Pure Mathematics 理论数学, 2023, 13(7), 1959-1965
Published Online July 2023 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2023.137202

Hans汉斯

子结式的两个新性质的证明

刘　美*，孙维昆

天津职业技术师范大学理学院，天津

收稿日期：2023年6月6日；录用日期：2023年7月10日；发布日期：2023年7月17日

摘　要

利用已有的结式性质得到了单变元多项式子结式的两个新性质，证明了一种乘积的子结式与两个子结式的乘积的等量关系式，并且给出了两个子结式互素的充要条件。

关键词

子结式，互素，单变元多项式

The Proof of Two New Properties of Subresultants

Mei Liu*, Weikun Sun

School of Sciences, Tianjin University of Technology and Education, Tianjin

Received: Jun. 6th, 2023; accepted: Jul. 10th, 2023; published: Jul. 17th, 2023

Abstract

Using the existing properties of resultants, the authors get two new properties of subresultants of univariate polynomials, which show that an equal relationship between the subresultants of product and the product of two subresultants and give a necessary and sufficient condition for the two subresultants to be relatively prime.

Keywords

Subresultants, Coprime, Univariate Polynomials

*通讯作者。

文章引用: 刘美, 孙维昆. 子结式的两个新性质的证明[J]. 理论数学, 2023, 13(7): 1959-1965.
DOI: 10.12677/pm.2023.137202

1. 引言

子结式是由 Burside 和 Panton 在结式的基础上首先提出的概念，求两个单变元多项式的最大公因式是计算代数和几何中的基本问题，在科学和工程中有着广泛的应用。人们对子结式的基础理论和应用进行了广泛的研究，比如在文献[1]中作者给出了子结式的一种比经典子结式更简洁的定义，这为子结式的性质证明提供了更好的方法。在文献[2]中作者介绍了子结式的一些性质，利用约化多项式余式序列产生的一些结果来提供计算子结式的新算法。Hong 和杨静[3]将两个多项式的子结式推广到多个多项式的情形，给出了多个多项式子结式的构造方法，为求解多个多项式的最大公因式问题提供了新的理论依据和研究方向。王东明，夏壁灿，李子明[4]在第三章介绍了结式和子结式的一些性质，利用综合分析，反证法等方法进行了证明，并通过例题来说明结式的应用。

本文讨论多项式子结式的两个新性质。先给出[1]中的一个定理和命题，通过该定理和命题我们得出子结式的两个新性质，并通过例子加以说明，最后对这两个新性质进行详细的证明。

首先，我们给出结式和子结式的定义。

定义 1.1 设 K 是一个域，$F(x),G(x)\in K[x]$，

$$F(x)=a_0x^m+a_1x^{m-1}+\cdots+a_{m-1}x+a_m$$

$$G(x)=b_0x^n+b_1x^{n-1}+\cdots+b_{n-1}x+b_n$$

其中 $a_0,b_0\neq 0$，$m\geq n>0$，则称以下矩阵为 *Sylvester* 矩阵，记为 $Syl(F,G)$：

$$Syl(F,G)=\begin{pmatrix} a_0 & a_1 & \cdots & a_m & & \\ & a_0 & a_1 & \cdots & a_m & \\ & & \ddots & \ddots & & \ddots \\ & & & a_0 & a_1 & \cdots & a_m \\ b_0 & b_1 & \cdots & b_n & & \\ & b_0 & b_1 & \cdots & b_n & \\ & & \ddots & \ddots & & \ddots \\ & & & b_0 & b_1 & \cdots & b_n \end{pmatrix}\begin{matrix}\left.\begin{matrix}\\\\\\\end{matrix}\right\}n\\ \left.\begin{matrix}\\\\\\\end{matrix}\right\}m\end{matrix}$$

$Syl(F,G)$ 的行列式称为多项式 $F(x)$，$G(x)$ 的结式，记为 $res(F,G)$。

对 $Syl(F,G)$ 进行删除行和列的操作：删除 $Syl(F,G)$ 中 n 行 F 系数中的最后 j 行和 m 行 G 系数中的最后 j 行，然后删除 $Syl(F,G)$ 的最后 $2j+1$ 列，但保留第 $m+n-i-j$ 列，这样所得到的子矩阵记为 S_{ij}，这里 $0\leq i\leq j<n$。

