中国科学院指定考研参考书

線性代數

李炯生　查建国　编著

中国科学技术大学出版社

1989

内 容 提 要

本书是作者在中国科学技术大学数学系多年教学的基础上编写而成的. 它由多项式、行列式、矩阵、线性空间、线性变换、Jordan 标准形、Euclid 空间、酉空间和双线性函数等九章组成. 在内容的叙述上,力图做到矩阵方法与几何方法并重. 每章都配有丰富的典型例题和充足的习题可供读者选用.

附录中收录龚昇教授编著的《线性代数五讲》,从现代数学,尤其是模论的观点来重新审视与认识线性代数,讨论了向量空间、线性变换,着重研究了主理想整环上的模及其分解,并以此来重新理解向量空间在线性算子作用下的分解,可以使读者从高一个层次上来认识线性代数.

本书适合作为综合性大学理科数学专业的教材,也可以作为各类大专院校师生的教学参考书,以及关心线性代数与矩阵论的科技工作者和数学爱好者的自学读物或参考书.

图书在版编目 (CIP) 数据

线性代数 / 李炯生,查建国编著. —合肥: 中国科学技术大学出版社,1989 (2005.9 重印,2010.10 重排)

(中国科学院指定考研参考书)

ISBN 978-7-312-00110-9

I. 线… II. ① 李… ② 查… III. 线性代数—高等学校—教材 IV. O 151.2

中国版本图书馆 CIP 数据核字(2003)第 078690 号

郑 重 声 明

序　言

本书初稿完成于1983年. 当时中国科学技术大学数学系领导冯克勤教授委托编著者编写一本供数学系用的线性代数讲义. 接受这项任务后,我们专程到北京,拜访了中国科学院系统科学研究所万哲先研究员、中国科学院数学研究所许以超研究员、北京大学数学系聂灵沼教授和中国科学院研究生院曾肯成教授,请教他们对数学系线性代数教学的设想. 他们都热情地给予指导,从而为编写讲义提供了坚实的基础. 1984年春天,讲义便开始在数学系83级使用,并作为数学系线性代数教材一直使用到现在. 1985年,讲义曾获得中国科学技术大学首次颁发的优秀教材一等奖. 此后,在使用过程中对讲义又作了进一步的修改. 出版前编著者又作了全面的加工和充实.

线性代数研究的是线性空间以及线性空间的线性变换. 在线性空间取定一组基下,线性变换便和矩阵建立了一一对应关系. 这样,线性变换就和矩阵紧密联系起来. 于是,研究线性空间以及线性空间关于线性变换的分解即构成了线性代数的几何理论,而研究矩阵在各种关系下的分类问题则是线性代数的代数理论. 本书编写的一个着眼点是,着力于建立线性代数的这两大理论之间的联系,并从这种联系去阐述线性代数的理论.

当然,线性代数内容非常丰富,本书尽可能地按照1980年教育部颁发的综合性大学理科数学专业高等代数教学大纲进行选择,并在体系安排与叙述方式上尽量吸收中国科学技术大学数学系长期从事线性代数教学的老师与同事们,特别是曾肯成教授、许以超研究员的教学经验. 在处理行列式理论时,采用了曾肯成教授1965年首先在中国科学技术大学数学系使用的将n阶行列式视为数域$\mathbb{F}$上的n维向量空间的规范反对称n重线性函数的讲法; 在处理线性方程组理论时,利用了矩阵在相抵下的标准形理论; 在处理Jordan标准形时,先考虑了线性空间关于线性变换的分解,然后再用纯矩阵方法处理了Jordan标准形. 同时也着重于阐述已故著名数学家华罗庚教授的独具特色的矩阵方法.

为了便于读者掌握解题技巧,提高分析问题、解决问题的能力,本书几乎每一章都专门用一节讲述各种典型例题. 这部分内容是为习题课安排的. 每一节后面都附有大量习题,教师与读者可以根据具体情况选择使用. 这些习题除了在众多的线性代数、矩阵论教材以及习题集中选取之外,有一些是取自我国历届研究生试题,还有一些是自己编撰的. 在教学过程中,有些同学对线性代数的某些课题产生了兴趣,进行了一些研究. 有些结果即成为本书的习题. 这里应该提到的有中国科学技术大学数学系 81 级同学陈贵忠、黄瑜、窦昌柱,82 级同学陈秀雄等.

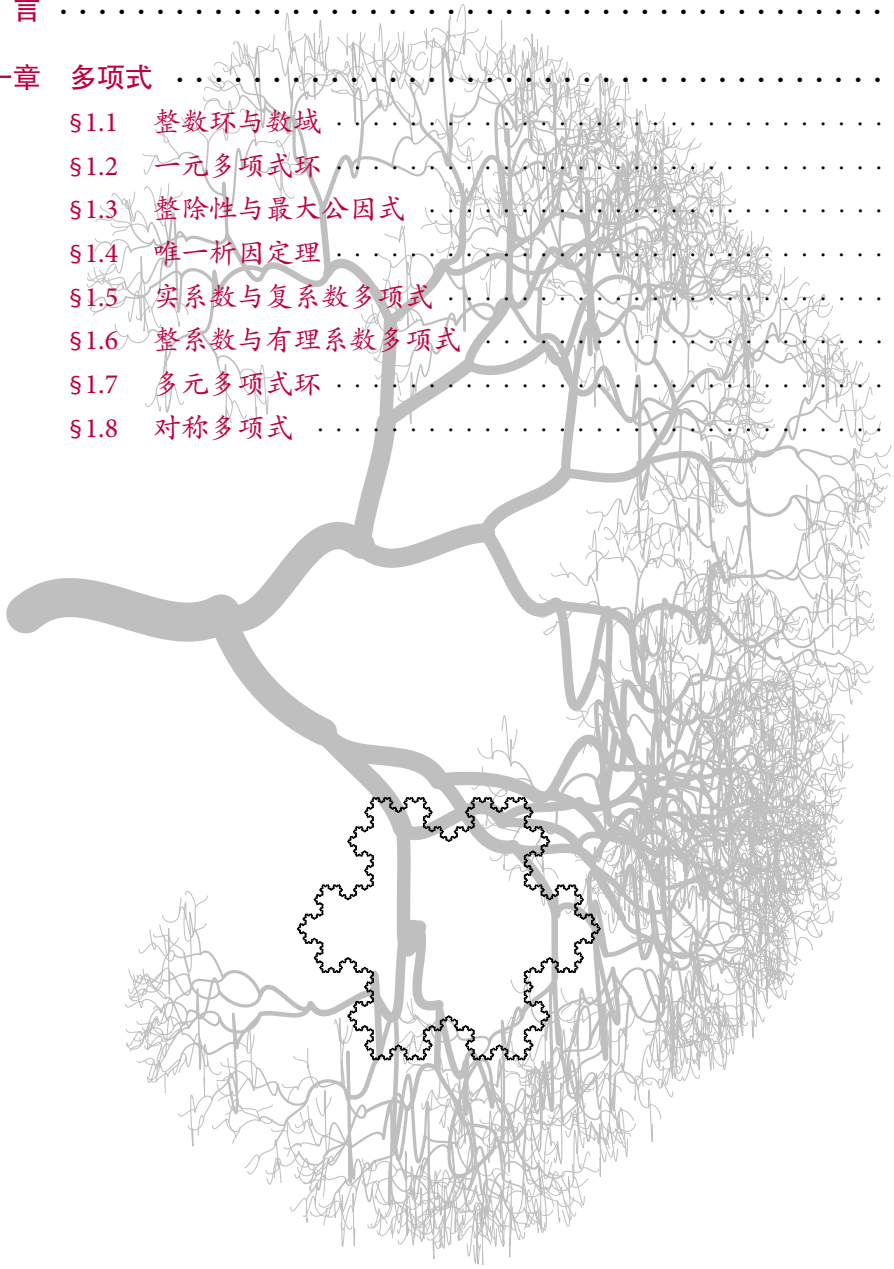
冯克勤教授对本书的编写自始至终都给予了热情的关心与帮助. 在编写过程中,得到万哲先、许以超、聂灵沼、曾肯成等研究员和教授的热心指导,编者谨致衷心感谢. 中国科学技术大学数学系陆洪文教授,杜锡录、李尚志副教授曾经使用本书的前身——《线性代数讲义》——作为教材,他们对讲义的修改提出许多有益的意见. 中国科学技术大学数学系讲师屈善坤、徐俊明协助编者仔细地审核了原稿,安徽大学数学系夏恩虎同志、中国科学技术大学 86 级硕士研究生黄道德审核了习题,在此一并致谢.

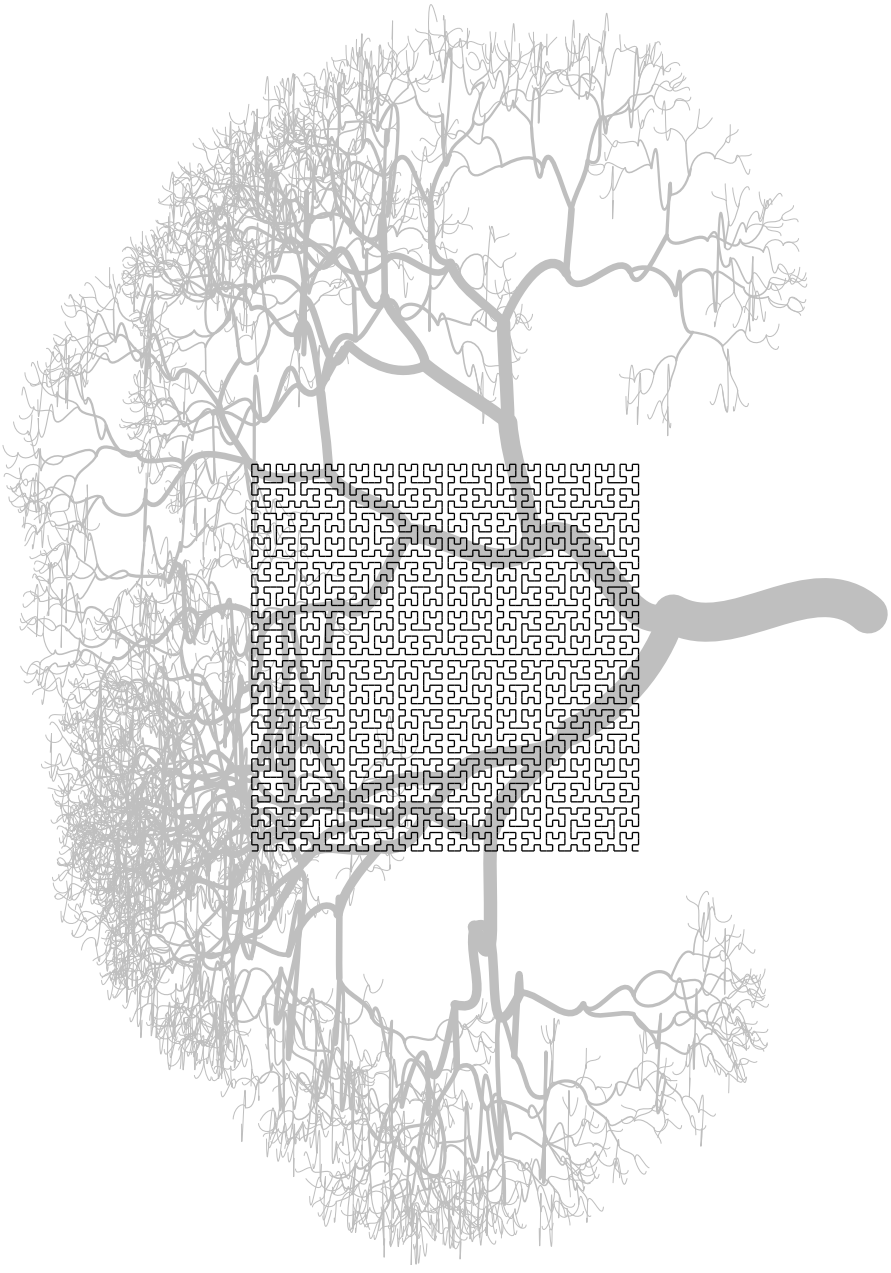
由于编著者水平所限,错误与缺点在所难免. 热忱欢迎同行们和广大读者批评指正.

李炯生　查建国

一九八八年元月于合肥

目　录





第一章

多项式

- 本章将介绍数域上的多项式理论. 读者如果有机会学习抽象代数中的环论的话,将会对本章的内容有更深刻的理解.
- §1.1 从代数的观点定义了数环与数域,即具有加法与乘法两种运算且满足一定的运算规则的数的集合.
- §1.2 给出了一元多项式环的定义,以及多项式的加法与乘法的基本性质. 读者将会看到,多项式有许多性质与整数相类似.
- §1.3 讨论了多项式的整除性以及一组多项式的最大公因式,这里的关键是两个多项式的辗转相除法.
- §1.4 给出了本章的第一个主要定理——唯一析因定理,即每一个多项式都可以唯一地写成不可约多项式的乘积. 读者把它同整数中的算术基本定理进行比较,就可知道这一定理的重要意义.
- 根据唯一析因定理,不可约多项式的地位相当于整数中素数的地位. 因此,自然需要一些方法来判定多项式的不可约性. §1.5 说明了复系数不可约多项式只能是一次多项式,而实系数不可约多项式只能是一次或二次多项式.
- §1.6 给出了最有应用价值的判断整系数多项式不可约性的 Eisenstein 准则.
- §1.7 把一元多项式推广为多元多项式.
- §1.8 含本章的第二个主要定理——对称多项式基本定理,即每一个对称多项式都是基本对称多项式的多项式.

§1.1 整数环与数域

迄今为止,我们已经接触到的数系有自然数系,整数系,有理数系,实数系与复数系. 在这些数系中,都可以进行加法运算与乘法运算. 譬如,自然数系中的加法运算是指一个对应关系,即对于任意一对自然数 m 与 n,按照加法,可以确定唯一一个自然数与它们对应,这个自然数就是 m 与 n 的和 $m+n$; 而自然数系中的乘法运算也是一个对应关系,即对于任意一对自然数 m 与 n,按照乘法,可以确定唯一一个自然数与它们对应,这个自然数就是 m 与 n 的积 mn.

抽象地说,所谓集合 S 中的**代数运算**是指一个对应关系,即对于集合 S 中任意一对元素 a 与 b,按照这一对应关系,可以确定集合 S 中的唯一一个元素 c 与它们对应. 例如,复数的加,减,乘,除四则运算都是复数系中的代数运算.

一个集合引进了代数运算,这些代数运算往往具有某些性质. 例如,整数系的加法运算与乘法运算具有以下的性质:

(A1) 加法结合律

$$(a+b)+c=a+(b+c);$$

(A2) 加法交换律

$$a+b=b+a;$$

(A3) 有整数 0,它具有性质:

$$a+0=0+a=a;$$

(A4) 对每个整数 a,总有负数 $-a$,使得

$$a+(-a)=(-a)+a=0;$$

(M1) 乘法结合律

$$(ab)c=a(bc);$$

(M2) 乘法交换律

$$ab=ba;$$

(M3) 有整数 1,它具有性质,

$$a1=1a=a;$$

(D) 加乘分配律

$$a(b+c)=ab+ac,$$

其中 a,b 和 c 是任意整数.

集合 S 的每一种代数运算所适合的一些最基本的性质,以及不同代数运算之间最基本的联系便构成了界定这些代数运算的**公理**. 例如,上面提到的整数的加法与乘法就适合结合律,交换律以及加乘分配律等.

把整数系连同加法与乘法运算的特性抽象化,便引出以下的定义.

定义 1.1.1 在集合 R 中规定两种代数运算,一种称为**加法**运算,即对于集合 R 中任意一对元素 a 与 b,按照加法运算,集合 R 中有唯一一个元素 $a+b$ 与它们对应,元素 $a+b$ 称为 a 与 b 的**和**. 另一种称为**乘法**运算,即对于集合 R 中任意一对元素 a 与 b,按照乘法运算,集合 R 中有唯一一个元素 ab 与它们对应,元素 ab 称为 a 与 b 的**积**.

并且,加法运算与乘法运算适合下列**公理**:对于 R 中任意元素 a,b 与 c,有

(A1) 加法结合律

$$(a+b)+c=a+(b+c);$$

(A2) 加法交换律

$$a+b=b+a;$$

(A3) 存在零元素 R 中存在一个元素,它称为 R 的**零元素**,记作 0,使得

$$a+0=0+a=a;$$

(A4) 存在负元素 对于 R 中每个元素 a,存在元素 b,使得

$$a+b=b+a=0,$$

元素 b 称为元素 a 的**负元素**,记为 $-a$;

(M1) 乘法结合律

$$a(bc) = (ab)c;$$

(M2) 乘法交换律

$$ab = ba;$$

(M3) 存在单位元素 R 中存在一个元素，它称为**单位元素**，记为 1，使得

$$a1 = 1a = a;$$

(D) 加乘分配律

$$a(b+c) = ab + ac,$$

则集合 R 称为**交换环**.

容易验证，整数系是一个交换环，它称为整数环，记为 $\mathbb{Z}$. 另外，有理数系，实数系与复数系也都是交换环，它们都是复数系的子集合.

凡复数系的子集合，如果对复数的加法与乘法成为交换环，则称为**数环**.

应当指出，有理数系，实数系和复数系的乘法运算所具有的性质有些是和整数环的乘法性质不同的. 例如，在整数环中，对于非零整数 $a \neq \pm 1$，不存在整数 b，使得 $ab = ba = 1$；但在实数环中，对于非零实数 a，一定存在实数 b，使得 $ab = ba = 1$. 为区别起见，引进以下的定义.

定义 1.1.2 设 $\mathbb{F}$ 是至少有两个元素的交换环. 如果对于 $\mathbb{F}$ 中每个非零元素 a，存在元素 $b \in \mathbb{F}$，使得 $ab = ba = 1$，则 b 称为 a 的**逆元素**，记作 a^{-1}. 这时交换环 $\mathbb{F}$ 称为**域**.

例如，有理数系，实数系与复数系都是域，它们依次称为有理数域，实数域与复数域，并依次记为 $\mathbb{Q}$，$\mathbb{R}$ 和 $\mathbb{C}$.

