系 统 科 学 与 数 学
J. Sys. Sci. & Math. Scis.
26(5) (2006, 10), 533–540

连续代数扩域上多项式因式分解的 Trager 算法*

袁 春 明

(中国科学院数学与系统科学研究院数学机械化重点实验室, 北京 100080)

摘要 多项式的因式分解是符号计算中最基本的算法，二十世纪六十年代开始出现的关于多项式因式分解的工作被认为是符号计算领域的起源. 目前多项式的因式分解已经成熟，并已在 Maple 等符号计算软件中实现，但代数扩域上的因式分解算法还有待进一步改进. 代数扩域上的基本算法是 Trager 算法. Weinberger 等提出了基于 Hensel 提升的算法. 这些算法是在单个扩域上做因式分解. 而在吴零点分解定理中，多个代数扩域上的因式分解是非常基本的一步，主要用于不可约升列的计算. 为了解决这一问题，吴文俊，胡森、王东明分别提出了基于方程求解的多个扩域上的因式分解算法. 王东明、林东岱提出了另外一个算法与 Trager 算法相似，将问题化为有理数域上的分解. 他们应用了吴的三角化算法，因此算法的终止性依赖于吴方法的计算. 支丽红则将提升技巧用于多个扩域上的因式分解算法. 本文将 Trager 的算法直接推广为连续扩域上的因式分解，只涉及结式计算与有理数域上的因式分解，给出了多个代数扩域上的因式分解一个直接的算法.

关键词 连续代数扩域，符号计算，吴零点分解，不可约升列，三角化，结式.

MR(2000) 主题分类号 12D05

1 算法的推广

我们考虑以下问题：设 F 是一个特征为零的域. $\alpha_1, \alpha_2, \cdots, \alpha_r$ 是 F 上的代数数. f 是 $F(\alpha_1, \alpha_2, \cdots, \alpha_r)$ 上的单变量多项式. 我们需要将 f 在 $F(\alpha_1, \alpha_2, \cdots, \alpha_r)$ 上进行因子分解.

根据吴零点分解定理 [1], $\alpha_1, \alpha_2, \cdots, \alpha_r$ 可以由以下不可约升列定义

$$(*) \qquad AS_r : \begin{cases} f_1(y_1) = 0, & \text{关于 } y_1 \text{ 为 } d_1 \text{ 次,} \\ f_2(y_1, y_2) = 0, & \text{关于 } y_2 \text{ 为 } d_2 \text{ 次,} \\ \vdots & \\ f_r(y_1, y_2, \cdots, y_r) = 0, & \text{关于 } y_r \text{ 为 } d_r \text{ 次,} \end{cases}$$

我们可以在 $f_i, (i \le r)$ 的初式中消去 $y_1, y_2, \cdots, y_r$, 使它们都是 F 中的元素，见 [2]. 下面我们假设 $\alpha_1, \alpha_2, \cdots, \alpha_r$ 的定义多项式的初式不含主变元 $y_1, y_2, \cdots, y_r$.

* 国家 “973” 项目 (2004318000) 资助.
收稿日期：2004-04-16, 收到修改稿日期：2005-05-30.

下面的两个引理是代数中的基本结果，为算法中使用方便，我们给出其构造性叙述 [3].

引理 1.1 设 F 为特征为零的域， α_1,α_2 为 F 上的代数元，则除了有限个 c 外，$\theta=\alpha_2+c\alpha_1$ 为 α_1,α_2 的本原元，即 $F(\theta)=F(\alpha_1,\alpha_2)$.

证 设 $f,g\in F[x]$ 分别为 α_1,α_2 的定义多项式， $K\supset F[\alpha_1,\alpha_2]$ 为 fg 的一个分裂域，设 f 和 g 在 K 中的零点分别为 $a_1,a_2,\cdots,a_m$ 和 $b_1,b_2,\cdots,b_n$, 其中 $a_1=\alpha_1,b_1=\alpha_2$. 对任意两个整数对 $(i,j)\neq(k,l)(i,k\leq m,j,l\leq n)$, 方程 $ta_i+b_j=ta_k+b_l$ 至多有一个解，若 $t\neq 0$, 则 $t=\frac{b_l-b_j}{a_i-a_k}$ 至多有 $\frac{m(m-1)n(n-1)}{2}$ 个可能值. 令 $h(t)=\prod\limits_{(i,j)\neq(k,l)}[t(a_i-a_k)+(b_j-b_l)]$ 由于 F 是无限域 (特征为零), 故除了有限个 $c\in F$ 外，可取到 c, 使得 $\theta=\alpha_2+c_1\alpha_1$, 其中 $c\in F$ 不满足方程 $h(t)=0$. 下面证明 $F[\theta]=F[\alpha_1,\alpha_2]$. 令 $p(x)=g(\theta-cx)\in F[\theta][x]$, 则 $p(\alpha_1)=0$, 而由 c 的取法， f 和 p 只有一个公共零点 α_1, 由 f 的不可约性 α 为 f 的单零点，故 $\mathrm{GCD}(f,p)=(x-\alpha_1)\in F[\theta][x]$, 从而 $\alpha_1\in F[\theta]$, 因此 $\alpha_2=\theta-c\alpha_1\in F[\theta]$.

