交换环2

2024 年 6 月 3 日

目录

1 广义除法

给定两个多项式$f(x), g(x) \in k[x]$，其中$g(x) \neq 0$，k是域，什么时候有$g(x)$是$f(X)$的因子呢？除法算式给出了唯一的多项式$q(x), r(x) \in k[x]$使得

$$f(x) = q(x)g(x) + r(x)$$

其中$r = 0$或者$\deg(r) < \deg(g)$，而$g \mid f$当且仅当$r = 0$。让我们从其他角度看这个公式，说$g \mid f$的意思是说$f \in (g)$，其中(g)是g生成的主理想。所以r在里面就是一个障碍，因此$f \in (g)$当且仅当$r = 0$

考虑一个更一般的情况，给定多项式

$$f(x), g_1(x), \cdots, g_m(x) \in k[x]$$

其中k是域，什么时候$d(x) = \gcd\{g_1(x), \cdots, g_m(x)\}$是$f$的因子？当然，我们可以用欧拉算法得到这个$d$，再由除法算式得到$d \mid f$。那么我们将这两种算法并起来，那么可以确定$f \in (g_1, \cdots, g_m) = (d)$

给定$f(X), g_1(X), \cdots, g_m(X) \in k[X]$，我们现在的问题是，是否存在一个能判断$f \in (g_1, \cdots, g_m)$的算法，$k[X]$中的除法算式将得到

$$r(X), a_1(X), \cdots, a_m(X) \in k[X]$$

其中$r(X)$是唯一的使得

$$f = a_1 g_1 + \cdots + a_m g_m + r$$

由于$(g_1, \cdots, g_m)$是一些g_i的线性组合生成的，除法算式再次说明了r是一个障碍。因此$f \in (g_1, \cdots, g_m)$当且仅当$r = 0$。我们本章的工作基本就是展示除法和欧几里得算法可以拓展到多变量的情况。

2 单项式序

$k[x]$中的除法独特的地方在于$r(x)$总是为较小的次数。否则该结论是无意义的。因为给定一个$Q[x] \in k[x]$，总有

$$f(x) = Q(x)g(x) + [f(x) - Q(x)g(x)]$$

我们来研究多个变量的情况，多个变量的多项式是形如$cx_1^{a_1} \cdots x_n^{a_n}$的单项式之和。那么我们可以给他们分配一些重数。

2.1 定义：重数

单项式$cx_1^{a_1}\cdots x_n^{a_n}\in k[x_1,\cdots,x_n]$的重数是$n$元组$a=(a_1,\cdots,a_n)$。其中$c\in k$非零。它们的总次数记为$|\ a\ |=a_1+\cdots+a_n$

当我们使用$g(x)$去除$f(x)$的时候，我们一般根据次数将$f(x)$的单项按照下降的顺序来排列

$$f(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0$$

考虑多变量的多项式$f(X)=f(x_1,\cdots,x_n)$。我们把$x_1,\cdots,x_n$简单用X去记。并将指数$a_1,\cdots,a_n$记为a，则多项式$f(X)$可以写为

$$f(x_1,\cdots,x_n)=\sum c_{a_1,\cdots,a_n}x_1^{a_1}\cdots x_n^{a_n}=f(X^a)=\sum_a c_aX^a$$

我们的目的就是将$f(X)$的单项以一种合理的方法去排列。我们可以通过对它们的多重次数排序来完成这些工作。

由自然数的所有有序n元数组构成的集合N^n关于下列的加法是幺半群[1]

$$(a_1,\cdots,a_n)+(b_1,\cdots,b_n)=(a_1+b_1,\cdots,a_n+b_n)$$

那么我们可以重新记单项为

$$X^aX^b=X^{a+b}$$

2.2 定义：良序

一个偏序集X称为是良序的，若每个非空集$S\subseteq X$都包含一个最小元，即存在一个$s_0\in S$使得对所有$s\in S$有$s_0\preceq s$

2.3 命题

设X是良序集

1. 若$x,y\in X$，则$x\preceq y$或者$y\preceq x$
2. 每个严格递减的的序列是有限的

证明： 比较简单，省略。

良序集的性质将会用来证明算法最终都是会停止的。

[1]即满足结合运算和存在元素1的集合。

2.4 定义：单项式序

单项式是N^n的一个良序，且满足

$$a \preceq b \Rightarrow a + r \preceq b + r$$

其中$a, b, r \in N^n$

那么我们可以用偏序来定义排序的问题，若$a \preceq b$，则定义$X^a \preceq X^b$。

2.5 定义：字典排序

若N^n带有一个单项式序，则每个$f(X) \in k[X]$按项的次数下降的方式可以写为：首先是最高次项，接着是它的次数更低的项：

$$f(X) = c_a X^a + \text{更低次的项}$$

定义其首项为$\mathrm{LT}(f) = c_a X^a$和它的次数为$\mathrm{DEG}(f) = a$，我们说其是首一的，这意味着$\mathrm{LT}(f) = X^a$，其中$c_a = 1$