如果复数域 $\mathbb{C}$ 的子集合 $\mathbb{F}$ 对复数的加法与乘法成为一个域，则 $\mathbb{F}$ 称为**数域**.

可以验证，复数域的子集合

$$\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$$

对复数的加法与乘法成为一个域，所以，$\mathbb{Q}\left[\sqrt{2}\right]$ 是一个数域.

习 题 1.1

1. 记 $\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$. 验证 $\mathbb{Q}\left[\sqrt{2}\right]$ 是数域.

2. 记 $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$. 验证 $\mathbb{Z}\left[\sqrt{2}\right]$ 是数环. $\mathbb{Z}\left[\sqrt{2}\right]$ 是数域吗?

3. 设 $\mathbb{F}$ 是数域，a, b 和 c 是 $\mathbb{F}$ 中的任意三个元素，证明下列性质成立.

(1) 如果 $a + b = a + c$，则 $b = c$；

(2) 定义 $a - b = a + (-b)$，则 $a + (b - a) = b$；

(3) $a0 = 0a = 0$；

(4) $(-1)a = -a$；

(5) 如果 $ab = 0$，则 $a = 0$，或 $b = 0$.

4. 设 $\mathbb{F}$ 是所有有序实数对 (a, b) 的集合，其中 $a, b \in \mathbb{R}$.

(1) 如果集合 $\mathbb{F}$ 的加法与乘法分别定义为

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b)(c, d) = (ac, bd),$$

那么 $\mathbb{F}$ 是否成为域?

(2) 如果 $\mathbb{F}$ 的加法与乘法分别定义为

$$(a,b)+(c,d)=(a+c,b+d),\quad (a,b)(c,d)=(ac-bd,ad+bc),$$

那么 $\mathbb{F}$ 是否成为域?

(3) 如果 $\mathbb{F}$ 表示所有有序复数对的集合; 加法与乘法仍如 (1) 与 (2) 那样规定,结论又怎样?

5. 证明,在交换环的定义中,如果除加法交换律外,其它公理都假定成立,则可以推出加法交换律也成立. 换句话说,在交换环的定义中,加法交换律这一公理可以去掉.

§1.2　一元多项式环

在中学里,我们遇到过一次方程与二次方程,它们可以从两方面推广. 一方面从次数推广,即推广为 3 次,4 次以至 n 次的方程; 另一方面从系数所属的范围推广. 由 §1.1 可以看到,系数所属的实数域可以推广为其它的数域. 这就引出以下的定义.

定义 1.2.1　设 $\mathbb{F}$ 是数域,x 是未定元,$a_1,a_2,\ldots,a_n\in\mathbb{F}$,$a_n\neq 0$,$n$ 是非负整数. 则

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

称为**数域 $\mathbb{F}$ 上的一元多项式**,数域 $\mathbb{F}$ 上的一元多项式 $f(x)$ 的全体所成的集合记为 $\mathbb{F}[x]$. 其中 a_ix^i 称为多项式 $f(x)$ 的 ***i* 次项**,数 a_i 称为 $f(x)$ 的 ***i* 次项系数**.

特别地,a_0 称为 $f(x)$ 的**常数项**,a_nx^n 称为 $f(x)$ 的**首项**(或**最高次项**),a_n 称为 $f(x)$ 的**首项系数**. 如果 $a_n=1$,则 $f(x)$ 称为**首一多项式**.

非负整数 n 称为 $f(x)$ 的**次数**,记为 $\deg f(x)$.

如果多项式 $f(x)$ 的系数全为零,则 $f(x)$ 称为**零多项式**,这时仍记为 0. 约定零多项式的次数为 $-\infty$. 注意,零次多项式不是零多项式. 有时也称零次多项式为**纯量多项式**.

如果上述定义中,把数域 $\mathbb{F}$ 改成数环,则 $f(x)$ 称为**数环 $\mathbb{F}$ 上的一元多项式**,其它的规定是相同的.

设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad a_n\neq 0;$$
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0,\quad b_m\neq 0$$

是数域 $\mathbb{F}$ 上的两个多项式. 如果 $f(x)$ 与 $g(x)$ 适合 $a_i=b_i$,$i=0,1,2,\ldots$,则 $f(x)$ 与 $g(x)$ 称为**相等**,记为 $f(x)=g(x)$.

多项式 $f(x)$ 与 $g(x)$ 的**和 $f(x)+g(x)$** 定义为多项式

$$(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots,$$

即多项式 $f(x)+g(x)$ 的 i 次项系数为 a_i+b_i,$i=1,2,\ldots$. 其中当 $n\geqslant m$ 时,约定 $g(x)$

的系数 $b_{m+1}, b_{m+2}, \ldots, b_n$ 都为零，而当 $n < m$ 时，约定 $f(x)$ 的系数 $a_{n+1}, a_{n+2}, \ldots, a_m$ 都为零. 于是便定义了多项式的加法. 容易看出，

$$\deg\big(f(x)+g(x)\big) \leqslant \max\big\{\deg f(x),\ \deg g(x)\big\}.$$

容易验证，多项式的加法满足以下公理. 设多项式 $f(x), g(x), h(x) \in \mathbb{F}[x]$，则

(A1) 加法结合律

$$\big(f(x)+g(x)\big)+h(x) = f(x)+\big(g(x)+h(x)\big);$$

(A2) 加法交换律

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

(A3) 存在零元素 即存在零多项式 $0 \in \mathbb{F}[x]$，使得

$$f(x)+0 = 0+f(x) = f(x);$$

(A4) 存在负元素 对每个多项式

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

都存在多项式

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

它称为多项式 $f(x)$ 的**负多项式**，使得

$$f(x)+\big(-f(x)\big) = \big(-f(x)\big)+f(x) = 0.$$

对于 $\mathbb{F}[x]$ 中两个多项式 $f(x)$ 和 $g(x)$，其**乘积** $f(x)g(x)$ 定义为

$$f(x)g(x) = c_{n+m}x^{n+m} + c_{n+m-1}x^{n+m-1} + \cdots + c_1 x + c_0,$$

其中

$$\begin{aligned}
c_{n+m} &= a_n b_m,\\
c_{n+m-1} &= a_n b_{m-1} + a_{n-1} b_m,\\
&\cdots\cdots\\
c_i &= \sum_{j+k=i} a_j b_k,\\
&\cdots\cdots\\
c_0 &= a_0 b_0.
\end{aligned}$$

于是规定了多项式的乘法. 因为 $a_n \neq 0, b_m \neq 0$，故 $a_n b_m \neq 0$. 所以，

$$\deg\big(f(x)g(x)\big) = \deg f(x) + \deg g(x).$$

容易验证，多项式的乘法适合以下的公理. 设 $f(x), g(x), h(x) \in \mathbb{F}[x]$，则

(M1) 乘法结合律

$$f(x)\big(g(x)h(x)\big) = \big(f(x)g(x)\big)h(x);$$

(M2) 乘法交换律

$$f(x)g(x) = g(x)f(x);$$

(M3) 存在单位元素 即存在纯量多项式 $e(x) = 1$，使得

$$f(x)e(x)=e(x)f(x)=f(x);$$

(D) 加乘分配律

$$f(x)\big(g(x)+h(x)\big)=f(x)g(x)+f(x)h(x).$$

于是根据定义，$\mathbb{F}[x]$ 是交换环，它称为数域 $\mathbb{F}$ 上的**一元多项式环**.

习　题　1.2

1. 设 $f(x),g(x)\in\mathbb{F}[x]$. 证明，当且仅当 $f(x)=0$，或 $g(x)=0$ 时，$f(x)g(x)=0$.

2. 设 $f(x),g(x),h(x)\in\mathbb{F}[x]$，且 $f(x)\neq 0$. 证明，若 $f(x)g(x)=f(x)h(x)$，则 $g(x)=h(x)$.

3. 设非零的实系数多项式 $f(x)$（即系数都是实数的多项式）满足 $f\big(f(x)\big)=f^k(x)$，其中 k 是给定的正整数. 求多项式 $f(x)$.

4. 设非零的实系数多项式 $f(x)$ 满足 $f(x^2)=f^2(x)$. 求多项式 $f(x)$.

5. 设实系数多项式 $f(x)=ax^2+bx+c,a\neq 0$. 证明，对任意给定的正整数 n，不存在 n 次实系数多项式 $g(x)$，使得 $f\big(g(x)\big)=g\big(f(x)\big)$.　　（本题似有误）

6. 设实系数多项式 $P(x)=a_0+a_1x+\cdots+a_nx^n$ 满足

$$0\leqslant a_0=a_n\leqslant a_1=a_{n-1}\leqslant\cdots\leqslant a_{[\frac{n}{2}]}=a_{[\frac{n+1}{2}]},$$

所有这样的多项式 $P(x)$ 的集合记作 $A(n)$. 证明，如果 $P(x)\in A(n),Q(x)\in A(m)$，则乘积

$$P(x)Q(x)\in A(n+m).$$

§1.3　整除性与最大公因式

数域 $\mathbb{F}$ 上的一元多项式环 $\mathbb{F}[x]$ 是我们遇到的第一个不是由数构成的交换环. 它的性质是否与数环，特别是与整数环 $\mathbb{Z}$ 相同？譬如，在整数环 $\mathbb{Z}$ 中，对于任意整数 $a,b\in\mathbb{Z},b\neq 0$，总存在唯一一对整数 q 和 $r,0\leqslant r<|b|$，使得 $a=qb+r$. 整数环 $\mathbb{Z}$ 的这一性质，多项式环 $\mathbb{F}[x]$ 是否也具有？对此，有

定理 1.3.1（带余除法） 设多项式 $f(x),g(x)\in\mathbb{F}[x],g(x)\neq 0$. 则存在唯一一对多项式 $q(x),r(x)\in\mathbb{F}[x],\deg r(x)<\deg g(x)$，使得

$$f(x)=q(x)g(x)+r(x).\tag{1.3.1}$$

证明　**存在性**　设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad a_n\neq 0,$$
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0,\quad b_m\neq 0.$$

显然，当 $n<m$ 时，取 $q(x)=0,r(x)=f(x)$，则式 (1.3.1) 成立. 当 $n\geqslant m$ 时，记

$$f(x)-\frac{a_n}{b_m}x^{n-m}g(x)=f_1(x),$$

显然，$\deg f_1(x)<\deg f(x)$.

于是对 $\deg f(x)=n$ 用归纳法，则存在多项式 $q_1(x),r(x)\in\mathbb{F}[x],\deg r(x)<$

$\deg g(x)$，使得

$$f(x)-\frac{a_n}{b_m}x^{n-m}g(x)=f_1(x)=q_1(x)g(x)+r(x).$$

因此，

$$f(x)=\Big(\frac{a_n}{b_m}x^{n-m}+q_1(x)\Big)g(x)+r(x).$$

这表明，如果记 $q(x)=a_nb_m^{-1}x^{n-m}+q_1(x)$，则式 (1.3.1) 成立.

唯一性 设 $q_1(x),r_1(x)\in\mathbb{F}[x]$，$\deg r_1(x)<\deg g(x)$，使得式 (1.3.1) 成立. 则

$$\big(q(x)-q_1(x)\big)g(x)=r_1(x)-r(x).$$

因此，如果 $q(x)\neq q_1(x)$，则由上式，

$$\deg g(x)<\deg\big(q(x)-q_1(x)\big)+\deg g(x)=\deg\big(r_1(x)-r(x)\big).$$

但因 $\deg r(x)<\deg g(x)$，$\deg r_1(x)<\deg g(x)$，因此，

$$\deg\big(r_1(x)-r(x)\big)<\deg g(x)$$

不可能. 所以，$q(x)=q_1(x)$，从而 $r(x)=r_1(x)$. ■

和整数环 $\mathbb{Z}$ 相仿，定理 1.3.1 中多项式 $q(x)$ 与 $r(x)$ 分别称为多项式 $f(x)$ 除以 $g(x)$ 的**商式**与**余式**.

应当指出，定理 1.3.1 关于商式 $q(x)$ 与余式 $r(x)$ 的存在性证明是构造性的. 换句话说，给定多项式 $f(x)$ 与 $g(x)$，$g(x)\neq 0$，可以按照定理 1.3.1 的证明方法求出商式 $g(x)$ 与余式 $r(x)$，其过程如下：

当 $\deg f(x)<\deg g(x)$ 时，$q(x)=0$，$r(x)=f(x)$.

当 $\deg f(x)\geqslant\deg g(x)$ 时，记

$$f(x)-\frac{a_n}{b_m}x^{n-m}g(x)=f_1(x).$$

如果 $\deg f_1(x)<\deg g(x)$，则

$$f(x)=\frac{a_n}{b_m}x^{n-m}g(x)+f_1(x),$$

此时 $q(x)=a_nb_m^{-1}x^{n-m}$，$r(x)=f_1(x)$.

如果 $\deg f_1(x)\geqslant\deg g(x)$，且 $f_1(x)$ 的首项系数为 $c_t\neq 0$，$t<\deg f(x)$，则记

$$f_1(x)-\frac{c_t}{b_m}x^{t-m}g(x)=f_2(x).$$

如果 $\deg f_2(x)<\deg g(x)$，则

$$f(x)=\Big(\frac{a_n}{b_m}x^{n-m}+\frac{c_t}{b_m}x^{t-m}\Big)g(x)+f_2(x),$$

此时 $q(x)=a_nb_m^{-1}x^{n-m}+c_tb_m^{-1}x^{t-m}$，$r(x)=f_2(x)$.

如果 $\deg f_2(x)\geqslant\deg g(x)$，则重复上述过程. 于是得到多项式序列 $f(x),f_1(x),\ldots,f_k(x),\ldots$，它们适合

$$\deg f(x)>\deg f_1(x)>\deg f_2(x)>\cdots>\deg f_k(x)>\cdots\geqslant\deg g(x).$$

由于 $\deg f(x)-\deg g(x)$ 是有限的，因此，经有限步后，必有 ℓ，使得

$$f_{\ell-1}(x)=\frac{d_s}{b_m}x^{s-m}g(x)+f_\ell(x),\qquad f_\ell(x)=\frac{e_h}{b_m}x^{h-m}g(x)+f_{\ell+1}(x),$$

其中 d_s 与 e_h 分别是多项式 $f_{\ell-1}(x)$ 与 $f_\ell(x)$ 的首项系数，$s>h\geqslant m$，并且

$$\deg f_{\ell+1}(x)<\deg g(x).$$

于是

$$f(x)=\left(\frac{a_n}{b_m}x^{n-m}+\frac{c_t}{b_m}x^{t-m}+\cdots+\frac{d_s}{b_m}x^{s-m}+\frac{e_h}{b_m}x^{h-m}\right)g(x)+f_{\ell+1}(x).$$

因此，

$$q(x)=\frac{a_n}{b_m}x^{n-m}+\frac{c_t}{b_m}x^{t-m}+\cdots+\frac{d_s}{b_m}x^{s-m}+\frac{e_h}{b_m}x^{h-m},$$
$$r(x)=f_{\ell+1}(x).$$

上述过程可写成表 1.3.1 的形式，这种算法称为 **Euclid 长除法**.

表 1.3.1　Euclid 长除法

$f(x)$		
$b_m^{-1}a_nx^{n-m}+b_m^{-1}c_tx^{t-m}+\cdots+b_m^{-1}d_sx^{s-m}+b_m^{-1}e_hx^{h-m}$	$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_{n-m}x^{n-m}+\cdots+a_1x+a_0$	$b_m^{-1}a_nx^{n-m}g(x)$
	$c_tx^t+c_{t-1}x^{t-1}+\cdots+c_{t-m}x^{t-m}+\cdots+c_0$	$f_1(x)$
	$\cdots\cdots\cdots\cdots\cdots\cdots$	$\cdots\cdots$
	$d_sx^s+\cdots+d_{s-m}x^{s-m}+\cdots+d_0$	$f_{\ell-1}(x)$
	$e_hx^h+\cdots+e_{h-m}x^{h-m}+\cdots+e_0$	$f_\ell(x)$
	$p_qx^q+\cdots+p_1x+p_0\ (q<m)$	$r(x)=f_{\ell+1}(x)$

表 1.3.2　Euclid 长除法（例 1.3.1）

$x^4+3x^3-x^2-4x-3$	$\frac{1}{3}x-\frac{1}{9}$
$3x^3+10x^2+2x-3$	
$-x^4-\frac{10}{3}x^3-\frac{2}{3}x^2$	
$-\frac{1}{3}x^3-\frac{5}{3}x^2-3x-3$	
$\frac{1}{3}x^3+\frac{10}{9}x^2+\frac{2}{9}x-\frac{1}{3}$	
$-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}$	

设多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{F}[x]$，$a\in\mathbb{F}$. 记

$$f(a)=a_na^n+a_{n-1}a^{n-1}+\cdots+a_1a+a_0.$$

$f(a)$ 称为**多项式 $f(x)$ 在 $x=a$ 处的值**. 若 $f(a)=0$，则 a 称为**多项式 $f(x)$ 的根**.

定理 1.3.1 的一个重要特例是：

推论 1.3.1（剩余定理） 设 $f(x)\in\mathbb{F}[x], a\in\mathbb{F}$，则存在唯一 $q(x)\in\mathbb{F}[x]$，使得

$$f(x)=(x-a)q(x)+f(a). \tag{1.3.2}$$

证明 由定理 1.3.1，存在唯一一对多项式 $q(x), r(x)\in\mathbb{F}[x]$，使得

$$f(x)=(x-a)q(x)+r(x),$$

其中 $\deg r(x)<1$. 将 $x=a$ 代入，得到 $f(a)=r(x)$. ■

例 1.3.1 设 $f(x)=x^4+3x^3-x^2-4x-3, g(x)=3x^3+10x^2+2x-3$，求 $f(x)$ 除以 $g(x)$ 的商式 $q(x)$ 和余式 $r(x)$.

