(4) $f(x)=\dfrac{x^n-1}{x-1}$, $g(x)=\dfrac{x^m-1}{x-1}$;

*12. 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\in K[x]$,
证明: $f(x)$ 的判别式

$$D(f)=(-1)^{\frac{n(n-1)}{2}}a_0^{-1}\operatorname{Res}(f,f').$$

*§4 吴消元法

上节学习的结式可以用来消去多项式方程组的变量, 反复施行求结式的运算, 最后得到一个字母个数最少的多项式, 求这个多项式的根, 并将其回代, 就能得到多项式方程组的解. 但是当方程个数较多时, 用结式消元的效率不高, 计算量大.

我国数学家吴文俊 (1919–) 为了研究几何定理的机器证明, 创立了数学机械化方法. 多元多项式组的消元法是其中的重要内容. 他提出的方法被称为吴消元法. 吴消元法为代数方程组的求解给出了完整的理论, 提供了有效的算法. 并且有广泛的应用. 在这里我们只能作一个简略的介绍.

设 K 是一个数域, 多元多项式的变量可以分成两组:

$$u_1,u_2,\cdots,u_s \text{ 与} x_1,x_2,\cdots,x_n.$$

其中 $u_1,u_2,\cdots,u_s$ 被看成参数 (相当于线性方程组的自由未知量), 为简单起见常常用一个字母 u 来表示. $x_1,x_2,\cdots,x_n$ 则是需求解的未知量, 以下称为变元. 由于机械化处理的需要, 这 n 个变元的下标代表了一个取定的序.

以下我们所说的多项式, 如果不特别指出, 总是指多元多项式环 $K[u_1,\cdots,u_s;x_1,\cdots,x_n]$ 中的元素. 而且所有的多项式组都只包含有限多个多项式.

回想线性方程组的情形, 具体求解线性方程组的有效方法是消元法. 其关键的步骤就是把方程组同解变形为阶梯形方程组. 吴消元法的基本思想也是如此. 如果能把原多项式方程组同解变形成如下的**阶梯形多项式方程组**

$$\begin{aligned}
&F_1(u;x_1,\cdots,x_{k_1})=0\\
&F_2(u;x_1,\cdots,x_{k_1},\cdots,x_{k_2})=0\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&F_r(u;x_1,\cdots,x_{k_1},\cdots,x_{k_2},\cdots,x_{k_r})=0
\end{aligned}$$

其中 $k_1<k_2<\cdots<k_r\le n$. 那么消元法的任务就告完成, 因为往后的事就是一元多项式的求根问题了. 在阶梯形多项式方程组里, 把 $x_{k_1},x_{k_2},\cdots,x_{k_r}$ 称

为主变元, 把 $x_1,\cdots,x_n$ 中不是主变元的变量作为自由未知量. 只要给出参数 u 以及自由未知量的一组值, 从第一个方程可以解出 x_{k_1}. 把 x_{k_1} 的解代入第 2 个方程, 又可解出 x_{k_2}. 如此继续下去就能得到所有可能的解. 因此我们的目标就是要把任意的多项式组变形成阶梯形多项式组. 在着手变形之前要作一些准备工作.

定义 4.1 设多项式

$$P(u,x_1,\cdots,x_n)=P(u_1,\cdots,u_s,x_1,\cdots,x_n)\in K[u;x_1,\cdots,x_n]. \tag{4.1}$$

把多项式 P 中实际出现的具有最大下标的变元 x_k 称为 P 的**主变元**. 主变元的下标 k 称为多项式 P 的**类** (*class*), 记为 $\mathrm{CLS}(P)$. 主变元最高次幂的系数称为多项式 P 的**初式** (*initial*), 记为 $\mathrm{I}(P)$.

例 4.1 设

$$P(u_1,u_2,u_3,x_1,x_2,x_3)=u_2u_3x_1^6+2u_1^2x_1x_2x_3^3-x_1x_2x_3^3-3u_3^2x_2^2x_3^2+1, \tag{4.2}$$

则 P 的主变元是 x_3, P 的类 $\mathrm{CLS}(P)=3$, P 关于主变元的幂 $\deg_{x_3}P=3$, P 的初式 $\mathrm{I}(P)=(2u_1^2-1)x_1x_2$. □

如果在多项式 P 中变元 $x_1,\cdots,x_n$ 不出现, 则 P 没有主变元, P 的类 $\mathrm{CLS}(P)=0$. 此外如果 P 的类 $\mathrm{CLS}(P)=k$, 那么一定有 $\mathrm{I}(P)\in K[u;x_1,\cdots,x_{k-1}]$, 即 $\mathrm{CLS}(\mathrm{I}(P))\le k-1$.

为了把多项式方程组约化成阶梯形方程组, 主要的手段就是利用多项式除法, 用得到的余式取代原来的多项式, 以达到降低方程次数的目的. 为了使得余式和商式仍然是多项式, 不出现有理分式, 有必要对一元多项式的带余除法加以变形, 称为**拟除法** (*pseudo-division*). 其思路类似于一元整数系数多项式的除法, 为了去除商式和余式中的分母所采取的变形. 我们先看一个这样的例子.

例 4.2 设 $F(x)=x^4+1$, $G(x)=2x^2+x+3$. 求它们相除的整系数余式.

我们有以下等式:

$$\begin{aligned}
2F(x)&=x^2G(x)+(-x^3-3x^2+2),\\
2(-x^3-3x^2+2)&=(-x)G(x)+(-5x^2+3x+4),\\
2(-5x^2+3x+4)&=(-5)G(x)+(11x+23).
\end{aligned}$$

因此

$$2^3F(x)=(2^2x^2-2x-5)G(x)+(11x+23).$$

注意这里 $G(x)$ 的初式 $\mathrm{I}(G)=2$, 上式可以改写为:

$$\mathrm{I}(G)^3F(x)=q(x)G(x)+R(x),$$

这里 $\deg R < \deg G$. 其实在等式的两边除以 2^3 后就得到了有理数域上的带余除法公式:

$$F(x) = \left(\frac{1}{2}x^2 - \frac{1}{4}x - \frac{5}{8}\right) G(x) + \left(\frac{11}{8}x + \frac{23}{8}\right). \qquad \square$$

命题 4.1 *设有两个多项式 $F, G \in K[u; x_1, \cdots, x_n]$. $\mathrm{CLS}(G) = k$. 则一定存在多项式 $q, R \in K[u; x_1, \cdots, x_n]$ 使得*

$$\mathrm{I}(G)^e \cdot F = q \cdot G + R$$

其中 e 是一个非负整数, $\deg_{x_k}(R) < \deg_{x_k}(G)$.

*这个过程称为***拟除法***, 并把余式 R 记为 $\mathrm{Rem}(F, G, x_k)$.* $\square$

我们不打算对命题 4.1 作严格的证明. 因为拟除法的基本思路与带余除法完全一样. 首先我们可以把 F 和 G 都看成变元 x_k 的一元多项式, 其系数是在多项式环 $K[u; x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n]$ 内取值的. 这时 G 可以表示成

$$G = \mathrm{I}(G)x_k^m + (x_k \text{ 的次数} < m \text{ 的项}).$$

然后使用例 4.2 所示的方法, 就可以得到所需的等式. 具体操作可参见下例.

例 4.3 设

$$F(x, y) = x^2y^3 - y,$$
$$G(x, y) = x^3y - 2.$$

求 F 关于 G 作拟除法的余式 $\mathrm{Rem}(F, G, y)$.

解: 我们把变元 x, y 看成 x_1, x_2. 则 G 的主变元是 y. 初式 $\mathrm{I}(G) = x^3$. 于是

$$(x^3)F = (x^2y^2)G + (2x^2y^2 - x^3y),$$
$$(x^3)(2x^2y^2 - x^3y) = (2x^2y)G + (-x^6y + 4x^2y),$$
$$(x^3)(-x^6y + 4x^2y) = (-x^6 + 4x^2)G + (-2x^6 + 8x^2).$$

经整理后得

$$(x^3)^3F = (x^8y^2 + 2x^5y - x^6 + 4x^2)G + (-2x^6 + 8x^2).$$

所以余式 $\mathrm{Rem}(F, G, y) = -2x^6 + 8x^2$. $\square$

现在我们要开始讨论多项式方程组的同解变形问题, 所以要引进零点集的概念. 其实解一个多项式方程组就是求出这个多项式组的零点集.

定义 4.2 设有 n 个变元的多项式

$$F, P_1, \cdots, P_t \in K[u_1, \cdots, u_s; x_1, \cdots, x_n]$$

以及多项式组 $\mathscr{P} \subset K[u_1, \cdots, u_s; x_1, \cdots, x_n]$. 定义它们的**零点集**为:

$$Z(F) \stackrel{\text{def}}{=} \{(a_1, \cdots, a_s, c_1, \cdots, c_n) \in \mathbb{C}^{s+n} | F(a_1, \cdots, a_s, c_1, \cdots, c_n) = 0\},$$

$$\begin{aligned} Z(P_1, \cdots, P_t) \stackrel{\text{def}}{=} \{&(a_1, \cdots, a_s, c_1, \cdots, c_n) \in \mathbb{C}^{s+n} \mid \\ &P_i(a_1, \cdots, a_s, c_1, \cdots, c_n) = 0,\ i = 1, \cdots, t\}, \end{aligned}$$

$$\begin{aligned} Z(\mathscr{P}) \stackrel{\text{def}}{=} \{&(a_1, \cdots, a_s, c_1, \cdots, c_n) \in \mathbb{C}^{s+n} \mid \\ &P(a_1, \cdots, a_s, c_1, \cdots, c_n) = 0,\ \forall P \in \mathscr{P}\}. \end{aligned}$$

注意我们的多项式的系数域可以是任意的数域 K, 但是它们的零点集却在 $\mathbb{C}^{s+n}$ 内考虑. 道理很简单: $x^2 + y^2 + 1$ 与 $2x^2 + 3y^2 = 1$ 在实数平面 $\mathbb{R}^2$ 内的零点集都是空集, 但在复数平面 $\mathbb{C}^2$ 内的零点集却是不相同的. 只有扩大到复数域才能把所有可能的零点都包含进去.

因此两个多项式 (方程) 组 $\mathscr{P}_1$ 与 $\mathscr{P}_2$ 是同解的当且仅当 $Z(\mathscr{P}_1) = Z(\mathscr{P}_2)$.

命题 4.2 设 F, G 是多项式, F 对于 G 未约化, F 被 G 除的余式为 R, 则 $Z(F, G) = Z(F, G, R)$. 此外, 如果初式 $\mathrm{I}(G)$ 在 $Z(G, R)$ 上处处不为零, 则 $Z(F, G) = Z(G, R)$.

证明: 由于 $R = \mathrm{I}(G)^e \cdot F - q \cdot G$, 所以 F, G 的公共零点也是 R 的零点, 即 $Z(F, G) \subseteq Z(F, G, R)$. 而反向的包含是显然的.

