第/1/章

基 本 概 念

高等代数是大学数学的基础课程之一，是中学数学的继续与提高. 通过对高等代数的学习，我们将会发现，它与中学数学有很大的不同. 这种不同不仅表现在内容的深度上，更重要的是体现在思维与方法上.

在高等数学里，每一个概念都是由具体事物经抽象而得到的. 在学习这些概念时，就要寻找这些概念的背景，才能获得对这些概念的深刻认识.

1.1 数学归纳法

数学归纳法是数学中一个非常重要的证明方法. 在中学的学习中，我们只知道用数学归纳法去证明有关正整数的命题，但不知道其原因. 如果有人问："为什么能证明有关正整数的命题?"回答只能是："老师教的."进入大学后，我们可不能用这样的回答来应付，于是就应该寻求数学归纳法的依据.

由于数学归纳法论证的对象是有关正整数集

$$\mathbb{N}^+ = \{1,2,\cdots,n,\cdots\}$$

的命题，于是数学归纳法的依据就应该是正整数集的属性.

1.1.1 正整数集

什么是正整数呢?

正整数——从 1 开始，一个接一个地数，数出来的数称为正整数.

所有正整数构成的集合称为**正整数集**.

这是一个粗浅的解释，其实质是：

(1) 正整数集有一个初始元 1；

(2) 正整数集中的任一个数 a 有继元 $a+1$.

上面两条属性是皮亚诺总结出来的，所以称为皮亚诺公理. 在我们给出的粗浅解释中，"一个接一个"就体现了"有继元".

ie：如果集合 A 有初始元 1，且 A 中任一元素 a 的继元 $a+1$ 也属于 A，则 A 就是正整数集.

由此，我们通过“类比”的思维方法，就得到了下面的归纳原理.

归纳原理　如果正整数集$\mathbb{N}^+$的初始元 1 具有属性 P，且当$\mathbb{N}^+$中任一元素 n 具有属性 P 时，n 的继元 $n+1$ 也具有属性 P，则正整数集中的所有元素都具有属性 P.

为了证明归纳原理，我们还得介绍正整数集的公理与最小数原理.

自然公理　$\forall n\in\mathbb{N}^+$，数集$\{1,2,\cdots,n\}$是有限集.

什么叫公理？在中学的解释是：大家公认的道理. 这个解释不确切. 为了解释公理，我们还得从数学的要求说起.

在数学王国里，有一个规定，即：不允许有循环的解释与循环的论证.

什么是循环的解释呢？例如在中文里，

多者，不少也；少者，不多也.

这就是一个循环的解释. 由于不允许有循环的解释就产生了最基本的概念；由于不允许有循环的论证就产生了最基本的道理. 我们把最基本的道理称为公理.

在这里，还有一个问题不能解决，即：什么叫有限集？可以说，对“有限集”的认识，还停留在“只可意会，不可言传”的阶段. 只有在学习实变函数这门课程后才有深刻的了解.

定理 1.1.1（最小数原理）　正整数集$\mathbb{N}^+$的任一非空子集必存在最小数.

对于一个定理，首先要解读它，然后才能证明它. 定理 1.1.1 指出，S 是$\mathbb{N}^+$中的任意一个非空的子集，则 S 中必有最小的数 n_0. 所谓最小数，必定在 S 中，而且 S 中所有数都不会比 n_0 小. 用数学语言来描述就是：

$$\forall S\subseteq\mathbb{N}^+, S\neq\varnothing,\quad \text{则 } \exists n_0\in S,\quad \ni\text{“}\forall n\in S, n\geqslant n_0\text{”}.$$

从这里，你可以看到，用数学语言描述的简捷性、准确性了吧. 在高等数学的学习中，要学会说理，更重要的是，要学会用简捷的数学语言去描述，做到“天衣无缝，滴水不漏”. 在下面的证明中，我们用日常用语与数学语言两种格式给出，让大家从日常用语的描述很快地转到数学语言的描述上来.

证　（日常用语）对于正整数集$\mathbb{N}^+$中的任一个子集 S，因为 S 不是空集，所以 S 中必定有一个数 m. 把 S 中不超过 m 的正整数汇集在一起构成一个集合并命名为 S_m，显然 S_m 是 S 的子集，而且集合 S_m 必定是一个有限集. 于是我们可以通过比较法获得集合 S_m 中的最小数 n_0. 比较法可行吗？我们说是可行的，是因为只有有限个数，所以才可行. 就如我们班的所有同学的身高构成一个数集 A，我们可以通过比较找出最矮者，最矮者的身高就是数集 A 中的最小数.

当找到 S_m 中的最小数 n_0 后，n_0 是不是 S 中的最小数呢？回答是肯定的. 因为 S 中的任一个数 n，要么在 S_m 中，要么不在 S_m 中. 如果在 S_m 中，则因为 n_0 是 S_m 中的最小数，所以 n 不会比 n_0 小. 如果不在 S_m 中，则 n 必定比 m 大，这是因为 S 中不超过 m 的数都在 S_m 中. 从而 S 中的所有数都不会比 n_0 小. 故正整数集的任意一个非空的子集必有最小数.

证　（数学语言）$\forall S\subset\mathbb{N}^+, S\neq\varnothing, \exists m\in S$. 于是数集

$$S_m = S\cap\{1,2,\cdots,m\}$$

是有限集，从而通过比较可获得 S_m 中的最小数 n_0. 所以 $\forall n \in S$.

$$\text{如果 } n \in S_m, \text{则 } n \geqslant n_0; \quad \text{如果 } n \notin S_m, \text{则 } n > m \geqslant n_0.$$

故结论成立.

对照两种描述，我们可以悟出，要理解数学语言的证明，必须把证明中字里行间的道理挖掘出来，才能说你看懂了. 看懂后，还要理清证明的过程，即思维方法. 如这个定理的证明过程是：先构造一个有限集，从而获得这个有限集的最小者 n_0，再论证有限集的最小者 n_0 就是我们要找的数.

我们可以把上面的方法称为“先读厚，再读薄”. 读厚的实质是挖掘字里行间的道理，读薄的实质是总结思维的过程.

以后的证明我们不再像这样赘述，完全靠大家去“悟”，并在悟中一步一步地走向成熟.

1.1.2 数学归纳法

定理 1.1.2（数学归纳法原理） 设 P 是一个有关正整数 n 的命题，如果：

(1) 当 $n=1$ 时，命题 P 成立；

(2) 假设 $n=k$ 时，命题 P 成立，能导出 $n=k+1$ 时，命题 P 也成立，则命题 P 对所有正整数都成立.

证 假设 $\exists k \in \mathbb{N}^+$，命题 P 对 k 不成立，则由已知条件知 $k \neq 1$，且命题 P 对 $k-1$ 也不成立. 继之推出命题 P 对 $k-2$ 也不成立.

由自然数公理知，数集 $\{1,2,\cdots,k\}$ 是有限集，所以我们可以一直推到 $k=1$ 时，命题 P 也不成立. 矛盾，故命题 P 对所有正整数都成立.

在定理 1.1.2 的证明中，我们用到了数理逻辑中“逆否命题”的结论，即

命题：P 对 n 成立$\Rightarrow P$ 对 n 的继元 $n+1$ 成立.

逆否命题：P 对 n 的继元 $n+1$ 不成立$\Rightarrow P$ 对 n 不成立.

结论：当一个命题为真时，其逆否命题亦为真.

在定理 1.1.2 中，“当 $n=1$ 时，命题 P 成立”称为归纳基础. 如果换为“当 $n=c$ 时，命题 P 成立”，则所得结论是

$$\forall n \geqslant c, \text{命题 } P \text{ 对 } n \text{ 都成立.}$$

例 1.1.1 证明：n 边形的内角和等于 $(n-2)\pi$.