引理 1.2 设 F 为特征为零的域, $\alpha_1,\alpha_2,\cdots,\alpha_r$ 为 F 上的代数元,则存在 $F(\alpha_1,\alpha_2,\cdots,\alpha_r)$ 的分裂域 $\overline{F}$ 上的多项式 $v(x_1,x_2,\cdots,x_{r-1})$, 使得如果 $v(a_1,a_2,\cdots,a_{r-1})\neq 0$, 则 $\theta=\alpha_r+a_{r-1}\alpha_{r-1}+\cdots+a_1\alpha_1$ 是 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 的本原元.

证 用归纳法, 对 r 作归纳. r=1 时, 显然命题成立. 下设 $r=k$ 时命题成立. 则 $r=k+1$ 时, 令 $\theta=\alpha_{k+1}+a_k\alpha_k+\cdots+a_1\alpha_1$, 分三种情况讨论. (1) $a_k=0$; (2) $a_k\neq 0(\frac{a_{k-1}}{a_k},\cdots,\frac{a_1}{a_k})$ 满足归纳假设得到的代数方程 $f_k(\frac{a_{k-1}}{a_k},\cdots,\frac{a_1}{a_k})=0$, 去分母后得到 $f_k^{'}(a_1,a_2,\cdots,a_k)=0$; (3) $a_k\neq 0, f_k(\frac{a_{k-1}}{a_k},\cdots,\frac{a_1}{a_k})\neq 0$, 则记 $\gamma=\alpha_k+\frac{a_{k-1}}{a_k}\alpha_{k-1}+\cdots+\frac{a_1}{a_k}\alpha_1$, γ 必为 $\alpha_1,\alpha_2,\cdots,\alpha_k$ 的本原元， $F(\gamma)=F(\alpha_1,\alpha_2,\cdots,\alpha_k)$. 则 $\theta=\alpha_{k+1}+a_k\gamma$, 设 γ,α_{k+1} 的定义多项式分别为 f,g 则 fg 在 $\overline{F}$ 上分裂, 设 f,g 在 $\overline{F}$ 中的零点分别为 $p_1,p_2,\cdots,p_m$ 和 $q_1,q_1,\cdots,q_n$, 其中 $p_1=\gamma,q_1=\alpha_{k+1}$, 则由引理 1.1 的证明知, 当 a_k 满足 $\prod\limits_{(i,j)\neq(k,l)}[a_k(p_i-p_k)+(q_j-q_l)]\neq 0$ 时， $\theta=\alpha_{k+1}+a_k\gamma$ 是 α_{k+1},γ 的本原元，其中 $p_i,q_j(i\leq m,j\leq n)$ 为 $\overline{F}$ 上关于 $a_1,a_2,\cdots,a_{k-1}$ 的代数元. 综合这三种情况，令 $f_{k+1}(a_1,a_2,\cdots,a_k)=a_k*f_k^{'}(a_1,a_2,\cdots,a_k)*\prod\limits_{(i,j)\neq(k,l)}[a_k(p_i-p_k)+(q_j-q_l)]$, 则对 $(a_1,a_2,\cdots,a_k)$ 使得 $\theta=\alpha_{k+1}+a_k\alpha_k+\cdots+a_1\alpha_1$ 不是本原元，则 $(a_1,a_2,\cdots,a_k)$ 必满足方程 $f_{k+1}(a_1,a_2,\cdots,a_k)=0$, 证毕.

引理 1.3 设 F 为特征为 0 的域， $y_1,y_2,\cdots,y_r$ 为 F 上的代数元， $[F(y_1,y_2,\cdots,y_r):F]=s,\theta\in F(y_1,y_2,\cdots,y_r)$ 且 $[F(\theta):F]=s$, 则 θ 为 $y_1,y_2,\cdots,y_r$ 的本原元. 即 $F(\theta)=F(y_1,y_2,\cdots,y_r)$.

证 用反证法. 显然有 $F(\theta)\subseteq F(y_1,y_2,\cdots,y_r)$. 设存在 $\beta\in F(y_1,y_2,\cdots,y_r),\beta\notin F(\theta)$, 则 $[F(\theta,\beta):F]\leq[F((y_1,y_2,\cdots,y_r)):F]=s$. 因为 $\beta\notin F(\theta)$, 所以 $[F(\theta,\beta):F(\theta)]=p>1$. 故 $[F(\theta,\beta):F]=[F(\theta,\beta):F(\theta)]*[F(\theta):F]=p*s>s$ 矛盾. 所以 $F(\theta)=F(y_1,y_2,\cdots,y_r)$.

下面我们考虑由不可约升列定义的代数元 $y_1,y_2,\cdots,y_r$. 设 AS_r 是由 r 个多项式组成的不可约升列 AS_r, 考虑 $y_1,y_2,\cdots,y_r$ 对基域 F 的本原元 $\theta,\theta=a_1y_1+\cdots+a_{r-1}y_{r-1}+y_r$. 由引理 1.2, 除满足某个代数方程 $v(a_1,a_2,\cdots,a_{r-1})=0$ 的 $a_1,a_2,\cdots,a_{r-1}$ 外， θ 为本原元.

对 $P\in F(y_1,y_2,\cdots,y_r)[y]$ 我们记

$$R=\mathrm{res}(P,AS_r),\tag{1}$$

称为 P 对 AS_r 的结式，其中 $\mathrm{res}(P,f_r,y_r)$ 为多项式 P 与 f_r 关于 y_r 的结式.

我们设基域为 F, $F=Q$ 或者 $Q(u_1,u_2,\cdots,u_d)$, 其中 $u_1,u_2,\cdots,u_d$ 为未定元，则由

于 AS_r 不可约，故 $[F(y_1,y_2,\cdots,y_r):F]=d_1d_2\cdots d_r$. 由引理 1.3, 如果 θ 为本原元，则 $[F(\theta):F]=d_1d_2\cdots d_r$.