如果 $\mathrm{I}(G)$ 在 $Z(G, R)$ 上处处不为零, 由于

$$\mathrm{I}(G)^e \cdot F = q \cdot G + R$$

对于 $(a_1, \cdots, a_s, c_1, \cdots, c_n) \in Z(G, R)$ 有

$$\mathrm{I}(G)^e(a_1, \cdots, a_s, c_1, \cdots, c_n) \cdot F(a_1, \cdots, a_s, c_1, \cdots, c_n) = 0.$$

已知 $\mathrm{I}(G)$ 在 $Z(G, R)$ 上处处不为零, 迫使 $F(a_1, \cdots, a_s, c_1, \cdots, c_n) = 0$. 于是 $Z(G, R) \subseteq Z(F, G)$. 另一方面有 $Z(F, G) = Z(F, G, R) \subseteq Z(G, R)$. 所以 $Z(F, G) = Z(G, R)$. □

命题 4.2 告诉我们, 在一定条件下 (初式 $\mathrm{I}(G)$ 在 $Z(G, R)$ 上处处不为零), 方程组 $F = 0, G = 0$ 可以同解变形为 $G = 0, R = 0$, 也就是说, F 可以用它的余式 R 取代. 这正是解线性方程组的消元法所做的事.

现在我们要引进吴消元法中一个重要的概念——升列. 升列就是有解的阶梯形多项式组.

定义 4.3 设有多项式组 $\mathscr{A}=\{A_1,\cdots,A_r\}$. 如果它满足以下条件, 就被称为**升列** (*ascending set*):

$0<\mathrm{CLS}(A_1)<\mathrm{CLS}(A_2)<\cdots<\mathrm{CLS}(A_r)$. 即 $\mathscr{A}$ 是阶梯形多项式组.

评注 4.1 升列的原始定义中还包括一个已约化的条件, 为了简化, 我们这里略去了, 因为这并不影响求方程组的解.

如果多项式组含有数域 K 中的一个非零常数或者一个只含参数 u 不含变元的多项式, 这个多项式组的零点集是空集, 称为矛盾的. 而根据升列定义, 升列中的多项式的类均大于 0, 因而升列总是非矛盾的.

现在可以定义一个多项式对于一个升列的余式.

定义 4.4 设 $\mathscr{A}=\{A_1,\cdots,A_r\}$ 是一个升列, F 是一个多项式. 设 A_i 的主变元是 x_{k_i} $(i=1,\cdots,r)$. 令

$$\begin{aligned}&\mathrm{Rem}(F,A_r,x_{k_r})=R_r,\\&\mathrm{Rem}(R_r,A_{r-1},x_{k_{r-1}})=R_{r-1},\\&\cdots\cdots\cdots\cdots\cdots\cdots\\&\mathrm{Rem}(R_2,A_1,x_{k_1})=R_1.\end{aligned}$$

则称 R_1 是 F 对于升列 $\mathscr{A}$ 的**余式** (*remainder*), 记为 $\mathrm{Rem}(F,\mathscr{A})$.

引理 4.3 设 $\mathscr{A}=\{A_1,\cdots,A_r\}$ 是一个升列, F 是一个多项式. 令 $R=\mathrm{Rem}(F,\mathscr{A})$, $I_i=\mathrm{I}(A_i)$ $(i=1,\cdots,r)$ 是 A_i 的初式, 则存在多项式 $q_1,\cdots,q_r$ 使得

$$I_1^{e_1}I_2^{e_2}\cdots I_r^{e_r}F=\sum_{i=1}^{r}q_iA_i+R.$$

证明: 写出多项式 F 对升列 $\mathscr{A}$ 作拟除法的等式如下:

$$\begin{aligned}I_r^{e_r}F&=q_r'A_r+R_r\\I_{r-1}^{e_{r-1}}R_r&=q_{r-1}'A_{r-1}+R_{r-1}\\&\cdots\cdots\cdots\cdots\cdots\cdots\\I_1^{e_1}R_2&=q_1'A_1+R\end{aligned}$$

在上面等式组中逐次消去 $R_2,\cdots,R_r$, 令 $q_i=I_1^{e_1}\cdots I_{i-1}^{e_{i-1}}q_i'$, 就得到需证的等式. □

很容易把对升列求余式推广到一组多项式.

定义 4.5 设有一组多项式 $\mathscr{P}=\{P_1,\cdots,P_t\}$ 以及一个升列 $\mathscr{A}=\{A_1,\cdots,A_r\}$, 把每个多项式 P_i 对 $\mathscr{A}$ 的余式记为 $R_i=\mathrm{Rem}(P_i,\mathscr{A})$, $i=1,\cdots,t$. 则多项式组 $\mathscr{R}=\{R_1,\cdots,R_t\}$ 称为多项式组 $\mathscr{P}$ 对升列 $\mathscr{A}$ 的**余式组**, 记为 $\mathrm{Rem}(\mathscr{P},\mathscr{A})$.

如果余式组 $\mathrm{Rem}(\mathscr{P},\mathscr{A})$ 中只含零多项式, 就称此余式组为零, 记为 $\mathrm{Rem}(\mathscr{P},\mathscr{A})=0$.

命题 4.4 设有多项式组 $\mathscr{P}$ 以及升列 $\mathscr{A}$. 如果 $\mathrm{Rem}(\mathscr{P},\mathscr{A})=0$, 则

$$Z(\mathscr{A}/J)\subseteq Z(\mathscr{P}).$$

这里的 J 是升列中所有多项式的初式的乘积, $Z(\mathscr{A}/J)=Z(\mathscr{A})\setminus Z(J)$, 即零点集 $Z(\mathscr{A})$ 中使 $J\neq 0$ 的零点的集合.

证明: 设 $\mathscr{P}=\{P_1,\cdots,P_t\}$, $\mathscr{A}=\{A_1,\cdots,A_r\}$. 把升列 $\mathscr{A}$ 中各多项式的初式分别记为 $I_1,\cdots,I_r$, 则 $J=I_1I_2\cdots I_r$. 根据引理 4.3, 考虑到所有的余式都等于 0, 可得下列等式:

$$\begin{aligned}
I_1^{e_{11}}\cdots I_r^{e_{1r}}P_1&=\sum_{i=1}^{r}q_{1i}A_i\\
I_1^{e_{21}}\cdots I_r^{e_{2r}}P_2&=\sum_{i=1}^{r}q_{2i}A_i\\
&\cdots\cdots\cdots\cdots\cdots\\
I_1^{e_{t1}}\cdots I_r^{e_{tr}}P_t&=\sum_{i=1}^{r}q_{ti}A_i
\end{aligned}$$

如果让上面的等式组在 $Z(\mathscr{A}/J)$ 上取值, 立即可知这些点也是多项式 $P_1,\cdots,P_t$ 的零点. 即

$$Z(\mathscr{A}/J)\subseteq Z(\mathscr{P}).\qquad\square$$

定理 4.5 设有多项式组 $\mathscr{P}$ 以及满足

$$Z(\mathscr{P})\subseteq Z(\mathscr{A})$$

的升列 $\mathscr{A}=\{A_1,\cdots,A_r\}$, 并且 $\mathrm{Rem}(\mathscr{P},\mathscr{A})=0$. 则有

$$Z(\mathscr{P})=Z(\mathscr{A}/J)\bigcup_{i=1}^{r}Z(\mathscr{P},I_i)$$

其中 $I_i=\mathrm{I}(A_i)$ $(i=1,\cdots,r)$, $J=I_1I_2\cdots I_r$.

证明: 由于 $Z(\mathscr{P}/J)=Z(\mathscr{P})\setminus Z(J)=Z(\mathscr{P})\setminus Z(\mathscr{P},J)$, 因此

$$Z(\mathscr{P})=Z(\mathscr{P}/J)\cup Z(\mathscr{P},J).$$

由于 $J = I_1 \cdots I_r$, 所以 $Z(\mathscr{P}, J) = \bigcup_{i=1}^{r} Z(\mathscr{P}, I_i)$. 另一方面由已知条件 $Z(\mathscr{P}) \subseteq Z(\mathscr{A})$ 可以得到

$$Z(\mathscr{P}/J) \subseteq Z(\mathscr{A}/J).$$

又因 $\mathrm{Rem}(\mathscr{P}, \mathscr{A}) = 0$, 根据命题 4.4 有 $Z(\mathscr{A}/J) \subseteq Z(\mathscr{P})$. 因此

$$Z(\mathscr{A}/J) \subseteq Z(\mathscr{P}/J).$$

这样就证明了 $Z(\mathscr{A}/J) = Z(\mathscr{P}/J)$. □

定理 4.5 是吴消元法的核心定理之一. 根据这个定理, 对于任意给定的多项式方程组 $\mathscr{P}$, 只要能找到满足定理条件的升列, 就可把求 $\mathscr{P}$ 的解归结为求这个升列的解以及一些新的多项式方程组的解. 注意到升列就是阶梯形多项式组, 因此求升列的零点集被认为是已经解决的问题. 而那些新的多项式方程组又可以用同样的方法归结为升列的解. 因而我们把满足定理 4.5 的条件的升列称为特征列. 特征列是吴消元法中最重要的概念.

定义 4.6 对于任意一个多项式组 $\mathscr{P}$, 如果多项式组 $\mathscr{C}$ 满足下列条件, 就称为 $\mathscr{P}$ 的**特征列** (*characteristic set*):

(1) $\mathscr{C}$ 是一个升列;

(2) $Z(\mathscr{P}) \subseteq Z(\mathscr{C})$;

(3) $\mathrm{Rem}(\mathscr{P}, \mathscr{C}) = 0$.

接下去的问题就是特征列的存在性. 这也是吴消元法的关键之一. 由于严格的证明太繁, 我们只作一个不严格的说明.

首先证明一个引理.

引理 4.6 设有两个多项式组 $\mathscr{A} \subseteq \mathscr{P}$, 其中 $\mathscr{A}$ 是升列. 则

$$Z(\mathscr{P}) = Z(\mathscr{P}, \mathscr{R}).$$

其中 $\mathscr{R} = \mathrm{Rem}(\mathscr{P}, \mathscr{A})$.

