目录

说明: 上述目录中打星号*的章节可以作为选读内容.

第 1 章　一元多项式理论

线性代数和多项式是代数学的最基本的研究对象和工具之一, 方法上不同但相互联系.

多项式这个词, 我们是不陌生的, 中学里就有了, 并已知道有关多项式因式分解的一些基本方法. 比如x^3+x^2-x-1, 它可分解为$(x+1)^2(x-1)$.

但我们现在要上升到一般的多项式理论来讨论, 对于多项式所处的数域也不再限于实数域或有理数域.

从方法上来说, 多项式理论可类比于整数理论(见附录B.2). 这其实不是偶然的, 读者若学过近世代数, 就会发现它们是统一在所谓的唯一分解整环下的.

解多项式方程是数学中最基本的课题之一. 自17世纪以来, 对它的研究几乎未曾中断. 要想获得解任意次多项式方程的较好方法, 就需要建立完整的关于多项式的理论, 比如证明复数域上每个多项式方程必有根, 实数域上怎样的多项式才是不可分解的, 等等. 本章将逐次展开这些相关内容的讨论.

§1.1　一元多项式

首先给出一元多项式的抽象定义.

给定一个数域$\mathbb{P}$, x为一符号(或称文字), 形如

$$f(x)\triangleq a_0+a_1x+\cdots+a_nx^n+a_{n+1}x^{n+1}+\cdots \tag{1.1.1}$$

的形式表达式称为**系数在数域$\mathbb{P}$上的一元多项式**(或简称: **$\mathbb{P}$上的一元多项式**), 其中对$i=0,1,\cdots,n,\cdots$, 所有$a_i\in\mathbb{P}$至多有限个不等于0. 我们把a_ix^i称为$f(x)$的i**次单项**(或i**次项**), a_i称为i次项的**系数**. 用连加符号可表为

$$f(x)\triangleq\sum_{i=0}^{+\infty}a_ix^i.$$

在上式中, 若$a_n\neq 0$但是对所有$s>n$有$a_s=0$, 就称a_nx^n为**首项**, 称a_n为**首项系数**, 称n为$f(x)$的**次数**, 并表为$\partial(f(x))$. 若一个多项式的所有系数全为 0, 则称之为**零多项式**, 并记作0. 零多项式的次数规定为$-\infty$.

注意: (1) 这里的运算"$+$"仅是一个"形式加法", 只是将不同单项"连结"在一起;

(2) 系数a_i与x^i之间的关系a_ix^i仅表示"形式数乘", 只是说明将两者"放在一起";

(3) 我们约定, 一个多项式$f(x)$中系数为0的单项可以写出来, 也可以不写出来. 比如, 设$\partial(f(x))=n$, 我们可以写

$$f(x)=a_0+a_1x+\cdots+a_nx^n+0x^{n+1}+0x^{n+2}+\cdots,$$

也可以写

$$f(x)=a_0+a_1x+\cdots+a_nx^n.$$

设

$$f(x)=a_0+a_1x+\cdots+a_nx^n+\cdots,$$
$$g(x)=b_0+b_1x+\cdots+b_nx^n+\cdots$$

是数域$\mathbb{P}$上的两个多项式.

(1) 若对$i=0,1,\cdots$, 有$a_i=b_i$, 则称$f(x)$与$g(x)$是**相等**的, 表为$f(x)=g(x)$.
由于零多项式的系数全为零, 因此它不与任何一个非零多项式相等.

(2) 定义$f(x)$与$g(x)$的**和**为如下的一个新的多项式:

$$f(x)+g(x)\triangleq(a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n+\cdots;$$

(3) $f(x)$与$g(x)$的**乘积**为如下的一个新的多项式:

$$f(x)g(x)\triangleq c_0+c_1x+\cdots+c_sx^s+\cdots,$$

其中s次单项的系数是

$$c_s=a_sb_0+a_{s-1}b_1+\cdots+a_1b_{s-1}+a_0b_s=\sum_{i+j=s}a_ib_j.$$

因此, 当$f(x)\neq0,\ g(x)\neq0$时, 令$\partial(f(x))=n,\ \partial(g(x))=m$, 那么$f(x)=g(x)$ 当且仅当$n=m$ 且对$i=0,1,\cdots,n$, 有$a_i=b_i$. 若$n\geqslant m,$ 则有

$$\begin{aligned}&f(x)+g(x)\\&=(a_0+a_1x+\cdots+a_mx^m+a_{m+1}x^{m+1}+\cdots+a_nx^n)\\&\quad+(b_0+b_1x+\cdots+b_mx^m+0x^{m+1}+\cdots+0x^n)\\&=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_m+b_m)x^m+(a_{m+1}+0)x^{m+1}+\cdots+(a_n+0)x^n.\end{aligned}$$

这时, 由上面多项式乘积的定义, 对$t>n+m$, 易见$c_t=0$. 因而,

$$f(x)g(x)=c_0+c_1x+\cdots+c_sx^s,$$

其中$s=n+m$. 对$0\leq i\leq s,$ i次项的系数是

$$c_i=a_ib_0+a_{i-1}b_1+\cdots+a_1b_{i-1}+a_0b_i.$$

特别地, $c_s=a_nb_m$.

零多项式0起到的作用就是线性空间中零元的作用, 这是因为:

(1) $0+f(x)=f(x)$. 事实上,

$$\begin{aligned}0+f(x)&=(0+0x+\cdots+0x^n)+(a_0+a_1x+\cdots+a_nx^n)\\&=(0+a_0)+(0+a_1)x+\cdots+(0+a_n)x^n\\&=a_0+a_1x+\cdots+a_nx^n\\&=f(x);\end{aligned}$$

(2) 同理, $f(x)+0=f(x)$;

(3) 再由乘法定义可证, $f(x)0=0f(x)=0$.

定义$f(x)$的**负多项式**为:

$$-f(x)\triangleq(-a_0)+(-a_1)x+\cdots+(-a_n)x^n.$$

定义$f(x)$与$g(x)$的**减法**为:

$$f(x)-g(x)\triangleq f(x)+(-g(x)).$$

那么,

$$f(x)-f(x)=0.$$

定义数c在多项式$f(x)$上的**数乘**为

$$cf(x)=ca_0+ca_1x+\cdots+ca_nx^n,$$

这也就是把c看作常数项多项式时与$f(x)$的多项式乘法得到的结果.

显然, 数域$\mathbb{P}$上两个多项式经加、减、乘运算后, 所得结果仍是$\mathbb{P}$上的多项式.

由多项式的次数定义, 我们有如下性质:

性质 1.1.1 对于任意两个非零多项式$f(x)=\sum a_ix^i,\ g(x)=\sum b_jx^j$, 若$\partial(f(x))=n$和$\partial(g(x))=m$, 那么,

(1) $\partial(f(x)+g(x))\leqslant\max\{\partial(f(x)),\ \partial(g(x))\}$;

(2) $\partial(f(x)g(x))=\partial(f(x))+\partial(g(x))$.

证明 (1) 不妨设$n\geqslant m$, 即$\partial(f(x))\geqslant\partial(g(x))$. 则由前面给出的两个多项式和的公式, 当$n>m$时, $f(x)+g(x)$ 的首项是$(a_n+0)x^n=a_nx^n\neq0$, 故这时

$$\partial(f(x)+g(x))=n=\partial(f(x))=\max\{\partial(f(x)),\ \partial(g(x))\};$$

当$n=m$时, 若$a_n+b_n\neq0$, 则$f(x)+g(x)$ 的首项是$(a_n+b_n)x^n$且

$$\partial(f(x)+g(x))=n=\partial(f(x))=\partial(g(x))=n;$$

若$a_n+b_n=0$, 则$\partial(f(x)+g(x))\leqslant n-1$.

因此总有$\partial(f(x)+g(x))\leqslant\max\{\partial(f(x)),\ \partial(g(x))\}$.

(2) 由多项式乘积的定义可得

$$f(x)g(x)=\sum_{t=0}^{m+n}\left(\sum_{i+j=t}a_ib_j\right)x^t,$$

其中$a_nb_m\neq0$. 所以它的首项是$a_nb_mx^{n+m}$, 因此

$$\partial(f(x)g(x))=n+m=\partial(f(x))+\partial(g(x)).$$ □

利用下面的性质1.1.2, 不难将上面的结论推广到多个多项式的情形.

多项式的运算与数的运算有类似的规律, 即:

性质 1.1.2 对数域$\mathbb{P}$上的多项式$f(x),\ g(x),\ h(x)$, 有:

(i) 加法交换律: $f(x)+g(x)=g(x)+f(x)$;

(ii) 乘法交换律: $f(x)g(x)=g(x)f(x)$;

(iii) 加法结合律: $(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$;

(iv) 乘法结合律: $(f(x)g(x))h(x)=f(x)(g(x)h(x))$;

(v) 乘法对加法的(左、右)分配律:

$$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x),$$
$$(g(x)+h(x))f(x)=g(x)f(x)+h(x)f(x);$$

(vi) 乘法的(左、右)消去律:

若$f(x)g(x)=f(x)h(x)$ (或$g(x)f(x)=h(x)f(x)$) 且$f(x)\neq0$, 则$g(x)=h(x)$.

证明 (i) 对$f(x)=\sum_{i=0}^{n}a_ix^i,\ g(x)=\sum_{i=0}^{m}b_ix^i$, 设$n\geqslant m$. 那么, 由加法定义可得:

$$\begin{aligned}
&f(x)+g(x)\\
&=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_m+b_m)x^m+(a_{m+1}+0)x^{m+1}+\cdots+(a_n+0)x^n\\
&=(b_0+a_0)+(b_1+a_1)x+\cdots+(b_m+a_m)x^m+(0+a_{m+1})x^{m+1}+\cdots+(0+a_n)x^n\\
&=g(x)+f(x).
\end{aligned}$$

(ii) 对$0 \le i \le n+m$, 有

$$c_i \triangleq a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i = b_ia_0 + b_{i-1}a_1 + \cdots + b_1a_{i-1} + b_0a_i.$$

于是,

$$f(x)g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m} = g(x)f(x).$$

(iii) 由加法定义即可得.

(iv) 对$f(x) = \sum\limits_{i=0}^{n} a_ix^i,\ g(x) = \sum\limits_{i=0}^{m} b_ix^i,\ h(x) = \sum\limits_{i=0}^{l} c_ix^i$, 依乘法定义,

$$\begin{aligned}
(f(x)g(x))h(x) &= \left(\sum_{s=0}^{n+m}\left(\sum_{i+j=s} a_ib_j\right)x^s\right)\left(\sum_{i=0}^{l} c_ix^i\right)\\
&= \sum_{t=0}^{n+m+l}\left(\sum_{s+k=t}\left(\sum_{i+j=s} a_ib_j\right)c_k\right)x^t\\
&= \sum_{t=0}^{n+m+l}\left(\sum_{i+j+k=t} a_ib_jc_k\right)x^t\\
&= \sum_{t=0}^{n+m+l}\left(\sum_{i+p=t} a_i\left(\sum_{j+k=p} b_jc_k\right)\right)x^t\\
&= f(x)(g(x)h(x)).
\end{aligned}$$

(v) 由加法定义和乘法定义可证得, 请读者自证.

(vi) 由$f(x)g(x) = f(x)h(x)$, 得$f(x)(g(x) - h(x)) = 0$.

由$f(x) \neq 0$得$\partial(f(x)) \ge 0$.

若$g(x) - h(x) \neq 0$, 则$\partial(g(x) - h(x)) \ge 0$, 进而

$$\partial(f(x)(g(x) - h(x))) = \partial(f(x)) + \partial(g(x) - h(x)) \ge 0 \neq -\infty.$$

但$\partial(0) = -\infty$, 这与$f(x)(g(x) - h(x)) = 0$矛盾. 所以$g(x) - h(x) = 0$, 即$g(x) = h(x)$. □

由上面(i), 当$i \neq j$时, $a_ix^i + b_jx^j = b_jx^j + a_ix^i$, 因而, 对任一多项式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

我们可以有另一表达式

$$f(x) = a_nx^n + \cdots + a_1x + a_0.$$

更多地, 我们会用这一降次排序写法, 这也就是为何称a_nx^n ($a_n \neq 0$) 是$f(x)$的首项的原因.

数域$\mathbb{P}$上的所有一元多项式全体我们表示为集合$\mathbb{P}[x]$. 由上, $\mathbb{P}[x]$中已有加法、乘法和数乘, 由它们的定义和多项式相等的条件, 以及上面的讨论, 特别是性质1.1.2 (i) (iii), 可知, $\mathbb{P}[x]$**是$\mathbb{P}$上线性空间**, 且若令

$$\mathbb{P}[x]_n = \{f(x) \in \mathbb{P}[x] : \partial(f(x)) < n\},$$

则$\mathbb{P}[x]_n$是一个以$1,\ x,\ \cdots,\ x^{n-1}$为基的$\mathbb{P}$上n维线性空间. 由此, 有子空间链:

$$\{0\} = \mathbb{P}[x]_0 \subset \mathbb{P}[x]_1 \subset \cdots \subset \mathbb{P}[x]_n \subset \mathbb{P}[x]_{n+1} \subset \cdots \subset \mathbb{P}[x].$$

而$\mathbb{P}[x]$本身是$\mathbb{P}$上**无限维的**线性空间, $\{1,\ x,\ \cdots,\ x^n,\ \cdots\}$是$\mathbb{P}[x]$的一组无限基.

又由性质1.1.2 (iv) (v), 我们将这个$\mathbb{P}$上线性空间$\mathbb{P}[x]$称为$\mathbb{P}$**上的一元多项式代数**.

一般的代数概念来自于近世代数课程, 它是一个有乘法的线性空间, 我们这里不再涉及.

我们在这里定义多项式的抽象概念, 目的是为了统一不同现实情况下出现的多项式的共性. 比如, 当符号x具体到中学数学里的未知数时, $f(x)=a_nx^n+\cdots+a_2x^2+a_1x+a_0$就代表一个未知数$x$的数字表达式, 加法和数乘就恢复到数的加、乘; 当x可以在数的一定范围内变动, 那么$f(x)$就成为x上的一个函数, 称为**多项式函数**. 当符号x具体到一个方阵$\boldsymbol{A}$时, $f(x)$就变成$f(\boldsymbol{A})=a_n\boldsymbol{A}^n+\cdots+a_2\boldsymbol{A}^2+a_1\boldsymbol{A}+a_0\boldsymbol{E}$, 这是一个矩阵表达式, 加法和数乘就具体到矩阵的加法和数乘. 看实际需要, 这个符号x还可以表示其他待定事物. 进一步, 我们就引入了形式化的多项式的运算来统一研究各类待定事物所满足的运算规律, 以得到它们普遍的共同的性质.

§1.2 整除理论

在一元多项式代数$\mathbb{P}[x]$中, 上节已定义了加减乘三种运算, 但乘法的逆运算—-除法—-通常是不可行的. 因为, 对某个多项式$f(x)\in\mathbb{P}[x]$, 若$\partial(f(x))\geq 1$, 则对任一非零多项式$g(x)\in\mathbb{P}[x]$, 必有

$$\partial(f(x)g(x))=\partial(f(x))+\partial(g(x))\geq\partial(f(x))\geq 1.$$

因此$f(x)g(x)\neq 1$, 故$\mathbb{P}[x]$中不存在$f(x)^{-1}$. 这说明除法是不可行的. 因此, 整除就成了某些多项式之间的特殊的重要关系.

数域$\mathbb{P}$上的多项式$g(x)$称为**整除**$f(x)$的, 若存在$\mathbb{P}$上的多项式$h(x)$使得

$$f(x)=g(x)h(x)$$

成立. 我们用$g(x)\mid f(x)$表示$g(x)$整除$f(x)$. 当$g(x)$不能整除$f(x)$时, 用$g(x)\nmid f(x)$表示. 当$g(x)\mid f(x)$时, 称$g(x)$是$f(x)$的**因式**, $f(x)$是$g(x)$的**倍式**.

显然, 对任一个$\mathbb{P}$上多项式$f(x)$和$0\neq a\in\mathbb{P}$, 必有$f(x)=1\cdot f(x)$, $0=0\cdot f(x)$, $f(x)=a(a^{-1}f(x))$, 因此总有:

$$f(x)|f(x),\quad f(x)|0,\quad a|f(x)\,.$$

由中学代数我们已经知道, 对两个具体的多项式, 可用一个去除另一个, 求得商和余式. 例如, 设$f(x)=3x^3+4x^2-5x+6$, $g(x)=x^2-3x+1$, 可以按下面的格式来作除法:

$$\begin{array}{r|l} & 3x\ +13 \\ \hline x^2-3x+1 & 3x^3+4x^2-5x+6 \\ & \underline{3x^3-9x^2+3x} \\ & \quad 13x^2-\ 8x+6 \\ & \quad \underline{13x^2-39x+13} \\ & \qquad\qquad 31x-7 \end{array}$$

即, 所得商为$3x+13$, 余式为$31x-7$. 上述竖式也可写为如下表达式:

$$f(x)=(3x+13)g(x)+(31x-7).$$

显然上述算式是对数字运算下的数字多项式进行的, 但不难看出, 事实上, 把上述多项式看作第一节中定义的"形式"多项式时, 算式一样成立. 也就是说, 我们可将此求商式和除式的方法用到"形式"多项式上. 这不是偶然的, 它建立在如下的结论上:

定理 1.2.1 (带余除法) 对于$\mathbb{P}[x]$中的任意两个多项式$f(x)$与$g(x)$, 其中$g(x)\neq$

0, 必存在唯一的$q(x)$, $r(x) \in \mathbb{P}[x]$ 使得

$$f(x) = q(x)g(x) + r(x) \tag{1.2.1}$$

成立, 且或者$r(x) = 0$或者$\partial(r(x)) < \partial(g(x))$.

证明 先证$q(x)$, $r(x)$的存在性.

当$f(x) = 0$时, 取$q(x) = r(x) = 0$即可.

当$f(x) \neq 0$时, 对$\partial(f(x)) = n$用归纳法.

当$\partial(f(x)) = 0$, 若$\partial(g(x)) = 0$, 令$g(x) = c \in \mathbb{P}$, 取$q(x) = c^{-1}f(x)$, $r(x) = 0$即可. 若$\partial(g(x)) > 0$, 取$q(x) = 0$, $r(x) = f(x)$即可.

假设$\partial(f(x)) < n$时结论成立, 考虑$\partial(f(x)) = n$时的情况.

事实上, 当$\partial(g(x)) > n$时, 取$q(x) = 0$, $r(x) = f(x)$即可.

当$\partial(g(x)) = m \leq n$时, 令$f(x)$和$g(x)$的首项分别是$ax^n$和$bx^m$, 则$b^{-1}ag(x)x^{n-m}$的首项也是$ax^n$, 故多项式$f_1(x) = f(x) - b^{-1}ax^{n-m}g(x)$的次数小于$f(x)$的次数$n$或$f_1(x) = 0$.

若$f_1(x) = 0$, 取$q(x) = b^{-1}a^{n-m}$, $r(x) = 0$即可;

若$f_1(x) \neq 0$, 则$\partial(f_1(x)) < n$. 由归纳假设, 对$f_1(x)$和$g(x)$, 存在$q_1(x)$, $r_1(x)$使得

$$f_1(x) = q_1(x)g(x) + r_1(x)$$

成立, 其中$\partial(r_1(x)) < \partial(g(x))$或$r_1(x) = 0$. 于是,

$$\begin{aligned} f(x) &= f_1(x) + b^{-1}ax^{n-m}g(x) \\ &= (q_1(x) + b^{-1}ax^{n-m})g(x) + r_1(x) \\ &= q(x)g(x) + r(x), \end{aligned}$$

其中$q(x) = q_1(x) + b^{-1}ax^{n-m}$, $r(x) = r_1(x)$. 自然地, $\partial(r(x)) < \partial(g(x))$.

由归纳法知, $q(x)$, $r(x)$的存在性成立.

再证上述$q(x)$, $r(x)$的唯一性.

若存在另一组$q^o(x)$, $r^o(x)$使得

$$f(x) = q^o(x)g(x) + r^o(x) \tag{1.2.2}$$

成立, 且$\partial(r^o(x)) < \partial(g(x))$或$r^o(x) = 0$. 将(1.2.1)与(1.2.2)两式相减, 得

$$(q(x) - q^o(x))g(x) = r^o(x) - r(x).$$

若$q(x) \neq q^o(x)$, 则

$$\partial((q(x) - q^o(x))g(x)) \geq \partial(g(x)) > \partial(r^o(x) - r(x)).$$

这与上述等式矛盾.

因此必有$q(x) = q^o(x)$. 由此, 又得$r(x) = r^o(x)$. □

由此, 把定理1.2.1前面的具体例子中的$f(x)$和$g(x)$代入公式(1.2.1), 那么它们计算后的表达式恰符合由形式多项式获得的公式(1.2.1). 这说明我们由抽象多项式的方法导出的结论能覆盖非抽象定义的多项式的相应结论.

上述定理中所得到的$q(x)$称为$g(x)$除$f(x)$的**商**, $r(x)$称为$g(x)$除$f(x)$的**余式**. 由定理1.2.1和整除的定义我们不难得出下面的引理.

引理 1.2.2 当$g(x) \neq 0$时, $g(x) \mid f(x)$当且仅当$g(x)$除$f(x)$时的余式为0.

当$g(x)|f(x)$, 且$g(x) \neq 0$ 时, $g(x)$除$f(x)$所得的商$q(x)$ 有时也用$\frac{f(x)}{g(x)}$ 来表示.

需要指出的是, 两个多项式之间的整除性不会因为系数域的扩大而改变. 即:

定理 1.2.3 设$\mathbb{P}$, $\bar{\mathbb{P}}$ 是两个数域, 且$\mathbb{P} \subseteq \bar{\mathbb{P}}$. 设$f(x)$, $g(x) \in \mathbb{P}[x]$, 那么在$\mathbb{P}$中$g(x)|f(x)$ 当且仅当在$\bar{\mathbb{P}}$ 中$g(x)|f(x)$.

证明 若$g(x) = 0$, 则在$\mathbb{P}$ 中$g(x)|f(x)$ 当且仅当$f(x) = 0$, 从而当且仅当在$\bar{\mathbb{P}}$中$g(x)|f(x)$.

若$g(x) \neq 0$, 则由定理1.2.1 的带余除法, 存在唯一的$q(x)$, $r(x) \in \mathbb{P}[x]$, 使得

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

(即定理1.2.1中的(1.2.1)式)成立, 且$\partial(r(x)) < \partial(g(x))$ 或$r(x) = 0$.

显然上述等式在$\bar{\mathbb{P}}[x]$ 中也成立.

因此, 由引理1.2.2, 在$\mathbb{P}[x]$ 中$g(x)|f(x)$ 当且仅当$r(x) = 0$, 从而当且仅当在$\bar{\mathbb{P}}[x]$中$g(x)|f(x)$. □

下面介绍整除性的几个常用性质:

性质 1.2.4 若$f(x)|g(x)$, $g(x)|f(x)$, 则存在非零常数c 使得$f(x) = cg(x)$成立.