证 当 $n=3$ 时，结论成立. 假设 $n=k$ 时，结论成立，则 $n=k+1$ 时，如图 1.1，连接 A_1A_3，于是 $k+1$ 边形的内角和等于 k 边形的内角和再加上 $\triangle A_1A_2A_3$ 的内角和，即

$$(k-2)\pi + \pi = [(k+1)-2]\pi.$$

故结论成立.

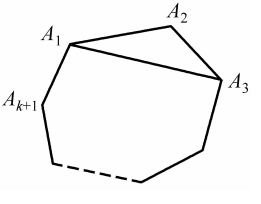

图 1.1

例 1.1.2 证明：含有 n 个元素的集合的所有子集的个数等于 2^n.

证　当 $n=1$ 时，集合 $\{a\}$ 的所有子集为 $\varnothing,\{a\}$，所以结论成立.

假设 $n=k$ 时，结论成立，即集合 $\{a_1,a_2,\cdots,a_k\}$ 的所有子集为

$$\varnothing,\{a_1\},\cdots,\{a_k\},\cdots,\{a_1,a_2,\cdots,a_k\},$$

共 2^k 个.

当 $n=k+1$ 时，集合 $\{a_1,a_2,\cdots,a_k,a_{k+1}\}$ 的所有子集除了上面的 2^k 个外，还有上面的集合中均增加 a_{k+1} 的集合

$$\{a_{k+1}\},\{a_1,a_{k+1}\},\cdots,\{a_k,a_{k+1}\},\cdots,\{a_1,a_2,\cdots,a_k,a_{k+1}\},$$

所以集合 $\{a_1,a_2,\cdots,a_k,a_{k+1}\}$ 的所有子集个数为 $2^k+2^k=2^{k+1}$. 故结论成立.

在某些情况下，仅用归纳假设“$n=k$ 时，命题 P 成立”还不够，而需要更强的假设，这就是下面的第二数学归纳法.

定理 1.1.3（**第二数学归纳法原理**）　设 P 是一个有关正整数 n 的命题，如果：

(1) 当 $n=1$ 时，命题 P 成立；

(2) 假设 $n\leqslant k$ 时，命题 P 成立，能导出 $n=k+1$ 时，命题 P 也成立，则命题 P 对所有正整数都成立.

证　假设 $\exists k\in\mathbb{N}^+$，命题 P 对 k 不成立，则 $k\neq 1$. 设

$$S=\{n:\ n\in\mathbb{N}^+,\text{命题 } P \text{ 对 } n \text{ 不成立}\},$$

则 $S\neq\varnothing$. 由最小数原理知

$$\exists h\in S,\quad \ni\text{“}\forall n\in S, n\geqslant h\text{”}.$$

于是 $n\leqslant h-1$ 时，命题 P 成立. 从而由(2)知命题 P 对 h 成立，此与 $h\in S$ 矛盾，故命题 P 对所有正整数都成立.

例 1.1.3　设 $a_1=1,a_2=5,a_3=2$，且 $a_{n+3}=2a_n+a_{n+1}-a_{n+2}$，证明：$\forall n\in\mathbb{N}^+,a_n\in\mathbb{Z}$.

证　当 $n=1,2,3$ 时结论成立. 假设 $n\leqslant k$ 时结论成立，即有

$$a_{k-2},a_{k-1},a_k\in\mathbb{Z},$$

则当 $n=k+1$ 时，$a_{k+1}=2a_{k-2}+a_{k-1}-a_k\in\mathbb{Z}$，故 $\forall n\in\mathbb{N}^+,a_n\in\mathbb{Z}$.

习题 1.1

1. 设 $x>-1$，证明：$\forall n\in\mathbb{N}^+,(1+x)^n\geqslant 1+nx$.

2. 证明：$\forall a_k\in\mathbb{R}^+(k=1,2,\cdots,n)$，

$$\sqrt[n]{a_1a_2\cdots a_n}\leqslant\frac{a_1+a_2+\cdots+a_n}{n}.$$

3. 证明二项式定理

$$(a+b)^n=\mathrm{C}_n^0a^n+\mathrm{C}_n^1a^{n-1}b+\cdots+\mathrm{C}_n^ka^{n-k}b^k+\cdots+\mathrm{C}_n^nb^n,$$

其中 $\mathrm{C}_n^k=\dfrac{n(n-1)\cdots(n-k+1)}{k!}$.

4. 证明斐波那契序列

$$a_1 = 1, a_2 = 2, a_n = a_{n-1} + a_{n-2} \quad (n \geqslant 3)$$

的通项公式为

$$a_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

1.2 数环与数域

1.2.1 数环与数域的概念

在讨论从实际问题中抽象出来的数学模型时，总要考虑这个数学模型与某个数集的联系. 例如多项式是一个数学模型，如果多项式的系数界定在某一个范围 F，对数集 F 的要求就必须知道. 由于多项式对和、差、积等运算后的结果仍是多项式，当然要求数集 F 就数的和、差、积等运算必须封闭，即和、差、积等运算的结果仍在 F 中. 在后面讨论的数学模型中，所涉及的数集还要求对除法运算封闭，这就得引入数环与数域的概念.

我们知道，在整数集$\mathbb{Z}$ 中，$\forall a, b \in \mathbb{Z}$，

$$a+b, a-b, ab \in \mathbb{Z},$$

即加、减、乘运算是封闭的. 而在$\mathbb{Z}$ 中，除法就没有封闭性了. 但在有理数集$\mathbb{Q}$ 中，$\forall a, b \in \mathbb{Q}$，

$$a+b, a-b, ab, \frac{a}{b}(b \neq 0) \in \mathbb{Q},$$

即四则运算封闭. 由此得到下面的定义.

定义 1.2.1 在复数集$\mathbb{C}$ 中，$S \subseteq \mathbb{C}$，$S \neq \varnothing$，如果

$$\forall a, b \in S, a+b, a-b, ab \in S,$$

则称 S 是一个**数环**.

由定义 1.2.1 知，整数集$\mathbb{Z}$，有理数集$\mathbb{Q}$，实数集$\mathbb{R}$ 以及复数集$\mathbb{C}$ 都是数环，而自然数集$\mathbb{N}$ 不是数环.

另外，所有偶数构成的集合亦是数环，特别地，由零元素构成的单点集$\{0\}$也是数环. 这不是因为我们想说它是数环，它就是数环了，而是因为我们用数环的定义得出的结论. 这告诉我们，在数学领域里，说话办事都必须做到有依有据，定义就是我们行动的指南.

例 1.2.1 设 $a \in \mathbb{Z}$，令 $S = \{x : x = na, n \in \mathbb{Z}\}$，则 S 是一个数环.

证 因为 $a \in S$，所以 $S \neq \varnothing$. 又 $\forall x_1, x_2 \in S$，$\exists n_1, n_2 \in \mathbb{Z}$，

$$\ni \text{“} x_1 = n_1 a, x_2 = n_2 a \text{”},$$

于是

$$x_1 \pm x_2 = (n_1 \pm n_2)a \in S, \quad x_1 x_2 = (n_1 n_2 a)a \in S,$$

这里 $n_1 n_2 a \in \mathbb{Z}$，故 S 是一个数环.

定义 1.2.2 设 $F \subseteq \mathbb{C}$，如果 $0, 1 \in F$，且

$$\forall a,b\in F,\quad a+b,a-b,ab,\frac{a}{b}(b\neq 0)\in F,$$

则称 F 是一个**数域**.