解 如表 1.3.2 作 Euclid 长除法. 由此得到

$$q(x)=\frac{1}{3}x-\frac{1}{9},\qquad r(x)=-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}.$$ ■

定义 1.3.1 设非零多项式 $g(x)\in\mathbb{F}[x]$. 如果存在 $q(x)\in\mathbb{F}[x]$，使得多项式

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

则多项式 $g(x)$ 称为多项式 $f(x)$ 的一个**因式**，而多项式 $f(x)$ 称为多项式 $g(x)$ 的一个**倍式**. 这时说多项式 $g(x)$ **整除**多项式 $f(x)$，记为 $g(x)\mid f(x)$. 否则就说多项式 $g(x)$ **不能整除**多项式 $f(x)$，记作 $g(x)\nmid f(x)$.

关于多项式的整除性，有以下性质.

性质 1.3.1 如果 $g(x)\mid f(x), h(x)\mid g(x)$，则 $h(x)\mid f(x)$.

性质 1.3.2 如果 $g(x)\mid f_1(x), g(x)\mid f_2(x)$，则对任意 $h_1(x), h_2(x)\in\mathbb{F}[x]$，

$$g(x)\mid\big(h_1(x)f_1(x)+h_2(x)f_2(x)\big).$$

性质 1.3.3 如果 $g(x)\mid f(x), f(x)\mid g(x)$，则存在非零的数 $\lambda\in\mathbb{F}$，使得

$$f(x)=\lambda g(x).$$

上述性质请读者自证之.

推论 1.3.2（因式定理） 设 $f(x)\in\mathbb{F}[x], a\in\mathbb{F}$. 则当且仅当 $f(a)=0$ 时，

$$(x-a)\mid f(x).$$

定义 1.3.2 设多项式 $f_1(x), f_2(x), h(x)\in\mathbb{F}[x]$. 如果 $h(x)$ 是 $f_1(x)$ 与 $f_2(x)$ 的因式，则 $h(x)$ 称为 $f_1(x)$ 与 $f_2(x)$ 的一个**公因式**. 设 $f_1(x)$ 与 $f_2(x)$ 不全为零. 如果首一多项式 $d(x)$ 是 $f_1(x)$ 与 $f_2(x)$ 的公因式，而且 $f_1(x)$ 与 $f_2(x)$ 的每个公因式都是 $d(x)$ 的一个因式，则 $d(x)$ 称为 $f_1(x)$ 与 $f_2(x)$ 的**最大公因式**，记为

$$d(x)=\big(f_1(x), f_2(x)\big).$$

关于两个不全为零的多项式 $f_1(x)$ 与 $f_2(x)$ 的最大公因式，有

定理 1.3.2 任意两个不全为零的多项式 $f_1(x)$ 与 $f_2(x)$ 的最大公因式 $d(x)$ 存在而且唯一.

证明 **唯一性** 设 $d_1(x)$ 与 $d_2(x)$ 都是 $f_1(x)$ 与 $f_2(x)$ 的最大公因式. 由最大公因式的定义, $d_1(x)$ 是 $f_1(x)$ 与 $f_2(x)$ 的一个公因式, 而 $d_2(x)$ 是 $f_1(x)$ 与 $f_2(x)$ 的最大公因式, 因此, $d_1(x) \mid d_2(x)$.

反之, 同样有 $d_2(x) \mid d_1(x)$. 由性质 1.3.3, 存在非零的数 $\lambda \in \mathbb{F}$, 使 $d_1(x) = \lambda d_2(x)$. 由于 $d_1(x)$ 与 $d_2(x)$ 都是首一多项式, 比较上式两边的首项系数, 得到 $\lambda = 1$, 即 $d_1(x) = d_2(x)$.

存在性 不妨设 $f_2(x) \neq 0$. 由定理 1.3.1, 存在多项式 $q_1(x)$ 与 $r_1(x)$, 使得

$$f_1(x) = q_1(x) f_2(x) + r_1(x),$$

其中 $\deg r_1(x) < \deg f_2(x)$.

如果 $\deg r_1(x) = -\infty$ 为零多项式, 则停止. 如果 $r_1(x)$ 是非零多项式, 则由定理 1.3.1, 存在多项式 $q_2(x)$ 与 $r_2(x)$, 使得

$$f_2(x) = q_2(x) r_1(x) + r_2(x),$$

其中 $\deg r_2(x) < \deg r_1(x)$.

如果 $r_2(x)$ 是零多项式, 则停止. 如果 $r_2(x)$ 是非零多项式, 则重复上述过程. 于是得一连串的等式:

$$f_1(x) = q_1(x) f_2(x) + r_1(x), \tag{1}$$
$$f_2(x) = q_2(x) r_1(x) + r_2(x), \tag{2}$$
$$r_1(x) = q_3(x) r_2(x) + r_3(x), \tag{3}$$
$$\cdots\cdots\cdots\cdots$$
$$r_{k-2}(x) = q_k(x) r_{k-1}(x) + r_k(x), \tag{k}$$
$$\cdots\cdots\cdots\cdots$$

其中

$$\deg f_2(x) > \deg r_1(x) > \deg r_2(x) > \cdots > \deg r_k(x) > \cdots.$$

由于 $\deg f_2(x)$ 是一个给定的非负整数, 因此, 存在某个正整数 ℓ, 使得 $r_\ell(x) \neq 0$, 而 $r_{\ell+1}(x) = 0$, 即最后必有

$$r_{\ell-2}(x) = q_\ell(x) r_{\ell-1}(x) + r_\ell(x), \tag{ℓ}$$
$$r_{\ell-1}(x) = q_{\ell+1}(x) r_\ell(x). \tag{$\ell+1$}$$

$(\ell+1)$ 式表明, $r_\ell(x) \mid r_{\ell-1}(x)$.

因此, 由 (ℓ) 式, $r_\ell(x) \mid r_{\ell-2}(x)$; 再由 $(\ell-1)$ 式, $r_\ell(x) \mid r_{\ell-3}(x)$, 等等. 于是 $r_\ell(x)$ 整除

$$r_{\ell-1}(x),\ r_{\ell-2}(x),\ \ldots,\ r_2(x),\ r_1(x).$$

因此, 由 (2), $r_\ell(x) \mid f_2(x)$. 最后, 由 (1) 式 $r_\ell(x) \mid f_1(x)$. 所以 $r_\ell(x)$ 是 $f_1(x)$ 与 $f_2(x)$ 的一个公因式.

反之, 设 $h(x)$ 是 $f_1(x)$ 与 $f_2(x)$ 的一个公因式. 由 (1) 式, $h(x)$ 是 $r_1(x)$ 的因式. 再由 (2) 式, $h(x)$ 是 $r_2(x)$ 的因式, 等等. 于是 $h(x)$ 是 $r_{\ell-2}(x)$ 及 $r_{\ell-1}(x)$ 的因式. 由

(ℓ) 式，$h(x)$ 是 $r_\ell(x)$ 的一个因式.

因此，如果 $r_\ell(x)$ 的首项系数为 a，则由最大公因式的定义，$d(x)=a^{-1}r_\ell(x)$ 是 $f_1(x)$ 与 $f_2(x)$ 的最大公因式. ■

定理 1.3.2 关于多项式 $f_1(x)$ 与 $f_2(x)$ 的最大公因式的存在性证明给出了求最大公因式的一个方法，即所谓**辗转相除法**.

其过程如下：设 $f_1(x),f_2(x)\in\mathbb{F}[x]$，$\deg f_1(x)\geqslant\deg f_2(x)$. 先对 $f_1(x)$ 与 $f_2(x)$ 用 Euclid 长除法，得到商式 $q_1(x)$ 与余式 $r_1(x)$，$\deg r_1(x)<\deg f_2(x)$；在进行长除法时，将商式 $q_1(x)$ 记入表 1.3.3 的右边.

$f_2(x)$	$f_1(x)$	$q_1(x)$ $q_2(x)$
	$-)\ q_1(x)f_1(x)$	
	$r_1(x)$	

表 1.3.3

	$f_2(x)$	$f_1(x)$	$q_1(x)$
	$-)\ q_2(x)r_1(x)$	$-)\ q_1(x)f_2(x)$	
	$r_2(x)$	$r_1(x)$	

表 1.3.4

如果 $r_1(x)$ 是零多项式，则停止. 如果 $r_1(x)$ 是非零多项式，则对 $f_2(x)$ 和 $r_1(x)$ 用长除法，得到商式 $q_2(x)$ 与余式 $r_2(x)$，$\deg r_2(x)<\deg r_1(x)$，在进行长除法时，将商式 $q_2(x)$ 记入表 1.3.4 的左边.

$q_2(x)$	$f_2(x)$	$f_1(x)$	$q_1(x)$
	$-)\ q_2(x)r_1(x)$	$-)\ q_1(x)f_2(x)$	
$q_4(x)$	$r_2(x)$	$r_1(x)$	$q_3(x)$
	$-)\ q_4(x)r_3(x)$	$-)\ q_3(x)r_2(x)$	
$q_6(x)$	$r_4(x)$	$r_3(x)$	$q_5(x)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

表 1.3.5

如果 $r_2(x)$ 是零多项式，则停止. 如果 $r_2(x)$ 是非零多项式，则对 $r_1(x)$ 和 $r_2(x)$ 用长除法，得到商式 $q_3(x)$ 和余式 $r_3(x)$，并把商式 $q_3(x)$ 记入表 1.3.5 的右边.

如此继续，即可求得 $f_1(x)$ 与 $f_2(x)$ 的最大公因式.

例 1.3.2 求多项式 $f_1(x)=x^4+3x^3-x^2-4x-3$ 与 $f_2(x)=3x^3+10x^2+2x-3$ 的最大公因式.

解 如表 1.3.6 所示，对多项式 $f_1(x)$ 和 $f_2(x)$ 作辗转相除法.

因此，$r_2(x)=9x+27$，$r_3(x)=0$. 于是，$\big(f_1(x),f_2(x)\big)=x+3$. ■

定理 1.3.3 设不全为零的多项式 $f(x),g(x)\in\mathbb{F}[x]$，$d(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式. 则存在多项式 $u(x),v(x)\in\mathbb{F}[x]$，使得

$$f(x)u(x)+g(x)v(x)=d(x). \tag{1.3.3}$$

证明 记 $f(x)=f_1(x)$，$g(x)=f_2(x)$. 由定理 1.3.2 的证明，存在多项式 $q_1(x)$，$q_2(x),\dots,q_{k+1}(x)$ 和 $r_1(x),r_2(x),\dots,r_k(x)$，使得

	$3x^3+10x^2+2x-3=f_2(x)$	$x^4+3x^3-x^2-4x-3=f_1(x)$	$\frac{1}{3}x$
		$-)\quad x^4+\frac{10}{3}x^3+\frac{2}{3}x^2-x$	
$-\frac{27}{5}x$	$3x^3+10x^2+2x-3=f_2(x)$	$-\frac{1}{3}x^3-\frac{5}{3}x^2-3x-3$	$-\frac{1}{9}$
$-)$	$3x^3+15x^2+18x$	$-)\quad -\frac{1}{3}x^3-\frac{10}{9}x^2-\frac{2}{9}x+\frac{1}{3}$	
9	$-5x^2-16x-3$	$-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}=r_1(x)$	
$-)$	$-5x^2-25x-30$		
	$9x+27=r_2(x)$	$-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}=r_1(x)$	$-\frac{5}{81}x$
		$-)\quad -\frac{5}{9}x^2-\frac{5}{3}x$	
	$9x+27=r_2(x)$	$-\frac{10}{9}x-\frac{10}{3}$	$-\frac{10}{81}$
		$-)\quad -\frac{10}{9}x-\frac{10}{3}$	
		$0=r_3(x)$	

表 1.3.6　辗转相除法(例 1.3.2)

$$
\begin{aligned}
f_1(x) &= q_1(x)f_2(x)+r_1(x), && (1)\\
f_2(x) &= q_2(x)r_1(x)+r_2(x), && (2)\\
r_1(x) &= q_3(x)r_2(x)+r_3(x),\\
&\cdots\cdots\cdots\cdots\\
r_{k-3}(x) &= q_{k-1}(x)r_{k-2}(x)+r_{k-1}(x), && (k-1)\\
r_{k-2}(x) &= q_k(x)r_{k-1}(x)+r_k(x), && (k)\\
r_{k-1}(x) &= q_{k+1}(x)r_k(x), && (k+1)
\end{aligned}
$$

其中

$$\deg f_2(x)>\deg r_1(x)>\deg r_2(x)>\cdots>\deg r_k(x)\geqslant 0;$$

而且 $r_k(x)=\lambda d(x)$，λ 为 $r_k(x)$ 的首项系数. 由式 (k) 得到，

$$\lambda d(x)=r_{k-2}(x)-r_{k-1}(x)q_k(x).$$

设 $u_1(x)=1, v_1(x)=-q_k(x)$，上式为

$$\lambda d(x)=r_{k-2}u_1(x)+r_{k-1}(x)v_1(x).$$

把式 $(k-1)$ 代入上式，得到

$$\lambda d(x)=r_{k-3}(x)v_1(x)+r_{k-2}(x)\big(u_1(x)-q_{k-1}(x)v_1(x)\big).$$

记 $u_2(x)=v_1(x), v_2(x)=u_2(x)-q_{k-1}(x)v_1(x)$，上式即为

$$\lambda d(x)=r_{k-3}(x)u_2(x)+r_{k-2}(x)v_2(x).$$

逐个地把以上等式代入. 假设进行了 $k-2$ 次，得到

$$\lambda d(x)=f_2(x)u_{k-1}(x)+r_1(x)v_{k-1}(x).$$

最后把式 (1) 代入上式，得到

$$\lambda d(x) = f_1(x)v_{k-1}(x) + f_2(x)\big(u_{k-1}(x) - q_1(x)v_{k-1}(x)\big).$$

取 $u(x) = \lambda^{-1}v_{k-1}(x)$, $v(x) = \lambda^{-1}\big(u_{k-1}(x) - q_1(x)v_{k-1}(x)\big)$,

即得定理 1.3.3. ■

容易看出,对两个不全为零的多项式 $f(x)$ 与 $g(x)$,所有零次多项式都是它们的公因式. 如果 $f(x)$ 与 $g(x)$ 除零次多项式外不含其它的公因式,则 $f(x)$ 与 $g(x)$ 称为**互素**.

根据最大公因式的定义可以看出,两个多项式互素的充分必要条件是它们的最大公因式为 1. 因此,由定理 1.3.3 直接得到

推论 1.3.3 多项式 $f(x)$ 与 $g(x)$ 互素当且仅当存在 $u(x)$ 与 $v(x)$,使得

$$f(x)u(x) + g(x)v(x) = 1. \tag{1.3.4}$$

关于两个多项式的互素,有以下性质.

性质 1.3.4 设 $f(x), g(x), h(x)$ 是多项式,$\big(f(x), g(x)\big) = 1, \big(f(x), h(x)\big) = 1$,则

$$\big(f(x), g(x)h(x)\big) = 1.$$

证明 因为 $\big(f(x), g(x)\big) = 1$,故存在多项式 $u(x)$ 和 $v(x)$,使得

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

上式两端同乘以 $h(x)$,得到

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

由此可知,如果多项式 $w(x)$ 是 $f(x)$ 与 $g(x)h(x)$ 的公因式,则 $w(x)$ 也是 $f(x)$ 与 $h(x)$ 的公因式. 由于 $\big(f(x), h(x)\big) = 1$,因此 $w(x)$ 是零次多项式. 这表明 $f(x)$ 与 $g(x)h(x)$ 除零次多项式外不含其它公因式,即 $f(x)$ 与 $g(x)h(x)$ 互素. ■

性质 1.3.5 设 $f(x), g(x)$ 与 $h(x)$ 是多项式,其中 $\big(g(x), h(x)\big) = 1$,并且 $h(x) \mid f(x)g(x)$,则

$$h(x) \mid f(x).$$

证明 因为 $\big(g(x), h(x)\big) = 1$,故存在多项式 $u(x)$ 与 $v(x)$,使得

$$h(x)u(x) + g(x)v(x) = 1.$$

上式两端同乘以 $f(x)$,得到

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

由此可知,$h(x) \mid f(x)$. ■

性质 1.3.6 设 $f(x), g(x)$ 与 $h(x)$ 是多项式,$f(x) \mid h(x), g(x) \mid h(x)$,且

$$\big(f(x), g(x)\big) = 1,$$

则 $f(x)g(x) \mid h(x)$.

例 1.3.3 求多项式 $u(x)$ 和 $v(x)$，使得

$$x^m u(x) + (1-x)^n v(x) = 1. \tag{1.3.5}$$

解 显然，多项式 x^m 与 $(1-x)^n$ 互素. 所以由定理 1.3.3，适合式 (1.3.5) 的多项式 $u(x)$ 与 $v(x)$ 是存在的.

如果 $\deg u(x) \geqslant n, \deg v(x) \geqslant m$，则由定理 1.3.1，存在多项式 $q_1(x), u_1(x), q_2(x)$ 与 $v_1(x), \deg u_1(x) < n, \deg v_1(x) < m$，使得

$$u(x) = (1-x)^n q_1(x) + u_1(x), \quad v(x) = x^m q_2(x) + v_1(x).$$

代入式 (1.3.5) 得到

$$x^m (1-x)^n \big(q_1(x) + q_2(x)\big) = 1 - x^m u_1(x) - (1-x)^n v_1(x).$$

比较两端多项式的次数，得到

$$x^m u_1(x) + (1-x)^n v_1(x) = 1.$$

因此可设 $\deg u(x) < n, \deg v(x) < m$.