证明 由$f(x)|g(x)$, $g(x)|f(x)$知, 分别存在$h_1(x)$, $h_2(x)$使得

$$g(x) = h_1(x)f(x), \text{ 且} f(x) = h_2(x)g(x)$$

成立. 于是

$$f(x) = h_1(x)h_2(x)f(x).$$

如果$f(x) = 0$, 则$g(x) = 0$, 结论显然成立.

如果$f(x) \neq 0$, 则由性质1.1.2 (vi)得$h_1(x)h_2(x) = 1$, 从而$\partial(h_1(x))+\partial(h_2(x)) = 0$. 特别地,

$$\partial(h_2(x)) = 0,$$

故$h_2(x) = c$, 其中$c \in \mathbb{P}$是一个非零常数. □

性质 1.2.5 (整除的传递性) 若$f(x)|g(x)$, $g(x)|h(x)$, 则$f(x)|h(x)$.

证明 存在$g_1(x)$, $h_1(x)$, 使得

$$g(x) = g_1(x)f(x), \ h(x) = h_1(x)g(x)$$

成立, 从而$h(x) = h_1(x)g_1(x)f(x)$, 即$f(x)|h(x)$. □

性质 1.2.6 若$f(x)|g_i(x)(i = 1, 2, \cdots, r)$, 则对任意多项式$u_i(x)(i = 1, 2, \cdots, r)$, 有$f(x)|(u_1(x)g_1(x) + \cdots + u_r(x)g_r(x))$.

证明 由题设, 存在$h_i(x)(i = 1, 2, \cdots, r)$ 使得$g_i(x) = h_i(x)f(x)$成立. 从而

$$\sum_{i=1}^{r} u_i(x)g_i(x) = \left(\sum_{i=1}^{r} u_i(x)h_i(x)\right) f(x),$$

故

$$f(x)|(u_1(x)g_1(x) + \cdots + u_r(x)g_r(x)).$$ □

推论 1.2.7 任一多项式$f(x)$与它的任一非零常数倍$cf(x)(c\neq 0)$有相同的因式和倍式.

因此, 在多项式整除性讨论中, 不妨假设$f(x)$的首项系数为1.

例 1.2.1 设$g(x)=ax+b, a,b\in\mathbb{P}, a\neq 0, f(x)\in\mathbb{P}[x]$, 求证: $g(x)|f(x)^2$的充要条件是$g(x)|f(x)$.

证明 充分性显然成立, 只需证明必要性也成立.

由带余除法, 存在$r\in\mathbb{P}$, 使得$f(x)=g(x)q(x)+r$成立. 所以

$$f(x)^2=g(x)^2q(x)^2+2rg(x)q(x)+r^2.$$

由$g(x)|f(x)^2$得$g(x)|r^2$, 故$r^2=0$, $r=0$, 即$g(x)|f(x)$. □

例 1.2.2 设$f(x), g(x)$及$h(x)\neq 0$为三个多项式. 证明: $h(x)|(f(x)-g(x))$当且仅当$f(x)$与$g(x)$除以$h(x)$所得的余式相等.

证明 由带余除法, 可设

$$f(x)=h(x)q_1(x)+r_1(x),\ g(x)=h(x)q_2(x)+r_2(x),$$

其中$r_i(x)=0$或$\partial(r_i(x))<\partial(h(x)), i=1,2$. 上面二式相减, 得

$$f(x)-g(x)=h(x)[q_1(x)-q_2(x)]+r_1(x)-r_2(x). \tag{1.2.3}$$

由于$\partial(r_i(x))<\partial(h(x))$, 故$\partial(r_1(x)-r_2(x))<\partial(h(x))$. 所以$h(x)$除$f(x)-g(x)$的商为$q_1(x)-q_2(x)$, 余式为$r_1(x)-r_2(x)$.

若$r_1(x)=r_2(x)$, 则由上述(1.2.3)式得

$$f(x)-g(x)=h(x)[q_1(x)-q_2(x)],$$

从而

$$h(x)|(f(x)-g(x)).$$

反之, 若$h(x)|(f(x)-g(x))$, 则由引理1.2.2知 $r_1(x)-r_2(x)=0$, 即$r_1(x)=r_2(x)$. □

习 题 1.2

1. 用带余除法, 求$g(x)$除$f(x)$所得的商$q(x)$与余式$r(x)$.
   (1) $f(x)=x^5-x^3+3x^2-1, g(x)=x^3-3x+2$;
   (2) $f(x)=x^3-3x^2-x-1, g(x)=3x^2-2x+1$;
   (3) $f(x)=x^5-x^3-1, g(x)=x-2$.
2. a,b是什么数时, 下列各题中的$f(x)$能被$g(x)$整除:
   (1) $f(x)=x^4-3x^3+6x^2+ax+b, g(x)=x^2-1$;
   (2) $f(x)=ax^4+bx^3+1, g(x)=(x-1)^2$.
3. 试给出$x^3-3px+2q$被$x^2+2ax+a^2$整除的条件.
4. 设$a\in\mathbb{P}$. 证明: 对任意的正整数n, 有$(x-a)\mid(x^n-a^n)$.
5. 设$f(x)\in\mathbb{P}[x]$, k是任一正整数. 证明: $x\mid f^k(x)$当且仅当$x\mid f(x)$.
6. 把$f(x)$表成$x-x_0$的方幂的和的形式, 即$f(x)=\sum\limits_{i=0}^{+\infty}a_i(x-x_0)^i$:
   (1) $f(x)=5x^4-6x^3+x^2+4, x_0=1$;
   (2) $f(x)=2x^5+5x^4-x^3+10x-6, x_0=-2$.

§1.3 最大公因式

定义 1.3.1 设$f(x)$, $g(x)$, $\varphi(x)$, $d(x) \in \mathbb{P}[x]$.

i) 若$\varphi(x)|f(x)$且$\varphi(x)|g(x)$, 则称$\varphi(x)$是$f(x)$, $g(x)$的一个**公因式**;

ii) 若$d(x)$是$f(x)$, $g(x)$的一个公因式, 且对$f(x)$, $g(x)$的任一公因式$\varphi(x)$均有$\varphi(x)|d(x)$, 则称$d(x)$是$f(x)$, $g(x)$的一个**最大公因式**.

例 1.3.1 (1) 设$f(x) = 2(x-1)^3(x^2+1)$, $g(x) = 4(x-1)^2(x+1)$. 则$f(x)$和$g(x)$的首项系数为1的公因式有1, $x-1$, $(x-1)^2$, 其中$(x-1)^2$是一个最大公因式.

(2) 任一多项式$f(x)$总是它自身和零多项式0的一个最大公因式.

(3) 两个零多项式的最大公因式就是0, 但任一非零多项式都是这两个零多项式的公因式.

注意: 通常, 最大公因式是不唯一的, 比如上述(1) 中, 最大公因式可以是$(x-1)^2$, 也可以是$2(x-1)^2$, 这两个最大公因式相差一个常数倍. 这不是偶然的, 事实上, 我们有:

命题 1.3.1 (唯一性) 两个多项式的最大公因式在可以相差非零常数倍的意义下是唯一确定的.

证明 设$f(x)$, $g(x)$有两个最大公因式$d_1(x)$和$d_2(x)$, 由最大公因式定义知

$$d_1(x)|d_2(x), \quad d_2(x)|d_1(x).$$

故由性质1.2.4知, 存在非零常数c, 使得$d_1(x) = cd_2(x)$成立. □

据此, $f(x)$, $g(x)$的最大公因式或者等于零(当$f(x) = g(x) = 0$), 或者都不等于零(当$f(x) \neq 0$或$g(x) \neq 0$), 我们**约定**用$(f(x), g(x))$表示这一零多项式或其中首项系数为1的那个最大公因式.

上面我们讨论了在最大公因式存在时的唯一性问题, 但更重要的是最大公因式的存在性. 事实上, 任两个多项式的最大公因式是必然存在的. 我们的证明将提供最大公因式的一个具体的求法. 由于方法上依赖于带余除法, 首先我们提出下述事实:

引理 1.3.2 若有等式$f(x) = q(x)g(x) + r(x)$成立, 那么$f(x)$和$g(x)$的(最大)公因式与$g(x)$和$r(x)$的(最大)公因式一致.

证明 若$\varphi(x)|f(x)$且$\varphi(x)|g(x)$, 由已知等式得$r(x) = f(x) - q(x)g(x)$. 从而$\varphi(x)$整除$r(x)$, 即$\varphi(x)$是$g(x)$, $r(x)$的公因式. 反之, 若$\varphi(x)|g(x)$且$\varphi(x)|r(x)$, 由已知等式得$\varphi(x)$整除$f(x)$, 即$\varphi(x)$是$f(x)$, $g(x)$的公因子. 因此, 两组多项式的公因式是一致的.

再由最大公因式的定义, 即有$(f(x), g(x)) = (g(x), r(x))$. □

定理 1.3.3 (存在性) 对于$\mathbb{P}[x]$中任意两个多项式$f(x)$及$g(x)$, 均存在最大公因式$d(x) = (f(x), g(x)) \in \mathbb{P}[x]$, 且存在$u(x)$, $v(x) \in \mathbb{P}[x]$使

$$d(x) = u(x)f(x) + v(x)g(x). \quad \text{(Bezout等式)}$$

证明 当$f(x)$, $g(x)$中至少有一个为零多项式时, 不妨设$g(x) = 0$, 那么$f(x)$就是它们的一个最大公因式. 设$f(x)$的首项系数a_0, 则有

$$d(x) = \frac{1}{a_0}f(x) = \frac{1}{a_0}f(x) + 1 \cdot 0.$$

当$f(x)$, $g(x)$ 均非零时, 由带余除法, 存在商$q_1(x)$, 余式$r_1(x)$使得

$$f(x)=q_1(x)g(x)+r_1(x).$$

若$r_1(x)=0$, 则$f(x)=q_1(x)g(x)$, 这时$g(x)$就是$f(x)$和$g(x)$的最大公因式, 且

$$g(x)=f(x)+(1-q_1(x))g(x).$$

若$r_1(x)\neq 0$, 用$r_1(x)$ 除$g(x)$, 存在商$q_2(x)$, 余式$r_2(x)$ 使得

$$g(x)=q_2(x)r_1(x)+r_2(x).$$

若$r_2(x)=0$, 则$r_1(x)|g(x)$, 从而$r_1(x)$ 是$g(x)$和$r_1(x)$ 的最大公因式. 由引理1.3.2, 它也是$f(x)$, $g(x)$ 的最大公因式.

若$r_2(x)\neq 0$, 用$r_2(x)$ 除$r_1(x)$, 存在商$q_3(x)$, 余式$r_3(x)$, 如此辗转相除下去, 由带余除法知, 所得余式链$r_1(x)$, $r_2(x)$, $\cdots$, 次数不断降低, 即

$$\partial(g(x))>\partial(r_1(x))>\partial(r_2(x))>\cdots$$

因此, 有限次之后, 必有余式$r_{s+1}(x)=0$, 从而得:

$$f(x)=q_1(x)g(x)+r_1(x), \tag{1.3.1}$$
$$g(x)=q_2(x)r_1(x)+r_2(x), \tag{1.3.2}$$
$$r_1(x)=q_3(x)r_2(x)+r_3(x), \tag{1.3.3}$$
$$\vdots \qquad\qquad \vdots$$
$$r_{i-2}(x)=q_i(x)r_{i-1}(x)+r_i(x), \tag{1.3.i}$$
$$\vdots \qquad\qquad \vdots$$
$$r_{s-3}(x)=q_{s-1}(x)r_{s-2}(x)+r_{s-1}(x), \tag{1.3.(s–1)}$$
$$r_{s-2}(x)=q_s(x)r_{s-1}(x)+r_s(x), \tag{1.3.s}$$
$$r_{s-1}(x)=q_{s+1}(x)r_s(x)+0, \tag{1.3.(s+1)}$$

由此, $r_s(x)|r_{s-1}(x)$, 故$r_s(x)$ 是$r_s(x)$ 和$r_{s-1}(x)$ 的一个公因式. 据引理1.3.2, $r_s(x)$ 也是 $r_{s-1}(x)$ 和$r_{s-2}(x)$ 的公因式, 依次倒推上去, $r_s(x)$ 是$f(x)$ 和$g(x)$ 的公因式.

又若$h(x)$是$f(x)$和$g(x)$的一个最大公因式, 由(1.3.1) 式得$h(x)|r_1(x)$; 由(1.3.2)式得$h(x)|r_2(x)$; 依次下去, 由(1.3.s)式得$h(x)|r_s(x)$. 故$r_s(x)$ 是$f(x)$和$g(x)$的最大公因式.

另一方面,

$$\begin{aligned} r_s(x)&=r_{s-2}(x)-q_s(x)r_{s-1}(x)\\ &=r_{s-2}(x)-q_s(x)(r_{s-3}(x)-q_{s-1}(x)r_{s-2}(x))\\ &=-q_s(x)r_{s-3}(x)+(1+q_s(x)q_{s-1}(x))r_{s-2}(x)\\ &=\cdots\cdots\\ &=u(x)f(x)+v(x)g(x), \end{aligned}$$

上述过程是用(1.3.(s−1)), $\cdots$, (1.3.2), (1.3.1)逐个地消去$r_{s-2}(x)$, $\cdots$, $r_2(x)$, $r_1(x)$等, 再并项得到$u(x)$和$v(x)$.

令$r_s(x)$的首项系数为$c\neq 0$, 则

$$(f(x),\ g(x))=\frac{1}{c}r_s(x),\quad \frac{1}{c}r_s(x)=\frac{1}{c}u(x)f(x)+\frac{1}{c}v(x)g(x). \qquad \square$$

上述定理证明中通过(1.3.1), $\cdots$, (1.3.s), (1.3.(s + 1)) 式, 求出最大公因式$r_s(x)$

的方法称为**辗转相除法**. 可按下面格式来操作. 例如:

例 1.3.2 设$f(x) = x^4 + 3x^3 - x^2 - 4x - 3$, $g(x) = 3x^3 + 10x^2 + 2x - 3$. 求$(f(x),\ g(x))$, 并求$u(x)$, $v(x)$使得$(f(x),\ g(x)) = u(x)f(x) + v(x)g(x)$成立.

用辗转相除法的格式来操作, 可写为:

	$g(x)$	$f(x)$	
$q_2(x) =$	$3x^3+10x^2+2x-3$	$x^4+3x^3-x^2-4x-3$	$\frac{1}{3}x-\frac{1}{9}$
$-\frac{27}{5}x+9$	$3x^3+15x^2+18x$	$x^4+\frac{10}{3}x^3+\frac{2}{3}x^2-x$	$=q_1(x)$
	$-5x^2-16x-3$	$-\frac{1}{3}x^3-\frac{5}{3}x^2-3x-3$	
	$-5x^2-25x-30$	$-\frac{1}{3}x^3-\frac{10}{9}x^2-\frac{2}{9}x+\frac{1}{3}$	
	$r_2(x)=9x+27$	$r_1(x)=-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}$	$-\frac{5}{81}x-\frac{10}{81}$
		$-\frac{5}{9}x^2-\frac{5}{3}x$	$=q_3(x)$
		$-\frac{10}{9}x-\frac{10}{3}$	
		$-\frac{10}{9}x-\frac{10}{3}$	
		0	

用等式写出来, 为:

$$\begin{aligned} f(x)&=(\frac{1}{3}x-\frac{1}{9})g(x)+(-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}),\\ g(x)&=(-\frac{27}{5}x+9)(-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3})+(9x+27),\\ -\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}&=(-\frac{5}{81}x-\frac{10}{81})(9x+27). \end{aligned}$$

因此, $9x+27$ 是$f(x), g(x)$ 的最大公因式, 故$(f(x),\ g(x)) = x + 3$.

又, 由

$$\begin{aligned} 9x+27&=g(x)-(-\frac{27}{5}x+9)(-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3})\\ &=g(x)-(-\frac{27}{5}x+9)(f(x)-(\frac{1}{3}x-\frac{1}{9})g(x))\\ &=(\frac{27}{5}x-9)f(x)+(-\frac{9}{5}x^2+\frac{18}{5}x)g(x) \end{aligned}$$

得

$$(f(x),\ g(x)) = (\frac{3}{5}x-1)f(x)+(-\frac{1}{5}x^2+\frac{2}{5}x)g(x).$$

定义 1.3.2 $\mathbb{P}[x]$ 中两个多项式$f(x)$, $g(x)$ 称为**互素(或互质)** 的, 若$(f(x),\ g(x)) = 1$.

由定义知, 两个多项式互素当且仅当它们除零次多项式外没有其他的公因式.

下面的定理刻画了两个多项式互素的特征:

定理 1.3.4 $\mathbb{P}[x]$ 中两个多项式$f(x)$, $g(x)$ 互素的充要条件是存在$u(x)$, $v(x) \in \mathbb{P}[x]$, 使得$u(x)f(x) + v(x)g(x) = 1$成立.

证明 **必要性:** 由定理1.3.3 直接得.

充分性: 设有$u(x),\ v(x)\in\mathbb{P}[x]$ 使$u(x)f(x)+v(x)g(x)=1$成立. 令$(f(x),\ g(x))=d(x)$, 则$d(x)|f(x),\ d(x)|g(x)$, 从而$d(x)|(u(x)f(x)+v(x)g(x))$, 于是$d(x)|1$. 由性质1.2.4可知, $d(x)$ 是非零常数. □

注 一般情况下, 对于多项式$f(x),\ g(x)\in\mathbb{P}[x]$, 即使存在多项式$u(x),\ v(x),\ d(x)\in\mathbb{P}[x]$ 使得$u(x)f(x)+v(x)g(x)=d(x)$成立，我们也不能断定$d(x)$是$f(x),\ g(x)$的一个最大公因式. 但是, 如果此时我们已知$d(x)$是$f(x),\ g(x)$的一个公因式，那么$d(x)$一定是$f(x),\ g(x)$的一个最大公因式.

对于多个多项式$f_1(x),\cdots,\ f_s(x)(s\geq 2)$, 从最大公因式的定义到性质刻画, 都是类似的. 我们下面列出, 不加以证明.

称$\varphi(x)\in\mathbb{P}[x]$为$f_1(x),\cdots,\ f_s(x)$ 的**公因式**, 若$\varphi(x)|f_i(x)(i=1,\cdots,\ s)$; 设$d(x)$是$f_1(x),\cdots,f_s(x)$ 的公因式, 且对任一其他公因式$\varphi(x)$ 都有$\varphi(x)|d(x)$, 那么就称$d(x)$是$f_1(x),\cdots,f_s(x)$ 的**最大公因式**. 当$d(x)$是零多项式或首项系数为1的多项式时, 表示为:

$$d(x)=(f_1(x),\cdots,f_s(x)).$$

多个多项式的最大公因式的关键是有下面的递推关系:

$$(f_1(x),\cdots,\ f_{s-1}(x),\ f_s(x))=((f_1(x),\cdots,\ f_{s-1}(x)),\ f_s(x)).$$

事实上, 令

$$(f_1(x),\cdots,\ f_{s-1}(x))=d(x),\ (d(x),\ f_s(x))=h(x),$$

那么

$$h(x)|f_s(x),\ h(x)|d(x),\ \text{而}d(x)|f_i(x),\ i=1,\cdots,\ s-1,$$

从而

$$h(x)|f_i(x)\ \ (i=1,\cdots,\ s-1,\ s).$$

设$\varphi(x)$ 是$f_1(x),\ \cdots,\ f_s(x)$ 的公因式, 那么$\varphi(x)|f_i(x)\ \ (i=1,\cdots,\ s-1,\ s)$, 从而$\varphi(x)|d(x)$. 又, $\varphi(x)|f_s(x)$, 故$\varphi(x)|h(x)$. 因此, $h(x)=(f_1(x),\cdots,\ f_s(x))$.

由此递推关系, 即可得到多个多项式的最大公因式的存在性以及存在多项式$u_1(x),\cdots,\ u_s(x)\in\mathbb{P}[x]$, 使得

$$u_1(x)f_1(x)+\cdots+u_s(x)f_s(x)=(f_1(x),\cdots,\ f_s(x))$$

成立.

一般地, 对满足$1<t_1<t_2<\cdots<t_l<s$的正整数$t_1,t_2,\cdots,t_l$, 有:

$$\begin{aligned}&((f_1(x),\cdots,f_{t_1}(x)),(f_{t_1+1}(x),\cdots,f_{t_2}(x)),\cdots,(f_{t_l+1}(x),\cdots,f_s(x)))\\&=(f_1(x),\cdots,\ f_{s-1}(x),\ f_s(x)).\end{aligned}$$

当$((f_1(x),\cdots,\ f_s(x))=1$时, 称$f_1(x),\cdots,\ f_s(x)$ 是**互素**(或**互质**)的.

注意: $f_1(x),\cdots,\ f_s(x)$ 互素时, 它们未必两两互素. 反之, 当$f_1(x),\cdots,\ f_s(x)$ 两两互素时, $f_1(x),\cdots,\ f_s(x)$ 必然是互素的.

对多个多项式的情况, 类似于定理1.3.4的结论也成立, 请读者自证.

现在给出与最大公因式有关的一些基本结论.

命题 1.3.5 若$(f(x),\ g(x))=1$ 且$f(x)|g(x)h(x)$, 那么$f(x)|h(x)$.

证明 由定理1.3.3, 存在$u(x),\ v(x)\in\mathbb{P}[x]$使得$u(x)f(x)+v(x)g(x)=1$成立, 从

而

$$u(x)f(x)h(x)+v(x)g(x)h(x)=h(x).$$

因为$f(x)|g(x)h(x)$, 所以

$$f(x)|(u(x)f(x)h(x)+v(x)g(x)h(x)),$$

从而$f(x)|h(x)$. □

命题 1.3.6 若$(f_1(x),f_2(x))=1$且$f_1(x)|g(x),f_2(x)|g(x)$. 那么, $f_1(x)f_2(x)|g(x)$.

证明 由 $f_1(x)|g(x)$ 知, 存在 $h_1(x)$ 使得 $g(x)=f_1(x)h_1(x)$; 又由$f_2(x)|g(x)$知, $f_2(x)|(f_1(x)h_1(x))$. 由命题1.3.5知$f_2(x)|h_1(x)$, 所以存在$h_2(x)$, 使得$h_1(x)=f_2(x)h_2(x)$成立. 于是将此式代入前式可得$g(x)=f_1(x)f_2(x)h_2(x)$, 故$(f_1(x)f_2(x))|g(x)$. □

与最大公因式对偶的一个概念是最小公倍式. 多项式$m(x)$称为多项式$f(x)$和$g(x)$的**最小公倍式**, 如果:

1) $m(x)$是$f(x),g(x)$的公倍式, 即$f(x)|m(x),\ g(x)|m(x)$;

2) $f(x),g(x)$ 的任一个公倍式$h(x)$都是$m(x)$的倍式, 即$m(x)|h(x)$.

在不考虑首项系数的情况下, 由定义直接可得最小公倍式的唯一性. 关于存在性, 我们由下面叙述即可知.