引理 1.4　使用以上引入的符号，$\theta=a_1y_1+\cdots+a_{r-1}y_{r-1}+y_r$ 为本原元当且仅当 $g(\theta)=\mathrm{res}(\theta-a_1y_1-\cdots-a_{r-1}y_{r-1}-y_r,AS_r)$ 为 $d_1d_2\cdots d_r$ 次的且不可约.

证　"$\Longrightarrow$". 首先 $g(\theta)=\mathrm{res}(\theta-a_1y_1+\cdots+a_{r-1}y_{r-1}+y_r,AS_r)$ 关于 θ 的次数小于等于 $d_1d_2\cdots d_r$. 用归纳法证之，对 r 作归纳，$r=1$ 时上述结论显然成立，设 $r=k$ 时结论成立，则 $r=k+1$ 时 $g(\theta)=\mathrm{res}(\theta-a_1y_1-a_2y_2-\cdots-a_{k+1}y_{k+1},AS_{k+1})=\mathrm{res}(\mathrm{res}(\cdots\mathrm{res}(\theta-a_1y_1-a_2y_2-\cdots-a_{k+1}y_{k+1},f_{k+1},y_{k+1}),\cdots,f_2,y_2),f_1,y_1)$. 由归纳假设 $g'(\theta,y_1)=\mathrm{res}(\cdots\mathrm{res}(\theta-a_1y_1-a_2y_2-\cdots-a_{k+1}y_{k+1},f_{k+1},y_{k+1}),\cdots,f_2,y_2)$. 关于 θ 次数小于等于 $d_2d_3\cdots d_{k+1}$, 故 $g(\theta)=\mathrm{res}(g'(\theta,y_1),f_1,y_1)$ 的 Sylvester 矩阵关于 θ 的系数共有 d_1 行，考虑关于 θ 的最高次项，它最多只能被乘 d_1 次，故 $g(\theta)$ 关于 θ 的次数不高于 $d_1d_2\cdots d_{k+1}$. 若 $\theta=a_1y_1+\cdots+a_{r-1}y_{r-1}+y_r$ 为本原元，则 $g(\theta)$ 关于 θ 的次数必为 $d_1d_2\cdots d_{k+1}$ 且不可约.

"$\Longleftarrow$" 若 $g(\theta)=\mathrm{res}(\theta-a_1y_1-\cdots-a_{r-1}y_{r-1}-y_r,AS_r)$ 为 $d_1d_2\cdots d_r$ 次的且不可约，则由引理 1.3, $g(\theta)$ 必为 $d_1d_2\cdots d_r$ 次的且不可约，证毕.

对任意的 $F(y_1,y_2,\cdots,y_r)[y]$ 上的多项式 $f(y,y_1,y_2,\cdots,y_r)$, 设 f 为无平方因子的. 由于 θ 为 $y_1,y_2,\cdots,y_r$ 的本原元，故 $y_1,y_2,\cdots,y_r$ 可由 θ 的多项式表示. 即可将 $f(y,y_1,y_2,\cdots,y_r)$ 写成 $f(y,\theta)$. 由引理 1.4, θ 的定义多项式为 $g(\theta)=\mathrm{res}(\theta-a_1y_1-a_2y_2-\cdots-y_r,AS_r)$. 则由 [4] 知，$\mathrm{res}(f,g,x)=(-1)^{\deg(f,x)*\deg(g,x)}\mathrm{Init}(f)^{\deg(f,x)}\prod\limits_{\alpha:g(\alpha)=0}f(\alpha)$, 其中 $\mathrm{Init}(f)$ 表示 f 关于 x 的首项系数. 故在相差 F 中的一个元素下，

$$g(\theta)=\prod_{[y_1,y_2,\cdots,y_r]:AS_r=0}(\theta-a_1y_1-a_2y_2-\cdots-a_ry_r).$$

由 Trager 的算法 [5] 可知，除了有限个 c 外，$R'=\mathrm{res}(f(y+c\theta,\theta),g(\theta),\theta)$ 为无平方因子的，并且若 R' 在 $F[y]$ 上的完全分解为 $R'=\prod\limits_i R'_i$, 则

$$f(y,\theta)=\prod_i\mathrm{GCD}(R'_i,f(y+c\theta,\theta))|_{y=y-c\theta}$$

为 f 在 $F(\theta)$ 上的完全分解，亦为 $F(y_1,y_2,\cdots,y_r)$ 上的完全分解. 其中 GCD 表示 $F[\theta][y]$ 中的最大公因子.

我们实际上已经提供了一个 $f(y,y_1,\cdots,y_r)$ 的分解算法，但需要将 y_i 用 θ 表示，因而不太实用，下面给出一个直接分解算法.

设 $\theta=a_1y_1+a_2y_2+\cdots+a_{r-1}y_{r-1}+y_r$ 为本原元.

$$\begin{aligned}f(y,y_1,y_2,\cdots,y_r)|_{y=y+c\theta}&=f(y+ca_1y_1+ca_2y_2+\cdots+cy_r,y_1,y_2,\cdots,y_r)\\&=f(y+c_1y_1+c_2y_2+\cdots+c_ry_r,y_1,y_2,\cdots,y_r),\end{aligned}$$

其中 $c_i=ca_i,i=1,2,\cdots,r-1,c_r=c,c\neq0$ 为使得 R' 为无平方因子的常数.