定义 1.2 对 $0\leq j<n$，称多项式

$$subres_j(F,G)=\sum_{i=0}^{j}\det(S_{ij})x^i$$

为 F 和 G 关于 x 的第 j 个子结式。

2. 主要结论

先给出文献[1]中的一个定理和一个命题。

定理 2.1 设 $F(x)$ 和 $G(x)$ 是 $K[x]$ 上如定义 1.1 所示的单变元多项式，且 $m \geq n > 0$，则 F 和 G 关于 x 的第 j 个子结式

$$subres_j(x) = (-1)^{j(m-j+1)} \det\left(M_j(x)\right), 0 \leq j < n$$

其中 $M_j(x)$ 为 $(m+n-j)\times(m+n-j)$ 阶矩阵，

$$M_j(x) = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & \cdots & a_m & & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & a_0 & a_1 & a_2 & \cdots & \cdots & a_m \\ & & & & & 1 & -x & \\ & & & & & & \ddots & \ddots \\ & & & & & & & 1 & -x \\ b_0 & b_1 & b_2 & \cdots & \cdots & \cdots & b_n & & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & b_0 & b_1 & b_2 & \cdots & \cdots & \cdots & b_n \end{pmatrix} \begin{matrix} \left.\begin{matrix}\\\\\\\end{matrix}\right\} n-j \\ \left.\begin{matrix}\\\\\end{matrix}\right\} j \\ \left.\begin{matrix}\\\\\\\end{matrix}\right\} m-j \end{matrix}$$

，其中 $0 \leq j < n$。

命题 2.2 设 K 是一个域，$G(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n, (b_0 \neq 0)$ 是 $K[x]$ 上的单变元多项式，则对任意的 $m > n$，有

$$\det\left(M_n(x)\right) = (-1)^{mn} b_0^{m-n-1} G.$$

其中 $M_n(x) = \begin{pmatrix} & & & & & & 1 & -x & \\ & & & & & & & \ddots & \ddots \\ & & & & & & & & 1 & -x \\ b_0 & b_1 & b_2 & \cdots & \cdots & \cdots & b_n & & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & b_0 & b_1 & b_2 & \cdots & \cdots & \cdots & b_n \end{pmatrix} \begin{matrix} \left.\begin{matrix}\\\\\end{matrix}\right\} n \\ \left.\begin{matrix}\\\\\\\end{matrix}\right\} m-n \end{matrix}$

基于如上的定理 2.1 和命题 2.2，我们得到了以下两个结论。

定理 2.3 设 K 是一个域，$F(x), G(x), V(x)$ 是 $K[x]$ 上首项系数分别为 a_0, b_0, c_0 的单变元多项式，$a_0b_0c_0 \neq 0$，$\deg\left(F(x)\right) = m \geq 1$，$\deg\left(G(x)\right) = n \geq 1$，$\deg\left(V(x)\right) = t \geq 1$，且 m, n, t 满足 $m > n + t + 1$，则

$$subres_{n+t}(F, VG) = b_0^{-t} c_0^{-n} subres_n(F, G) subres_t(F, V)$$

定理 2.4 设 K 是一个域，$F(x)$ 和 $G(x)$ 是 $K[x]$ 上如定义 1.1 所示的单变元多项式，若 $m > n+1$，且存在 $0 \neq r \in K, s \in \mathbb{Z}_{\geq 2}$，使得 $H(x) = G(x) + rx^s F(x) \neq 0$。

则 $subres_m\left(H(x), F(x)\right)$ 与 $subres_n\left(F(x), G(x)\right)$ 互素的充要条件是 $F(x)$ 与 $G(x)$ 互素。

下面我们举例来加以说明定理 2.3 和定理 2.4：

例 2.5 设 K 是一个域，$F(x), G(x), V(x)$ 是 $K[x]$ 上首项系数分别为 a_0, b_0, c_0 的单变元多项式，$a_0b_0c_0 \neq 0$.