事实上, 当$f(x),g(x)$不全为0时, 则$(f(x),\ g(x))\neq 0$且$(f(x),\ g(x))|f(x)g(x)$. 这时可证明$\dfrac{f(x)g(x)}{(f(x),\ g(x))}$是$f(x),g(x)$的最小公倍式(见本节习题第4题, 请读者自己完成证明). 据此, 我们以$[f(x),\ g(x)]$表示$f(x)$和$g(x)$的或为零或为首项系数为1的那个唯一的最小公倍式. 从而, 我们知道, 当$f(x),g(x)$ 的首项系数为1时,

$$[f(x),\ g(x)]=\frac{f(x)g(x)}{(f(x),\ g(x))}.$$

例 1.3.3 若$f(x)$和$g(x)$互素, 求证: $f(x^m)$和$g(x^m)$也互素.

证明 因为$f(x)$和$g(x)$互素, 存在多项式$u(x),\ v(x)$, 使得

$$f(x)u(x)+g(x)v(x)=1$$

成立. 故$f(x^m)u(x^m)+g(x^m)v(x^m)=1$, 即$f(x^m)$和$g(x^m)$互素. □

例 1.3.4 若$(f(x),\ g(x))=d(x)$, 求证: $(f(x^m),\ g(x^m))=d(x^m)$.

证明 因为$(f(x),\ g(x))=d(x)$, 存在多项式$u(x),\ v(x)$, 使得

$$f(x)u(x)+g(x)v(x)=d(x),\ d(x)|f(x),\ d(x)|g(x)$$

成立. 故

$$f(x^m)u(x^m)+g(x^m)v(x^m)=d(x^m),\ d(x^m)|f(x^m),\ d(x^m)|g(x^m),$$

即$(f(x^m),\ g(x^m))=d(x^m)$. □

例 1.3.5 (i) 对$f(x),g(x),h(x)\in\mathbb{P}[x]$, 设有$(f(x),g(x))=1$, $(f(x),h(x))=1$, 则

$$(f(x),g(x)h(x))=1;$$

(ii) 设$f_1(x),\cdots,f_m(x),g_1(x),\cdots,g_n(x)\in\mathbb{P}[x]$, 则

$$(f_1(x)\cdots f_m(x),\ g_1(x)\cdots g_n(x))=1$$

当且仅当对任意$i=1,\cdots,m;\ j=1,2,\cdots n$均有$(f_i(x),g_j(x))=1$.

证明 (i) 由已知, 存在$u(x),v(x),s(x),t(x)\in\mathbb{P}[x]$使得

$$u(x)f(x)+v(x)g(x)=1,\ s(x)f(x)+t(x)h(x)=1$$

成立, 两式相乘, 得:

$$\big(u(x)s(x)f(x)+v(x)g(x)s(x)+u(x)t(x)h(x)\big)f(x)+\big(v(x)t(x)\big)\big(g(x)h(x)\big)=1.$$

由定理1.3.4, $(f(x),g(x)h(x))=1$.

(ii) 先证必要性. 因为

$$(f_1(x)\cdots f_m(x),\ g_1(x)\cdots g_n(x))=1,$$

所以存在$u(x),v(x)\in\mathbb{P}[x]$, 使得

$$u(x)f_1(x)\cdots f_m(x)+v(x)g_1(x)\cdots g_n(x)=1$$

成立. 可得

$$f_i(x)p_i(x)+g_j(x)q_j(x)=1,$$

其中

$$p_i(x)=u(x)f_1(x)\cdots f_{i-1}(x)f_{i+1}(x)\cdots f_m(x),$$
$$q_j(x)=v(x)g_1(x)\cdots g_{j-1}(x)g_{j+1}(x)\cdots g_n(x).$$

这意味着

$$(f_i(x),g_j(x))=1,(i=1,2,\cdots,m;\ j=1,2,\cdots,n).$$

再证充分性.

因为$(f_1(x),g_j(x))=1,\quad (j=1,2,\cdots,n)$, 所以由$(i)$得:

$$(f_1(x),g_1(x)\cdots g_n(x))=1.$$

同理

$$(f_2(x),g_1(x)\cdots g_n(x))=1,\cdots,(f_m(x),g_1(x)\cdots g_n(x))=1.$$

所以

$$(f_1(x)f_2(x)\cdots f_m(x),g_1(x)g_2(x)\cdots g_n(x))=1.$$ □

习 题 1.3

1. 设$f(x)=4x^4-2x^3-16x^2+5x+9,\ g(x)=2x^3-x^2-5x+4$. 求$(f(x),\ g(x))$, 并求$u(x),v(x)$, 使得$u(x)f(x)+v(x)g(x)=(f(x),\ g(x))$成立.
2. 设$f(x)=x^3+(1+t)x^2+2x+2u,\ g(x)=x^3+tx+u$的最大公因式是二次多项式, 求$t,\ u$.
3. 设$(f_1(x),f_2(x))=d(x)\neq 0$. 证明: $\left(\dfrac{f_1(x)}{d(x)},\dfrac{f_2(x)}{d(x)}\right)=1$.
4. 用最小公倍式的定义证明: 如果$f(x)$与$g(x)$都是首项系数为1的多项式, 则
$$[f(x),\ g(x)](f(x),\ g(x))=f(x)g(x).$$
5. 设$\mathbb{P}[x]$ 中两个非零多项式$f(x)$及$g(x)$互素，证明存在唯一的$u(x),\ v(x)\in\mathbb{P}[x]$，满足$\partial(u(x))<\partial(g(x)),\partial(v(x))<\partial(f(x))$，使
$$u(x)f(x)+v(x)g(x)=1.$$

§1.4 因式分解

多项式的一个核心问题，就是讨论因式分解，即将一个多项式表达为同样数域上的若干个多项式的乘积. 在这方面我们在中学代数中已学过一些具体方法，使得一个多项式分解为“不能再分”的因式的乘积. 但那时对这个问题的讨论是不深入的，所谓的“不能再分”，常常只是看不出怎样“分”下去的意思，而不是严格地论证确实“不可再分”的. 其实是否能再分解常常是相对于所在数域而言的，例如x^4-4, 在$\mathbb{Q}$上，$x^4-4=(x^2-2)(x^2+2)$就不能再分了；但在数域$\mathbb{P}=\mathbb{Q}(\sqrt{2})$，或更大的数域$\mathbb{R}$上，可再分解为$x^4-4=(x-\sqrt{2})(x+\sqrt{2})(x^2+2)$，进一步，在$\mathbb{C}$上，还可再分解为$x^4-4=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}i)(x+\sqrt{2}i)$.

因此，只有明确所在系数域后，才能确定是否可再分解.

在下面讨论中，我们选定一个数域$\mathbb{P}$作为系数域，然后研究$\mathbb{P}[x]$中多项式的因式分解.

定义 1.4.1 设$p(x)\in\mathbb{P}[x]$且$\partial(p(x))\geqslant 1$，若$p(x)$不能表成$\mathbb{P}[x]$中两个次数小于$p(x)$的多项式之积，就称$p(x)$是$\mathbb{P}$**上的不可约多项式**. 常数项多项式我们排除在不可约多项式之外.

比如，$\mathbb{P}$上的一次多项式总是不可约的. x^2+2是$\mathbb{R}$上不可约多项式，但在$\mathbb{C}$上不是不可约的. 从例子看出，一个多项式是否不可约依赖于它所在的系数域.

由定义可见，一个多项式是不可约的当且仅当它的因式只有非零常数和它自身的非零常数倍. 据此可得:

性质 1.4.1 若$p(x)\in\mathbb{P}[x]$是不可约多项式，则对任一$f(x)\in\mathbb{P}[x]$，或者$(p(x),\ f(x))=1$或者$p(x)|f(x)$.

证明 令$(p(x),\ f(x))=d(x)$，则$d(x)|p(x)$，从而$d(x)$或者是1或者是$cp(x)$，这里$c\in\mathbb{P}$是一个非零常数.

若$d(x)=1$，则 $(p(x),\ f(x))=1$ 成立.

若$d(x)\neq 1$，则$d(x)=cp(x)$，故$p(x)|d(x)$，而$d(x)|f(x)$，于是$p(x)|f(x)$. □

性质 1.4.2 设$p(x)\in\mathbb{P}[x]$是不可约的，$f(x),\ g(x)\in\mathbb{P}[x]$，那么当$p(x)|f(x)g(x)$时，必$p(x)|f(x)$或$p(x)|g(x)$.

证明 若$p(x)\nmid f(x)$，由性质1.4.1知，$(p(x),\ f(x))=1$；由命题1.3.5知，$p(x)|g(x)$.□

推论 1.4.3 设$p(x)\in\mathbb{P}[x]$是不可约的，$f_i(x)\in\mathbb{P}[x](i=1,\cdots,s)$，那么当$p(x)$整除$f_1(x)\cdots f_s(x)$ 时，必存在某i使得$p(x)|f_i(x)$成立.

关于多项式因式分解的最关键性质是如下的主要结论:

定理 1.4.4 (因式分解及唯一性定理) 设$f(x)$是数域$\mathbb{P}$上的多项式且其次数≥ 1. 则

(i) $f(x)$可以分解成数域$\mathbb{P}$上的有限个不可约多项式的乘积;

(ii) 如果不计零次因式的差异，$f(x)$分解成数域$\mathbb{P}$上的有限个不可约多项式的乘积

时, 其分解式是唯一的. 即, 如果

$$f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_t(x),$$

其中$p_i(x)$, $q_j(x)$ $(i,\ j=1,\ 2,\ \cdots,\ s)$均为不可约的, 那么$s=t$且适当排列因式的次序后有$p_i(x)=c_iq_i(x)$ $(i=1,\ 2,\ \cdots,\ s)$, 其中$c_i\in\mathbb{P}, c_i\neq 0$ $(i=1,\ 2,\ \cdots,\ s)$.

证明 (i) 对$\partial(f(x))=k$作数学归纳法. 当$\partial(f(x))=1$时, $f(x)$是一次多项式, 故$f(x)$是不可约的.

假设$\partial(f(x))<k$时, 结论成立. 下面考虑$\partial(f(x))=k$时的情况.

如果$f(x)$已是不可约的, 结论自然成立.

如果$f(x)$不是不可约的, 那么存在$f_1(x)$, $f_2(x)\in\mathbb{P}[x]$使得$f(x)=f_1(x)f_2(x)$成立, 且满足$\partial(f_1(x))<k$, $\partial(f_2(x))<k$. 由归纳假设, $f_1(x)$和$f_2(x)$分别可分解为$\mathbb{P}$上不可约多项式之积, 从而得到$f(x)$的分解.

(ii) 设

$$f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_t(x),$$

其中$p_i(x)$, $q_j(x)\in\mathbb{P}[x], (i=1,\cdots,s; j=1,\cdots,t)$均为不可约多项式. 对$s$作归纳法证明.

当$s=1$时, $f(x)$是不可约多项式, 由不可约多项式定义, 必有$t=1$, 从而

$$f(x)=p_1(x)=q_1(x).$$

假设$s=l-1$时结论成立. 考虑$s=l$时的情况, 即:

$$f(x)=p_1(x)\cdots p_{l-1}(x)p_l(x)=q_1(x)\cdots q_t(x).$$

这时$p_l(x)|q_1(x)\cdots q_t(x)$, 由推论1.4.3, 不妨设$p_l(x)|q_t(x)$, 但$q_t(x)$也不可约, 故存在$c_t\in\mathbb{P}(c_t\neq 0)$使得$p_l(x)=c_tq_t(x)$成立. 于是,

$$p_1(x)\cdots p_{l-1}(x)=c_t^{-1}q_1(x)\cdots q_{t-1}(x).$$

由归纳假设知, $l-1=t-1$即$l=t$, 并且适当排列次序后有非零常数c_1, $\cdots$, c_{l-1} 使得

$$p_1(x)=c_1c_t^{-1}q_1(x),\ p_2(x)=c_2q_2(x),\ \cdots,\ p_{l-1}(x)=c_{l-1}q_{l-1}(x)$$

成立. □

在上述定理的不可约分解式中, 某些不可约因式相互间可能仅差一个常数项. 把它的首项系数提出, 那么它们就成为相等的首项系数为1的因式. 再把相同的不可约因式合并, 于是$f(x)$的分解式可写成

$$f(x)=cp_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x),$$

其中$0\neq c\in\mathbb{P}$是$f(x)$的首项系数, $p_i(x)(i=1,\ \cdots,\ s)$均为不同的首项系数为1的不可约多项式, r_1, $\cdots$, r_s是正整数. 上述分解式称为$f(x)$的**标准分解式**.

如果我们已知多项式$f(x)$和$g(x)$的标准分解式, 则可以直接写出它们的最大公因式和最小公倍式. 事实上, 令

$$f(x)=ap_1^{r_1}(x)p_2^{r_2}(x)\cdots p_u^{r_u}(x),\quad g(x)=bp_1^{s_1}(x)p_2^{s_2}(x)\cdots p_u^{s_u}(x),$$

其中$p_i(x)$是不可约的, $r_i,\ s_i\geq 0$ $(i=1,\ \cdots,\ u)$且$r_i,\ s_i$至少有一个是非零的. 那么,

$$(f(x),\ g(x))=p_1^{t_1}(x)p_2^{t_2}(x)\cdots p_u^{t_u}(x),$$

$$[f(x),\ g(x)] = p_1^{k_1}(x)p_2^{k_2}(x)\cdots p_u^{k_u}(x),$$

其中$t_i = \min\{r_i,\ s_i\},\ k_i = \max\{r_i,\ s_i\}$对$i = 1, \cdots, u$.

于是, 得关系式:

$$(f(x), g(x))[f(x), g(x)] = f(x)g(x).$$

这恰好是前面提到过的两个多项式的最大公因式和最小公倍式的关系.

下面讨论不可约多项式为重因式的刻画问题.

定义 1.4.2 (i) 对$f(x),\ p(x) \in \mathbb{P}[x]$, 其中$p(x)$是不可约的, 若$p^k(x)|f(x)$且$p^{k+1}(x) \nmid f(x)$, 则称$p(x)$是$f(x)$的$k$-**重因式**.

(ii) 上述k的情形: 若$k = 0$, 则$p(x)$不是$f(x)$的因式; 若$k = 1$, 称$p(x)$是$f(x)$的**单因式**; 若$k > 1$, 称$p(x)$是$f(x)$的**重因式**.

如果能直接写出$f(x)$的标准分解式$f(x) = cp_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x)$, 当然马上知道$p_i(x)$是否重因式了. 但问题是, 通常未必有办法写出标准分解式. 因此有必要在没给出分解式的情况下, 给出判别某不可约因式是否重因式的方法.

为此, 我们需引入多项式微分(或称导数)的概念.

设

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{P}[x],$$

则定义

$$f'(x) = a_n n x^{n-1} + a_{n-1}(n-1)x^{n-2} + \cdots + a_1,$$

称$f'(x)$是$f(x)$的**微商**(也称**导数**). 进一步, 我们可定义**高阶微商**,

$$f''(x) = (f'(x))',\ \cdots,\ f^{(k)}(x) = (f^{(k-1)}(x))'.$$

显然, 当$\partial(f(x)) = n$, 则

$$\partial(f'(x)) = n-1,\ \partial(f''(x)) = n-2,\ \cdots,\ \partial(f^{(n)}(x)) = 0,\ \partial(f^{(n+1)}(x)) = -\infty,$$

即: $f(x)$的n阶微商为常数, $n+1$阶微商为0.

由定义直接看出, 把$f(x)$看作一个可导函数, 那么$f'(x)$和微积分中导数的定义导出的公式是一致的. 但它的定义的意义和可导函数的微商意义是不同的, 在这里只能看作是一个形式的定义. 即使如此, 由于微分定义的形式的一致, 由此导出的一些关系也是一样的. 比如, 直接验证即可得出如下基本公式:

$$\begin{aligned}
&(f(x)+g(x))' = f'(x)+g'(x);\\
&(cf(x))' = cf'(x);\\
&(f(x)g(x))' = f'(x)g(x)+f(x)g'(x);\\
&(f^m(x))' = mf^{m-1}(x)f'(x).
\end{aligned}$$

有意思的是, 虽然微商定义对多项式只是形式的, 但是却可用于刻画多项式的实际问题, 比如下面刻画是否有重因式的问题.

定理 1.4.5 (i) 在$\mathbb{P}[x]$中, 若不可约多项式$p(x)$是$f(x)$的k-重因式($k \geq 1$), 那么它是微商$f'(x)$的$(k-1)$-重因式;

(ii) 反之, 若不可约多项式$p(x)$是$f'(x)$的$(k-1)$-重因式同时也是$f(x)$的因式, 则$p(x)$是$f(x)$的k-重因式.

证明 (i) 由假设, 存在$g(x) \in \mathbb{P}[x]$使得$f(x) = p^k(x)g(x)$, 但$p(x) \nmid g(x)$. 于是

$$f'(x) = p^{k-1}(x)\big(kg(x)p'(x) + p(x)g'(x)\big),$$

从而

$$p^{k-1}(x)|f'(x).$$

又, 因为$p(x)\nmid g(x)$且$p(x)\nmid p'(x)$, 所以$p(x)\nmid g(x)p'(x)$, 从而

$$p(x)\nmid (kg(x)p'(x)+p(x)g'(x)).$$

因此$p^k(x)\nmid f'(x)$, 即$p(x)$是$f'(x)$的$(k-1)$-重因式.

(ii) 因为$p(x)$是$f(x)$的因式, 可设$p(x)$是s-重因式, $s\geq 1$. 那么由(i), $p(x)$是$f'(x)$的$(s-1)$-重因式. 于是, $s-1=k-1$, 从而$s=k$. □

推论 1.4.6 如果不可约多项式$p(x)$是$f(x)$的k-重因式$(k\geq 1)$, 则$p(x)$分别是$f(x)$, $f'(x)$, $\cdots$, $f^{(k-1)}(x)$ 的k-重, $(k-1)$-重, $\cdots$, 1-重因式, 但不是$f^{(k)}(x)$的因式.

说明: 定理1.4.5 (ii)中若没有条件"$p(x)$同时也是$f(x)$的因式", 一般是导不出"$p(x)$是$f(x)$的k-重因式"的. 例如, $f(x)=(x+1)^2(x-1)$, $f'(x)=(3x-1)(x+1)$, 其中$3x-1$是$f'(x)$的单重因式, 但不是$f(x)$的因式, 更不是2-重因式.

推论 1.4.7 不可约多项式$p(x)$是多项式$f(x)$的重因式当且仅当$p(x)$是$f(x)$和$f'(x)$的公因式.

证明 当 $p(x)$是 $f(x)$的k-重因式 $(k>1)$, 则 $p(x)$是 $f'(x)$的$(k-1)$-重因式, 从而 $p(x)$是 $f(x)$和$f'(x)$的公因式.

反之, 若 $p(x)|(f(x),\ f'(x))$, 设 $p(x)$是 $f(x)$的k-重因式, 那么是 $f'(x)$的$(k-1)$-重因式. 于是 $k-1\geq 1$, 故 $k\geq 2$. □

推论 1.4.8 多项式$f(x)$没有重因式当且仅当$f(x)$与$f'(x)$ 互素.

证明 由推论1.4.7直接得. □

由推论1.4.8知, 判别多项式$f(x)$有无重因式, 只需通过辗转相除法求出$f(x)$和$f'(x)$的最大公因式即可. 这是机械的方法.

另一方面, 用这种方法可以由一个多项式找出和它有相同因式但没有重因式的对应多项式. 事实上, 令

$$f(x)=cp_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x)\ \ (c\in\mathbb{P},\ r_1,\ \cdots,\ r_s\geq 1).$$

由定理1.4.5可得,

$$(f(x),\ f'(x))=p_1^{r_1-1}(x)p_2^{r_2-1}(x)\cdots p_s^{r_s-1}(x),$$

于是

$$\frac{f(x)}{(f(x),\ f'(x))}=cp_1(x)p_2(x)\cdots p_s(x)$$

是无重因式的.

习 题 1.4

1. 设在$\mathbb{P}[x]$中有不全为零的多项式$g_1(x),g_2(x),\cdots,g_s(x)$, $d(x)$是这些多项式的一个公因式, 且在$\mathbb{P}[x]$中有分解式

   $$g_j(x)=d(x)h_j(x), j=1,2,\cdots,s.$$

   证明: $d(x)$是$g_1(x)$, $g_2(x)$, $\cdots$, $g_s(x)$的一个最大公因式当且仅当$h_1(x),h_2(x),\cdots,h_s(x)$互素.

2. 证明: $(f(x),\ g(x))=1$的充要条件是$(f(x)g(x),\ f(x)+g(x))=1$.
3. 证明: 如果$(f(x),\ g(x))=1,\ (f(x),\ h(x))=1$, 那么$(f(x),\ g(x)h(x))=1$. 该结论能推广吗? 为什么?
4. 设$f(x),\ g(x),\ h(x)$是任意多项式, 且$f(x)\neq 0$.
   (1) 证明: 若$(f(x),\ g(x))=1$则$(f(x),\ g(x)h(x))=(f(x),\ h(x))$.
   (2) 问: 上述结论反之是否成立?
5. 设$f(x),\ g(x),\ h(x)\in\mathbb{P}[x]$, 且$(f(x),\ g(x))=1$. 证明: 若$f(x)$与$g(x)$都整除$h(x)$, 那么$f(x)g(x)$也整除$h(x)$. 此结论能推广吗? 为什么?
6. 证明: 两个非零多项式的一个公因式是最大公因式当且仅当这个公因式是次数最大的公因式.

§1.5 重根和多项式函数

对于$f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbb{P}[x]$, 我们可定义$\mathbb{P}$上的函数$f:\mathbb{P}\to\mathbb{P}$使得$\alpha\mapsto f(\alpha)=a_n\alpha^n+\cdots+a_1\alpha+a_0$, 称之为$\mathbb{P}$上的一个**多项式函数**. 当$\mathbb{P}$是实域或复域时, 此多项式函数$f$分别是实分析和复分析研究的对象. 注意: $f(x)=\sum a_ix^i$中的加法和数乘是形式的; 但$f(\alpha)=\sum a_i\alpha^i$ 中的加法、乘法和数乘都是$\mathbb{P}$的加法和乘法.

虽然$f(x)$是抽象地定义的多项式, x只是一个文字, 但与此多项式函数f有着非常密切的关系. 我们可以借助此$\mathbb{P}$上函数f来刻画说明多项式$f(x)$的结构. 首先, 我们有:

引理 1.5.1 *对$f(x),\ g(x)\in\mathbb{P}[x]$, 若$f(x)=g(x)$, 那么作为$\mathbb{P}$上函数, $f=g$.*

证明 只要证明当$f(x)=0$时, $\mathbb{P}$上函数$f=0$.