证明: 根据命题 4.2, 有 $Z(\mathscr{P}, \mathscr{A}) = Z(\mathscr{P}, \mathscr{A}, \mathscr{R})$. 由 $\mathscr{A} \subseteq \mathscr{P}$ 可得

$$Z(\mathscr{P}) = Z(\mathscr{P}, \mathscr{A}) = Z(\mathscr{P}, \mathscr{A}, \mathscr{R}) \subseteq Z(\mathscr{P}, \mathscr{R}) \subseteq Z(\mathscr{P}).$$

所以 $Z(\mathscr{P}) = Z(\mathscr{P}, \mathscr{R})$. □

对于任意的多项式组 $\mathscr{P}$, 我们可以用下述方法构造一个满足 $\mathscr{B} \subseteq \mathscr{P}$ 的升列 $\mathscr{B}$, 并称之为 $\mathscr{P}$ 的**基列** (*basic set*): 首先在 $\mathscr{P}$ 中选取一个类最小且在同类多项式中关于主变元的幂也是最小的多项式 (在不唯一时任取其中之一, 下同), 记为 B_1. 如果 $\mathrm{CLS}(B_1) = 0$, 则多项式组 $\mathscr{P}$ 是矛盾的, 基列不存在. 记为

$\mathscr{B}=\emptyset$. 现在假定已经选取了多项式 $B_1,\cdots,B_i$, 把 $\mathscr{P}$ 中的类 $>\mathrm{CLS}(B_i)$ 的多项式构成的子集记为 $\mathscr{Q}_i$, 再在 $\mathscr{Q}_i$ 中选取一个类最小且在同类多项式中关于主变元的幂也是最小的多项式作为 B_{i+1}. 显然经有限步后必有 $\mathscr{Q}_r=\emptyset$. 则多项式组 $\mathscr{B}=\{B_1,\cdots,B_r\}$ 就定义为 $\mathscr{P}$ 的基列. 如果令 $\mathscr{R}=\mathrm{Rem}(\mathscr{P},\mathscr{B})$, 根据引理 4.6, 一定有

$$Z(\mathscr{P})=Z(\mathscr{P},\mathscr{R}).$$

现在我们可以用下述递归方法构造任意多项式组 $\mathscr{P}$ 的特征列. 令 $\mathscr{P}_1=\mathscr{P}$, 记 $\mathscr{P}_1$ 的基列为 $\mathscr{B}_1$. 如果基列不存在, 则 $\mathscr{P}_1$ 是矛盾的多项式组, 过程中断. 否则, 取余式组 $\mathscr{R}_1=\mathrm{Rem}(\mathscr{P}_1,\mathscr{B}_1)$.

令 $\mathscr{P}_2=\mathscr{B}_1\cup\mathscr{R}_1$. 注意

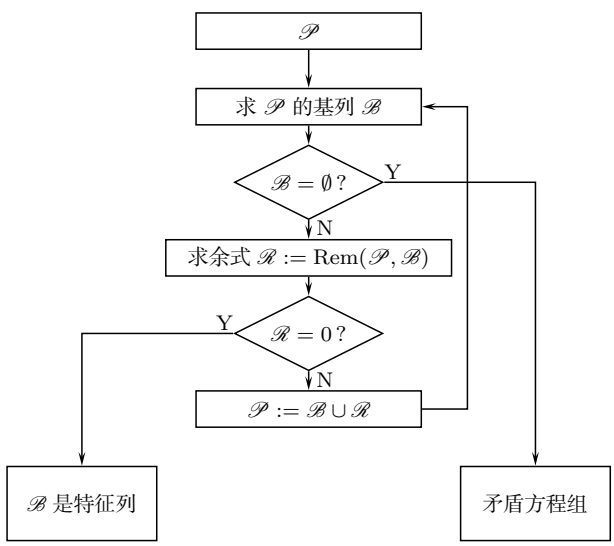
$$Z(\mathscr{P})=Z(\mathscr{P}_1)=Z(\mathscr{P}_1,\mathscr{R}_1)\subseteq Z(\mathscr{B}_1,\mathscr{R}_1)=Z(\mathscr{P}_2).$$

同样地取 $\mathscr{P}_2$ 的基列 $\mathscr{B}_2$ 以及余式组 $\mathscr{R}_2=\mathrm{Rem}(\mathscr{P}_2,\mathscr{B}_2)$. 如此继续下去, 直至以下两种情况之一出现, 使过程中断:

(a) $\mathscr{B}_t=\emptyset$, 也就是说 $\mathscr{P}_t$ 里有不含变元的多项式 (即 $\mathrm{CLS}=0$ 的多项式), 说明 $\mathscr{P}_t$ 是矛盾的, 从而 $Z(\mathscr{P})\subseteq\cdots\subseteq Z(\mathscr{P}_t)=\emptyset$, 原多项式组也是矛盾的;

(b) $\mathscr{R}_t=0$. 这时基列 $\mathscr{B}_t$ 是升列, 并且 $Z(\mathscr{B}_t)\supseteq Z(\mathscr{P}_t)\supseteq\cdots\supseteq Z(\mathscr{P})$. 说明 $\mathscr{B}_t$ 满足特征列定义 4.6 的前两个条件. 至于第三个条件则需要进一步的论证才能验证, 这里略去了. 总之, $\mathscr{B}_t$ 是 $\mathscr{P}$ 的特征列.

上述过程可以归结成以下流程图:



当然这里的关键是证明这个过程经有限步后一定会遇到上述两个情况之

一. 这就需要给基列定义一个序"$\prec$", 证明 $\mathscr{B}_{i+1} \prec \mathscr{B}_i$, 并且下降过程不可能是无限的. 这些细节已超出本书的范围. 最终得到的定理是

定理 4.7 *对于任意的多项式组 $\mathscr{P}$, 存在一个机械化的算法, 经过有限多步运算后或能求出 $\mathscr{P}$ 的一个特征列, 或能判定 $\mathscr{P}$ 是矛盾的.* □

由于基列的选取不是唯一的, 因此特征列也不是唯一的. 此外, 特征列当然与变元的排序有关. 变元的次序的变化会给求解工作量带来很大的影响.

总结前面的讨论, 可以把吴消元法归结成以下定理:

定理 4.8 *对于任意的多项式组 $\mathscr{P}$, 存在一个机械化的算法, 经过有限多步运算后或能判定 $\mathscr{P}$ 是矛盾的, 或能将其零点集分解成特征列的零点集之并:*

$$Z(\mathscr{P}) = \bigcup_k Z(\mathscr{C}_k/J_k),$$

其中 J_k 是特征列 $\mathscr{C}_k$ 中各多项式的初式的乘积, 指标 k 的集合是有限的.

证明: 根据定理 4.7, 在 $\mathscr{P}$ 不是矛盾多项式组的前提下, 可以得到一个特征列 $\mathscr{C}$. 根据定理 4.5, 有分解

$$Z(\mathscr{P}) = Z(\mathscr{C}/J)\bigcup_i Z(\mathscr{P}, I_i)$$

其中指标 i 的集合有限, I_i 是 $\mathscr{C}$ 中各多项式的初式, J 是这些 I_i 的乘积. 对于多项式组 $\mathscr{P} \cup \{I_i\}$ 又可用同样的方法得到其特征列或判定其为矛盾的. 这样又可得到零点集 $Z(\mathscr{P}, I_i)$ 的类似分解. 如此反复进行下去, 只要能证明这个过程经过有限多步后必定终止, 定理得证. 由于篇幅所限, 这个关键的证明只能略去. □

这样我们用不太大的篇幅就完成了吴消元法的介绍. 读者会发现好几处关键论证都给略去了. 确实如此, 吴消元法的思想是很清楚的, 不需要太复杂的讲解就能理解. 但是在这简洁的介绍背后隐藏着复杂的严格证明.

评注 4.2 与特征列概念类似的有格罗布讷 (Gröbner) 基理论, 在计算代数、计算代数几何、计算数论等诸多领域里起着重要的作用. 现有的符号计算软件中一般使用格罗布讷基求解多元多项式方程组. 其思路与吴消元法类似, 不过已经超出本书的范围.

例 4.4 解多项式方程组:

$$\begin{cases} x^2 - 2xz + 1 = 0 \\ xy + z^2 = 0 \\ 3y^2 - 2z^2 = 0. \end{cases}$$

解: 为了演示吴消元法的流程, 我们采用分步计算的方式, 并把逐次使用的命令列出 (读者应先阅读本节末尾的上机实验). 下面分别使用 Maple 或 Mathematica 计算本题.

用 Maple 求解:

```
>read ‘c:/maple/share/wsolve2‘;
>P1:=x^2-2*x*z+1; P2:=x*y+z^2; P3:=3*y^2-2*z^2;
>PS1:={P1,P2,P3};
>ord:=[z,y,x];
```

现在我们完成了输入已知数据的工作. `PS1` 相当于 $\mathscr{P}_1 = \mathscr{P}$.

(1) 求基列 $\mathscr{B}_1$:

```
>B1:=basset(PS1,ord);
```

得到的结果是:

$$\mathscr{B}_1 = \{x^2 - 2xz + 1\}.$$

求余式组 $\mathscr{R}_1 = \mathrm{Rem}(\mathscr{P}_1, \mathscr{B}_1)$:

```
>R1:=remseta(PS1,B1,ord);
```

得到的结果是:

$$\mathscr{R}_1 = \{4x^3y + x^4 + 2x^2 + 1, -6x^2y^2 + x^4 + 2x^2 + 1\}.$$

(2) 生成 $\mathscr{P}_2 = \mathscr{B}_1 \cup \mathscr{R}_1$:

```
>PS2:={op(B1)} union R1;
```

说明: 因为 `B1` 是顺序表 (两边用方括号括起来的), `R1` 则是一个集合 (两边用花括号括起来的), 为了做集合的并 (运算符是 `union`), 要先把 `B1` 转换成集合, 所以在上面的命令中要使用 `{op(B1)}`, 不能直接用 `B1`.

求基列 $\mathscr{B}_2$:

```
>B2:=basset(PS2,ord);
```

得到的结果是:

$$\mathscr{B}_2 = \{x^2 - 2xz + 1, 4x^3y + x^4 + 2x^2 + 1\}.$$

求余式组 $\mathscr{R}_2 = \mathrm{Rem}(\mathscr{P}_2, \mathscr{B}_2)$:

```
>R2:=remseta(PS2,B2,ord);
```

得到的结果是:

$$\mathscr{R}_2 = \{5x^8 + 4x^6 - 10x^4 - 12x^2 - 3\}.$$

(3) 生成 $\mathscr{P}_3 = \mathscr{B}_2 \cup \mathscr{R}_2$:

```
>PS3:={op(B2)} union R2;
```

求基列 $\mathscr{B}_3$:

```
>B3:=basset(PS3,ord);
```

得到的结果是:

$$\mathscr{B}_3=\{x^2-2xz+1,4x^3y+x^4+2x^2+1,5x^8+4x^6-10x^4-12x^2-3\}.$$

求余式组 $\mathscr{R}_3=\mathrm{Rem}(\mathscr{P}_3,\mathscr{B}_3)$:

```
>R3:=remseta(PS3,B3,ord);
```

得到的结果是:

$$\mathscr{R}_3=0.$$

因此 $\mathscr{B}_3$ 就是特征列. 我们求它的初式的乘积:

```
>J:=Initial(B3[1],ord)*Initial(B3[2],ord)
*Initial(B3[3],ord);
```