例 1.2.2　设 $F=\{x:\ x=a+b\sqrt{2},a,b\in\mathbb{Q}\}$,则 F 是一个数域.

证　显然取 $a=b=0$ 知 $0\in F$,取 $a=1,b=0$ 知 $1\in F$,又 $\forall x,y\in F$,$\exists a,b,c,d\in\mathbb{Q}$,

$$\ni\text{“}x=a+b\sqrt{2},y=c+d\sqrt{2}\text{”},$$

于是

$$x\pm y=(a\pm c)+(b\pm d)\sqrt{2}\in S,\quad xy=(ac+2bd)+(ad+bc)\sqrt{2}\in S.$$

而当 $c+d\sqrt{2}\neq 0$ 时,如果 $d=0$,则 $c\neq 0$,即 $c-d\sqrt{2}\neq 0$;如果 $d\neq 0$,因为 $c\in\mathbb{Q}$,所以 $c-d\sqrt{2}\neq 0$. 于是

$$\frac{x}{y}=\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}=\frac{ac-2bd}{c^2-2d^2}+\frac{bc-ad}{c^2-2d^2}\sqrt{2},$$

因为

$$\frac{ac-2bd}{c^2-2d^2},\frac{bc-ad}{c^2-2d^2}\in\mathbb{Q},$$

所以 $\dfrac{x}{y}\in F$,故 F 是一个数域.

上面两个例子的证明告诉我们,证明的过程就是诉说条件到结论的过程,其中推导的依据是定义. 在生活中,我们常说:“按章办事”,在数学领域里,那就是“用定义说话”.

数域有如下重要性质.

定理 1.2.1　任何数域都包含有理数域.

证　设 F 是一个数域,则 $0,1\in F$,用数 1 与自身相加而得自然数集 $\mathbb{N}$,所以由加法的封闭性知 $\mathbb{N}\subseteq F$;又由减法的封闭性而得整数集 $\mathbb{Z}$,所以 $\mathbb{Z}\subseteq F$;再由除法的封闭性而得有理数集 $\mathbb{Q}$,所以 $\mathbb{Q}\subseteq F$. 故结论成立.

定理 1.2.1 指出,有理数域 $\mathbb{Q}$ 是最小的数域.

上面两个结论的关系是:

任何数域都包含有理数域⇒有理数域 $\mathbb{Q}$ 是最小的数域.

你能悟出其中的道理来吗? 这可是学习数学的基本要求呀. 有人对这样的问题是停留在“只可意会,不可言传”的阶段,这是不可取的. 要想获得这一推导的理由,只需用数学的反证法即可. 假设有理数域 $\mathbb{Q}$ 不是最小的数域,则必有比 $\mathbb{Q}$ 小的数域 P,看看“任何数域都包含有理数域”,不就得到 $P\supset\mathbb{Q}$ 吗,矛盾出来后,就得到推理是正确的.

总结定理 1.2.1 的证明,还可得到下面的结论.

自然数集是二元集 $\{0,1\}$ 赋予加法运算后,接纳运算结果而扩充得到的数集.

想来,你应该能悟出其中的道理来吧.

1.2.2 整数环的一些整除性质

为了学习多项式,有一个简单的类比对象,那就是整数集在通常运算下所构成的环——整数环.我们在这里给大家介绍整数环的一些整除性质.

定义 1.2.3 设 $a,b\in\mathbb{Z}$,如果能找到一个整数 d,使得 $b=ad$,则称 a 整除 b(或称 b 被 a 整除),记作 $a|b$.这时称 a 是 b 的**因数**,b 是 a **倍数**,否则称 a 不能整除 b,记作 $a\nmid b$.

ie: $a|b\Leftrightarrow\exists d\in\mathbb{Z}$,$\ni$"$b=ad$". $a\nmid b\Leftrightarrow\forall d\in\mathbb{Z}$,$b\neq ad$.

定理 1.2.2 整除有如下基本性质.

(1) 如果 $a|b,b|c$,则 $a|c$;

(2) 如果 $a|b,a|c$,则 $a|(b+c)$;

(3) 如果 $a|b$,则 $\forall c\in\mathbb{Z}$,$a|bc$;

(4) 如果 $a|b,b|a$,则 $a=\pm b$.

证 (1) 因为 $a|b$,所以 $\exists d\in\mathbb{Z}$,$\ni$"$b=ad$".同理由 $b|c$ 得

$$\exists e\in\mathbb{Z},\quad \ni\text{“}c=be\text{”}.$$

从而 $c=be=ade=a(de)$,故 $a|c$.

同理可证(2)、(3)、(4).

推论 如果 $\forall i\in\{1,2,\cdots,k\}$,$a|b_i$,则 $\forall\lambda_i\in\mathbb{Z}$,$a|(\lambda_1b_1+\lambda_2b_2+\cdots+\lambda_kb_k)$.

定理 1.2.3(带余除法) 设 $a,b\in\mathbb{Z}$,$a\neq0$,则

$$\exists|q,r\in\mathbb{Z},\quad \ni\text{“}b=aq+r\text{ 且 }0\leqslant r<|a|\text{”}.$$

证 令 $S=\{x:x=b-an\geqslant0,n\in\mathbb{Z}\}$,则 $S\subseteq\mathbb{N}$ 且 $S\neq\varnothing$.于是由最小数原理知

$$\exists q\in\mathbb{Z},\quad \ni\text{“}r=b-aq=\min S\text{”}.$$

从而 $b=aq+r$,且由最小性知 $0\leqslant r<|a|$.

假设还 $\exists q',r'\in\mathbb{Z}$,$\ni$"$b=aq'+r'$且 $0\leqslant r'<|a|$",则

$$a(q-q')+(r-r')=0.$$

如果 $q-q'\neq0$,则 $|r-r'|\geqslant a$,此与 $0\leqslant r<|a|$,$0\leqslant r'<|a|$ 矛盾,故 $q=q'$,$r=r'$,所以唯一性得证.

在带余除法中,q,r 分别称为**商**与**余数**,且

$$a\mid b\Leftrightarrow r=0.$$

定义 1.2.4 设 $a,b\in\mathbb{Z}$,$d\in\mathbb{Z}^+$,a,b 不全为零,如果:

(1) d 是 a,b 的公因数,即 $d|a$ 且 $d|b$;

(2) a,b 的所有公因数都是 d 的因数,即

$$c\mid a\text{ 且 }c\mid b,\quad \text{则 }c\mid d,$$

那么称 d 是 a,b 的**最大公因数**,记作 $d=(a,b)$.

$$\text{ie: } d=(a,b)\Leftrightarrow\begin{cases}(1)\ d|a,d|b,\\(2)\ \forall c,c|a,c|b\Rightarrow c|d.\end{cases}$$

在这里，你能悟出“最大”的数学描述吗？当你不清楚时，回头看看我们对“最小”的解释. 千万不要停留在“只可意会，不可言传”的阶段.

一般地，

$$d=(a_1,a_2,\cdots,a_n)\Leftrightarrow\begin{cases}(1)\ \forall k\in\{1,2,\cdots,n\},d\mid a_k,\\(2)\ \forall k\in\{1,2,\cdots,n\},c\mid a_k\Rightarrow c\mid d.\end{cases}$$

显然，$\forall a\in\mathbb{Z}$，$(a,0)=|a|$.

定理 1.2.4　任意 $n(n\geqslant 2)$ 个不全为零的整数 $a_1,a_2,\cdots,a_n$，必存在唯一的最大公因数.