令$f(x)=a_nx^n+\cdots+a_1x+a_0$. 由$f(x)=0$, 则$a_i=0$, 对$i=0,\ 1,\ \cdots,\ n$. 从而对任何$\alpha\in\mathbb{P}$, $f(\alpha)=\sum a_i\alpha=0$, 即$f=0$. □

因此, 当$h_1(x)=f(x)+g(x),\ h_2(x)=f(x)g(x)$时, 自然有: 对$\alpha\in\mathbb{P}$,

$$h_1(\alpha)=f(\alpha)+g(\alpha),\quad h_2(\alpha)=f(\alpha)g(\alpha).$$

对一个多项式, 一次因式如果存在当然是最简单的不可约因式. 它们直接和多项式的根联系在一起. 首先, 我们有:

定理 1.5.2 (余数定理) *对任一$f(x)\in\mathbb{P}[x],\ \alpha\in\mathbb{P}$, 用$x-\alpha$去除多项式$f(x)$, 所得余式必为常数, 且此常数等于函数值$f(\alpha)$.*

证明 由带余除法, 存在$q(x),\ r(x)\in\mathbb{P}[x]$, 使得$f(x)=(x-\alpha)q(x)+r(x)$成立, 其中$\partial(r(x))<\partial(x-\alpha)=1$, 从而$r(x)=c$为一个常数项多项式. 于是, 由引理1.5.1,

$$f(\alpha)=(\alpha-\alpha)q(\alpha)+c=c.$$ □

据此, 我们得

推论 1.5.3 *对$f(x)\in\mathbb{P}[x],\ \alpha\in\mathbb{P},\ (x-\alpha)|f(x)$ 当且仅当$f(\alpha)=0$.*

当多项式函数f在α处值为0, 即$f(\alpha)=0$时, 我们称α是多项式$f(x)$的一个**根**或**零点**.

对一般不可约多项式前面已经有重因式的概念. 对一次因式是重因式的情况, 我们就有重根的概念, 即: 当$x-\alpha$是$f(x)$的$k-$重因式, 称α是$f(x)$的k-**重根**. 当$k=1$时, 称α是**单根**; 当$k\geq 2$时, α称为**重根**.

例 1.5.1 设u是复数域中的某个数, 若u是某个有理系数多项式(或整系数多项式) $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$的根, 则称$u$是一个**代数数**. 证明: 对任一代数数$u$, 存在唯一的次数最小的首一有理不可约多项式$g(x)$, 使得$g(u)=0$. 这时, $g(x)$被称为u的**最小多项式**或**极小多项式**.

证明 存在性显然, 只需证明唯一性. 若$h(x)$是另一个最小多项式, 假设

$$h(x)=g(x)q(x)+r(x),\quad \partial(r(x))<\partial(g(x)),$$

则由$h(u)=g(u)=0$, 可知$r(u)=0$. 若$r(x)\neq 0$, 则与$g(x)$是最小多项式矛盾(u适合一个次数比$g(x)$更小的多项式$r(x)$). 因此$r(x)=0$, 即$g(x)|h(x)$. 再因为$h(x)$也是最小多项式, $h(x)$和$g(x)$次数相等且只差一个常数, 而它们又都是首一的, 所以只能相等, 唯一性得证. □

正如前面已经提到, 求解一元多项式的根是多项式理论发展的基本动力. 关于根的存在性, 下一节我们会再讨论. 现在先给出根的个数的一个估计.

定理 1.5.4 $\mathbb{P}[x]$中n次多项式$f(x)(n\geq 0)$在数域$\mathbb{P}$中的根不可能多于n个(重根按重数计算).

证明 当$\partial(f(x))=0$, 根的个数当然是零个.

当$\partial(f(x))\neq 0$, 设$\alpha_1,\cdots,\alpha_s$分别是$f(x)$的$r_1,\cdots,r_s$-重根且$\alpha_i\neq\alpha_j$, 对任何$i\neq j$, 则对任何i, $(x-\alpha_i)^{r_i}\mid f(x)$. 于是, 由$((x-\alpha_i)^{r_i},(x-\alpha_j)^{r_j})=1$对任何$i,j$, 导出

$$(x-\alpha_1)^{r_1}\cdots(x-\alpha_s)^{r_s}\mid f(x),$$

这意味着$r_1+\cdots+r_s\leq\partial(f(x))$. □

再回到多项式与它的多项式函数的关系, 考虑引理1.5.1的逆命题, 即, 当$f=g$时, 是否$f(x)=g(x)$?

作为准备, 下面定理以$n+1$个数代替所有的数取值, 对讨论问题是有很强可操作性的方法.

定理 1.5.5 若多项式$f(x),g(x)\in\mathbb{P}[x]$的次数都不超过正整数$n$, 而函数$f,g$在$n+1$个不同的数$\alpha_1,\cdots,\alpha_{n+1}$上有相同的值, 即$f(\alpha_i)=g(\alpha_i)$ $(i=1,\cdots,n+1)$, 那么$f(x)=g(x)$.

证明 令$h(x)=f(x)-g(x)$, 则 $\partial(h(x))\leq\max\{\partial(f(x)),\partial(g(x))\}\leq n$, 且

$$h(\alpha_i)=f(\alpha_i)-g(\alpha_i)=0\ \ (i=1,\cdots,n+1),$$

即$h(x)$有$n+1$个不同的根, 由定理1.5.4, $h(x)=0$, 从而$f(x)=g(x)$. □

由定理1.5.5, 容易证明著名的拉格朗日插值定理(留作练习).

推论 1.5.6 (拉格朗日插值定理) 对于数域$\mathbb{P}$上给定的$2(n+1)$个数

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_{n+1},\ \beta_1,\ \beta_2,\ \cdots,\ \beta_{n+1},$$

其中$\alpha_i\neq\alpha_j$ $(\forall i\neq j)$. 构造多项式

$$f(x)=\beta_1f_1(x)+\beta_2f_2(x)+\cdots+\beta_{n+1}f_{n+1}(x),$$

称之为**拉格朗日插值公式**, 其中, 对$j=1,2,\cdots,n+1$,

$$f_j(x)=\frac{(x-\alpha_1)\cdots(x-\alpha_{j-1})(x-\alpha_{j+1})\cdots(x-\alpha_{n+1})}{(\alpha_j-\alpha_1)\cdots(\alpha_j-\alpha_{j-1})(\alpha_j-\alpha_{j+1})\cdots(\alpha_j-\alpha_{n+1})}.$$

则

(1) 多项式$f(x)$的次数不超过n且满足$f(\alpha_i)=\beta_i\ (i=1,2,\cdots,n+1)$;

(2) 拉格朗日插值公式中$f(x)$是满足(1)的唯一多项式.

推论 1.5.7 对$f(x),\ g(x)\in\mathbb{P}[x]$, 当它们的多项式函数$f=g$时, 有$f(x)=g(x)$.

证明 设$\partial(f(x)),\ \partial(g(x))$都小于$n$. $f=g$意味着对任何$\alpha\in\mathbb{P},\ f(\alpha)=g(\alpha)$, 当然能找到$n+1$个不同的$\alpha_1,\ \cdots,\ \alpha_{n+1}\in\mathbb{P}$使得$f(\alpha_i)=g(\alpha_i)$, 再由定理1.5.5即可. □

由引理1.5.1和推论1.5.7知, 对$f(x),\ g(x)\in\mathbb{P}[x]$, 作为$\mathbb{P}$上函数, $f=g$当且仅当$f(x)=g(x)$.

例 1.5.2 设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$是实系数多项式, 求证:

(1) 若$(-1)^ia_i$全是正数或全是负数, 则$f(x)$没有负实根;

(2) 若a_i全是正数或全是负数, 则$f(x)$没有正实根.

证明 (1) 若$f(x)$有负实根$-c,c>0$, 代入后得

$$f(-c)=a_n(-c)^n+a_{n-1}(-c)^{n-1}+\cdots+a_1(-c)+a_0,$$

则当$(-1)^ia_i$全是正数, 有$f(-c)>0$; 当$(-1)^ia_i$全是负数, 有$f(-c)<0$, 这和$-c$是根矛盾. 因此$f(x)$无负实根.

同理可证(2). □

例 1.5.3 设$h(x),k(x),f(x),g(x)$是实系数多项式, 且

$$(x^2+1)h(x)+(x+1)f(x)+(x-2)g(x)=0, \tag{1.5.1}$$

$$(x^2+1)k(x)+(x-1)f(x)+(x+2)g(x)=0. \tag{1.5.2}$$

则$f(x),g(x)$能被x^2+1整除.

证明 将$x=i$, 这里$i^2=-1$, 代入(1.5.1)和(1.5.2), 得

$$(i+1)f(i)+(i-2)g(i)=0,$$
$$(i-1)f(i)+(i+2)g(i)=0,$$

解得$f(i)=g(i)=0$, 所以$(x-i)|f(x),(x-i)|g(x)$.

类似将$x=-i$代入, 可得$f(-i)=g(-i)=0$, 故$(x+i)|f(x),\ (x+i)|g(x)$.

从而

$$(x^2+1)|f(x),\ (x^2+1)|g(x).$$ □

习 题 1.5

1. 证明:

(1) $(8x^9-6x^7+4x-7)^3(2x^5-3)^7$的展开式中各项系数之和为1.

(2) $(6-\frac{1}{\sqrt{2}}\,x-5x^2-x^3)^{97}(1-6x^2+5x^4+\sqrt{2}\,x^6)^{99}$ 的展开式各项系数之和为-2.

2. 证明: 多项式

$$f(x)=(x^{50}-x^{49}+x^{48}-x^{47}+\cdots+x^2-x+1)(x^{50}+x^{49}+\cdots+x+1)$$

的展开式中无奇数次项.

(提示: $f(x)$对应的多项式函数是偶函数.)

3. 若复系数非零多项式$f(x)$没有重因式，证明: $(f(x)+f'(x), f(x))=1$.
4. 求下列多项式的公共根:
$$f(x)=x^4+2x^2+9与g(x)=x^4-4x^3+4x^2-9.$$
5. (1) 证明: a是$f(x)$的$k+1$重根的充分必要条件是
$$f(a)=f'(a)=\cdots=f^{(k)}(a)=0, \text{ 而}f^{(k+1)}(a)\neq 0.$$
(2) 举例说明断语"若a是$f'(x)$的m重根, 那么a是$f(x)$的$m+1$重根"是不对的.
6. 判断$f(x)=x^5-10x^2+15x-6$有无重根, 若有, 试求它的所有根并确定重数.
7. 问p, q取何值时, 多项式$f(x)=x^3+px+q$有重根?
8. 证明: 多项式$f(x)=x^n+ax^{n-m}+b$不存在重数大于2的非零根.
9. 问当正整数n取何值时, 多项式$f(x)=(x+1)^n-x^n-1$有重因式?
10. 证明: 下列多项式没有重根.
(1) $f(x)=1+x+\dfrac{x^2}{2!}+\cdots+\dfrac{x^n}{n!}$;
(2) $g(x)=x^n+nx^{n-1}+n(n-1)x^{n-2}+\cdots+n(n-1)\cdots 3\cdot 2x+n!$

§1.6 代数基本定理与复、实多项式因式分解

以后对于$\mathbb{P}=\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$的情况, 多项式分别称为**复多项式、实多项式、有理多项式**.

上节我们给出了一般数域$\mathbb{P}$上多项式的根的个数估计, 即根的个数不能超过它的次数. 另一方面, 对于根的存在性, 我们可以看到, 比如: $f(x)=x^2+1$, 它在$\mathbb{Q}$上和$\mathbb{R}$上都不可能有根的, 但在$\mathbb{C}$上是有根$\pm i$的, 由此可见, 数域$\mathbb{P}$越大, 多项式的根越可能存在且个数也可能越多. 事实上, 我们有

定理 1.6.1 (代数基本定理) *任一次数≥ 1的复多项式在复数域中至少有一个根.*

这一定理体现了复数域作为一个数系是完善的, 也是讨论具体数域$\mathbb{C}$和$\mathbb{R}$上多项式因式分解的出发点. 它的证明可以在复函数论课程中由复函数的性质很简洁地给出, 而其完全的代数方法证明则较为复杂, 所以本书省略这一证明. 代数基本定理的第一个实质性证明是德国数学家高斯(Gauss)在他的博士学位论文中给出的.

由前面根与一次因式的关系, 即推论1.5.3, 代数基本定理等价于说: 每个次数≥ 1的多项式在复数域上必有一次因式(或说: 次数≥ 2的多项式在复数域上都是可约的).

设$f(x)\in\mathbb{C}[x]$且$\partial(f(x))\geq 1$, 那么$f(x)$有一次因式, 设为$x-\alpha_1$. 令$x-\alpha_1$在$f(x)$中是l_1-重因式, 则$(x-\alpha_1)^{l_1}|f(x)$. 令
$$f_1(x)=\frac{f(x)}{(x-\alpha_1)^{l_1}}.$$
若$\partial(f_1(x))\geq 1$, 则同理, $f_1(x)=\dfrac{f(x)}{(x-\alpha_1)^{l_1}}$也有一次因式$x-\alpha_2$, 设其重数为$l_2$. 则$(x-\alpha_2)^{l_2}|f_1(x)$, 依次得
$$f(x),\quad f_1(x)=\frac{f(x)}{(x-\alpha_1)^{l_1}},\ \cdots,\quad f_t(x)=\frac{f_{t-1}(x)}{(x-\alpha_t)^{l_t}},$$

使得

$$\partial(f_t(x)) = 0.$$

因此

$$f(x) = a_n(x-\alpha_1)^{l_1}(x-\alpha_2)^{l_2}\cdots(x-\alpha_t)^{l_t},$$

其中$\alpha_1, \cdots, \alpha_t$ 是不同的复数, $l_1, \cdots, l_t$ 是正整数, 且$l_1+\cdots+l_t = \partial(f(x))$. 这是$f(x)$ 的标准分解, 从而得:

定理 1.6.2 (i) 复数域上每个次数≥ 1 的多项式都可以唯一地分解成一次因式的乘积;

(ii) 复数域上每个n 次多项式恰有n个复根(重根按重数计算).

下面讨论实多项式的因式分解.

设$f(x) = a_nx^n+\cdots+a_1x+a_0 \in \mathbb{R}[x]$. 当然$f(x)$ 也是$\mathbb{C}[x]$ 中的多项式. 由代数基本定理, $f(x)$ 至少有一个复根, 设为α, 即:

$$f(\alpha) = a_n\alpha^n+\cdots+a_1\alpha+a_0 = 0.$$

上式两边取复数共轭, 因为$a_i = \bar{a}_i$, 从而:

$$f(\bar{\alpha}) = a_n\bar{\alpha}^n+\cdots+a_1\bar{\alpha}+a_0 = 0.$$

这说明$\bar{\alpha}$ 也是$f(x)$ 的一个根.

如果α 是一个实数, 那么$\alpha = \bar{\alpha}$且$x-\alpha$ 是$f(x)$ 的一个一次因式.

如果$\alpha \in \mathbb{C}$ 不是实数, 那么$\alpha \neq \bar{\alpha}$, 从而$x-\alpha$ 和$x-\bar{\alpha}$ 是$f(x)$ 的两个不同的复一次因式. 因为

$$(x-\alpha,\ x-\bar{\alpha}) = 1,$$

所以，在$\mathbb{C}[x]$上，

$$(x-\alpha)(x-\bar{\alpha}) \mid f(x).$$

因为

$$(x-\alpha)(x-\bar{\alpha}) = x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$$

是一个实二次多项式. 从而在$\mathbb{R}[x]$上也有$(x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha})|f(x)$成立. 又, 由因式分解唯一性知道,

$$x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$$

是实不可约多项式. 据此, 我们得

命题 1.6.3 一个实多项式$f(x)$ 的非实复根总是成对出现的, 即当非实复数α是$f(x)$的根时, $\bar{\alpha}$也是$f(x)$的根, 并且$x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$ 是$f(x)$在实数域上的不可约二次因式.

对于$f(x) \in \mathbb{R}[x]$, 把它看作$\mathbb{C}[x]$中的多项式, 由命题1.6.3, 不妨设$f(x)$在$\mathbb{C}$中的不同根有:

$$\alpha_1, \cdots, \alpha_r, \beta_1, \cdots, \beta_s, \bar{\beta}_1, \cdots, \bar{\beta}_s,$$

其中$\alpha_1, \cdots, \alpha_r \in \mathbb{R}$, $\beta_1, \cdots, \beta_s \in \mathbb{C}$ 是非实的. 那么$f(x)$的标准分解式可以写为:

$$\begin{aligned} f(x) &= a_n\left(\prod_{i=1}^{r}(x-\alpha_i)^{l_i}\right)\left(\prod_{j=1}^{s}(x-\beta_j)^{k_j}(x-\bar{\beta}_j)^{k_j}\right) \\ &= a_n\left(\prod_{i=1}^{r}(x-\alpha_i)^{l_i}\right)\left(\prod_{j=1}^{s}(x^2-(\beta_j+\bar{\beta}_j)x+\beta_j\bar{\beta}_j)^{k_j}\right), \end{aligned}$$

其中$x-\alpha_i$ $(i=1, \cdots, r)$是实一次因式, $x^2-(\beta_j+\bar{\beta}_j)x+\beta_j\bar{\beta}_j$是实二次不可约因式.

综上所述, 即有:

定理 1.6.4 每个次数≥ 1的实多项式在实数域上总可以唯一地分解为一次因式和二次不可约因式的乘积.

习 题 1.6

1. 分别写出下列多项式在实数域$\mathbb{R}$和复数域$\mathbb{C}$上的因式分解.

   (1) $f(x)=x^4-4x^3+2x^2+x+6$;

   (2) $g(x)=x^3+x^2+x+1$.

2. 设复系数多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0$$

(其中$a_n\neq 0,\ a_0\neq 0$)的n个复根为$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$, 求复系数多项式

$$g(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-2}x^2+a_{n-1}x+a_n$$

的所有复根.

§1.7 有理多项式的因式分解

作为一种特殊情形, 我们当然可以说, 每个次数≥ 1的有理多项式总能唯一地分解为有理不可约多项式的乘积, 这里有理不可约多项式是指它是有理多项式且在$\mathbb{Q}[x]$是不可约的.

由前面可知, 复不可约多项式是一次的, 实不可约多项式是一次或二次的, 那么有理不可约多项式如何呢? 本节我们将证明, 有理不可约多项式的次数可以是任意的.

本节的另一个主要任务是讨论有理多项式的有理根判别问题.

我们的方法是将有理多项式的因式分解归结为整系数多项式的因式分解问题.

对于整系数多项式, 我们有如下概念:

定义 1.7.1 一个非零的整系数多项式

$$g(x)=b_nx^n+\cdots+b_1x+b_0$$

的系数$b_n,\ \cdots,\ b_1, b_0$如果是互素的, 即

$$(b_0,\ b_1,\ \cdots,\ b_n)=1,$$

那么称$g(x)$是一个**本原多项式**.

命题 1.7.1 任一非零有理多项式$f(x)$可表成一个有理数r与一个本原多项式$g(x)$之积, 且这样的分解在允许差一个正负号的情况下是唯一的.

证明 令$f(x)=a_nx^n+\cdots+a_1x+a_0$, 其中$a_i=\dfrac{b_i}{c_i}\in\mathbb{Q}$, $b_i,\ c_i\neq 0$是整数, $a_n\neq 0$. 则

$$\begin{aligned}f(x)=&\frac{1}{c_0c_1\cdots c_n}(c_0c_1\cdots c_{n-1}b_nx^n+c_0c_1\cdots c_{n-2}c_nb_{n-1}x^{n-1}+\cdots\\&+c_0c_2c_3\cdots c_nb_1x^1+c_1\cdots c_nb_0).\end{aligned}$$

令

$$c_0c_1\cdots c_n=c,\ c_0c_1\cdots c_{n-1}b_n=d_n,\ c_0c_1\cdots c_{n-2}c_nb_{n-1}=d_{n-1},\ \cdots,$$
$$c_0c_2c_3\cdots c_nb_1=d_1,\ c_1c_2c_3\cdots c_nb_0=d_0.$$

再令$(d_0,\ d_1,\ \cdots,\ d_n)=d,\ \dfrac{d_i}{d}=t_i$. 则

$$f(x)=\frac{d}{c}(\sum_{i=0}^{n}t_ix^i),$$

其中$(t_0,\ t_1,\ \cdots,\ t_n)=1$, 即

$$f_1(x)\triangleq\sum_{i=0}^{n}t_ix^i$$

是本原的.

假设有另一个分解$f(x)=\dfrac{d'}{c'}f_2(x)$, 其中

$$f_2(x)=\sum_{i=0}^{n}t_i'x^i$$

是本原的, d', c' 是整数, 则

$$c'df_1(x)=cd'f_2(x)\ .$$

因为$f_1(x)$与$f_2(x)$都是本原的，所以整系数多项式$c'df_1(x)$ 与$cd'f_2(x)$ 的系数的最大公因数分别是$c'd$与cd', 但它们其实是同一个多项式. 故

$$c'd=\pm cd',\ t_i=\pm t_i'\ \ (i=0,\ 1,\ \cdots,\ n).$$

从而结论成立. □

由命题1.7.1, 我们可以将有理多项式的因式分解归结为本原多项式的因式分解. 进一步的关键是我们将证明, 一个本原多项式能否分解为两个次数较低的有理多项式之积, 与它能否分解为两个次数较低的整系数多项式之积是一致的(定理1.7.3). 这样我们就把问题完全转化到了整系数多项式的范围内的因式分解了. 作为准备, 首先证明:

引理 1.7.2 (Gauss引理) *两个本原多项式的积仍为本原多项式.*

证明 设

$$f(x)=a_nx^n+\cdots+a_1x+a_0,$$
$$g(x)=b_mx^m+\cdots+b_1x+b_0$$

是两个本原多项式, 则:

$$h(x)\triangleq f(x)g(x)=d_{n+m}x^{n+m}+\cdots+d_1x+d_0,$$

其中$d_l=\sum\limits_{s+t=l}a_sb_t$ 对于$l=0,\ 1,\ \cdots,\ n+m$.

令$(d_0,\ d_1,\ \cdots,\ d_{n+m})=d$. 假如$h(x)$不是本原多项式, 则整数$d\neq1$, 从而$d$至少有一个素因数, 设为$p$, 那么$p\mid d_i\ \ (i=0,\ 1,\ \cdots,\ n+m)$.

但$f(x)$和$g(x)$是本原的, 故p不能整除它们所有的系数, 从而存在i和j, 使得:

$$p\mid a_0,\ \cdots,\ p\mid a_{i-1}\text{但}p\nmid a_i;$$
$$p\mid b_0,\ \cdots,\ p\mid b_{j-1}\text{但}p\nmid b_j.$$

考虑

$$d_{i+j} = a_i b_j + (a_{i+1}b_{j-1} + a_{i+2}b_{j-2} + \cdots + a_{i+j}b_0) + (a_{i-1}b_{j+1} + a_{i-2}b_{j+2} + \cdots + a_0 b_{i+j}),$$

其中$p \mid d_{i+j}$, 从而也整除右边. 但p实际上整除右边除了$a_i b_j$外的所有项, 所以p不能整除右边. 这是矛盾.

所以$h(x)$是本原多项式. □

定理 1.7.3 一个非零的整系数多项式若能分解为两个较低次有理多项式之积, 必也能分解为两个较低次整系数多项式之积.