结果是 $J=x^4$. 这表明

$$Z(\mathscr{P})=Z(\mathscr{B}_3/x)\cup Z(\mathscr{P},x).$$

先求 $Z(\mathscr{B}_3/x)$:

```
>solveas(B3,ord,{x});
```

得到的解是:

$$\begin{cases}x=-\mathrm{i}\\ y=0\\ z=0\end{cases}\qquad\begin{cases}x=\mathrm{i}\\ y=0\\ z=0\end{cases}$$

$$\begin{cases}x=\dfrac{\sqrt{15+10\sqrt{6}}}{5}\\ y=-\dfrac{2(11+4\sqrt{6})}{(3+2\sqrt{6})\sqrt{15+10\sqrt{6}}}\\ z=\dfrac{4+\sqrt{6}}{\sqrt{15+10\sqrt{6}}}\end{cases}\qquad\begin{cases}x=\dfrac{1}{5}\mathrm{i}\sqrt{-15+10\sqrt{6}}\\ y=\dfrac{2\mathrm{i}(-11+4\sqrt{6})}{(-3+2\sqrt{6})\sqrt{-15+10\sqrt{6}}}\\ z=\dfrac{(-4+\sqrt{6})\mathrm{i}}{\sqrt{-15+10\sqrt{6}}}\end{cases}$$

$$\begin{cases}x=-\dfrac{1}{5}\mathrm{i}\sqrt{-15+10\sqrt{6}}\\ y=\dfrac{-2\mathrm{i}(-11+4\sqrt{6})}{(-3+2\sqrt{6})\sqrt{-15+10\sqrt{6}}}\\ z=\dfrac{-\mathrm{i}(-4+\sqrt{6})}{\sqrt{-15+10\sqrt{6}}}\end{cases}\qquad\begin{cases}x=-\dfrac{\sqrt{15+10\sqrt{6}}}{5}\\ y=\dfrac{2(11+4\sqrt{6})}{(3+2\sqrt{6})\sqrt{15+10\sqrt{6}}}\\ z=-\dfrac{4+\sqrt{6}}{\sqrt{15+10\sqrt{6}}}\end{cases}$$

如果我们用 wsolve 直接构造特征列

```
>CS:=wsolve(PS1,ord);
```

可得到两个特征列: $\{x^2-2xz+1, 5x^3y+4x^2+2, 5x^4-6x^2-3\}$ 及 $\{z, y, x^2+1\}$. 这是由于函数包 wslove 采用了一些优化算法, 对于可以分解的多项式作了因式分解, 降低多项式组的次数, 以减少计算量. 最后用 `solveas(CS,ord,{});` 求根, 得到与前面一样的结果. 同理, 用

```
>wsolve_s(PS1,ord,{});
```

也可得到同样的解.

剩下的是求 $Z(\mathscr{P}, x)$. 先构造 $\mathscr{P}_{11}=\mathscr{P}\cup\{x\}$, 再计算基列及余式列:

```
>PS11:=PS1 union {x};
>B11:=basset(PS11,ord);
>R11:=remseta(PS11,B11,ord);
```

得到基列 $\mathscr{B}_{11}=\{x, 3y^2-2z^2\}$, 余式列 $\mathscr{R}_{11}=\{1\}$. 因此这是矛盾多项式组.

用 Mathematica 求解:

```
p1=x^2-2x z+1; p2=x y+z^2; p3=3y^2-2z^2;
ps1={p1,p2,p3}
ord={x,y,z}
```

现在我们完成了输入已知数据的工作. PS1 相当于 $\mathscr{P}_1=\mathscr{P}$.

(1) 求基列 $\mathscr{B}_1$:

```
b1=BasicSet[ps1,ord]
```

得到的结果是:

$$\mathscr{B}_1=\{x^2-2xz+1\}.$$

求余式组 $\mathscr{R}_1=\mathrm{Rem}(\mathscr{P}_1, \mathscr{B}_1)$:

```
r1=Complement[PseudoRemainderSet[ps1,b1,ord],{0}]
```

由于使用函数 PseudoRemainderSet 求出的余式组里可能含有零多项式, 如果不删除这些零多项式会引起以后计算的困难, 因此我们使用求集合补的命令 Complement 去除其中的零多项式. 得到的结果是:

$$\mathscr{R}_1=\{4x^3y+x^4+2x^2+1, -6x^2y^2+x^4+2x^2+1\}.$$

(2) 生成 $\mathscr{P}_2=\mathscr{B}_1\cup\mathscr{R}_1$:

```
ps2=Union[b1,r1]
```

求基列 $\mathscr{B}_2$:

```
b2=BasicSet[ps2,ord]
```

得到的结果是:

$$\mathscr{B}_2 = \{x^2 - 2xz + 1, 4x^3y + x^4 + 2x^2 + 1\}.$$

求余式组 $\mathscr{R}_2 = \mathrm{Rem}(\mathscr{P}_2, \mathscr{B}_2)$:

```
r2=Complement[PseudoRemainderSet[ps2,b2,ord],{0}]
```

得到的结果是:

$$\mathscr{R}_2 = \{5x^8 + 4x^6 - 10x^4 - 12x^2 - 3\}.$$

(3) 生成 $\mathscr{P}_3 = \mathscr{B}_2 \cup \mathscr{R}_2$:

```
ps3=Union[b2,r2]
```

求基列 $\mathscr{B}_3$:

```
b3=BasicSet[ps3,ord]
```

得到的结果是:

$$\mathscr{B}_3 = \{x^2 - 2xz + 1, 4x^3y + x^4 + 2x^2 + 1, 5x^8 + 4x^6 - 10x^4 - 12x^2 - 3\}.$$

求余式组 $\mathscr{R}_3 = \mathrm{Rem}(\mathscr{P}_3, \mathscr{B}_3)$:

```
r3=Complement[PseudoRemainderSet[ps3,b3,ord],{0}]
```

得到的结果是:

$$\mathscr{R}_3 = 0.$$

因此 $\mathscr{B}_3$ 就是特征列. 我们求它的初式的乘积:

```
j=Initial[b3[[1]],ord]*Initial[b3[[2]],ord]
*Initial[b3[[3]],ord]
```

结果是 $J = 40x^4$. 这表明

$$Z(\mathscr{P}) = Z(\mathscr{B}_3/x) \cup Z(\mathscr{P}, x).$$

先求 $Z(\mathscr{B}_3/x)$:

```
WuRittEqnsSolve[b3,ord]
```

得到的解是:

$$\begin{cases} x = -\mathrm{i} \\ y = 0 \\ z = 0 \end{cases} \qquad \begin{cases} x = \mathrm{i} \\ y = 0 \\ z = 0 \end{cases}$$

$$\begin{cases} x=\sqrt{\dfrac{3}{5}+\dfrac{2\sqrt{6}}{5}} \\ y=-\dfrac{2(11+4\sqrt{6})}{\sqrt{5}(3+2\sqrt{6})^{3/2}} \\ z=\dfrac{4+\sqrt{6}}{\sqrt{5(3+2\sqrt{6})}} \end{cases} \qquad \begin{cases} x=\mathrm{i}\sqrt{\dfrac{1}{5}(-3+2\sqrt{6})} \\ y=\dfrac{2\mathrm{i}(-11+4\sqrt{6})}{\sqrt{5}(-3+2\sqrt{6})^{3/2}} \\ z=\dfrac{\mathrm{i}(-4+\sqrt{6})}{\sqrt{5(-3+2\sqrt{6})}} \end{cases}$$

$$\begin{cases} x=-\mathrm{i}\sqrt{\dfrac{1}{5}(-3+2\sqrt{6})} \\ y=-\dfrac{2\mathrm{i}(-11+4\sqrt{6})}{\sqrt{5}(-3+2\sqrt{6})^{3/2}} \\ z=-\dfrac{\mathrm{i}(-4+\sqrt{6})}{\sqrt{5(-3+2\sqrt{6})}} \end{cases} \qquad \begin{cases} x=-\sqrt{\dfrac{3}{5}+\dfrac{2\sqrt{6}}{5}} \\ y=\dfrac{2(11+4\sqrt{6})}{\sqrt{5}(3+2\sqrt{6})^{3/2}} \\ z=-\dfrac{4+\sqrt{6}}{\sqrt{5(3+2\sqrt{6})}} \end{cases}$$

如果我们用 `CharacteristicSet` 直接构造特征列

```
cs=CharacteristicSet[ps1,ord]
```

可得到特征列: $\{x^2-2xz+1, x^4+4x^3y+2x^2+1, -5x^8-4x^6+10x^4+12x^2+3\}$. 同理, 用

```
WuRittEqnsSolve[cs,ord]
```

也可得到同样的解. 类似地. 用

```
WuRittEqnsSolve[CharacteristicSet[ps1, ord], ord]
```

可以从方程组 $\mathscr{P}_1$ 直接求出所有的解.

剩下的是求 $Z(\mathscr{P},x)$. 先构造 $\mathscr{P}_{11}=\mathscr{P}\cup\{x\}$, 再计算基列及余式列:

```
ps11=Union[ps1,{x}]
b11=BasicSet[ps11,ord]
r11=Complement[PseudoRemainderSet[ps11,b11,ord],{0}]
```

得到基列 $\mathscr{B}_{11}=\{x, 3y^2-2z^2\}$, 由于余式列中含有 1, 因此这是矛盾多项式组. □

上机实验 中国科学院系统科学研究所数学机械化研究中心的王定康博士开发了在 Maple 环境下运行的函数包 wsolve, 这个函数包的任务就是实现吴消元法. 我们在这里将介绍它的主要功能. 不过为了适合我们的教材, 本书作者做了一点修改, 新版本命名为 wsolve2, 以示区别.

读者可用: `http://wims.math.ecnu.edu.cn/gj/wsolve2` 下载文件 wsolve2, 或到华东师范大学数学系主页 `http://www.math.ecnu.edu.cn` 去查看有关信息. 假设这个文件被存放在子目录 `c:\maple\share` 内. 为了使用 wsolve, 首先要执行下面的命令以把这个库载入内存 (注意路径中的反斜杠"\"要用斜杠"/"代替):

```
>read ‘c:/maple/share/wsolve2‘;
```

作为例子, 先输入例 4.1 的多项式:

```
>P:=u2*u3*x1^6+2*u1^2*x1*x2*x3^3-x1*x2*x3^3-3*u3^2*x2^2*x3^2+1;
```

然后输入变元的顺序. 注意这个函数包定义的变元顺序与课文中定义的顺序相反. 例如课文中定义的顺序是 x_1, x_2, x_3, 那么应该按 `x3, x2, x1` 的顺序输入:

```
>ord:=[x3,x2,x1];
```

求多项式的类 $\mathrm{CLS}(P)$ 使用以下命令:

```
>Class(P,ord);
```

求多项式的主变元使用以下命令:

```
>Mainvar(P,ord);
```

求多项式的初式 $\mathrm{I}(P)$ 使用以下命令:

```
>Initial(P,ord);
```

再输入例 4.4 的多项式:

```
>F:=x^2*y^3-y;
>G:=x^3*y-2;
```

求 F 对于 G 作拟除法的余式 $\mathrm{Rem}(F, G, y)$ 可使用以下命令:

```
>R:=NPrem(F,G,y);
```

注意这里求得的结果是 $8-2x^4$, 与我们在例 4.4 算得的结果 $8x^2-2x^6$ 不同, 这是因为 wsolve 对算法作了优化, 消去了 $\mathrm{I}(G)^s = x^9$ 与余式 R 的最大公因子 x^2.