$$F(x) = a_0x^7 + a_1x^6 + a_2x^5 + a_3x^4 + a_4x^3 + a_5x^2 + a_6x + a_7$$

$$G(x) = b_0x^3 + b_1x^2 + b_2x + b_3$$

$$V(x) = c_0x^2 + c_1x + c_2$$

则由定理 2.1 和命题 2.2 知

$$subres_5\left(F,VG\right)=\left(b_0c_0\right)^{7-5-1}VG=b_0c_0VG$$

$$subres_3\left(F,G\right)=b_0^{7-3-1}G=b_0^3G$$

$$subres_2\left(F,V\right)=c_0^{7-2-1}V=c_0^4V$$

所以 $subres_5\left(F,VG\right)=b_0^{-2}c_0^{-3}subres_3\left(F,G\right)subres_2\left(F,V\right)$。

取 $r=1,s=2$，则 $H\left(x\right)=G\left(x\right)+x^2F\left(x\right)\neq 0$，且 $\deg\left(H\left(x\right)\right)=9$。

所以根据定理 2.1 和命题 2.2 知

$$subres_7\left(H\left(x\right),F\left(x\right)\right)=a_0^{9-7-1}F\left(x\right)=a_0F\left(x\right)$$

$$subres_3\left(F\left(x\right),G\left(x\right)\right)=b_0^{7-3-1}G\left(x\right)=b_0^3G\left(x\right)$$

所以 $subres_7\left(H\left(x\right),F\left(x\right)\right)$ 与 $subres_3\left(F\left(x\right),G\left(x\right)\right)$ 互素的充要条件是 $F\left(x\right)$ 与 $G\left(x\right)$ 互素。

定理 2.3 和定理 2.4 给出了子结式的两个比较重要的性质，定理 2.3 将一种乘积的子结式与两个子结式的乘积进行转化，它在一定程度上简化了子结式的计算，比如当我们遇到两个可分解的且次数比较高的多项式时，如果对其直接求子结式，涉及的计算量会很大，但采用定理 2.3 结论，我们对所求子结式转化成两个低次数的子结式的乘积，这样可以比较容易求出多项式的子结式，减少计算量。定理 2.4 给出两个子结式互素的充要条件，这使得对求解两个单变元多项式的最大公因式提供了更好的理论支撑和更加系统的算法。

3. 定理和命题的证明

李永彬[1]给出了子结式的一种新定义，利用矩阵初等变换以及行列式的性质证明了新定义的子结式与经典子结式定义的等价关系。下面命题 2.2 主要采用这种方法进行证明。关剑成，刘金旺[5]利用分析综合方法证明了交换环上一种乘积的结式等于结式的乘积以及结式为零的一个充分条件，因此对于定理 2.3 和定理 2.4 的证明，我们采取类似的方法。

命题 2.2 的证明。

证明：将 $\det\left(M_n\left(x\right)\right)$ 按第一列展开得

$$\det\left(M_n\left(x\right)\right)=\left(-1\right)^{1+n+1}b_0\begin{vmatrix} & & & 1 & -x & & \\ & & & & \ddots & \ddots & \\ & & & & & 1 & -x \\ b_0 & b_1 & \cdots & b_n & & & \\ & \ddots & \ddots & \ddots & \ddots & & \\ & & & b_0 & b_1 & \cdots & b_n \end{vmatrix}\begin{matrix}\\ \\ \\ \\ \\ \\ \end{matrix}\begin{matrix}\left.\begin{matrix}\\ \\ \end{matrix}\right\}n \\ \left.\begin{matrix}\\ \\ \\ \end{matrix}\right\}m-n-1\end{matrix}$$

由于 $\det\left(M_n\left(x\right)\right)$ 的余子式 $\begin{vmatrix} & & 1 & -x & & \\ & & & \ddots & \ddots & \\ & & & & 1 & -x \\ b_0 & b_1 & \cdots & b_n & & \\ & \ddots & \ddots & \ddots & \ddots & \\ & & b_0 & b_1 & \cdots & b_n \end{vmatrix}\begin{matrix}\left.\begin{matrix}\\ \\ \end{matrix}\right\}n \\ \left.\begin{matrix}\\ \\ \\ \end{matrix}\right\}m-n-2\end{matrix}$ 与 $\det\left(M_n\left(x\right)\right)$ 有相似的结构，因此对其余子式再按第一列展开得

$$\text{原式}=(-1)^{2(n+2)}b_0^2\begin{vmatrix} & & 1 & -x & & \\ & & & \ddots & \ddots & \\ & & & & 1 & -x \\ b_0 & b_1 & \cdots & b_n & & \\ & \ddots & \ddots & \ddots & \ddots & \\ & & b_0 & b_1 & \cdots & b_n \end{vmatrix}\begin{matrix}\}n\\ \\ \\ \}m-n-2\end{matrix}$$