我们给出一些排序的例子：

2.6 定义：字典顺序

N^n上的字典顺序定义为$a \preceq_{lex} b$，其中$a = b$或$b - a$的第一个坐标是非零且为正的。

我们来看看怎么排序的，若$a \prec_{lex} b$，这意味着从1开始，到某个$i - 1$，此时在$i - 1$前的项都是相同的。并可知在i后有严格的不等式$a_i < b_i$。我们用下列几个单词做说明，它的排序为$a < b < c \cdots z$

ausgehen
ausladen
auslagen

就是前三个元是相同的。

2.7 命题

N^n字典序是一种单项序

证明： 偏序的证明比较简单，我们直接证明良序，设S是N^n的一个子集，定义

$$C_1 = \{S\text{中所有有序n元组的第一个坐标}\}$$

其中δ_1是C_1中最小的数，然后定义

$$C_2 = \{\text{所有有序n元组}(\delta_1, a_2, \cdots, a_n \in S\text{的第二个坐标})\}$$

由于$C_2 \neq \emptyset$，故存在一个最小数δ_2，以此类推我们归纳的可以得到有序n元组的第$i+1$个坐标构成的集合，定义δ_{i+1}是C_{i+1}中的最小数。我们就得到一个最小n元组$\delta = (\delta_1, \cdots, \delta_n)$在$S$中。取$a = (a_1, \cdots, a_n) \in S$。则对于每个$a - \delta$，第一个坐标都是非负的。那么就有$\delta \preceq_{lex} a$。所以字典序是一个良序。

其次，若$a \preceq_{lex} b$，则对所有的$r \in N$

$$a + r \preceq_{lex} b + r$$

若$a = b$，则$a + r = b + r$。若$a \prec_{lex}$，则$b - a$的第一个非零坐标是正的，但

$$(b + r) - (a + r) = b - a$$

故$a + r \prec_{lex} b + r$。因此它是单项式序。

2.8 定义：正字

若X是集合且$n \geq 1$，我们定义X上长度为n的正字w是函数$w : \{1, 2, \cdots, n\} \to X$记为

$$w = x_1 x_2 \cdots x_n$$

其中$x_i = w(i)$。我们不需要保证单射，即可能存在重复的x。两个正字是可以相乘的，若$w' = x'_1 \cdots x'_m$，则

$$ww' = x_1 x_2 \cdots x_n x'_1 \cdots x'_m$$

然后我们引入空子，它是长度为0的字，记为1，对所有的正字，$1w = w1 = w$，在这些定义下，所有空字和集合X上所有正字构成的集合$W(X)$是一个幺半群。

2.9 推论

设X是良序集，则按照字典序，$W(X)$是良序的。

证明： 我们证明其是字典序，对所有的$w \in W(X)$，定义$1 \prec_{lex} w$。其次，对给定的字u, v，我们在短的字末尾添加1来使得他们的长度相等。我们重新记为u', v'。若$m \geq \max\{p, q\}$，则我们可以认为$u', v' \in X^m$。我们定义$u \prec_{lex} v$若在X^m中$u' \prec_{lex} v'$。

2.10 定义：次数-字典序

我们把N^n上的次数-字典序定义为$a \prec_{dlex} b$若$a = b$或者

$$\mid a \mid = \sum_{i=1}^{n} a_i < \sum^{n} i = 1 b_i = \mid b \mid$$

或，若$\mid a \mid = \mid b \mid$，则$b - a$的第一个非零坐标是正的。

这个定义的操作是，先检查重数的总次数，一般来说，若$\mid a \mid < \mid b \mid$，则$a \prec_{dlex} b$，例如有两个4元组$(1, 2, 3, 0)$和$(0, 2, 5, 0)$。其次，若总次数相同，我们利用字典排序法排序，例如$(1, 2, 3, 4) \prec_{dlex} (1, 2, 5, 2)$

2.11 命题：

次数-字典序$\preceq_{dlex}$是N^n上的单项式序。

2.12 命题

设$\preceq$是一个N^n上的单项式序，$f(X), g(X), h(X) \in k[X] = k[x_1, \cdots, x_n]$

1. 若$\mathrm{DEG}(f) = \mathrm{DEG}(g)$，则$\mathrm{LT}(g) \mid \mathrm{LT}(f)$
2. $\mathrm{LT}(hg) = \mathrm{LT}(h)\mathrm{LT}(g)$
3. 若$\mathrm{DEG}(f) = \mathrm{DEG}(hg)$，则$\mathrm{LT}(g) \mid \mathrm{LT}(f)$

证明： 若$\mathrm{DEG}(f) = a = \mathrm{DEG}(g)$，则$\mathrm{LT}(g) = dX^n$，而$\mathrm{LT}(f) = cX^n$，因此$\mathrm{LT}(g) \mid \mathrm{LT}(f)$

证明2： 令$\mathrm{LT}(h) = cX^r$和$\mathrm{LT}(g) = bX^b$，那么cbX^{r+b}是一个$h(X)g(X)$的项。设$c_u X^u$是$h(X)$中满足$u < r$的任意一项，$b_v X^v$是满足$v < b$的一项，那么$\mathrm{DEG}(c_u X^u b_v X^v) = u + v$。由于单项式序是偏序集，那么$u + v \prec r + v \prec r + b$。所以$cbX^{r+b}$是多项式中次数最大的。

证明3： 由于$\mathrm{DEG}(f)=\mathrm{DEG}(hg)$，则由1有$\mathrm{LT}(hg)\mid\mathrm{LT}(f)$。利用2有$\mathrm{LT}(h)\mathrm{LT}(g)=\mathrm{LT}(hg)$。就有$\mathrm{LT}(g)\mid\mathrm{LT}(f)$