证明 设整系数多项式

$$f(x) = g(x)h(x),$$

其中$g(x),\ h(x) \in \mathbb{Q}[x]$且$\partial(g(x)) < \partial(f(x)),\ \partial(h(x)) < \partial(f(x))$, 则存在本原多项式$f_1(x),\ g_1(x),\ h_1(x)$使得

$$f(x) = af_1(x), \quad g(x) = rg_1(x), \quad h(x) = sh_1(x),$$

其中$a \in \mathbb{Z},\ r,\ s \in \mathbb{Q}$, 从而$af_1(x) = rsg_1(x)h_1(x)$. 由Gauss引理, $g_1(x)h_1(x)$是本原多项式, 由命题1.7.1, $f_1(x) = \pm g_1(x)h_1(x),\ a = \mp rs$, 即$rs \in \mathbb{Z}$. 于是

$$f(x) = (rsg_1(x))h_1(x),$$

其中$rsg_1(x)$是整系数多项式. □

用证明此定理的同样方法, 易得:

命题 1.7.4 设$f(x),\ g(x)$是整系数多项式且$g(x)$是本原的. 若$f(x) = g(x)h(x)$, 其中$h(x)$是有理多项式, 那么$h(x)$必为整系数的.

请读者作为练习自己完成上述命题的证明.

由这一命题我们可以得到求整系数多项式全部有理根的方法. 即, 我们有:

定理 1.7.5 设$f(x) = a_n x^n + \cdots + a_1 x + a_0$是一个整系数多项式, $\alpha = \dfrac{r}{s}$是$f(x)$的一个有理根, 其中r与s是互素的整数, 那么必有$r \mid a_0,\ \ s \mid a_n$.

证明 因为$f(\alpha) = 0$, 所以在$\mathbb{Q}$上有$(x - \alpha) \mid f(x)$. 从而$(sx - r) \mid f(x)$. 由r与s互素知, $sx - r$是本原多项式, 故由命题1.7.4知存在整系数多项式$b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$, 使得

$$f(x) = (sx - r)(b_{n-1}x^{n-1} + \cdots + + b_1 x + b_0).$$

比较上式两边的整系数, 得:

$$a_n = sb_{n-1}, \quad a_0 = -rb_0.$$

因此我们有$r \mid a_0,\ \ s \mid a_n$. □

直接考虑定理1.7.5中$a_n = 1$, 易得:

推论 1.7.6 若$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$是一个首项系数为1的整系数多项式, 那么$f(x)$可能的有理根必为整数且均为$a_0$的因子.

根据上述定理, 我们可以给出求任一有理多项式$f(x)$的有理根的步骤如下:

(1) 分解

$$f(x) = af_1(x),$$

其中$a \in \mathbb{Q}$, $f_1(x) = a_n x^n + \cdots + a_1 x + a_0$是本原多项式.

(2) 给出a_n与a_0的完全素数分解, 找出a_n和a_0的所有整数因子, 分别设为

$$s_1, \cdots, s_p; \quad r_1, \cdots, r_q.$$

(3) 看哪些$\frac{r_i}{s_j}$满足

$$f_1(\frac{r_i}{s_j}) = 0,$$

这些就是$f(x)$的所有有理根.

例 1.7.1 求多项式$f(x) = 3x^4 + 5x^3 + x^2 + 5x - 2$的所有有理根.

解 $a_4 = 3$, 所有因子是± 1, ± 3; $a_0 = -2$, 所有因子是± 1, ± 2. 因此$f(x)$的所有可能的有理根是: ± 1, $\pm\frac{1}{3}$, ± 2, $\pm\frac{2}{3}$. 将它们分别代入$f(x)$中, 或者用带余除法, 求出$f(x)$的值, 可得:

$$f(1) = 12, \quad f(-1) = -8, \quad f(\frac{1}{3}) = 0, \quad f(-\frac{1}{3}) = -\frac{100}{27},$$
$$f(2) = 100, \quad f(-2) = 0, \quad f(\frac{2}{3}) = \frac{104}{27}, \quad f(-\frac{2}{3}) = -\frac{156}{27}.$$

因此$f(x)$共有两个有理根$\frac{1}{3}$和-2.

例 1.7.2 证明$f(x) = x^3 + 2x^2 + x + 1$在有理数域上是不可约的.

证明 若$f(x)$可约, 因$\partial(f(x)) = 3$, 故至少有一个一次因式, 即$f(x)$有有理根. 由定理1.7.5, $f(x)$的有理根只能是± 1, 但$f(\pm 1) \neq 0$. 所以实际上$f(x)$没有有理根, 因此$f(x)$是不可约的. □

需要指出的是, 上述方法只是给出可能的有理根, 也就是有理一次因式. 当$f(x)$没有有理根时, 不能说$f(x)$就是不可约的, 即可能有次数大于1的有理因式.

上面我们解决了有理多项式的有理根求解问题. 下面讨论有理不可约多项式的判别问题.

定理 1.7.7 (Eisenstein判别法) 设$f(x) = a_n x^n + \cdots + a_1 x + a_0$是一个整系数多项式. 如果存在素数$p$使得:

1) $p \nmid a_n$;

2) $p \mid a_{n-1}, a_{n-2}, \cdots, a_0$;

3) $p^2 \nmid a_0$.

那么$f(x)$在有理数域上是不可约多项式.

证明 用反证法. 若$f(x)$在$\mathbb{Q}$上可约的, 即由定理1.7.3, $f(x)$可分解为两个次数较低次整系数多项式之积, 设为:

$$f(x) = (b_s x^s + \cdots + b_1 x + b_0)(c_t x^t + \cdots + c_1 x + c_0).$$

那么, $a_n = b_s c_t$, $a_0 = b_0 c_0$. 一般地, 对$0 \leq k \leq n$, 有

$$a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k.$$

因为$p \mid a_0$, 所以$p \mid b_0$或$p \mid c_0$, 但$p^2 \nmid a_0$. 故不能同时有$p \mid b_0$和$p \mid c_0$, 不妨设$p \mid b_0$但$p \nmid c_0$.

另一方面, $p \nmid a_n$故$p \nmid b_s$, 假设$b_0, b_1, \cdots, b_s$中第一个不能被p整除的是b_i, 那

么$0 \leq i \leq s \lneqq n$. 但是

$$a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_0 c_i,$$

其中a_i, b_0, $\cdots$, b_{i-1}均可被p整除, 故$p \mid b_i c_0$, 得$p \mid b_i$或$p \mid c_0$, 这与假设矛盾. □

例 1.7.3 证明下述多项式在$\mathbb{Q}$中是不可约的:

i) $f(x) = 2x^4 + 3x^3 - 9x^2 - 3x + 6$;

ii) $f(x) = x^n + 2x + 2$;

iii) $f(x) = x^n + 2$,

其中 ii)和 iii)中的n可取任意正整数.

证明 i) 用Eisenstein判别法. 取$p = 3$, 则

$$3 \nmid 2,\ 3^2 \nmid 6,\ 3 \mid 3,\ 3 \mid (-9),\ 3 \mid (-3),\ 3 \mid 6.$$

所以$f(x)$在$\mathbb{Q}$上是不可约的.

ii)和 iii) 取$p = 2$, 由Eisenstein判别法即可. □

例 1.7.4 多项式$x^p + px + 1$ (p为奇素数)在有理数域上是否可约?

解 令$x = y - 1$, 则:

$$\begin{aligned} f(x) &= x^p + px + 1 \\ &= (y^p - py^{p-1} + C_p^2 y^{p-2} + \cdots + C_p^{p-1} y - 1) + (py - p) + 1 \\ &= y^p - py^{p-1} + C_p^2 y^{p-2} - \cdots - C_p^{p-2} y^2 + 2py - p \\ &\triangleq g(y), \end{aligned}$$

这里

$$C_n^i = \frac{n!}{(n-i)!i!}.$$

显然$f(x)$的可约性等价于$g(y)$的可约性. 但对素数p, 用Eisenstein判别法知, $g(y)$是不可约的, 从而$f(x)$也是不可约的.

需要注意的是, Eisenstein判别法只是给出了多项式不可约的一个充分而非必要的条件. 即如果找不到适当的p使条件成立, 也不能说多项式一定是可约的.

习 题 1.7

1. 若已知多项式$f(x)$为本原多项式，证明: 多项式$f(x+1)$也为本原多项式.
2. 判断下列多项式是否有有理根, 若有, 请求之:
   (1) $2x^5 - 4x^4 - 5x^3 + 10x^2 - 3x + 6$;
   (2) $5x^4 + 3x^3 - x^2 + 2x + 14$;
   (3) $12x^4 - 20x^3 - 11x^2 + 5x + 2$.
3. 判断下列多项式在有理数域上是否可约.
   (1) $5x^4 - 6x^3 + 12x + 6$;
   (2) $x^6 + x^3 + 1$;
   (3) $f(x) = x^p + px + 2p - 1$, p为素数;
   (4) $f(x) = 1 + x + \dfrac{x^2}{2!} + \cdots + \dfrac{x^p}{p!}$, p为素数.

4. 证明：如果一个本原多项式写成两个整系数多项式的乘积，则每个整系数多项式都是本原的.
5. 证明：x^3-9在$\mathbb{Q}$上不可约.

补 充 题

1. 设$f_0(x),\ f_1(x),\ \cdots,\ f_{n-1}(x)\in\mathbb{P}[x]$, 并且在$\mathbb{P}$上, x^n-a整除$\sum\limits_{i=0}^{n-1}f_i(x^n)x^i$. 证明: $x-a$整除$f_i(x),\ i=0,\ 1,\ 2,\ \cdots,\ n-1$.
(提示: 设$f_i(x)=(x-a)q_i(x)+r_i,\ i=0,\ 1,\ 2,\ \cdots,\ n-1$. 由此可得
$$\sum_{i=0}^{n-1}f_i(x^n)x^i=(x^n-a)\sum_{i=0}^{n-1}q_i(x^n)x^i+\sum_{i=0}^{n-1}r_ix^i,$$
再利用已知条件即可.)
2. 设$d,\ n$是两个正整数, 证明: $(x^d-1)\mid(x^n-1)$当且仅当$d\mid n$.
3. 设$f_1(x)=af(x)+bg(x),\ g_1(x)=cf(x)+dg(x)$, 且$ad-bc\neq 0,$ 证明
$$(f(x),\ g(x))=(f_1(x),\ g_1(x)).$$
4. 设$m,\ n$为大于1的整数. 证明: 多项式
$$f(x)=x^{m-1}+x^{m-2}+\cdots+x+1,\ g(x)=x^{n-1}+x^{n-2}+\cdots+x+1$$
互素当且仅当m与n互素.
5. 设$f_1(x),f_2(x),g_1(x),g_2(x)$为非零多项式, 且$(f_i(x),g_j(x))=1,\ i,j=1,2$, 证明:
$$(f_1(x)g_1(x),\ f_2(x)g_2(x))=(f_1(x),\ f_2(x))(g_1(x),\ g_2(x)).$$
6. 设m为任一自然数, 证明: $g^m(x)|f^m(x)$当且仅当$g(x)|f(x)$.
7. 证明: 多项式$f(x)$与$g(x)$互素的充要条件是, 对任意正整数$n,\ f^n(x)$与$g^n(x)$都互素.
8. 证明: 设$f(x)\in\mathbb{P}[x]$, 且$\partial(f(x))=n\geq 1,$ 则如下陈述等价:
   (1) $f'(x)|f(x)$;
   (2) $f'(x)$中不含$f(x)$中没有的不可约因式;
   (3) $f(x)$有n重根.
9. 证明: 如果n次多项式$f(x)$的根为$x_1,\ x_2,\ \cdots,\ x_n,$ 而数c不是$f(x)$的根, 则
$$\sum_{i=1}^{n}\frac{1}{x_i-c}=-\frac{f'(c)}{f(c)}.$$
10. 设$f_1(x),\ f_2(x),\ \cdots,\ f_n(x)$都是实多项式. 证明: 存在实多项式$f(x)$和$g(x)$, 使得
$$\sum_{i=1}^{n}f_i^2(x)=f^2(x)+g^2(x).$$
11. 证明: 三次实多项式$f(x)=x^3+a_1x^2+a_2x+a_3$ 的根都在左半复平面内(即根的实部为负数)当且仅当$a_1,\ a_2,\ a_3$均为正数, 且$a_3<a_2a_1$.
12. 设 n次整系数多项式函数$f(x)$在多于 n个整数 x处取值1或-1, 这里 $n\geq 1$. 证明: 多项式$f(x)$在有理数域上不可约.

第 2 章　多元多项式理论

§2.1　多元多项式

设$\mathbb{P}$是一个数域, $x_1, \cdots, x_n$是n个文字, 形式为

$$\sum_{k_1,\, k_2,\, \cdots,\, k_n} a_{k_1 k_2 \cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

的式子被称为一个n**元多项式**, 其中和是形式和, 不同文字间的乘积是可换的, $a_{k_1 \cdots k_n} \in \mathbb{P}$ 是$x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$的系数, 且和式中至多有限个系数非零, $a_{k_1 \cdots k_n} x_1^{k_1} \cdots x_n^{k_n}$被称为一个**单项式**(或**单项**). 我们通常用$f(x_1, \cdots, x_n)$表示上述n元多项式, 有时也表为$f(x)$, 其中$x = (x_1, \cdots, x_n)^{\mathrm{T}}$. 如果两个单项式中相同文字的幂完全一样, 就称它们是**同类项**, 它们可以相加, 将系数相加即可.

n元多项式的**相等**、**相加**、**相减**、**相乘**与一元多项式一样类似可以定义. 例如:

$$(5x_1^3 x_2 x_3^2 + 4x_1^2 x_2^2 x_3) + (2x_1^2 x_2^2 x_3 - x_1^4 x_2 x_3) = 5x_1^3 x_2 x_3^2 + 6x_1^2 x_2^2 x_3 - x_1^4 x_2 x_3;$$

$$\begin{aligned}(5x_1^3 x_2 x_3^2 + 4x_1^2 x_2^2 x_3)(2x_1^2 x_2^2 x_3 - x_1^4 x_2 x_3) = {} & 10x_1^5 x_2^3 x_3^3 - 5x_1^7 x_2^2 x_3^3 + \\ & 8x_1^4 x_2^4 x_3^2 - 4x_1^6 x_2^3 x_3^2.\end{aligned}$$

所有系数在$\mathbb{P}$中的n元多项式的全体被称为$\mathbb{P}$上的n**元多项式环**, 记为$\mathbb{P}[x_1, \cdots, x_n]$.

每个单项式$ax_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ 由一个对应的n元数组$(k_1, k_2, \cdots, k_n)$唯一决定, 其中$k_i \geq 0$. 这样的对应是$1-1$的, 表示$\boldsymbol{\alpha} = (k_1, k_2, \cdots, k_n)$, 那么$ax_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$可以表示为$ax^{\boldsymbol{\alpha}} = ax_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$. 对于此单项式, 当$a \neq 0$时, $k_1 + k_2 + \cdots + k_n$称为其**次数**.

当一个多项式$f(x_1, x_2, \cdots, x_n)$表成一些不同类的单项式之和时, 其系数不为零的单项式的次数最大数被称为此**多项式的次数**, 表示为$\partial(f(x_1, x_2, \cdots, x_n))$. 例如: $\partial(3x_1^2 x_2^2 + 2x_1 x_2^2 x_3 + x_3^3) = 4$.

一元多项式中的单项式依照各单项的次数自然地排出了一个顺序, 但这种顺序法对多元多项式中的单项就不适用了, 因为不同类的单项式可能有相同的次数. 正如一元多项式单项的降幂排法对于问题的讨论带来方便, 也有必要在多元多项式的单项间引入一种适当的排序法, 最常用的就是模仿字典中单词排列原则给出的所谓**字典排序法**.

前面已提到, 每一类单项式$x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$对应于一个$n$元数组$(k_1, k_2, \cdots, k_n)$. 因此, 要定义两类单项式间的排序, 只要定义这样的n元数组间的一种序就可以了, 具体如下:

对两个n元数组$(k_1, k_2, \cdots, k_n)$和$(l_1, l_2, \cdots, l_n)$, 如果数列

$$k_1 - l_1, k_2 - l_2, \cdots, k_n - l_n$$

中第一个不为零的数是正的, 即: 存在$i \leqslant n$使得

$$k_1 - l_1 = 0, \cdots, k_{i-1} - l_{i-1} = 0, k_i - l_i > 0,$$

就称$(k_1,\ k_2,\ \cdots,\ k_n)$ 先于$(l_1,\ l_2,\ \cdots,\ l_n)$, 表为

$$(k_1,\ k_2,\ \cdots,\ k_n) > (l_1,\ l_2,\ \cdots,\ l_n).$$

这时, 就说单项$x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$排在单项$x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$之前.

例如: 多项式$2x_2^2x_3^4 - x_1x_2^2x_3^4 + x_2x_3^5 + x_3^7 + 3x_1x_2^3x_3^2$ 的对应数组按大小排列为

$$(1,\ 3,\ 2) > (1,\ 2,\ 4) > (0,\ 2,\ 4) > (0,\ 1,\ 5) > (0,\ 0,\ 7).$$

因此这个多项式按字典排序法写就是:

$$3x_1x_2^3x_3^2 - x_1x_2^2x_3^4 + 2x_2^2x_3^4 + x_2x_3^5 + x_3^7.$$

按字典排序法写出来的第一个系数不为零的单项式称为是多项式的**首项**, 例如上面的多项式的首项是$3x_1x_2^3x_3^2$. 应该注意的是: 首项的次数未必是所有单项式中最大的, 比如上面的多项式的首项的次数是6, 小于末项x_3^7的次数7. 这与一元多项式是不同的.

当$n = 1$时, 字典排序法就是一元多项式中的降幂排序法.

由定义易见, 对任意两个不同的n元数组$(k_1, k_2, \cdots, k_n)$和$(l_1, l_2, \cdots, l_n)$, 必有

$$(k_1,\ k_2,\ \cdots,\ k_n) > (l_1,\ l_2,\ \cdots,\ l_n)$$

或者

$$(l_1,\ l_2,\ \cdots,\ l_n) > (k_1,\ k_2,\ \cdots,\ k_n)$$

其一成立. 而且排序具有传递性, 即若

$$(k_1,\ k_2,\ \cdots,\ k_n) > (l_1,\ l_2,\ \cdots,\ l_n),\ (l_1,\ l_2,\ \cdots,\ l_n) > (m_1,\ m_2,\ \cdots,\ m_n),$$

则必有

$$(k_1,\ k_2,\ \cdots,\ k_n) > (m_1,\ m_2,\ \cdots,\ m_n).$$

因此, 这种排序法保证了任一多元多项式均可据此对各单项式进行排序.

引理 2.1.1 设n元数组

$$(p_1,\ p_2,\ \cdots,\ p_n) \geq (l_1,\ l_2,\ \cdots,\ l_n),\ (q_1,\ q_2,\ \cdots,\ q_n) \geq (k_1,\ k_2,\ \cdots,\ k_n).$$

则有

$$(p_1 + q_1,\ p_2 + q_2,\ \cdots,\ p_n + q_n) \geq (l_1 + k_1,\ l_2 + k_2,\ \cdots,\ l_n + k_n).$$

证明 当$(p_1, p_2, \cdots, p_n) = (l_1, l_2, \cdots, l_n)$, $(q_1, q_2, \cdots, q_n) > (k_1, k_2, \cdots, k_n)$时, 必存在$i$使得$q_1 = k_1,\ \cdots,\ q_{i-1} = k_{i-1},\ q_i > k_i$. 从而$p_1 + q_1 = k_1 + l_1,\ \cdots,\ p_{i-1} + q_{i-1} = k_{i-1} + l_{i-1},\ p_i + q_i > k_i + l_i$, 即

$$(p_1 + q_1,\ p_2 + q_2,\ \cdots,\ p_n + q_n) \geq (l_1 + k_1,\ l_2 + k_2,\ \cdots,\ l_n + k_n).$$

当$(p_1,\ p_2,\ \cdots,\ p_n) > (l_1,\ l_2,\ \cdots,\ l_n)$, $(q_1,\ q_2,\ \cdots,\ q_n) = (k_1,\ k_2,\ \cdots,\ k_n)$时, 同理可得结论成立.

当$(p_1,\ p_2,\ \cdots,\ p_n) > (l_1,\ l_2,\ \cdots,\ l_n)$, $(q_1,\ q_2,\ \cdots,\ q_n) > (k_1,\ k_2,\ \cdots,\ k_n)$时, 存在$i,\ j$使得:

$$p_1 = l_1,\ \cdots,\ p_{i-1} = l_{i-1},\ p_i > l_i;$$
$$q_1 = k_1,\ \cdots,\ q_{j-1} = k_{j-1},\ q_j > k_j.$$

不妨设$i \geq j$, 那么

$$p_1 + q_1 = l_1 + k_1,\ \cdots,\ p_{j-1} + q_{j-1} = l_{j-1} + k_{j-1},\ p_j + q_j > l_j + k_j,$$

从而

$$(p_1 + q_1,\ p_2 + q_2,\ \cdots,\ p_n + q_n) \geq (l_1 + k_1,\ l_2 + k_2,\ \cdots,\ l_n + k_n). \qquad \square$$

字典排序法的一个重要的性质是如下的:

定理 2.1.2 设$f(x_1, x_2, \cdots, x_n)$, $g(x_1, x_2, \cdots, x_n)$是两个非零n元多项式. 则它们的乘积$f(x_1, x_2, \cdots, x_n)g(x_1, x_2, \cdots, x_n)$的首项等于$f(x_1, x_2, \cdots, x_n)$的首项与$g(x_1, x_2, \cdots, x_n)$的首项乘积.

证明 由n元多项式的首项的定义和上面引理2.1.1易得. □

由定理2.1.2, 不难得:

推论 2.1.3 若$f(x_1, x_2, \cdots, x_n) \neq 0$, $g(x_1, x_2, \cdots, x_n) \neq 0$, 则

$$f(x_1, x_2, \cdots, x_n)g(x_1, x_2, \cdots, x_n) \neq 0.$$

用归纳法进一步可得:

推论 2.1.4 若$f_1(x), \cdots, f_m(x)$是n元非零多项式, 则$f_1(x)\cdots f_m(x)$是非零多项式且它的首项是$f_1(x), \cdots, f_m(x)$ 的首项之积.

多元多项式的众多单项式的次数看起来没有次序而难以把握, 但我们可以依次数的大小而把多项式分解为若干多项式之和, 其中每个作为加法项的多项式中所有单项式的次数一致. 这样分解后, 可以让多项式的性质讨论变得容易.

首先, 一个多项式

$$r(x_1, \cdots, x_n) = \sum_{k_1,k_2,\cdots,k_n} a_{k_1k_2\cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

中, 若每个单项式的次数都相等, 设为m, 即总有$k_1 + \cdots + k_n = m$, 则称此多项式$r(x_1,\cdots,x_n)$ 是一个m**次齐次多项式**. 例如:

$$f(x_1, x_2, x_3) = 2x_1x_2x_3^2 + x_1^2x_2^2 + 3x_1^4$$

是一个4次齐次多项式.

显然, 两个齐次多项式之积仍是齐次多项式, 其次数是原两个齐次多项式的次数之和.