下面记 $\theta=c_1y_1+c_2y_2+\cdots+c_ry_r$, 由于 θ 为本原元，y_i 可以由 θ 表示，有

$$h(y+\theta,\theta)=f(y,y_1(\theta),y_2(\theta),\cdots,y_r(\theta))|_{y=y+c_1y_1(\theta)+c_2y_2(\theta)+\cdots+c_ry_r(\theta)}.\tag{2}$$

定理 1.5 设 $(y_1, y_2, \cdots, y_r)$ 为 F 上的代数元， $f(y, y_1, \cdots, y_r) \in F(y_1, y_2, \cdots, y_r)[y]$ 为 y 的无平方因子的多项式， $\theta = c_1y_1 + c_2y_2 + \cdots + c_ry_r$ 为 $y_1, y_2, \cdots, y_r$ 的本原元，且使得 $R^{'} = \mathrm{res}(h(y+\theta, \theta), g(\theta), \theta)$ 为无平方因子的，其中 $h(y+\theta, \theta)$ 由 (2) 定义，则在相差 F 上的一个元素下 $R = R^{'}$，其中 R 由 (1) 定义.

证 我们用 "=" 表示两者在相差 F 上的元素下相等.

$$
\begin{aligned}
R &= \mathrm{res}(f, AS_r)|_{y=y+c_1y_1+c_2y_2+\cdots+c_ry_r} \\
&= \mathrm{res}(\cdots \mathrm{res}(\mathrm{res}(f(y + c_1y_1 + c_2y_2 + \cdots + c_ry_r, y_1, y_2, \cdots, y_r), f_r, y_r), f_{r-1}, y_{r-1}), \cdots, f_1, y_1) \\
&= \mathrm{res}\Big(\cdots \mathrm{res}\Big(\prod_{\overline{y}_r : f_r(y_1, \cdots, y_{r-1}, \overline{y}_r)=0} f(y + c_1y_1 + c_2y_2 + \cdots + \\
&\qquad c_{r-1}y_{r-1} + c_r\overline{y}_r, y_1, y_2, \cdots, \overline{y}_r), f_{r-1}, y_{r-1}\Big), \cdots, f_1, y_1\Big) \\
&= \cdots \\
&= \prod_{\overline{y}_1 : f_1(\overline{y}_1)=0} \prod_{\overline{y}_2 : f_2(\overline{y}_1, \overline{y}_2)=0} \cdots \prod_{\overline{y}_r : f_r(\overline{y}_1, \overline{y}_2, \cdots, \overline{y}_r)=0} f(y + c_1\overline{y}_1 + c_2\overline{y}_2 + \cdots + c_r\overline{y}_r, \overline{y}_1, \overline{y}_2, \cdots, \overline{y}_r) \\
&\triangleq \prod_{[y_1, y_2, \cdots, y_r] : AS_r = 0} f(y + c_1y_1 + c_2y_2 + \cdots + c_ry_r, y_1, y_2, \cdots, y_r).
\end{aligned}
$$

$$
\begin{aligned}
R^{'} &= \mathrm{res}(h(y+\theta, \theta), g(\theta), \theta) \\
&= \mathrm{res}(f(y + \theta, y_1(\theta), y_2(\theta), \cdots, y_r(\theta)), g(\theta), \theta) \\
&= \prod_{\overline{\theta} : g(\overline{\theta})=0} f(y + \overline{\theta}, y_1(\overline{\theta}), y_2(\overline{\theta}), \cdots, y_r(\overline{\theta})) \\
&= \prod_{[y_1, y_2, \cdots, y_r] : AS_r = 0} f(y + c_1y_1 + c_2y_2 + \cdots + c_ry_r, y_1, y_2, \cdots, y_r).
\end{aligned}
$$

其中最后一个等式是因为在相差 F 上的一个因子下， $g(\theta) = \mathrm{res}(\theta - c_1y_1 - c_2y_2 - \cdots - c_ry_r, AS_r) = \prod_{[y_1, y_2, \cdots, y_r] : AS_r = 0} (\theta - c_1y_1 - c_2y_2 - \cdots - c_ry_r)$. 所以有 $R = R^{'}$，证毕.

方案 (*): 先取 a_{r-1} 的 $\frac{(\prod_{i=1}^{r-1} d_i)(\prod_{i=1}^{r-1} d_i+1)(\prod_{i=1}^{r} d_i)(\prod_{i=1}^{r} d_i+1)}{2} + 1$ 个非零值；然后再取 a_{r-2} 的 $\frac{(\prod_{i=1}^{r-2} d_i)(\prod_{i=1}^{r-2} d_i+1)(\prod_{i=1}^{r-1} d_i)(\prod_{i=1}^{r-1} d_i+1)}{2} + 1$ 个非零值；以此类推，取 a_1 的 $\frac{d_1(d_1-1)d_1d_2(d_1d_2-1)}{2} + 1$ 个非零值 (不妨取 a_i 为整数).

引理 1.6 设 $a_i \neq 0, 1 \leq i \leq r-1$, AS_r 由前面定义, 则对于 $\theta = a_1y_1 + \cdots + a_{r-1}y_{r-1} + y_r$, 由方案 (*) 选取 $a_1, a_2, \cdots, a_{r-1}$, 则除了有限的组合外，必能得到 θ 为本原元.