3 广义除法算式

我们现在用单项式序来给出多远多项式的除法算法。

3.1 定义：简化

令$\preceq$是在N^n上的单项式序，再令$f(X).g(X)\in k[X]=k[x_1,\cdots,x_n]$，若这里存在非零项$c_bX^b\in f(X)$使得$\mathrm{LT}(g)\mid c_bX^b$且

$$h(X)=f(X)-\frac{c_bX^b}{\mathrm{LT}(g)}$$

则简化$f\xrightarrow{g}h$表示用h替换f

简化是单项式多变量的长除法中的通常步骤，若$f\xrightarrow{g}h$，我们用g消去f的一项就得到了h。

3.2 命题

设$\preceq$是N^n上的一个多项式序。设$f\xrightarrow{g}h$，即存在$f(X)$的一个非零项c_bX^b使得$\mathrm{LT}(g)\mid c_bX^b$，且$h(X)=f(X)-\frac{c_bX^b}{\mathrm{LT}(g)}g(x)$

若$b=\mathrm{DEG}(f)$，则

$$h(X)=0\text{或者}\mathrm{DEG}(h)\prec\mathrm{DEG}(f)$$

其次，若$b\prec\mathrm{DEG}(f)$，则$\mathrm{DEG}(h)=\mathrm{DEG}(f)$，在任意一种情形下，均有

$$\mathrm{DEG}\left(\frac{c_bX^b}{\mathrm{LT}(g)}g(X)\right)\prec\mathrm{DEG}(f)$$

证明： 记

$$f(X)=\mathrm{LT}(f)+c_kX^k+\text{低次项}$$

由于c_bX^b是$f(X)$的项，我们有$b\preceq\mathrm{DEG}(f)$。若$\mathrm{LT}(g)=a_rX^r$，那么$\mathrm{DEG}(g)=r$。我们令

$$g(X)=a_rX^r+a_yX^y+\text{低次项}$$

因此

$$\begin{aligned} h(X) =& f(X) - \frac{c_b X^b}{\mathrm{LT}(g)} g(X) \\ =& f(X) - \frac{c_b X^b}{\mathrm{LT}(g)} [\mathrm{LT}(g) + a_y X^y + \cdots] \\ =& [f(X) - c_b X^b] - \frac{c_b X^b}{\mathrm{LT}(g)} [a_y X^y + \cdots] \end{aligned}$$

由于$\mathrm{LT}(g) \mid c_b X^b$，则$b - r \in N^n$。我们说

$$\mathrm{DEG}\left(-\frac{c_b X^b}{\mathrm{LT}(g)} [a_y X^y + \cdots] \right) = y + b - r \prec b$$

这个不等式成立，因而$\mathrm{DEG}(h) \prec \mathrm{DEG}(f)$。我们证明其他情况

若$h(X) \neq 0$，那么

$$\mathrm{DEG}(h) \preceq \max \left\{ \mathrm{DEG}(f(x) - c_b X^b), \mathrm{DEG}\left(-\frac{c_b X^b}{\mathrm{LT}(g)} [a_y X^y + \cdots] \right) \right\}$$

若$b = \mathrm{DEG}(f)$，则$c_b X^b = \mathrm{LT}(f)$，那么

$$f(X) - c_b X^b = f(X) - \mathrm{LT}(f) = c_k X^k + \text{低次项}$$

因此$\mathrm{DEG}(f(X) - \mathrm{LT}(f)) = k \prec \mathrm{DEG}(f)$。因此$\mathrm{DEG}(h) \prec \mathrm{DEG}(f)$。

那么，$\mathrm{DEG}\left(-\frac{c_b X^b}{\mathrm{LT}(g)} [a_y X^y + \cdots] \right) \prec b \prec \mathrm{DEG}(f)$，那么有$\mathrm{DEG}(h) = \mathrm{DEG}(f)$

3.3 定义：既约

设$\{g_1, \cdots, g_m\}$，其中$g_i = g_i(X) \in k[X]$，多项式$r(X)$称为 $\mod \{g_1, \cdots, g_m\}$既约的，若$r(X) = 0$或没有$\mathrm{LT}(g_i)$能整除$r(X)$的任意非零项。

3.4 定理：广义除法算式

设$\prec$是N^n上的单项式序，$k[X] = k[x_1, \cdots, x_n]$。若$f(X) \in k[X]$且$G = [g_1(X), \cdots, g_m(X)]$是$k[X]$上的多项式$m$元有序组，则存在一个算律，他能给出多项式$r(X), a_1(X), \cdots, a_m(X) \in k[X]$使得

$$f = a_1 g_1 + \cdots + a_m g_m + r$$

其中r是 $\mod \{g_1, \cdots, g_m\}$既约的，且对所有$i$有$\mathrm{DEG}(a_i g_i) \preceq \mathrm{DEG}(f)$

3.5 定义：余式

给定N^n的一个单项式序，一个多项式$f(X) \in k[X]$，以及一个m元有序组$G = [g_1, \cdots, g_m]$，我们称除法算式的输出项$r(X)$为$f \mod G$的余式。

3.6 例子

设$f(x, y, z) = x^2y^2 + xy$，再令$G = [g_1, g_2, g_3]$，其中

$$\begin{aligned} g_1 =& y^2 + z^2 \\ g_2 =& x^2y + yz \\ g_3 =& z^3 + xy \end{aligned}$$

