = 1$
2. $\forall p \in G$ に対し, $\mathrm{LT}(p) \notin I_L(\mathrm{LT}(G - \{p\}))$

を満たすとき, G を I の **左極小 Gröbner 基底** という.

元の数が極小になったからといって, 左極小 Gröbner 基底が一意に定まるわけではない. 次に定める左簡約 Gröbner 基底が, 単項式順序を固定したときに, 左イデアルの左 Gröbner 基底を一意にするものである.

Definition 2.12 左イデアル $I \subset R'$ の左 Gröbner 基底 G が,

1. $\forall p \in G$ に対し, $\mathrm{LC}(p) = 1$
2. $\forall p \in G$ に対し, p の任意の項 m に対して $m \notin I_L(\mathrm{LT}(G - \{p\}))$

を満たすとき, G を I の **左簡約 Gröbner 基底** という.

左簡約 Gröbner 基底の存在と一意性は次の命題により示される.

Proposition 2.13 $I(\neq \{0\}) \subset R'$ を左イデアルとする. このとき, I の左簡約 Gröbner 基底が一意に存在する.

(Proof)
G を I の左極小 Gröbner 基底とする. $g \in G$ の任意の項 m が $m \notin I_L(\mathrm{LT}(G - \{g\}))$ のとき, g を G で簡約されたと定義することにより, G のすべての元を簡約することで左簡約 Gröbner 基底を構成することが出来る. g が G で簡約されているならば, I の他のどの左極小 Gröbner 基底に対しても, 簡約されているのは明らかである. $g \in G$ に対し, $g' = \overline{g}^{G-\{g\}}$ とおき, $G' = (G - \{g\}) \bigcup \{g'\}$ とする. つまり, G の元 g を g' と入れ替えたものを G' とする. g' は g を右から $G - \{g\}$ で割ったものであるから, G の極小性の定義より, $\mathrm{LT}(g)$ は左除法定理アルゴリズムの余り段階にいく. つまり, 剰余多項式 g' の先導項は $\mathrm{LT}(g)$, すなわち $\mathrm{LT}(g') = \mathrm{LT}(g)$ となる. このことより, $I_L(\mathrm{LT}(G')) = I_L(\mathrm{LT}(G))$ となり, $G' \subset I$ から, G' もまた I の左極小 Gröbner 基底となる. さらに g' は g を $G - \{g\}$ で右から割ったときの剰余多項式より, g' の任意の項は, $\mathrm{LT}(G - \{g'\}) (= \mathrm{LT}(G - \{g\}))$ の任意の元で右から割り切れない. よって, g' は G で簡約されている. 一度簡約されると他のどの元を簡約しても明らかに簡約されたままであるので, この操作を G のすべての元に施すことにより, 具体的に左簡約 Gröbner 基底が構成出来る. 次に一意性を示す. G と G'' を I の左簡約 Gröbner 基底とする. G と G'' の極小性

から明らかに $\mathrm{LT}(G) = \mathrm{LT}(G'')$ である. すなわち, $g \in G$ に対し, $\mathrm{LT}(g) = \mathrm{LT}(g'')$ を満たす $g'' \in G''$ が存在する. ここで, $g = g''$ を示せば, 一意性は証明される. $g - g'' \in I$ で, G は左 Gröbner 基底より, $\overline{g - g''}^G = 0$. $\mathrm{LT}(g) = \mathrm{LT}(g'')$ より, $g - g''$ の先導項は消去されていて, 残りの項, すなわち, g, g'' の両方の項のなかで消去されていないものは, 簡約性の定義より $\mathrm{LT}(G)\,(= \mathrm{LT}(G''))$ の任意の元で右から割り切れない. 以上のことから, $0 = \overline{g - g''}^G = g - g''$. よって, $g = g''$.
(証明終わり)

以後, 左 Gröbner 基底は, 特に断わらない限り, 簡約化されたものを扱うことにする.

上の証明における構成方法により, 左簡約 Gröbner 基底を計算することができる. 左 (簡約)Gröbner 基底アルゴリズムを数式処理ソフト *Mathematica* にリスト処理計算を用いて, さらに計算スピードに関して幾つかの改良を施して実装したプログラム `NCGroebner` を付録 B に掲げる. 以下, このプログラムを用いた具体例の計算結果について述べる.

Example 2.14

1. $k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$ において

$$\begin{cases} f_1 = x + 1 \\ f_2 = y + 1 \end{cases}$$

とする.

```
In[7]:=f1=x+1;f2=y+1
```

左イデアル $I = I_L(f_1, f_2)$ の辞書式順序 $x > y$ に関する左 (簡約)Gröbner 基底を求める.

```
In[8]:=NCGroebner[{f1,f2},lex,{x,y,t}]
```

```
Out[8]={1}
```

よって, I の左 (簡約)Gröbner 基底は,

$$\{1\}$$

である.
すなわち, この例から示されることは,

$$I_L(x+1, y+1) = k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$$

ということである.

$$1 = \frac{y + \alpha}{\alpha - 1} \cdot (x+1) - \frac{\alpha x + 1}{\alpha - 1} \cdot (y+1) \in I_L(x+1, y+1)$$

からも, 明らかであろう (なお, $\alpha \to 1$ とすると発散する).

2. $k(\alpha)\langle x, y, z\rangle / (yx - \alpha xy, zy - \alpha yz, zx - \alpha xz)$ において

$$\begin{cases} f_1 = x - z^4 \\ f_2 = y - z^5 \\ f_3 = x + y \end{cases}$$

とする.

```
In[9]:=f1=x-z^4;f2=y-z^5;f3=x+y
```

左イデアル $J = I_L(f_1, f_2, f_3)$ の総次数辞書式順序 $x > y > z$ に関する左 (簡約)Gröbner 基底を求める.

```
In[10]:=NCGroebner[{f1,f2,f3},grlex,{x,y,z,t}]
```

Out[10]=$\{z^4, x, y\}$

よって, J の左 (簡約)Gröbner 基底は,

$$\left\{x, y, z^4\right\}$$

である.
ちなみに, 可換多項式環では, イデアル $(f_1, f_2, f_3) \subset k[x, y, z]$ の総次数辞書式順序 $x > y > z$ に関する (簡約)Gröbner 基底は,

$$\left\{x + y, yz + y, y^2 + y, z^4 + y\right\}$$

である.

1 章で可換多項式環において, 多項式を Gröbner 基底で割った剰余多項式は, 単項式順序や割る順番に関わらず定まることを述べたが, 非可換多項式環 R' についても同様のことがいえる.

Proposition 2.15 $G = \{g_1, \cdots, g_t\}$ を左イデアル $I \subset R'$ の左 Gröbner 基底とし, $f \in R'$ とする. このとき, 次の条件を満たす $r \in R'$ が一意に定まる.

1. $r = 0$ または, r の任意の項は, 各 i に対し, $\mathrm{LT}(g_i)$ で右から割り切れない.

2. $f - r \in I$.

特に, r は, f を G で任意の単項式順序と任意の割る順番で右から割った時の剰余多項式である.

(Proof)
左除法定理より $f = a_1g_1 + \cdots + g_tf_t + r$ と表わせ, $g = a_1g_1 + \cdots + g_tf_t$ とおくことによって, 条件は満たされる. 次に r の一意性を示す. $f = g + r = g' + r'$ を条件を満たすものとする. そうすると, $r - r' = g' - g \in I$. ここで $r \neq r'$ と仮定すると, $\mathrm{LT}(r - r') \in I_L(\mathrm{LT}(I)) = I_L(\mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_t))$ となる. このことより, $\mathrm{LT}(r - r')$ を右から割り切るような $\mathrm{LT}(g_i)$ が存在する. このことは, 条件 1 に矛盾する. よって, $r = r'$ である.
(証明終わり)
この命題から次の系が導きだされる.

Corollary 2.16 G を左イデアル $I \subset R'$ の左 Gröbner 基底とし, $f \in R'$ とする. このとき,

$$f \in I \quad \Longleftrightarrow \quad f \text{ を } G \text{ で右から割った時の剰余多項式が零多項式.}$$

(Proof)
($\Longleftarrow$): 明らか.
($\Longrightarrow$): $f \in I$ とすると, $f - 0 \in I$ は, 前命題の条件を満たすので, 0 が剰余多項式.
(証明終わり)

この系から, 多項式 $f \in R'$ と左イデアル $I \subset R'$ の生成元が, 与えられたとき, f が I の元であるかという問題 (左イデアルの所属問題) が, I の左 Gröbner 基底を計算し, f に左除法定理アルゴリズムを適用したときの剰余多項式が零多項式かどうかを見ることによって解決出来る.

2.2 左消去イデアルと左単項生成イデアルの共通部分

この節では, 左 Gröbner 基底アルゴリズムの応用例として, 左消去イデアルを求めるアルゴリズムと左単項生成イデアルの共通部分の生成元を計算するアルゴリズムを紹介する.

まず, l 番目左消去イデアルを定義し, アルゴリズムを紹介する.

Definition 2.17 $I \subset R'$ を左イデアルとするとき,

$$I_l := I \cap k(\alpha)\langle x_{l+1}, \cdots, x_n \rangle / (x_j x_i - \alpha x_i x_j \mid j > i \geq l+1)$$

を l **番目左消去イデアル**という.

Theorem 2.18 $I \subset R'$ を左イデアル, G を I の l 番目消去型順序に関する左簡約 Gröbner 基底とする. このとき,

$$G_l := G \cap k(\alpha)\langle x_{l+1}, \cdots, x_n \rangle / (x_j x_i - \alpha x_i x_j \mid j > i \geq l+1)$$

は l 番目左消去イデアル I_l の左簡約 Gröbner 基底である.

(Proof)

$R'_l = k(\alpha)\langle x_{l+1}, \cdots, x_n \rangle / (x_j x_i - \alpha x_i x_j \mid j > i \geq l+1)$ とおく. まず, $G_l \subset I_l$ を示す. しかしこのことは, $G \subset I$ を R'_l に制限したことより明らか. よって, G_l が I_l の左 Gröbner 基底であることを示すには, $I_L(\mathrm{LT}(I_l)) = I_L(\mathrm{LT}(G_l))$ を示せば良い. ($\supset$) は常に成り立っているので, $f \in I_l$ に対し $\mathrm{LT}(f) \in I_L(\mathrm{LT}(G_l))$ を示せば良い. $f \in I_l \subset I$ で G は I の左 Gröbner 基底より, ある $g \in G$ について, $\mathrm{LT}(f)$ は左から $\mathrm{LT}(g)$ で割り切れる. このとき, $\mathrm{LT}(f) \in R'_l$ より, $\mathrm{LT}(g) \in R'_l$. 今, 単項式順序は l 番目消去型順序より, g の項に $x_1, \cdots, x_n$ の変数が含まれることはない. よって, $g \in G_l$ となり, $\mathrm{LT}(f) \in I_L(\mathrm{LT}(G_l))$ が示された. 残りは G_l の簡約性を示せばよいが, このことは G が簡約で G_l はその部分集合より簡約性の条件を満たすのは明らか.
(証明終わり)

1 章の可換多項式環 $k[x_1, \cdots, x_n]$ の場合と同様, l 番目消去順序で計算した l 番目左消去イデアルの生成元は, 総次数逆辞書式順序に関して左簡約 Gröbner 基底となる.

$R'[t]$ を R' に可換な変数 t を付加した環とする. このとき, 次の定理から, 変数 $t > x_1 > \cdots > x_n$ に関する 1 番目左消去イデアルを計算することにより, R' の左生成イデアルの共通部分の生成元が計算出来る. なお, 環 $R'[t]$ の左 Gröbner 基底とアルゴリズムについては特に述べなかったが, 変数 $t > x_1 > \cdots > x_n$ に対し,

$$\mathrm{sig}(t^p x^a, t^q x^b) = \alpha^e \quad ただし, e = \sum_{i=1}^{n-1} \left(b_i \sum_{j=i+1}^{n} a_j \right)$$

と定義することにより, R' の場合と同様の議論が成り立つ. このことは, 証明をたどっていけば明らかであろう.

Theorem 2.19 $I_1, I_2 \subset R'$ を左イデアルする. このとき, 左イデアル $J = I_L\left(tI_1 + (1-t)I_2\right) \subset R'[t]$ に対し,

$$I_1 \cap I_2 = J \cap R'.$$

(Proof)
($\subset$): $h \in I_1 \cap I_2$ とすると, t は可換な変数より,

$$h = th + (1-t)h \in tI_1 + (1-t)I_2 = R'tI_1 + R'(1-t)I_2 = I_L\left(tI_1 + (1-t)I_2\right) = J.$$

また, 明らかに $h \in R'$ より, $h \in J \bigcap R'$.
($\supset$): $h \in J \cap R'$ とする. $h \in J$ より, ある $f \in I_1, g \in I_2$ に対し, $h = tf + (1-t)g$ と表わせる. $h \in R'$ でもあるので, h の項の中で t を含む項は消去されている. よって, $t = 1$ としたとき, $h = f \in I_1$. また, $t = 0$ としたとき, $h = g \in I_2$.
(証明終わり)

3 章では, この定理を用いて, 2 変数非可換多項式環 R における左単項生成イデアルの共通部分 $Rf \cap Rg$ $(f, g \in R)$ の左簡約 Gröbner 基底を実際に計算し, その個数などについて考察する.

第3章　左単項生成イデアルの共通部分の生成元

この章では, 2 変数非可換多項式環 $R = k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$ に限定して, 2 章で紹介したアルゴリズムを用いて, 実際に左単項生成イデアルの共通部分の生成元を計算する. さらにこの計算結果から, 生成元が高々2 元で生成されるのではないかという予想をたてる. この章でも, 非可換多項式環上で可換の積を表したい場合には『$*$』の記号を用いることにする.

3.1　生成元についての考察

$f, g \in R$ に対して $Rf \cap Rg$ の生成元を考察するわけだが, まず初めに, f, g が共に零多項式でないとすると, 必ず $Rf \cap Rg$ は零でない多項式を含むことを証明しておく.

Proposition 3.1 $f, g \in R^{\times}$ とする. このとき,

$$Rf \cap Rg \neq \{0\}.$$

(Proof)

$$hf = h'g \tag{3.1}$$

を満たす零でない $h, h' \in R$ の存在性を示せば良い. $\deg(f) = p$, $\deg(g) = q$ (p, q は既知数), $\deg(h) = r + q$, $\deg(h') = r + p$ (r は未知数) とおき, (3.1) の両辺をそれぞれ展開し, 未知数の係数を比較する方程式を解く. $\deg(hf) = \deg(h'g) = r + p + q$ より, (3.1) の両辺は $r + p + q$ 次式である. 一般に n 次式の係数の数は高々 $a_n = \dfrac{(n+1)(n+2)}{2}$ 個より, (3.1) の両辺の係数を比較する方程式は高々 a_{r+p+q} 個である. また, 方程式の未知数の数は $a_{r+p} + a_{r+q}$ である. この方程式は線形なので, 『方程式の数 $<$ 未知数の数』, つまりここでは,

$$a_{r+p+q} < a_{r+p} + a_{r+q} \tag{3.2}$$

を満たす $r(\geq 0)$ が存在すれば, この方程式は零解以外の解を持つことになる. よって, 共に零でない $h, h' \in R$ の存在性が示される. (3.2) を満たす $r(\geq 0)$ の存在性は,

$$\lim_{r \to +\infty} (a_{r+p} + a_{r+q} - a_{r+p+q}) = +\infty$$

より明らか.
(証明終わり)

この証明は高橋宣能氏の示唆を受けたものである. なお, (3.2) の不等式を r について解くことにより,

$$r > \frac{-3+\sqrt{8pq+1}}{2}$$

に対して $Rf \cap Rg$ は, $(r+p+q)$ 次以下の元を含むことがわかる. また, この命題は,

$$x_j x_i = c_{ij} x_i x_j + p_{ij} \ (\ 1 \le i < j \le n,\ c_{ij} \in k^{\times},\ p_{ij} < x_i x_j\ )$$

を満たす *solvable type* といわれる非可換多項式環 $k\langle x_1, \cdots, x_n\rangle/(x_j x_i - c_{ij} x_i x_j - p_{ij} \mid i < j)$ についても成り立つ. ただし, $p_{ij} < x_i x_j$ とは, p_{ij} の任意の項 t_{ij} に対し, $t_{ij} < x_i x_j$ を表す. しかし, 一般的な非可換多項式環 $k\langle x_1, \cdots, x_n\rangle$ では成り立たない. 次がその例である.