设

$$u(x) = \sum_{i=0}^{n-1} a_i (1-x)^i, \qquad v(x) = \sum_{j=0}^{m-1} b_j x^j.$$

显然，

$$a_i = \frac{(-1)^i}{i!} u^{(i)}(1), \qquad b_j = \frac{1}{j!} v^{(j)}(0).$$

将 $u(x)$ 与 $v(x)$ 代入式 (1.3.5). 令 $x = 0$，则得到 $b_0 = v(0) = 1$. 令 $x = 1$，则得到 $a_0 = u(1) = 1$. 对式 (1.3.5) 求 k 阶微商，得到

$$\sum_{i=0}^{k} \mathrm{C}_k^i \frac{m!}{(m-k+i)!} x^{m-k+i} u^{(i)}(x) + \sum_{i=0}^{k} (-1)^{k-i} \mathrm{C}_k^i \frac{n!}{(n-k+i)!} (1-x)^{n-k+i} v^{(i)}(x) = 0. \tag{1.3.6}$$

设 $1 \leqslant k \leqslant m-1$，则 $m-k+i \geqslant 1$，其中 $i = 0, 1, \ldots, k$. 在式 (1.3.6) 中令 $x = 0$，得到

$$\sum_{i=0}^{k} (-1)^{k-i} \mathrm{C}_k^i \frac{n!}{(n-k+i)!} v^{(i)}(0) = 0.$$

由此知

$$\sum_{i=0}^{k} (-1)^i \mathrm{C}_n^{k-i} b_i = 0.$$

进而解得 $b_j = \mathrm{C}_{n+j-1}^j$. 于是，

$$v(x) = \sum_{i=0}^{m-1} \mathrm{C}_{n+j-1}^j x^j.$$

同样，设 $1 \leqslant k \leqslant n-1$，则 $n-k+i \geqslant 1$，其中 $i = 0, 1, \ldots, k$. 在式 (1.3.6) 中令 $x = 1$，得到

$$\sum_{i=0}^{k} \mathrm{C}_k^i \frac{m!}{(m-k+i)!} u^{(i)}(1) = 0.$$

由此知

$$\sum_{i=0}^{k}(-1)^i C_m^{k-i} a_i = 0.$$

解得 $a_i = C_{m+i-1}^{i}$. 因此,

$$u(x) = \sum_{i=0}^{n-1} C_{m+i-1}^{i}(1-x)^i. \qquad \blacksquare$$

注 对于给定多项式 $f(x)$ 与 $g(x)$,求多项式 $u(x)$ 与 $v(x)$,使得

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

这里 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式,其方法很多的.

方法之一是,用辗转相除法,求出定理 1.3.3 的证明中的等式 (1),(2),...,(k);然后,如同定理 1.3.3 的证明,把这里些等式逐个地由后往前代入,即可求出 $u(x)$ 与 $v(x)$.

方法之二是,由于定理 1.3.3 保证了 $u(x)$ 与 $v(x)$ 的存在性,因此可以用**待定系数法**. 例 1.3.3 采用的就是待定系数法.

最大公因式的概念可以推广到有限多个不全为零的多项式的情形.

定义 1.3.3 设不全为零的多项式 $f_1(x), f_2(x), \ldots, f_s(x) \in \mathbb{F}[x]$, $h(x) \in \mathbb{F}[x]$. 如果对任意 $i = 1, 2, \ldots, s$,都有

$$h(x) \mid f_i(x),$$

则 $h(x)$ 称为 $f_1(x), f_2(x), \ldots, f_s(x)$ 的**公因式**. 如果首一多项式 $d(x) \in \mathbb{F}[x]$ 是 $f_1(x)$, $f_2(x), \ldots, f_s(x)$ 的公因式,而 $f_1(x), f_2(x), \ldots, f_s(x)$ 的每个公因式都是 $d(x)$ 的因式,则 $d(x)$ 称为 $f_1(x), f_2(x), \ldots, f_s(x)$ 的**最大公因式**,记为

$$d(x) = \big(f_1(x), f_2(x), \ldots, f_s(x)\big).$$

定理 1.3.4 不全为零的多项式 $f_1(x), f_2(x), \ldots, f_s(x)$ 的最大公因式存在且唯一,而且

$$d(x) = \big(f_1(x), f_2(x), \ldots, f_s(x)\big) = \big(\big(f_1(x), f_2(x), \ldots, f_{s-1}(x)\big), f_s(x)\big). \tag{1.3.7}$$

证明 先证明最大公因式的存在性与式 (1.3.7) 成立. 对多项式的个数 s 用归纳法. 当 $s = 2$ 时,显然最大公因式存在且式 (1.3.7) 成立.

假设当 $s = k-1$ 时最大公因式存在且式 (1.3.7) 成立. 记 $k-1$ 个不全为零的多项式 $f_1(x), f_2(x), \ldots, f_{k-1}(x)$ 的最大公因式为 $\widetilde{d}(x)$. 由定理 1.3.2,多项式 $\widetilde{d}(x)$ 与 $f_k(x)$ 的最大公因式存在,记为 $d(x)$.

显然,$d(x)$ 是 $\widetilde{d}(x)$ 与 $f_k(x)$ 的公因式. 由于 $\widetilde{d}(x)$ 是 $f_1(x), f_2(x), \ldots, f_{k-1}(x)$ 的公因式,因此,$d(x)$ 是 $f_1(x), f_2(x), \ldots, f_k(x)$ 的公因式.

另一方面,设 $h(x)$ 是 $f_1(x), f_2(x), \ldots, f_k(x)$ 的公因式,则 $h(x)$ 是 $f_1(x), f_2(x)$, $\ldots, f_{k-1}(x)$ 的公因式,从而 $h(x)$ 是 $\widetilde{d}(x)$ 的因式. 即 $h(x)$ 是 $\widetilde{d}(x)$ 和 $f_k(x)$ 的公因式. 因此,$h(x)$ 也是 $d(x)$ 的因式.

这表明,$d(x)$ 是 $f_1(x), f_2(x), \ldots, f_k(x)$ 的最大公因式. 即

$$d(x)=\big(\widetilde{d}(x),f_k(x)\big).$$

这就证明了 $f_1(x),f_2(x),\dots,f_k(x)$ 的最大公因式存在而且式 (1.3.7) 成立.

至于唯一性的证明和 $s=2$ 的情形是类似的. 从略. ■

由式 (1.3.7) 与定理 1.3.3 直接得到,

推论 1.3.4 设 $d(x)$ 是多项式 $f_1(x),f_2(x),\dots,f_s(x)\in\mathbb{F}[x]$ 的最大公因式,则存在多项式 $u_1(x),u_2(x),\dots,u_s(x)\in\mathbb{F}[x]$,使得

$$f_1(x)u_1(x)+f_2(x)u_2(x)+\cdots+f_s(x)u_s(x)=0. \tag{1.3.8}$$

如果多项式 $f_1(x),f_2(x),\dots,f_s(x)$ 的公因式只能是零次多项式,则称 $f_1(x),f_2(x),\dots,f_s(x)$ 是互素的.

容易看出,多项式 $f_1(x),f_2(x),\dots,f_s(x)$ 互素的充分必要条件是它们的最大公因式为 1. 注意,当 $s>2$ 时,如果 $f_1(x),f_2(x),\dots,f_s(x)$ 互素,这些多项式并不一定两两互素.

习 题 1.3

1. 设多项式 $g(x)=x^2-2ax+2$ 整除多项式 $f(x)=x^4+3x^2+ax+b$,求 a 和 b. 这里 $a,b\in\mathbb{R}$.

2. 设 m,n 和 p 为正整数. 证明,多项式 $g(x)=x^2+x+1$ 整除多项式 $f(x)=x^{3m}+x^{3n+1}+x^{3p+2}$.

3. 证明,当 $n=6m+5$ 时,多项式 x^2+xy+y^2 整除多项式 $(x+y)^n-x^n-y^n$;当 $n=6m+1$ 时,多项式 $(x^2+xy+y^2)^2$ 整除多项式 $(x+y)^n-x^n-y^n$. 这里 m 是使 $n>0$ 的整数,而 x 与 y 是实数.

4. 求多项式 $f(x)$ 与 $g(x)$ 的最大公因式.

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

(2) $f(x)=x^6+2x^4-4x^3-3x^2+8x-5$, $g(x)=x^5+x^2-x+1$;

(3) $f(x)=3x^6-x^5-9x^4-14x^3-11x^2-3x-1$, $g(x)=3x^5+8x^4+9x^3+15x^2+10x+9$.

5. 确定多项式 $u(x)$ 与 $v(x)$,使得 $f(x)u(x)+g(x)v(x)=d(x)$,其中 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式.

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

(2) $f(x)=3x^5+5x^4-16x^3-6x^2-5x-6$, $g(x)=3x^4-4x^3-x^2-x-2$;

(3) $f(x)=3x^3-2x^2+x+2$, $g(x)=x^2-x+1$;

(4) $f(x)=x^4-x^3-4x^2+4x+1$, $g(x)=x^2-x-1$.

6. 用待定系数法确定多项式 $u(x)$ 与 $v(x)$,使得 $f(x)u(x)+g(x)v(x)=1$,其中 $f(x)$ 与 $g(x)$ 如下:

(1) $f(x)=x^3$, $g(x)=(1-x)^2$; (2) $f(x)=x^4$, $g(x)=(1-x)^4$;

(3) $f(x)=x^4-4x^3+1$, $g(x)=x^3-3x^2+1$.

7. 求次数最低的多项式 $u(x)$ 与 $v(x)$,使得

(1) $(x^4-2x^3-4x^2+6x+1)u(x)+(x^3-5x-3)v(x)=x^4$;

(2) $(x^4+2x^3+x+1)u(x)+(x^4+x^3-2x^2+2x-1)v(x)=x^3-2x$.

8. 求次数最低的多项式 $f(x)$,使得 $f(x)$ 被多项式 $(x-1)^2$ 除时余式为 $2x$,被多项式 $(x-2)^3$ 除时余式为 $3x$.

9. 求次数最低的多项式 $f(x)$，使得 $f(x)$ 被多项式 $x^4-2x^3-2x^2+10x-7$ 除时余式为 x^2+x+1，被多项式 $x^4-2x^3-3x^2+13x-10$ 除时余式为 $2x^2-3$.

10. 设 $f(x)$ 是 $2n+1$ 次多项式，n 为正整数，$f(x)+1$ 被 $(x-1)^n$ 整除，而 $f(x)-1$ 被 $(x+1)^n$ 整除. 求 $f(x)$.

§1.4 唯一析因定理

大家知道，在整数环 $\mathbb{Z}$ 中素数起着重要的作用. 所谓素数是指，除 ±1 和自身外不含其它因子的整数. 整数环 $\mathbb{Z}$ 中每个非零整数都可以分解为若干个素数的乘积，而且不计素因子的正负号和顺序，这种分解是唯一的.

对数域 $\mathbb{F}$ 上的一元多项式环 $\mathbb{F}[x]$，也有类似的结论. 为了介绍多项式环的唯一析因定理，先引述以下的定义.

定义 1.4.1 设 $f(x)$ 是数域 $\mathbb{F}$ 上的 n 次多项式，$n\geqslant 1$. 如果存在次数小于 n 的多项式 $g(x),h(x)\in\mathbb{F}[x]$，使得 $f(x)=g(x)h(x)$，则多项式 $f(x)$ 称为**在 $\mathbb{F}$ 上可约**. 如果多项式 $f(x)$ 不是在 $\mathbb{F}$ 上可约，则 $f(x)$ 称为**在 $\mathbb{F}$ 上不可约**.

应当注意，一个多项式在数域 $\mathbb{F}$ 上不可约，在包含数域 $\mathbb{F}$ 的数域 $\mathbb{K}$ 上这个多项式有可能是可约的. 例如，多项式 x^2+1 在实数域 $\mathbb{R}$ 上不可约，但是，由于

$$x^2+1=(x-\mathrm{i})(x+\mathrm{i}),$$

这里 $\mathrm{i}^2=-1$. 因此多项式 x^2+1 在复数域上是可约的. 所以，多项式的不可约性是相对给定的数域而言的.

关于不可约多项式，有以下简单性质.

性质 1.4.1 设多项式 $p(x)$ 在 $\mathbb{F}$ 上不可约，且 a 是 $\mathbb{F}$ 中非零的数，则多项式 $ap(x)$ 在 $\mathbb{F}$ 上不可约.

性质 1.4.2 设多项式 $f(x)\in\mathbb{F}[x]$，且 $p(x)$ 是 F 上的不可约多项式，则 $p(x)\,|\,f(x)$，或者 $p(x)$ 与 $f(x)$ 互素.

证明 设 $f(x)$ 与 $p(x)$ 不互素，则它们的最大公因式 $d(x)\neq 1$，即 $d(x)$ 是 $p(x)$ 的因式. 因为 $p(x)$ 在 $\mathbb{F}$ 上不可约，所以 $p(x)=ad(x),a\in\mathbb{F}$. 而 $d(x)$ 是 $f(x)$ 的因式，故 $p(x)$ 也是 $f(x)$ 的因式，即 $p(x)\,|\,f(x)$. ■

性质 1.4.3 设多项式 $f(x),g(x)\in\mathbb{F}[x]$，$p(x)$ 是数域 $\mathbb{F}$ 上的不可约多项式. 如果 $p(x)\,|\,f(x)g(x)$，则 $p(x)\,|\,f(x)$，或者 $p(x)\,|\,g(x)$.

证明 如果 $p(x)\nmid f(x)$，则 $\big(p(x),f(x)\big)=1$. 因此，存在多项式 $u(x),v(x)\in\mathbb{F}[x]$，使得

$$p(x)u(x)+f(x)v(x)=1.$$

因此，

$$p(x)\big(u(x)g(x)\big)+\big(f(x)g(x)\big)v(x)=g(x).$$

由此即知，$p(x)\mid g(x)$. ■

下面是本节的主要定理.

定理 1.4.1（唯一析因定理） 设 n 次多项式 $f(x)\in\mathbb{F}[x]$，则存在数域 $\mathbb{F}$ 上的不可约多项式 $p_1(x),p_2(x),\dots,p_s(x)\in\mathbb{F}[x]$，使得

$$f(x)=p_1(x)p_2(x)\cdots p_s(x).$$

如果另有不可约多项式 $q_1(x),q_2(x),\dots,q_t(x)\in\mathbb{F}[x]$，使得

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

则 $s=t$，并且可以适当调动因式的次序，使得

$$q_i(x)=a_ip_i(x),$$

其中 $a_i\in\mathbb{F}$，$i=1,2,\dots,s$.

如果不可约多项式 $p(x)$ 整除多项式 $f(x)$，则 $p(x)$ 称为 $f(x)$ 的**不可约因式**. 把多项式 $f(x)$ 分解为若干个不可约因式的乘积，称为**对 $f(x)$ 施行不可约分解**. 于是，定理 1.4.1 可以简单叙述为：

每个多项式都可以分解为不可约因式的乘积，而且如果不计不可约因式的次序和零次因式，这种不可约分解是唯一的.

证明 **存在性** 对多项式的次数 n 用归纳法.

显然，一次多项式在数域 $\mathbb{F}$ 上都是不可约的，因此结论对 $n=1$ 成立. 假设结论对次数小于 n 的多项式都成立，下面证明结论对 n 次多项式 $f(x)$ 成立.

如果 $f(x)$ 本身在 $\mathbb{F}$ 上不可约，则 $f(x)$ 的不可约分解由自身组成；如果 $f(x)$ 在 $\mathbb{F}$ 上可约，则存在次数小于 n 的多项式 $g(x),h(x)\in\mathbb{F}[x]$，使得

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

由于 $g(x)$ 和 $h(x)$ 的次数都小于 n，故由归纳假设，存在不可约多项式 $p_1(x),p_2(x),\dots,p_k(x)$ 和 $p_{k+1}(x),\dots,p_s(x)\in\mathbb{F}[x]$，使得

$$g(x)=p_1(x)p_2(x)\cdots p_k(x),\qquad h(x)=p_{k+1}(x)p_{k+2}(x)\cdots p_s(x).$$

于是，

$$f(x)=p_1(x)p_2(x)\cdots p_k(x)p_{k+1}(x)\cdots p_s(x).$$

唯一性 现在设多项式 $f(x)$ 具有两个不可约分解，即设

$$f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_t(x). \tag{1.4.1}$$

因为 $q_1(x)$ 在 $\mathbb{F}$ 上不可约，并且 $q_1(x)\mid p_1(x)p_2(x)\cdots p_s(x)$，因此，由性质 1.4.3，存在某 $1\leqslant i\leqslant s$ 使得 $q_1(x)\mid p_i(x)$. 适当地调整不可约因式 $p_1(x),p_2(x),\dots,p_s(x)$ 的次序，可设 $q_1(x)\mid p_1(x)$. 由于 $p_1(x)$ 在 $\mathbb{F}$ 上不可约，因此，存在 $a_1\in\mathbb{F}$ 使得 $p_1(x)=a_1q_1(x)$. 于是由式 (1.4.1) 得到：

$$\big(a_1p_2(x)\big)p_3(x)\cdots p_s(x)=q_2(x)q_3(x)\cdots q_t(x)=g(x). \tag{1.4.2}$$

由性质 1.4.1，$a_1p_2(x)$ 在 $\mathbb{F}$ 上不可约. 因此式 (1.4.2) 是次数小于 n 的多项式 $g(x)$ 的两个不可约分解，根据归纳假设得到，$s-1=t-1$，即 $s=t$. 并且可适当调整不可约因式 $a_1p_2(x),p_3(x),\dots,p_s(x)$ 的次序，使得

$$q_2(x)=a_2'a_1p_2(x),q_3(x)=a_3p_3(x),\dots,q_s(x)=a_sp_s(x),$$

其中 $a_2',a_3,\dots,a_s\in\mathbb{F}$. 记 $a_2'a_1=a_2$，则得到 $q_i(x)=a_ip_i(x),i=1,2,\dots,s.$ ■

应当指出，如果要求数域 $\mathbb{F}$ 上的不可约多项式是首一的，则由定理 1.4.1 直接得到，存在首一不可约多项式 $p_1(x),p_2(x),\dots,p_s(x)\in\mathbb{F}[x]$，使得多项式 $f(x)$ 可以表为

$$f(x)=a_0p_1(x)p_2(x)\cdots p_s(x),$$

其中 a_0 为 $f(x)$ 的首项系数. 对于多项式 $f(x)$ 的这种不可约分解，除了不可约因式的次序外是唯一的.

一般地说，出现在多项式 $f(x)$ 的一个不可约分解中的不可约因式不一定都不相同. 如果不可约因式 $p(x)$ 不只出现一次，则 $p(x)$ 称为 $f(x)$ 的**重因式**，否则称为**单因式**. 如果 $p(x)$ 恰好出现 k 次，则 $p(x)$ 称为 $f(x)$ 的 $\boldsymbol{k}$ **重因式**.