我们使用N^3上的次数-字典序，由于$y^2 = \mathrm{LT}(g_1) \mid \mathrm{LT}(f) = x^2y^2$，做$f \xrightarrow{g_1} h$，其中$h = f - \frac{x^2y^2}{y^2}(y^2 + z^2) = -x^2z^2 + xy$，因为$h$是 $\mod G$既约的，因为h不被$\mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3)$的首项整除。我们对其他的应用算法看看。

我们对g_2做$f \xrightarrow{g_2} h'$有

$$h' = f - \frac{x^2y^2}{x^2y}(x^2y + yz) = -y^2z + xy$$

我们可以发现，h'不是既约的，为此我们做 $\mod g_1$约分，得到

$$h'' = h' - \frac{-y^2z}{y^2}(y^2 + z^2) = z^3 + xy$$

但这 $\mod g_3$非既约的，我们做$h'' \xrightarrow{g_3} h^{(3)}$就有$h^{(3)} = 0$了

3.7 格罗布纳基

我们看到，由除法算式而得的$f \mod [g_1, \cdots, g_m]$的余式依赖于$g_i$的排列。理想$I = (g_1, \cdots, g_m)$的格罗布纳基是一组满足下列性质的基：对任意一个由$g_i$组成的$m$元有序组$G$，$f \mod G$的余式确定了$f$是否在$I$中。这是一个关于定义的推论。

3.8 定义：格罗布纳基

我们说多项式集$\{g_1, \cdots, g_m\}$是理想$I = (g_1, \cdots, g_m)$的一个格罗布纳基，若对每个非零$f \in I$，存在某个g_i使得$\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$

对上述例子3.6，我们知道f就不是一个格罗布纳基，因为对理想I，x^2y^2，化简后得到$-x^2z^2 \in I$，但不被G整除。

3.9 命题

多项式集$\{g_1, \cdots, g_m\}$是理想$I = (g_1, \cdots, g_m)$的一个格罗布纳基当且仅当对每个m元有序组$G_\sigma = \{g_{\sigma(1)}, \cdots, g_{\sigma(m)}\}$，其中$\sigma \in S_m$，每个$f \in I$的余式是$0 \mod G_\sigma$

证明： 设存在置换$\sigma \in S_m$和某个$f \in I$使得$f \mod G_\sigma$的余式不为0，并选择所有这样的多项式找那个次数最小的一个。由于$\{g_1, \cdots, g_m\}$是格罗布纳基，故对某个i存在$\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$，也存在简化$f \xrightarrow{g_{\sigma(i)}} h$的$\sigma(i)$,我们选择其中最小的$\sigma(i)$，并记为$h$。由命题3.2除法算式给出一系列的简化，$h = h_0 \to h_1 \to \cdots \to h_p = 0$，我们就得到了$f \mod G_\sigma$的余式是0，矛盾。

反之，我们设$\{g_1, \cdots, g_m\}$是$I = (g_1, \cdots, g_m)$的一个格罗布纳基。若对每个i存在一个非零$f \in I$使得$\mathrm{LT}(g_i) \nmid \mathrm{LT}(f)$，则存在任意一个简化$f \xrightarrow{g_i} h$中，我们有$\mathrm{LT}(h) = \mathrm{LT}(f)$。若$G = [g_1, \cdots, g_m]$，则在 $\mod G$下应用除法算式就得到简化$f \to h_1 \to h_2 \to \cdots \to h_p = r$，其中$\mathrm{LT}(r) = \mathrm{LT}(f)$。因此$r \neq 0$与我们的假设矛盾。也就是说$f \mod G$的余式不是0

3.10 推论

设$I = (g_1, \cdots, g_m)$是理想，并设$\{g_1, \cdots, g_m\}$是格罗布纳基，令$G = [g_1, \cdots, g_m]$是g_i构成的m元有序组，若$f(X) \in k[X]$，则存在唯一的$r(X) \in k[X]$使得$f - r \in I$，其中$r(X)$是 $\mod \{g_1, \cdots, g_m\}$既约的。即$r(X)$是$f \mod G$的余式。

证明： 除法算式给出了一个 $\mod \{g_1, \cdots, g_m\}$的余式$r$以及满足$f = a_1 g_1 + \cdots + a_m g_m$的多项式$a_1, \cdots a_m$，则$f - r = a_1 g_1 + \cdots + a_m g_m \in I$。

然后我们证明唯一性，我们设存在两个既约余项r, r'，那么$f - r$和$f - r'$依然在I中，故$(f-r)-(f-r') = r-r' \in I$。由于$r, r'$是既约的，则$r-r'$是不被任何一个$g_i$整除的。若$r - r' \neq 0$，则不存在能被任何$\mathrm{LT}(g_i)$整除的项，矛盾。因此$r - r' = 0$

3.11 推论

设$I = (g_1, \cdots, g_m)$是一个理想，$\{g_1, \cdots, g_m\}$是一个I的格罗布纳基，

$G=[g_1,\cdots,g_m]$为m元有序组

1. 若$f(X)\in k[X]$,$G_\sigma=[g_{\sigma(1)},\cdots,g_{\sigma(m)}]$，其中$\sigma\in S_m$是一个置换，则$f \mod G$的余式等于$f \mod G_\sigma$的余式。

2. 多项式$f\in I$当且仅当$f \mod G$的余式是0

证明： 若r是$f \mod G$的余式，那么r是满足$f-r\in I$和 $\mod\{g_1,\cdots,g_m\}$的既约唯一多项式。同样，r_σ是$f \mod G_\sigma$且满足上述的既约唯一多项式。利用推论3.10这样的$f-r\in I$的多项式只有一个，因此$r=r_\sigma$