Example 3.2 $R = k\langle x, y\rangle$ とすると, $Rx \cap Ry = \{0\}$.

例として, 非可換多項式環 R において $f = x+1$ と $g = y+1$ でそれぞれ単項生成される左イデアルの共通部分の生成元を計算する.

Example 3.3 $f = x+1, g = y+1 \in R$ とする.

```
In[11]:=f=x+1;g=y+1
```

$Rf \cap Rg$ の生成元を計算する. まず,R に可換な変数 t を付加した環の左イデアル $J = I_L(tf, (1-t)g)$ の, 変数 $t > x > y$ の 1 番目消去順序による左 Gröbner 基底を計算する. ちなみに `NCGroebner` は 2 章でも紹介したように 3 番目の変数に関しては可換になるようにプログラムを組んでいたのでここでは 3 番目に t をいれる. よって, 変数 $t > x > y$ の 1 番目消去順序の行列表示は, 変数を $\{x, y, t\}$ と入力するとき,

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

となる.

```
In[12]:=J=NCGroebner[{t*f,(1-t)*g},{{0,0,1},{1,1,1},{1,0,1},{0,1,1},{1,1,0}},
        {x,y,t}]
```

Out[12]=$\left\{\frac{1}{-1+\alpha} - \frac{t}{-1+\alpha} + \frac{y}{-1+\alpha} + \frac{t\alpha}{-1+\alpha} + \frac{x\alpha}{-1+\alpha} + \frac{xy\alpha}{-1+\alpha},\right.$
$\left. x + x^2 + xy + x^2 y + \frac{1}{\alpha} + \frac{x}{\alpha} + \frac{y}{\alpha} + \frac{xy}{\alpha}, xy + xy^2 + \frac{y}{\alpha^2} + \frac{y^2}{\alpha^2} + \frac{1}{\alpha} + \frac{x}{\alpha} + \frac{y}{\alpha} + \frac{xy}{\alpha}\right\}$

よって, J の左 Gröbner 基底は,

$$\left\{t + \frac{\alpha xy}{\alpha-1} + \frac{\alpha x}{\alpha-1} + \frac{y}{\alpha-1} + \frac{1}{\alpha-1}, x^2 y + x^2 + \frac{(\alpha+1)}{\alpha}xy + \frac{(\alpha+1)}{\alpha}x + \frac{y}{\alpha} + \frac{1}{\alpha},\right.$$
$$\left. xy^2 + \frac{(\alpha+1)}{\alpha}xy + \frac{y^2}{\alpha^2} + \frac{x}{\alpha} + \frac{(\alpha+1)}{\alpha^2}y + \frac{1}{\alpha}\right\}$$

である. この集合を R に制限する, すなわち, 元のなかで t を含むものを除くと $Rf \cap Rg$ の生成元になる. よって,

```
In[13]:={J[[2]],J[[3]]}
```

Out[13]= $\left\{x+x^2+xy+x^2y+\frac{1}{\alpha}+\frac{x}{\alpha}+\frac{y}{\alpha}+\frac{xy}{\alpha}, xy+xy^2+\frac{y}{\alpha^2}+\frac{y^2}{\alpha^2}+\frac{1}{\alpha}+\frac{x}{\alpha}+\frac{y}{\alpha}+\frac{xy}{\alpha}\right\}$

より,

$$
\begin{aligned}
(*)\ R\cdot(x+1)\cap R\cdot(y+1) = R\cdot&\left(x^2y+x^2+\frac{(\alpha+1)}{\alpha}xy+\frac{(\alpha+1)}{\alpha}x+\frac{y}{\alpha}+\frac{1}{\alpha}\right)\\
+R\cdot&\left(xy^2+\frac{(\alpha+1)}{\alpha}xy+\frac{y^2}{\alpha^2}+\frac{x}{\alpha}+\frac{(\alpha+1)}{\alpha^2}y+\frac{1}{\alpha}\right)
\end{aligned}
$$

である. 2 章でもふれたが, この生成元は総次数逆辞書式順序に関して左簡約 Gröbner 基底になっている.

この例の計算結果 (∗) が正しいことを検証しておく.
まず,

$$
\begin{cases}
h_1 = tf = t+tx\\
h_2 = (1-t)g = 1-t+y-ty\\
g_1 = t+\dfrac{\alpha xy}{\alpha-1}+\dfrac{\alpha x}{\alpha-1}+\dfrac{y}{\alpha-1}+\dfrac{1}{\alpha-1}\\
g_2 = x^2y+x^2+\dfrac{(\alpha+1)}{\alpha}xy+\dfrac{(\alpha+1)}{\alpha}x+\dfrac{y}{\alpha}+\dfrac{1}{\alpha}\\
g_3 = xy^2+\dfrac{(\alpha+1)}{\alpha}xy+\dfrac{y^2}{\alpha^2}+\dfrac{x}{\alpha}+\dfrac{(\alpha+1)}{\alpha^2}y+\dfrac{1}{\alpha}
\end{cases}
$$

とおく.

```
In[14]:=h1=t+t*x;h2=1-t+y-t*y;g1=J[[1]];g2=J[[2]];g3=J[[3]]
```

まず, $I_L(h_1,h_2)=I_L(g_1,g_2,g_3)(\subset R[t])$ を示す.
$(\subset)$: $h_1,h_2\in I_L(g_1,g_2,g_3)$ を示せば良い. 左除法定理アルゴリズムより,

```
In[15]:=NCPolyDiv[h1,{g1,g2,g3},{{0,0,1},{1,1,1},{1,0,1},{0,1,1},{1,1,0}},{x,y,t}]
```

Out[15]= $\left\{\left\{1+x,-\frac{\alpha}{-1+\alpha},0\right\},0\right\}$

```
In[16]:=NCPolyDiv[h2,{g1,g2,g3},{{0,0,1},{1,1,1},{1,0,1},{0,1,1},{1,1,0}},{x,y,t}]
```

Out[16]= $\left\{\left\{-1-y,0,\frac{\alpha^2}{-1+\alpha}\right\},0\right\}$

よって,

$$
h_1 = (x+1)\,g_1-\frac{\alpha}{\alpha-1}g_2+0\cdot g_3\in I_L(g_1,g_2,g_3)
$$
$$
h_2 = -(y+1)\,g_1+0\cdot g_2+\frac{\alpha^2}{\alpha-1}g_3\in I_L(g_1,g_2,g_3)
$$

このことは, 手計算によって確認出来る.
(⊃): $g_i = a_i h_1 + b_i h_2$ となる a_i, b_i を求めたいが, $\{h_1, h_2\}$ が左 Gröbner 基底でないため, 単純に左除法定理アルゴリズムを適用しても剰余多項式が 0 にならない (先の例では,$\{g_1, g_2, g_3\}$ が左 Gröbner 基底であろうという予想があったから, 左イデアルの所属問題から左除法定理アルゴリズムのみで判定が出来た). よって, ここでは, より一般的に多項式 $f \in R[t]$ と左イデアル $I = I_L(f_1, \cdots, f_s) \subset R[t]$ が与えられたときに, $f \in I$ ならば, 具体的に, $f = a_1 f_1 + \cdots + a_s f_s \quad (a_i \in R[t])$ のような表現のひとつを計算するアルゴリズムが欲しい. このアルゴリズムは左 S 多項式と左 Gröbner 基底アルゴリズムと左除法定理アルゴリズムを組み合わせることにより構成することが出来るが, ここでは具体的な表現が知りたいだけなのでアルゴリズムの構成方法については省略する. そこで, 数式処理ソフト $Mathematica$ でリスト処理計算を用いて組んだプログラム NCIdealRepr を用いて, $g_1, g_2, g_3 \in I_L(h_1, h_2)$ を確かめる. なお, プログラムと説明については, 付録 C を参照のこと.

In[18]:=NCIdealRepr[g1,{h1,h2},{x,y,t}]

Out[18]= $\left\{\frac{y}{-1+\alpha} + \frac{\alpha}{-1+\alpha}, \frac{1}{-1+\alpha} + \frac{x\alpha}{-1+\alpha}\right\}$

In[19]:=NCIdealRepr[g2,{h1,h2},{x,y,t}]

Out[19]= $\left\{x + \frac{1}{\alpha} + \frac{y}{\alpha} + \frac{xy}{\alpha}, x + x^2 + \frac{1}{\alpha} + \frac{x}{\alpha}\right\}$

In[20]:=NCIdealRepr[g3,{h1,h2},{x,y,t}]

Out[20]= $\left\{\frac{y}{\alpha^2} + \frac{y^2}{\alpha^2} + \frac{1}{\alpha} + \frac{y}{\alpha}, xy + \frac{y}{\alpha^2} + \frac{1}{\alpha} + \frac{x}{\alpha}\right\}$

よって,

$$\begin{aligned} g_1 &= \left(\frac{y}{\alpha-1} + \frac{\alpha}{\alpha-1}\right) h_1 + \left(\frac{1}{\alpha-1} + \frac{\alpha x}{\alpha-1}\right) h_2 \in I_L(h_1, h_2) \\ g_2 &= \left(x + \frac{1}{\alpha} + \frac{y}{\alpha} + \frac{xy}{\alpha}\right) h_1 + \left(x^2 + \frac{\alpha+1}{\alpha} x + \frac{1}{\alpha}\right) h_2 \in I_L(h_1, h_2) \\ g_3 &= \left(\frac{y^2}{\alpha^2} + \frac{\alpha+1}{\alpha^2} y + \frac{1}{\alpha}\right) h_1 + \left(xy + \frac{y}{\alpha^2} + \frac{1}{\alpha} + \frac{x}{\alpha}\right) h_2 \in I_L(h_1, h_2) \end{aligned}$$

このことが正しいことは, 手計算によって確認出来る.

最後に $\{g_1, g_2, g_3\}$ が 1 番目消去順序 $t > x > y$ に関する左簡約 Gröbner 基底であることを示す. 左 Gröbner 基底であることは, $\overline{S_L(g_1, g_2)}^{\{g_1,g_2,g_3\}} = \overline{S_L(g_1, g_3)}^{\{g_1,g_2,g_3\}} = \overline{S_L(g_2, g_3)}^{\{g_1,g_2,g_3\}} = 0$ を示せば十分である.

$$S_L(g_1, g_2) = x^2 y g_1 - t g_2 = \frac{x^2 y}{\alpha-1} + \frac{x^2 y^2}{\alpha-1} + \frac{\alpha^2 x^3 y}{\alpha-1} + \frac{\alpha^2 x^3 y^2}{\alpha-1} - txy - tx - tx^2 - \frac{t}{\alpha} - \frac{tx}{\alpha} - \frac{ty}{\alpha} - \frac{txy}{\alpha} = r_{12}$$

$$\begin{aligned} S_L(g_1, g_3) &= xy^2 g_1 - t g_3 \\ &= \frac{xy^2}{\alpha-1} + \frac{xy^3}{\alpha-1} + \frac{\alpha^3 x^2 y^2}{\alpha-1} + \frac{\alpha^3 x^2 y^3}{\alpha-1} - txy - \frac{ty}{\alpha^2} - \frac{ty^2}{\alpha^2} - \frac{t}{\alpha} - \frac{tx}{\alpha} - \frac{ty}{\alpha} - \frac{txy}{\alpha} = r_{13} \end{aligned}$$

$$S_L(g_2, g_3) = \frac{y}{\alpha^2} g_2 - x g_3 = \frac{xy^2}{\alpha} + \frac{y}{\alpha^3} + \frac{y^2}{\alpha^3} - \frac{x}{\alpha} - \frac{x^2}{\alpha} - \frac{x^2 y}{\alpha} = r_{23}$$

このことが正しいことは, 手計算によって確認出来る.

In[21]:=r12= $\frac{x^2 y}{\alpha-1} + \frac{x^2 y^2}{\alpha-1} + \frac{\alpha^2 x^3 y}{\alpha-1} + \frac{\alpha^2 x^3 y^2}{\alpha-1} - txy - tx - tx^2 - \frac{t}{\alpha} - \frac{tx}{\alpha} - \frac{ty}{\alpha} - \frac{txy}{\alpha}$

`In[22]:=r13=`$\dfrac{xy^2}{\alpha-1}+\dfrac{xy^3}{\alpha-1}+\dfrac{\alpha^3x^2y^2}{\alpha-1}+\dfrac{\alpha^3x^2y^3}{\alpha-1}-txy-\dfrac{ty}{\alpha^2}-\dfrac{ty^2}{\alpha^2}-\dfrac{t}{\alpha}-\dfrac{tx}{\alpha}-\dfrac{ty}{\alpha}-\dfrac{txy}{\alpha}$

`In[23]:=r23=`$\dfrac{xy^2}{\alpha}+\dfrac{y}{\alpha^3}+\dfrac{y^2}{\alpha^3}-\dfrac{x}{\alpha}-\dfrac{x^2}{\alpha}-\dfrac{x^2y}{\alpha}$

左除法定理アルゴリズムより,

`In[24]:=NCPolyDiv[r12,{g1,g2,g3},{{0,0,1},{1,1,1},{1,0,1},{0,1,1},{1,1,0}},{x,y,t}]`

`Out[24]=`$\left\{\left\{-x-x^2-xy-\dfrac{1}{\alpha}-\dfrac{x}{\alpha}-\dfrac{y}{\alpha}-\dfrac{xy}{\alpha},\dfrac{1}{-1+\alpha}+\dfrac{y}{-1+\alpha}+\dfrac{xy}{-1+\alpha}+\dfrac{x\alpha}{-1+\alpha},0\right\},0\right\}$

`In[25]:=NCPolyDiv[r13,{g1,g2,g3},{{0,0,1},{1,1,1},{1,0,1},{0,1,1},{1,1,0}},{x,y,t}]`

`Out[25]=`$\left\{\left\{-xy-\dfrac{y}{\alpha^2}-\dfrac{y^2}{\alpha^2}-\dfrac{1}{\alpha}-\dfrac{x}{\alpha}-\dfrac{y}{\alpha}-\dfrac{xy}{\alpha},\dfrac{1}{-1+\alpha}+\dfrac{y}{-1+\alpha}+\dfrac{y}{(-1+\alpha)\,\alpha}+\dfrac{y^2}{(-1+\alpha)\,\alpha},0\right\},0\right\}$

`In[26]:=NCPolyDiv[r23,{g1,g2,g3},{{0,0,1},{1,1,1},{1,0,1},{0,1,1},{1,1,0}},{x,y,t}]`

`Out[26]=`$\left\{\left\{0,-\dfrac{1}{\alpha},-\dfrac{1}{\alpha}\right\},0\right\}$

よって,

$$r_{12}=-\left(x+x^2+xy+\frac{1}{\alpha}+\frac{x}{\alpha}+\frac{y}{\alpha}+\frac{xy}{\alpha}\right)g_1+\left(\frac{1}{\alpha-1}+\frac{y}{\alpha-1}+\frac{xy}{\alpha-1}+\frac{\alpha x}{\alpha-1}\right)g_2+0\cdot g_3+0$$
$$r_{13}=-\left(xy+\frac{y}{\alpha^2}+\frac{y^2}{\alpha^2}+\frac{1}{\alpha}+\frac{x}{\alpha}+\frac{y}{\alpha}+\frac{xy}{\alpha}\right)g_1+\left(\frac{1}{\alpha-1}+\frac{y}{\alpha-1}+\frac{y}{\alpha\,(\alpha-1)}+\frac{y^2}{\alpha\,(\alpha-1)}\right)g_2+0\cdot g_3+0$$
$$r_{23}=0\cdot g_1-\frac{1}{\alpha}g_2+\frac{1}{\alpha}g_3+0$$

このことが正しいことは,手計算によって確認出来る. よって, $\{g_1,g_2,g_3\}$ は, 1 番目消去順序 $t>x>y$ に関する左 Gröbner 基底である. 簡約性については容易に確認出来る.