证　令 $S=\{x:x=\lambda_1a_1+\lambda_2a_2+\cdots+\lambda_na_n>0,\lambda_1,\lambda_2,\cdots,\lambda_n\in\mathbb{Z}\}$，则

$$S\subseteq\mathbb{N}^+\quad 且\quad S\neq\varnothing.$$

于是由最小数原理知

$$\exists d\in\mathbb{Z}^+,\quad \ni“d=\min S”.$$

$\forall k\in\{1,2,\cdots,n\}$，由带余除法得

$$a_k=dq_k+r_k,\quad 0\leqslant r_k<d.$$

如果 $r_k>0$，因为 $d\in S$，所以 $r_k=a_k-dq_k\in S$，此与 $d=\min S$ 矛盾，故

$$\forall k\in\{1,2,\cdots,n\},\quad r_k=0,\quad 即\quad \forall k\in\{1,2,\cdots,n\},\quad d\mid a_k.$$

又 $\forall c\in\mathbb{Z}^+$，$\forall k\in\{1,2,\cdots,n\}$，$c\mid a_k$，则 $\forall s\in S$，$c\mid s$，所以 $c\mid d$，故 $d=(a_1,a_2,\cdots,a_n)$.

如果 $d'=(a_1,a_2,\cdots,a_n)$，则 $d\mid d'$，且 $d'\mid d$，即 $d'=d$. 故结论成立.

推论　如果 $d=(a_1,a_2,\cdots,a_n)$，则 $\exists\lambda_1,\lambda_2,\cdots,\lambda_n\in\mathbb{Z}$，

$$\ni“d=\lambda_1a_1+\lambda_2a_2+\cdots+\lambda_na_n”.$$

证　因为 $d=\min S$，所以 $d\in S$，故结论成立.

定义 1.2.5　如果 $(a_1,a_2,\cdots,a_n)=1$，则称 $a_1,a_2,\cdots,a_n$ 互素.

定理 1.2.5　$(a_1,a_2,\cdots,a_n)=1\Leftrightarrow\exists\lambda_1,\lambda_2,\cdots,\lambda_n\in\mathbb{Z}$，$\ni“\lambda_1a_1+\lambda_2a_2+\cdots+\lambda_na_n=1”$.

证　($\Rightarrow$)由定理 1.2.4 的推论知结论成立.

($\Leftarrow$)设 $\exists\lambda_1,\lambda_2,\cdots,\lambda_n\in\mathbb{Z}$，$\ni“\lambda_1a_1+\lambda_2a_2+\cdots+\lambda_na_n=1”$，令 $d=(a_1,a_2,\cdots,a_n)$，则 $d\mid 1$，所以 $d=1$. 故结论成立.

最后给出素数的一些简单性质.

定义 1.2.6　如果大于 1 的整数 p 只有 $\pm1,\pm p$ 为其因数，则称 p 为素数.

性质 1　如果 p 为素数，则 $\forall a\in\mathbb{Z}$，$(a,p)=1$ 或 $(a,p)=p$.

证　如果 $p\mid a$，则 $(a,p)=p$；如果 $p\nmid a$，则 $(a,p)=1$，故结论成立.

性质 2　如果 p 为素数，$p\mid ab$，则 $p\mid a$ 或 $p\mid b$.

证　如果 $p\mid a$，则结论成立. 如果 $p\nmid a$，则 $(a,p)=1$，于是 $\exists s,t\in\mathbb{Z}$，$\ni“sa+tp=1”$. 从而

$$sab+tpb=b.$$

因为 $p\mid ab$，所以 $p\mid(sab+tpb)$，即 $p\mid b$. 故结论成立.

1.2.3 群、环与域

当我们讨论的对象是一般集合 G 时，在 G 上赋予运算后就成了一个代数系统. 根据运算的属性就获得此代数系统的名称.

定义 1.2.7 设 G 是一个非空集合，$\forall a,b\in G$，按某种规定，G 中有唯一元素 c 与有序元素对 (a,b) 对应，则称此对应为 G 中的**二元运算**，记作 $*$.

ie：$a*b=c$.

定义 1.2.8 如果 G 中的二元运算 $*$ 满足：

(1) 封闭性：$\forall a,b\in G, a*b\in G$；

(2) 结合律：$\forall a,b,c\in G,(a*b)*c=a*(b*c)$；

(3) 恒元：$\exists e\in G,\ni$“$\forall a\in G, e*a=a$”；

(4) 逆元：$\forall a\in G,\exists b\in G,\ni$“$a*b=e$”，

则称 G 为一个**群**，记作 $(G,*)$ 或 G. 其中 e 称为 G 对运算 $*$ 的**单位元**或**恒元**，b 称为 a 的**逆元**，记作 a^{-1}.

如果二元运算 $*$ 满足封闭性与结合律，则称 $(G,*)$ 为**半群**.

ie：含有单位元与逆元的半群称为群.

如果群 $(G,*)$ 还具有交换律，即

$$\forall a,b\in G,\quad a*b=b*a,$$

则称 $(G,*)$ 为**交换群**或**阿贝尔(Abel)群**.

群的运算记为 $+$ 时称为加法运算. 此时恒元记为 0，并称为零元；a 的逆元记为 $-a$，并称为负元. 有了负元后，就可以获得群中的减法运算.

定义 1.2.9 在群 $(G,+)$ 中，定义减法“$-$”为

$$\forall a,b\in G,\quad a-b=a+(-b).$$

并称减法运算为加法运算的逆运算.

群的运算记为 $\cdot$ 时称为乘法运算. 恒元称为单位元，a 的逆元记为 a^{-1}，并获得群中的除法运算.

定义 1.2.10 在群 $(G,\cdot)$ 中，定义除法“$\div$”为

$$\forall a,b\in G,\quad a\div b=a\cdot b^{-1}.$$

并称除法运算为乘法运算的逆运算.

ie：群就是具有一个运算与其逆运算的集合.

定义 1.2.11 如果集合 E 中有两个二元运算，记作 $+$ 和 $\cdot$，分别称为加法运算与乘法运算，且满足：

(1) $(E,+)$ 是交换群；

(2) $(E,\cdot)$ 是半群；

(3) 分配律：$\forall a,b,c\in E$，

$$a\cdot(b+c)=a\cdot b+a\cdot c,\quad (b+c)\cdot a=b\cdot a+c\cdot a,$$

则称 E 是一个**环**，记作$(E,+,\cdot)$或 E.

ie：环就是具有加、减、乘运算并满足分配律的集合.

定义 1.2.12　如果集合 F 中有两个二元运算＋和 $\cdot$，且满足：

(1) $(F,+)$是交换群；

(2) $(F\backslash\{0\},\cdot)$是交换群；

(3) 分配律：$\forall a,b,c\in F$，

$$a\cdot(b+c)=a\cdot b+a\cdot c,\quad (b+c)\cdot a=b\cdot a+c\cdot a,$$

则称集合 F 是一个**域**.

ie：域就是具有加、减、乘、除运算并满足分配律的集合.

习题 1.2

1. 证明：两个数环的交还是一个数环，两个数域的交还是一个数域，问两个数环的并是不是数环？

2. 证明 $S=\left\{x:\ x=\dfrac{n}{2^m},m,n\in\mathbb{Z}\right\}$是一个数环，问 S 是不是一个数域？

3. 指定 $a,b\in\mathbb{Z}$，记

$$aZ+bZ=\{x:\ x=ma+nb,m,n\in\mathbb{Z}\},$$
$$aZ=\{x:\ x=ma,m\in\mathbb{Z}\},$$

证明：

(1) $aZ+bZ$ 是一个数环；　　(2) $aZ\subseteq bZ\Leftrightarrow a\mid b$；

(3) $aZ+bZ=dZ$，其中 $d=(a,b)$；　　(4) $aZ+bZ=\mathbb{Z}\Leftrightarrow(a,b)=1$.