证明2： 命题3.9有若$f\in I$，则$r=0$，反之，若r是$f \mod G$的余式，则$f=q+r$，其中$q\in I$，若$r=0$则$f\in I$

有一些算式比较麻烦，我们来一些认识一些记号。

3.12 定义：$\vee$

设$\alpha=(\alpha_1,\cdots,\alpha_n)$和$\beta=(\beta_1,\cdots,\beta_n)$都在$N^n$中。定义

$$\alpha\vee\beta=\mu$$

其中$\mu=(\mu_1,\cdots,\mu_n)$由$\mu_i=\max\{\alpha_i,\beta_i\}$给出。

不难发现，$X^{\alpha\vee\beta}$就是X^α和X^β最小公倍数。

3.13 定义：S-多项式

设$f(X),g(X)\in k[X]$，其中$\mathrm{LT}(f)=a_\alpha X^\alpha$，$\mathrm{LT}(g)=b_\beta X^\beta$，定义

$$L(f,g)=X^{\alpha\vee\beta}$$

那么$S-$多项式$S(f,g)$定义如下：

$$\begin{aligned}S(f,g)=&\frac{L(f,g)}{\mathrm{LT}(f)}f-\frac{L(f,g)}{\mathrm{LT}(g)}g\\=&a_\alpha^{-1}X^{(\alpha\vee\beta)-\alpha}f(X)-b_\beta^{-1}X^{(\alpha\vee\beta)-\beta}g(X)\end{aligned}$$

对于下面的引理，我们使用$\alpha(j)$来表示g_i中第j个函数g_j的幂次。

3.14 引理

给定$g_1(X),\cdots,g_t(X)\in k[X]$和单项式$c_jX^{\alpha(j)}$，设$h(X)=\sum_{j=1}^{\ell}c_jX^{\alpha(j)}g_j(X)$

设δ是一个多重次数，若$\mathrm{DEG}(h)\prec\delta$且对所有的$j<\ell$有$\mathrm{DEG}(c_jX^{\alpha(j)}g_j(X))=\delta$，则存在$d_j\in k$使得

$$h(X)=\sum_j d_jX^{\delta-\mu(j)}S(g_j,g_{j+1})$$

其中$\mu(j)=\mathrm{DEG}(g_i)\vee\mathrm{DEG}(g_{j+1})$。且对所有$j<\ell$有

$$\mathrm{DEG}\big(X^{\delta-\mu(j)}S(g_j,g_{j+1})\big)\prec\delta.$$

注记： 该定理的意思是，若$\mathrm{DEG}(\sum_j a_jg_j)$，其中$a_j$是多项式，而对所有$j$，$\mathrm{DEG}(a_jg_j)=\delta$，则$h$可以被重写为一些$S$多项式的线性组合，这些线性组合以单项式作为系数且次数严格小于δ

证明： 令$\mathrm{LT}(g_j)=b_jX^{\beta(j)}$，那么$\mathrm{LT}(c_jX^{\alpha(j)}g_j(X))=c_jb_jX^{\delta}$。$X^{\delta}$的系数在$h(X)$中是$\sum_j c_jb_j$。由于$\mathrm{DEG}(h)\prec\delta$，那么$\sum_j c_jb_j=0$。定义首一多项式

$$u_j(X)=b_j^{-1}X^{\alpha(j)}g_j(X)$$

那么

$$\begin{aligned}h(X)=&\sum_{j=1}^{\ell}c_jX^{\alpha(j)}g_j(X)\\=&\sum_{j=1}^{l}c_jb_ju_j.\\=&c_1b_1(u_1-u_2)+(c_1b_1+c_2b_2)(u_2-u_3)\\&+\cdots+(c_1b_1+\cdots+c_\ell b_{\ell-1})(u_{\ell-1}-u_\ell)\\&+(c_1b_1+\cdots+c_\ell b_\ell)u_\ell\end{aligned}$$

由于$\sum_j c_jb_j=0$，所以最后一项为0。而由于对于$j<\ell$的项的次数为δ，则有$\alpha(j)+\beta(j)=\delta$。则对所有的$j$都有$X^{\beta(j)}\mid X^{\delta}$。若我们记$\mu(j)=\beta(j)\vee$

$\beta(j+1)$，则$\delta-\mu(j)\in N^n$，但是

$$\begin{aligned}X^{\delta-\mu(j)}S(g_j,g_{j+1}) &= X^{\delta-\mu(j)}\left(\frac{X^{\mu(j)}}{\mathrm{LT}(g_j)}g_j(X)-\frac{X^{\mu(j)}}{\mathrm{LT}(g_{j+1})}g_{j+1}(X)\right)\\ &= \frac{X^{\delta}}{\mathrm{LT}(g_j)}g_j(X)-\frac{X^{\delta}}{\mathrm{LT}(g_{j+1})}g_{j+1}(X)\\ &= b_j^{-1}X^{a(j)}g_i-b_{j+1}^{-1}X^{a(j+1)}g_{j+1}\\ &= u_j-u_{j+1}.\end{aligned}$$

带入就有

$$h(x)=c_1b_1X^{\delta-\mu(1)}S(g_1,g_2)+(c_1b_1+c_2b_2)X^{\delta-\mu(2)}S(g_2,g_3)+\cdots$$