设多项式 $f(x)$ 具有不可约分解

$$f(x)=a_0p_1(x)p_2(x)\cdots p_s(x), \tag{1.4.3}$$

其中 $p_1(x),p_2(x),\dots,p_s(x)$ 是不可约的首一多项式，a_0 是 $f(x)$ 的首项系数. 又设分解式 (1.4.3) 中所有不同的不可约因式为 $p_1(x),p_2(x),\dots,p_\ell(x)$，它们分别是 $f(x)$ 的 $k_1,k_2,\dots,k_\ell$ 重因式，则式 (1.4.3) 可以写成

$$f(x)=a_0p_1^{k_1}(x)p_2^{k_2}(x)\cdots p_\ell^{k_\ell}(x). \tag{1.4.4}$$

设多项式 $f(x)$ 和 $g(x)$ 的所有不同的首一不可约因式分别为 $h_1(x),h_2(x),\dots,h_s(x)$ 和 $q_1(x),q_2(x),\dots,q_s(x)$. 它们的并集记为 $\{p_1(x),p_2(x),\dots,p_\ell(x)\}$. 则 $f(x)$ 与 $g(x)$ 的不可约分解可以表为

$$f(x)=a_0p_1^{k_1}(x)p_2^{k_2}(x)\cdots p_\ell^{k_\ell}(x),$$
$$g(x)=b_0p_1^{e_1}(x)p_2^{e_2}(x)\cdots p_\ell^{e_\ell}(x),$$

其中 a_0 与 b_0 分别是 $f(x)$ 和 $g(x)$ 的首项系数，而 k_i 与 e_i 是非负整数，$i=1,2,\dots,\ell$. 于是，$f(x)$ 与 $g(x)$ 的最大公因式为

$$\big(f(x),g(x)\big)=p_1^{m_1}(x)p_2^{m_2}(x)\cdots p_\ell^{m_\ell}(x),$$

其中 $m_i=\min\{k_i,e_i\},i=1,2,\dots,\ell.$

§1.5 实系数与复系数多项式

系数都是实数或者都是复数的多项式分别称为**实系数**或**复系数多项式**. 这节讨论实系数多项式与复系数多项式的唯一析因理论. 先证明以下的定理.

定理 1.5.1 数域 $\mathbb{F}$ 上的 n 次多项式 $f(x)$ 在 $\mathbb{F}$ 上至多有 n 个不同的根, $n \geqslant 1$.

证明 设 $a_1, a_2, \ldots, a_r$ 是 $f(x)$ 的不同的根, $a_1, a_2, \ldots, a_r \in \mathbb{F}$. 下面对 r 用归纳法证明

$$(x-a_1)(x-a_2)\cdots(x-a_r) \mid f(x).$$

事实上, 当 $r=1$ 时. 因为 a_1 是 $f(x)$ 的根, 故由因式定理, $(x-a_1) \mid f(x)$.

假设结论对 $r-1$ 成立, 现在证明结论对 r 成立. 因为 $a_1, a_2, \ldots, a_{r-1}$ 是 $f(x)$ 的根, 故由归纳假设, $(x-a_1)(x-a_2)\cdots(x-a_{r-1}) \mid f(x)$,

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_{r-1})h(x).$$

其中 $h(x) \in \mathbb{F}[x]$. 由于 a_r 为 $f(x)$ 的根, 故

$$f(a_r) = (a_r-a_1)(a_r-a_2)\cdots(a_r-a_{r-1})h(a_r) = 0.$$

因为 $a_1, a_2, \ldots, a_r$ 是 $f(x)$ 的不同的根, 因此 $a_r - a_i \neq 0, i = 1, 2, \ldots, r-1$. 所以 $h(a_r) = 0$. 由因式定理, $h(x) = (x-a_r)g(x)$, 于是,

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_{r-1})(x-a_r)g(x). \qquad \blacksquare$$

定理 1.5.1 并没有告诉我们, n 次多项式 $f(x) \in \mathbb{F}[x]$ 一定在数域 $\mathbb{F}$ 上有根. 例如, 多项式 x^2+1 在实数域 $\mathbb{R}$ 上就没有根. 但是, 当数域 $\mathbb{F}$ 为复数域 $\mathbb{C}$ 时, 有

定理 1.5.2(代数基本定理) 任意一个 n 次复系数多项式一定有复数根, $n \geqslant 1$.

这个定理是人们早就知道的. 直到 1797 年, 二十岁的德国大数学家 Gauss 才第一个给出证明. 后来 Gauss 又给出三个证明. 由于十九世纪以前的代数是以研究代数方程为中心的, 而这个定理对代数方程论又具有基本重要性, 所以人们称它为代数基本定理. 这个定理的证明有的涉及复变函数论知识, 而初等证明的篇幅又嫌太长, 这里就不给出了.

利用代数基本定理容易证明,

定理 1.5.3 设 $f(x)$ 是任意一个 n 次复系数多项式, $n > 0$, 则 $f(x)$ 恰有 n 个复数根 $c_1, c_2, \ldots, c_n$, 而且

$$f(x) = a_0(x-c_1)(x-c_2)\cdots(x-c_n), \tag{1.5.1}$$

其中 a_0 是 $f(x)$ 的首项系数.

证明 对多项式 $f(x)$ 的次数 n 用归纳法. 当 $n=1$ 时定理显然成立.

假设定理对次数为 $n-1$ 的多项式成立, $f(x)$ 是 n 次复系数多项式. 由代数基

本定理，$f(x)$ 具有复数根 c_1，由因式定理，$f(x)=(x-c_1)g(x)$，其中 $g(x)$ 为 $n-1$ 次复系数多项式.

由归纳假设，$g(x)$ 恰有 $n-1$ 个复数根 $c_2,c_3,\dots,c_n$，并且

$$g(x)=a_0(x-c_2)(x-c_3)\cdots(x-c_n).$$

于是，$f(x)=a_0(x-c_1)(x-c_2)\cdots(x-c_n)$. 显然，$c_1,c_2,\dots,c_n$ 是 $f(x)$ 的 n 个复数根，而且 a_0 是 $f(x)$ 的首项系数. ■

应当说明，n 次多项式 $f(x)$ 的 n 个根 $c_1,c_2,\dots,c_n$ 不一定都不相同. 如果 $f(x)$ 的根 c 在 $c_1,c_2,\dots,c_n$ 中出现 k 次，则 c 称为 $f(x)$ 的 ***k* 重根**. 1 重根称为**单根**.

设 n 次多项式 $f(x)$ 的所有不同的根为 $c_1,c_2,\dots,c_s$，它们的重数分别为 $k_1,k_2,\dots,k_s$，则 $f(x)$ 的分解式 (1.5.1) 可以写为

$$f(x)=a_0(x-c_1)^{k_1}(x-c_2)^{k_2}\cdots(x-c_s)^{k_s},$$

其中正整数 $k_1,k_2,\dots,k_s$ 适合 $k_1+k_2+\cdots+k_s=n$.

我们知道，复系数一次多项式一定是不可约的. 定理 1.5.2 表明，任何 n 次复系数多项式 $f(x)$ 在复数域上都是可约的，其中 $n\geqslant 2$. 因此，复系数多项式 $p(x)$ 在复数域 $\mathbb{C}$ 上不可约的充分必要条件是 $\deg p(x)=1$. 利用这一事实和 §1.4 证明的唯一析因定理，也可以直接得到定理 1.5.3. 所以，定理 1.5.3 是复系数多项式的唯一析因定理.

下面讨论实系数多项式的不可约分解.

定理 1.5.4 实系数多项式 $f(x)$ 的复数根共轭成对出现.

证明 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，其中 $a_0,a_1,\dots,a_n\in\mathbb{R}$，且设 c 是 $f(x)$ 的复数根，则

$$f(c)=a_nc^n+a_{n-1}c^{n-1}+\cdots+a_1c+a_0=0.$$

上式两端取共轭，并注意 a_i 是实数，$i=1,2,\dots,n$，则得到，

$$a_n\bar{c}^n+a_{n-1}\bar{c}^{n-1}+\cdots+a_1\bar{c}+a_0=0.$$

其中 $\bar{c}$ 是 c 的共轭复数，即 $f(\bar{c})=0$. 因此，$\bar{c}$ 也是 $f(x)$ 的根. ■

对复系数多项式，定理 1.5.4 并不成立. 例如，复系数多项式 $x^2-\mathrm{i}x=x(x-\mathrm{i})$ 的根为 0 和 i，它们并不共轭.

由定理 1.5.4 可以知道，奇次实系数多项式一定有实数根.

定理 1.5.5 实系数多项式 $p(x)$ 在实数域上不可约，则 $p(x)$ 的次数为 1 或 2.

证明 反证法. 设 $\deg p(x)=n\geqslant 3$. 根据定理 1.5.2，作为复系数多项式，$p(x)$ 具有复数根. 如果 $p(x)$ 具有实数根 a，则由因式定理，

$$p(x)=(x-a)f(x),$$

其中 $f(x)$ 是实系数多项式. 这表明，$p(x)$ 在实数域上可约，与假设矛盾.

如果 $p(x)$ 的根都是复数(不能是实数),则由定理 1.5.4,n 为偶数. 设 $n=2k$, $k\geqslant 2$,且设 $c_1,\overline{c}_1,c_2,\overline{c}_2,\dots,c_k,\overline{c}_k$ 是 $p(x)$ 的根. 因此,

$$p(x)=a_0(x-c_1)(x-\overline{c}_1)\cdots(x-c_k)(x-\overline{c}_k).$$

记

$$p_i(x)=(x-c_i)(x-\overline{c}_i)=x^2-(c_i+\overline{c}_i)x+c_i\overline{c}_i,$$

其中 $i=1,2,\dots,k$. 显然,$p_i(x)$ 是实系数的. 因此,$p(x)$ 在实数域上可约,与假设矛盾. 这就证明,$1\leqslant \deg(x)\leqslant 2$. ■

利用二次方程的判别式,容易知道,实二次多项式 x^2+px+q 在实数域上不可约的充分必要条件是,它的判别式 $p^2-4q<0$.

定理 1.5.6　n 次实系数多项式 $f(x)$ 可分解为一次因式和二次不可约因式的乘积,即

$$\begin{aligned}f(x)=a_0(x-c_1)^{k_1}(x-c_2)^{k_2}\cdots(x-c_s)^{k_s}\\ \times(x^2+p_1x+q_1)^{e_1}(x^2+p_2x+q_2)^{e_2}\cdots(x2+p_tx+q_t)^{e_t},\end{aligned}\tag{1.5.2}$$

其中 k_i 和 e_j 是正整数,$1\leqslant i\leqslant s$,$1\leqslant j\leqslant t$,且

$$k_1+k_2+\cdots+k_s+2(e_1+e_2+\cdots+e_t)=n,$$

而 a_0 是 $f(x)$ 的首项系数,$c_1,c_2,\dots,c_s,p_1,p_2,\dots,p_t$ 和 $q_1,q_2,\dots,q_t$ 都是实数,并且

$$p_j^2-4q_j<0.$$

当然,如果 $f(x)$ 没有实根,则式 (1.5.2) 中的一次因式不出现; 如果 $f(x)$ 的根都是实数,则二次因式不出现.

证明　这是 §1.4 中唯一析因定理和定理 1.5.5 的直接推论. ■

习　题　1.5

1. 把下列复系数多项式分解为一次因式的乘积.

(1) $(x+\cos\theta+\mathrm{i}\sin\theta)^n+(x+\cos\theta-\mathrm{i}\sin\theta)^n$;

(2) $(x+1)^n-(x-1)^n$;

(3) $x^n-\mathrm{C}_{2n}^2x^{n-1}+\mathrm{C}_{2n}^4x^{n+2}+\cdots+(-1)^n\mathrm{C}_{2n}^{2n}$;

(4) $x^{2n}+\mathrm{C}_{2n}^2x^{2n-2}(x^2-1)+\mathrm{C}_{2n}^4x^{2n-4}(x^2-1)^2+\cdots+(x^2-1)^n$;

(5) $x^{2n+1}+\mathrm{C}_{2n+1}^2x^{2n-1}(x^2-1)+\mathrm{C}_{2n+1}^4x^{2n-3}(x^2-1)^2+\cdots+x(x^2-1)^n$.

2. 把下列实系数多项式分解为实的不可约因式的乘积.

(1) x^4+1;

(2) x^6+27;

(3) $x^4+4x^3+4x^2+1$;

(4) $x^{2n}-2x^n+2$;

(5) $x^4-ax^2+1,-2<a<2$;

(6) $x^{2n}+x^n+1$.

3. 证明,复系数多项式 $f(x)$ 对所有实数 x 恒取正值的充分必要条件是,存在没有实数根的复系数多项式 $\varphi(x)$,使得 $f(x)=|\varphi(x)|^2$.

4. 证明,实系数多项式 $f(x)$ 对所有实数 x 恒取非负实数值的充分必要条件是,存在实系数多项式 $\varphi(x)$ 和 $\psi(x)$,使得 $f(x)=\varphi^2(x)+\psi^2(x)$.

§1.6 整系数与有理系数多项式

系数都是整数或者都是有理数的多项式称为**整系数多项式**或**有理系数多项式**. 根据定理 1.4.1,有理系数多项式可以分解为有理系数不可约多项式的乘积,而且不计不可约因式的次序与零次因式,不可约分解是唯一的. 问题是,如何判定一个有理系数多项式是否在有理数域 $\mathbb{Q}$ 上不可约? 另外,定理 1.4.1 (即多项式的唯一析因定理)是对数域 $\mathbb{F}$ 而言的,对整数环 $\mathbb{Z}$,唯一析因定理是否仍成立,这是本节所要讨论的.

和数域 $\mathbb{F}$ 上不可约多项式的定义相仿,可以给出不可约整系数多项式的定义.

设 n 是正整数,如果 n 次整系数多项式 $f(x)$ 可以表为两个次数小于 n 的整系数多项式的乘积,则 $f(x)$ 称为在整数环 $\mathbb{Z}$ 上**不可约**. 否则,$f(x)$ 称为在整数环 $\mathbb{Z}$ 上**可约**. 容易看出,如果整系数多项式 $f(x)$ 在 $\mathbb{Z}$ 上可约,则作为有理系数多项式,$f(x)$ 在有理数域 $\mathbb{Q}$ 上也可约. 反之,如果整系数多项式 $f(x)$ 在 $\mathbb{Q}$ 上可约,$f(x)$ 是否在 $\mathbb{Z}$ 上也可约?

为了回答这个问题,先引进以下的概念.

定义 1.6.1 如果整系数多项式 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 的系数 $a_0,a_1,\ldots,a_n$ 的最大公因子为 1,则 $f(x)$ 称为**本原多项式**.

设整系数多项式 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 的系数的最大公因子为

$$d=(a_0,a_1,\ldots,a_n),$$

则 $a_i=da_i'$,其中 $a_i'\in\mathbb{Z}$,$i=0,1,\ldots,n$,并且 $(a_0',a_1',\ldots,a_n')=1$. 因此,

$$f(x)=d(a_0'+a_1'x+\cdots+a_n'x^n).$$

记 $f_1(x)=a_0'+a_1'x+\cdots+a_n'x^n$. 显然,$f_1(x)$ 是本原多项式,并且

$$f(x)=df_1(x).$$

这说明,每个整系数多项式都可以表成系数的最大公因子和本原多项式的乘积.

Gauss 引理 任意两个本原多项式的乘积是本原多项式.

证明 设 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 与 $g(x)=b_0+b_1x+\cdots+b_mx^m$ 是本原多项式. 设 $f(x)g(x)=c_0+c_1x+\cdots+c_{n+m}x^{n+m}$,其中对于 $k=0,1,\ldots,n+m$,

$$c_k=a_0b_k+a_1b_{k-1}+\cdots+a_{k-1}b_1+a_kb_0,$$

这里约定,当 $i>m$ 时,$b_i=0$,而当 $j>n$ 时,$a_j=0$.

如果 $f(x)g(x)$ 不是本原的,则 $(c_0,c_1,\ldots,c_{n+m})\neq 1$. 设素数 p 是 $c_0,c_1,\ldots,c_{n+m}$ 的公因子. 由于 $f(x)$ 是本原的,故 p 不是 $a_0,a_1,\ldots,a_n$ 的公因子. 因此,可设 a_i 是 $a_0,a_1,\ldots,a_n$ 中第一个不被 p 整除的系数. 同理可设 b_j 是 $b_0,b_1,\ldots,b_m$ 第一个不

被 p 整除的系数.

现在考察 $f(x)g(x)$ 的系数

$$c_{i+j} = a_0b_{i+j} + \cdots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0.$$

由于素数 p 整除 $a_0, a_1, \ldots, a_{i-1}, b_0, b_1, \ldots, b_{j-1}$ 和 c_{i+j}，因此，p 整除 a_ib_j. 因为 p 是素数，故 p 整除 a_i，或者整除 b_j，不可能. 因此，

$$(c_0, c_1, \ldots, c_{n+m}) = 1.$$ ■

定理 1.6.1 设 n 次整系数多项式 $f(x)$ 在 $\mathbb{Z}$ 上不可约，则 $f(x)$ 在 $\mathbb{Q}$ 不可约.

证明 设 $f(x)$ 在 $\mathbb{Q}$ 上可约，则存在次数小于 n 的 $g(x), h(x) \in \mathbb{Q}[x]$，使得

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

将多项式 $g(x)$ 的系数通分，得到 $g(x) = b_1g_1(x), b_1 \in \mathbb{Q}, g_1(x) \in \mathbb{Z}[x]$. 而 $g_1(x)$ 可以表为系数最大公因子 d_1 和本原多项式 $\widetilde{g}(x)$ 的乘积. 因此，$g(x) = b\widetilde{g}(x)$，其中 $b = b_1d_1 \in \mathbb{Q}$.