第/2/章

多 项 式

在中学已经学习过多项式.在这里,我们将系统地研究它.值得注意的是,中学的学习重在计算,而这里的学习重在“说理”.当然,由计算转为说理有一定的难度,但我们只要掌握说理的方法就不会感到困难.方法是:说理的每一个过程都必须做到“有依有据”,这些依据不是我们想象中的“准则”,而是源于定义以及已经证明了的性质、定理.可以说,学会说理,是这一章的重点和难点,也是我们学习后面章节的基础.

2.1 一元多项式及其运算

2.1.1 一元多项式的概念

定义 2.1.1 设 E 是一个数环,x 是一个文字,表达式

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

称为数环 E 上的一元多项式,其中

$$n \in \mathbb{N}, \quad a_k \in E, \quad k \in \{0,1,2,\cdots,n\}.$$

$a_k x^k$ 称为第 k 项,a_k 称为第 k 项的系数,a_0 称为常数项.

我们规定,在多项式中,可以任意添加或去掉系数为零的有限项;除常数项外,系数为 1 时,可以不写系数.

一元多项式常用 $f(x)$,$g(x)$ 等表示.因为一元多项式由其系数唯一确定,所以也可以用 $n+1$ 元有序数组

$$(a_n, a_{n-1}, \cdots, a_1, a_0)$$

表示.这种表示是由多项式到有序数组的抽象结果,也可以说有序数组的一个背景是多项式.

定义 2.1.2 在多项式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

中,如果系数全为零,则称多项式 $f(x)$ 为**零多项式**,记作 0;如果 $a_n \neq 0$,则称 $a_n x^n$ 为最高次数项,自然数 n 称为多项式 $f(x)$ 的**次数**,记作 $\partial^0(f(x))$ 或 $\partial^0(f)$.

零多项式没有次数(有的书出于某种需要,称零多项式的次数为无穷次),零次多项式是一个非零常数.以后谈到多项式 $f(x)$ 的次数时,总假定 $f(x) \neq 0$.

多项式的表达式亦可按升次幂排列，即

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n.$$

例如 $f(x)=\frac{1}{2}x^7+3x-2$ 是数域$\mathbb{Q}$ 上的多项式，而 $g(x)=\sqrt{3}x^2+1.3x-5$ 是数域$\mathbb{R}$ 上的多项式.

值得注意的是，可把 $f(x)$视为数域$\mathbb{R}$ 上的多项式，而不能把 $g(x)$视为数域$\mathbb{Q}$ 上的多项式.

又如有理数域$\mathbb{Q}$ 上的多项式 $f(x)$的每一项同时乘以某个整数后都能变为整系数多项式，即整数环上的多项式，但不能说 $f(x)$是整数环上的多项式.

有时候，我们会把多项式

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

表示为

$$f(x) = \sum_{k=0}^{n} a_kx^k.$$

值得注意的是，任一非零多项式必有次数. 而

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$$

不是多项式.

数环 E 上的所有多项式构成的集合记作 $E[x]$. 在 $E[x]$中，有任意次数的多项式，但不存在最高次数的多项式. 这种性质称为**有限性**. 并请注意它与有界性的区别，这是以后学习实变函数中“有限性”的一个简单实例.

2.1.2　一元多项式的运算

要给出多项式的运算，必须先给出两个多项式相等的概念.

定义 2.1.3　设 $f(x),g(x)\in E[x]$，如果 $f(x),g(x)$的同次项系数相等，则称 $f(x)$与 $g(x)$相等，记作 $f(x)=g(x)$.

ie：$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$，$g(x)=b_0+b_1x+b_2x^2+\cdots+b_mx^m$，

则 $f(x)=g(x)\Leftrightarrow m=n$ 且 $\forall k\in\{0,1,2,\cdots,n\}$，$a_k=b_k$，即

$$(a_0,a_1,a_2,\cdots,a_n) = (b_0,b_1,b_2,\cdots,b_n).$$

定义 2.1.4　设 $f(x),g(x)\in E[x]$，

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, \quad m \leqslant n,$$

多项式 $f(x)$与 $g(x)$的和 $f(x)+g(x)$是指多项式

$$(a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n,$$

其中，当 $m<n$ 时，$b_{m+1}=b_{m+2}=\cdots=b_n=0$.

ie：$f(x)=(a_0,a_1,a_2,\cdots,a_n)$，$g(x)=(b_0,b_1,b_2,\cdots,b_m)$，则

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

或

$$(a_0,a_1,\cdots,a_n)+(b_0,b_1,\cdots,b_n)=(a_0+b_0,a_1+b_1,\cdots,a_m+b_m,a_{m+1}+0,\cdots,a_n+0).$$

数 $\lambda\in E$ 与多项式 $f(x)$ 的**数乘** $\lambda f(x)$ 是指多项式

$$\lambda a_0+\lambda a_1x+\lambda a_2x^2+\cdots+\lambda a_nx^n.$$

ie: $\lambda f(x)=\lambda a_0+\lambda a_1x+\lambda a_2x^2+\cdots+\lambda a_nx^n$,

或

$$\lambda(a_0,a_1,a_2,\cdots,a_n)=(\lambda a_0,\lambda a_1,\lambda a_2,\cdots,\lambda a_n).$$

多项式的和与数乘具有下列运算律:

$$\forall f(x),g(x),h(x)\in E[x],\quad \forall\lambda,\mu\in E.$$

(1) 加法的交换律: $f(x)+g(x)=g(x)+f(x)$;

(2) 加法的结合律: $(f(x)+g(x))+h(x)=g(x)+(f(x)+h(x))$;

(3) 加法中的零元: $0+f(x)=f(x)$;

(4) 加法中的负元: $\forall f(x)\in E[x],\exists|\, g(x)\in E[x],\ni$ "$f(x)+g(x)=0$",
其中 $g(x)$ 称为 $f(x)$ 的负元. $f(x)$ 的负元记作 $-f(x)$;

(5) 数乘对加法的分配律: $\lambda(f(x)+g(x))=\lambda f(x)+\lambda g(x)$;

(6) 数乘对数加的分配律: $(\lambda+\mu)f(x)=\lambda f(x)+\mu f(x)$;

(7) 数乘结合律: $(\lambda\mu)f(x)=\lambda(\mu f(x))$;

(8) 数乘单位元: $1f(x)=f(x)$.

由于我们都熟悉这些运算律,所以不再给出它们的验证.

有了负元后,就可以定义多项式的减法运算,即

定义 2.1.5 减去一个多项式等于加上这个多项式的负元.

ie: $f(x)-g(x)=f(x)+(-g(x))$.

