第三节　整除的概念

主要内容

- 引入
- 带余除法
- 整除

一、引入

二、带余除法

带余除法 对于 $P[x]$ 中任意两个多项式 $f(x)$ 与 $g(x)$，其中 $g(x) \neq 0$，一定有 $P[x]$ 中的多项式 $q(x), r(x)$ 存在，使

$$f(x) = q(x)\,g(x) + r(x) \qquad (1)$$

成立，其中 $\partial(r(x)) < \partial(g(x))$ 或者 $r(x) = 0$，并且这样的 $q(x), r(x)$ 是唯一决定的.

证明 等式

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

中 $q(x)$ 和 $r(x)$ 的存在性可以由前面所说的除法直接得出. 下面用归纳法的语言来叙述.

如果 $f(x) = 0$，取 $q(x) = r(x) = 0$ 即可.

以下设 $f(x) \neq 0$. 令 $f(x)$, $g(x)$ 的次数分别为 n , m . 对 $f(x)$ 的次数 n 作(第二)数学归纳法.

当 $n < m$ 时，显然取 $q(x) = 0$， $r(x) = f(x)$ ，结论成立.

下面讨论 $n \geq m$ 的情形. 假设当 $f(x)$ 的次数小于 n 时， $q(x)$, $r(x)$ 的存在性已证. 现来看次数为 n 的情形.

令 ax^n , bx^m 分别是 $f(x)$, $g(x)$ 的首项，显然 $b^{-1}ax^{n-m}g(x)$ 与 $f(x)$ 有相同的首项，因而多项式

$$f_1(x) = f(x) - b^{-1}ax^{n-m}g(x)$$

的次数小于 n 或为 0 . 对于后者，取

$$q(x) = b^{-1}ax^{n-m} \quad , \quad r(x) = 0 \ ;$$

对于前者，由归纳法假设，对 $f_1(x)$, $g(x)$ 有

$q_1(x)$, $r_1(x)$ 存在使

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

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

$$\left.\begin{aligned} f_1(x) &= f\,(x) - b^{-1} a x^{n-m}\, g(x) \\ f_1(x) &= q_1(x)\, g(x) + r_1(x) \end{aligned}\right\} \Rightarrow$$

$$f\,(x) = (q_1(x) + b^{-1} a x^{n-m}\,)\, g(x) + r_1(x)\ ,$$

也就是说，有 $q\,(x) = q_1(x) + b^{-1} a x^{n-m}$ ， $r(x) = r_1(x)$

使 $f\,(x) = q(x)\, g(x) + r(x)$ 成立. 存在性得证.

下面再来证唯一性. 设另有 $q'(x)$, $r'(x)$ 使

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

其中 $\partial(r'(x)) < \partial(g(x))$ 或者 $r'(x) = 0$. 于是

$$q(x)\,g(x) + r(x) = q'(x)\,g(x) + r'(x)\,,$$

即

$$(q(x) - q'(x))\,g(x) = r'(x) - r(x)\,.$$

如果 $q(x) \neq q'(x)$，又据假设 $g(x) \neq 0$，那么

$$r'(x) - r(x) \neq 0,$$

且有

$$\partial (q(x) - q'(x)) + \partial (g(x)) = \partial (r'(x) - r(x)) .$$

但是

$$\partial (g(x)) > \partial (r'(x) - r(x)) ,$$

所以上式不可能成立. 这就证明了$q(x) = q'(x)$，因此 $r'(x) = r(x)$. 唯一性得征.

证毕

带余除法中所得的 $q(x)$ 通常称为 $g(x)$ 除 $f(x)$ 的**商**， $r(x)$ 通常称为 $g(x)$ 除 $f(x)$ 的**余式**.

三、整除

1. 定义

定义 5 数域 P 上的多项式 $g(x)$ 称为**整除** $f(x)$，如果有数域 P 上的多项式 $h(x)$ 使等式

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

成立. 我们用“$g(x) \mid f(x)$”表示 $g(x)$ 整除 $f(x)$，用“$g(x) \nmid f(x)$”表示 $g(x)$ 不能整除 $f(x)$.