依次对后面产生的余子式按同样的方法展开，我们得到

$$\begin{aligned}\det\left(M_n(x)\right)&=(-1)^{(m-n-1)(n+2)}b_0^{m-n-1}\begin{vmatrix} & & 1 & -x & & \\ & & & \ddots & \ddots & \\ & & & & 1 & -x \\ b_0 & b_1 & \cdots & \cdots & \cdots & b_n \end{vmatrix}\begin{matrix}\\ \\ \}n\end{matrix}\\ &=(-1)^{(m-n-1)(n+2)}b_0^{m-n-1}\left((-1)^{n+2}b_0(-x)^n+(-1)^{n+3}b_1(-x)^{n-1}+\cdots+(-1)^{2n+2}b_n\right)\\ &=(-1)^{mn}b_0^{m-n-1}\left(b_0x^n+b_1x^{n-1}+\cdots+b_n\right)\\ &=(-1)^{mn}b_0^{m-n-1}G\end{aligned}$$

定理 2.3 的证明。

证明：因为 $m>n+t+1$，所以结合定理 2.1 和命题 2.2 可以得到

$$subres_{n+t}\left(F,VG\right)=\left(b_0c_0\right)^{m-n-t-1}VG$$

$$subres_n\left(F,G\right)=b_0^{m-n-1}G$$

$$subres_t\left(F,V\right)=c_0^{m-t-1}V$$

所以 $b_0^{-t}subres_n\left(F,G\right)=b_0^{m-n-t-1}G$，$c_0^{-n}subres_t\left(F,V\right)=c_0^{m-n-t-1}V$。

从而

$$\begin{aligned}subres_{n+t}\left(F,VG\right)&=\left(b_0c_0\right)^{m-n-t-1}VG\\ &=b_0^{m-n-t-1}c_0^{m-n-t-1}VG\\ &=b_0^{-t}c_0^{-n}subres_n\left(F,G\right)subres_t\left(F,V\right)\end{aligned}$$

利用定理 2.3，当 $d_1>\sum_{i=2}^{n}d_i$ 时，我们有

$$\begin{aligned}subres_p\left(F_1,\prod_{i=2}^{n}F_i\right)&=subres_{p_1}\left(F_1,\prod_{i=2}^{n-1}F_i\right)subres_{k_n}\left(F_1,F_n\right)\\ &=subres_{p_2}\left(F_1,\prod_{i=2}^{n-2}F_i\right)subres_{k_{n-1}}\left(F_1,F_{n-1}\right)subres_{k_n}\left(F_1,F_n\right)\\ &=\cdots\\ &=\prod_{i=2}^{n}subres_{k_i}\left(F_1,F_i\right)\end{aligned}$$

其中 $p=\sum_{i=2}^{n}k_i$，$F_1,F_2,\cdots,F_n$ 是 $K[x]$ 上首项系数都为 1 的单变元多项式，$d_1,d_2,\cdots,d_n$ 分别为 $F_1,F_2,\cdots,F_n$ 的次数。

定理 2.4 的证明。

证明：充分性 由于 $\deg\left(H\left(x\right)\right)=s+m>m+1$，所以结合定理 2.1 和命题 2.2 得

$$subres_m\left(H\left(x\right),F\left(x\right)\right)=subres_m\left(G\left(x\right)+rx^sF\left(x\right),F\left(x\right)\right)=a_0^{s-1}F\left(x\right)$$

$$subres_n\left(F\left(x\right),G\left(x\right)\right)=b_0^{m-n-1}G\left(x\right)$$

因为 $F\left(x\right)$ 与 $G\left(x\right)$ 互素，所以存在 $u_1\left(x\right),v_1\left(x\right)\in K\left[x\right]$，使得

$$u_1\left(x\right)F\left(x\right)+v_1\left(x\right)G\left(x\right)=1$$

所以 $a_0^{s-1}b_0^{m-n-1}u_1\left(x\right)F\left(x\right)+a_0^{s-1}b_0^{m-n-1}v_1\left(x\right)G\left(x\right)=a_0^{s-1}b_0^{m-n-1}$。