证 我们设 $a_i \neq 0, 1 \leq i \leq r-1$, 则 $\theta = a_1y_1 + \cdots + a_{r-1}y_{r-1} + y_r = (\cdots((b_1y_1 + y_2) + y_3)b_3 + \cdots + y_{r-1})b_{r-1} + y_r$, 其中 $b_i = \frac{a_i}{a_{i+1}}, a_r = 1$.

下面我们考虑使得 θ 为本原元的 b_i 的取值. 我们的方法是：在 $b_1, b_2, \cdots, b_{k-1}$, 为使得 $\gamma_k = (\cdots(b_1y_1 + y_2)b_2 + \cdots + y_{k-1})b_{k-1} + y_k) = y_k + \frac{a_{k-1}}{a_k}y_{k-1} + \cdots + \frac{a_1}{a_k}y_1$ 是 $y_1, y_2, \cdots, y_k$ 的本原元的前提下，取 b_k, 使得 $\gamma_{k+1} = (\cdots(b_1y_1 + y_2)b_2 + \cdots + y_{k-1})b_{k-1} + y_k)b_k + y_{k+1} = y_k + \frac{a_k}{a_{k+1}}y_k + \cdots + \frac{a_1}{a_{k+1}}y_1$ 为 $y_1, y_2, \cdots, y_{k+1}$ 的本原元.

由上面的讨论知 γ_k 在 F 上的定义多项式为： $f(\gamma) = \prod_{[y_1, y_2, \cdots, y_k] : AS_k = 0} (\gamma - \frac{a_1}{a_k}y_1 - \cdots -$

$\frac{a_{k-1}}{a_k}y_{k-1}-y_k)$ 为 $d_1d_2\cdots d_k$ 次的，设 y_{k+1} 在 F 上的定义多项式为 $h(y_{k+1})=\prod_i(y_{k+1}-q_i)$，令 $w(y_{k+1})=\mathrm{res}(f_{k+1},AS_k)\in F[y_{k+1}]$, 则有 $h(y_{k+1})|w(y_{k+1})$, 因而 $\deg(h,y_{k+1})\le\prod_{i=1}^{k+1}d_i$.

由引理 1.1 的证明知，至多除了 $\frac{(\prod_{i=1}^{k}d_i)(\prod_{i=1}^{k}d_i+1)(\prod_{i=1}^{k+1}d_i)(\prod_{i=1}^{k+1}d_i+1)}{2}$ 个值外， b_k 可使 γ_{k+1} 为 $y_1,y_2,\cdots,y_{k+1}$ 的本原元．又由于对于给定的 $a_{i+1},\cdots,a_{r-1}$, b_i 与 a_i 一一对应，故我们可以按照方案 $(*)$ 取 a_i 的值．由上面的分析，遍历这些值的所有组合，则必能找到一组 $a_1,a_2,\cdots,a_{r-1}$, 使得 $\theta=a_1y_1+\cdots+a_{r-1}y_{r-1}+y_r$ 为本原元.

2 算法与例子

由前面的讨论知:对 $[c_1,c_2,\cdots,c_r]$, $c_r\neq0$ 而言,除了满足一个代数方程 $v(\frac{c_1}{c_r},\cdots,\frac{c_{r-1}}{c_r})=0$ 及有限个 c_r 外， R 为无平方因子的，并且若 $R=\prod_i R_i$ 为 R 在 $F[y]$ 上的不可约分解，则

$$\begin{aligned}&f(y,y_1,y_2,\cdots,y_r)\\&=\prod_i\mathrm{GCD}(R_i,f(y+c_1y_1+c_2y_2+\cdots+c_ry_r,y_1,y_2,\cdots,y_r))|_{y=y-c_1y_1-c_2y_2-\cdots-c_ry_r}\end{aligned}$$

为 f 在 $F(y_1,y_2,\cdots,y_r)$ 上的完全分解．下面给出我们的算法.

算法

输入：代数数 $(y_1,y_2,\cdots,y_r)$ 的不可约定义升列 AS_r, $F(y_1,y_2,\cdots,y_r)$ 上的无平方因子多项式 $f(y,y_1,y_2,\cdots,y_r)$.

输出： $f(y,y_1,y_2,\cdots,y_r)$ 在 $F(y_1,y_2,\cdots,y_r)$ 上的因式分解.

第一步：若 f 关于 y 的次数小于等于 1, 则输出 f; 否则按照方案 $(*)$ 给 $a_i(1\le i\le r-1)$ 取值，检验 $\mathrm{res}(\gamma-y_r-a_{r-1}y_{r-1}-\cdots-a_1y_1,AS_r)$ 是否是不可约的．若是，则由引理 1.4, $\gamma=y_r+a_{r-1}y_{r-1}+\cdots+a_1y_1$ 为 $y_1,y_2,\cdots,y_r$ 的本原元 (又由引理 1.6, 可在有限步内得到), 进行下一步；否则换一组 a_i, 重复第一步.

第二步：取 $c=\pm1,\pm2,\cdots$, 若 $R(y)=\mathrm{res}(f,AS_r)|_{y=y+c\gamma}$ 为无平方因子的，则记 $c_i=ca_i(i\le r-1)$, $c_r=c$, 进行下一步；否则换一个 c, 重复第二步.

第三步：在 $F(y)$ 上分解 $R(y)$, 设 $R(y)=\prod_i R_i(y)$ 为 $R(y)$ 的完全分解.