当 $g(x) \mid f(x)$ 时， $g(x)$ 就称为 $f(x)$ 的**因式**，$f(x)$ 称为 $g(x)$ 的**倍式**.

当 $g(x) \neq 0$ 时，带余除法给出了整除性的一个判别法.

2. 整除的条件

定理 1 对于数域 P 上的任意两个多项式 $f(x)$ 和 $g(x)$，其中 $g(x) \neq 0$， $g(x) \mid f(x)$ 的充分必要条件是 $g(x)$ 除 $f(x)$ 的余式为零.

证明 如果 $r(x)=0$，那么 $f(x)=q(x)g(x)$，

即 $g(x)\mid f(x)$.

反过来，如果 $g(x)\mid f(x)$，那么

$$f(x)=q(x)g(x)=q(x)g(x)+0,$$

即 $r(x)=0$.

证毕

带余除法中 $g(x)$ 必须不为零. 但 $g(x)\mid f(x)$ 中，$g(x)$ 可以为零. 这时 $f(x)=g(x)h(x)=0\cdot h(x)=0$.

当 $g(x) \mid f(x)$ 时，如 $g(x) \neq 0$ ， $g(x)$ 除 $f(x)$ 所得的商 $q(x)$ 有时也可用

$$\frac{f(x)}{g(x)}$$

来表示.

由定义还可看出，任一个多项式 $f(x)$ 一定整除它自身，即 $f(x) \mid f(x)$ ，因为 $f(x) = 1 \cdot f(x)$ ；任一多项式 $f(x)$ 都整除零多项式 0, 因为 $0 = 0 \cdot f(x)$ ；零次多项式，也就是非零常数，能整除任一个多项

式，因为当 $a \neq 0$ 时， $f(x) = a(a^{-1} f(x))$.

下面介绍整除性的几个常用的性质：

2. 整除性的性质

性质 1 如果 $f(x) \mid g(x)$, $g(x) \mid f(x)$, 那么

$$f(x) = c\, g(x),$$

其中 c 为非零常数.

证明

性质 2　整除的传递性

如果 $f(x) \mid g(x)$, $g(x) \mid h(x)$, 那么 $f(x) \mid h(x)$.

证明☜

性质 3　如果 $f(x) \mid g_i(x)$, $i = 1, 2, \ldots, r$,

那么

$$f(x) \mid (u_1(x) g_1(x) + u_2(x) g_2(x) + \ldots + u_r(x) g_r(x)),$$

其中 $u_i(x)$ 是数域 P 上任意的多项式.

证明☜

通常，$u_1(x)g_1(x)+u_2(x)g_2(x)+\ldots+u_r(x)g_r(x)$ 称为多项式 $g_1(x), g_2(x), \ldots, g_r(x)$ 的一个组合.

由以上的性质可以看出，多项式 $f(x)$ 与它的任一个非零常数倍 $cf(x)$ $(c\neq 0)$ 有相同的因式，也有相同的倍式. 所以，在多项式整除性的讨论中，$f(x)$ 常常可以用 $cf(x)$ 来代替.

最后我们指出，两个多项式之间的整除关系不因为系数域的扩大而改变. 也就是说，如果 $f(x)$,

$g(x)$ 是 $P[x]$ 中两个多项式，P_1 是包含 P 的一个较大的数域. 当然，$f(x)$, $g(x)$ 也可以看成是 $P_1[x]$ 中的多项式. 从带余除法可以看出，不论把 $f(x)$, $g(x)$ 看成是 $P[x]$ 中或者是 $P_1[x]$ 中的多项式，用 $g(x)$ 去除 $f(x)$ 所得的商式及余式都是一样的. 因此，如果在 $P[x]$ 中 $g(x)$ 不能整除 $f(x)$，那么在 $P_1[x]$ 中，$g(x)$ 也不能整除 $f(x)$.

本节作业

P. 44: 2, 3, 4