任取一个m次多项式$f(x_1, \cdots, x_n)$. 对$0 \leq i \leq m$, 把$f(x_1, \cdots, x_n)$中所有i次单项式之和记为$f_i(x_1, \cdots, x_n)$, 那么$f_i(x_1, \cdots, x_n)$是一个i次齐次多项式且

$$f(x_1, \cdots, x_n) = \sum_{i=0}^{m} f_i(x_1, \cdots, x_n).$$

称$f_i(x_1, \cdots, x_n)$是$f(x_1, \cdots, x_n)$的 i **次齐次成分**. 若$f(x_1, \cdots, x_n)$没有 i 次单项式, 那么$f_i(x_1, \cdots, x_n) = 0$.

设另一个l次多项式

$$g(x_1, \cdots, x_n) = \sum_{j=0}^{l} g_j(x_1, \cdots, x_n),$$

其中$g_j(x_1, \cdots, x_n)$是其j次齐次成分. 那么

$$f(x_1, \cdots, x_n)g(x_1, \cdots, x_n) = \sum_{k=0}^{m+l} \sum_{i+j=k} f_i(x_1, \cdots, x_n)g_j(x_1, \cdots, x_n),$$

其中

$$h_k(x_1, \cdots, x_n) \triangleq \sum_{i+j=k} f_i(x_1, \cdots, x_n)g_j(x_1, \cdots, x_n)$$

是此乘积的k次齐次成分, 其最高次齐次成分为

$$h_{m+l}(x_1, \cdots, x_n) = f_m(x_1, \cdots, x_n)g_l(x_1, \cdots, x_n).$$

从而我们得:

定理 2.1.5 多元多项式的乘积的次数等于各因式次数的和.

最后, 与一元多项式一样, 由一个多元多项式我们可以定义一个多元**多项式函数**. 设$\mathbb{P}$上的n元多项式:

$$f(x_1, \cdots, x_n) = \sum_{k_1,k_2,\cdots,k_n} a_{k_1k_2\cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}.$$

定义$f : \mathbb{P}^n \longrightarrow \mathbb{P}$ 使得

$$(c_1, \cdots, c_n) \longmapsto f(c_1, \cdots, c_n) \triangleq \sum_{k_1,k_2,\cdots,k_n} a_{k_1k_2\cdots k_n} c_1^{k_1} c_2^{k_2} \cdots c_n^{k_n}.$$

那么f是一个$\mathbb{P}^n$到$\mathbb{P}$的n元函数. 显然, 当

$$f(x_1, \cdots, x_n) + g(x_1, \cdots, x_n) = h(x_1, \cdots, x_n),$$
$$f(x_1, \cdots, x_n)g(x_1, \cdots, x_n) = p(x_1, \cdots, x_n)$$

时, 对任一$(c_1, \cdots, c_n) \in \mathbb{P}^n$, 有下列等式:

$$f(c_1, \cdots, c_n) + g(c_1, \cdots, c_n) = h(c_1, \cdots, c_n),$$
$$f(c_1, \cdots, c_n)g(c_1, \cdots, c_n) = p(c_1, \cdots, c_n).$$

习 题 2.1

1. 按多元多项式的字典排序法改写以下两个多项式, 指出它们的乘积的首项和最高次项, 并写出各自的齐次分解:
   $f(x_1, x_2, x_3, x_4) = 3x_2^6x_4^3 - \frac{1}{2}x_1^3x_2x_3^2 + 5x_2^3x_4 + 7x_3^2 + 2x_1^3x_2x_3^4 - 8 + 6x_2x_4^2$,
   $g(x_1, x_2, x_3, x_4) = x_3^2x_4 + x_3x_4^2 + x_1^2x_2 + x_1x_2^2$.
2. 已知方程$2x^3 - 5x^2 - 4x + 12 = 0$有一个二重根, 解此方程.
3. 证明: 若方程$x^3 + px^2 + qx + r = 0$的三个根成等比数列, 则$q^3 = p^3r$.

§2.2 对称多项式

对称多项式是多元多项式中常用的而且重要的一种. 本节专门讨论对称多项式. 让我们先从一元多项式的求根问题入手.

设

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n$$

是$\mathbb{P}[x]$中的一个多项式, 并假设$f(x)$在$\mathbb{P}$中恰有n个根$\alpha_1, \alpha_2, \cdots, \alpha_n$, 那么

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n),$$

展开, 得

$$f(x) = x^n - (\alpha_1 + \alpha_2 + \cdots + \alpha_n)x^{n-1} + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n)x^{n-2}$$
$$- \cdots + (-1)^i \left(\sum_{k_1<k_2<\cdots<k_i} \alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i} \right) x^{n-i} + \cdots + (-1)^n\alpha_1\alpha_2\cdots\alpha_n .$$

与$f(x)$的原表示式比较, 得

$$\begin{cases} -a_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_n, \\ a_2 = \sum\limits_{k_1<k_2} \alpha_{k_1}\alpha_{k_2}, \\ \quad\vdots \\ (-1)^i a_i = \sum\limits_{k_1<k_2<\cdots<k_i} \alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}, \\ \quad\vdots \\ (-1)^n a_n = \alpha_1\alpha_2\cdots\alpha_n. \end{cases} \tag{2.2.1}$$

上述各式对于各个α_i是对称的. 因此可以说, $f(x)$系数对称地依赖于方程的根.

上面(2.2.1)式表达了$f(x)$的**根与系数的关系**, 又称为**韦达(Vieta)定理**.

易见, (2.2.1)式中右边事实上是如下的n个n元多项式的多项式函数, 这些多项式是

$$\begin{cases} \sigma_1 = x_1 + x_2 + \cdots + x_n, \\ \sigma_2 = \sum\limits_{k_1<k_2} x_{k_1}x_{k_2}, \\ \quad\vdots \\ \sigma_i = \sum\limits_{k_1<k_2<\cdots<k_i} x_{k_1}x_{k_2}\cdots x_{k_i}, \\ \quad\vdots \\ \sigma_n = x_1x_2\cdots x_n. \end{cases} \tag{2.2.2}$$

它们对称地依赖于文字$x_1, x_2, \cdots, x_n$, 因此是一种特殊的"对称"多项式. 对于一般的对称多项式, 可以如下定义:

定义 2.2.1 如果n元多项式$f(x_1, \cdots, x_n)$对于任意的i, j $(1 \le i < j \le n)$, 都有

$$f(x_1, \cdots, x_i, \cdots, x_j, \cdots, x_n) = f(x_1, \cdots, x_j, \cdots, x_i, \cdots, x_n)$$

就称$f(x_1, \cdots, x_n)$是一个**对称多项式**.

从定义可知, 所谓"对称"的意义就是, 任换两个文字得到的多项式仍是原来的多项式.

据定义2.2.1, (2.2.2)式中的多项式$\sigma_1, \cdots, \sigma_n$都是关于$x_1, \cdots, x_n$的对称多项式. 下面定理2.2.2将说明, 它们是最基本的, 称为**初等对称多项式**.

当然, 绝大多数对称多项式都是非初等的, 比如:

$$f(x_1, x_2, x_3) = x_1^2x_2 + x_2^2x_1 + x_1^2x_3 + x_3^2x_1 + x_2^2x_3 + x_3^2x_2$$

由对称多项式的定义2.2.1直接可得:

引理 2.2.1 (i) 对称多项式的和、差、积还是对称多项式.

(ii) 对称多项式的多项式还是对称多项式, 即若$f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$是$n$元对称多项式, 而$g(y_1, \cdots, y_m)$是任一多项式, 那么

$$g(f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)) = h(x_1, x_2, \cdots, x_n)$$

仍是n元对称多项式.

注意, 上面$g(f_1(x), \cdots, f_m(x))$相当于函数的复合, 称为**复合多项式**.

特别地, 虽然初等对称多项式的多项式还是对称多项式, 但不一定是初等对称的.

对称多项式的基本事实是: 任一对称多项式都能表成初等对称多项式的多项式, 即

定理 2.2.2 设$f(x_1, x_2, \cdots, x_n)$是n元对称多项式, 那么存在唯一的n元多项式$\varphi(y_1, y_2, \cdots, y_n)$, 使得

$$f(x_1, x_2, \cdots, x_n) = \varphi(\sigma_1, \sigma_2, \cdots, \sigma_n).$$

证明 首先用构造法证明存在性.

设$f(x_1, x_2, \cdots, x_n)$的首项是$ax_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}(a \neq 0)$, 则必有

$$l_1 \geq l_2 \geq \cdots \geq l_n \geq 0.$$

否则, 设有$l_i < l_{i+1}$, 因为$f(x_1, x_2, \cdots, x_n)$是对称的, 所以在包含$ax_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$的同时必包含$ax_1^{l_1}\cdots x_i^{l_{i+1}}x_{i+1}^{l_i}\cdots x_n^{l_n}$, 但此项按字典排序法应先于$ax_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$, 与首项要求不符.

作多项式

$$\varphi_1 = a\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\cdots\sigma_n^{l_n},$$

由引理2.2.1, φ_1是对称多项式, 而$\sigma_1, \sigma_2, \cdots, \sigma_n$的首项分别是$x_1, x_1x_2, \cdots, x_1x_2\cdots x_n$. 所以由推论2.1.4, φ_1的首项是

$$ax_1^{l_1-l_2}(x_1x_2)^{l_2-l_3}\cdots(x_1x_2\cdots x_n)^{l_n} = ax_1^{l_1}x_2^{l_2}\cdots x_n^{l_n},$$

即φ_1与$f(x_1, x_2, \cdots, x_n)$的首项相同, 从而对称多项式

$$f_1(x) = f(x) - \varphi_1$$

的首项比$f(x) = f(x_1, x_2, \cdots, x_n)$的首项要排后.

对$f_1(x)$重复对$f(x)$的做法, 并继续做下去, 得到一系列的对称多项式:

$$f(x),\ f_1(x) = f(x) - \varphi_1,\ f_2(x) = f_1(x) - \varphi_2, \cdots$$

其中$f_i(x)$的首项随i越排越后, 而φ_i是$\sigma_1, \sigma_2, \cdots, \sigma_n$的多项式.

但因为排在$ax_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$后面的单项的指数$n$元数组只有有限个, 所以$f_i(x)$只能有有限个非零, 即存在$h > 0$, 使得$f_h(x) = f_{h-1}(x) - \varphi_h = 0$. 于是,

$$f(x) = \varphi_1 + \varphi_2 + \cdots + \varphi_h$$

是$\sigma_1, \sigma_2, \cdots, \sigma_n$的多项式.

要证明唯一性, 只需证明: 对多项式$\varphi(y_1, y_2, \cdots, y_n)$, 若$\varphi(\sigma_1, \sigma_2, \cdots, \sigma_n) = 0$, 则有$\varphi(y_1, y_2, \cdots, y_n) = 0$.

若否, 因为$\varphi(\sigma_1, \sigma_2, \cdots, \sigma_n) = 0$, 所以$\varphi(y_1, y_2, \cdots, y_n)$必不是单项式. 设$ay_1^{k_1}y_2^{k_2}\cdots y_n^{k_n}$与$by_1^{l_1}y_2^{l_2}\cdots y_n^{l_n}$是$\varphi(y_1, y_2, \cdots, y_n)$的两个非零单项, 则$a\sigma_1^{k_1}\sigma_2^{k_2}\cdots\sigma_n^{k_n}$的首项为

$$ax_1^{k_1+k_2+\cdots+k_n}x_2^{k_2+\cdots+k_n}\cdots x_n^{k_n},$$

而$b\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}$的首项为

$$bx_1^{l_1+l_2+\cdots+l_n}x_2^{l_2+\cdots+l_n}\cdots x_n^{l_n}.$$

显然, 这两个首项是同类项当且仅当

$$k_1 = l_1,\ k_2 = l_2,\ \cdots,\ k_n = l_n,$$

即 $ay_1^{k_1}y_2^{k_2}\cdots y_n^{k_n}$ 与 $by_1^{l_1}y_2^{l_2}\cdots y_n^{l_n}$ 也是同类项. 所以对于 $\varphi(y_1,\ y_2,\ \cdots,\ y_n)$的所有互异非零单项 $ay_1^{k_1}y_2^{k_2}\cdots y_n^{k_n}$, 多项式 $a\sigma_1^{k_1}\sigma_2^{k_2}\cdots\sigma_n^{k_n}$的首项互不相同. 而这些首项按字典排序法重新排序后的首项即为$\varphi(\sigma_1,\ \sigma_2,\ \cdots,\ \sigma_n)$的首项, 从而有 $\varphi(\sigma_1,\ \sigma_2,\ \cdots,\ \sigma_n) \neq 0$. 此为矛盾. □

上述用构造法证明存在性的过程也是把一个对称多项式具体表为初等对称多项式的多项式的过程.

例 2.2.1 把对称多项式$f(x_1,\ x_2,\ x_3) = x_1^3 + x_2^3 + x_3^3$表成初等对称多项式$\sigma_1,\ \sigma_2,\ \sigma_3$ 的多项式.

解法一 $f(x_1,\ x_2,\ x_3)$的首项x_1^3, 其三元数组为$(3,\ 0,\ 0)$, 因此

$$\varphi_1 = \sigma_1^{3-0}\sigma_2^{0-0}\sigma_3^0 = \sigma_1^3 = (x_1 + x_2 + x_3)^3,$$

$$f_1(x_1,\ x_2,\ x_3) = f(x_1,\ x_2,\ x_3) - \varphi_1 = -3(x_1^2x_2 + x_2^2x_3 + \cdots) - 6x_1x_2x_3.$$

因为$f_1(x_1,\ x_2,\ x_3)$的首项$-3x_1^2x_2$, 其三元数组为$(2,\ 1,\ 0)$, 故

$$\varphi_2 = -3\sigma_1^{2-1}\sigma_2^{1-0}\sigma_3^0 = -3\sigma_1\sigma_2 = -3(x_1^2x_2 + x_2^2x_1 + \cdots) - 9x_1x_2x_3.$$

于是

$$f_2(x_1,\ x_2,\ x_3) = f_1(x_1,\ x_2,\ x_3) - \varphi_2 = 3x_1x_2x_3 = 3\sigma_3,$$

从而

$$\begin{aligned} f(x_1,\ x_2,\ x_3) &= f_1(x_1,\ x_2,\ x_3) + \varphi_1 = f_2(x_1,\ x_2,\ x_3) + \varphi_2 + \varphi_1 \\ &= 3\sigma_3 - 3\sigma_1\sigma_2 + \sigma_1^3. \end{aligned}$$

解法二(待定系数法) 因为多项式$f(x_1,\ x_2,\ x_3)$的首项是x_1^3, 所以有

指数组	对应σ的方幂的乘积
$(3,0,0)$	σ_1^3
$(2,1,0)$	$\sigma_1\sigma_2$
$(1,1,1)$	σ_3

故可设$f(x_1,\ x_2,\ x_3) = \sigma_1^3 + a\sigma_1\sigma_2 + b\sigma_3$.

令$x_1 = x_2 = 1,\ x_3 = 0$, 则$f(x_1,\ x_2,\ x_3) = 2,\ \sigma_1 = 2,\ \sigma_2 = 1,\ \sigma_3 = 0$. 所以$8 + 2a = 2$, 即$a = -3$.

令$x_1 = x_2 = x_3 = 1$, 则$f(x_1,\ x_2,\ x_3) = 3,\ \sigma_1 = \sigma_2 = 3,\ \sigma_3 = 1$. 所以$27 - 27 + b = 3$, 即$b = 3$.

所以$f(x_1,\ x_2,\ x_3) = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

最后, 作为对称多项式理论的一个应用, 我们介绍一元高次多项式的重根存在性的判别法.

设$f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{C}[x]$, 那么在$\mathbb{C}$中, $f(x)$可表为

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n),$$

其中$\alpha_i(i=1,\,2,\,\cdots,\,n)$是$f(x)$在$\mathbb{C}$上的$n$个根. 令

$$g(x_1,\,x_2,\,\cdots,\,x_n)=\prod_{1\leq i<j\leq n}(x_i-x_j)^2\in\mathbb{C}[x_1,\,\cdots,\,x_n],$$

$$D(f)\triangleq g(\alpha_1,\,\alpha_2,\,\cdots,\,\alpha_n)=\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2.$$

那么, $f(x)$在$\mathbb{C}$中有重根当且仅当$D(f)=0$.

但要讨论$D(f)$是否为零, 不可能通过直接求出$\alpha_1,\,\cdots,\,\alpha_n$再代入$g(x_1,\,\cdots,\,x_n)$算出$D$来进行. 我们的办法是将$D(f)$表达为$f(x)$的系数$a_1,\,a_2,\,\cdots,\,a_n$的函数, 从而可算出$D(f)$.

事实上, $g(x_1,\,x_2,\,\cdots,\,x_n)$显然是$x_1,\,x_2,\,\cdots,\,x_n$的对称多项式, 故由定理2.2.2知, $g(x_1,\,x_2,\,\cdots,\,x_n)$可表达为$\sigma_1,\,\sigma_2,\,\cdots,\,\sigma_n$的多项式. 但是, 由韦达定理,

$$\begin{cases}a_1=-\sigma_1(\alpha_1,\,\alpha_2,\,\cdots,\,\alpha_n),\\ a_2=\sigma_2(\alpha_1,\,\alpha_2,\,\cdots,\,\alpha_n),\\ \quad\vdots\\ a_k=(-1)^k\sigma_k(\alpha_1,\,\alpha_2,\,\cdots,\,\alpha_n),\\ \quad\vdots\\ a_n=(-1)^n\sigma_n(\alpha_1,\,\alpha_2,\,\cdots,\,\alpha_n).\end{cases}$$

于是, $D(f)=g(\alpha_1,\,\alpha_2,\,\cdots,\,\alpha_n)$可表达为$a_1,\,a_2,\,\cdots,\,a_n$的一个多项式函数, 写为$D(f)=D(a_1,\,a_2,\,\cdots,\,a_n)$, 从而直接计算即可得$D(f)$的值. 这样求得的$D(f)=D(a_1,\,a_2,\,\cdots,\,a_n)$称为$f(x)$的**判别式**. 从而, $f(x)$有重根当且仅当

$$D(f)=D(a_1,\,a_2,\,\cdots,\,a_n)=0\,.$$

例 2.2.2 求多项式$f(x)=x^2+px+q$的判别式.

解 设$g(x_1,\,x_2)=(x_1-x_2)^2$, 首项是x_1^2, 则

$$\varphi_1=\sigma_1^{2-0}\sigma_2^0=\sigma_1^2=(x_1+x_2)^2,$$

于是得

$$f_1(x_1,\,x_2)=g(x_1,\,x_2)-\varphi_1=(x_1-x_2)^2-(x_1+x_2)^2=-4x_1x_2.$$

又有

$$\varphi_2=-4\sigma_1^{1-1}\sigma_2^1=-4\sigma_2,$$

故

$$f_2(x_1,\,x_2)=f_1(x_1,\,x_2)-\varphi_2=0,$$

从而,

$$g(x_1,\,x_2)=\varphi_1+\varphi_2=\sigma_1^2-4\sigma_2.$$

于是,

$$D(f)=g(\alpha_1,\,\alpha_2)=\sigma_1(\alpha_1,\,\alpha_2)^2-4\sigma_2(\alpha_1,\,\alpha_2).$$

由韦达定理, $\sigma_1(\alpha_1,\,\alpha_2)=-p$, $\sigma_2(\alpha_1,\,\alpha_2)=q$. 因此,

$$D(f)=p^2-4q.$$

进一步, 请读者自己用类似方法证明三次多项式

$$x^3+a_1x^2+a_2x+a_3$$

的判别式是

$$D(f)=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3.$$

上面描述的是多项式判别式求解的一般原则, 具体的计算方法常常通过下节的结式理论.

习 题 2.2

1. 用初等对称多项式表出下列对称多项式:

   (1) $f(x_1,\,x_2,\,x_3,\,x_4)=(x_1x_2+x_3x_4)(x_1x_3+x_2x_4)(x_1x_4+x_2x_3)$;
   (2) $f(x_1,\,x_2,\,x_3)=(x_1+x_2)(x_1+x_3)(x_2+x_3)$;
   (3) $f(x_1,\,x_2,\,x_3)=(x_1-x_2)^2(x_2-x_3)^2+(x_2-x_3)^2(x_3-x_1)^2+(x_3-x_1)^2(x_1-x_2)^2$.

2. 用初等对称多项式表出下列n元对称多项式:

   (1) $\Sigma\, x_1^2x_2 \quad (n\geq 3)$;
   (2) $\Sigma\, x_1^2x_2^2x_3 \quad (n\geq 5)$;
   (3) $\Sigma\, x_1^3x_2^2x_3 \quad (n\geq 3)$;
   (4) $\Sigma\, x_1^3x_2x_3 \quad (n\geq 5)$.

   (这里$\Sigma\, x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$表示所有由 $x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$经过对换得到的项的和.)

3. 证明: 如果多项式$f(x)=x^3+px+q$的根为$x_1,\,x_2,\,x_3$, 则以

   $$y_1=(x_1-x_2)^2,\ y_2=(x_1-x_3)^2,\ y_3=(x_2-x_3)^2$$

   为根的首1多项式为$g(y)=y^3+6py^2+9p^2y+4p^3+27q^2$.

4. 证明: 四次方程$a_0x^4+a_1x^3+a_2x^2+a_3x+a_4=0\ \ (a_0\neq 0)$ 有两根之和为零的充要条件是:

   $$a_1^2a_4+a_0a_3^2-a_1a_2a_3=0.$$

§2.3 结式及二元高次方程组的求解

本节的目的是利用多项式理论和线性方程组求解, 给出二元高次方程组的求解方法. 我们的基本工具是所谓的结式.

首先, 讨论两个一元多项式有非常数公因式的条件.

引理 2.3.1 设$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$和$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m$是数域$\mathbb{P}$上的两个非零多项式, 且$a_0,\,b_0$均不为0. 那么$f(x)$和$g(x)$非互素的充要条件是在$\mathbb{P}[x]$中存在$u(x),\,v(x)$满足$1<\partial(u(x))<m,\ 1<\partial(v(x))<n$, 并且$u(x)f(x)=v(x)g(x)$.

证明 **必要性:** 令$(f(x),\,g(x))=d(x)\neq 1$, 那么, 存在$f_1(x),\,g_1(x)\in\mathbb{P}[x]$, 使得

$$f(x)=d(x)f_1(x),\ g(x)=d(x)g_1(x),$$

其中, $\partial(f_1(x))<\partial(f(x))\leq n,\ \partial(g_1(x))<\partial(g(x))\leq m$.

取$u(x)=g_1(x),\ v(x)=f_1(x)$, 则

$$u(x)f(x)=g_1(x)d(x)f_1(x)=g(x)v(x).$$

充分性: 因为$a_0 \neq 0$, 故$\partial(f(x)) = n$. 由条件, 存在$u(x), v(x) \in \mathbb{P}[x]$, 满足$\partial(u(x)) < m, \partial(v(x)) < n$, 使得$u(x)f(x) = v(x)g(x)$.

如果$(f(x), g(x)) = 1$, 则由$f(x) \mid v(x)g(x)$可得$f(x) \mid v(x)$, 这与$\partial(v(x)) < \partial(f(x))$矛盾. 故$f(x)$和$g(x)$非互素. □

由上述引理, $\partial(u(x)) < m$, $\partial(v(x)) < n$, 故不妨设

$$u(x) = u_0x^{m-1} + u_1x^{m-2} + \cdots + u_{m-1},$$
$$v(x) = v_0x^{n-1} + v_1x^{n-2} + \cdots + v_{n-1},$$

其中u_0, v_0可能为零.