同理，$h(x) = c\widetilde{h}(x), c \in \mathbb{Q}, \widetilde{h}(x)$ 为本原多项式. 于是，

$$f(x) = bc\widetilde{g}(x)\widetilde{h}(x).$$

由 Gauss 引理，$\widetilde{g}(x)\widetilde{h}(x)$ 是本原多项式，记 $bc = uv^{-1}, u, v \in \mathbb{Z}$. 由于 $f(x)$ 是整系数多项式，且 $\widetilde{g}(x)\widetilde{h}(x)$ 是本原的，因此，$v \mid u$. 所以，$bc \in \mathbb{Z}$. 这就说明，$f(x)$ 在 $\mathbb{Z}$ 上可约，但这是一个矛盾. ■

定理 1.6.1 说，如果整系数多项式 $f(x)$ 在 $\mathbb{Q}$ 上可约，则 $f(x)$ 在 $\mathbb{Z}$ 上可约；反之，如果整系数多项式 $f(x)$ 在 $\mathbb{Z}$ 上可约，$f(x)$ 当然在 $\mathbb{Q}$ 上可约. 因此，整系数多项式 $f(x)$ 相对于整数环 $\mathbb{Z}$ 和有理数域 $\mathbb{Q}$ 的不可约性是相同的.

定理 1.6.2 n 次整系数多项式 $f(x)$ 可以分解为一个整数和若干个本原不可约多项式的乘积，而且不计因式的次序和符号，这种分解是唯一的.

证明 根据数域 $\mathbb{F}$ 上的多项式的唯一析因定理，作为有理系数多项式，$f(x)$ 可以表为

$$f(x) = a_0p_1(x)\cdots p_s(x),$$

其中 $a_0 \in \mathbb{Q}$ 是 $f(x)$ 的首项系数，诸 $p_i(x)$ 是首一有理系数多项式，并且都在 $\mathbb{Q}$ 上不可约.

如同定理 1.6.1 的证明，$p_i(x) = b_iq_i(x)$，其中 $b_i \in \mathbb{Q}$，而 $q_i(x)$ 是本原多项式.

如果 $q_i(x)$ 在 $\mathbb{Z}$ 上可约，则 $q_i(x)$ 在 $\mathbb{Q}$ 上可约，从而 $p_i(x)$ 在 $\mathbb{Q}$ 可约，不可能. 因此，$q_i(x)$ 在 $\mathbb{Z}$ 上不可约，$i = 1, 2, \ldots, s$. 于是，

$$f(x) = a_0b_1\cdots b_sq_1(x)q_2(x)\cdots q_s(x).$$

和定理 1.6.1 的证明相同，可以证明，$a_0b_1\cdots b_s \in \mathbb{Z}$. 因此，$f(x)$ 可以表示为一个整数和若干个本原多项式的乘积.

现在设

$$f(x)=a_0p_1(x)p_2(x)\cdots p_s(x)=b_0q_1(x)q_2(x)\cdots q_s(x),$$

其中 $a_0,b_0\in\mathbb{Z}$，$p_1(x),p_2(x),\ldots,p_s(x)$ 和 $q_1(x),q_2(x),\ldots,q_s(x)$ 是本原不可约多项式. 根据定理 1.6.1，$p_1(x),\ldots,p_s(x)$ 和 $q_1(x),\ldots,q_s(x)$ 在 $\mathbb{Q}$ 上不可约. 显然，$a_0p_1(x),b_0q_1(x)$ 在 $\mathbb{Q}$ 上也不可约. 把 $f(x)$ 视为有理系数多项式，根据有理数域 $\mathbb{Q}$ 上的多项式的唯一析因定理，$s=t$，并且可以适当地调整不可约因式的次序，使得相应的有理系数不可约因式只相差一个有理数因子. 为简单计，设

$$a_0p_1(x)=c_1b_0q_1(x),p_2(x)=c_2q_2(x),\ldots,p_s(x)=c_sq_s(x),$$

其中 $c_1,c_2,\ldots,c_s\in\mathbb{Q}$.

当 $2\leqslant i\leqslant s$ 时，由于 $p_i(x)$ 与 $q_i(x)$ 是本原的，因此，$c_i=\pm1$，即 $p_i(x)=\pm q_i(x)$. 由于 $p_1(x)=a_0^{-1}c_1b_0q_1(x)$，且 $p_1(x)$ 与 $q_1(x)$ 是本原的，因此，$a_0^{-1}c_1b_0=\pm1$，即 $a_0=\pm c_1b_0$，所以，$p_1(x)=\pm q_1(x)$. 从而 $a_0=\pm b_0$. ■

定理 1.6.3（Eisenstein 判别准则） 设 $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$. 如果存在素数 p，使得 $p\mid a_i,i=0,\ldots,n-1$，但 $p\nmid a_n$ 且 $p^2\nmid a_0$，则 $f(x)$ 在 $\mathbb{Z}$ 上不可约.

证明 反证法. 设 $f(x)$ 在 $\mathbb{Z}$ 可约，则

$$f(x)=(b_0+b_1x+\cdots+b_kx^k)(c_0+c_1x+\cdots+c_\ell x^\ell),$$

其中 $b_i,c_j\in\mathbb{Z}$，并且 $k<n,\ell<n,k+\ell=n$. 于是得到，

$$a_r=b_0c_r+b_1c_{r-1}+\cdots+b_{r-1}c_1+b_rc_0,$$

其中 $r=0,1,\ldots,n$；并且当 $i\geqslant k+1$ 时，约定 $b_k=0$；当 $j\geqslant\ell+1$ 时，约定 $c_j=0$.

由于 $p\mid a_0,a_0=b_0c_0$，故 $p\mid b_0$，或者 $p\mid c_0$. 由于 $p^2\nmid a_0$，故 p 不同时整除 b_0 与 c_0. 因此可设 $p\mid b_0$，但 $p\nmid c_0$.

又因为 $p\nmid a_n$，故 $p\nmid b_k$. 所以必有某个 $1\leqslant i_0\leqslant k$，使得 $p\mid b_i,i=0,1,\ldots,i_0-1$，但 $p\nmid b_{i_0}$. 由于 $p\nmid a_{i_0},p\mid b_i,i=0,1,\ldots,i_0-1$，并且

$$a_{i_0}=b_0c_{i_0}+b_1c_{i_0-1}+\cdots+b_{i_0-1}c_1+b_0c_0,$$

故 $p\mid b_{i_0}c_0$. 因为 $p\nmid b_i$，故 $p\mid c_0$. 与 $p\nmid c_0$ 的假设相矛盾. ■

利用 Eisenstein 判别准则容易看出，对每个整数 $n\geqslant2$，都存在 n 次多项式 $f(x)\in\mathbb{Q}[x]$，使得，$f(x)$ 在 $\mathbb{Q}$ 不可约. 例如，多项式 $f(x)=x^n+2\in\mathbb{Z}[x]$，取 $p=2$，则 $f(x)$ 适合 Eisenstein 判别准则的条件，因此，$f(x)$ 在 $\mathbb{Z}$ 上不可约. 根据定理 1.6.1，作为有理系数多项式，$f(x)$ 在 $\mathbb{Q}$ 上不可约.

例 1.6.1 设 p 是素数. 多项式

$$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$$

称为**分圆多项式**. 证明，分圆多项式 $\Phi_p(x)$ 在 $\mathbb{Z}$ 上（当然也在 $\mathbb{Q}$ 上）不可约.

证明 令 $x=y+1$. 则

$$f(y)=\Phi_p(y+1)=\frac{(y+1)^p-1}{(y+1)-1}$$

$$= y^{p-1} + py^{p-2} + \cdots + \mathrm{C}_p^{k-1} y^{p-k} + \cdots + \mathrm{C}_p^{p-2} y + p.$$

显然，p 不能整除 $f(y)$ 的首项系数，p^2 不能整除 $f(y)$ 的常数项，但 p 整除 $f(y)$ 中首项系数外的其它各项. 根据 Eisenstein 判别准则，$f(y)$ 在 $\mathbb{Z}$ 上不可约.

如果 $\Phi_p(x)$ 在 $\mathbb{Z}$ 上可约，则

$$\Phi_p(x) = g(x)h(x),$$

其中 $g(x), h(x) \in \mathbb{Z}[x]$，且 $\deg g(x) < p-1, \deg h(x) < p-1$. 于是，

$$f(y) = g(y+1)h(y+1).$$

显然，$g(y+1), h(y+1) \in \mathbb{Z}[y]$. 从而 $f(y)$ 在 $\mathbb{Z}$ 上可约，矛盾. ■

例 1.6.2 设 $a_1, a_2, \ldots, a_n$ 是 n 个不同的整数. 证明，多项式

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_n) - 1$$

在 $\mathbb{Q}$ 上不可约.

证明 设 $f(x)$ 在 $\mathbb{Q}$ 上可约，则 $f(x)$ 在 $\mathbb{Z}$ 上可约，因此，

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

其中 $g(x), h(x) \in \mathbb{Z}[x]$，且 $\deg g(x) < \deg f(x), \deg h(x) < \deg f(x)$.

由于 $f(a_i) = g(a_i)h(a_i) = -1$，故 $|g(a_i)| = |h(a_i)| = 1$，且 $g(a_i) + h(a_i) = 0$. 这表明，多项式 $g(x) + h(x)$ 至少有 n 个不同的根.

由于 $\deg g(x) < n, \deg h(x) < n$，因此，$\deg(g(x) + h(x)) < n$. 因此若 $g(x) + h(x)$ 是非零多项式，则 $g(x) + h(x)$ 的根的个数小于 n，不可能. 因此，$g(x) + h(x)$ 是零多项式，从而 $f(x) = -g^2(x)$. 这和 $f(x)$ 的首项系数为 1 相矛盾. ■

习 题 1.6

1. 利用 Eisenstein 判别准则判定下述整系数多项式的不可约性.

(1) $x^4 - 8x^3 + 12x^2 - 6x + 2$；　　(2) $x^4 - x^3 + 2x + 1$；

(3) $x^4 + 1$；　　(4) $x^6 + x^3 + 1$；

(5) $\sum_{i=0}^{p-1} (x+1)^i$，其中 p 是素数.

2. 设 $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$ 是整系数多项式，且素数 p 适合：$p \nmid a_0, p \nmid a_1, \ldots, p \nmid a_k, p \mid a_i, i = k+1, k+2, \ldots, n$，而 $p^2 \nmid a_n$. 证明，$f(x)$ 具有次数不低于 $n-k$ 的整系数不可约因式.

3. 设

$$f(x) = a_0 x^{2n+1} + \cdots + a_n x^{n+1} + a_{n+1} x^n + \cdots + a_{2n} x + a_{2n+1}$$

是整系数多项式，且素数 p 适合：$p \nmid a_0, p \mid a_i, i = 1, \ldots, n, p^2 \mid a_i, i = n+1, \ldots, 2n+1$，但 $p^3 \nmid a_{2n+1}$. 证明 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

4. 设 $a_1, a_2, \ldots, a_n$ 是 n 个不同的整数. 证明，多项式

$$f(x) = (x-a_1)^2 (x-a_2)^2 \cdots (x-a_n)^2 + 1$$

在 $\mathbb{Q}$ 上不可约.

5. 试给出有理系数多项式 $f(x)=x^4+px^2+q$ 在 $\mathbb{Q}$ 上不可约的充分必要条件.

6. 设整系数多项式 $f(x)$ 在 x 的 4 个不同整数值上都取值为 1,则 $f(x)$ 在 x 的其它整数值上的值不可能是 −1.

7. 证明,设正整数 $n\geqslant 12$,并且 n 次整系数多项式 $f(x)$ 在 x 的 $\left[\frac{n}{2}\right]+1$ 个以上的整数值上取值为 ± 1,则 $f(x)$ 在 $\mathbb{Q}$ 不可约. 次数 n 的下界 12 是否还可缩小?

8. 设整系数多项式 ax^2+bx+1 在有理数域 $\mathbb{Q}$ 上不可约,并且设

$$\varphi(x)=(x-a_1)(x-a_2)\cdots(x-a_n),$$

其中 $a_1,a_2,\ldots,a_n$ 是 n 个不同的整数,$n\geqslant 7$. 证明,多项式

$$f(x)=a\varphi^2(x)+b\varphi(x)+1$$

在 $\mathbb{Q}$ 上不可约. 并问次数 n 的下界 7 是否还可缩小?

§1.7 多元多项式环

设 $\mathbb{F}$ 是数域,$x_1,x_2,\ldots,x_n$ 是 n 个未定元. 设 $\mathbb{N}$ 是所有非负整数的集合. 记

$$\mathbb{N}^n=\big\{(k_1,k_2,\ldots,k_n)\,\big|\,k_1,k_2,\ldots,k_n\in\mathbb{N}\big\}.$$

设 $(k_1,k_2,\ldots,k_n)\in\mathbb{N}$,$a_{k_1k_2\cdots k_n}\in\mathbb{F}$,则

$$a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$$

称为**数域 $\mathbb{F}$ 上的 n 元单项式**,$k_1+k_2+\cdots+k_n$ 称为它的**次数**,$a_{k_1k_2\cdots k_n}$ 称为它的**系数**.

设 M 是集合 $\mathbb{N}^n$ 的有限子集合,则

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

称为**数域 $\mathbb{F}$ 上的 n 元多项式**,其中 $a_{k_1k_2\cdots k_n}\in\mathbb{F}$. n 元多项式 $f(x_1,x_2,\ldots,x_n)$ 的所有单项式的最高次数称为 $f(x_1,x_2,\cdots,x_n)$ 的**次数**,记为 $\deg f(x_1,x_2,\ldots,x_n)$,或简记为 $\deg f$; $a_{k_1k_2\cdots k_n}$ 称为项 $a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 的**系数**.

例如,

$$f(x_1,x_2,x_3)=4x_1x_2x_3+\sqrt{3}\,x_2^3x_3+\pi x_1^3x_2^2$$

是实数域 $\mathbb{R}$ 上的 5 次 3 元多项式.

所有数域 $\mathbb{F}$ 上的 n 元多项式的集合记为 $\mathbb{F}[x_1,x_2,\ldots,x_n]$.

给定数域 $\mathbb{F}$ 上的 n 元多项式 $f(x_1,x_2,\ldots,x_n)$,可以按照**字典排列法**把它所有的项逐一写出来. 设

$$a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\text{ 和 }a_{\ell_1\ell_2\cdots\ell_n}x_1^{\ell_1}x_2^{\ell_2}\cdots x_n^{\ell_n}$$

是 $f(x_1,x_2,\ldots,x_n)$ 的两个项. 如果存在正整数 i,$1\leqslant i\leqslant n$,使得 $k_1=\ell_1,k_2=\ell_2,\ldots,k_{i-1}=\ell_{i-1}$,而 $k_i>\ell_i$,则将项 $a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 写在项 $a_{\ell_1\ell_2\cdots\ell_n}x_1^{\ell_1}x_2^{\ell_2}\cdots x_n^{\ell_n}$ 之前.

例如,3 元多项式

$$f(x_1,x_2,x_3)=x_1x_2^2x_3^2+x_1^3x_2+x_1x_3^3+x_1^2x_2x_3^2$$

可以按照字典排列写成

$$f(x_1,x_2,x_3)=x_1^3x_2+x_1^2x_2x_3^2+x_1x_2^2x_3^2+x_2x_3^3.$$

按照字典排列法写在多项式 $f(x_1,x_2,\dots,x_n)$ 的和式中最前面的项称为 $f(x_1,x_2,\dots,x_n)$ 的**首项**,相应的系数称为 $f(x_1,x_2,\dots,x_n)$ 的**首项系数**.

注意,$f(x_1,x_2,\dots,x_n)$ 的首项不一定是最高次项.

设 $f(x_1,x_2,\dots,x_n)$ 与 $g(x_1,x_2,\dots,x_n)$ 是数域 $\mathbb{F}$ 上的 n 元多项式. 如果它们的相应项的系数都相等. 则 $f(x_1,x_2,\dots,x_n)$ 与 $g(x_1,x_2,\dots,x_n)$ 称为**相等**. 两个 n 元多项式的**和**是以它们相应项的系数之和作为相应项的系数的多项式,记为

$$f(x_1,x_2,\dots,x_n)+g(x_1,x_2,\dots,x_n).$$

具体地说,设

$$f(x_1,x_2,\dots,x_n)=\sum_{(k_1,k_2,\dots,k_n)\in M_1}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},$$

$$g(x_1,x_2,\dots,x_n)=\sum_{(k_1,k_2,\dots,k_n)\in M_2}b_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},$$

其中 $M_1,M_2\subseteq\mathbb{N}^n$. 记 $M=M_1\cup M_2$,当 $(k_1,k_2,\dots,k_n)\in M_1$ 但 $(k_1,k_2,\dots,k_n)\notin M_2$ 时,约定 $b_{k_1k_2\cdots k_n}=0$; 而当 $(k_1,k_2,\dots,k_n)\notin M_1$,$(k_1,k_2,\dots,k_n)\in M_2$ 时,约定 $a_{k_1k_2\cdots k_n}=0$. 则 $f(x_1,\dots,x_n)$ 与 $g(x_1,\dots,x_n)$ 的和为

$$f(x_1,x_2,\dots,x_n)+g(x_1,x_2,\dots,x_n)=\sum_{(k_1,k_2,\dots,k_n)\in M}\left(a_{k_1k_2\cdots k_n}+b_{k_1k_2\cdots k_n}\right)x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}.$$

容易看出,

$$\deg\bigl(f(x_1,\dots,x_n)+g(x_1,\dots,x_n)\bigr)\leqslant\max\bigl\{\deg f(x_1,\dots,x_n),\ \deg g(x_1,\dots,x_n)\bigr\}.$$

对 n 元多项式的加法,容易验证下述公理成立:

(A1) 结合律 对任意 $f(x_1,x_2,\dots,x_n),g(x_1,x_2,\dots,x_n)$ 和 $h(x_1,x_2,\dots,x_n)\in\mathbb{F}[x_1,x_2,\dots,x_n]$,

$$\bigl(f(x_1,x_2,\dots,x_n)+g(x_1,x_2,\dots,x_n)\bigr)+h(x_1,x_2,\dots,x_n)$$
$$=f(x_1,x_2,\dots,x_n)+\bigl(g(x_1,x_2,\dots,x_n)+h(x_1,x_2,\dots,x_n)\bigr);$$

(A2) 交换律 对任意 $f(x_1,x_2,\dots,x_n),g(x_1,x_2,\dots,x_n)\in\mathbb{F}[x_1,x_2,\dots,x_n]$,

$$f(x_1,x_2,\dots,x_n)+g(x_1,x_2,\dots,x_n)=g(x_1,x_2,\dots,x_n)+f(x_1,x_2,\dots,x_n);$$