以上により, $\{g_1,g_2,g_3\}$ は, 左イデアル $I_L(h_1,h_2)\quad(\subset R\,[t])$ の 1 番目消去順序 $t>x>y$ に関する左簡約 Gröbner 基底であることは示された. よって Theorem 2.19 より $(*)$ が確認出来た.

今求めた左イデアル $R\cdot(x+1)\cap R\cdot(y+1)$ の生成元 $\{g_2,g_3\}$ が総次数逆辞書式順序に関して左簡約 Gröbner 基底になっていることより, 次の補題から, この左イデアルは単項生成でないことがわかる.

Lemma 3.4 *$I\subset R$ を左イデアルとし, I の左簡約 Gröbner 基底 G を, $|G|\geq 2$ を満たすようにする単項式順序が存在するとする. このとき, I は単項生成ではない.*

(Proof)

そうでないとする. すなわち, $Rh=I$ を満たす $h\in R$ が存在するとする. $\{h\}$ は, どの単項式順序に関しても左 Gröbner 基底である**左普遍 Gröbner 基底**であり, 先導項の係数が 1 になるように定数倍することにより, $\{h\}$ は左簡約 Gröbner 基底としてよい. 左簡約 Gröbner 基底の一意性より, ある単項式順序で左簡約 Gröbner 基底が G になることはありえない. よって, 矛盾.

(証明終わり)

よって, この計算例により, 非可換多項式環 R では, 一般的に左単項生成イデアルの共通部分は単項生成にならないことがわかる.

また, g_2,g_3 をそれぞれ `NCPolyDiv` を用いて右から $x+1,y+1$ で割ることにより, 次の 2 通りの既

約因子分解が得られる.

$$g_2 = x^2y + x^2 + \frac{(\alpha+1)}{\alpha}xy + \frac{(\alpha+1)}{\alpha}x + \frac{y}{\alpha} + \frac{1}{\alpha} = \frac{1}{\alpha}(xy + \alpha x + y + 1)(x+1) = \frac{1}{\alpha}(\alpha x + 1)(x+1)(y+1)$$

$$g_3 = xy^2 + \frac{(\alpha+1)}{\alpha}xy + \frac{y^2}{\alpha^2} + \frac{x}{\alpha} + \frac{(\alpha+1)}{\alpha^2}y + \frac{1}{\alpha} = \frac{1}{\alpha^2}(y+\alpha)(y+1)(x+1)$$
$$= \frac{1}{\alpha^2}(\alpha^2xy + \alpha x + y + \alpha)(y+1)$$

よって, このことから, 非可換多項式環 R では, 一般的に多項式の既約因子分解が一意でないことがわかる.

ここで一般に $Rf \cap Rg$ の生成元の数はどうなるのかという疑問が残る. そこで, いろいろな $f, g \in R$ に対し, 生成元の数を計算すると次の表になる.

f	g	生成元の数 (grevlex order)	生成元の数 (lex order)
$x+1$	$y+1$	2	2
$x+y$	$y+1$	2	2
x^2+1	y^2+1	2	2
x^3+y	y^3+1	2	2
x^3+1	y^3+1	2	2
$x^{10}y^8-x^5y^6$	$x^7y^3-x^2y^2$	2	2
$xy+x+1$	$x+y$	2	2
$xy+x+1$	$x+y+1$	2	2
$x+y+1$	$xy+1$	2	2
$x^2+x+y+1$	$y+1$	2	2
$x+y^2+1$	x^2+1	2	2
x^2+y^2	$x+1$	2	2
x^2-y^2-1	$x-y$	2	2
x^2-y^2-1	$x-y+1$	2	2
x^4-xy	$y-1$	2	2
x^2y-xy	xy^2-xy	2	2
$x^2y-xy-x$	xy^2-xy+y	2	2
x^4-xy	$x+y^3$	3	2
x^2+y	y^2+x	3	2
x^3+y	y^3+x	3	2
x^3+y^2	y^3+x^2	3	2
x^3y+y^2	xy^3+x^2	3	2
x^3y+xy^2	xy^3+x^2	3	2
$x^5y+x^3y^2$	xy^3+x^2y	3	2
$x^5y^{10}+x^3y^7$	$x^{10}y^3+x^2y^8$	3	2
$x^{165}y^{30}-xy$	$x^{15}y^{46}-x^{21}y^6$	3	?
$x^3y^2+xy^5$	$x^2y+x^6y^2$	3	2
$x^3y^6+xy^{10}$	$x^2y+x^{10}y^2$	3	2
x^4-y	$x+y^3$	3	2
$x-y$	x^2-y^2	1	1
$x+y$	x^2-y^2	1	1
$x-y$	x^2+y^2	1	1
$x+y$	x^2+y^2	1	1
xy^2+y	$x^3y^2+x^2y+1$	1	1
$y+1$	x^2y+x^2+1	1	1
$x^5y^4+x^2y^3+y+1$	$x^7y^4+x^4y^3+x^2y+x^2+1$	1	1
$x^5y^4+x^2y^3+y+1$	$x^7y^4+x^4y^3+x^2y+x^2+x$	1	1
$x^5y^4+x^2y^3+y+1$	$x^7y^4+x^4y^3+x^2y+x^2+y$	1	1
x^2y+y^3+1	$\alpha^6x^4y^4+\alpha^2x^2y^2+x^2y^6+y^4+x^2y^3+y+1$	1	1
x^2y+y^3+1	$\alpha^6x^4y^4+\alpha^2x^2y^2+x^2y^6+y^4+x^2y^3+2y$	1	1

表の一番右の欄は, 辞書式順序に関して左簡約 Gröbner 基底を計算し直したものである. ここで計算した例では, 生成元は, 辞書式順序に関しては高々2 元になった. ただし,『?』のところは容量超過のため計算が完了しなかった. また, 単項生成になる例もあった.

それでは, 単項生成になる場合はどんな時であろうか. 明らかに単項生成になる場合として, 次の 2 つ場合が挙げられる. 証明は明らかなので省略する.

Lemma 3.5 $f, g \in k[x]$ または $f, g \in k[y]$ のとき,

$$Rf \cap Rg = R \cdot \mathrm{lcm}(f, g).$$

Lemma 3.6 $f, g \in R$, f は g で右から割り切れるとする. このとき,

$$Rf \cap Rg = Rf.$$

そこで, これらの場合ほど明らかでない単項生成の場合について論じる.

議論に入る前に, 幾つかの定義と補題等を紹介する.

Definition 3.7 $f \in R$, $f = \sum_{\gamma=(a,b)} c_\gamma x^a y^b$, $c_\gamma \in k(\alpha)$ は有限個を除いて 0 とする. このとき,

$$F_f := \left\{ f^* \in R \quad | \quad f^* = \sum_{\gamma=(a,b)} c'_\gamma x^a y^b \quad c'_\gamma \in k(\alpha) \quad c_\gamma = 0 \Longleftrightarrow c'_\gamma = 0 \right\}$$

と定義する.

F_f は, 直観的には, 多項式 f の項の係数を 0 でない任意の係数に置き換えた多項式 f^* の全体の集合である.

Lemma 3.8 $f, m \in R$, m は単項式とする. このとき, $fm = mf^*$ を満たすような $f^* \in F_f$ が存在する.

(Proof)
$f = \sum_{\gamma=(a,b)} c_\gamma x^a y^b$, $c_\gamma \in k(\alpha)$ は有限個を除いて 0 とする. また, $m = x^{a'} y^{b'}$ とする.

$$\begin{aligned}
fm &= \left(\sum_{\gamma=(a,b)} c_\gamma x^a y^b \right) x^{a'} y^{b'} \\
&= \sum_{\gamma=(a,b)} c_\gamma \mathrm{sig}(x^a y^b, x^{a'} y^{b'}) x^{a+a'} y^{b+b'} \\
&= \sum_{\gamma=(a,b)} x^{a'} y^{b'} c_\gamma \frac{\mathrm{sig}(x^a y^b, x^{a'} y^{b'})}{\mathrm{sig}(x^{a'} y^{b'}, x^a y^b)} x^a y^b \\
&= x^{a'} y^{b'} \sum_{\gamma=(a,b)} c_\gamma \frac{\mathrm{sig}(x^a y^b, x^{a'} y^{b'})}{\mathrm{sig}(x^{a'} y^{b'}, x^a y^b)} x^a y^b = m \sum_{\gamma=(a,b)} c_\gamma \frac{\mathrm{sig}(x^a y^b, x^{a'} y^{b'})}{\mathrm{sig}(x^{a'} y^{b'}, x^a y^b)} x^a y^b
\end{aligned}$$

よって, $f^* = \sum_{\gamma=(a,b)} c_\gamma \frac{\mathrm{sig}(x^a y^b, x^{a'} y^{b'})}{\mathrm{sig}(x^{a'} y^{b'}, x^a y^b)} x^a y^b \in F_f$.
(証明終わり)

Definition 3.9 前補題の f^* を f_m^* と表す.

Proposition 3.10 $f(\neq 0) \in R$ とし, m_f を可換の意味での f の各項の最大公約単項式とする. このとき,

$$f = \widetilde{f} \cdot m_f$$

と表す表現が一意に存在する.

(Proof)

f は m_f で右から割り切れるので, 左除法定理から $\widetilde{f} \in R$ の存在性は明らか. また, 1 つの元で左除法定理アルゴリズムを用いて右から割るので, $\widetilde{f}$ の一意性についても明らか.
(証明終わり)

Definition 3.11 上の表現 $f = \widetilde{f} \cdot m_f$ を f の**単項式表現**という.

Example 3.12 $f = x^2y + xy^2 \in R$ とする.

$$f = \left(x + \frac{1}{\alpha}y\right) \cdot xy \quad \left(\widetilde{f} = x + \frac{1}{\alpha}y \quad m_f = xy\right)$$

が f の単項式表現である.

Lemma 3.13 $f(\neq 0) \in R$ とし, $f = \widetilde{f} \cdot m_f$ を f の単項式表現とする. このとき,

1. $m_{\widetilde{f}} = 1$.
2. $\forall \widetilde{f}^* \in F_{\widetilde{f}}$ に対し, $m_{\widetilde{f}^*} = 1$.
3. f が右から単項式 $m \in R$ で割り切れるとする. このとき, m_f は右から m で割り切れる.

(Proof)

1. 単項式表現の定義から明らか.
2. $\widetilde{f}$ と $\widetilde{f}^*$ では, 各項の変数の部分は同じなので, 明らか.
3. $f = t_1 + \cdots + t_s$ (t_i は f の項で互いに打ち消し合うものはない) とする. f が右から m で割り切れるということは, $t_i = a_i m$ を満たすような項 $a_i \in R$ が存在する. $t_i = \mathrm{sig}(a_i, m)(a_i * m)$ より, m は可換の意味で f の任意の項を割り切る. m_f は可換の意味で各項の最大公約単項式より, m_f は可換の意味で m で割り切れる. よって, $m_f = b * m = \dfrac{1}{\mathrm{sig}(b, m)} bm$ を満たす単項式 $b \in R$ が存在する. このことから, m_f は右から m で割り切れる.

(証明終わり)

Proposition 3.14 $f, g \in R$ を共に零でない多項式とし, $f = \widetilde{f} \cdot m_f, \quad g = \widetilde{g} \cdot m_g$ をそれぞれの単項式表現とする. このとき,

$$m_{fg} = m_f * m_g.$$

特に, $m_{fg} = m_{gf}$ である.

(Proof)
$fg = (\widetilde{f} \cdot m_f) \cdot (\widetilde{g} \cdot m_g) = (\widetilde{f} \cdot \widetilde{g}^*_{m_f}) m_f m_g = \left\{ \mathrm{sig}(m_f, m_g) \cdot \widetilde{f} \cdot \widetilde{g}^*_{m_f} \right\} (m_f * m_g)$
後は, $m_{\widetilde{f} \cdot \widetilde{g}^*_{m_f}} = 1$ を示せば良い. ここで着目したいのは, $h \in R$ に対し, $m_h = 1$ であるということは, h の項には, 定数項があるか, もしくは, x のみを含む項と y のみを含む項が共にあるということである. 今, $m_{\widetilde{f}} = m_{\widetilde{g}^*_{m_f}} = 1$ より,

$$\widetilde{f} = p + a_1 x^{b_1} + a_2 y^{b_2} + a_3 \quad \widetilde{g}^*_{m_f} = q + c_1 x^{d_1} + c_2 y^{d_2} + c_3$$
$p, q \in R$: 後の 3 つの単項式を含まない.
$b_i, d_i \geq 0$: それぞれ, x のみを含む項, y のみを含む項の次数として最小になるようにとる.
$$a_i, c_i \in k(\alpha)$$
$$a_3 = 0 \Longrightarrow a_1 \neq 0, \quad a_2 \neq 0, \quad b_1 > 0, \quad b_2 > 0$$
$$c_3 = 0 \Longrightarrow c_1 \neq 0, \quad c_2 \neq 0, \quad d_1 > 0, \quad d_2 > 0$$

とおける. $a_3 = c_3 = 0$ のとき,b_i, d_i の最小性から,

$$\widetilde{f} \cdot \widetilde{g}^*_{m_f} = r + a_1 c_1 x^{b_1 + d_1} + a_2 c_2 y^{b_2 + d_2}$$
$r \in R$: 後の 2 つの単項式を含まない.

のように表せ, $a_i c_i \neq 0, b_i + d_i > 0$ から x のみを含む項と y のみを含む項が共にあるので, $m_{\widetilde{f} \cdot \widetilde{g}^*_{m_f}} = 1$. $a_3 \neq 0$ かつ $c_3 \neq 0$ のとき, $\widetilde{f} \cdot \widetilde{g}^*_{m_f}$ には定数項 $a_3 c_3 (\neq 0)$ があるので, $m_{\widetilde{f} \cdot \widetilde{g}^*_{m_f}} = 1$. $a_3 \neq 0, c_3 = 0$ のとき,d_i の最小性から,

$$\widetilde{f} \cdot \widetilde{g}^*_{m_f} = r' + a_3 c_1 x^{d_1} + a_3 c_2 y^{d_2}$$
$r' \in R$: 後の 2 つの単項式を含まない.