两边乘法展开, 比较对应系数相等, 那么, 由$u(x)f(x) = v(x)g(x)$,

$$\begin{cases} a_0u_0 & = b_0v_0 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots x^{n+m-1} \\ a_1u_0 + a_0u_1 & = b_1v_0 + b_0v_1 \cdots\cdots\cdots\cdots\cdots\cdots x^{n+m-2} \\ a_2u_0 + a_1u_1 + a_0u_2 & = b_2v_0 + b_1v_1 + b_0v_2 \cdots\cdots\cdots x^{n+m-3} \\ & \vdots \\ a_nu_{m-2} + a_{n-1}u_{m-1} & = b_mv_{n-2} + b_{m-1}v_{n-1} \cdots\cdots\cdots x \\ a_nu_{m-1} & = b_mv_{n-1} \cdots\cdots\cdots\cdots\cdots\cdots\cdots 1 \end{cases} \tag{2.3.1}$$

把这$n+m$个等式看作$n+m$个未知数$u_0, u_1, \cdots, u_{m-1}, v_0, v_1, \cdots, v_{n-1}$的方程组. 令

$$\boldsymbol{A} = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & a_2 & \cdots & a_n & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & a_0 & a_1 & a_2 & \cdots & a_n \end{pmatrix}_{m\times(n+m)},$$

$$\boldsymbol{B} = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & b_2 & \cdots & b_m & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & b_0 & b_1 & b_2 & \cdots & b_m \end{pmatrix}_{n\times(n+m)}.$$

不难看出, 此线性方程组的系数矩阵$\boldsymbol{C}$的转置是$\boldsymbol{C}^{\mathrm{T}} = \begin{pmatrix} \boldsymbol{A} \\ -\boldsymbol{B} \end{pmatrix}$.

显然$|\boldsymbol{C}^{\mathrm{T}}| = 0$当且仅当行列式:

$$R(f,\ g) \triangleq \begin{vmatrix} \boldsymbol{A} \\ \boldsymbol{B} \end{vmatrix}$$

等于零.

因此$R(f,\ g) = 0$, 当且仅当$|\boldsymbol{C}^{\mathrm{T}}| = 0$, 当且仅当方程组(2.3.1)有非零解, 当且仅当存在非零的$u(x)$, $v(x)$, 满足$\partial(u(x)) < m$, $\partial(v(x)) < n$, 使得, $u(x)f(x) = v(x)g(x)$. 又由引理2.3.1, 当且仅当$f(x)$和$g(x)$在$\mathbb{P}[x]$中有非常数的公因式.

称$R(f,\ g)$是$f(x)$与$g(x)$的**结式**.

综上可得:

定理 2.3.2 设

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n,$$

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m$$

是$\mathbb{P}[x]$中的两个多项式, 且$a_0\neq 0,\ b_0\neq 0,\ m,\ n>0$. 那么, $f(x)$和$g(x)$有非常数的公因式当且仅当结式$R(f,\ g)=0$.

由于当$\mathbb{P}=\mathbb{C}$时, $f(x)$和$g(x)$有非常数的公因式当且仅当它们有公共根, 因此有

推论 2.3.3 设

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,$$

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m$$

是$\mathbb{C}[x]$中的两个多项式, 且$a_0\neq 0, b_0\neq 0$, 则$f(x)$和$g(x)$有公共根当且仅当$R(f,g)=0$.

由此推论, 我们可进一步给出解二元高次方程组的方法, 即:

假设$f(x,\ y),\ g(x,\ y)\in\mathbb{C}[x,\ y]$, 求解方程组

$$\begin{cases} f(x,\ y)=0,\\ g(x,\ y)=0 \end{cases} \tag{2.3.2}$$

在$\mathbb{C}$中的全部解.

事实上, $f(x,\ y)$和$g(x,\ y)$可以分别写成

$$F_y(x)=f(x,\ y)=a_0(y)x^n+a_1(y)x^{n-1}+\cdots+a_n(y),$$
$$G_y(x)=g(x,\ y)=b_0(y)x^m+b_1(y)x^{m-1}+\cdots+b_m(y),$$

其中$a_i(y), b_j(y)\ (i=0,1,\cdots,n; j=0,1,\cdots,m)$是$y$的多项式, 且$a_0(y)\neq 0, b_0(y)\neq 0$.

考虑上述方程组的解时, 实际上是将$f(x,\ y)$和$g(x,\ y)$看作$x,\ y\in\mathbb{C}$的多项式函数. 因此, 将y看作一个固定值时, $f(x,\ y)$和$g(x,\ y)$就成为了x的一元多项式函数.

令

$$\boldsymbol{A}=\begin{pmatrix} a_0(y) & a_1(y) & a_2(y) & \cdots & a_n(y) & 0 & \cdots & 0\\ 0 & a_0(y) & a_1(y) & a_2(y) & \cdots & a_n(y) & \cdots & 0\\ \vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \vdots\\ 0 & 0 & \cdots & a_0(y) & a_1(y) & a_2(y) & \cdots & a_n(y) \end{pmatrix}_{m\times(n+m)},$$

$$\boldsymbol{B}=\begin{pmatrix} b_0(y) & b_1(y) & b_2(y) & \cdots & b_m(y) & 0 & \cdots & 0\\ 0 & b_0(y) & b_1(y) & b_2(y) & \cdots & b_m(y) & \cdots & 0\\ \vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \vdots\\ 0 & 0 & \cdots & b_0(y) & b_1(y) & b_2(y) & \cdots & b_m(y) \end{pmatrix}_{n\times(n+m)}.$$

则

$$R_x(f,\ g)\triangleq R(F_y,\ G_y)=\begin{vmatrix} \boldsymbol{A}\\ \boldsymbol{B} \end{vmatrix}$$

是一个关于y的复系数多项式函数.

当$(x_0,\ y_0)$是方程组(2.3.2)的一个复数解, 那么x_0就是一元多项式$F_{y_0}(x)$和$G_{y_0}(x)$的一个公共根. 由推论2.3.3, 有$R(F_{y_0},\ G_{y_0})=0$, 从而y_0是$R(F_y,\ G_y)=0$的一个根. 由此可得:

定理 2.3.4 给定$f(x,\ y),\ g(x,\ y)\in\mathbb{C}[x,\ y]$. 若$(x_0,\ y_0)$是方程组

$$\begin{cases} f(x,\ y)=0,\\ g(x,\ y)=0 \end{cases}$$

的一个复数解, 那么y_0是$R_x(f,\ g)$的一个根. 反之, 若y_0是$R_x(f,\ g)$的一个根, 那么, 或者$a_0(y_0)=b_0(y_0)=0$, 或者存在一个复数x_0, 使$(x_0,\ y_0)$是该方程组的一个解.

证明 第一部分结论由前面讨论即得.

第二部分的证明: 反之, 假设y_0是$R_x(f,\ g)$的一个根.

当 $a_0(y_0)=b_0(y_0)=0$时, 总有$R_x(f,g)=0$, 这与y_0是$R_x(f,\ g)$的根的条件符合. 但这时定理2.3.2的条件不满足, 所以可以看出, 未必有x_0使得(x_0,y_0)是该方程组的解.

当$a_0(y_0)\neq 0,\ b_0(y_0)\neq 0$时, 由定理2.3.2知, $F_{y_0}(x)=f(x,y_0)$与$G_{y_0}(x)=g(x,y_0)$有关于x的非常数的公因式, 从而存在复数x_0, 使$(x_0,\ y_0)$是方程组(2.3.2)的一个解.

当$a_0(y_0)\neq 0,\ b_0(y_0)=0$时, 若所有$b_0(y_0),\ \cdots,\ b_m(y_0)$ 均为0, 则只要求出

$$F_{y_0}(x)=f(x,\ y_0)=a_0(y_0)x^n+a_1(y_0)x^{n-1}+\cdots+a_n(y_0)$$

的根x_0, 则(x_0,y_0)就是方程组(2.3.2)的一个解.

若存在l使得$b_0(y_0)=\cdots=b_{l-1}(y_0)=0$但$b_l(y_0)\neq 0$, 令$g_1(x)=b_l(y_0)x^{m-l}+\cdots+b_m(y_0)$, 则

$$R(f(x,y_0),\ g_1(x))=R(F_{y_0}(x),G_{y_0}(x))=R_x(f,g)(y_0)=0.$$

于是, 由定理2.3.2知, 存在一个复数x_0使$(x_0,\ y_0)$是方程组

$$\begin{cases} f(x,\ y)=0,\\ g_1(x)=0 \end{cases}$$

的一个解, 从而也是方程组(2.3.2)的一个解.

$a_0(y_0)=0,\ b_0(y_0)\neq 0$的情形同理. □

此定理后半部分说明, 只要先由$R_x(f,\ g)=0$求解出$y=y_0$, 将$y=y_0$代入方程组

$$\begin{cases} f(x,\ y)=0,\\ g(x,\ y)=0, \end{cases}$$

就成为求两个一元多项式公共根的问题. 若能求出其公共根$x=x_0$, 就可求得方程组的解$(x_0,\ y_0)$.

例 2.3.1 解方程组

$$\begin{cases} y^2-\ \ 7xy+4x^2+13x-2y-3=0,\\ y^2-14xy+9x^2+28x-4y-5=0. \end{cases}$$

解 原方程组改写为

$$\begin{cases} F_x(y)=f(x,\ y)=y^2-(\ 7x+2)y+(4x^2+13x-3)=0,\\ G_x(y)=g(x,\ y)=y^2-(14x+4)y+(9x^2+28x-5)=0, \end{cases}\tag{2.3.3}$$

于是,

$$R_y(f,\,g)=\begin{vmatrix} 1 & -7x-2 & 4x^2+13x-3 & 0\\ 0 & 1 & -7x-2 & 4x^2+13x-3\\ 1 & -14x-4 & 9x^2+28x-5 & 0\\ 0 & 1 & -14x-4 & 9x^2+28x-5 \end{vmatrix}$$

$$=\begin{vmatrix} 1 & -7x-2 & 4x^2+13x-3 & 0\\ 0 & 1 & -7x-2 & 4x^2+13x-3\\ 0 & -7x-2 & 5x^2+15x-2 & 0\\ 0 & 0 & -7x-2 & 5x^2+15x-2 \end{vmatrix}$$

$$\begin{aligned}&=(5x^2+15x-2)^2+(7x+2)^2(4x^2+13x-3)-(7x+2)^2(5x^2+15x-2)\\ &=(5x^2+15x-2)^2-(7x+2)^2(x+1)^2\\ &=(5x^2+15x-2-7x^2-9x-2)(5x^2+15x-2+7x^2+9x+2)\\ &=-24(x^2-3x+2)(x^2+2x)\\ &=-24x(x-1)(x-2)(x+2),\end{aligned}$$

从而, 得$R_y(f,\,g)$的4个根是$x=0,\,1,\,2,\,-2$.

将$x=0$代入原方程组, 得

$$\begin{cases} y^2-2y-3=0,\\ y^2-4y-5=0. \end{cases}$$

这个方程组中两个方程的根分别是$y=3,\,-1$和$y=5,\,-1$, 故有公共根$y=-1$, 于是得到原方程组的解是$(0,\,-1)$. 另外, 分别代入$x=1,\,2,\,-2$, 依次可得方程组的解是$(1,\,2)$, $(2,\,3)$, $(-2,\,1)$. 这四个解是方程组的全部解.

本节最后给出结式的计算公式和用于求解一元多项式判别式的公式.

定理 2.3.5 设$\mathbb{C}[x]$中多项式

$$f(x)=a_0x^n+\cdots+a_{n-1}x+a_n,\ g(x)=b_0x^m+\cdots+b_{m-1}x+b_m,$$

其中$a_0\neq 0,\ b_0\neq 0$. 令$\alpha_1,\cdots,\alpha_n$和$\beta_1,\cdots,\beta_m$分别是$f(x)$和$g(x)$的所有复根, 那么,

$$\begin{aligned}R(f,g)&=a_0^m\prod_{i=1}^{n}g(\alpha_i)\\ &=(-1)^{mn}b_0^n\prod_{j=1}^{m}f(\beta_j)\\ &=a_0^mb_0^n\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j).\end{aligned}$$

证明 对$g(x)$的次数进行归纳.

当$\partial(g(x))=1$, 即$g(x)=b_0x+b_1$时, $g(x)$有唯一根$\beta=-\dfrac{b_1}{b_0}$. 此时多项式$f(x)$与$g(x)$的

结式是

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n \\ b_0 & b_1 & 0 & \cdots & 0 & 0 \\ 0 & b_0 & b_1 & \cdots & 0 & 0 \\ \vdots & \cdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & b_1 & 0 \\ 0 & 0 & 0 & \cdots & b_0 & b_1 \end{vmatrix} \xrightarrow[i=1,2,\cdots,n]{C_{i+1}+\beta C_i}$$

$$\begin{vmatrix} a_0 & a_1+a_0\beta & \cdots & a_{n-1}+a_{n-2}\beta+\cdots+a_0\beta^{n-1} & f(\beta) \\ b_0 & 0 & \cdots & 0 & 0 \\ 0 & b_0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & b_0 & 0 \end{vmatrix}$$

$$= (-1)^n b_0^n f(\beta) = (-1)^n a_0 b_0^n (\beta-\alpha_1)\cdots(\beta-\alpha_n) = a_0 \prod_{i=1}^{n} g(\alpha_i)\,.$$

假设$\partial(g(x)) = m-1$时结论成立, 下证$\partial(g(x)) = m$时结论也成立.

当$g(x) = b_0x^m + \cdots + b_{m-1}x + b_m$时, 令$g(x) = (x-\beta_m)g_1(x)$, 其中$g_1(x) = c_0x^{m-1} + \cdots + c_{m-2}x + c_{m-1}$. 则有

$$b_0 = c_0,\ b_1 = c_1 - c_0\beta_m,\ \cdots,\ b_{m-1} = c_{m-1} - c_{m-2}\beta_m,\ b_m = -c_{m-1}\beta_m.$$

此时$f(x)$与$g(x)$的结式是

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_m & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & b_0 & b_1 & \cdots & b_m \end{vmatrix}$$

$$\xrightarrow[i=1,2,\cdots,n+m-1]{C_{i+1}+\beta_m C_i} \begin{vmatrix} a_0 & a_0\beta_m+a_1 & \cdots & f(\beta_m) & 0 & \cdots & 0 \\ 0 & a_0 & a_0\beta_m+a_1 & \cdots & f(\beta_m) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & a_0 & a_0\beta_m+a_1 & \cdots & f(\beta_m) \\ c_0 & c_1 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & c_0 & c_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & c_0 & c_1 & \cdots & 0 \end{vmatrix}$$

$$\xrightarrow[i=m-1,\cdots,2,1]{R_i-\beta_m R_{i+1}} \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & a_0 & a_1 & \cdots & f(\beta_m) \\ c_0 & c_1 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & c_0 & c_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & c_0 & c_1 & \cdots & 0 \end{vmatrix}$$

$$= (-1)^n f(\beta_m) R(f, g_1)$$

$$= (-1)^n f(\beta_m)(-1)^{(m-1)n} b_0^n \prod_{j=1}^{m-1} f(\beta_j)$$

$$= (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j)$$

$$= a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$$

$$= a_0^m \prod_{i=1}^{n} g(\alpha_i).$$

从而结论成立. □

定理 2.3.6 设$\mathbb{C}[x]$中多项式

$$f(x) = a_0 x^n + \cdots + a_{n-1} x + a_n,$$

其中$a_0 \neq 0$, 那么, $f(x)$的判别式

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

证明 设$f(x)$的所有复根是$\alpha_1, \cdots, \alpha_n$, 那么由定理2.3.5, 可得

$$R(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i). \tag{2.3.4}$$

由$f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n)$易得

$$f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j), \quad i = 1, \cdots, n.$$

将此代入(2.3.4)式, 得

$$R(f, f') = a_0^{2n-1} \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j). \tag{2.3.5}$$

对于任意i和j $(i < j)$, 在(2.3.5)式中, $\alpha_i - \alpha_j$和$\alpha_j - \alpha_i$这两个因子都出现了一次, 它们的乘积为$-(\alpha_i - \alpha_j)^2$. 由于满足$1 \leq i < j \leq n$的指标对(i, j)共有$\dfrac{n(n-1)}{2}$对, 所以由(2.3.5)式可得

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_0^{2n-1} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} a_0^{2n-1} D(f). \qquad \square$$

例 2.3.2 求二次多项式$f(x) = ax^2 + bx + c$的判别式.

解 $f'(x)=2ax+b$, 于是

$$\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = -a(b^2-4ac).$$

由定理2.3.6得,

$$D(f)=(-1)^{\frac{2(2-1)}{2}}a^{-(2\times 2-1)}R(f,f')=a^{-2}(b^2-4ac).$$

注意: 上述例2.3.2所得的二次多项式的判别式与在通常二次函数观点下所定义的判别式差一个常数a^{-2}, 这并不影响我们对于是否有重根的判别. 关键是本教材的判别式定义对任意阶多项式而言是完全自然的.

习 题 2.3

1. 证明: 三次多项式$x^3+a_1x^2+a_2x+a_3$ 的判别式是

$$D(f)=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3.$$

2. 求下列各题中f与g的结式:

(1) $f(x)=x^2-3x+2,\ g(x)=x^n+1$;
(2) $f(x)=\dfrac{x^5-1}{x-1},\ g(x)=\dfrac{x^7-1}{x-1}$;
(3) $f(x)=x^n+x+1,\ g(x)=x^2-3x+2$;
(4) $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$,
$g(x)=a_0x^{n-1}+a_1x^{n-2}+\cdots+a_{n-2}x+a_{n-1}$, 其中$a_0\neq 0,\ a_n\neq 0$.

3. 解下列各方程组:

(1) $\begin{cases} 5y^2-6xy+5x^2-16=0, \\ y^2-xy+2x^2-y-x-4=0. \end{cases}$
(2) $\begin{cases} x^2+y^2+4x-2y+3=0, \\ x^2+4xy-y^2+10y-9=0. \end{cases}$
(3) $\begin{cases} x^2y+x^2+2xy+y^3=0, \\ x^2-3y^2-6x=0. \end{cases}$

4. 当k取何值时, 多项式$f(x)=x^4-4x+k$有重根?
5. 求下列多项式的判别式:

(1) x^n+2x+1;
(2) x^n+2;
(3) $x^{n-1}+x^{n-2}+\cdots+x+1$.

6. 设多项式

$$f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_{m-1}x+a_m,$$
$$g(x)=b_0x^n+b_1x^{n-1}+\cdots+b_{n-1}x+b_n.$$

证明: $R(f,\ g)=0$的充要条件是: "$a_0=b_0=0$"与"$f(x)$和$g(x)$在复数域$\mathbb{C}$上有公共根"至少有一条成立.

7. 设$f(x)$, $g_1(x)$, $g_2(x)$分别为m次, s次和t次多项式, 证明:

$$R(f,\ g_1g_2) = R(f,\ g_1)R(f,\ g_2).$$

8. 证明: 多项式$f(x) = x^4 + px + q$有重因子的充要条件是$27p^4 = 256q^3$.

9. 设$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$. 证明:

(1) $R(f,g) = (-1)^{mn}R(g,f)$;

(2) 若a,b为常数, $R(af,bg) = a^mb^nR(f,g)$.

§2.4 多元多项式的几何

欧氏空间$\mathbb{R}^3$中的平面可以用一个线性函数的零点表示, 直线可以用两个线性函数的公共零点表示.给定数域K, 一个非零的n变量的线性函数的零点集可以看作K^n中的“超平面”, 而若干个线性函数的公共零点集可以看成低维的“平面”. 从而我们可以把一些欧氏空间中的几何结论推广到K^n 中, 例如平面束可以推广为:

命题 2.4.1 设$l_i = \sum_{j=1}^n a_{ij}x_j + b_i (1 \leq i \leq 2)$是两个线性函数, 且$v_1 := (a_{11}, a_{12}, ..., a_{1n})$与$v_2 := (a_{21}, a_{22}, ..., a_{2n})$线性无关.则线性函数$l = \sum_{j=1}^n t_ix_j + s_i$经过$l_1, l_2$的公共零点集当且仅当存在$k_1, k_2 \in K$使得$l = k_1l_1 + k_2l_2$.

证明 若$l = k_1l_1 + k_2l_2$, 则显然l经过l_1, l_2的公共零点集.为了证明另一半, 首先我们把一般情况约化到$b_1 = b_2 = 0$的情形. 任取$(c_1, c_2, ..., c_n)$满足$l_1(c_1, c_2, ..., c_n) = l_2(c_1, c_2, ..., c_n) = 0$. 定义坐标变换$x_i' = x_i - c_i$, l_1, l_2变换后为$l_i'(x_1', ..., x_n') = l_i(x_1' + c_1, ..., x_n' + c_n)(i = 1, 2)$, 则$l_1', l_2'$均经过原点, 即此时的$b_1' = b_2' = 0$.记变换后的$l$为$l'$, 不妨设$l' \neq 0$. 只需证明存在$k_1, k_2 \in K$使得$l' = k_1l_1' + k_2l_2'$. 因为$v_1, v_2$线性无关, 此时$l_1', l_2'$的公共零点集是$n-2$维的子空间$L$, 由于$l'$非零, l'的零点集是包含L的$n-1$维子空间. 在l'的零点集中取一个不在L 中的点$u := (u_1, u_2, ..., u_n)$, 则$l_1'(u), l_2'(u)$ 不全为零.则非零线性函数$l'' := l_2'(u)l_1' - l_1'(u)l_2'$的零点集包含$L$且经过$u$, 从而$l''$的零点集和$l'$的零点集相同.因此存在非零元素$k \in K$, 使得$l' = kl'' = kl_2'(u)l_1' + (-kl_1'(u))l_2'$. 命题得证. □

以上命题当然可以看作线性方程组的结论, 但是几何的证明更加方便.

一般的多元多项式的零点对应了更复杂的几何对象, 比如实变量的多项式$x^2 + yz - 1$的零点就是一个单叶双曲面, 而且多元多项式组和其公共零点集的对应关系也远比线性方程组复杂.我们引入一些术语来说明在代数几何中如何研究这些对象.

定义 2.4.1 设$f_1, f_2, ...f_m \in K[x_1, x_2, ..., x_n]$, 记它们的公共零点集为$Z(\{f_1, f_2, ..., f_m\})$, 即$Z(\{f_1, f_2, ..., f_m\}) = \{(a_1, a_2, ..., a_n) | f_i(a_1, a_2, ..., a_n) = 0, i = 1, 2, ..., m\}$. 更一般地, 对$T \subseteq K[x_1, x_2, ..., x_n]$, 定义$Z(T) = \{(a_1, a_2, ..., a_n) | \forall f \in T, f(a_1, a_2, ..., a_n) = 0\}$. 所有形如$Z(T)$的集合称为$K^n$中的代数集.