定义$d_j=c_1b_1+\cdots+c_jb_j$即得到我们要的等式。

其次，由于u_j,u_{j+1}均是次数为δ的多项式，相对应的就有$\mathrm{DEG}(u_j-u_{j+1})\prec\delta$

3.15 定理：布切贝哥

集合$\{g_1,\cdots,g_m\}$是理想$I=(g_1,\cdots,g_m)$的一个格罗布纳基当且仅当对所有的p,q，$S(g_p,g_q)\mod G$的余式为0，其中$G=[g_1,\cdots,g_m]$

证明： 作为g_q,g_p的一个线性组合，$S(g_p,g_q)$显然在I中。若$G=\{g_1,\cdots,g_m\}$是格罗布纳基，那么由命题3.9可知$S(g_p,g_q)\mod G$的余式就是0。

反之，设全部$p,q,S(g_q,g_p)\mod G$的余式是0，我们证明对每个$f\in I$ $\mod G$的余式是0.由于$f\in I=(g_1,\cdots,g_m)$，我们记$\sum_i h_ig_i$，那么

$$\mathrm{DEG}(f)\preceq\max\{\mathrm{DEG}(h_ig_i)\}$$

若对某个i存在$\mathrm{DEG}(f)=\mathrm{DEG}(h_ig_i)$，则$\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$正是我们要的。那么我们当然可以设有严格不等式$\mathrm{DEG}(f)\prec\max_i\{\mathrm{DEG}(h_ig_i)\}$

多项式f可以用一些方法写成g_i的线性组合。在所有形如$f=\sum_i h_ig_i$的表示中，选择一个使得$\delta=\max_i\{\mathrm{DEG}(h_ig_i)\}$是最小的。若$\mathrm{DEG}(f)=\delta$，就和上面一样直接证明完毕。因此我们继续设有其他的严格不等式$\mathrm{DEG}(f)\prec\delta$，记

$$f=\sum_{\substack{\mathrm{j}\\ \mathrm{DEG}(h_jg_j)=\delta}}h_jg_j+\sum_{\substack{\mathrm{j}\\ \mathrm{DEG}(h_\ell g_\ell)<\delta}}h_\ell g_\ell.$$

若$\mathrm{DEG}(\sum_j h_i g_i) = \delta$，则$\mathrm{DEG}(f) = \delta$矛盾，为此$\mathrm{DEG}(\sum_j h_j g_j) \prec \delta$

但这个和式中X^δ是从首项得到的，那么就有

$$\mathrm{DEG}(\sum_j \mathrm{LT}(h_i) g_i) \prec \delta$$

注意$\sum_j \mathrm{LT}(h_j) g_j$是一个满足定理3.14的多项式，那么就存在常量$d_j$以及多重次数$\mu(j)$使得

$$\sum_j \mathrm{LT}(h_j) g_j = \sum_j d_j X^{\delta - \mu(j)} S(g_j, g_{j+1}) \tag{1}$$

并且其中$\mathrm{DEG}(X^{\delta-\mu(j)} S(g_j, g_{j+1})) \prec \delta$

由于$S(g_j, g_{j+1})$是 $\bmod G$余式为0的。除法算式给出唯一的表示，即存在$a_{ji} \in k[X]$使得

$$S(g_j, g_{j+1}) = \sum_i a_{ji} g_i$$

其中对所有的j,i $\mathrm{DEG}(a_{ji} g_i) \preceq \mathrm{DEG}(\sum_i S(g_i, g_{j+1}))$，我们有

$$X^{\delta-\mu(j)} S(g_j, g_{j+1}) = \sum_j X^{\delta-\mu(j)} a_{ji} g_i$$

再利用引理3.14，机油

$$\mathrm{DEG}(X^{\delta-\mu(j)} a_{ji}) \preceq \mathrm{DEG}(X^{\delta-\mu(j)} S(g_j, g_{j+1})) \prec \delta \tag{2}$$

把上述式子带入(2)有

$$\begin{aligned}
\sum_j \mathrm{LT}(h_j) g_j &= \sum_j d_j X^{\partial - \mu(j)} S(g_j, g_{j+1}) \\
&= \sum_j d_j \left(\sum_i X^{\delta-\mu(j)} a_{ji} g_i \right) \\
&= \sum_i \big(\sum_j d_j X^{\delta-\mu(j)} a_{ii} \big) g_i.
\end{aligned}$$

现在记$\sum_j d_j X^{\delta-\mu(j)} a_{ji}$为$h_i'$，则

$$\sum_j \mathrm{LT}(h_j) g_j = \sum_i h_i' g_i$$

其中，对所有的i，$\mathrm{DEG}(h_i' g_i) \prec \delta$ 。带入我们一开始列出的式子，就有

$$\begin{aligned} f &= \sum_{j,\mathrm{DEG}(h_j g_j)=\delta} h_j g_j + \sum_{\ell,\mathrm{DEG}(h_\ell g_\ell)\prec\delta} h_\ell g_\ell \\ &= \sum_{j,\mathrm{DEG}(h_j g_j)=\delta} \mathrm{LT}(h_j) g_j + \sum_{j,\mathrm{DEG}(h_j g_j)=\delta} [h_j - \mathrm{LT}(h_j)] g_j + \sum_{\ell,\mathrm{DEG}(h_j g_j)<\delta} h_\ell g_\ell \\ &= \sum_i h_i' g_i \quad + \sum_{j,\mathrm{DEG}(h_j g_j)} [h_j - \mathrm{LT}(h_j)] g_j \quad + \sum_{\mathrm{DEG}(h_\ell g_\ell)<\delta} h_\ell g_\ell. \end{aligned}$$