把 $subres_m\left(H\left(x\right),F\left(x\right)\right)=a_0^{s-1}F\left(x\right)$，$subres_n\left(F\left(x\right),G\left(x\right)\right)=b_0^{m-n-1}G\left(x\right)$ 代入上式得

$$b_0^{m-n-1}u_1\left(x\right)subres_m\left(H\left(x\right),F\left(x\right)\right)+a_0^{s-1}v_1\left(x\right)subres_n\left(F\left(x\right),G\left(x\right)\right)=a_0^{s-1}b_0^{m-n-1}$$

从而 $\frac{u_1\left(x\right)}{a_0^{s-1}}subres_m\left(H\left(x\right),F\left(x\right)\right)+\frac{v_1\left(x\right)}{b_0^{m-n-1}}subres_n\left(F\left(x\right),G\left(x\right)\right)=1$。

所以 $subres_m\left(H\left(x\right),F\left(x\right)\right)$ 与 $subres_n\left(F\left(x\right),G\left(x\right)\right)$ 互素。

必要性 因为 $subres_m\left(H\left(x\right),F\left(x\right)\right)$ 与 $subres_n\left(F\left(x\right),G\left(x\right)\right)$ 互素，所以存在 $u\left(x\right),v\left(x\right)\in K\left[x\right]$，使得

$$u\left(x\right)\cdot subres_m\left(H\left(x\right),F\left(x\right)\right)+v\left(x\right)\cdot subres_n\left(F\left(x\right),G\left(x\right)\right)=1$$

由于 $\deg\left(H\left(x\right)\right)=s+m>m+1$，所以结合定理 2.1 和命题 2.2 得

$$subres_m\left(H\left(x\right),F\left(x\right)\right)=subres_m\left(G\left(x\right)+rx^sF\left(x\right),F\left(x\right)\right)=a_0^{s-1}F\left(x\right)$$

$$subres_n\left(F\left(x\right),G\left(x\right)\right)=b_0^{m-n-1}G\left(x\right)$$

从而 $a_0^{s-1}u\left(x\right)\cdot F\left(x\right)+b_0^{m-n-1}v\left(x\right)\cdot G\left(x\right)=1$。

所以 $F\left(x\right)$ 与 $G\left(x\right)$ 互素。

4. 总结与展望

对于子结式的性质目前还有大量的问题需要解决。当两个单变元多项式的次数满足合适的大小关系时，我们可以利用已有的结式的性质进一步得到子结式的新性质。文中证明了一种乘积的子结式与两个子结式的乘积的等量关系式以及两个子结式互素的充要条件。然而，定理 2.3 给出的等量关系式具有一定的局限性，比如把域改为环，我们不能保证在该环中某些元素是否存在逆元，这会导致结论不一定成立。定理 2.4 给出两个子结式的充要条件，由于子结式也是多项式，所以我们可以利用两个单变元多项式互素的充要条件[6]进一步得出结论。但是定理 2.4 的结论只是对于由多项式次数决定的子结式才成立，比如对于该定理中多项式 $H\left(x\right)$，$F\left(x\right)$ 的子结式必须是第 m 个子结式，m 就是 $F\left(x\right)$ 的次数，换成其它的子结式结论可能会不成立。对于两个多项式下的任意子结式，目前还没有好的方法讨论它们的互素条件。

基金项目

天津市教委科研计划项目(2020KJ115)。

参考文献

[1] Li, Y.-B. (2006) A New Approach for Constructing Subresultants. *Applied Mathematics and Computation*, **183**, 471-476. https://doi.org/10.1016/j.amc.2006.05.120

[2] Collins, G.E. (1967) Subresultants and Reduced Polynomial Remainder Sequences. *Journal of the ACM* (*JACM*), **14**, 128-142. https://doi.org/10.1145/321371.321381

[3] Hong, H. and Yang, J. (2021) Subresultant of Several Univariate Polynomials. arXivpreprintarXiv:2112.15370

[4] 王东明, 夏壁灿, 李子明. 计算机代数[M]. 第 2 版. 北京: 北京大学出版社, 2007: 38-53.

[5] 关剑成, 刘金旺. 交换环上多项式结式的性质[J]. 数学理论与应用, 2014, 34(2): 13-17.

[6] 北京大学数学系前代数小组. 高等代数[M]. 第 5 版. 北京: 高等教育出版社, 2019.