第四步： 设 $F_i=\mathrm{GCD}(R_i,f(y+c_1y_1+c_2y_2+\cdots+c_ry_r,y_1,y_2,\cdots,y_r))|_{y=y-c_1y_1-c_2y_2-\cdots-c_ry_r}$ 为 R_i 与 $f(y+c_1y_1+c_2y_2+\cdots+c_ry_r,y_1,y_2,\cdots,y_r)$ 在 $F[y_1,y_2,\cdots,y_r][y]$ 中的最大公因子．设 $G_1,G_2,\cdots,G_s$ 为 F_i 关于 y 的次数大于零的，则可计算 $C,D\in F[y_1,y_2,\cdots,y_r]$ 关于 AS_r 约化，使得 $D*f=C*\prod_i G_i$, 又由 [2], 可将 D 化为 F 上的常数，记为 $f=C*\prod_i G_i$. 输出 G_i,C.

算法中第四步用到了代数扩域中的 GCD算法，见 [1,6].

引理 1.5　$AS_r=f_1,f_2,\cdots,f_r$ 为 $y_1,y_2,\cdots,y_r$ 的定义升列， $f(y,y_1,y_2,\cdots,y_r)\in F(y_1,y_2,\cdots,y_r)[y]$, $R(y,y_1,y_2,\cdots,y_r)=\mathrm{prem}(f,f_r,y_r)$, 则 $\mathrm{res}(f,f_r,y_r)$ 与 $\mathrm{res}(R,f_r,y_r)$ 只相差 F 上的一个因子.

证　记 I_r 为 f_r 的初式．因为 $R=\mathrm{prem}(f,f_r,y_r)=I_r^s*f-\prod_i Q*f_r$. 记 Detpol() 为行

列式多项式函数 (见 [7]), $\deg(f,y_r)=s_r,\deg(f_r,y_r)=d_r,\deg(R,y_r)=t_r$ 则

$$\begin{aligned}\mathrm{res}(f,f_r,y_r)&=\mathrm{Detpol}(y_r^{d_r-1}f,\cdots,y_rf,f,y_r^{s_r-1}f_r,\cdots,y_rf_r,f_r)\\&=\frac{1}{I_r^{s*d_r}}*\mathrm{Detpol}(I_r^sy_r^{d_r-1}f,\cdots,I_r^sy_rf,I_r^sf,y_r^{s_r-1}f_r,\cdots,y_rf_r,f_r)\\&=\frac{1}{I_r^{s*d_r}}*(I_r^{s_r-t_r})*\mathrm{Detpol}(y_r^{d_r-1}R,\cdots,y_rR,R,y_r^{t_r-1}f_r,\cdots,y_rf_r,f_r)\\&=\frac{1}{I_r^{s*d_r}}*(I_r^{s_r-t_r})*\mathrm{res}(R,f_r,y_r).\end{aligned}$$

证毕.

由上述引理我们定义 $\mathrm{PRes}(A(x),B(x))\triangleq\mathrm{res}(\mathrm{prem}(A(x),B(x),x),B(x))$ 则用 PRes 代替算法中的 res 也可.

下面介绍来自参考文献 [8] 的一个例子

$$h_1=u_3\,{y_1}^2+2\,u_1\,u_2\,y_1+2\,{u_1}^2y_1-u_3\,{u_1}^2,$$

$$h_2=u_3\,{y_2}^2-2\,u_1\,u_2\,y_2+2\,{u_1}^2y_2-u_3\,{u_1}^2,$$

$$h_3=u_3\,{y_3}^2-{u_3}^2y_3-{u_2}^2y_3+{u_1}^2y_3-u_3\,{u_1}^2.$$

开始时我们在 $Q(u_1,u_2,u_3,y_1)$ 上分解 h_2, 其中 y_1 的添加多项式为 h_1, 我们用 PRes 代替 res 进行计算. 取 $c_1=1$, 发现 h_2 在 $Q(u_1,u_2,u_3,y_1)$ 上是不可约的. 故 h_1,h_2 为 y_1,y_2 的不可约升列.

我们按照上述算法步骤的第一步取 $(c_1,c_2)=(1,1)$, 由上面知 $\gamma=y_2+y_1$ 是 (y_1,y_2) 的本原元. 在第二步取 $c=1$ 通过计算 $R(y_3)$ 是一个无平方因子多项式, $h=h_3|_{y_3=y_3+y_2+y_1}$. 第三步, 分解因式 $R(y_3)=t_0t_1t_2$, 其中 $t_0\in Q(u_1,u_2,u_3)$, 故只需要考虑 t_1,t_2. 第四步计算最大公因子 $r_1=\mathrm{GCD}(t_1,h)|_{y_3=y_3-y_1-y_2};r_2=\mathrm{GCD}(t_2,h)|_{y_3=y_3-y_1-y_2}$, 得到 h_3 的两个因子为 r_1,r_2.