我们这么做的目的主要是为了跟除法算式一样，利用最小多项式得到矛盾，现在我们重写了一开始的多项式，其中每项都是严格小于δ，这与我们定义的δ是最小矛盾，因而这样子的余式不存在，矛盾。

3.16 推论

若$I = (f_1, \cdots, f_s) \in k[X]$是单项式理想，即其中每个$f_i$是单项式，则$\{f_1, \cdots, f_s\}$是$I$的格罗布纳基。

证明： 我们证明，若f, g是单项式，则$S(f, g) = 0$。由于f, g是单项式，设他们的次数是α, β，那么$\mathrm{LT}(f) = f = X^\alpha, \mathrm{LT}(g) = g = X^\beta$，则

$$S(f,g) = \frac{L(f,g)}{\mathrm{LT}(f)} f - \frac{L(f,g)}{\mathrm{LT}(g)} g = \frac{X^{\alpha\vee\beta}}{f} f - \frac{X^{\alpha\vee\beta}}{\mathrm{LT}(g)} g = 0$$

由定理3.15，$p, q, S(f, g)$的余式都是0，因而I是格罗布纳基。

3.17 定理：布切贝哥算法

$k[X]$中每一个理想$I = (f_1, \cdots, f_s)$都有格罗布纳基，且可以由一个算法得到。

证明： 我们给出算法的伪代码

$$\begin{gathered} \texttt{Input: } B = \{f_1, \cdots, f_s\}\ G = [f_1, \cdots, f_s] \\ \texttt{Output: 格罗布纳基 } B = \{g_1, \cdots, g_m\} \\ \texttt{Containing } \{f_1, \cdots, f_s\} \\ B := \{f_1, \cdots, f_s\}, G := [f_1, \cdots, f_s] \end{gathered}$$

代码指出我们定义了一些比较初始的参数，第三行指的是定义B是包含理想I的。

接着我们定义循环结构

REPEAT

$B' = B, G' = G$

FOR each pair $g, g'$with$g \neq g' \in B'$ DO

$r := S(g, g')$ mod G'的余式

IF$r \neq 0$ THEN

$B := B \cup \{r\}$, $G' = [g_1, \cdots, g_m, r]$

END IF

END FOR

这段代码的意思是，将每个包含I的子集B扩大，我们将通过添加S多项式$S(g, g')$的一个 mod G余式到其中，由于$g, g' \in I$。所以$S(g, g')$的余式在I中。故更大的集$B \cup \{r\}$也在I中。

唯一的问题是，r什么时候是0，因此，若算法结束，由布切贝哥定理，B'是格罗布纳基。

我们来证明算法是会停止的。设一个循环从B'开始，到B结束，由于$B' \subseteq B$，我们就有一个单项式理想的包含关系

$$(\mathrm{LT}(g') : g' \in B') \subseteq (\mathrm{LT}(g) : g \in B)$$

若$B' \subseteq B$，则存在一个严格的理想间的包含关系，我们设r是某个S mod B'的多项式的余式，且$B = B' \cup \{r\}$，但r是 mod G既约的，故对任意$g' \in B'$，r都不被$\mathrm{LT}(g')$整除。所以$\mathrm{LT}(r) \notin (\mathrm{LT}(g') : g' \in B')$。另一方面就有$\mathrm{LT}(r) \in (\mathrm{LT}(g) : g \in B)$ 。若算法不停止，我们就有一个严格无限上升的理想链，这与希尔伯特基定理相悖。因为$k[X]$是一个ACC

记得我们的例子3.6吗，$x^2z^2 - y^2z$不被G整除，但是我们添加了这个多项式进去之后就得到一个格罗布纳基了。

3.18 推论

1. 若$I = (f_1, \cdots, f_t)$是$k[X]$中的一个理想，则存在一个决定一个多项式$h(X) \in k[X]$是否在I中的一个算法。

2. 若$I = (f_1, \cdots, f_t)$，$I' = (f'_1, \cdots, f'_s)$是$k[X]$中的理想，则存在一个判断$I = I'$是否成立的一个算法。

证明 这个证明比较简单，由布切贝哥算法我们可以得到一组格罗布纳基，再利用格罗布纳基去计算$h \mod G$的余式就行。而$h \in I$当且仅当$r = 0$

证明： 我们用算法先得到一组I, I'的格罗布纳基$\{g_1, \cdots, g_t\}$和$\{g'_1, \cdots, g'_t\}$。证明1表示我们得到了一个可以确定是否有每个$g'_j \in I$以及若每个$g'_j \in I$是否有$I' \subseteq I$的算法。

对于反包含。我们只需要把证明的过程反过来就行，我们有判断是否有$g \in I'$的算法，以及利用布切贝哥定理就可以得到对每个g是否有$I \subseteq I'$的算法。

一个格罗布纳基可以非常大，因此我们在下列过程中尽量的找最小的格罗布纳基。

3.19 定义：

理想I的一个基$\{g_1, \cdots, g_m\}$是既约的，若

1. 每个g_i是首一的

2. 每个g_i是 $\mod \{g_1, \cdots, \hat{g_i}, \cdots, g_m\}$既约的。

我们的思想就是，我们将给出一个算法，来将一个格罗布纳基收缩为一个既约的格罗布纳基。

我们可以考虑一下线性的多项式，即

$$f_i(X) = a_{i1}x_1 + \cdots + a_{in}x_n$$

这种情况下，公共零点$\mathrm{Var}(f_1, \cdots, f_t)$是一个有$n$个未知量，$t$个方程的齐次方程组的解，它的系数组成$A = [a_{ij}]$为$t \times n$矩阵。那么既约的格罗布纳基对应于矩阵$A$的既约阶梯形式。