(A3) 存在零多项式 每个系数都为零的 n 元多项式称为**零多项式**,记为 0,同时零多项式的次数约定为 $-\infty$. 显然,$0\in\mathbb{F}[x_1,x_2,\dots,x_n]$,并且对任意 $f(x_1,x_2,\dots,x_n)\in\mathbb{F}[x_1,x_2,\dots,x_n]$,

$$f(x_1,x_2,\dots,x_n)+0=0+f(x_1,x_2,\dots,x_n)=f(x_1,x_2,\dots,x_n);$$

(A4) 存在负多项式 设

$$f(x_1,x_2,\dots,x_n)=\sum_{(k_1,k_2,\dots,k_n)\in M}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\in\mathbb{F}[x_1,x_2,\dots,x_n].$$

多项式

$$\sum_{(k_1,k_2,\dots,k_n)\in M}\left(-a_{k_1k_2\cdots k_n}\right)x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\in\mathbb{F}[x_1,x_2,\dots,x_n]$$

称为 $f(x_1,x_2,\dots,x_n)$ 的**负多项式**. 记为 $-f(x_1,x_2,\dots,x_n)$. 显然,

$$f(x_1,x_2,\dots,x_n)+\big(-f(x_1,x_2,\dots,x_n)\big)=0=\big(-f(x_1,x_2,\dots,x_n)\big)+f(x_1,x_2,\dots,x_n).$$

设

$$f(x_1,x_2,\dots,x_n)=\sum_{(k_1,k_2,\dots,k_n)\in M_1}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},$$

$$g(x_1,x_2,\dots,x_n)=\sum_{(\ell_1,\ell_2,\dots,\ell_n)\in M_2}b_{\ell_1\ell_2\cdots\ell_n}x_1^{\ell_1}x_2^{\ell_2}\cdots x_n^{\ell_n},$$

是数域 $\mathbb{F}$ 上的 n 元多项式. 又令 $m_i=k_i+\ell_i$, $i=1,2,\dots,n$, 且记

$$M=\big\{(m_1,m_2,\dots,m_n)\,\big|\,(k_1,k_2,\dots,k_n)\in M_1,(\ell_1,\ell_2,\dots,\ell_m)\in M_2\big\}.$$

则 $f(x_1,x_2,\dots,x_n)$ 与 $g(x_1,x_2,\dots,x_n)$ 的**乘积** $f(x_1,x_2,\dots,x_n)g(x_1,x_2,\dots,x_n)$ 规定为

$$f(x_1,x_2,\dots,x_n)g(x_1,x_2,\dots,x_n)=\sum_{(m_1,m_2,\dots,m_n)\in M}c_{m_1m_2\cdots m_n}x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n},$$

其中

$$c_{m_1m_2\cdots m_n}=\sum_{\substack{1\leqslant j\leqslant n\\ k_j+\ell_j=m_j}}a_{k_1k_2\cdots k_n}b_{\ell_1\ell_2\cdots\ell_n}.$$

显然, $f(x_1,x_2,\dots,x_n)g(x_1,x_2,\dots,x_n)\in\mathbb{F}[x_1,x_2,\dots,x_n]$, 并且其首项系数等于 $f(x_1,x_2,\dots,x_n)$ 与 $g(x_1,x_2,\dots,x_n)$ 的首项系数的乘积, 即

$$\deg\big(f(x_1,x_2,\dots,x_n)g(x_1,x_2,\dots,x_n)\big)=\deg f(x_1,x_2,\dots,x_n)+\deg g(x_1,x_2,\dots,x_n).$$

此外, 对 n 元多项式的乘法, 乘法结合律、乘法交换律以及乘法对加法的分配律成立. 同时, 对任意 $f(x_1,x_2,\dots,x_n)\in\mathbb{F}[x_1,x_2,\dots,x_n]$, 均有

$$1\cdot f(x_1,x_2,\dots,x_n)=f(x_1,x_2,\dots,x_n)=f(x_1,x_2,\dots,x_n)\cdot 1,$$

其中 1 是数域 $\mathbb{F}$ 上的零次多项式.

于是, $\mathbb{F}[x_1,x_2,\dots,x_n]$ 在上述多项式的加法与乘法下构成一个交换环. 它称为数域 $\mathbb{F}$ 上的 ***n* 元多项式环**.

习 题 1.7

1. 设 $f(x_1,x_2,\dots,x_n),g(x_1,x_2,\dots,x_n)\in\mathbb{F}[x_1,x_2,\dots,x_n]$. 证明, 如果

$$f(x_1,x_2,\dots,x_n)g(x_1,x_2,\dots,x_n)$$

为零多项式, 则 $f(x_1,x_2,\dots,x_n)$ 与 $g(x_1,x_2,\dots,x_n)$ 至少有一个是零多项式.

2. 设 $f(x_1,x_2,\dots,x_n),g(x_1,x_2,\dots,x_n),h(x_1,x_2,\dots,x_n)\in\mathbb{F}[x_1,x_2,\dots,x_n]$. 证明, 如果

$$f(x_1,x_2,\dots,x_n)g(x_1,x_2,\dots,x_n)=f(x_1,x_2,\dots,x_n)h(x_1,x_2,\dots,x_n),$$

则 $g(x_1,x_2,\dots,x_n)=h(x_1,x_2,\dots,x_n)$.

3. 验证 $\mathbb{F}[x_1,x_2,\dots,x_n]$ 在 n 元多项式的加法与乘法下成为一个交换环.

§1.8 对称多项式

设 $\mathbb{F}[x_1, x_2, \ldots, x_n]$ 是数域 $\mathbb{F}$ 上的 n 元多项式环. 在 n 元多项式中,经常遇到的是所谓对称多项式. 其定义如下:

定义 1.8.1 设 $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. 如果对自然数 $1, 2, \ldots, n$ 的任意一个排列 $i_1 i_2 \cdots i_n$,都有

$$f(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) = f(x_1, x_2, \ldots, x_n),$$

则 $f(x_1, x_2, \ldots, x_n)$ 称为 n 元**对称多项式**.

例如,容易看出,

$$\sigma_1 = x_1 + x_2 + \cdots + x_n = \sum_{1 \leqslant i_1 \leqslant n} x_{i_1},$$

$$\sigma_2 = x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n = \sum_{1 \leqslant i_1 < i_2 \leqslant n} x_{i_1}x_{i_2},$$

$$\cdots\cdots\cdots\cdots$$

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1}x_{i_2}\cdots x_{i_k},$$

$$\cdots\cdots\cdots$$

$$\sigma_n = x_1x_2\cdots x_n,$$

都是 n 元对称多项式. 它们称为 n 元**基本对称多项式**.

可验证,两个 n 元对称多项式之和、差与积仍是 n 元对称多项式.

此外,对任意多项式 $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$,如果用基本对称多项式 $\sigma_1, \sigma_2, \ldots, \sigma_n$ 分别替换 $f(x_1, x_2, \ldots, x_n)$ 中的未定元 $x_1, x_2, \ldots, x_n$,得到 $f(\sigma_1, \sigma_2, \ldots, \sigma_n)$,则 $f(\sigma_1, \sigma_2, \ldots, \sigma_n)$ 是一个关于未定元 $x_1, x_2, \ldots, x_n$ 的对称多项式. 例如取 $n = 3$, $f(x_1, x_2, x_3) = x_1x_2 + 2x_3 \in \mathbb{R}[x_1, x_2, x_3]$. 用 $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$ 与 $\sigma_3 = x_1x_2x_3$ 分别替换 $f(x_1, x_2, x_3)$ 的未定元 x_1, x_2, x_3,得到

$$f(\sigma_1, \sigma_2, \sigma_3) = \sigma_1\sigma_2 + 2\sigma_3 = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2 + 5x_1x_2x_3,$$

显然,它是一个三元对称多项式. 反之,有

定理 1.8.1(对称多项式基本定理) 设 $f(x_1, x_2, \ldots, x_n)$ 是数域 $\mathbb{F}$ 上的 n 元对称多项式. 则存在唯一的多项式 $g(x_1, x_2, \ldots, x_n) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$,使得

$$f(x_1, x_2, \ldots, x_n) = g(\sigma_1, \sigma_2, \ldots, \sigma_n),$$

其中 $\sigma_1, \sigma_2, \ldots, \sigma_n$ 是数域 $\mathbb{F}$ 上的 n 元基本对称多项式.

证明 **存在性** 设对称多项式 $f(x_1, x_2, \ldots, x_n)$ 的首项为

$$a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},$$

则一定有 $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_n$. 否则,将有某个 j,使得 $k_j < k_{j+1}$. 由于 $f(x_1, x_2, \ldots, x_n)$

是对称的，则通过对换未定元 x_j 和 x_{j+1} 便可着出，$f(x_1,x_2,\dots,x_n)$ 含有项

$$a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_{j-1}^{k_{j-1}}x_j^{k_{j+1}}x_{j+1}^{k_j}x_{j+1}^{k_{j+1}}\cdots x_n^{k_n}.$$

显然，按字典排列法它应排在项 $a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 之前，这和 $a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 为 $f(x_1,x_2,\dots,x_n)$ 的首项的假设相矛盾.

取 n 元对称多项式 $\varphi_1(x_1,x_2,\dots,x_n)$ 为

$$\varphi_1(x_1,x_2,\dots,x_n)=a_{k_1k_2\cdots k_n}\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\cdots\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}.$$

容易看出，$\sigma_1,\sigma_2,\dots,\sigma_n$ 的首项依次是 $x_1,x_1x_2,\dots,x_1x_2\cdots x_n$. 因此，$\varphi_1(x_1,x_2,\dots,x_n)$ 的首项为 $a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$. 于是，

$$f_1(x_1,x_2,\dots,x_n)=f(x_1,x_2,\dots,x_n)-\varphi_1(x_1,x_2,\dots,x_n)$$

是数域 $\mathbb{F}$ 上的 n 元对称多项式.

如果 $f_1(x_1,x_2,\dots,x_n)$ 是零多项式，则 $f(x_1,x_2,\dots,x_n)=\varphi_1(x_1,x_2,\dots,x_n)$ 是关于 $\sigma_1,\sigma_2,\dots,\sigma_n$ 的多项式.

如果 $f_1(x_1,x_2,\dots,x_n)$ 是非零多项式，则 $f(x_1,x_2,\dots,x_n)$ 的首项 $a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 应在 $f_1(x_1,x_2,\dots,x_n)$ 的首项 $b_{\ell_1\ell_2\cdots\ell_n}x_1^{\ell_1}x_2^{\ell_2}\cdots x_n^{\ell_n}$ 之前，其中 $\ell_1\geqslant\ell_2\geqslant\cdots\geqslant\ell_n$. 记

$$\varphi_2(x_1,x_2,\dots,x_n)=b_{\ell_1\ell_2\cdots\ell_n}\sigma_1^{\ell_1-\ell_2}\sigma_2^{\ell_2-\ell_3}\cdots\sigma_{n-1}^{\ell_{n-1}-\ell_n}\sigma_n^{\ell_n}.$$

则数域 $\mathbb{F}$ 上的 n 元对称多项式

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

为零多项式，或为非零多项式，并且 $f_1(x_1,x_2,\dots,x_n)$ 的首项在 $f_2(x_1,x_2,\dots,x_n)$ 的首项之前.

设 $f_2(x_1,x_2,\dots,x_n)$ 为非零多项式. 重复上述过程，得到对称多项式序列：

$$\begin{aligned}
f_0(x_1,x_2,\dots,x_n)&=f(x_1,x_2,\dots,x_n),\\
f_1(x_1,x_2,\dots,x_n)&=f_0(x_1,x_2,\dots,x_n)-\varphi_1(x_1,x_2,\dots,x_n),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
f_{i+1}(x_1,x_2,\dots,x_n)&=f_i(x_1,x_2,\dots,x_n)-\varphi_{i+1}(x_1,x_2,\dots,x_n),
\end{aligned}$$

其中 $\varphi_{i+1}(x_1,x_2,\dots,x_n)$ 是关于 $\sigma_1,\sigma_2,\dots,\sigma_n$ 的多项式，而且 $f_i(x_1,x_2,\dots,x_n)$ 的首项在 $f_{i+1}(x_1,x_2,\dots,x_n)$ 的首项之前，$i=0,1,\dots$.

设 $f_i(x_1,x_2,\dots,x_n)$ 的首项为 $c_{m_1m_2\cdots m_n}x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$，则 $m_1\geqslant m_2\geqslant\cdots\geqslant m_n$，并且由于 $f(x_1,x_2,\dots,x_n)$ 的首项在 $f_i(x_1,x_2,\dots,x_n)$ 的首项之前，故 $k_1\geqslant m_1$.

因为适合 $k_1\geqslant m_1$ 的非负整数 m_1 只有有限多个，而且对每个适合 $k_1\geqslant m_1$ 的非负整数 m_1，适合 $m_1\geqslant m_2\geqslant\cdots\geqslant m_n$ 的 n 元非负整数组 $(m_1,m_2,\dots,m_n)$ 也只有有限多个，因此存在某个 j，使得 $f_j(x_1,x_2,\dots,x_n)=0$. 于是，

$$f(x_1,\dots,x_n)=\varphi_1(x_1,\dots,x_n)+\varphi_2(x_1,\dots,x_n)+\cdots+\varphi_j(x_1,\dots,x_n).$$

这就证明，$f(x_1,x_2,\dots,x_n)$ 可以表为系数在 $\mathbb{F}$ 中的关于 $\sigma_1,\sigma_2,\dots,\sigma_n$ 的多项式.

唯一性 设存在 $g(x_1,x_2,\dots,x_n),h(x_1,x_2,\dots,x_n)\in\mathbb{F}[x_1,x_2,\dots,x_n]$,使得

$$f(x_1,x_2,\dots,x_n)=g(\sigma_1,\sigma_2,\dots,\sigma_n)=h(\sigma_1,\sigma_2,\dots,\sigma_n). \tag{1.8.1}$$

设 $g(x_1,x_2,\dots,x_n)$ 与 $h(x_1,x_2,\dots,x_n)$ 的首项分别为

$$a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\text{ 与 }b_{\ell_1\ell_2\cdots\ell_n}x_1^{\ell_1}x_2^{\ell_2}\cdots x_n^{\ell_n}.$$

于是,

$$g\big(\sigma_1(x_1,x_2,\dots,x_n),\sigma_2(x_1,x_2,\dots,x_n),\dots,\sigma_n(x_1,x_2,\dots,x_n)\big)$$

的首项为

$$a_{k_1k_2\cdots k_n}x_1^{k_1}(x_1x_2)^{k_2}\cdots(x_1x_2\cdots x_n)^{k_n}=a_{k_1k_2\cdots k_n}x_1^{k_1+k_2+\cdots+k_n}x_2^{k_2+\cdots+k_n}\cdots x_n^{k_n},$$

而

$$h\big(\sigma_1(x_1,x_2,\dots,x_n),\sigma_2(x_1,x_2,\dots,x_n),\dots,\sigma_n(x_1,x_2,\dots,x_n)\big)$$

的首项为

$$b_{\ell_1\ell_2\cdots\ell_n}x_1^{\ell_1+\ell_2+\cdots+\ell_n}x_2^{\ell_2+\cdots+\ell_n}\cdots x_n^{\ell_n}.$$

由式 (1.8.1),$a_{k_1k_2\cdots k_n}=b_{\ell_1\ell_2\cdots\ell_n}$,并且

$$\begin{aligned}
k_1+k_2+\cdots+k_n&=\ell_1+\ell_2+\cdots+\ell_n,\\
k_1+k_2+\cdots+k_{n-1}&=\ell_1+\ell_2+\cdots+\ell_{n-1},\\
&\cdots\cdots\cdots\\
k_{n-1}+k_n&=\ell_{n-1}+\ell_n,\\
k_n&=\ell_n.
\end{aligned}$$

由此得到 $k_1=\ell_1,k_2=\ell_2,\dots,k_n=\ell_n$. 即 $g(x_1,x_2,\dots,x_n)$ 与 $h(x_1,x_2,\dots,x_n)$ 具有相同的首项. 从 $g(x_1,x_2,\dots,x_n)$ 与 $h(x_1,x_2,\dots,x_n)$ 中各减去首项,分别记为 $g_1(x_1,x_2,\dots,x_n)$ 与 $h_1(x_1,x_2,\dots,x_n)$. 显然,

$$\begin{aligned}
&g_1\big(\sigma_1(x_1,x_2,\dots,x_n),\sigma_2(x_1,x_2,\dots,x_n),\dots,\sigma_n(x_1,x_2,\dots,x_n)\big)\\
&\quad=h_1\big(\sigma_1(x_1,x_2,\dots,x_n),\sigma_2(x_1,x_2,\dots,x_n),\dots,\sigma_n(x_1,x_2,\dots,x_n)\big),
\end{aligned}$$

上式是关于 $x_1,x_2,\dots,x_n$ 的对称多项式,记为 $f_1(x_1,x_2,\dots,x_n)$.

再对 $f_1(x_1,x_2,\dots,x_n),g_1(x_1,x_2,\dots,x_n)$ 与 $h_1(x_1,x_2,\dots,x_n)$ 用上述证明,如此继续,即可证明

$$g(x_1,x_2,\dots,x_n)=h(x_1,x_2,\dots,x_n)$$ ■

定理 1.8.1 中关于存在性部分的证明是构造性的,它给出了对称多项式表为关于基本对称多项式 $\sigma_1,\sigma_2,\dots,\sigma_n$ 的多项式的具体方法.

各个项次数相等的多项式称为**齐次多项式**,否则称为**非齐次多项式**.

例如,多项式

$$g(x_1,x_2,\dots,x_n)=\sum_{1\leqslant i<j\leqslant n}x_i^2x_j$$

是一个三次齐次多项式.

对于给定的 m 次齐次多项式 $f(x_1,x_2,\dots,x_n)$,可以把它的同次项归并在一起,

得到

$$f(x_1,x_2,\dots,x_n)=\sum_{j=0}^{m}f_j(x_1,x_2,\dots,x_n),$$

其中 $f_j(x_1,x_2,\dots,x_n)$ 是 j 次齐次多项式，即 $f(x_1,x_2,\dots,x_n)$ 可以表为若干个齐次多项式之和.