$$\begin{aligned}r_1=\;&5{u_1}^2{u_2}^4y_2+12{u_2}^2y_3{u_1}^4+4u_3y_1{}^2{u_1}^4-14{u_1}^4{u_2}^2y_2-2{u_1}^2y_3{u_3}^4-14{u_2}^2y_1{u_1}^4\\&+4u_3{y_2}^2{u_1}^4-2u_3{u_2}^2{u_1}^4+6{u_2}^3y_1{u_1}^3+4{u_3}^3{y_2}^2{u_1}^2+5{u_3}^4{u_1}^2y_1+5{u_2}^4y_1{u_1}^2\\&-12{u_3}^2y_3{u_1}^4+2{u_3}^3{u_2}^2{u_1}^2+5{u_3}^4{u_1}^2y_2+14{u_3}^2{u_1}^4y_2+4{u_3}^3y_1{}^2{u_1}^2-2{u_2}^4y_3{u_1}^2\\&-5u_2y_1{u_1}^5+14{u_3}^2y_1{u_1}^4+5u_2y_2{u_1}^5-6{u_2}^3y_2{u_1}^3+u_1{u_2}^5y_2+{u_3}^5y_2y_1-{u_2}^5y_1u_1\\&-4{u_3}^2{u_2}^2y_3{u_1}^2-4{u_3}^3y_3y_1{u_1}^2+u_3{u_2}^4y_2y_1+u_3{u_1}^4y_1y_2+{u_3}^4u_1u_2y_2-u_2{u_3}^4y_1u_1\\&+2{u_3}^3{u_1}^2y_1y_2+10{u_3}^2{u_1}^2y_2{u_2}^2-4{u_3}^3{u_1}^2y_3y_2+2{u_3}^2u_1{u_2}^3y_2-4u_3{u_1}^4y_2y_3\\&+2{u_3}^3y_2{u_2}^2y_1-8u_3u_2y_1{}^2{u_1}^3+2{u_3}^2u_2y_1{u_1}^3+4u_3{u_2}^2y_1{}^2{u_1}^2+10{u_3}^2{u_2}^2y_1{u_1}^2\\&-2{u_2}^3{u_3}^2y_1u_1-4u_3y_3y_1{u_1}^4+8{u_1}^3u_2{y_2}^2u_3+4u_3{u_2}^2{y_2}^2{u_1}^2-2{u_3}^2u_2y_2{u_1}^3+u_3{u_1}^6\\&+{u_3}^5{u_1}^2-10y_3{u_1}^6+9y_1{u_1}^6-4u_3{u_1}^2{u_2}^2y_2y_3+9{u_1}^6y_2+2{u_3}^3{u_1}^4-4u_3{u_2}^2y_1y_3{u_1}^2\\&-2u_3{u_1}^2{u_2}^2y_1y_2+8u_3u_2y_1y_3{u_1}^3-8u_3{u_1}^3u_2y_2y_3+u_3{u_2}^4{u_1}^2,\end{aligned}$$

$$
\begin{aligned}
r_2 = {} & 16{u_1}^4{u_3}^{17} + 4{u_1}^2{u_2}^2y_1y_2{u_3}^{15} - 16{u_1}^3u_2y_1{u_3}^{15}y_3 + 12{u_3}^{13}{u_1}^8 - 2{u_1}^2{u_3}^{18}y_2 \\
& +8{u_1}^2{u_3}^{17}{u_2}^2 - 10{u_1}^6y_1{u_3}^{14} - 12{u_1}^4y_1{u_3}^{16} + 4{u_3}^{13}{u_2}^4{u_1}^4 + 4{u_3}^{13}{u_2}^6{u_1}^2 \\
& -20{u_3}^{13}{u_2}^2{u_1}^6 + 12{u_3}^{14}{u_1}^6y_3 - 2{u_1}^2y_1{u_3}^{18} - 12{u_1}^4{u_3}^{16}y_2 + 8{u_1}^4{u_3}^{16}y_3 \\
& +28{u_1}^4{u_3}^{15}{u_2}^2 + 10{u_1}^2{u_3}^{15}{u_2}^4 + 8{u_1}^2{u_2}^2y_1{u_3}^{15}y_3 + 2{u_1}^2{u_3}^{19} - 2{u_3}^{19}y_2y_1 \\
& -10{u_1}^6y_2{u_3}^{14} - 4{u_3}^{18}y_3{u_1}^2 - 8{u_1}^4{u_3}^{15}{y_2}^2 - 4{u_3}^{17}y_2{u_2}^2y_1 - 8{u_3}^{16}{u_2}^2y_3{u_1}^2 \\
& -10{u_1}^5u_2y_2{u_3}^{14} - 4u_1{u_2}^3y_2{u_3}^{16} + 12{u_1}^4{u_2}^2y_2{u_3}^{14} - 2{u_1}^2{u_2}^4y_2{u_3}^{14} - 4{u_3}^{14}{u_2}^4y_3{u_1}^2 \\
& -8{u_3}^{14}{u_2}^2y_3{u_1}^4 - 2{u_3}^{15}{u_2}^4y_2y_1 - 8{u_1}^2{u_3}^{17}{y_2}^2 + 8{u_1}^4y_2{u_3}^{15}y_3 - 16{u_1}^3{u_3}^{15}u_2{y_2}^2 \\
& -8{u_1}^2{u_3}^{15}{y_2}^2{u_2}^2 - 8{u_1}^2{u_2}^2{y_1}^2{u_3}^{15} + 16{u_1}^3{u_3}^{15}{y_1}^2u_2 + 2u_1{u_2}^5y_1{u_3}^{14} + 2u_1u_2y_1{u_3}^{18} \\
& +4u_1{u_2}^3y_1{u_3}^{16} + 10{u_1}^5u_2y_1{u_3}^{14} + 4{u_1}^3{u_3}^{16}u_2y_2 - 4{u_1}^2{u_3}^{16}y_2{u_2}^2 + 8{u_1}^2{u_3}^{17}y_3y_2 \\
& -2{u_1}^4y_1y_2{u_3}^{15} + 8{u_1}^4y_1{u_3}^{15}y_3 - 4{u_1}^2y_1{u_3}^{17}y_2 - 2{u_1}^2{u_2}^4y_1{u_3}^{14} + 12{u_1}^4{u_2}^2y_1{u_3}^{14} \\
& -4{u_1}^2{u_2}^2y_1{u_3}^{16} - 12{u_1}^3{u_2}^3y_1{u_3}^{14} - 8{u_1}^4{u_3}^{15}{y_1}^2 - 4{u_1}^3u_2y_1{u_3}^{16} + 8y_1{u_3}^{17}y_3{u_1}^2 \\
& +12{u_1}^3{u_2}^3y_2{u_3}^{14} - 2u_1{u_2}^5y_2{u_3}^{14} - 2u_1u_2y_2{u_3}^{18} - 8{u_1}^2{y_1}^2{u_3}^{17} + 16{u_1}^3u_2y_2{u_3}^{15}y_3 \\
& +8{u_1}^2{u_2}^2y_2{u_3}^{15}y_3 + 26{u_3}^{15}{u_1}^6.
\end{aligned}
$$