求多项式 `F` 对升列 `as` 的余式可使用以下命令:

```
>Premas(F,as,ord);
```

如:

```
>as:=[x3^2+2*x3*x2,x2^2+x1*x2,x1^2+u];
>F:=x1^5+x1^2*x3^2+x2^3*x3+x3^4+u*x2;
>ord:=[x3,x2,x1];
>Premas(F,as,ord);
```

下面 3 条命令是用来验证刚才得到的结果的:

```
>r1:=NPrem(F,as[1],ord[1]);
>r2:=NPrem(r1,as[2],ord[2]);
>r3:=NPrem(r2,as[3],ord[3]);
```

求多项式组 `ps` 对升列 `as` 的余式组可使用以下命令:

```
>remseta(ps,as,ord);
```

如果 `as, F, ord` 保持刚才输入的值. 再执行以下命令:

```
>ps:=[F,as[3]*x1,as[2]*x2];
>remseta(ps,as,ord);
```

结果得到一个多项式, 因为另两个都是 0. 如果把 `ps` 中的第 2 项改成 `as[3]*x1+u`, 得到的结果是 {1}, 说明余式组是矛盾的. 如果把 `ps` 中的 `F` 删去, 就得到空集 { }, 说明 $\mathrm{Rem}(\mathrm{ps}, \mathrm{as}) = 0$.

求多项式组 `ps` 的基列可使用以下命令:

```
basset(ps,ord);
```

有了上面介绍的命令, 已经足以从已知的多项式组求出相应的特征列. 这个函数包也提供了直接求特征列的命令:

```
wsolve(ps,ord,nonzero);
```

其中参数 ord, nonzero 都是可选的. 当使用命令 wsolve(ps); 时, 程序自己确定一个变元的顺序. 参数 nonzero 要求给出一个多项式集例如 {x}, 这个集合中的多项式应该在计算过程中取非零的值. 当这个参数不给出时, 就被假设取空集. 这个程序一开始就检查其中的多项式能否作因式分解, 如能分解, 就把原多项式组分解成几个多项式组, 然后分别求特征列. 分解后的多项式组降低了次数, 减少了计算量. 每遇到一个多项式组, 就会在屏幕上显示 A New Component. 所以这句话出现几次, 就有几个特征列.

如果想从特征列 (或升列) 求出具体的解, 可使用命令:

```
solveas(as,ord); 或solveas(as,ord,nonzero);
```

其中 as 是一个升列. nonzero 是多项式的集合 (即用花括号括起来的几个多项式). 如果 nonzero 给出的多项式集合是 N, as 给出的升列是 $\mathscr{A}$, 则前一条不含 nonzero 参数的命令得出的解集是 $Z(\mathscr{A})$, 后一条命令得出的解集是 $Z(\mathscr{A}/N)$. 另一个命令:

```
wsolve_s((ps,ord,nonzero);
```

的作用就是把上述两条命令 wsolve 及 solveas 一起执行. 一下子求出多项式组 ps 的解 $Z(\mathscr{P}/N)$. 这里的 N 就是参数 nonzero 所指出的多项式集. 与 wsolve 以及 solveas 不同, 这个参数必须给出, 否则要出错. 一般可取空集 {}. 不过要注意, 以上所谓的解都是指 $Z(\mathscr{C}/J)$ (参见定理 4.5), 如要求 $Z(\mathscr{P}, I_i)$ 的解还需继续进行.

最后再介绍一个通过对多项式的因式分解把一个多项式组分解成多个多项式组的命令:

```
Nrs(rs,ord,nonzero);
```

其中 rs 给出了一个多项式组, nonzero 可以取成 {}.

较复杂的多项式组很可能会耗尽计算机的资源而无法用全自动的方法如 wsolve 或 wsolve_s 求解. 这时只好尝试用人机对话的交互方式, 根据中间结果, 不断人工干预, 调整策略. 所以我们介绍上列命令, 可供分步执行之用.

Maple 也有一个利用格罗布讷基求解多项式方程组的函数 Solve, 由于这个函数包含在包 Groebner 之内, 因此其调用命令是:

```
Groebner[Solve](ps,var,nonzero);
```

也可以先使用命令 with(Groebner): 把整个函数包载入内存, 以后就可以用

```
Solve(ps,var,nonzero);
```

调用此函数. 其中参数 ps 和 nonzero 的含义同 wsolve. 参数 nonzero 可以不出现. var 给出欲求解的变量的集合. 执行结果得到一个或几个特征列. 以例 4.4 为例, 用以下命令输入数据:

```
>ps:={x^2-2*x*z+1,x*y+z^2,3*y^2-2*z^2};
>var:=[x,y,z];
```

再执行命令

```
>cs:=Groebner[Solve](ps,var);
```

生成如下 2 个特征列:

```
cs:={[[z,y,x^2+1], plex(x,y,z), {}], [[-4-12*z^2+15*z^4,5*z^3+4*y-2*z,
8*x-15*z^3+6*z], plex(x,y,z), {z}]}
```

每个特征列 (以第一个 cs[1] 为例) 包含 3 个部分, 第一部分 cs[1][1] 是由 3 个多项式构成的特征列. 第二部分 cs[1][2] 表示消元过程中变元的顺序, 与课文中定义的顺序相同, 但与 wsolve 中 ord 的定义相反. 使用命令 op(cs[1][2]) 可以得到其中的变量集合 x,y,z. 第三部分 cs[1][3] 就是参数 nonzero. 为了求解这些特征列, 可以使用以下命令:

```
>solve(cs[1][1],{op(cs[1][2])});
```

读者会发现这样得到的解不易看懂, 因此不妨使用以下命令得到更明显的表达式:

```
>allvalues(solve(cs[1][1],{op(cs[1][2])}));
```

第二个特征列的解也可用以下命令得到:

```
>allvalues(solve(cs[2][1],{op(cs[2][2])}));
```

如果读者使用的是比较旧的 Maple 版本, 那么 Groebner 包里的函数 `Solve` 要改名为 `gsolve`. 此外, solve 函数不接受 `cs[1][1]` 作为变量, 而要改为 `{op(cs[1][1])}`, 也就是改用以下形式的命令:

```
>cs:=Groebner[gsolve](ps,var);
>solve({op(cs[1][1])},{op(cs[1][2])});
>allvalues(solve({op(cs[1][1])},{op(cs[1][2])}));
```

天津工业大学的刘华山同学参考 wsolve 创作了 Mathematica 里的函数包 WuRittSolva. 感谢他提供给大家自由使用. 读者可用:

```
http://wims.math.ecnu.edu.cn/gj/HowtoInstallWuRittSolva.pdf
```

以及

```
http://wims.math.ecnu.edu.cn/gj/WRS_Setup.rar
```

去下载 2 个文件, 或到华东师范大学数学系主页 `http://www.math.ecnu.edu.cn` 去查看有关信息. 其中 HowtoInstallWuRittSolva.pdf 是安装说明, 简而言之, 就是先安装好一个 Mathematica, 然后执行从 WRS_Setup.rar 解压得到的 setup.exe, 按照它的提示执行, 安装在此程序选取的默认目录 (Mathematica 下面的子目录 `AddOns\Autoload`) 里就可以了.

作为例子, 先输入例 4.1 的多项式:

```
p=u2 u3 x1^6+2u1^2 x1 x2 x3^3-x1 x2 x3^3-3u3^2 x2^2 x3^2+1
```

然后输入变元的顺序:

```
ord={x1,x2,x3}
```

求多项式的主变元使用以下命令:

```
MainVariable[p,ord]
```

求多项式的初式 I(P) 使用以下命令:

```
Initial[p,ord]
```

再输入例 4.4 的多项式:

```
f=x^2 y^3-y
g=x^3 y-2
```

求 f 对于 g 作拟除法的余式 Rem(f, g, y) 可使用以下命令:

```
r=PseudoRemainder[f,g,y]
```

求多项式 `f` 对升列 `as` 的余式可使用以下命令:

```
AuxPseudoRemainder[f,as,ord]
```

如:

```
as={x3^2+2x3 x2,x2^2+x1 x2,x1^2+u}
f=x1^5+x1^2 x3^2+x2^3 x3+x3^4+u x2
ord={x1,x2,x3}
AuxPseudoRemainder[f,as,ord]
```

下面 3 条命令是用来验证刚才得到的结果的:

```
r1=PseudoRemainder[f,as[[1]],ord[[3]]]
r2=PseudoRemainder[r1,as[[2]],ord[[2]]]
r3=PseudoRemainder[r2,as[[3]],ord[[1]]]
```

求多项式组 `ps` 对升列 `as` 的余式组可使用以下命令:

```
PseudoRemainderSet[ps,as,ord]
```

如果 as, f, ord 保持刚才输入的值. 再执行以下命令:

```
ps={f,as[[3]]*x1,as[[2]]*x2}
PseudoRemainderSet[ps,as,ord]
```

如果把 ps 中的第 2 项改成 as[[3]]*x1+u, 得到的结果中有一个不含变量的多项式 u, 说明余式组是矛盾的. 如果把 ps 中的 f 删去, 就得到 {0, 0}, 说明 $\mathrm{Rem}(\mathrm{ps},\mathrm{as})=0$.

求多项式组 ps 的基列可使用以下命令:

```
BasicSet[ps,ord]
```

有了上面介绍的命令, 已经足以从已知的多项式组求出相应的特征列. 这个函数包也提供了直接求特征列的命令:

```
CharacteristicSet[ps,ord]
```

如果想从特征列 (或升列) 求出具体的解, 可使用命令:

```
WuRittEqnsSolve[as,ord]
```

把上面两个命令复合起来:

```
WuRittEqnsSolve[CharacteristicSet[ps,ord],ord]
```

就能一下子求出多项式组 ps 的解 $Z(\mathscr{C}/J)$ (参见定理 4.5), 如要求 $Z(\mathscr{P},I_i)$ 的解还需继续进行.

较复杂的多项式组很可能会耗尽计算机的资源而无法用全自动的方法求解. 这时只好尝试用人机对话的交互方式, 根据中间结果, 不断人工干预, 调整策略. 所以我们介绍上列命令, 可供分步执行之用.

习 题 12–4

1. 仿照例 4.4 分别用分步法及一步法解多项式方程组:

$$\begin{cases} -12x_2^2+7x_1x_2-2=0, \\ -2x_3+x_1^2=0, \\ -x_3^2+x_1x_2+2=0. \end{cases}$$

2. 解多项式方程组:

$$\begin{cases} 2x_3^2-x_1^2-x_2^2=0, \\ x_1x_3-2x_3+x_1x_2=0, \\ x_1^2-x_2^2=0. \end{cases}$$

*§5 几何定理的机器证明

我们知道, 数值计算与定理证明是数学中两项最主要的活动形式. 总的说来, 计算易而繁, 证明妙而难. 计算之所以容易, 主要是由于计算过程往往已经或易于做到刻板化或机械化. 而与之相反, 即使叙述颇为简单的初中几何证明题, 也往往使许多大几何学家棘手. 机械化证明的目的就是要把定理证明化难为易, 即使弃简就繁也在所不惜. 问题就是: 定理证明是否也可以像数值计算那样机械化, 进而通过计算机实现定理证明的自动化.