のように表せ, $a_3 c_i \neq 0, d_i > 0$ から x のみを含む項と y のみを含む項が共にあるので, $m_{\widetilde{f} \cdot \widetilde{g}^*_{m_f}} = 1$. $a_3 = 0, c_3 \neq 0$ のときも同様に示せる. 以上により, $m_{\widetilde{f} \cdot \widetilde{g}^*_{m_f}} = 1$. よって, $m_{fg} = m_f * m_g$ がいえる. このことから, 特に, $m_{fg} = m_f * m_g = m_g * m_f = m_{gf}$ が成り立つ.
(証明終わり)

ここからは, 単項生成になることが明らかでないいくつかの場合の構成方法について述べる.

どちらか一方が単項式の場合, 計算実験より, 単項生成になるであろうという予想がつき, 単項生成元を具体的に構成し, それが正しいことを証明した.

Proposition 3.15 $f, m \in R$, m は単項式, 可換の意味で $\gcd(m_f, m) = m''$ とし, 可換の除法で $m' = \dfrac{m}{m''}$ とする. このとき,

$$Rf \cap Rm = Rm'f.$$

(Proof)

f は右から m'' で割り切れるので, $f = gm''$ を満たす $g \in R$ が存在する.

($\supset$): $m'f \in Rf$ は自明. また,

$$m'f = m'gm'' = g^*_{m'}m'm'' = g^*_{m'}\frac{1}{\mathrm{sig}(m', m'')}(m' * m'') = \frac{1}{\mathrm{sig}(m', m'')}g^*_{m'}m \in Rm.$$

($\subset$): $h \in Rf \cap Rm$ とする. h は, ある $a, b \in R$ によって $h = af = bm$ と表わせる.

$$agm'' = af = bm = b(m' * m'') = \frac{1}{\mathrm{sig}(m', m'')}bm'm''$$

よって, $ag = \dfrac{1}{\mathrm{sig}(m', m'')}bm'$ より, ag は右から m' で割り切れる. $a = \tilde{a} \cdot m_a$, $g = \tilde{g} \cdot m_g$ をそれぞれの単項式表現とすると, Proposition 3.14, Lemma 3.13 より, $m_a * m_g$ は右から m' で割り切れる. ここで, 可換の意味で $\gcd(m_g, m') = 1$ を示す. m'' のとりかたにより, g は m' の可換の意味での (定数以外の) 約数で割り切れない. よって, m_g は Proposition 3.14 より, m' の可換の意味での定数以外の任意の約数で割り切れない. 以上により, $\gcd(m_g, m') = 1$ である. 一方で, $m_a * m_g$ は右から m' で割り切れるので, 可換の意味でも $m_a * m_g$ は m' で割り切れることから, 可換の意味で m_a は m' で割り切れる. もちろん, m_a は右からも m' で割り切れるので, a は右から m' で割り切れる. よって, $a = pm$ を満たす $p \in R$ が存在し, $h = af = pm'f \in Rm'f$ である.

(証明終わり)

表での単項生成になる例はすべて f, g とも単項式ではない. 実はすべて $f = ag + cm$ ($c \in k(\alpha)$, $a, m \in R$, m は単項式) の関係を満たしている. さらに一般化して, $f = f'l$, $\ g = g'l$ (f', g' の右共通因子は定数以外にない) と表わした時に $f' = ag' + cm$ $\ (c \in k(\alpha),\ \ a, m \in R$, m は単項式) の関係を満たしている場合も, 単項生成になるであろうという予想を計算実験からたて, 単項生成元を具体的に構成し, それが正しいことを証明した. 特に $c = 1, a = 0$ とおくことにより, 前命題はこの場合の特別な例だったことがわかる.

Proposition 3.16 $f, g \in R$ を, $f', g', l \in R$ (f' と g' の右共通因子は定数のみ) を用いて, $f = f'l$, $g = g'l$ と表す. このとき,

$$g' = af' + cm$$
$$a, m \in R,\ m \text{ は単項式},\ c \in k(\alpha)^\times$$

と表すことが出来るならば,

$$Rf \cap Rg = R{f'}^*_m g.$$

(Proof)

($\supset$): ${f'}^*_m g \in Rg$ は明らか. また,

$${f'}^*_m g = {f'}^*_m g'l = {f'}^*_m(af' + cm)l = ({f'}^*_m af' + c{f'}^*_m m)l = ({f'}^*_m af' + cmf')l = ({f'}^*_m a + cm)f \in Rf.$$

($\subset$): $h \in Rf \cap Rg$ とする. $h \in Rg$ より, ある $p \in R$ によって, $h = pg = p(af' + cm)l$ と表せる. よって, p が右から ${f'}^*_m$ で割り切れることを示せばよい. 一方で, $h \in Rf$ でもあるので, ある $q \in R$ によって $h = qf$ と表せる. よって, $qf = p(af' + cm)l$ の両辺を右から l で割り, 式を整理することにより, $r = q - pa$ に対し,

$$cpm = rf' \tag{3.3}$$

となる. p, r, f' の単項式表現をそれぞれ, $p = \widetilde{p} \cdot m_p, r = \widetilde{r} \cdot m_r, f' = \widetilde{f}' \cdot m_{f'}$ とおき, (3.3) の両辺の単項式表現の単項式の部分を比較することにより,

$$m_p * m = m_r * m_{f'} \tag{3.4}$$

が得られる. また, p が右から ${f'}^*_m$ で割り切れることを示せばよいことと, (3.3) から, rf' が右から ${f'}^*_m m$ で割り切れることを示せばよいことになる. さらに, ${f'}^*_m m = mf'$ から, r が右から m で割り切れることを示せばよいことになる. 今, m と $m_{f'}$ が, 可換の意味で定数以外の共通因子 γ を持つとすると, m と $m_{f'}$ はそれぞれ右から γ で割り切れる. よって, $g' = a \cdot \widetilde{f}' \cdot m_{f'} + cm$ から, g' は右から γ で割り切れる. また, $f' = \widetilde{f}' \cdot m_{f'}$ も右から γ で割り切れる. このことは, f' と g' のとり方に矛盾する. よって, m と $m_{f'}$ は可換の意味で互いに素である. よって, (3.4) より, 可換の意味で m_r は m で割り切れる. よって, m_r は 右から m で割り切れるので, r は右から m で割り切れる.
(証明終わり)

一般に R では, 既約因子分解は一意ではなかった. よって, この命題における f', g' も一意ではない. また, f', g' を固定しても, $f' = ag' + cm$ の表現も一意ではない. 例えば, $f' = 2x^2 + xy$, $g' = x + y$ に対し, $f' = xg' + x^2 = 2xg' - xy$ である. しかし, この命題からわかることは, 表し方は一意ではないが, とにかく, ${g'}^*_m$ は 0 でない定数倍を除いて一意に定まるということである.

Example 3.17 $f, g \in R$ を

$$\begin{cases} f = (x+y)(x+1)(y+1) = (x+1)(x+y)(y+1) = x^2y + \alpha xy^2 + x^2 + (\alpha+1)xy + y^2 + x + y \\ g = (x+1)(x+y)(y+1) = x^2y + xy^2 + x^2 + 2xy + y^2 + x + y \end{cases}$$

と定める. f, g を共に右から $y+1$ で割ると, $f' = x^2 + \alpha xy + x + y, g' = x^2 + xy + x + y$ とおけ, f, g の右共通因子は定数のみであることが容易に確かめられる. ここで,

$$f' = g' + (\alpha - 1)xy$$

と表せ,

$${g'}^*_{xy} = \alpha^2 x^2 + xy + \alpha x + \frac{y}{\alpha}$$

より,

$$Rf \cap Rg = R \cdot \left(\alpha^2 x^2 + xy + \alpha x + \frac{y}{\alpha}\right) f = Rh$$

$$\begin{aligned} h = \alpha^2 x^4 y + \alpha^2 (\alpha+1) x^3 y^2 + \alpha^2 x^2 y^3 + \alpha^2 x^4 + \alpha(\alpha+1)^2 x^3 y + \alpha(3\alpha+2) x^2 y^2 + (\alpha+1) xy^3 \\ + \alpha(\alpha+1) x^3 + \alpha(2\alpha+3) x^2 y + 2(\alpha+1) xy^2 + \frac{y^3}{\alpha} + \alpha x^2 + (\alpha+1) xy + \frac{y^2}{\alpha} \end{aligned}$$

である. ちなみに左 $Gr\ddot{o}bner$ 基底アルゴリズムを用いて生成元を計算すると,

```
In[27]:=f=x^2*y+α*x*y^2+x^2+(α+1)*x*y+y^2+x+y
In[28]:=g=x^2*y+x*y^2+x^2+2x*y+y^2+x+y
In[29]:=NCGroebner[{t*f,(1-t)*g},{{0,0,1},{1,1,1},{1,0,1},{0,1,1},{1,1,0}},
         {x,y,t}]
```

Out[29]=
$$\left\{-\frac{tx}{-1+\alpha}-\frac{tx^2}{-1+\alpha}-\frac{ty}{-1+\alpha}-\frac{txy}{-1+\alpha}-\frac{tx^2y}{-1+\alpha}-\frac{ty^2}{-1+\alpha}-\frac{x\alpha}{-1+\alpha}+\frac{tx\alpha}{-1+\alpha}-\frac{x^2\alpha}{-1+\alpha}+\frac{tx^2\alpha}{-1+\alpha}-\frac{y\alpha}{-1+\alpha}+\frac{ty\alpha}{-1+\alpha}-\frac{2xy\alpha}{-1+\alpha}+\frac{txy\alpha}{-1+\alpha}-\frac{x^2y\alpha}{-1+\alpha}+\frac{tx^2y\alpha}{-1+\alpha}-\frac{y^2\alpha}{-1+\alpha}+\frac{ty^2\alpha}{-1+\alpha}-\frac{xy^2\alpha}{-1+\alpha},\right.$$
$$\frac{x}{-1+\alpha}+\frac{x^2}{-1+\alpha}+\frac{y}{-1+\alpha}+\frac{2xy}{-1+\alpha}-\frac{txy}{-1+\alpha}+\frac{x^2y}{-1+\alpha}+\frac{y^2}{-1+\alpha}+\frac{xy^2}{-1+\alpha}-\frac{txy^2}{-1+\alpha}+\frac{txy\alpha}{-1+\alpha}+\frac{txy^2\alpha}{-1+\alpha},$$
$$-\frac{ty^2}{-1+\alpha}-\frac{ty^3}{-1+\alpha}-\frac{x\alpha}{-1+\alpha}-\frac{x^2\alpha}{-1+\alpha}-\frac{y\alpha}{-1+\alpha}-\frac{2xy\alpha}{-1+\alpha}-\frac{x^2y\alpha}{-1+\alpha}-\frac{2y^2\alpha}{-1+\alpha}+\frac{ty^2\alpha}{-1+\alpha}-\frac{xy^2\alpha}{-1+\alpha}-\frac{y^3\alpha}{-1+\alpha}+\frac{ty^3\alpha}{-1+\alpha}-\frac{x^2\alpha^2}{-1+\alpha}-\frac{x^3\alpha^2}{-1+\alpha}-\frac{2xy\alpha^2}{-1+\alpha}-\frac{2x^2y\alpha^2}{-1+\alpha}-\frac{x^3y\alpha^2}{-1+\alpha}-\frac{3xy^2\alpha^2}{-1+\alpha}-\frac{x^2y^2\alpha^2}{-1+\alpha}-\frac{xy^3\alpha^2}{-1+\alpha}-\frac{x^2y\alpha^3}{-1+\alpha}-\frac{x^2y^2\alpha^3}{-1+\alpha},$$
$$\left.x^3+x^4+2x^2y+2x^3y+x^4y+3x^2y^2+x^3y^2+x^2y+\frac{y^2}{\alpha^3}+\frac{y^3}{\alpha^3}+\frac{xy}{\alpha^2}+\frac{2xy^2}{\alpha^2}+\frac{xy^3}{\alpha^2}+\frac{x^2}{\alpha}+\frac{x^3}{\alpha}+\frac{xy}{\alpha}+\frac{3x^2y}{\alpha}+\frac{x^3y}{\alpha}+\frac{2xy^2}{\alpha}+\frac{2x^2y^2}{\alpha}+\frac{xy^3}{\alpha}+x^3y\alpha+x^3y^2\alpha\right\}$$

より, $Rf\cap Rg=Rh'$,

$$h'=x^4y+(\alpha+1)\,x^3y^2+x^2y^3+x^4+\frac{(\alpha+1)^2}{\alpha}x^3y+\frac{(3\alpha+2)}{\alpha}x^2y^2+\frac{(\alpha+1)}{\alpha^2}xy^3+\frac{(\alpha+1)}{\alpha}x^3+\frac{(2\alpha+3)}{\alpha}x^2y+\frac{2\,(\alpha+1)}{\alpha^2}xy^2+\frac{y^3}{\alpha^3}+\frac{x^2}{\alpha}+\frac{(\alpha+1)}{\alpha^2}xy+\frac{y^2}{\alpha^3}$$

である. $h=\alpha^2h'$ より, 前命題の構成方法から求めたものと, 左 Gröbner 基底アルゴリズムを用いて求めたものは定数倍 (α^2 倍) を除いて同じである.

今までに紹介した単項生成になる例はすべてこのタイプであった. そこで疑問になるのが, それ以外の単項生成になる例が見つけられないかということである. そこで次の例がどうやら Proposition3.16 の逆の反例になっているようである.