定义 2.1.6 设 $f(x),g(x)\in E[x]$,

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n,\quad g(x)=b_0+b_1x+b_2x^2+\cdots+b_mx^m,$$

多项式 $f(x)$ 与 $g(x)$ 的**积** $f(x)g(x)$ 是指多项式

$$c_0+c_1x+c_2x^2+\cdots+c_{m+n}x^{m+n},$$

其中

$$c_k=a_0b_k+a_1b_{k-1}+\cdots+a_{k-1}b_1+a_kb_0,\quad k=0,1,\cdots,m+n,$$

且

$$a_{n+1}=a_{n+2}=\cdots=a_{n+m}=0,\quad b_{m+1}=b_{m+2}=\cdots=b_{m+n}=0.$$

ie: $f(x)=(a_0,a_1,a_2,\cdots,a_n)$, $g(x)=(b_0,b_1,b_2,\cdots,b_m)$, 则

$$f(x)g(x)=\Big(\sum_{i+j=0}a_ib_j,\sum_{i+j=1}a_ib_j,\cdots,\sum_{i+j=k}a_ib_j,\cdots,\sum_{i+j=m+n}a_ib_j\Big).$$

其中

$$\sum_{i+j=0} a_i b_j = a_0 b_0, \sum_{i+j=1} a_i b_j = a_0 b_1 + a_1 b_0, \cdots, \sum_{i+j=m+n} a_i b_i = a_n b_m.$$

对于上面的数学式,可以用竖式运算来理解,即

$$\begin{array}{llllll}
 & a_0 & a_1 & a_2 & \cdots & a_n \\
 & \times\, b_0 & b_1 & b_2 & \cdots & b_m \\
\hline
 & a_0 b_0 & a_1 b_0 & a_2 b_0 & \cdots & a_n b_0 \\
\sum\limits_{i+j=0} a_i b_j & a_0 b_1 & a_1 b_1 & \cdots & a_{n-1} b_1 & a_n b_1 \\
\sum\limits_{i+j=1} a_i b_j & a_0 b_2 & \cdots & a_{n-2} b_2 & a_{n-1} b_2 & a_n b_2 \\
\sum\limits_{i+j=2} a_i b_j & \vdots & & \vdots & \vdots & \vdots \\
 & a_0 b_m & \cdots & a_{n-2} b_m & a_{n-1} b_m & a_n b_m
\end{array} \quad \sum_{i+j=m+n} a_i b_j$$

即

$$f(x) = \sum_{k=0}^{n} a_k x^k, \quad g(x) = \sum_{k=0}^{m} b_k x^k,$$

则

$$f(x)g(x) = \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i b_j \Big) x^k.$$

多项式的乘法具有下列运算律:

$$\forall f(x), g(x), h(x) \in E[x].$$

(1) 交换律: $f(x)g(x)=g(x)f(x)$;

(2) 结合律: $(f(x)g(x))h(x)=g(x)(f(x)h(x))$;

(3) 分配律: $f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$;

(4) 消去律: 若 $f(x)g(x)=f(x)h(x)$,且 $f(x)\neq 0$,则 $g(x)=h(x)$.

下面给出结合律的证明.

证　设

$$f(x) = \sum_{k=0}^{m} a_k x^k, \quad g(x) = \sum_{k=0}^{n} b_k x^k, \quad h(x) = \sum_{k=0}^{r} c_k x^k.$$

再设

$$f(x)g(x) = \sum_{k=0}^{m+n} d_k x^k, \quad g(x)h(x) = \sum_{k=0}^{m+r} e_k x^k,$$

其中

$$d_i = \sum_{s+t=i} a_s b_t, \quad i \in \{0,1,2,\cdots,m+n\},$$

$$e_j = \sum_{t+u=j} b_t c_u, \quad j \in \{0,1,2,\cdots,n+r\}.$$

于是$[f(x)g(x)]h(x)$的第$k\in\{0,1,2,\cdots,m+n+r\}$次项的系数为

$$\sum_{i+u=k}d_ic_u=\sum_{i+u=k}\Big(\sum_{s+t=i}a_sb_t\Big)c_u=\sum_{s+t+u=k}a_sb_tc_u,$$

$f(x)[g(x)h(x)]$的第$k\in\{0,1,2,\cdots,m+n+r\}$次项的系数为

$$\sum_{s+j=k}a_se_j=\sum_{s+j=k}a_s\Big(\sum_{t+u=j}b_tc_u\Big)=\sum_{s+t+u=k}a_sb_tc_u,$$

所以$[f(x)g(x)]h(x)$与$f(x)[g(x)h(x)]$的同次项系数相等,故结论成立.

关于多项式在加法与乘法运算中的次数有下面的定理.

定理 2.1.1 $\forall f(x),g(x)\in E[x],f(x)\neq0,g(x)\neq0$,则:

(1) 当$f(x)+g(x)\neq0$时,$\partial^0(f(x)+g(x))\leqslant\max\{\partial^0(f(x)),\partial^0(g(x))\}$;

(2) $\partial^0(f(x)g(x))=\partial^0(f(x))+\partial^0(g(x))$.

证 由定义即知结论成立.

最后指出,在$E[x]$上,我们赋予了加、减、乘运算,且皆封闭,所以$E[x]$构成了一个环,故称$E[x]$为**一元多项式环**.另外,如果我们界定多项式的系数属于某数域F,则记为$F[x]$,并称为数域F上的多项式环.例如:

$Q[x]$——有理数域$\mathbb{Q}$上的多项式环;

$R[x]$——实数域$\mathbb{R}$上的多项式环;

$C[x]$——复数域$\mathbb{C}$上的多项式环.

习题 2.1

1. 设$f(x),g(x),h(x)\in R[x]$,证明:若

$$f^2(x)=xg^2(x)+xh^2(x),\quad \text{则}\quad f(x)=g(x)=h(x)=0.$$

2. 在$C[x]$中寻求一组多项式$f(x),g(x),h(x)$,满足

$$f^2(x)=xg^2(x)+xh^2(x).$$

3. 设$\partial^0(f_1(x))\leqslant\partial^0(g_1(x)),\partial^0(f_2(x))\leqslant\partial^0(g_2(x))$.证明:

$$\partial^0(f_1(x)f_2(x))\leqslant\partial^0(g_1(x)g_2(x)).$$

问是否一定有$\partial^0(f_1(x)+f_2(x))\leqslant\partial^0(g_1(x)+g_2(x))$?举例说明.

4. 设$f(x),g(x)$是两个非零多项式,且$f(x)+g(x)\neq0$,问$f(x),g(x)$满足什么条件时,$\partial^0(f_1(x)+f_2(x))=\max\{\partial^0(g_1(x)),\partial^0(g_2(x))\}$?

2.2 多项式的整除性

2.2.1 整除的概念与性质

由于在一元多项式环中,除法不是皆可施行的,因此要研究多项式的整除性.由于封闭性的要求,我们在这里讨论的对象是数域上的多项式.

定义 2.2.1　设 F 为一数域，$f(x),g(x)\in F[x]$，如果在 $F[x]$ 中能找到一个多项式 $h(x)$ 满足

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

则称 $f(x)$**整除** $g(x)$，记作 $f(x)\mid g(x)$. 并称 $f(x)$ 是 $g(x)$ 的一个**因式**，$g(x)$ 是 $f(x)$ 的一个**倍式**. 记法 $f(x)\nmid g(x)$ 表示 $f(x)$**不能整除** $g(x)$.

ie：$f(x)\mid g(x)\Leftrightarrow \exists h(x)\in F[x],\ni "g(x)=f(x)h(x)"$；

$f(x)\nmid g(x)\Leftrightarrow \forall h(x)\in F[x],g(x)\neq f(x)h(x)$.

例 2.2.1　因为 $x^3-1=(x-1)(x^2+x+1)$，所以

$$(x-1)\mid (x^3-1),\quad (x^2+x+1)\mid (x^3-1).$$

又因为 $x^n-1=(x-1)(x^{n-1}+\cdots+x+1)$，所以 $x-1$ 是 x^n-1 的因式.

同理，$x^{n-1}+\cdots+x+1$ 也是 x^n-1 的因式.

多项式关于整除具有下面的性质.

性质 1　如果 $f(x)\mid g(x),g(x)\mid h(x)$，则 $f(x)\mid h(x)$.

证　因为 $f(x)\mid g(x),g(x)\mid h(x)$，所以 $\exists u(x),v(x)\in F[x]$，

$$\ni "g(x)=f(x)u(x),h(x)=g(x)v(x)".$$

从而 $h(x)=f(x)(u(x)v(x))$. 故 $f(x)\mid h(x)$.