事实上, 早在十七世纪莱布尼茨时就有机械化证明的设想. 直至 1947 年塔尔斯基 (Alfred Tarski, 1902–1983, 波兰人) 证明初等几何 (以及初等代数) 的定理证明可以机械化. 然而他的方法却不是切实可行的.

在 1899 年出版的希尔伯特 (David Hilbert, 1862–1943, 德国人) 的经典著作《几何基础》中, 就有着机械化的结果, 只是从来没有人注意过. 他证明了初等几何中只涉及从属与平行关系的定理证明可以机械化. 这一定理当然是塔尔斯基定理的一个特例. 但希尔伯特的机械化证明方法是切实可行的.

我国数学家吴文俊从 70 年代未开始研究定理证明的机械化问题, 证明了初等几何中只牵涉到从属、平行与全合关系的定理证明可以机械化. 其基本原理是将几何定理代数化, 然后采用一种机械化的方法判定几何定理是否正确. 这种机械化方法在理论上需要用到代数几何的工具. 里特 (R. F. Ritt) 在 30 年代提出的代数几何的构造性理论恰好满足这种需要. 吴文俊改进了里特的方法, 将其用于几何定理的机械化证明.

吴的结果包括了希尔伯特的定理, 但仍包括于塔尔斯基的定理之中. 然而, 与希尔伯特定理相似而与塔尔斯基定理不同之处是吴的机械化方法是切实可行的. 即使用手算也可证明相当艰深的定理, 而且还发现了新的定理. 不过直到现在还没有找到一种切实可行的方法来实现整个初等几何定理证明的机械化.

为了把几何问题代数化, 就要把命题的假设和结论表示成多项式方程组. 我们发现, 至少下列几何性质可以用多项式方程来表示.

命 题 5.1 *设 $A(x_1,y_1)$, $B(x_2,y_2)$, $C(x_3,y_3)$, $D(x_4,y_4)$, $E(x_5,y_5)$, $F(x_6,y_6)$, $G(x_7,y_7)$, $H(x_8,y_8)$ 是平面上的点, 则下列几何性质可以表达为一个或几个多项式方程:*

(1) *两线平行: $AB//CD$ 可以表示为:*

$$(x_2-x_1)(y_4-y_3)-(x_4-x_3)(y_2-y_1)=0;$$

(2) *三点共线: A,B,C 共线可以表示为:*

$$(x_2-x_1)(y_3-y_1)-(x_3-x_1)(y_2-y_1)=0;$$

(3) *一点是两点的中点: B 是 A,C 的中点可以表示为:*

$$\begin{cases}2x_2-x_1-x_3=0\\2y_2-y_1-y_3=0;\end{cases}$$

(4) *一点分两点成定比: C 分 A,B 成定比 r 可以表示为:*

$$\begin{cases}x_3-x_1-r(x_2-x_3)=0\\y_3-y_1-r(y_2-y_3)=0;\end{cases}$$

(5) 三线共点: AB, CD, EF 三条直线都经过 G 点可以用三个等式表示, 这三个等式分别表示 A, B, G 三点共线, C, D, G 三点共线, 以及 E, F, G 三点共线;

(6) 线段相等: $|AB| = |CD|$ 可以表示为:

$$(x_2 - x_1)^2 + (y_2 - y_1)^2 - (x_4 - x_3)^2 - (y_4 - y_3)^2 = 0;$$

(7) 线段的比相等: 线段 AB 与 CD 的长度之比等于 r 可以表示为:

$$(x_2 - x_1)^2 + (y_2 - y_1)^2 - r^2[(x_4 - x_3)^2 + (y_4 - y_3)^2] = 0;$$

线段 AB 与 CD 的长度之比等于线段 EF 与 GH 的长度之比可以表示为:

$$\begin{aligned}&[(x_2 - x_1)^2 + (y_2 - y_1)^2][(x_8 - x_7)^2 + (y_8 - y_7)^2]\\ -&[(x_4 - x_3)^2 + (y_4 - y_3)^2][(x_6 - x_5)^2 + (y_6 - y_5)^2] = 0;\end{aligned}$$

(8) 两线垂直: $AB \perp CD$ 可以表示为:

$$(x_2 - x_1)(x_4 - x_3) + (y_2 - y_1)(y_4 - y_3) = 0;$$

(9) 两角相等: $\angle ABC = \angle DEF$ 可以表示为:

$$\begin{aligned}&[(x_1-x_2)(y_3-y_2)-(x_3-x_2)(y_1-y_2)][(x_4-x_5)(x_6-x_5)+(y_4-y_5)(y_6-y_5)]\\ -&[(x_4-x_5)(y_6-y_5)-(x_6-x_5)(y_4-y_5)][(x_1-x_2)(x_3-x_2)+(y_1-y_2)(y_3-y_2)]\\ =&0;\end{aligned}$$

(10) 点在分角线上: D 在 $\angle ABC$ 的分角线上可以表示为:

$$\begin{aligned}&[(x_1-x_2)(y_4-y_2)-(x_4-x_2)(y_1-y_2)][(x_4-x_2)(x_3-x_2)+(y_4-y_2)(y_3-y_2)]\\ -&[(x_4-x_2)(y_3-y_2)-(x_3-x_2)(y_4-y_2)][(x_1-x_2)(x_4-x_2)+(y_1-y_2)(y_4-y_2)]\\ =&0;\end{aligned}$$

(11) 一点在一圆上: B 在以 A 为圆心, r 为半径的圆上可以表示为:

$$(x_2 - x_1)^2 + (y_2 - y_1)^2 - r^2 = 0;$$

(12) 四点共圆: 为刻划四点 A, B, C, D 共圆, 可以设这个圆的圆心是 E, 半径是 r, 而把这四点共圆表示为:

$$\begin{cases}(x_1 - x_5)^2 + (y_1 - y_5)^2 - r^2 = 0\\ (x_2 - x_5)^2 + (y_2 - y_5)^2 - r^2 = 0\\ (x_3 - x_5)^2 + (y_3 - y_5)^2 - r^2 = 0\\ (x_4 - x_5)^2 + (y_4 - y_5)^2 - r^2 = 0.\end{cases}$$

证明: 这些都是前面已经学过的解析几何知识. 只有 (9) 较复杂些. 这里利用了公式

$$\tan\angle ABC = \frac{k_{BC} - k_{BA}}{1 + k_{BC}k_{BA}},$$

再用等式 $\tan\angle ABC = \tan\angle DEF$ 导出所求的多项式等式. 而 (10) 则等价于 $\angle ABD = \angle DBC$. □

几何定理机械化证明的吴方法的原理可以表达成以下定理:

定理 5.2 *设定理的假设条件可以用多项式组 $\mathscr{P} = 0$ 表示, 定理的结论可以用多项式 $G = 0$ 表示. 设 $\mathscr{C} = \{C_1, \cdots, C_r\}$ 是 $\mathscr{P}$ 的特征列, C_i 的初式是 I_i $(i = 1, \cdots, r)$. 如果 $\mathrm{Rem}(G, \mathscr{C}) = 0$, 则在非退化条件 $J = I_1 I_2 \cdots I_r \neq 0$ 下 $G = 0$ 可以由 $\mathscr{P} = 0$ 推出. 也就是说, 在非退化条件下定理成立.*

证明: 根据引理 4.3, 由 $\mathrm{Rem}(G, \mathscr{C}) = 0$ 可得

$$I_1^{s_1} I_2^{s_2} \cdots I_r^{s_r} G = \sum_{i=1}^{r} q_i C_i.$$

从上式可以得到

$$\mathscr{C} = 0, J \neq 0 \Longrightarrow G = 0,$$

而根据定理 4.5 的证明, 有 $Z(\mathscr{P}/J) = Z(\mathscr{C}/J)$, 即

$$\mathscr{C} = 0, J \neq 0 \Longleftrightarrow \mathscr{P} = 0, J \neq 0,$$

所以

$$\mathscr{P} = 0, J \neq 0 \Longrightarrow G = 0. \qquad \square$$

从上面定理可以看到, 不能用多项式方程组表示的几何性质无法利用这个定理作机械化证明. 例如一些涉及大小和次序的几何性质就不能用多项式等式关系来表达. 另一方面定理中出现了非退化条件 $J \neq 0$, 这些条件往往是有几何含义的. 这是因为在几何定理的陈述或证明过程中, 常常有一些隐含的假设: 即所考虑的几何图形必须处于某种一般的状况, 譬如说三角形, 总是意味三个顶点不在一直线上. 如果出现了退化, 即三个顶点共线了, 则定理的结论可能不再正确. 所以许多定理的结论不包括退化的情形是很自然的事. 定理 5.2 中的 $J = 0$ 就是退化的情形. 原定理的结论在退化情形是否仍然有效, 必须通过对扩大的多项式组 $\mathscr{P} \cup \{J\}$ 进行讨论才能确定. 因此定理 5.2 中对 $J \neq 0$ 的限制并不是一个缺陷, 而是由几何定理本身的特点所决定的必然结果.

下面我们通过几个例子来看如何对几何定理作机械化证明.

例 5.1 (德扎格 (Gérard Desargues, 1593–1662, 法国人) 定理) 如图 12–2, 设平面上有两条直线 L_1, L_2 相交于 O 点, 在 L_1 上任取两点 A_1, A_2, 在 L_2 任

取一点 B_1. 过 A_2 作直线平行于 A_1B_1, 交 L_2 于 B_2. 在平面上任取一点 C_1, 过 A_2, B_2 分别作直线与 A_1C_1, B_1C_1 平行, 两直线相交于 C_2. 则 O, C_1, C_2 三点共线.

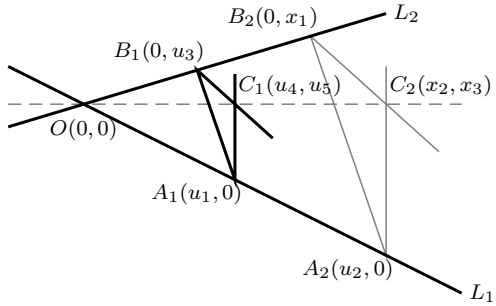


图 12–2

证明: 这是个仿射问题, 因此可以选取斜角坐标系. 以 O 作为原点, L_1, L_2 分别作为 x 轴和 y 轴. 设上述各点的坐标为:

$$\begin{aligned} &O(0,0), \quad A_1(u_1,0),\ A_2(u_2,0), \quad B_1(0,u_3) \\ &C_1(u_4,u_5),\ B_2(0,x_1),\ C_2(x_2,x_3). \end{aligned}$$

这里 $u_1, u_2, \cdots, u_5$ 是参数, x_1, x_2, x_3 是变元.