单点集是代数集: 任给$(a_1, a_2, ..., a_n) \in K^n$, 取$T = \{x_1 - a_1, x_2 - a_2, ..., x_n - a_n\}$, 则$Z(T) = (a_1, a_2, ..., a_n)$. 以上讨论的超平面是线性函数的零点集, 所以也是代数集.

命题2.4.1可以推广到多项式情形吗？如果$f=\sum_{i=1}^{n}f_ig_i$其中$g_i\in K[x_1,x_2,...,x_n]$, 那么$Z(\{f_1,f_2,...,f_m\})\subseteq Z(\{f\})$. 反过来, 如果$Z(\{f_1,f_2,...,f_m\})\subseteq Z(f)$, f一定可以写成$f=\sum_{i=1}^{n}f_ig_i$的形式吗？为了更好地表述这个问题, 我们引入以下定义.

定义 2.4.2 若非空子集$I\subseteq K[x_1,x_2,...,x_n]$满足

- $\forall f,f\in I,f-g\in I$, 即$I$在多项式加法下是群
- $\forall f\in I,\forall g\in K[x_1,x_2,...,x_n],fg\in I$

则称I是理想.

设$f_1,f_2,...f_m\in K[x_1,x_2,...,x_n]$, 由以上定义容易看出$I:=\{\sum_{i=1}^{n}f_ig_i|g_i\in K[x_1,x_2,...,x_n]\}$是理想, 称为由$f_1,f_2,...,f_m$生成的理想, 记为$(f_1,f_2,...,f_m)$. 易知$Z(\{f_1,f_2,...,f_m\})=Z((f_1,f_2,...,f_m))$, 所以以上问题等价于：

例 2.4.1 如果$Z((f_1,f_2,...,f_m))\subseteq Z(\{f\})$, 那么$f\in(f_1,f_2,...,f_m)$吗？

我们先看一个最简单的情况.

引理 2.4.2 给定$(a_1,a_2,...,a_n)\in K^n$, 记$m=(x_1-a_1,x_2-a_2,...,x_n-a_n)$, 则$Z(m)\subseteq Z(\{f\})$当且仅当$f\in m$.

证明 通过坐标变换不妨设$a_i=0$, 则$Z(m)\subseteq Z(\{f\})$等价于$f(0,0,...,0)=0$. 若$f=\sum_{i=1}^{n}x_ig_i$, 则显然$f(0,0,...,0)=0$. 反过来若$f(0,0,...,0)=0$, 则f的常数项为0, 依次将含有$x_1,x_2,...,x_n$的项合并, 可得$f=\sum_{i=1}^{n}x_ig_i(x_i,x_{i+1},...,x_n)$, 从而$f\in m$. □

一般而言问题2.4.1的结论是否定的, 一个直接的原因就是对任意$k\in\mathbb{N}^*$, f^k的零点集和f的零点集相同, 所以我们能够期望成立的结论是对某个$k\in\mathbb{N}^*$, $f^k\in(f_1,f_2,...,f_m)$. 在今后的交换代数课程中, 我们会知道当数域为$\mathbb{C}$(或一般的代数封闭域)时, 这是Hilbert零点定理的推论.$f=1$的特殊情况称为Hilbert零点定理的弱形式, 这和多项式的结式密切相关.下面我们对复数域上2元多项式的情形加以讨论, 一般情况可以用归纳法证明.

命题 2.4.3 设$f,g\in\mathbb{C}[x,y]$,则$f(x,y)=g(x,y)=0$无解的充要条件是存在$h_1,h_2\in\mathbb{C}[x,y]$, 使得$fh_1+gh_2=1$.

证明 如上讨论, 充分性是显然的.下面证明必要性.设$f(x,y)$中次数最高项为$\sum_{i=0}^{m}a_ix^iy^{m-i}$, 其中$a_i$不全为零；$g(x,y)$中次数最高项为$\sum_{i=0}^{n}b_ix^iy^{n-i}$, 其中$b_i$不全为零.考虑变量替换$x'=x,y'=y-cx$, 则$\sum_{i=0}^{m}a_ix^iy^{m-i}=\sum_{i=0}^{m}a_ix'^i(y'+cx')^{m-i},\sum_{i=0}^{n}b_ix'^i(y'+cx')^{n-i}$, 从而可选择$c$使得$f$中$x'^m$和$g$中$x'^n$的系数均非零, 即$f'(x',y')=f(x,y)=x'^n+...,g'(x',y')=g(x,y)=x^m+....$ 易知$f(x,y)=g(x,y)=0$等价于$f'(x',y')=g'(x',y')=0$无解, 而$f'=g'=0$的充要条件时$R_y(f,g)=0$有解, 其中R_y是f',g'作为x的多项式的结式. 所以$f'(x',y')=g'(x',y')=0$无解等价于结式R_y是非零常值多项式, 记为k.又存在h_1',h_2'使得$R_y=f'h_1'+g'h_2'$, 从而存在$h_1,h_2\in\mathbb{C}[x,y]$, 使得$fh_1+gh_2=k$, 两边除以$k$即得$fh_1+gh_2=1$. □

例 2.4.2 $f=x+y,g=x^2-y^2-1$, 此时$f\cdot(x-y)-g=1$, 所以$f=g=0$无解.

关于$Z(T)$还有如下的基本问题：

1. 对任意子集T, 总存在有限个多项式$f_1, f_2, ..., f_m$使得$Z(T) = Z(\{f_1, f_2, ..., f_m\})$吗?
2. 代数集的交是代数集吗? 代数集的并是代数集吗?

对$T \subseteq K[x_1, x_2, ..., x_n]$, 包含$T$的所有理想的交称为$T$生成的理想, 记为$(T)$, 则$Z(T) = Z((T))$. 根据交换代数中的结论, (T) 可有有限个多项式生成, 从而第一个问题的回答是肯定的, 这里我们就不给证明了.关于第二个问题, 我们可以证明下面的结论:

引理 2.4.4 设$Z(T_\alpha), \alpha \in J$是一族代数集, 则$\bigcap Z(T_\alpha)$是代数集; 设$Z(T_i), 1 \leq i \leq k$是有限个代数集, 则$\bigcup_{i=1}^{k} Z(T_i)$ 是代数集.

证明 令$T = \bigcup_{\alpha \in J} T_\alpha$, 则$Z(T) = \bigcap Z(T_\alpha)$为代数集.对有限个代数集的交, 我们仅需证明$k = 2$就能用归纳法得到一般结论.令$T = \{fg | f \in T_1, g \in T_2\}$, 则$Z(T_1) \bigcup Z(T_2) = Z(T)$成立: 首先若$(a_1, a_2, ..., a_n) \in Z(T_1) \bigcup Z(T_2)$, 不妨$(a_1, a_2, ..., a_n) \in Z(T_1)$, 则$\forall f \in T_1, f(a_1, a_2, ..., a_n) = 0$, 从而$fg(a_1, a_2, ..., a_n)$也均为0. 反过来, 若$(a_1, a_2, ..., a_n) \notin Z(T_1) \bigcup Z(T_2)$, 则有某个$f_0 \in T_1$和某个$g_0 \in T_2$使得$f_0(a_1, a_2, ..., a_n), g_0(a_1, a_2, ..., a_n)$均不为0, 从而$(f_0 g_0)(a_1, a_2, ..., a_n)$不为0, 所以$(a_1, a_2, ..., a_n) \notin Z(T)$. □

又明显有$Z(\{1\}) = \emptyset, Z(\{0\}) = K^n$, 因此$\mathcal{F} = \{Z(T) | T \subseteq K[x_1, x_2, ..., x_n]\}$定义了$K^n$上的拓扑, 称为Zariski拓扑, 该拓扑中的闭集就是代数集.

习 题 2.4

1. $l_i \in K[x_1, x_2, ..., x_n] (1 \leq i \leq m)$为若干个线性函数, 假设它们的公共零点集是空集, 证明存在$k_i \in K$, 使得$\sum_{i=1}^{m} k_i l_i = 1$.

2. 对$1 \leq i < j \leq 4$, 定义$W_{ij} \in K[x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4]$为$W_{ij} = x_i y_j - x_j y_i$, 证明$W_{14}^2 \in (W_{12}, W_{13}, W_{24}, W_{34}, W_{14} + W_{23})$, 并由此推出

$$Z(\{W_{12}, W_{13}, W_{14}, W_{23}.W_{24}, W_{34}\}) = Z(\{W_{12}, W_{13}, W_{24}, W_{34}, W_{14} + W_{23}\}).$$

§2.5* 多元高次方程组的消元法简介

宋元之交的杰出数学家朱世杰, 在《四元王鉴》中以天元、地元、人元、物元为未知数, 建立了高次联立方程组求解的消元法. 到近代, 多元多项式方程组的求解理论的研究促进产生了代数几何这个重要的理论分支的发展.

本节, 我们仅介绍求解多元高次方程组的初步理论①. 该理论通常被称为吴文俊-Ritt方法, 是吴文俊关于数学机械化工作的核心, 是方程求解、几何定理机器证明的基础. 这一方法是吴文俊基于中国古代数学的求解代数方程组消去法的思想并借鉴Ritt关于微分代数的工作 (J. F. Ritt. *Differential Algebra*. Amer. Math. Soc. Colloquium. 1950) 提出的.

本节中, 为书写方便, 我们总假设

① 本节材料来源于文献[17][18].

$$p(x)=p(x_1,x_2,\cdots,x_n)\in\mathbb{P}[x_1,x_2,\cdots,x_n]$$

是数域 $\mathbb{P}$上关于变元$x_1,\cdots,x_n$的一个 n元多项式. 如果 $p(x)$中实际出现的变元的最大下标为$i(1\leq i\leq n)$, 则称x_i为$p(x)$**的主变元**. 我们有

$$p(x)=I(x)\cdot x_i^{d_i}+(x_i\text{ 的低次项}),$$

其中 d_i是 $p(x)$对主元 x_i的最高次幂, 记作

$$d_i=\deg_{x_i}(p),$$

而$I(x)$是数域$\mathbb{P}$上关于变元$x_1,x_2,\cdots,x_{i-1}$ 的多项式, 一般称之为 $p(x)$的**初式**.

设 $p(x)$与 $q(x)$ 均为 $\mathbb{P}[x_1,x_2,\cdots,x_n]$ 中的多项式, $p(x)$的主变元为 x_i, 初式为 $I(x)=I(x_1,x_2,\cdots,x_{i-1})$, 则与一元多项式相类似, 成立如下**余式公式**

$$I^s(x)q(x)=\lambda(x)p(x)+R(x),\qquad \deg_{x_i}(R(x))<\deg_{x_i}(p(x)),\tag{2.5.1}$$

这里 s是某个非负整数, $R(x)\in\mathbb{P}[x_1,x_2,\cdots,x_n]$为多项式. 类似地, 我们称 $R(x)$为多项式 $q(x)$对 $p(x)$的**余式** .

定义 2.5.1 设 $p(x)$与 $q(x)$都是 $\mathbb{P}[x_1,x_2,\cdots,x_n]$ 中的多项式, 他们的主元分别为 x_i与 x_j , 若 $p(x)$中出现的 x_j的最高次幂(记作 $\deg_{x_j}(p(x))$)低于 $\deg_{x_j}(q(x))$, 或$\deg_{x_j}(p(x))<\deg_{x_j}(q(x))$, 则称多项式 $p(x)$对 $q(x)$已经**约化**.

定义 2.5.2 称 $\mathbb{P}[x_1,x_2,\cdots,x_n]$中的一个多项式组

$$(I):p_1(x),p_2(x),\cdots,p_r(x)$$

为一个**升列**, 如果它们满足:

(1) $\forall 1\leq i\leq r$, $p_i(x)$的主变元为 x_i, 此时, 我们称 (I)是三角化的;

(2) $\forall 1\leq j<i\leq r, p_i(x)$对 $p_j(x)$ 已经约化, 即

$$\deg_{x_j}(p_i(x))<\deg_{x_j}(p_j(x)).$$

依定义2.5.2, 数域 $\mathbb{P}$中任一非零常数构成一类特殊的升列. 通常, 我们称之为**矛盾升列**.

设 $p(x)\in\mathbb{P}[x_1,x_2,\cdots,x_r]$, $p_1(x),p_2(x),\cdots,p_r(x)$ 是 $\mathbb{P}[x_1,x_2,\cdots,x_r]$中的升列多项式, 则依余式公式(2.5.1)可得,

$$\begin{aligned}
&I_r^{s_r}(x)p(x)=\lambda_r(x)p_r(x)+R_{r-1}(x), && \deg_{x_r}(R_{r-1}(x))<\deg_{x_r}(p_r(x))\\
&I_{r-1}^{s_{r-1}}(x)R_{r-1}(x)=\lambda_{r-1}(x)p_{r-1}(x)+R_{r-2}(x), && \deg_{x_{r-1}}(R_{r-2}(x))<\deg_{x_{r-1}}(R_{r-1}(x))\\
&\qquad\vdots && \qquad\vdots\\
&I_2^{s_2}(x)R_2(x)=\lambda_2(x)p_2(x)+R_1(x), && \deg_{x_2}(R_1(x))<\deg_{x_2}(R_2(x))\\
&I_1^{s_1}(x)R_1(x)=\lambda_1(x)p_1(x)+R_0(x), && \deg_{x_1}(R_0(x))<\deg_{x_1}(R_1(x))
\end{aligned}$$

从而有

$$I_1^{s_1}(x)I_2^{s_2}(x)\cdots I_r^{s_r}(x)p(x)=Q_r(x)p_r(x)+Q_{r-1}(x)p_{r-1}(x)+\cdots+Q_1(x)p_1(x)+R_0(x)\tag{2.5.2}$$

这里 $I_1(x),I_2(x),\cdots,I_r(x)$为上述余式公式所确定, $Q_1(x),Q_2(x),\cdots,Q_r(x)$由这些余式公式中的多项式经过乘法及加法运算所确定. 一般地, 我们称公式(2.5.2)为**多项式** $p(x)$**关于升列** $p_1(x),p_2(x),\cdots,p_r(x)$ **的余式公式**, 称$\mathbb{P}$上关于$x_1,x_2,\cdots,x_r$ 的多

项式 $R_0(x)$ 为 **多项式** $p(x)$**关于升列** $p_1(x), p_2(x), \cdots, p_r(x)$ **的余项**, 它满足

$$\deg_{x_i}(R_0(x)) < \deg_{x_i}(p_i(x)), \quad i = 1, 2, \cdots, r.$$

设 (PS) : $p_1(x), p_2(x), \cdots, p_r(x)$ 是数域 $\mathbb{P}$上关于变元$x_1, x_2, \cdots, x_n$的一个多项式组, 将他们按主变元进行分类, 主变元为 x_i的类记作 (x_i). 取出 (x_i)中一个关于x_i的幂最低的多项式, 则这些多项式形成 PS的一个部分组, 记这个部分组为 PPS.

定义 2.5.3 *若 PPS中的多项式构成一个升列, 即其任意两个多项式之间都已约化, 则称 PPS为 PS的一组***基列***. PS的一组基列通常记做BS.*

基列BS是一个升列. 多项式组 PS的一组基列可以通过如下步骤寻找. 将 (PS)的类 (x_i)排序如下:

$$(x_{i_1}), (x_{i_2}), \cdots, (x_{i_k}), \quad 1 \le i_1 \le i_2 \le \cdots \le i_k \le r.$$

在 (x_{i_1})中选出 x_{i_1}的一个最低幂次的多项式 $B_1(x)$, 这样的 $B_1(x)$ 总是存在的. 在(x_{i_2})中寻找 x_{i_2} 的最低幂次多项式 $B_2(x)$, 使 $B_1(x)$与 $B_2(x)$约化. 若这样的 $B_2(x)$存在, 则记$B = \{B_1(x), B_2(x)\}$. 若 (x_{i_2})中不存在这样的 $B_2(x)$, 则记$B = \{B_1(x)\}$. 在(x_{i_3})中寻找 x_{i_3}的最低幂次多项式 $B_3(x)$, 使之与 B中的多项式均约化. 若这样的$B_3(x)$存在, 则记$B = \{B_1(x), B_2(x), B_3(x)\}$, 否则 B不变. 依次选遍所有的类, 所得的B中多项式便构成多项式组 PS的一个基列.

吴-Ritt方法的主要目的, 就是将一个多元多项式方程组转化为一个"梯形" 形式的多元多项式方程组. 从这点看, 它类似于求解线性方程组的 Gauss消元法. 利用上述所建立的概念, 以下我们介绍吴-Ritt消元法.

设$f_i(x) \in \mathbb{P}[x], (i = 1, 2, \cdots, m)$ 为 $\mathbb{P}$上关于变元$x_1, x_2, \cdots, x_n$ 的多项式组, 记

$$PS = \{f_1(x), f_2(x), \cdots, f_m(x)\}.$$

消元法分为三步:

第一步: 选出 PS的一组基列 BS, 将 PS中的每一个多项式$f_i(x)(i = 1, 2, \cdots, m)$对 BS求余, 所得的非零余式的全体记为 RS.

第二步: 把 RS中的所有多项式添加到 PS中得到新的一多项式组 PS_1, 取出其一组基列 BS_1, 将 PS_1中的每一个多项式对 BS_1 求余, 所得的非零多项式的全体记为RS_1.

第三步: 若已得多项式组$PS_{i-1}(i > 1)$, 选出其一组基列BS_{i-1}, 把PS_{i-1}中的每一个多项式对BS_{i-1}求余, 将所有不为零的余式添入PS_{i-1}中得到新的多项式组BS_i. 由于 PS中多项式是给定的, 变元个数及其相应的幂次都是有限的, 每经过一次对升列的求余, 余式的主变元幂次都要减少或降低. 因此, 经过有限次重复求余后, 可得多项式组PS_k及其一组基列BS_k, 使得PS_k中的任何多项式对BS_k的余式RS_k均为零.

这里BS_k是一组升列, 为"梯形"形式的多项式方程组. 上述通过求余得到的BS_k的过程称为**吴-Ritt消元过程**, 也称为**整序过程**.

假设

$$RS_k = \{R_1^k(x) = 0, R_2^k(x), \cdots, R_s^k(x)\},$$

吴-Ritt理论证明了多项式方程组

$$\begin{cases} f_1(x)=0, \\ f_2(x)=0, \\ \quad\vdots \\ f_m(x)=0 \end{cases}$$

的零点集与上述BS_k中多项式所形成的方程组

$$\begin{cases} R_1^k(x)=0, \\ R_2^k(x)=0, \\ \quad\vdots \\ R_s^k(x)=0 \end{cases}$$

的零点集有着非常紧密的联系(吴-Ritt零点分解定理).

例 2.5.1 试利用吴方法简化下列多项式方程组

$$\begin{cases} -x_2^2+x_1x_2+1=0, \\ -2x_3+x_1^2=0, \\ -x_3^2+x_1x_2-1=0. \end{cases}$$

解 为了书写的方便, 本例简记

$$PS=\{p_1,p_2,p_3\},$$

其中

$$p_1=-x_2^2+x_1x_2+1,\quad p_2=-2x_3+x_1^2,\quad p_3=-x_3^2+x_1x_2-1.$$

显然,

$$(x_1)=\emptyset\,(\text{空集}),\quad (x_2)=\{p_1\},\quad (x_3)=\{p_2,p_3\}.$$

在这里以及整本书中, $\emptyset$ 都表示空集. 从而,

$$PPS=\{p_1,p_2\}.$$

由于PPS 中的两个多项式已经约化, 故

$$BS=PPS.$$

将PS中的每一个多项式对BS求余:

$$p_1=1\cdot p_1+0p_2+0,\ \ p_2=0p_1+1\cdot p_2+0,\ \ 4p_3=0p_1+(x_3+x_1^2)p_2+r_1,$$

这里$r_1=4(x_2x_1-1)-x_1^4$. 因此,

$$RS=\{r_1\}.$$

令

$$PS_1=\{p_1,p_2,p_3,r_1\},$$

对于PS_1, 我们有

$$(x_1)=\emptyset,\quad (x_2)=\{p_1,r_1\},\quad (x_3)=\{p_2,p_3\}.$$

易知

$$PPS_1 = \{p_2, r_1\}, \quad BS_1 = PPS_1.$$

将PS_1中的每一个多项式对BS_1求余, 可得p_2, p_3, r_1所对应余项均为0而p_1所对应余式为

$$r_2 = x_1^8 + 4x_1^6 - 8x_1^4 - 16x_1^2 + 16,$$

故

$$RS_1 = \{r_2\}.$$

令

$$PS_2 = \{p_1, p_2, p_3, r_1, r_2\},$$

则

$$(x_1) = \{r_2\}, \quad (x_2) = \{p_1, r_1\}, \quad (x_3) = \{p_2, p_3\}.$$

仿前可得

$$PPS_2 = \{p_2, r_1, r_2\}, \quad BS_2 = PPS_2.$$

由于PS_2中的每个多项式对BS_2求余所得的余式均为0, 故所得的与原方程组零点相关的"梯形"形式方程组为

$$\begin{cases} r_2 = 0, \\ r_1 = 0, \\ p_2 = 0. \end{cases} \quad \text{或} \quad \begin{cases} x_1^8 + 4x_1^6 - 8x_1^4 - 16x_1^2 + 16 = 0, \\ 4(x_2x_1 - 1) - x_1^4 = 0, \\ -2x_3 + x_1^2 = 0. \end{cases}$$

对本节课题有兴趣的读者可进一步参看数学机械化方面的书籍, 比如[16][17][18].

补 充 题

1. 求下列曲线的直角坐标方程:

$$x = t^2 - t + 1, \ y = 2t^2 + t - 3.$$

2. 求参数曲线

$$\begin{cases} x = \dfrac{2(t+1)}{t^2+1}, \\ y = \dfrac{t^2}{2t-1} \end{cases}$$

的直角坐标方程.

3. 设x_1, x_2, x_3为$f(x) = 2x^3 + x^2 - 3x + 2$的根, 求

$$\varphi = \frac{x_2}{x_1} + \frac{x_1}{x_2} + \frac{x_3}{x_2} + \frac{x_2}{x_3} + \frac{x_1}{x_3} + \frac{x_3}{x_1}$$

的值.

4. (本题针对具备置换群初步知识的读者) 设$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \in S_5$. 将$\sigma$表示成一些不相交的圈, 并将它写成几个对换的乘积.

5*. (本题针对具备"群的作用"初步知识的读者)利用性质"任意$\sigma \in S_n$可写成若干对换的乘积", 证明: $f(x_1, \cdots, x_n) \in \mathbb{P}[x_1, \cdots, x_n]$是对称多项式$\Leftrightarrow \sigma \cdot f(x_1, \cdots, x_n) = f(x_1, \cdots, x_n), \forall \sigma \in S_n$.

6. 证明：映射$\phi : \mathbb{P}[x_1, \cdots, x_n] \to V = \{f : \mathbb{P}^n \to \mathbb{P}\}, f(x_1, \cdots, x_n) \mapsto f$, 保持乘法.
7. (1) 已知当$y = x$时, 二元多项式$h(x, y) = 0$, 即, $h(x, x) = 0$(零多项式).证明：$y - x | h(x, y)$.(比如$x^n - y^n$就是一个例子.)

   (2) 已知当$y = ax + b$时, 二元多项式$h(x, y) = 0$.证明：$y - ax - b | h(x, y)$.