Example 3.18 $f,g\in R$ を

$$\begin{cases} f=x^2y+x^2+\dfrac{(\alpha+1)}{\alpha}xy+\dfrac{(\alpha+1)}{\alpha}x+\dfrac{y}{\alpha}+\dfrac{1}{\alpha}\\ g=xy^2+\dfrac{(\alpha+1)}{\alpha}xy+\dfrac{y^2}{\alpha^2}+\dfrac{x}{\alpha}+\dfrac{(\alpha+1)}{\alpha^2}y+\dfrac{1}{\alpha}\end{cases}$$

と定める. 実はこの f,g は, $R\cdot(x+1)\cap R\cdot(y+1)$ の生成元であったが, $Rf\cap Rg$ の生成元を 左 Gröbner 基底アルゴリズムを用いて計算すると, 単項生成になり, その生成元は,

$$h=x^2y^2+\frac{(\alpha+1)}{\alpha}x^2y+\frac{(\alpha+1)}{\alpha^2}xy^2+\frac{x^2}{\alpha}+\frac{2\,(\alpha+1)}{\alpha^2}xy+\frac{y^2}{\alpha^3}+\frac{(\alpha+1)}{\alpha^2}$$

となる. 今, h をそれぞれ右から f と g で割ると,

$$h = \left(\frac{y}{\alpha^2} + \frac{1}{\alpha}\right) f = \left(x + \frac{1}{\alpha}\right) g$$

となる. もし, この f と g が Proposition3.16 の仮定 (f と g は入れ替えても良い) を満たしているとするならば,

$$f = f'l_1,\quad g = p^*l_1 \quad (p^* \in F_{y+1}, f' \text{と } p^* \text{の右共通因子は定数のみ}) \text{ を満たす } l_1 \in R \text{ が存在する.} \tag{3.5}$$

もしくは,

$$f = q^*l_2,\quad g = g'l_2 \quad (q^* \in F_{x+1}, q^* \text{と } g' \text{の右共通因子は定数のみ}) \text{ を満たす } l_2 \in R \text{ が存在する.} \tag{3.6}$$

を満たしているはずである. ところが,

$$\begin{cases} r_1 = \alpha xy + x + y + 1 \\ r_2 = \alpha xy + \alpha x + y + \alpha \\ r_3 = \alpha xy + \alpha x + y + 1 \end{cases} \qquad r_1, r_2, r_3 \in R$$

に対し,

$$\begin{cases} g = \left(\dfrac{y}{\alpha^2} + \dfrac{1}{\alpha}\right) r_1 & \dfrac{y}{\alpha^2} + \dfrac{1}{\alpha} \in F_{y+1} \\ g = \left(\dfrac{y}{\alpha^2} + \dfrac{1}{\alpha^2}\right) r_2 & \dfrac{y}{\alpha^2} + \dfrac{1}{\alpha^2} \in F_{y+1} \\ f = \left(\dfrac{x}{\alpha} + \dfrac{1}{\alpha}\right) r_3 & \dfrac{x}{\alpha} + \dfrac{1}{\alpha} \in F_{x+1} \end{cases} \tag{3.7}$$

と表されるが, f を右から r_1, r_2, g を右から r_3 で割ると.

$$\begin{cases} f = \left(\dfrac{x}{\alpha} + \dfrac{1}{\alpha}\right) r_1 + \dfrac{(\alpha-1)}{\alpha} x^2 + \dfrac{(\alpha-1)}{\alpha} x \\ f = \left(\dfrac{x}{\alpha} + \dfrac{1}{\alpha}\right) r_2 - \dfrac{(\alpha-1)}{\alpha} x - \dfrac{(\alpha-1)}{\alpha} \\ g = \left(\dfrac{y}{\alpha^2} + \dfrac{1}{\alpha^2}\right) r_3 + \dfrac{(\alpha-1)}{\alpha^2} y + \dfrac{(\alpha-1)}{\alpha^2} \end{cases}$$

となり, 割り切れない. ここで, $g = p^*r,\quad f = q^*r' \quad (p^* \in F_{y+1},\quad q^* \in F_{x+1} \quad r, r' \in R)$ と表せたときのそれぞれの因子は, (3.7) の因子の零でない定数倍のみであろう. よって, 同じく, f を右から r_1, r_2 の零でない定数倍, g を右から r_3 の零でない定数倍で割っても割り切れない. よって, (3.5) を満たす l_1 と, (3.6) を満たす l_2 は存在しないと思われる. 以上により, この例は, Proposition3.16 の仮定を満たしていないと思われるが, 単項生成になる.

さらに, $Rf \cap Rg$ が単項生成になるような $f, g \in R$ に対し、次の 2 つの補題が成り立つ.

Lemma 3.19 $f, g \in R$ に対し, $Rf \cap Rg$ が単項生成とする. その生成元を pg $(p \in R)$ とすると任意の単項式 $m \in R$ に対し,

$$Rf \cap Rmg = Rp'^*_{m''}mg.$$

ただし, 単項式 $m' \in R$ を p, m の右最大共通因子とし, $p = p'm'$, $m = m' * m''$ $(p', m'' \in R,\ m''$ は単項式) とする.

(Proof)
($\supset$):
$$p'^{*}_{m''}mg = \frac{1}{\mathrm{sig}(m'', m')}p'^{*}_{m''}m''m'g = \frac{1}{\mathrm{sig}(m'', m')}m''p'm'g = \frac{1}{\mathrm{sig}(m'', m')}m''pg.$$
$pg \in Rf$ でもあるので, $p'^{*}_{m''}mg \in Rf \cap Rmg$.
($\subset$): $q \in Rf \bigcap Rmg$ とすると, ある $s, t \in R$ によって, $q = sf = tmg$ と表せる. よって, t が右から $p'^{*}_{m''}$ で割り切れることを示せばよい. 一方で, $q \in Rf \cap Rg$ でもあるので, ある $r \in R$ によって, $q = rpg$ と表せる. よって, $rpg = tmg$ の両辺を右から g で割り, 式を整理することにより,
$$rp' = \frac{1}{\mathrm{sig}(m'', m,)}tm''$$
となる. さらに, 両辺の左から m'' をかけて, 式を整理することにより,
$$r^{*}_{m''}p'^{*}_{m''} = \frac{1}{\mathrm{sig}(m'', m')}m''t$$
となる. よって, $m''t$ は右から $p'^{*}_{m''}$ で割り切れて, さらに m'' のとり方により, t は右から $p'^{*}_{m''}$ で割り切れる.
(証明終わり)

Lemma 3.20 $f, g \in R$ に対し, $Rf \cap Rg$ が単項生成とする. その生成元を pg ($p \in R$) とすると任意の $a \in R$ に対し,
$$Rf \cap R \cdot (af + g) = Rp(af + g).$$
(Proof)
($\supset$): $p(af + g) = paf + pg$ で, $pg \in Rf$ より, $p(af + g) \in Rf \cap Rp(af + g)$.
($\subset$): $q \in Rf \cap R \cdot (af + g)$ とすると, ある $s, t \in R$ によって, $q = sf = t(af + g)$ と表せる. よって, t が右から p で割り切れることを示せばよい. $sf = t(af + g)$ を整理して, $(s - ta)f = tg$ となり, tg は右から f で割り切れる. よって, $tg \in Rf$ となり, さらに, $tg \in Rg$ より, $tg \in Rpg$ となる. よって, t は右から p で割り切れる.
(証明終わり)
この 2 つの補題をまとめることにより, 次の命題が導かれる.

Proposition 3.21 $f, g \in R$ に対し, $Rf \cap Rg$ が単項生成とする. その生成元を pg ($p \in R$) とすると, 任意の $a \in R$, $c \in k(\alpha)^{\times}$, 任意の単項式 $m \in R$ に対し,
$$Rf \cap R \cdot (af + cmg) = Rp'^{*}_{m''}(af + cmg).$$
ただし, 単項式 $m' \in R$ を p, m の右最大共通因子とし, $p = p'm'$, $m = m' * m''$ ($p', m'' \in R$, m'' は単項式) とする.

ここで疑問となるのが, 単項生成になるための必要十分条件は何かということである. さらに, 前に述べたが, 計算機実験の計算結果から, 左単項生成イデアルの共通部分の生成元は, 特に辞書式順序に関して, 高々2 元で生成されるのではないかという予想がたつ. またさらにその 2 つの元でそれぞれ単項生成される左イデアルの共通部分の生成元を計算したところ単項生成になったことから, この場合も単項生成になるのではないかという予想もたつ. 次節でこれらの問題と予想をまとめた. この節では最後に, 表での単項生成にならない例での, 辞書式順序に関しての 2 つの生成元を記載しておく.

Example 3.22

1. $f = x + y, g = y + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は
$$\left\{x^2y - \frac{y^3}{\alpha^3} + x^2 - \frac{(\alpha+1)}{\alpha^2}xy - \frac{\left(\alpha^2+\alpha+1\right)}{\alpha^3}y^2 - \frac{(\alpha+1)}{\alpha^2}x - \frac{(\alpha+1)}{\alpha^2}y, xy^2 + \frac{y^3}{\alpha^2} + \frac{(\alpha+1)}{\alpha}xy + \frac{(\alpha+1)}{\alpha^2}y^2 + \frac{x}{\alpha} + \frac{y}{\alpha}\right\}$$
である．

2. $f = x^2 + 1, g = y^2 + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は
$$\left\{x^4y^2 + x^4 + \frac{\left(\alpha^4+1\right)}{\alpha^4}x^2y^2 + \frac{\left(\alpha^4+1\right)}{\alpha^4}x^2 + \frac{y^2}{\alpha^4} + \frac{1}{\alpha^4}, x^2y^4 + \frac{y^4}{\alpha^8} + \frac{\left(\alpha^4+1\right)}{\alpha^4}x^2y^2 + \frac{x^2}{\alpha^4} + \frac{\left(\alpha^4+1\right)}{\alpha^8}y^2 + \frac{1}{\alpha^4}\right\}$$
である．

3. $f = x^3 + y, g = y^3 + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は
$$\left\{x^6y^3 + \frac{\left(\alpha^9+1\right)}{\alpha^9}x^3y^4 + x^6 + \frac{y^5}{\alpha^{12}} + \frac{\left(\alpha^9+1\right)}{\alpha^9}x^3y + \frac{y^2}{\alpha^{12}}, x^3y^6 + \frac{y^7}{\alpha^{18}} + \frac{\left(\alpha^9+1\right)}{\alpha^9}x^3y^3 + \frac{\left(\alpha^9+1\right)}{\alpha^{18}}y^4 + \frac{x^3}{\alpha^9} + \frac{y}{\alpha^9}\right\}$$
である．

4. $f = x^3 + 1, g = y^3 + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は
$$\left\{x^6y^3 + x^6 + \frac{\left(\alpha^9+1\right)}{\alpha^9}x^3y^3 + \frac{\left(\alpha^9+1\right)}{\alpha^9}x^3 + \frac{y^3}{\alpha^9} + \frac{1}{\alpha^9}, x^3y^6 + \frac{\left(\alpha^9+1\right)}{\alpha^9}x^3y^3 + \frac{y^6}{\alpha^{18}} + \frac{x^3}{\alpha^9} + \frac{\left(\alpha^9+1\right)}{\alpha^{18}}y^3 + \frac{1}{\alpha^9}\right\}$$
である．

5. $f = x^{10}y^8 - x^5y^6, g = x^7y^3 - x^2y^2$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は
$$\left\{x^{15}y^{10} - \alpha^{15}x^{15}y^9 - \frac{x^{10}y^9}{\alpha^{35}} + \alpha^{10}x^{10}y^7 + \frac{x^5y^7}{\alpha^{40}} - \frac{x^5y^6}{\alpha^{10}}, x^{20}y^6 - \frac{x^{15}y^9}{\alpha^{45}} - \frac{x^{15}y^8}{\alpha^{25}} - \frac{x^{15}y^7}{\alpha^5} + \frac{x^{10}y^8}{\alpha^{75}} + \frac{x^{10}y^7}{\alpha^{50}} + \frac{x^{10}y^6}{\alpha^{25}} - \frac{x^5y^6}{\alpha^{75}}\right\}$$
である．

6. $f = xy + x + 1, g = x + y$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は
$$\left\{x^3y + \frac{\left(\alpha^4+3\alpha^3+3\alpha^2+2\alpha+1\right)}{\alpha\left(2\alpha^2+2\alpha+1\right)}x^2y^2 + \frac{\left(\alpha^2+3\alpha+1\right)}{\alpha\left(2\alpha^2+2\alpha+1\right)}xy^3 + x^3 + \frac{\left(\alpha^3+3\alpha^2+4\alpha+2\right)}{2\alpha^2+2\alpha+1}x^2y + \frac{\left(\alpha^3+\alpha^2+2\alpha+1\right)}{\alpha\left(2\alpha^2+2\alpha+1\right)}xy^2\right.$$
$$+\frac{\left(2\alpha^3+3\alpha^2+\alpha-1\right)}{\alpha\left(2\alpha^2+2\alpha+1\right)}x^2 + \frac{\left(2\alpha^4+3\alpha^3+2\alpha^2+2\alpha+1\right)}{\alpha\left(2\alpha^2+2\alpha+1\right)}xy + \frac{\left(\alpha^2+3\alpha+1\right)}{\alpha^3\left(2\alpha^2+2\alpha+1\right)}y^2 + \frac{\left(\alpha^2-1\right)}{\alpha\left(2\alpha^2+2\alpha+1\right)}x + \frac{\left(\alpha^2-1\right)}{\alpha\left(2\alpha^2+2\alpha+1\right)}y,$$
$$\left.x^2y^3 + \frac{xy^4}{\alpha^3} + \frac{(\alpha+1)}{\alpha}x^2y^2 + \frac{(\alpha+1)}{\alpha^3}xy^3 + \frac{\left(\alpha^2-1\right)}{\alpha^3}x^2y + \frac{xy^2}{\alpha^2} + \frac{y^3}{\alpha^6} - \frac{x^2}{\alpha^3} + \frac{y^2}{\alpha^4} - \frac{x}{\alpha^3} - \frac{y}{\alpha^3}\right\}$$
である．

7. $f = xy + x + 1, g = x + y + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は
$$\left\{x^3y - \frac{xy^3}{\alpha^3} + x^3 - \frac{(\alpha+1)}{\alpha^3}x^2y - \frac{\left(\alpha^3+\alpha^2+2\alpha+1\right)}{\alpha^4}xy^2 + \frac{\left(\alpha^3-\alpha-1\right)}{\alpha^3}x^2 - \frac{\left(\alpha^3+2\alpha^2+2\alpha+2\right)}{\alpha^4}xy - \frac{y^2}{\alpha^5} - \frac{\left(2\alpha^2+2\alpha+1\right)}{\alpha^4}x\right.$$
$$-\frac{\left(\alpha^3+\alpha^2+\alpha+1\right)}{\alpha^5}y - \frac{\left(\alpha^2+\alpha+1\right)}{\alpha^4},$$
$$\left.x^2y^2 + \frac{xy^3}{\alpha^2} + \frac{\left(\alpha^2+\alpha+1\right)}{\alpha^2}x^2y + \frac{(\alpha+1)^2}{\alpha^3}xy^2 + \frac{(\alpha+1)}{\alpha^2}x^2 + \frac{2\left(\alpha^2+\alpha+1\right)}{\alpha^3}xy + \frac{y^2}{\alpha^4} + \frac{(\alpha+1)^2}{\alpha^3}x + \frac{\left(\alpha^2+\alpha+1\right)}{\alpha^4}y + \frac{(\alpha+1)}{\alpha^3}\right\}$$
である．

8. $f = x + y + 1, g = xy + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\Bigg\{x^3y + \frac{\left(\alpha^4+3\alpha^3+2\alpha^2+2\alpha+1\right)}{\alpha\left(\alpha^2+2\alpha+2\right)}x^2y^2 + \frac{\left(\alpha^2+3\alpha+1\right)}{\alpha\left(\alpha^2+2\alpha+2\right)}xy^3 + \frac{\left(\alpha^3+2\alpha^2+4\alpha+3\right)}{\alpha\left(\alpha^2+2\alpha+2\right)}x^2y + \frac{\left(2\alpha^3+4\alpha^2+3\alpha+1\right)}{\alpha^2\left(\alpha^2+2\alpha+2\right)}xy^2 + x^2$$

$$+\frac{\left(\alpha^4+3\alpha^3+4\alpha^2+5\alpha+2\right)}{\alpha^2\left(\alpha^2+2\alpha+2\right)}xy + \frac{\left(\alpha^2+3\alpha+1\right)}{\alpha^3\left(\alpha^2+2\alpha+2\right)}y^2 + \frac{\left(2\alpha^3+4\alpha^2+3\alpha+1\right)}{\alpha^3\left(\alpha^2+2\alpha+2\right)}y + \frac{(2\alpha+3)}{\alpha\left(\alpha^2+2\alpha+2\right)},$$

$$x^2y^3 + \frac{xy^4}{\alpha^3} + \frac{x^2y^2}{\alpha^2} + \frac{(\alpha+1)}{\alpha^4}xy^3 - \frac{x^2y}{\alpha^3} + \frac{xy^2}{\alpha^4} + \frac{y^3}{\alpha^6} + \frac{(\alpha+1)}{\alpha^6}y^2 - \frac{x}{\alpha^3} - \frac{\left(\alpha^2-1\right)}{\alpha^5}y - \frac{1}{\alpha^3}\Bigg\}$$