过程中我们应用了引理 1.5, 消去或添加了 $Q(u_1,u_2,u_3)$ 中的一些因子. 经检验所得确为 h_3 的因子. 因为 $[h_1,h_2]$ 为不可约的, 首系数与 y_1,y_2 无关, 因此可将 r_1,r_2 关于 y_3 的首项系数中的 y_1,y_2 消去 [2], 再移去一些 $Q(u_1,u_2,u_3)$ 中的常数因子, 最后得到化简后的两个因子 p_1,p_2.

$$
\begin{aligned}
p_1 &= -{u_1}^2u_3 - {u_1}^2y_1 + u_1u_2y_1 - {u_1}^2y_2 - u_1u_2y_2 + 2{u_1}^2y_3 - u_3y_2y_1, \\
p_2 &= -{u_1}^2{u_3}^2 + 2{u_1}^4 - 2{u_2}^2{u_1}^2 + {u_3}^2y_2y_1 + y_1{u_1}^2u_3 \\
&\quad -y_1u_3u_1u_2 + y_2{u_1}^2u_3 + y_2u_3u_1u_2 + 2{u_1}^2u_3y_3.
\end{aligned}
$$

计算得

$$
h_3 = \frac{p_1 * p_2}{4u_1^4} \qquad \bmod[h_1,h_2].
$$

参 考 文 献

[1] 吴文俊. 数学机械化. 北京：科学出版社， 2003.

[2] Gao X S. The minimal characteristic basis of a polynomial ideal. *Systems Science and Mathmatical Sciences*, 1989, **2**(3): 236–242.

[3] Buchberger B, Collins G E, Loos R, Albrecht R. Computer Algebra, Symbolic and Algebraic Computation. World Publishing Corporation, Beijing, 1988.

[4] Geddes K O, Czapor S R, Labahn G. Algotithms for Computer Algebra. Klumer Academic Publishers, 1992.

[5] Trager B M. Algebraic Factoring and Rational Function Intergration. Proc. ACM SYMSAC, 1976: 219–226.

[6] van Hoeij M and Monagan M. Algorithms for Polynomial GCD Computaton over Algebraic Function Fields. Proc. of ISSAC2004, 2004: 297–304.

[7] Mishra B. Algorithmic Algebra (影印版). 北京：科学出版社， 2001.

[8] Wang D. Elimination Methods. Springer, Wien New York, 2001.

[9] Hu S and Wang D. Fast factorization of polynomials over rational number field or its extension fields. *Kexue Tongbao*, 1986, **31**: 133–152.

[10] Wang D and Lin D. A method for multivariate polynomial factorization over successive algebraic extension fields. 数学与数学机械化, 2001: 138–172.
[11] Weinberger P J and Rothschild L P. Factoring polynomials over algebraic number fields. *ACM Trans. Math. Software*, 1979, **2**: 335–350.
[12] Wang P S. Factoring multivariate polynomial over algebraic number fields. *Math. Comp.*, 1978, **30**: 324–336.
[13] Zhi L H. An optimal method for algebraic factoring. *J. of Computer Science and Technology*, 1997, **12**: 1–9.

TRAGER'S FACTORIZATION ALGORITHM OVER SUCCESSIVE EXTENSION FIELDS

Yuan Chunming

(*Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100080)

Abstract Polynomial factorizations are basic problems in symbolic computation. Polynomial factorization algorithms appeared in the 1960's are considered to be the origin of the field of symbolic computation. At present, polynomial factorization algorithms are well established and implemented in symbolic computation software such as MAPLE. But factorization algorithms over successive algebraic extension fields are still under investigation. The basic factorization algorithm over algebraic extension fields is Trager's algorithm. Algorithms for a single algebraic extension field based on Hensel lifting are given by Weinberger et al. However, in order to compute the irreducible ascending chain in Wu's method, polynomial factorizations over successive algebraic extension fields are needed. Wu, Hu, and Wang independently put forward factorization algorithms over successive algebraic extension fields based on methods of equation solving. Similar to the Trager's algorithm, Wang and Lin proposed another algorithm reducing the problem to the factorization over the rational number field. In their approach, Wu's triangularization algorithm is used, and hence the termination of the algorithm depends on the computation of Wu's method. Zhi applied the lifting technique to the factorization over successive algebraic extension fields. A direct algorithm on factorization over successive algebraic extension fields is given in this paper, extending Trager's algorithm to factorization over successive algebraic extension fields. The proposed algorithm only uses resultant computation and factorization over the rational number field.

Key words Successive algebraic-extension field, symbolic computation, Wu-Zero decomposition, irreducible ascending chain, triangularization, resultant.