性质 2　如果 $h(x)\mid f(x),h(x)\mid g(x)$，则 $h(x)\mid (f(x)\pm g(x))$.

证　因为 $h(x)\mid f(x),h(x)\mid g(x)$，所以 $\exists u(x),v(x)\in F[x]$，

$$\ni "f(x)=h(x)u(x),g(x)=h(x)v(x)".$$

从而 $f(x)\pm g(x)=h(x)(u(x)\pm v(x))$. 故 $h(x)\mid (f(x)\pm g(x))$.

性质 3　如果 $f(x)\mid g(x)$，则 $\forall h(x)\in F[x],f(x)\mid g(x)h(x)$.

证　因为 $f(x)\mid g(x)$，所以 $\exists u(x)\in F[x]$，

$$\ni "g(x)=u(x)f(x)".$$

从而 $g(x)h(x)=f(x)(u(x)h(x))$. 故 $f(x)\mid g(x)h(x)$.

性质 4　如果 $\forall k\in\{1,2,\cdots,n\},h(x)\mid f_k(x)$，则 $\forall g_k(x)\in F[x]$，

$$h(x)\mid (f_1(x)g_1(x)\pm f_2(x)g_2(x)\pm\cdots\pm f_n(x)g_n(x)).$$

证　由性质 2 与性质 3 即知上式成立.

除了上面的性质外，我们还有下面的结论.

(1) 任一多项式都能整除其自身.

实因：$\forall f(x)\in F[x],f(x)=1f(x)$.

(2) 零多项式是任意多项式的倍式，零多项式的倍式只有零多项式.

实因：$\forall f(x)\in F[x],0=0f(x)$.

(3) 零次多项式是任意多项式的因式，而零次多项式的因式只有零次多项式.

实因：$\forall f(x)\in F[x],\lambda\neq 0$，则 $f(x)=\lambda(\lambda^{-1}f(x))$.

(4) 相互整除的两个多项式只相差一个零次因式.

实因：由 $f(x)=g(x)u(x)$，$g(x)=f(x)v(x)$ 得 $f(x)=f(x)u(x)v(x)$，于是 $u(x)v(x)=1$. 所以 $u(x)=c$，$v(x)=c^{-1}$.

(5) 数域扩大不改变多项式的整除性.

ie：$F\subseteq\overline{F}$，在 $F[x]$ 里，$f(x)\nmid g(x)$，则在 $\overline{F}[x]$ 里，亦有 $f(x)\nmid g(x)$.

实因：假设在 $\overline{F}[x]$ 里，$f(x)\mid g(x)$，则 $\exists u(x)\in\overline{F}[x]$，

$$\ni\text{“}g(x)=f(x)u(x)\text{”},$$

所以 $u(x)$ 的系数是由 $f(x)$，$g(x)$ 的系数经四则运算而确定. 又

$$f(x),g(x)\in F[x],$$

于是 $u(x)\in F[x]$，即在 $F[x]$ 里 $f(x)\mid g(x)$，此与在 $F[x]$ 里 $f(x)\nmid g(x)$ 矛盾，故结论成立.

2.2.2 带余除法

在整数的整除性理论中有带余除法，在一元多项式环中，同样有带余除法. 于是两个带余除法可对照理解.

定理 2.2.1（**带余除法**） $\forall f(x),g(x)\in F[x],g(x)\neq 0$，则

$$\exists!q(x),r(x)\in F[x],\quad \ni\text{“}f(x)=g(x)q(x)+r(x)\text{”},$$

其中 $r(x)=0$ 或 $\partial^0(r(x))<\partial^0(g(x))$.

证 （存在性）设 $S[x]=\{p(x):p(x)=f(x)-g(x)u(x),u(x)\in F[x]\}$，则 $S[x]\subseteq F[x]$.

如果 $0\in S[x]$，则

$$\exists q(x)\in F[x],\quad \ni\text{“}0=f(x)-g(x)q(x)\text{”},$$

于是 $f(x)=g(x)q(x)$，此时取 $r(x)=0$ 即知结论成立.

如果 $0\notin S[x]$，则取 $r(x)$ 为 $S[x]$ 中次数最小的多项式，于是

$$\exists q(x)\in F[x],\quad \ni\text{“}r(x)=f(x)-g(x)q(x)\text{”},$$

于是 $f(x)=g(x)q(x)+r(x)$. 从而只需证明 $\partial^0(r(x))<\partial^0(g(x))$ 即可.

假设 $\partial^0(r(x))\geqslant\partial^0(g(x))$，则

$$\exists u(x)\in F[x],\quad \ni\text{“}\partial^0(r(x)-g(x)u(x))<\partial^0(r(x))\text{”}.$$

设 $r'(x)=r(x)-g(x)u(x)$，则

$$r'(x)=f(x)-g(x)(q(x)+u(x)),$$

即 $r'(x)\in S[x]$，此与 $r(x)$ 为 $S[x]$ 中次数最小的多项式矛盾，故 $\partial^0(r(x))<\partial^0(g(x))$.

（唯一性）假设还 $\exists\overline{q}(x),\overline{r}(x)\in F[x]$，

$$\ni\text{“}f(x)=g(x)\overline{q}(x)+\overline{r}(x)\text{”},$$

其中 $\overline{r}(x)=0$ 或 $\partial^0(\overline{r}(x))<\partial^0(g(x))$，则

$$g(x)(q(x)-\overline{q}(x))=r(x)-\overline{r}(x).$$

如果 $q(x)-\overline{q}(x)\neq 0$，则 $\partial^0(g(x))\leqslant\partial^0(r(x)-r'(x))$，此与

$$\partial^0(r(x))<\partial^0(g(x)),\partial^0(\overline{r}(x))<\partial^0(g(x))$$

矛盾，故

$$q(x)=\overline{q}(x),\quad r(x)=\overline{r}(x).$$

在带余除法中，多项式 $q(x)$与 $r(x)$分别称为 $g(x)$除 $f(x)$的商式与余式.

在带余除法的证明中，没有给出求商式与余式的方法. 对于求商式与余式，得用初等代数中的长除法，这里复习一下.

例 2.2.2　设 $f(x)=2x^4+4x^2-5x+6$，$g(x)=x^2-3x+1$，求 $g(x)$除 $f(x)$的商式与余式.

解

$$\begin{array}{r|l}
2x^4+4x^2-5x+6 & x^2-3x+1 \\
\cline{2-2}
2x^4-6x^3+2x^2 & 2x^2+6x+20 \\
\cline{1-1}
6x^3+2x^2-5x+6 & \\
6x^3-18x^2+6x & \\
\cline{1-1}
20x^2-11x+6 & \\
20x^2-60x+20 & \\
\cline{1-1}
49x-14 &
\end{array}$$

由长除法得 $g(x)$除 $f(x)$的商式 $q(x)=2x^2+6x+20$，余式 $r(x)=49x-14$.

在长除法中可以看到，如果除式的最高次数项的系数为 1，则多项式除法可在数环中进行.

习题 2.2

1. 求 $f(x)$被 $g(x)$除所得的商式与余式：

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

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

2. 证明：$\forall k\in\mathbb{N}^+$，$x\mid f^k(x)\Leftrightarrow x\mid f(x)$.

3. 已知$(x^2+x-2)\mid(x^4+x^3+mx+n)$，求 m,n.

4. 证明：如果 $h(x)\mid f(x)$，$h(x)\nmid g(x)$，则 $h(x)\nmid(f(x)+g(x))$. 举例说明：

$h(x)\nmid f(x)$，$h(x)\nmid g(x)$，不能得到 $h(x)\nmid(f(x)+g(x))$.

5. 证明：$(x^d-1)\mid(x^n-1)\Leftrightarrow d\mid n$.