把对称多项式 $f(x_1,x_2,\dots,x_n)$ 表为关于基本对称多项式 $\sigma_1,\sigma_2,\dots,\sigma_n$ 的多项式，除了定理 1.8.1 所给出的方法外，还可以采用待定系数法，其步骤如下：

(1) 把多项式 $f(x_1,x_2,\dots,x_n)$ 分解为齐次多项式之和. 容易看出，由于 $f(x_1,x_2,\dots,x_n)$ 是对称的，因此，这些齐次多项式也是对称的；

(2) 设 m 次齐次对称多项式 $f_m(x_1,x_2,\dots,x_n)$ 的首项是

$$a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},$$

其中 $k_1\geqslant k_2\geqslant\cdots\geqslant k_n$，并且 $k_1+k_2+\cdots+k_n=m$. 写出所有可能排在 $f_m(x_1,x_2,\dots,x_n)$ 的首项之后的项 $a_{\ell_1\ell_2\cdots\ell_n}x_1^{\ell_1}x_2^{\ell_2}\cdots x_n^{\ell_n}$，其中 $\ell_1\geqslant\ell_2\geqslant\cdots\geqslant\ell_n$，$\ell_1+\ell_2+\cdots+\ell_n=m$，并且存在某个 j，使得 $k_1=\ell_1,\dots,k_{j-1}=\ell_{j-1},k_j>\ell_j,1\leqslant j\leqslant n$，这里 j 与项 $a_{\ell_1\ell_2,\dots\ell_n}x_1^{\ell_1}x_2^{\ell_2}\cdots x_n^{\ell_n}$ 有关. 所有适合这些条件的 $(\ell_1,\ell_2,\dots,\ell_n)\in\mathbb{R}^n$ 的集合记为 M；

(3) 对每个可能出现的项 $a_{\ell_1\ell_2\cdots\ell_n}x_1^{\ell_1}x_2^{\ell_2}\cdots x_n^{\ell_n}$ 构作一个项

$$A_{\ell_1\ell_2\cdots\ell_n}\sigma_1^{\ell_1-\ell_2}\sigma_2^{\ell_2-\ell_3}\cdots\sigma_{n-1}^{\ell_{n-1}-\ell_n}\sigma_n^{\ell_n},$$

并令

$$f(x_1,x_2,\dots,x_n)=\sum_{(\ell_1,\ell_2,\dots,\ell_n)\in M}A_{\ell_1\ell_2\cdots\ell_n}\sigma_1^{\ell_1-\ell_2}\sigma_2^{\ell_2-\ell_3}\cdots\sigma_{n-1}^{\ell_{n-1}-\ell_n}\sigma_n^{\ell_n},$$

其中 $A_{\ell_1\ell_2\cdots\ell_n}$ 为待定常数；

(4) 取 $x_1,x_2,\dots,x_n$ 的一些特殊值，代入上式，便得到一组关于 $A_{\ell_1\ell_2\cdots\ell_n}$ 的方程，解之即得 $A_{\ell_1\ell_2\cdots\ell_n}$. 通常特殊值可以取为 $x_1=x_2=\cdots=x_k=1,x_{k+1}=\cdots=x_n=0$. 把它们代入 $\sigma_j(x_1,x_2,\dots,x_n)$，得到

$$\sigma_j\Big(\underbrace{1,1,\dots,1}_{k\text{个}},0,\dots,0\Big)=\begin{cases}\mathrm{C}_k^j, & 1\leqslant j\leqslant k,\\ 0, & k<j\leqslant n.\end{cases}$$

例 1.8.1 把 n 元对称多项式

$$f(x_1,x_2,\dots,x_n)=\sum_{1\leqslant j_1<j_2<j_3\leqslant n}\left(x_{j_1}^2x_{j_2}^2x_{j_3}+x_{j_1}^2x_{j_2}x_{j_3}^2+x_{j_1}x_{j_2}^2x_{j_3}^2\right)$$

表为关于基本对称多项式的多项式，其中 $n\geqslant 5$.

解 $f(x_1,x_2,\dots,x_n)$ 本身是 5 次齐次对称多项式，它的首项是 $x_1^2x_2^2x_3$. 可能出现在它后面的项有 $x_1^2x_2x_3x_4,x_1x_2x_3x_4x_5$. 令

$$\begin{aligned}f(x_1,x_2,\dots,x_n)&=\sigma_1^{2-1}\sigma_2^{2-1}\sigma_3^{1}+A\sigma_1^{2-1}\sigma_2^{1-1}\sigma_3^{1-1}\sigma_4+B\sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^{1-1}\sigma_4^{1-1}\sigma_5^{1}\\&=\sigma_2\sigma_3+A\sigma_1\sigma_4+B\sigma_5.\end{aligned}$$

取 $x_1=x_2=x_3=x_4=1,x_5=0$. 则 $\sigma_1=\mathrm{C}_4^1=4,\sigma_2=\mathrm{C}_4^2=6,\sigma_3=\mathrm{C}_4^3=4,\sigma_4=\mathrm{C}_4^4=1,\sigma_5=0$，并且 $f(1,1,1,1,0,\dots,0)=12$. 因此，$12=24+4A$. 所以，$A=-3$.

再取 $x_1=x_2=\cdots=x_5=1, x_6=x_7=\cdots=x_n=0$. 则 $\sigma_1=\mathrm{C}_5^1=5, \sigma_2=\mathrm{C}_5^2=10, \sigma_3=\mathrm{C}_5^3=10$, $\sigma_4=\mathrm{C}_5^4=5, \sigma_5=1$, 并且 $f(1,1,1,1,1,0,\ldots,0)=3\mathrm{C}_5^3=30$. 因此, $30=100-3\times 25+B$. 所以, $B=5$.

由此得到,

$$f(x_1,x_2,\ldots,x_n)=\sigma_2\sigma_3-3\sigma_1\sigma_4+5\sigma_5. \qquad \blacksquare$$

利用基本对称多项式, 可以得到关于一元多项式的根与系数的定理.

定理 1.8.2 (Viète 定理) 设数域 $\mathbb{F}$ 上的 n 次多项式

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

的根为 $c_1,c_2,\ldots,c_n$, 则对于 $k=0,1,\ldots,n$,

$$a_k=(-1)^{n-k}\sigma_{n-k}(c_1,c_2,\ldots,c_n),$$

其中 $a_n=1$, 且 $\sigma_0(c_1,c_2,\ldots,c_n)=1$.

证明　因为 $c_1,c_2,\ldots,c_n$ 是首一多项式 $f(x)$ 的根, 所以

$$f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n=(x-c_1)(x-c_2)\cdots(x-c_n).$$

上式右端乘开, 并比较上式两端同次项系数, 得到

$$\begin{aligned}
a_{n-1}&=-(c_1+c_2+\cdots+c_n)\\
&=-\sigma_1(c_1,c_2,\ldots,c_n),\\
a_{n-2}&=c_1c_2+c_1c_3+\cdots+c_1c_n+c_2c_3+\cdots+c_2c_n+\cdots+c_{n-1}c_n\\
&=\sigma_2(c_1,c_2,\ldots,c_n),\\
&\cdots\cdots\cdots\cdots\\
a_k&=(-1)^{n-k}(c_1\cdots c_{n-k-1}c_{n-k}+c_1\cdots c_{n-k-1}c_{n-k+1}+\cdots+c_1\cdots c_{n-k-1}c_n\\
&\qquad +c_1\cdots c_{n-k-2}c_{n-k}c_{n-k+1}+\cdots+c_1\cdots c_{n-k-2}c_{n-k}c_n+\cdots+c_{k+1}c_{k+2}\cdots c_n)\\
&=(-1)^{n-k}\sigma_{n-k}(c_1,c_2,\ldots,c_n),\\
&\cdots\cdots\cdots\cdots\\
a_1&=(-1)^{n-1}(c_1c_2\cdots c_{n-1}+c_1c_2\cdots c_{n-2}c_n+c_1c_2\cdots c_{n-3}c_{n-1}c_n+\cdots+c_2c_3\cdots c_n)\\
&=(-1)^{n-1}\sigma_{n-1}(c_1,c_2,\ldots,c_n),\\
a_0&=(-1)^n(c_1c_2\cdots c_n)\\
&=(-1)^n\sigma_n(c_1,c_2,\ldots,c_n).
\end{aligned}$$

$\blacksquare$

例 1.8.2　证明多项式 $f(x)=x^9+x^7+x^5+x^2+x-1$ 的根的平方和为 -2.

证明　设 $c_1,c_2,\ldots,c_n$ 是 $f(x)$ 的根. 把 $f(x)$ 的根的平方和表为基本对称多项式的多项式, 得到

$$\sum_{j=1}^{9}c_j^2=\sigma_1^2(c_1,c_2,\ldots,c_n)-2\sigma_2(c_1,c_2,\ldots,c_n).$$

由定理 1.8.2, $\sigma_1(c_1,c_2,\ldots,c_n)=0, \sigma_2(c_1,c_2,\ldots,c_n)=1$, 于是,

$$\sum_{j=1}^{9}c_j^2=-2. \qquad \blacksquare$$

在对称多项式中,除基本对称多项式外,还有一组重要的对称多项式,即**等幂和**,其定义为,对于 $k=0,1,2,\ldots$,

$$s_k(x_1,x_2,\ldots,x_n)=x_1^k+x_2^k+\cdots+x_n^k.$$

关于基本对称多项式与等幂和,有

定理 1.8.3(Newton 恒等式) 当 $k\geqslant n$ 时,

$$s_k-\sigma_1 s_{k-1}+\sigma_2 s_{k-2}+\cdots+(-1)^{n-1}\sigma_{n-1}s_{k-n+1}+(-1)^n\sigma_n s_{k-n}=0;$$

当 $k<n$ 时,

$$s_k-\sigma_1 s_{k-1}+\sigma_2 s_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}s_1+(-1)^k k\sigma_k=0.$$

证明 将 $x_1,x_2,\ldots,x_n$ 视为常数,考虑多项式

$$f(x)=(x-x_1)(x-x_2)\cdots(x-x_n).$$

由 Vièta 定理,

$$f(x)=\sum_{j=0}^{n}(-1)^{n-j}\sigma_{n-j}(x_1,x_2,\ldots,x_n)x^j. \tag{1.8.2}$$

因为 $f(x)=(x-x_1)(x-x_2)\cdots(x-x_n)$,所以

$$f'(x)=f(x)\sum_{i=1}^{n}\frac{1}{x-x_i}.$$

记

$$g(x)=f(x)\sum_{i=1}^{n}\frac{x_i^{k+1}}{x-x_i},$$

显然,$\deg g(x)<n$. 于是,对任意正整数 k,

$$\begin{aligned}x^{k+1}f'(x)-g(x)&=f(x)\sum_{i=1}^{n}\frac{x^{k+1}-x_i^{k+1}}{x-x_i}\\&=f(x)\sum_{i=1}^{n}(x^k+x^{k-1}x_i+\cdots+x_i^k)\\&=f(x)\sum_{i=1}^{n}(nx^k+s_1x^{k-1}+\cdots+s_{k-1}x+s_k).\end{aligned}$$

即

$$x^{k+1}f'(x)=f(x)\sum_{i=1}^{n}(nx^k+s_1x^{k-1}+\cdots+s_{k-1}x+s_k)+g(x),$$

其中 $\deg g(x)<n$. 将 (1.8.2) 代入上式,得到

$$\sum_{i=1}^{n}(-1)^{n-i}i\sigma_{n-i}x^{k+i}=\Big(\sum_{j=0}^{n}(-1)^{n-j}\sigma_{n-j}x^j\Big)\Big(\sum_{i=0}^{k}s_ix^{k-i}\Big)+g(x). \tag{1.8.3}$$

当 $k<n$ 时,比较上式两端 n 次项系数,得到

$$(-1)^k(n-k)\sigma_k=s_k-\sigma_1s_{k-1}+\cdots+(-1)^{k-1}\sigma_{k-1}s_1+(-1)^k n\sigma_k.$$

因此,当 $k<n$ 时,

$$s_k-\sigma_1s_{k-1}+\cdots+(-1)^{k-1}\sigma_{n-1}s_1+(-1)^k k\sigma_k=0.$$

当 $k \geqslant n$ 时，比较式 (1.8.3) 两端 n 次项系数，得到

$$s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{n-1}\sigma_{n-1}s_{k-n+1} + (-1)^n \sigma_n s_{k-n} = 0. \qquad \blacksquare$$

利用 Newton 恒等式，可以把基本对称多项式表为等幂和的多项式. 例如，

$$\sigma_1 = s_1, \qquad \sigma_2 = \frac{s_1^2 - s_2}{2}, \qquad \sigma_3 = \frac{s_1^3 - 3s_1 s_2 + 2s_3}{6},$$

等等. 于是再利用定理 1.8.1，即可得到

推论 1.8.1　数域 $\mathbb{F}$ 上的 n 元对称多项式 $f(x_1, x_2, \ldots, x_n)$ 可以唯一地表为关于等幂和 $s_1, s_2, \ldots, s_n$ 的多项式，即存在唯一的 $g(x_1, x_2, \ldots, x_n) \in \mathbb{F}[x]$，使得

$$f(x_1, x_2, \ldots, x_n) = g\big(s_1(x_1, x_2, \ldots, x_n), s_2(x_1, x_2, \ldots, x_n), \ldots, s_n(x_1, x_2, \ldots, x_n)\big).$$

习　题　1.8

1. 把下列对称多项式表为关于基本对称多项式的多项式.

(1) $(x_1^2 + x_2^2)(x_2^2 + x_3^2)(x_3^2 + x_1^2)$;

(2) $(2x_1 - x_2 - x_3)(2x_2 - x_3 - x_1)(2x_3 - x_1 - x_2)$;

(3) $(-x_1 + x_2 + \cdots + x_n)(x_1 - x_2 + \cdots + x_n)\cdots(x_1 + x_2 + \cdots + x_{n-1} - x_n)$;

(4) $\sum\limits_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2$;　　(5) $\sum\limits_{\substack{1 \leqslant i < j \leqslant n \\ k \neq i, j}} (x_i + x_j - x_k)^2$;

(6) $\sum\limits_{\left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{smallmatrix}\right)} \left(a_1 x_{i_1} + a_2 x_{i_2} + \cdots + a_n x_{i_n}\right)^2$，这里的求和号表示对遍历自然数 $1, 2, \ldots, n$ 的所有排列 $i_1, i_2, \ldots, i_n$ 求和.

2. 证明，三次实系数方程 $x^3 + ax^2 + bx + c = 0$ 的每个根的实部都是负数的充分必要条件为

$$a > 0, \qquad ab - c > 0, \qquad c > 0.$$

3. 设三次方程 $x^3 + ax^2 + bx + c = 0$ 的三个根是某个三角形的内角的正弦. 证明，

$$a(4ab - a^3 - 8c) = 4c^2.$$

4. 设 $x_1, x_2, \ldots, x_n$ 是多项式 $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ 的 n 个根. 证明，关于 $x_2, x_3, \ldots, x_n$ 的对称多项式可以表为关于 x_1 的多项式.

5. 求

$$\sum_{i=1}^{n} \frac{\partial \sigma_k}{\partial x_i},$$

其中求和号后的偏导数表示 $\sigma_k(x_1, x_2, \ldots, x_n)$ 关于 x_i 的偏导数.

6. 设对称多项式 $f(x_1, x_2, \ldots, x_n)$ 满足

$$f(x_1 + a, x_2 + a, \ldots, x_n + a) = f(x_1, x_2, \ldots, x_n),$$

其中 a 是任意常数. 设 $f(x_1, x_2, \ldots, x_n) = g(\sigma_1, \sigma_2, \ldots, \sigma_n)$. 证明

$$n\frac{\partial g}{\partial \sigma_1} + (n-1)\sigma_1 \frac{\partial g}{\partial \sigma_2} + \cdots + \sigma_{n-1}\frac{\partial g}{\partial \sigma_n} = 0.$$

7. 把 n 元等幂和 $s_1, s_2, \ldots, s_6$ 表为关于 n 元基本对称多项式的多项式，其中 $n \geqslant 6$.

8. 把 n 元基本对称多项式 $\sigma_4, \sigma_5, \sigma_6$ 表为 n 元等幂和 $s_1, s_2, \ldots$ 的多项式.

9. 把下列 n 元对称多项式表为 n 元等幂和的多项式，其中 k 是正整数.

(1) $\sum\limits_{1 \leqslant i < j \leqslant n} x_i^k x_j^k$;　　(2) $\sum\limits_{1 \leqslant i < j \leqslant n} (x_i + x_j)^k$;　　(3) $\sum\limits_{1 \leqslant i < j \leqslant n} (x_i - x_j)^{2k}$.

10. 求多项式

$$f(x)=x^n+(a+b)x^{n-1}+(a^2+b^2)x^{n-2}+\cdots+(a^{n-1}+b^{n-1})x+(a^n+b^n)$$

的根的等幂和 $s_1,s_2,\ldots,s_n$.

11. 自然数 $1,2,\ldots,n$ 的**循环排列**是指排列 $12\cdots n$ 与 $j(j+1)\cdots n12\cdots(j-1)$, $j=2,3,\ldots,n$. 如果对于 $1,2,\ldots,n$ 的每个循环排列 $j(j+1)\cdots n12\cdots(j-1)$, 多项式 $f(x_1,\ldots,x_n)$ 适合

$$f\big(x_j,x_{j+1},\ldots,x_n,x_1,x_2,\ldots,x_{j-1}\big)=f(x_1,x_2,\ldots,x_n),$$

其中 $j=2,3,\ldots,n$, 则 $f(x_1,x_2,\ldots,x_n)$ 称为在未定元 $x_1,x_2,\ldots,x_n$ 的**循环变换下不变**. 证明, 循环变换下不变的多项式 $f(x_1,x_2,\ldots,x_n)$ 可表为多项式

$$g_j(x_1,x_2,\ldots,x_n)=x_1\omega^j+x_2\omega^{2j}+\cdots+x_n\omega^{nj}$$

的多项式, 其中 $j=0,1,\ldots,n-1$, $\omega,\omega^2,\ldots,\omega^n$ 分别是方程 $x^n=1$ 的 n 个相异复数根.