根据假设条件可以得到下列多项式方程:

$$\begin{aligned} P_1 &\stackrel{\text{def}}{=} u_1x_1 - u_2u_3 = 0, && (A_1B_1 /\!/ A_2B_2) \\ P_2 &\stackrel{\text{def}}{=} u_4(x_3 - x_1) - x_2(u_5 - u_3) = 0, && (B_1C_1 /\!/ B_2C_2) \\ P_3 &\stackrel{\text{def}}{=} (u_1 - u_4)x_3 - u_5(u_2 - x_2) = 0, && (A_1C_1 /\!/ A_2C_2) \end{aligned}$$

这样定理假设可以归结成一个多项式组 $\mathscr{P} = \{P_1, P_2, P_3\}$.

定理结论是 O, C_1, C_2 三点共线, 可以归结为多项式方程

$$G \stackrel{\text{def}}{=} u_4x_3 - u_5x_2 = 0.$$

现在我们分别用 Maple 和 Mathematica 来实现几何定理的机械化证明.

利用 Maple 的函数包 wsolve2:

```
>read `c:/maple/share/wsolve2`;
>P1:=u1*x1-u2*u3;
>P2:=u4*(x3-x1)-x2*(u5-u3);
>P3:=(u1-u4)*x3-u5*(u2-x2);
>PS1:={P1,P2,P3};
>G:=u4*x3-u5*x2;
```

```
>ord:=[x3,x2,x1];
>CS:=wsolve(PS1,ord);
```

计算过程中除去了两个不含变量的因子: $u_1u_5-u_1u_3+u_3u_4$ 以及 u_1-u_4. 得到的结果是 $\mathscr{C}=\{C_1,C_2,C_3\}$ (我们把输出的结果改成按类递增):

$$\begin{aligned}C_1&=u_1x_1-u_2u_3,\\C_2&=u_1x_2-u_2u_4,\\C_3&=u_1x_3-u_2u_5.\end{aligned}$$

计算 $\mathrm{Rem}(G,\mathscr{C})$:

```
>Premas(G,CS[1],ord);
```

得到的结果是 0. 根据定理 5.2 可知在非退化条件下, 德扎格定理成立.

计算 J:

```
>J:=Initial(CS[1][1],ord)*Initial(CS[1][2],ord)*Initial
(CS[1][3],ord);
```

得到 $J=u_1^3$. 因此退化条件包含 3 个不可约因式: $u_1u_5-u_1u_3+u_3u_4$, u_1-u_4, u_1. 以下分别研究:

(1) 当 $u_1=0$ 时, A_1 与 O 重合. 这样 B_2 不存在, 定理无意义.

(2) 当 $u_1u_5-u_1u_3+u_3u_4=0$ 时, C_1 位于直线 A_1B_1 上, 因此 C_2 点是不确定的, 定理无意义.

(3) 当 $u_1-u_4=0$ 时, 在多项式组 $\mathscr{P}$ 里以 u_1 代 u_4 重新计算, 除去一个不含变量的因式 u_5 后得到新的特征列 $\mathscr{C}$ 为:

$$\begin{aligned}C_1&=u_1x_1-u_2u_3,\\C_2&=-x_2+u_2,\\C_3&=u_1x_3-u_2u_5.\end{aligned}$$

并且 $\mathrm{Rem}(G,\mathscr{C})=0$. 初式 $J=u_1^2$. 退化条件的不可约因式是: u_1 及 u_5. $u_1=0$ 已在 (1) 讨论过. 当 $u_5=0$ 时, 又可归结为 (2), 定理无意义. 因此在非退化条件 $u_1u_5\neq0$ 下定理成立.

❁ 利用 Mathematica 的函数包 WuRittSolva,

```
p1=u1 x1-u2 u3
p2=u4(x3-x1)-x2(u5-u3)
p3=(u1-u4)x3-u5(u2-x2)
ps1={p1,p2,p3}
```

```
g=u4 x3-u5 x2
ord={x1,x2,x3}
cs=CharacteristicSet[ps1,ord]
```

得到的结果是 $\mathscr{C}=\{C_1,C_2,C_3\}$:

$$\begin{aligned}
C_1 &= u_1x_1-u_2u_3,\\
C_2 &= (u_1^2u_3-u_1^2u_5-u_1u_3u_4)x_2-u_1u_2u_3u_4+u_1u_2u_4u_5+u_2u_3u_4^2,\\
C_3 &= (u_1-u_4)x_3+u_5x_2-u_2u_5.
\end{aligned}$$

计算 $\mathrm{Rem}(G,\mathscr{C})$:

```
AuxPseudoRemainder[g,Reverse[cs],ord]
```

得到的结果是 0. 根据定理 5.2 可知在非退化条件下, 德扎格定理成立. 上述命令中的函数 `Reverse` 的作用是把集合的元素倒过来排列, 这是为了适应函数 `AuxPseudoRemainder` 的要求.

计算 J:

```
j=Initial[cs[[1]],ord]*Initial[cs[[2]],ord]
*Initial[cs[[3]],ord]
```

得到 $J=u_1^2(u_1-u_4)(u_1u_3-u_3u_4-u_1u_5)$. 因此退化条件包含 3 个不可约因式: $u_1u_3-u_1u_5-u_3u_4$, u_1-u_4, u_1. 以下分别研究:

(1) 当 $u_1=0$ 时, A_1 与 O 重合. 这样 B_2 不存在, 定理无意义.

(2) 当 $u_1u_3-u_1u_5-u_3u_4=0$ 时, C_1 位于直线 A_1B_1 上, 因此 C_2 点是不确定的, 定理无意义.

(3) 当 $u_1-u_4=0$ 时, 在多项式组 $\mathscr{P}$ 里以 u_1 代 u_4 重新计算, 得到新的特征列 $\mathscr{C}$ 为:

$$\begin{aligned}
C_1 &= u_1x_1-u_2u_3,\\
C_2 &= u_5(x_2-u_2),\\
C_3 &= u_1x_3+(u_3-u_5)x_2-u_1x_1.
\end{aligned}$$

并且 $\mathrm{Rem}(G,\mathscr{C})=0$. 初式 $J=u_1^2u_5$. 退化条件的不可约因式是: u_1 及 u_5. $u_1=0$ 已在 (1) 讨论过. 当 $u_5=0$ 时, 又可归结为 (2), 定理无意义. 因此在非退化条件 $u_1u_5\neq 0$ 下定理成立. □

从这个例子可以看到非退化条件的几何意义及其必要性.

评注 5.1 利用 Maple 里的 Groebner 包也可以证明几何定理, 对于例 5.1, 可以使用以下命令:

```
>CS:=Groebner[Solve](PS1,{x1,x2,x3});
```

```
>Groebner[Reduce](G,CS[1][1],CS[1][2],‘s‘);
```

这里的函数 `Groebner[Reduce]`(多项式, 升列, 变量的序, 输出变量的名称) 可以求出多项式关于升列的余式, 最后的可选参数 “输出变量的名称” 是一个未经赋值或没有使用过的变量, 函数运行后会把升列的初式 J 的因子赋值给此变量. 像例 5.1 的运算结果是 0, 表示 $\mathrm{Rem}(G,\mathscr{C})=0$, 而运算后变量 `s` 的值等于 u_1. 不过函数 `Groebner[Solve]` 在运行时不会显示被除去的不含变量的因子, 因此失去了另外两个非退化条件 $u_1u_5-u_1u_3+u_3u_4$ 与 u_1-u_4.

如果使用 Maple 的旧版本, 则应把函数 `Solve` 与 `Reduce` 分别改名为 `gsolve` 与 `reduce`.

例 5.2 证明: 从三角形外接圆上一点到三角形三边所作垂线的垂足共线 (这线称为西摩松 (Simson) 线).

证明: 如图 12–3, 取 $\triangle ABC$ 的 A 点为原点, AB 边所在的直线为横轴. 设它的外接圆的圆心为 O. 设 P 为外接圆上一点, 它到 $\triangle ABC$ 三边 AB,BC,CA 所作垂线的垂足分别为 L,M,N. 各点的坐标如图所示.

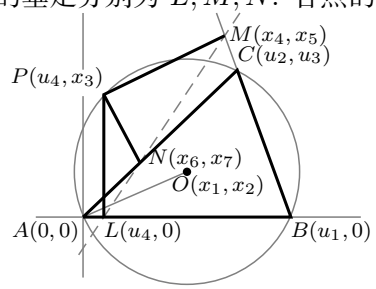


图 12–3

根据假设条件可以得到下列多项式方程:

$$
\begin{aligned}
&P_1 \overset{\text{def}}{=} u_1^2-2u_1x_1=0, && (|OB|=|OA|)\\
&P_2 \overset{\text{def}}{=} u_2^2-2u_2x_1+u_3^2-2x_2u_3=0, && (|OC|=|OA|)\\
&P_3 \overset{\text{def}}{=} u_4^2-2u_4x_1+x_3^2-2x_3x_2=0, && (|OP|=|OA|)\\
&P_4 \overset{\text{def}}{=} (x_3-x_5)u_3+(u_4-x_4)(u_2-u_1)=0, && (PM\perp BC)\\
&P_5 \overset{\text{def}}{=} (x_3-x_7)u_3+(u_4-x_6)u_2=0, && (PN\perp AC)\\
&P_6 \overset{\text{def}}{=} x_5(u_2-u_1)-u_3(x_4-u_1)=0, && (M\text{ 在 }BC\text{ 上})\\
&P_7 \overset{\text{def}}{=} x_7u_2-x_6u_3=0, && (N\text{ 在 }CA\text{ 上})
\end{aligned}
$$

定理结论是 L,M,N 三点共线, 可以归结为多项式方程

$$G \overset{\text{def}}{=} x_7(x_4-u_4)-(x_6-u_4)x_5=0.$$

现在我们分别用 Maple 和 Mathematica 来实现几何定理的机械化证明.

利用 Maple 的函数包 wsolve2, 应用 `wsolve` 除去不含变量的因式

u_1, u_2, u_3 后, 得到特征列 $\mathscr{C}$:

$$
\begin{aligned}
C_1 &= -2x_1 + u_1,\\
C_2 &= 2u_3x_2 + u_1u_2 - u_2^2 - u_3^2,\\
C_3 &= u_3x_3^2 + (u_1u_2 - u_2^2 - u_3^2)x_3 - u_1u_3u_4 + u_3u_4^2,\\
C_4 &= (-u_1^2 + 2u_1u_2 - u_2^2 - u_3^2)x_4 + u_3(u_2 - u_1)x_3 + u_1^2u_4 - 2u_1u_2u_4\\
&\quad + u_1u_3^2 + u_2^2u_4,\\
C_5 &= (-u_1^2 + 2u_1u_2 - u_2^2 - u_3^2)x_5 + u_3^2x_3 + u_1^2u_3 - u_1u_2u_3 - u_1u_3u_4\\
&\quad + u_2u_3u_4,\\
C_6 &= (-u_2^2 - u_3^2)x_6 + u_2u_3x_3 + u_2^2u_4,\\
C_7 &= (u_2^2 + u_3^2)x_7 - u_3^2x_3 - u_2u_3u_4.
\end{aligned}
$$

经计算可得 $\mathrm{Rem}(G, \mathscr{C}) = 0$, 根据定理 5.2 可知在非退化条件下, 定理成立.