である．

9. $f = x^2 + x + y + 1, g = y + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\Bigg\{x^3y + x^3 + \frac{(\alpha+1)}{\alpha}x^2y + \frac{xy^2}{\alpha^2} + \frac{(\alpha+1)}{\alpha}x^2 + \frac{\left(\alpha^2+\alpha+1\right)}{\alpha^2}xy + \frac{y^2}{\alpha^2} + \frac{(\alpha+1)}{\alpha^2}x + \frac{(\alpha+1)}{\alpha^2}y + \frac{1}{\alpha},$$

$$x^2y^2 + \frac{(\alpha+1)}{\alpha}x^2y + \frac{xy^2}{\alpha^2} + \frac{y^3}{\alpha^4} + \frac{x^2}{\alpha} + \frac{(\alpha+1)}{\alpha^2}xy + \frac{\left(\alpha^2+\alpha+1\right)}{\alpha^4}y^2 + \frac{x}{\alpha} + \frac{\left(\alpha^2+\alpha+1\right)}{\alpha^3}y + \frac{1}{\alpha}\Bigg\}$$

である．

10. $f = x + y^2 + 1, g = x^2 + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\Bigg\{\alpha^2x^2y^4 + \left(\alpha^4+1\right)x^3y^2 + x^4 + \frac{\left(\alpha^4+1\right)}{\alpha^2}x^2y^2 + \frac{y^4}{\alpha^6} + \frac{\left(\alpha^2+1\right)}{\alpha^2}x^3 + \frac{\left(\alpha^4+1\right)}{\alpha^4}xy^2 + \frac{\left(\alpha^2+1\right)}{\alpha^2}x^2 + \frac{\left(\alpha^4+1\right)}{\alpha^6}y^2 + \frac{\left(\alpha^2+1\right)}{\alpha^2}x + \frac{1}{\alpha^2},$$

$$\frac{x^2y^6}{\alpha^4} + x^3y^4 + \frac{\left(\alpha^4+\alpha^2+1\right)}{\alpha^8}x^2y^4 + \frac{y^6}{\alpha^{16}} + \frac{\left(\alpha^2+1\right)}{\alpha^6}x^3y^2 + \frac{xy^4}{\alpha^8} + \frac{\left(2\alpha^4+\alpha^2+1\right)}{\alpha^{10}}x^2y^2 + \frac{\left(\alpha^4+\alpha^2+1\right)}{\alpha^{16}}y^4 + \frac{2x^3}{\alpha^{10}} + \frac{\left(\alpha^2+1\right)}{\alpha^{10}}xy^2$$

$$+\frac{2x^2}{\alpha^{10}} + \frac{\left(2\alpha^4+\alpha^2+1\right)}{\alpha^{14}}y^2 + \frac{2x}{\alpha^{10}} + \frac{2}{\alpha^{10}}\Bigg\}$$

である．

11. $f = x^2 + y^2, g = x + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{x^4 + x^2y^2 + \frac{\left(\alpha^2+1\right)}{\alpha^2}x^3 + \frac{\left(\alpha^2+1\right)}{\alpha^2}xy^2 + \frac{x^2}{\alpha^2} + \frac{y^2}{\alpha^2}, x^3y^2 + \frac{xy^4}{\alpha^4} + \frac{x^2y^2}{\alpha^4} + \frac{y^4}{\alpha^8} + \frac{x^3}{\alpha^6} + \frac{xy^2}{\alpha^6} + \frac{x^2}{\alpha^6} + \frac{y^2}{\alpha^6}\right\}$$

である．

12. $f = x^2 - y^2 - 1, g = x - y$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\Bigg\{x^4 - \left(\alpha^2+1\right)x^3y + (\alpha-1)x^2y^2 + \frac{\left(\alpha^2+1\right)}{\alpha^2}xy^3 - \frac{y^4}{\alpha^3} - x^2 + \frac{\left(\alpha^2+1\right)}{\alpha^2}xy - \frac{y^2}{\alpha^3},$$

$$x^3y^2 - \frac{x^2y^3}{\alpha^2} - \frac{xy^4}{\alpha^4} + \frac{y^5}{\alpha^8} + \frac{x^3}{\alpha^5(\alpha-1)} - \frac{x^2y}{\alpha^3(\alpha-1)} - \frac{\left(\alpha^2-\alpha+1\right)}{\alpha^5(\alpha-1)}xy^2 + \frac{\left(\alpha^3+\alpha-1\right)}{\alpha^8(\alpha-1)}y^3 + \frac{x}{\alpha^5(\alpha-1)} + \frac{y}{\alpha^5(\alpha-1)}\Bigg\}$$

である．

13. $f = x^2 - y^2 - 1, g = x - y + 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{x^4 - \frac{(\alpha+1)}{\alpha}x^2y^2 + \frac{y^4}{\alpha^5} + \frac{\left(\alpha^3+\alpha^2+\alpha+1\right)}{\alpha^3(\alpha-1)}x^3 - \frac{\left(2\alpha^3+\alpha^2+1\right)}{\alpha^3(\alpha-1)}x^2y - \frac{\left(\alpha^3+\alpha^2+\alpha+1\right)}{\alpha^3(\alpha-1)}xy^2 + \frac{\left(2\alpha^3+\alpha^2+1\right)}{\alpha^5(\alpha-1)}y^3\right.$$

$$-\frac{\left(\alpha^5-\alpha^4-2\alpha^2-\alpha-1\right)}{\alpha^4(\alpha-1)}x^2 - \frac{\left(2\alpha^3+\alpha^2+1\right)}{\alpha^5(\alpha-1)}y^2 - \frac{\left(\alpha^3+\alpha^2+\alpha+1\right)}{\alpha^3(\alpha-1)}x + \frac{\left(2\alpha^3+\alpha^2+1\right)}{\alpha^5(\alpha-1)}y - \frac{\left(2\alpha^2+\alpha+1\right)}{\alpha^4(\alpha-1)},$$

$$x^3y - \frac{x^2y^2}{\alpha} + \frac{y^4}{\alpha^5} - \frac{xy^3}{\alpha^2} + \frac{(\alpha+1)}{\alpha^3(\alpha-1)}x^3 - \frac{\left(\alpha^2+1\right)}{\alpha^3(\alpha-1)}x^2y - \frac{(\alpha+1)}{\alpha^3(\alpha-1)}xy^2 + \frac{\left(\alpha^2+1\right)}{\alpha^5(\alpha-1)}y^3 + \frac{(\alpha+1)}{\alpha^4(\alpha-1)}x^2 - \frac{xy}{\alpha^2}$$

$$\left.-\frac{\left(\alpha^2+1\right)}{\alpha^5(\alpha-1)}y^2 - \frac{(\alpha+1)}{\alpha^3(\alpha-1)}x + \frac{\left(\alpha^2+1\right)}{\alpha^5(\alpha-1)}y - \frac{(\alpha+1)}{\alpha^4(\alpha-1)}\right\}$$

である．

14. $f = x^4 - xy, g = y - 1$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{x^7y - x^7 - \frac{\left(\alpha^3+1\right)}{\alpha^6}x^4y + \frac{\left(\alpha^3+1\right)}{\alpha^6}x^4 - \frac{xy^3}{\alpha^9} + \frac{\left(\alpha^6+\alpha^3+1\right)}{\alpha^9}xy^2 - \frac{\left(\alpha^3+1\right)}{\alpha^6}xy, x^4y^2 - \frac{\left(\alpha^3+1\right)}{\alpha^3}x^4y + \frac{x^4}{\alpha^3} - \frac{xy^3}{\alpha^6} + \frac{\left(\alpha^3+1\right)}{\alpha^6}xy^2 - \frac{xy}{\alpha^3}\right\}$$

である．

15. $f = x^2y - xy, g = xy^2 - xy$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{x^3y^2 - x^3y - \frac{(\alpha+1)}{\alpha}x^2y^2 + \frac{(\alpha+1)}{\alpha}x^2y + \frac{xy^2}{\alpha} - \frac{xy}{\alpha}, x^2y^3 - \frac{(\alpha+1)}{\alpha}x^2y^2 - \frac{xy^3}{\alpha^2} + \frac{x^2y}{\alpha} + \frac{(\alpha+1)}{\alpha^2}xy^2 - \frac{xy}{\alpha}\right\}$$

である．

16. $f = x^2y - xy - x, g = xy^2 - xy + y$ とする．$Rf \cap Rg$ の辞書式順序に関する Gröbner 基底は

$$\left\{x^4y^3 - \frac{\alpha(2\alpha+3)}{\alpha^2+2\alpha+2}x^3y^4 - x^4y^2 + \frac{\left(\alpha^4-4\alpha^2-5\alpha-2\right)}{\alpha^2\left(\alpha^2+2\alpha+2\right)}x^3y^3 + \frac{(2\alpha+3)}{\alpha^2\left(\alpha^2+2\alpha+2\right)}x^2y^4 + \frac{\left(\alpha^4+3\alpha^3+4\alpha^2+5\alpha+2\right)}{\alpha^2\left(\alpha^2+2\alpha+2\right)}x^3y^2\right.$$

$$-\frac{\left(\alpha^3-3\alpha-3\right)}{\alpha^3\left(\alpha^2+2\alpha+2\right)}x^2y^3 + \frac{x^3y}{\alpha} - \frac{\left(\alpha^4+4\alpha^3+8\alpha^2+6\alpha+1\right)}{\alpha^3\left(\alpha^2+2\alpha+2\right)}x^2y^2 + \frac{(2\alpha+3)}{\alpha^4\left(\alpha^2+2\alpha+2\right)}xy^3 - \frac{\left(\alpha^4+2\alpha^3+3\alpha^2+5\alpha+4\right)}{\alpha^3\left(\alpha^2+2\alpha+2\right)}x^2y$$

$$+\frac{\left(\alpha^3+5\alpha^2+6\alpha+3\right)}{\alpha^4\left(\alpha^2+2\alpha+2\right)}xy^2 + \frac{\left(\alpha^2+5\alpha+4\right)}{\alpha^3\left(\alpha^2+2\alpha+2\right)}xy,$$

$$x^3y^5 - \frac{\left(\alpha^2-1\right)}{\alpha^2}x^3y^4 - \frac{x^2y^5}{\alpha^4} - \frac{(\alpha+1)}{\alpha^3}x^3y^3 + \frac{\left(\alpha^2-1\right)}{\alpha^5}x^2y^4 + \frac{x^3y^2}{\alpha^3} + \frac{(\alpha+2)}{\alpha^4}x^2y^3 - \frac{xy^4}{\alpha^7} - \frac{\left(\alpha^2-1\right)}{\alpha^5}x^2y^2 - \frac{(\alpha+1)}{\alpha^7}xy^3 - \frac{x^2y}{\alpha^4}$$

$$\left.+\frac{\left(\alpha^2-1\right)}{\alpha^6}xy^2 + \frac{xy}{\alpha^4}\right\}$$

である．

17. $f = x^4 - xy, g = x + y^3$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{\alpha^5x^4y^6 + \left(\alpha^8+1\right)x^5y^3 - \frac{xy^7}{\alpha^{13}} + x^6 - \frac{\left(\alpha^8+1\right)}{\alpha^9}x^2y^4 - x^3y, \frac{x^4y^{11}}{\alpha^8} + x^5y^8 - \frac{xy^{12}}{\alpha^{41}} - \frac{x^2y^9}{\alpha^{24}} + \frac{x^4y^3}{\alpha^{15}} + \frac{x^5}{\alpha^{23}} - \frac{xy^4}{\alpha^{24}} - \frac{x^2y}{\alpha^{23}}\right\}$$

である．

18. $f = x^2 + y, g = y^2 + x$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{\alpha x^2y^4 + (\alpha+1)\,x^3y^2 + \frac{y^5}{\alpha^7} + x^4 + \frac{\left(\alpha^3+1\right)}{\alpha^4}xy^3 + x^2y,\ \frac{x^2y^5}{\alpha^3} + x^3y^3 + \frac{y^6}{\alpha^{13}} + \frac{xy^4}{\alpha^6} + \frac{x^2y^2}{\alpha^4} + \frac{x^3}{\alpha^7} + \frac{y^3}{\alpha^8} + \frac{xy}{\alpha^7}\right\}$$

である．

19. $f = x^3 + y, g = y^3 + x$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{\alpha^5x^3y^6 + \left(\alpha^8+1\right)x^4y^3 + \frac{y^7}{\alpha^{13}} + x^5 + \frac{\left(\alpha^8+1\right)}{\alpha^9}xy^4 + x^2y,\ \frac{x^3y^{11}}{\alpha^8} + x^4y^8 + \frac{y^{12}}{\alpha^{41}} + \frac{xy^9}{\alpha^{24}} - \frac{x^3y^3}{\alpha^{15}} - \frac{x^4}{\alpha^{23}} - \frac{y^4}{\alpha^{24}} - \frac{xy}{\alpha^{23}}\right\}$$

である．

20. $f = x^3 + y^2, g = y^3 + x^2$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{\alpha^3x^3y^7 + \alpha^{11}x^5y^4 + \frac{y^9}{\alpha^{18}} + \frac{x^2y^6}{\alpha} + \alpha^5x^4y^3 + x^6 + \frac{xy^5}{\alpha^4} + x^3y^2,\right.$$

$$\left.\frac{x^3y^8}{\alpha^{10}} + x^5y^5 + \frac{y^{10}}{\alpha^{34}} + \frac{x^2y^7}{\alpha^{15}} + \frac{\left(\alpha^5-1\right)}{\alpha^{12}}x^4y^4 + \frac{\left(\alpha^5-1\right)}{\alpha^{24}}xy^6 + \frac{x^3y^3}{\alpha^{13}} + \frac{x^5}{\alpha^{18}} + \frac{y^5}{\alpha^{22}} + \frac{x^2y^2}{\alpha^{18}}\right\}$$

である．

21. $f = x^3y + y^2, g = xy^3 + x^2$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{\alpha^3x^4y^7 + \frac{\left(\alpha^8+1\right)}{\alpha}x^5y^4 + \frac{xy^8}{\alpha^{15}} + x^6y + \frac{\left(\alpha^8+1\right)}{\alpha^{10}}x^2y^5 + x^3y^2,\ \frac{x^4y^{12}}{\alpha^9} + x^5y^9 + \frac{xy^{13}}{\alpha^{42}} + \frac{x^2y^{10}}{\alpha^{24}} - \frac{x^4y^4}{\alpha^{13}} - \frac{x^5y}{\alpha^{20}} - \frac{xy^5}{\alpha^{22}} - \frac{x^2y^2}{\alpha^{20}}\right\}$$

である．

22. $f = x^3y + xy^2, g = xy^3 + x^2$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{x^3y^7 + \frac{xy^8}{\alpha^{12}} + \frac{\left(\alpha^5+1\right)}{\alpha}x^4y^4 + \frac{\left(\alpha^5+1\right)}{\alpha^7}x^2y^5 + x^5y + x^3y^2,\ \frac{x^3y^9}{\alpha^6} + \frac{xy^{10}}{\alpha^{22}} + x^4y^6 + \frac{x^2y^7}{\alpha^{10}} + \frac{x^3y^4}{\alpha^6} + \frac{xy^5}{\alpha^{12}} + \frac{x^4y}{\alpha^{10}} + \frac{x^2y^2}{\alpha^{10}}\right\}$$