最后，我们来证明如何求理想的交的一个基结束我们的学习。当给定一个多元多项式方程组，求解的一个方法就是消元。给定一个理想$I \subseteq k[X]$，我们导出一个关于部分未定元的理想，它实质上是带一个低维平面$\mathrm{Var}(I)$的交。

3.20 定义：消去理想

设k是域，$I \subseteq k[X,Y]$是理想，其中$k[X,Y]$是关于不相交变量集$X \cup Y$的多项式环，消去理想是

$$I_X = I \cap k[X]$$

例如，$I = (x^2, xy)$，这个理想是一个单项式理想，因此它的格罗布纳基就是$\{x^2, xy\}$，且$I_x = (x^2) \subseteq k[x]$

3.21 命题

设k是域，$k[X] = k[x_1, \cdots, x_n]$有个使得$x_1 \succ \cdots \succ x_n$成立的单项式序且对固定的$p > 1$，设$Y = x_p, \cdots, x_n$，若$I \subseteq k[X]$有一个格罗布纳基$G = \{g_1, \cdots, g_m\}$，则对于消去理想$I_Y = I \cap k[x_p, \cdots, x_n]$,$G \cap I_Y$是格罗布纳基。

证明： 若$\{g_1, \cdots, g_m\}$是$I = (g_1, \cdots, g_m)$的格罗布纳基，则对每个$f \in I$都有某个g_i使得$\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$。设$f(x_p, \cdots, x_n) \in I_Y$非零，由于$I \subseteq I_Y$。所以存在某个$g_i(X)$使得$\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$。因此$\mathrm{LT}(g_i)$只涉及到后面的变量。不妨设$\mathrm{DEG}(\mathrm{LT}(g_i)) = \beta$。若$g_i$有一项$C_a X^a$涉及到前面的变量$x_i$，$i < P$。则因为$x_1 \succ \cdots \succ x_p \succ x_n$有$a \succ \beta$。由于$\beta$是$g_i$首项的次数，这个偏序告诉我们出现了矛盾，因为首项比其他项的次数都大。从而$g_i \in k[x_p, \cdots, x_n]$。因此，对于$I_Y = I \cap k[x_p, \cdots, x_n]$。因此$G \cap k[x_p, \cdots, x_n]$是格罗布纳基

3.22 命题

设k是一个域，$I_1, \cdots, I_t$是$k[X]$中的理想，其中$X = x_1, \cdots, x_n$

1. 考虑$n+t$个不定元的多项式环$k[X, y_1, \cdots, y_t]$，对所有的j，若J是$k[X, y_1, \cdots, y_t]$中由$1 - (y_1 + \cdots + y_t)$和$y_j I_j$生成的理想，则$\bigcap_{j=1}^t I_j = J_X$
2. 给定$I_1, \cdots I_t$的格罗布纳基，$\bigcap_{j=1}^t I_j$的格罗布纳基可以被计算出来。

证明： 若$f = f(X) \in J_X = J \cap k[X]$，则$f \in J$。由题设，我们可以得到等式

$$f(X) = g(X,Y)(1 - \sum y_j) + \sum_j h_j(X, y_1, \cdots, y_t) y_j q_j(X)$$

其中$g, h_j \in k[X, Y]$和$q_j \in I_j$。令$y_j = 1$而其他的y_i为0，那么有$f = (X, 0, \cdots, 1, \cdots, 0)q_j(X)$，注意$h_j(X, 0 \cdots, 1, \cdots, 0) \in k[X]$，因此$f \in I_j$对某个$j$成立。由于$j$的任意性，则$f \in \cap I_j$，即$J_X \subseteq \cap I_j$。

对反包含。若$f \in \cap I_j$，则我们有等式

$$f = f(1 - \sum y_j) + \sum_j y_i f = f - \sum y_i f + \sum y_i f$$

表明$f \in J_X$。

证明2： 我们利用证明1和3.21。如果采用单项式序，只需要令X的所有变量先于Y的变量即可。由命题1，$\cap_{j=1}^{i} I_j = J_X$，而命题3.21告诉我们对于消去理想J_X，$G \cap J_X$就是一个格罗布纳基。

3.23 例子

考虑理想$I = (x) \cap (x^2, xy, y^2) \subseteq k[x, y]$。其中$k$是域。我们用格罗布纳基来说明命题3.22。设$u, v$是新的变量。定义

$$J = (1 - u - v, ux, ux^2, uxy, vy^2) \subseteq k[x, y, u, v]$$

我们要来求一个J的格罗布纳基，按照字典序$x \prec y \prec v \prec u$。两个多项式的$S-$多项式为0，自然的就在格罗布纳基中，现在我们用布切贝哥算法给出一个J的格罗布纳基G

$$G = \{v + u - 1, x^2, yx, ux, uy^2 - y^2\}$$

那么I的一个格罗布纳基纠是$G \cap k[x, y]$，即不含有u, v元素的多项式，那么

$$I = (x) \cap (x^2, xy, y^2) = (x^2, xy)$$