2.3　多项式的最大公因式

2.3.1　最大公因式与辗转相除法

如果多项式 $h(x)$既是 $f(x)$的因式，又是 $g(x)$的因式，则称 $h(x)$是 $f(x)$与 $g(x)$的**公因式**. 显然，任意两个多项式都有公因式. 例如零次多项式就是它们的公因式. 在公因式中，最重要的是最大公因式.

定义 2.3.1 设 $f(x),g(x)\in F[x]$,如果 $d(x)\in F[x]$满足:

(1) $d(x)$是 $f(x)$与 $g(x)$的公因式;

(2) $f(x)$与 $g(x)$的所有公因式都是 $d(x)$的因式,

则称 $d(x)$是 $f(x)$与 $g(x)$的一个**最大公因式**.

如果 $f(x)=g(x)=0$,则 $f(x)$与 $g(x)$的最大公因式 $d(x)=0$;如果 $f(x)\neq 0$,则 $f(x)$与 0 的最大公因式是 $f(x)$. 当 $f(x)$与 $g(x)$不全为 0 时,$d(x)\neq 0$.

显然,若 $d(x)$是 $f(x)$与 $g(x)$的最大公因式,则 $\forall a\in F,a\neq 0,ad(x)$也是 $f(x)$与 $g(x)$的最大公因式. 于是我们约定 $f(x)$与 $g(x)$的最大公因式是指最高次项的系数为 1 的那一个,记作$(f(x),g(x))$.

ie: $d(x)=(f(x),g(x))\Leftrightarrow d(x)$的最高次项的系数为 1,且

$$\begin{cases}(1)\ d(x)\mid f(x),d(x)\mid g(x),\\ (2)\ \forall h(x)\in F[x],h(x)\mid f(x),h(x)\mid g(x)\Rightarrow h(x)\mid d(x).\end{cases}$$

定理 2.3.1 $\forall f(x),g(x)\in F[x]$,当 $f(x)$与 $g(x)$不全为 0 时,

$$\exists|d(x)\in F[x],\quad \ni\text{“}d(x)=(f(x),g(x))\text{”}.$$

证 (存在性)如果 $f(x)$与 $g(x)$有一个为 0 时,如 $f(x)=0$,则 $d(x)=af(x)$,其中 a 是使 $af(x)$的最高次项的系数为 1 的数.

如果 $f(x)$与 $g(x)$都不为 0,设

$$S[x]=\{p(x):p(x)=f(x)v(x)+g(x)u(x),u(x),v(x)\in F[x]\},$$

于是 $S[x]$中必有次数最小的多项式. 设 $S[x]$中次数最小且次数最高项的系数为 1 的多项式为 $d(x)$,则 $d(x)=(f(x),g(x))$.

实因: $d(x)=f(x)u(x)+g(x)v(x)$,如果 $d(x)\nmid f(x)$,则由带余除法得

$$f(x)=d(x)q(x)+r(x),\quad 0\leqslant\partial^0(r(x))<\partial^0(d(x)),$$

于是

$$r(x)=f(x)-d(x)q(x)=f(x)(1-u(x)q(x))+g(x)(-v(x)q(x)),$$

即 $r(x)\in S[x]$. 此与 $d(x)$是 $S[x]$中次数最小的多项式矛盾,故 $d(x)\mid f(x)$. 同理可得 $d(x)\mid g(x)$,所以 $d(x)$是 $f(x)$与 $g(x)$的公因式.

又 $\forall c(x)\in F[x],c(x)\mid f(x),c(x)\mid g(x)$,由于

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

所以 $c(x)\mid d(x)$,故 $d(x)=(f(x),g(x))$.

(唯一性)如果还 $\exists h(x)\in F[x],\ni\text{“}h(x)=(f(x),g(x))\text{”}$. 则

$$h(x)\mid d(x)\quad 且\quad d(x)\mid h(x),$$

故 $h(x)=d(x)$,唯一性得证.

推论 设 $f(x),g(x)\in F[x]$,若 $d(x)$是 $f(x)$与 $g(x)$的最大公因式,则

$$\exists u(x),v(x)\in F[x],\quad \ni\text{“}d(x)=f(x)u(x)+g(x)v(x)\text{”}.$$

证 若 $d(x)=0$,则取 $u(x)=v(x)=0$ 即可. 若 $d(x)\neq 0$,则由 $d(x)\in S[x]$即知结论

成立.

注意：推论的逆不成立.即由 $d(x)=f(x)u(x)+g(x)v(x)$不能得到 $d(x)$是 $f(x)$与 $g(x)$的最大公因式.例如：

$$f(x)=x,\quad g(x)=x+1,\quad u(x)=x,\quad v(x)=x+1,$$

显然 $f(x)u(x)+g(x)v(x)=2x^2+2x+1$ 不是 $f(x)$与 $g(x)$的最大公因式.

定理 2.3.1 只给出最大公因式的存在性,并没有给出求最大公因式的方法.

要求出两个多项式的最大公因式及推论中的 $u(x)$与 $v(x)$,得应用辗转相除法.

辗转相除法源于寻找能度量完两条长度为有理数的线段的最长尺子.

设长度为 a 与 b 的线段,$a,b\in\mathbb{Q}^+$,不妨设 $a<b$,可用短线段 a 作为尺子去度量线段 b,如果刚好度量完,则线段 a 就是所要寻找的尺子.如果度量不完,则用剩下的线段 $c=b-ka$ 去度量线段 a.如果刚好度量完,则线段 c 就是尺子.如果度量不完,又用剩下的线段 $d=a-lc$ 去度量线段 c,这个方法称为辗转相除法.由于最长尺子是存在的,所以这个方法可行.

这个方法用到求两个多项式的最大公因式上就是：

用次数不超过 $f(x)$的 $g(x)$去度量 $f(x)$,即

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

若刚好度量完,即 $r_1(x)=0$,则 $g(x)$就是 $f(x)$与 $g(x)$的最大公因式.若度量不完,即 $r_1(x)\neq0$,则用 $r_1(x)$去度量 $g(x)$,即

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

若刚好度量完,即 $r_2(x)=0$,则 $r_1(x)$就是 $f(x)$与 $g(x)$的最大公因式.若 $r_2(x)\neq0$,则用 $r_2(x)$去度量 $r_1(x)$,即

$$r_1(x)=r_2(x)q_3(x)+r_3(x).$$

因为辗转相除后,次数会越来越小,所以这个做法一定会终止,即 $\exists k$,

$$\ni\text{“}r_{k-2}(x)=r_{k-1}(x)q_k(x)+r_k(x),r_{k-1}(x)=r_k(x)q_{k+1}(x)\text{”}.$$

于是 $r_k(x)$就是 $f(x)$与 $g(x)$的最大公因式.

实因：$r_k(x)\mid r_{k-1}(x)$,于是

$$r_k(x)\mid r_{k-2}(x),\cdots,r_k(x)\mid r_1(x),r_k(x)\mid g(x),r_k(x)\mid f(x),$$

所以 $r_k(x)$就是 $f(x)$与 $g(x)$的公因式.

又 $\forall c(x)\in F[x]$,$c(x)\mid f(x)$,$c(x)\mid g(x)$,则 $c(x)\mid r_1(x)$,于是 $c(x)\mid r_2(x)$,继之 $c(x)\mid r_k(x)$,故 $r_k(x)$就是 $f(x)$与 $g(x)$的最大公因式.

如果要求出满足

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

的 $u(x)$与 $v(x)$,则由

$$d(x)=r_k(x)=r_{k-2}(x)-r_{k-1}(x)q_k(x)$$

反推到 $f(x)$与 $g(x)$的表达式即可.