である．

23. $f = x^5y + x^3y^2, g = xy^3 + x^2y$ とする．$Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{\alpha x^5y^5 + \left(\alpha^3+1\right)x^6y^3 + \frac{x^3y^6}{\alpha^7} + x^7y + \frac{\left(\alpha^3+1\right)}{\alpha^4}x^4y^4 + x^5y^2,\ \frac{x^5y^6}{\alpha^3} + x^6y^4 + \frac{x^3y^7}{\alpha^{13}} + \frac{x^4y^5}{\alpha^6} + \frac{x^5y^3}{\alpha^4} + \frac{x^6y}{\alpha^7} + \frac{x^3y^4}{\alpha^8} + \frac{x^4y^2}{\alpha^7}\right\}$$

である．

24. $f = x^5y^{10} + x^3y^7, g = x^{10}y^3 + x^2y^8$ とする．$Rf \cap Rg$ の辞書式順序に関する Gröbner 基底は

$$\left\{-\alpha^{44}x^{13}y^{24} - \frac{x^5y^{29}}{\alpha^{124}} - \frac{x^{11}y^{21}}{\alpha^{18}} - \frac{x^3y^{26}}{\alpha^{162}} + x^{15}y^{10} + \frac{x^7y^{15}}{\alpha^{56}} + x^{13}y^7 + \frac{x^5y^{12}}{\alpha^{32}},\right.$$

$$\left.x^{13}y^{27} + \frac{x^5y^{32}}{\alpha^{192}} + \frac{x^{11}y^{24}}{\alpha^{68}} + \frac{x^3y^{29}}{\alpha^{236}} + \frac{x^{13}y^{10}}{\alpha^{78}} + \frac{x^5y^{15}}{\alpha^{134}} + \frac{x^{11}y^7}{\alpha^{78}} + \frac{x^3y^{12}}{\alpha^{110}}\right\}$$

である．

25. $f = x^{165}y^{30} - xy, g = x^{15}y^{46} - x^{21}y^6$ とする. $Rf \cap Rg$ の**総次数逆辞書式順序**に関する左 Gröbner 基底は

$$\left\{ x^{179}y^{155} - \frac{\left(\alpha^{6734}+1\right)}{\alpha^{6320}}x^{185}y^{75} + \frac{x^{191}y^{35}}{\alpha^{6146}} - \frac{x^{15}y^{86}}{\alpha^{13940}} + \frac{\left(\alpha^{6734}+1\right)}{\alpha^{13700}}x^{21}y^{46} - \frac{x^{27}y^{6}}{\alpha^{6966}}, \right.$$
$$x^{343}y^{104} - \alpha^{348}x^{349}y^{64} - \frac{\left(\alpha^{6734}+1\right)}{\alpha^{12136}}x^{179}y^{75} + \frac{\left(\alpha^{6734}+1\right)}{\alpha^{11962}}x^{185}y^{35} + \frac{x^{15}y^{46}}{\alpha^{12782}} - \frac{x^{21}y^{6}}{\alpha^{12782}},$$
$$\left. x^{349}y^{75} - \alpha^{174}x^{355}y^{35} - \frac{x^{179}y^{86}}{\alpha^{886}} + \frac{x^{191}y^{6}}{\alpha^{646}} + \frac{x^{15}y^{57}}{\alpha^{10070}} - \frac{x^{21}y^{17}}{\alpha^{10004}} \right\}$$

である. この例での辞書式順序に関する左 Gröbner 基底は, 容量超過のため計算が完了しなかった. しかし, この例でも辞書式順序に関しては 2 元で生成されるのではないかと予想している.

26. $f = x^3y^2 + xy^5, g = x^2y + x^6y^2$ とする. $Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{ \alpha^4x^6y^9 + \frac{\left(\alpha^{14}+1\right)}{\alpha^2}x^8y^6 + x^{10}y^3 + \frac{x^2y^8}{\alpha^{24}} + \frac{\left(\alpha^{14}+1\right)}{\alpha^{18}}x^4y^5 + \frac{x^6y^2}{\alpha^4}, \frac{x^6y^{13}}{\alpha^{16}} + x^8y^{10} + \frac{x^2y^{12}}{\alpha^{60}} + \frac{x^4y^9}{\alpha^{32}} + \frac{x^6y^6}{\alpha^{24}} + \frac{x^8y^3}{\alpha^{36}} + \frac{x^2y^5}{\alpha^{40}} + \frac{x^4y^2}{\alpha^{40}} \right\}$$

である.

27. $f = x^3y^6 + xy^{10}, g = x^2y + x^{10}y^2$ とする. $Rf \cap Rg$ の辞書式順序に関する Gröbner 基底は

$$\left\{ \alpha^{22}x^{10}y^{15} + \frac{\left(\alpha^{34}+1\right)}{\alpha^2}x^{12}y^{11} + x^{14}y^7 + \frac{x^2y^{14}}{\alpha^{82}} + \frac{\left(\alpha^{34}+1\right)}{\alpha^{74}}x^4y^{10} + \frac{x^6y^6}{\alpha^{40}}, \right.$$
$$\left. \frac{x^{10}y^{28}}{\alpha^{36}} + x^{12}y^{24} + \frac{x^2y^{27}}{\alpha^{244}} + \frac{x^4y^{23}}{\alpha^{176}} + \frac{x^{10}y^{11}}{\alpha^{122}} + \frac{x^{12}y^7}{\alpha^{154}} + \frac{x^2y^{10}}{\alpha^{194}} + \frac{x^4y^6}{\alpha^{194}} \right\}$$

である.

28. $f = x^4 - y, g = x + y^3$ とする. $Rf \cap Rg$ の辞書式順序に関する左 Gröbner 基底は

$$\left\{ \alpha^8x^4y^6 + \left(\alpha^{11}+1\right)x^5y^3 - \frac{y^7}{\alpha^{16}} + x^6 - \frac{\left(\alpha^{11}+1\right)}{\alpha^{12}}xy^4 - x^2y, \frac{x^4y^{14}}{\alpha^{11}} + x^5y^{11} - \frac{y^{15}}{\alpha^{67}} - \frac{xy^{12}}{\alpha^{44}} - \frac{x^4y^3}{\alpha^{26}} - \frac{x^5}{\alpha^{37}} + \frac{y^4}{\alpha^{38}} + \frac{xy}{\alpha^{37}} \right\}$$

である.

3.2 問題と予想

まず, R の左単項生成イデアルの共通部分が単項生成になるための必要十分条件は何かという問題を提起する.

Problem 3.23 $R = k(\alpha)\langle x, y\rangle / (yx - \alpha xy), \quad f, g \in R$ とする. このとき, $Rf \cap Rg$ が単項生成になるための必要十分条件は何か？

この問題について, Proposition 3.16, Proposition 3.21 に関連して, 高橋宣能氏は次の予想を提起している.

Conjecture 3.24 (*Takahashi's Conjecture*) $f, g \in k[x, y]$ を $k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$ の元とみる. f, g が可換の意味で $\gcd(f, g) = 1$ を満たし, さらに, $Rf \cap Rg$ が単項生成で, その生成元 $h \in R$ が

$$\lim_{\alpha \to 1} h = f * g$$

を満たすとすると, $f = g = 0$ は 可換の意味で $xy = 0$ となるような解のみを持つ.

最後に R の左単項生成イデアルの共通部分は高々2元で生成されるのではないかという予想と, その2元でそれぞれ単項生成される左イデアルの共通部分は単項生成されるのではないかという予想を述べておく.

Conjecture 3.25 $R = k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$, $f, g \in R$ とする. このとき, $Rf \cap Rg$ は,(辞書式順序 $x > y$ に関して) 高々2元の左簡約 Gröbner 基底で生成される.

この予想は Example 3.22 の例に関しては成り立っている.

Conjecture 3.26 $R = k(\alpha)\langle x, y\rangle / (yx - \alpha xy)$, $Rf \cap Rg (f, g \in R)$ は辞書式順序 $x > y$ に関して左簡約 Gröbner 基底 $\{h_1, h_2\}\,(h_1, h_2 \in R)$ を持つとき, $Rh_1 \cap Rh_2$ は単項生成である.

この予想も Example 3.22 の例に関しては成り立っている.

付 録A　左除法定理プログラム

以下は, 数式処理ソフト $Mathematica$ で左除法を実行するプログラムである.

```
In[1]:=
NCPolyDiv[polynomial_, generator_, monoorder_, valueorder_] :=
   Module[{LT2, ListPoly, PolyList, Polymono2, sig, PolyDiv2, popo},
   (* 単項式順序を辞書式順序に設定する関数 *)
   If[monoorder == lex,
      LT2[f_] :=LT2[f] =
        Module[{s, lt, a},
          s = Length[f];
          lt = f[[1]];
          Do[If[DeleteCases[lt[[2]] - f[[a]][[2]], 0][[1]] < 0,
             lt = f[[a]]], {a,2,s}];
          lt]];
   (* 単項式順序を総次数辞書式順序に設定する関数 *)
   If[monoorder == grlex,
      LT2[f_] :=LT2[f] =
        Module[{s, lt, t, sum1, sum2, a},
          s = Length[f];
          lt = f[[1]];
          t = Length[lt[[2]]];
          Do[sum1 = Sum[lt[[2]][[i]], {i, t}];
            sum2 = Sum[f[[a]][[2]][[i]], {i, t}];
            If[sum1 < sum2,
              lt = f[[a]],
              If[sum1 == sum2,
                If[DeleteCases[lt[[2]] - f[[a]][[2]], 0][[1]] < 0,
                  lt = f[[a]]]]], {a, 2, s}];
          lt]];
   (* 単項式順序を総次数逆辞書式順序に設定する関数 *)
   If[monoorder == grevlex,
      LT2[f_] :=LT2[f] =
        Module[{s, lt, t, sum1, sum2, a},
          s = Length[f];
          lt = f[[1]];
          t = Length[lt[[2]]];
          Do[sum1 = Sum[lt[[2]][[i]], {i, t}];
            sum2 = Sum[f[[a]][[2]][[i]], {i, t}];
            If[sum1 < sum2,
              lt = f[[a]],
                If[sum1 == sum2,
                  If[DeleteCases[lt[[2]] - f[[a]][[2]], 0][[-1]] > 0,
                    lt = f[[a]]]]], {a, 2, s}];
          lt]];
   (* 単項式順序を行列表示で設定する関数 *)
   If[monoorder =!= lex && monoorder =!= grlex && monoorder =!= grevlex,
      LT2[f_] :=LT2[f] =
        Module[{s, lt, t, c, j},
          s = Length[f];
          lt = f[[1]];
          t = Length[monoorder];
          Do[c = False;
            j = 1;
            While[c == False,
              If[monoorder[[j]].lt[[2]] =!= monoorder[[j]].f[[i]][[2]],
                c = True;
                If[monoorder[[j]].lt[[2]] < monoorder[[j]].f[[i]][[2]],
                  lt = f[[i]]]];
                  j = j + 1], {i, 2, s}];
          lt]];
```

```
(* 入力された多項式の組をリスト表示に変換する関数 *)
PolyList[F_, val_] :=
  Module[{s, PolyListone},
    PolyListone[f_, v_] :=PolyListone[f, v] =
      Module[{getcoeff, MonomialList, aa, bb, kkk, tta, cce, ii, dc},
        getcoeff[m_, b_] := getcoeff[m, b] =
          Module[{a, c},
            If[Variables[m] =!= {},
              a = Exponent[m, b];
              c = Times @@ (b^a);
              If[c =!= 1,
                {Coefficient[m, Times @@ (b^a)], a},
                {m, a}],
              {m,Table[0, {Length[b]}]}]];
        MonomialList[aiueo_] :=
          Module[{sasisuseso, full},
            kakikukeko = Expand[aiueo] + sasisuseso;
            full = FullForm[kakikukeko];
            DeleteCases[Table[full[[1]][[iii]], {iii, 1, Length[full[[1]]]}],
              sasisuseso]];
        aa = MonomialList[f];
        bb = Length[aa];
        tta = Table[getcoeff[aa[[i]], v], {i, 1, bb}];
        cce = True;
        Do[ii = j + 1;
          cce = True;
          While[cce,
            If[tta[[j]][[2]] == tta[[ii]][[2]],
              cce = False;
              tta = ReplacePart[tta, {tta[[ii]][[1]] + tta[[j]][[1]], tta[[ii][[2]]},ii];
              tta = ReplacePart[tta, True, j]];
            If[ii == Length[tta],
              cce = False,
              ii = ii + 1]], {j, 1, Length[tta] - 1}];
        dc = DeleteCases[tta, True];
        Table[{Expand[Simplify[dc[[iii]][[1]]]], dc[[iii]][[2]]},
          {iii, 1, Length[dc]}]];
    s = Length[F];
    Table[PolyListone[F[[i]], val], {i, s}]];
(* リスト表示の多項式の組を多項式に変換する関数 *)
ListPoly[F_, val_] :=ListPoly[F, val] =
  Module[{ListPolyone, s, FF},
    ListPolyone[f_, v_] :=ListPolyone[f, v] =
      Module[{s, ss},
        s = Length[f];
        ss = Length[v];
        Sum[f[[i]][[1]]*Product[v[[j]]^(f[[i]][[2]][[j]]), {j, 1, ss}], {i, 1, s}]];
    s = Length[F];
    FF = {};
    Do[FF = Append[FF, ListPolyone[F[[i]], val]], {i, s}];
    FF];
(* リスト表示の多項式にリスト表示の項を加える関数 *)
Polymono2[f_, m_] :=Polymono2[f, m] =
  Module[{ff, fgfg, s, c, a},
    ff = f;
    s = Length[ff];
    If[s == 0,
      ff = {m},
      c = True;
      a = 1;
      While[c,
        If[DeleteCases[m[[2]] - ff[[a]][[2]], 0] == {},
          fgfg = Expand[Simplify[Together[ff[[a]][[1]] + m[[1]]]]];
          ff = ReplacePart[ff, {fgfg, m[[2]]}, a];
          If[ff[[a]][[1]] == 0,
            ff = Delete[ff, a]];
          c = False,
          a = a + 1];
        If[a == s + 1,
          ff = Append[ff, m];
          c = False]]];
```

```
    ff];
(* リスト表示の 2 つの項をかけたときの sig を計算する関数 *)
sig[le_, ri_] :=
   Module[{s},
      s = Length[le] - 1;
      α^(Sum[Sum[le[[b]], {b, a + 1, s}]*ri[[a]], {a, 1, s - 1}])];
(* リスト表示の多項式において左除法定理を計算する関数 *)
PolyDiv2[f_, g_] :=PolyDiv2[f, g] =
   Module[{s, a, r, p, i, c, h1, h2},
      s = Length[g];
      a = {};
      Do[a = Append[a, {}], {s}];
      r = {};
      p = f;
     While[p =!= {},
        i = 1;
        c = True;
        While[i <= s && c,
          h1 = LT2[p][[2]] - LT2[g[[i]]][[2]];
          If[Select[h1, #1 < 0 &] == {},
            h2 = LT2[p][[1]]/(sig[h1, LT2[g[[i]]][[2]]]*LT2[g[[i]]][[1]]);
            a = ReplacePart[a, Polymono2[a[[i]], {h2, h1}], i];
            gg = g[[i]];
            While[gg =!= {},
               p = Polymono2[p,
                 {-sig[h1, LT2[gg][[2]]]*h2*LT2[gg][[1]],h1 + LT2[gg][[2]]}];
               gg = Polymono2[gg, {-LT2[gg][[1]], LT2[gg][[2]]}]];
            c = False,
            i = i + 1]];
        If[c,
          r = Polymono2[r, LT2[p]];
          p = Polymono2[p, {-LT2[p][[1]], LT2[p][[2]]}]]];
     {a, r}];
(* 実際に計算 *)
 popo = PolyDiv2[PolyList[{polynomial}, valueorder][[1]],
   PolyList[generator, valueorder]];
 Expand[Simplify[{ListPoly[popo[[1]], valueorder],
   ListPoly[{popo[[2]]}, valueorder][[1]]}]]]
```

プログラムの説明： $f, f_1, \cdots, f_s \in R'$, $x_1 > \cdots > x_n$ を満たす単項式順序 (monomialorder) $>$ に対し,

$$\texttt{NCPolyDiv[}\ f,\ \{\ f_1, \cdots, f_s\ \},\ \texttt{monomialorder},\ \{\ x_1, \cdots, x_n, t\ \}\ \texttt{]}$$

と入力すると, 左除法定理 $f = a_1 f_1 + \cdots + a_s f_s + r$ における商多項式と剰余多項式の組

$$\{\{\ a_1, \cdots, a_{\supset s}\ \},\ r\ \}$$

を出力する. ただし monomialorder には, 単項式順序を加重行列表示したものを入力する. 単項式順序が辞書式順序, 総次数辞書式順序, 総次数逆辞書式順序の場合には, それぞれ, lex, grlex, grevlex と入力してもよい. また, 変数のリストの部分に余分な変数 t があるのは, R' に可換な変数 t を付加した環でこのプログラムを使用するために予め最後の変数は可換になるように組んだためである. よって, ここでは最後の変数 x_n が可換にならないように, ダミー変数 t を付加しておく.