经计算: $J = (u_1^2 + u_3^2)^2(u_1^2 - 2u_1u_2 + u_2^2 + u_3^2)^2u_3^2$. 因此退化条件的不可约因式是: u_1, u_2, u_3, $u_1^2 + u_3^2$ 以及 $(u_1 - u_2)^2 + u_3^2$. 由于我们只考虑实数域, 所以第三个因式相当于 $u_1 = u_3 = 0$, 最后的因式相当于 $u_1 - u_2 = 0$ 及 $u_3 = 0$. 因而退化的情形可分成两类:

(1) $u_1 = 0$ 时, B 与 A 重合, 而 $u_3 = 0$ 时, C 在直线 AB 上, 这样 ABC 不再成为三角形, 定理无意义.

(2) $u_2 = 0$ 时, $\angle BAC$ 是直角, 而 $u_1 = u_2$ 时, $\angle ABC$ 是直角, 这样 $\triangle ABC$ 是直角三角形, 定理仍有可能成立. 不过需要修改多项式组 $\mathscr{P}$, 分别使 $u_2 = 0$ 或 $u_2 = u_1$, 再重新计算特征列及余式. 通过计算, 可以知道这两种情形定理仍然成立.

综上所述, 只要三角形不退化, 本定理成立.

✡ 利用 Mathematica 的函数包 WuRittSolva, 得到特征列 $\mathscr{C}$:

$$
\begin{aligned}
C_1 &= u_1(-2x_1 + u_1),\\
C_2 &= 2u_3x_2 - 2u_2x_1 + u_2^2 + u_3^2,\\
C_3 &= x_3^2 - 2x_2x_3 - 2u_1x_1 + u_1^2,\\
C_4 &= (-u_1^2 + 2u_1u_2 - u_2^2 - u_3^2)x_4 + u_3(u_2 - u_1)x_3 + u_1((u_1 - u_2)^2 + u_3^2\\
C_5 &= -u_3x_5 + (u_1 - u_2)x_4 + u_3x_3 - u_1(u_1 - u_2)\\
C_6 &= (-u_2^2 - u_3^2)x_6 + u_2u_3x_3 + u_1u_2^2,\\
C_7 &= -u_3x_7 - u_2x_6 + u_3x_3 + u_1u_2.
\end{aligned}
$$

经计算可得 $\mathrm{Rem}(G,\mathscr{C})=0$, 根据定理 5.2 可知在非退化条件下, 定理成立.

经计算: $J=4u_1u_3^3(u_2^2+u_3^2)^2(u_1^2-2u_1u_2+u_2^2+u_3^2)^2u_3^2$. 因此退化条件的不可约因式是: u_1, u_3, $u_2^2+u_3^2$ 以及 $(u_1-u_2)^2+u_3^2$. 由于我们只考虑实数域, 所以第三个因式相当于 $u_2=u_3=0$, 最后的因式相当于 $u_1-u_2=0$ 及 $u_3=0$. 因而退化的情形可分成两类:

(1) $u_1=0$ 时, B 与 A 重合, 而 $u_3=0$ 时, C 在直线 AB 上, 这样 ABC 不再成为三角形, 定理无意义.

(2) $u_2=0$ 时, $\angle BAC$ 是直角, 而 $u_1=u_2$ 时, $\angle ABC$ 是直角, 这样 $\triangle ABC$ 是直角三角形, 定理仍有可能成立. 不过需要修改多项式组 $\mathscr{P}$, 分别使 $u_2=0$ 或 $u_2=u_1$, 再重新计算特征列及余式. 通过计算, 可以知道这两种情形定理仍然成立.

综上所述, 只要三角形不退化, 本定理成立. □

评注 5.2 如同评注 5.1 所指出的, 如果利用 Maple 里的 Groebner 包计算例 5.2 的话, 会失去一个非退化条件 $u_1=0$.

从例 5.2 可以看出, 吴方法可以证明非平凡的定理. 此外, 吴方法还可以用来发现未知量之间的关系. 例如, 已知三角形的 3 条边长是 a,b,c, 则三角形的面积可以表示为:

$$\Delta=\sqrt{s(s-a)(s-b)(s-c)},\quad s=\frac{1}{2}(a+b+c).$$

这个公式被称为海伦公式. 但实际上, 比海伦公式约早 600 年, 我国古代数学家秦九韶在《算书九章》中已经给出了三角形面积的公式:

$$\Delta=\frac{1}{2}\sqrt{小^2大^2-\left(\frac{大^2+小^2-中^2}{2}\right)^2},$$

其中大中小分别表示三角形的 3 条边长 a,b,c. 简单演算可知, 海伦公式就是秦九韶公式. 这些公式的证明都不是简单的. 我们这里用数学机械化的方法给出一个证明.

例 5.3 证明秦九韶–海伦公式.

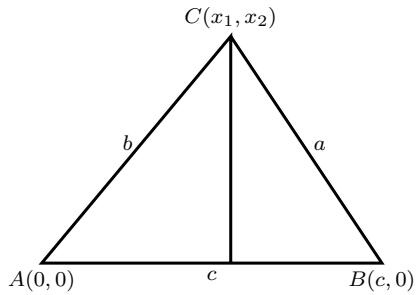


图 12–4

证明: 如图 12–4, 若把三角形的面积 Δ 记为 m, 可以得到多项式方程组:

$$\begin{aligned} P_1 &\stackrel{\text{def}}{=} cx_2 - 2m = 0, \\ P_2 &\stackrel{\text{def}}{=} x_1^2 + x_2^2 - b^2 = 0, \\ P_3 &\stackrel{\text{def}}{=} (c - x_1)^2 + x_2^2 - a^2 = 0. \end{aligned}$$

由于我们的目的是消去 x_1, x_2, 得到 a, b, c, m 之间的关系, 因此把变量的次序取为 m, x_1, x_2. 用吴方法求出多项式组 $\mathscr{P} = \{P_1, P_2, P_3\}$ 的特征列 $\mathscr{C} = \{C_1, C_2, C_3\}$ 如下:

$$\begin{aligned} C_1 &= c^2(-2c^2b^2 + 16m^2 + c^4 - 2c^2a^2 + a^4 - 2a^2b^2 + b^4), \\ C_2 &= c^2(-c^2 + 2cx_1 + a^2 - b^2), \\ C_3 &= cx_2 - 2m. \end{aligned}$$

于是 $C_1 = 0$ 可得

$$\begin{aligned} 16m^2 &= 2a^2b^2 + 2a^2c^2 + 2b^2c^2 - a^4 - b^4 - c^4 \\ &= 4a^2b^2 - (a^2 + b^2 - c^2)^2 \\ &= (a + b + c)(a + b - c)(a + c - b)(b + c - a). \end{aligned}$$

这就是秦九韶–海伦公式.

又从 $C_2 = 0$ 可以得出

$$a^2 = b^2 + c^2 - 2cx_1,$$

注意到 $x_1 = b\cos\angle BAC$, 就得到余弦定理. □

上机实验 为了方便几何定理的机械化证明, WuRittSolva 包把命题 5.1 里的关系式写成了函数. 详情可参看帮助菜单下 Addons & Links 栏中的 WuRittSolva → WuRittSolva Tools → Section WRS_III: Tools for Geo2AlgLib. 对例 5.1 的德扎格定理, 我们也可如下证明:

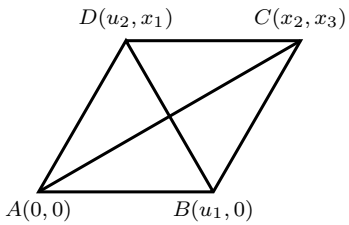
```
precoord={O->{0,0},A1->{u1,0},A2->{u2,0},B1->{0,u3},B2->{0,x1},
C1->{u4,u5},C2->{x2,x3}}
prethmcfg={TwoLinesParallel[{A1,B1},{A2,B2}],
TwoLinesParallel[{B1,C1},{B2,C2}],TwoLinesParallel[{A1,C1},{A2,C2}]}
prethmcnd={TriplePointsCollinear[O,C1,C2]}
ord={x1,x2,x3}
const={u1,u2,u3,u4,u5}
WuRittSmartProver[precoord,{prethmcfg,prethmcnd},ord,const]
```

习 题 12–5

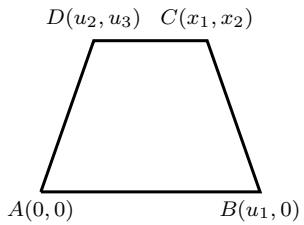
说明: 为了减少解题的的工作量, 有些图中的点已经标注了坐标. 不过这仅供参考, 读者可以自己选择坐标的变元.

1. 证明: 菱形的对角线互相垂直.

2. 证明: 等腰梯形底角相等.

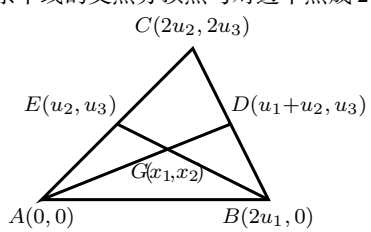


第 1 题



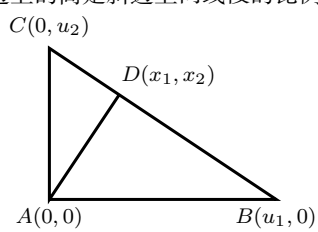
第 2 题

3. 证明: 三角形的两条中线的交点分顶点与对边中点成 2 : 1.



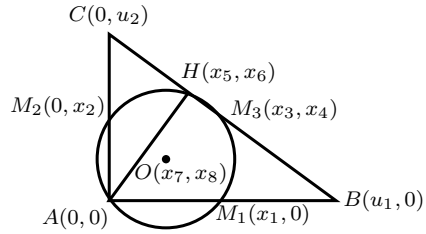
第 3 题

4. 证明: 直角三角形斜边上的高是斜边上两线段的比例中项.



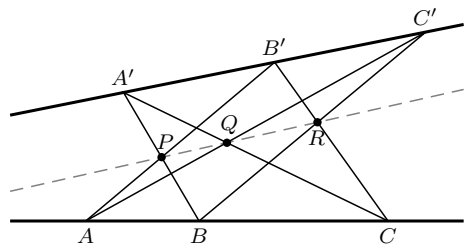
第 4 题

5. 如图, 设 $\triangle ABC$ 中 $\angle A$ 是直角, M_1, M_2, M_3 分别是 AB, AC, BC 边的中点. $AH \perp BC$ 并且 H 是垂足. 证明 M_1, M_2, M_3, H 四点共圆.



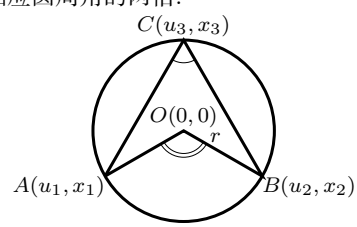
第 5 题

6. 如图, A,B,C 三点在一条直线上, A',B',C' 三点在另一条直线上. P,Q,R 是它们连线的交点. 证明: P,Q,R 三点共线.



第 6 题

7. 证明: 圆心角等于相应圆周角的两倍.



第 7 题