付 録B　左簡約Gröbner基底プログラム

以下は, 数式処理ソフト *Mathematica* で左簡約 Gröbner 基底を計算するプログラムである. ただし, プログラム内の関数で, `NCPolyDiv` で用いたものについては省略してある.

```
In[6]:=
NCGroebner[generator_, monoorder_, valueorder_] :=
   Module[{LT2, ListPoly, PolyList, Polymono2, sig, PolyDiv2, S2, Groeb3,
   MinGroeb,RedGroeb},
  「まずここで単項式順序を指定する. プログラムについては NCPolyDiv 内の初めの
   4つの If 文を参照のこと」;
   (* 入力された多項式の組をリスト表示に変換する関数 *)
  PolyList[F_, val_] :=「省略: NCPolyDiv 内の PolyList を参照のこと」;
  (* リスト表示の多項式の組を多項式に変換する関数 *)
  ListPoly[F_, val_] :=「省略: NCPolyDiv 内の ListPoly を参照のこと」;
  (* リスト表示の多項式にリスト表示の項を加える関数 *)
  Polymono2[f_, m_] :=「省略: NCPolyDiv 内の Polymono2 を参照のこと」;
  (* 2つのリスト表示の項をかけたときの sig を計算する関数 *)
  sig[le_, ri_] :=「省略: NCPolyDiv 内の sig を参照のこと」;
  (* リスト表示の多項式において左除法定理を計算する関数 *)
  PolyDiv2[f_, g_] :=「省略: NCPolyDiv 内の PolyDiv2 を参照のこと」;
  (* リスト表示の多項式の左 S 多項式を計算する関数 *)
   S2[f_, g_] := S2[f, g] =
     Module[{mf, mg, s, c, a, b, si1, si2, sisi, z, aa, ff, gg},
       mf = LT2[f][[2]];
       mg = LT2[g][[2]];
       s = Length[mf];
       c = {};
       Do[c = Append[c, Max[{mf[[i]], mg[[i]]}]], {i, 1, s}];
       a = {1/(LT2[f][[1]]), c - mf};
       b = {1/(LT2[g][[1]]), c - mg};
       si1 = sig[a[[2]], LT2[f][[2]]];
       si2 = sig[b[[2]], LT2[g][[2]]];
       sisi = si2/si1;
       z = {};
       aa = {};
       ff = f;
       While[ff =!= z,
         aa = Polymono2[aa,
           {sisi*sig[a[[2]], LT2[ff][[2]]]*a[[1]]*LT2[ff][[1]],
           a[[2]] + LT2[ff][[2]]}];
         ff = Polymono2[ff,
           {-LT2[ff][[1]], LT2[ff][[2]]}]];
       gg = g;
       While[gg =!= z,
         aa = Polymono2[aa,
           {-sig[b[[2]], LT2[gg][[2]]]*b[[1]]*LT2[gg][[1]],
           b[[2]] + LT2[gg][[2]]}];
         gg = Polymono2[gg, {-LT2[gg][[1]], LT2[gg][[2]]}]];
       aa];
  (* リスト表示の多項式の組の左 Groebner 基底を計算する関数 *)
  Groeb3[F_] :=Groeb3[F] =
     Module[{s, B, G, t, ss, k, S},
       s = Length[F];
       B = {};
       Do[Do[B = Append[B, {i, j}], {j, i + 1, s}], {i, 1, s - 1}];
       G = F;
       t = s;
       ss = Length[F[[1]][[1]][[2]]];
       While[B =!= {},
         k = B[[1]];
```

```
      S = PolyDiv2[S2[G[[k[[1]]]], G[[k[[2]]]]], G][[2]];
      If[S =!= {},
        t = t + 1;
        G = Append[G, S];
        Do[B = Append[B, {tt, t}], {tt, 1, t - 1}]];
      B = Delete[B, 1]];
    G];
(* リスト表示の左 Groebner 基底を極小化する関数 *)
MinGroeb[F_] :=MinGroeb[F] =
  Module[{G, s, a, h, ss, t, sss, aa},
    G = Groeb3[F];
    s = Length[G];
    Do[
      Do[
        If[i =!= j && G[[j]] =!= a && G[[i]] =!= a,
          h = LT2[G[[i]]][[2]] - LT2[G[[j]]][[2]];
          If[Select[h, #1 < 0 &] == {},
            G = ReplacePart[G, a, i]]];
      j = j + 1, {j, s}];
    i = i + 1, {i, s}];
    G = DeleteCases[G, a];
    ss = Length[G];
    Do[t = LT2[G[[k]]][[1]];
      If[t =!= 1,
        sss = Length[G[[k]]];
        aa = G[[k]];
        Do[aa = ReplacePart[aa,
          {Expand[Simplify[aa[[m]][[1]]/t]], aa[[m]][[2]]}, m], {m,sss}];
        G = ReplacePart[G, aa, k]], {k, ss}];
    G];
(* リスト表示の左極小 Groebner 基底を簡約化する関数 *)
RedGroeb[F_] :=RedGroeb[F] =
  Module[{G, s, k},
    G = MinGroeb[F];
    s = Length[G];
    Do[k = PolyDiv2[G[[j]], Delete[G, j]][[2]];
      G = ReplacePart[G, k, j], {j, s}];
    G];
(* 実際に計算 *)
Expand[Simplify[ListPoly[RedGroeb[PolyList[generator,valueorder]],
  valueorder]]]]
```

プログラムの説明： $f_1, \cdots, f_s \in R'$, $x_1 > \cdots > x_n$ を満たす単項式順序 (`monomialorder`) $>$ に対し,

$$\texttt{NCGroebner[\{ } f_1, \cdots, f_s \texttt{ \}, monomialorder, \{ } x_1, \cdots, x_n, t \texttt{ \}]}$$

と入力すると, 左イデアル $I_L(f_1, \cdots, f_s)$ の左 (簡約)Gröbner 基底

$$\{ g_1, \cdots, g_t \}$$

を出力する. ただし `monomialorder` とダミー変数 t については, `NCPolyDiv` と同様である.

付 録C　左イデアル所属判定プログラム

以下は, 数式処理ソフト *Mathematica* で多項式が, 与えられた左イデアルに属するかどうかを判定し, 属する場合については具体的表現を計算するプログラムである. ただし, プログラム内の関数で, NCPolyDiv 及び NCGroebner で用いたものについては省略してある.

```
In[17]:=
NCIdealRepr[polynomial_, generator_, valueorder_] :=
   Module[{monoorder, LT2, ListPoly, PolyList, Polymono2, sig, PolyPlus,
   PolyTimes, PolyDiv2, S2, Groeb3, fmc, gmc, lenlen, datedate, ans, qp,
   kake, tashi, kotae},
  (* 単項式順序を総次数逆辞書式に設定 *)
  monoorder = grevlex;
   「まずここで単項式順序を総次数逆辞書式に設定する. プログラムについては
   NCPolyDiv 内の初めの４つの If 文の３つ目を参照のこと」;
  (* 入力された多項式の組をリスト表示に変換する関数 *)
  PolyList[F_, val_] :=「省略: NCPolyDiv 内の PolyList を参照のこと」;
  (* リスト表示の多項式の組を多項式に変換する関数 *)
  ListPoly[F_, val_] :=「省略: NCPolyDiv 内の ListPoly を参照のこと」;
  (* リスト表示の多項式にリスト表示の項を加える関数 *)
  Polymono2[f_, m_] :=「省略: NCPolyDiv 内の Polymono2 を参照のこと」;
  (* ２つのリスト表示の項をかけたときの sig を計算する関数 *)
  sig[le_, ri_] :=「省略: NCPolyDiv 内の sig を参照のこと」;
  (* リスト表示の多項式において左除法定理を計算する関数 *)
   (* リスト表示の多項式の加法を計算する関数 *)
   PolyPlus[f_, g_] :=
    Module[{k, ff},
       k = Length[g];
       ff = f;
       Do[ff = Polymono2[ff, g[[i]]], {i, 1, k}];
       ff];
   (* リスト表示の多項式の乗法を計算する関数 *)
  PolyTimes[f_, g_] :=
     Module[{k, ff, q},
       If[f == {} || g == {},
         {},
         m = Length[f];
         k = Length[g];
         ff[i_] := Table[
           {sig[f[[i]][[2]], g[[kk]][[2]]]*f[[i]][[1]]*g[[kk]][[1]],
           f[[i]][[2]] + g[[kk]][[2]]}, {kk, 1, k}];
         q = {};
         Do[q = PolyPlus[q, ff[ii]], {ii, 1, m}];
         q]];
  (* リスト表示の多項式において左除法定理を計算する関数 *)
  PolyDiv2[f_, g_] :=「省略: NCPolyDiv 内の PolyDiv2 を参照のこと」;
  (* リスト表示の多項式の左 S 多項式を計算する関数 *)
  S2[f_, g_] := 「省略: NCGroebner 内の S2 を参照のこと」;
  (* リスト表示の多項式の組の左 Groebner 基底を計算する関数
     (注: NCGroebner 内のものとは違う) *)
  Groeb3[F_] :=Groeb3[F] =
     Module[{s, B, G, t, ss, k, S4, S, S3},
        s = Length[F];
        B = {};
        Do[Do[B = Append[B, {i, j}], {j, i + 1, s}], {i, 1, s - 1}];
        G = F;
        t = s;
        ss = Length[F[[1]][[1]][[2]]];
        While[B =!= {},
          k = B[[1]];
          S4 = PolyDiv2[S2[G[[k[[1]]]], G[[k[[2]]]]], G];
```

```
        S = S4[[2]];
        S3 = S4[[1]];
        Do[
          If[S3[[i]] =!= {},
            S3 = ReplacePart[S3,
              Table[{-S3[[i]][[j]][[1]], S3[[i]][[j]][[2]]},
                {j, 1, Length[S3[[i]]]}], i]], {i, 1, Length[S4[[1]]]}];
        S3 = ReplacePart[S3, Polymono2[S3[[B[[1]][[1]]]], fmc], B[[1]][[1]]];
        S3 = ReplacePart[S3, Polymono2[S3[[B[[1]][[2]]]], gmc], B[[1]][[2]]];
        If[S =!= {},
          t = t + 1;
          G = Append[G, S];
          datedate = Append[datedate, S3];
          Do[B = Append[B, {tt, t}], {tt, 1, t - 1}]];
        B = Delete[B, 1]];
      G];
 (* 実際に計算 *)
 lenlen = Length[generator];
 datedate = Table[{}, {lenlen}];
 datedate = Table[datedate, {lenlen}];
 Do[datedate = ReplacePart[datedate,
   ReplacePart[Table[{}, {lenlen}], {{1, Table[0, {Length[valueorder]}]}}, i],      i], {i, 1, lenlen}];
 ans = Expand[Simplify[ListPoly[Groeb3[PolyList[generator,
   valueorder]], valueorder]]];
 Do[
   Do[datedate = ReplacePart[datedate,
     Join[Table[PolyPlus[PolyTimes[datedate[[i]][[k]], datedate[[j]][[i]]],
       datedate[[j]][[k]]], {k, 1, lenlen}],
       Table[datedate[[j]][[p]], {p, lenlen + 1, j - 1}]], j],
     {j, i + 1, Length[ans]}], {i, lenlen + 1, Length[ans] - 1}];
 Do[datedate = ReplacePart[datedate,
   Delete[datedate[[i]], Table[{j}, {j, lenlen + 1, i - 1}]], i],
   {i, lenlen + 2, Length[ans]}];
 qp = PolyDiv2[PolyList[{polynomial}, valueorder][[1]],
   PolyList[ans, valueorder]];
 If[qp[[2]] =!= {},
   False,
   kotae = Table[kake = Table[PolyTimes[qp[[1]][[j]], datedate[[j]][[i]]],
     {j, 1, Length[ans]}];
     tashi = {};
     Do[tashi = PolyPlus[tashi, kake[[j]]], {j, 1, Length[ans]}];
     tashi, {i, 1, lenlen}];
   Expand[Simplify[ListPoly[kotae, valueorder]]]]]
```

プログラムの説明： $f, f_1, \cdots, f_s \in R'[t]$ に対し,

$$\texttt{NCIdealRepr[}\ f, \texttt{\{}\ f_1, \cdots, f_s\ \texttt{\}}, \texttt{\{}\ x_1, \cdots, x_n, t\ \texttt{\}}\ \texttt{]}$$

と入力すると, $f \in I_L(f_1, \cdots, f_s)$ のときは, $f = a_1 f_1 + \cdots + a_s f_s \quad (a_i \in R'[t])$ を満たすような

$$\texttt{\{}\ a_1, \cdots, a_s\ \texttt{\}}$$

を出力する. また, $f \notin I_L(f_1, \cdots, f_s)$ のときは

False

を出力する.

関連図書

[1] D. Cox, J. Little, D. O'Shea: *Ideals, Varieties, and Algorithm*, Springer, 1996.

[2] T. Becker, V. Weispfenning: *Gröbner Bases*, Springer, 1993.

[3] D. Bayer, M. Stillman: *A theorem on refining division orders by the reverse lexicographic order*, Duke J. Math. 55, pp. 321–328, 1987.

[4] L. Robbiano: *On the theory of graded structures*, J. Symbolic Comput. 2, pp. 139–170, 1986.

[5] A. Kandri-Roby, V. Weispfenning: *Non-commutative Gröbner bases in algebras of solvable type*, J. Symbolic Comput. 9, no. 1, pp. 1–26, 1990.

[6] 上野健爾, 志賀浩二, 砂田利一 編集: 数学のたのしみ, No. 11 「多項式環の視点: グレブナー基底」, 日本評論社, 1999.