信息安全数学基础

第五章 多项式环

聂旭云
信息与软件工程学院
电子科技大学

信息安全数学基础

多项式的基本概念

聂旭云
信息与软件工程学院
电子科技大学

多项式定义

- 定义5.1.1：如果R是整环，则R上未定元x的一个多项式是形如

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

的一个表达式，这里每一个$a_i\in R$，$0\le i\le n$，称a_i为x^i在$f(x)$中的系数。

- 使得$a_n\ne 0$的最大整数n称为$f(x)$的次数，记为$degf(x)$，称a_n为$f(x)$的首项系数
- 如果$f(x)=a_0$（即常数多项式）且$a_0\ne 0$，则记$f(x)$次数为0
- 所有系数都为0的多项式$f(x)$称为零多项式，为了方便，定义它的次数为$-\infty$
- 如果$f(x)$首项系数为1，则称$f(x)$是首一的
- 把R上的全体多项式集合记为$R[x]$
- 约定$x^0=1$，其中1是整环R中的单位元
- 通常我们用求和号来表示多项式，即$f(x)=\sum_{i=0}^{n}a_ix^i$

多项式相等的定义

- 定义5.1.2 设多项式$f(x)=\sum_{i=0}^{n} a_i x^i$ 和 $g(x)=\sum_{i=0}^{m} b_i x^i$ 整环R上的两个多项式。若满足

$$n=m\text{且}a_i=b_i, 0\leq i\leq n$$

则称$f(x)=g(x)$。

- 简而言之，两个多项式相等需满足次数相等且相同次数项对应的系数相等

多项式中的运算

- 多项式的加法：相同次数项对应系数相加。
- 设多项式$f(x)=\sum_{i=0}^{n} a_i x^i$ 和 $g(x)=\sum_{i=0}^{m} b_i x^i$ 是整环R上的两个多项式。
- 令$M=max\{m,n\}$，约定
  - $a_{n+1}=a_{n+2}=\cdots=a_M=0$，如果$n<M$
  - $b_{m+1}=b_{m+2}=\cdots=b_M=0$，如果$m<M$
- 多项式$f(x)$和$g(x)$可写成 $f(x)=\sum_{i=0}^{M} a_i x^i$ 和 $g(x)=\sum_{i=0}^{M} b_i x^i$，且有

$$f(x)+g(x)=\sum_{i=0}^{M}(a_i+b_i)x^i$$

多项式中的运算（续）

- 多项式的乘法：
- 设多项式$\boldsymbol{f(x)=\sum_{i=0}^{n} a_i x^i}$和 $\boldsymbol{g(x)=\sum_{i=0}^{m} b_i x^i}$是整环R上的两个多项式。
- 则

$$\boldsymbol{f(x)\cdot g(x)}$$

$$= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1)\boldsymbol{x}$$

$$+ a_0 b_0 = \sum_{s=0}^{m+n} (\sum_{i+j=s} a_i b_j) x^s$$

多项式运算律

- 加法交换律：$f(x)+g(x)=g(x)+f(x)$
- 加法结合律：$(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$
- 乘法交换律：$f(x)g(x)=g(x)f(x)$
- 乘法结合律：$(f(x)g(x))h(x)=f(x)(g(x)h(x))$
- 乘法对加法的分配律：$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$

多项式环

- **R**为一个整环，**x**是**R**上的未定元，**R[x]**对于多项式的加法和乘法构成环，称为多项式环。
  - 显然，$\boldsymbol{R[x]}$中的多项式对于加法和乘法封闭，
  - 对于加法，**R[x]**为加法交换群
    - 满足结合律和交换律
    - 有零元：零多项式**0**
    - 有负元：多项式$\boldsymbol{f(x)=\sum_{i=0}^{n}a_i x^i}$，有$\boldsymbol{-f(x)=\sum_{i=0}^{n}(-a_i)x^i}$，满足$\boldsymbol{f(x)+\big(-f(x)\big)=\big(-f(x)\big)+f(x)=0}$
  - 对于乘法
    - 满足结合律和交换律
    - 有单位元：$\boldsymbol{x^0=1}$
  - 乘法对加法满足分配律

多项式环（续）

定理5.1.1 整环R上的多项式环R[x]是整环。

证明要点： 紧扣整环定义，只需证明R[x]中无零因子

证明：设$f(x), g(x) \in R[x]$，且$f(x)g(x) = 0$。

若$f(x) = 0$，则定理得证。

不妨设 $f(x) = \sum_{i=0}^{n} a_i x^i$，其中$a_n \neq 0$，又设$g(x) = \sum_{i=0}^{m} b_i x^i$，由

$$f(x) \cdot g(x)$$

$$= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1) x + a_0 b_0$$

$$= 0$$

定理证明（续）

- 可得

$$
\begin{cases}
a_n b_m = 0 \\
a_n b_{m-1} + a_{n-1} b_m = 0 \\
a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m = 0 \\
\vdots \\
a_n b_0 + a_{n-1} b_1 + \cdots + a_{n-m} b_m = 0 \\
\vdots \\
a_1 b_0 + a_0 b_1 = 0 \\
a_0 b_0 = 0
\end{cases}
$$

- 因为整环R中无零因子，所以由$a_n \neq 0, a_n b_m = 0$，可得$b_m = 0$。将$b_m = 0$代入第二个式子，同样因为整环R中无零因子，可得$b_{m-1} = 0$，依次推导可得

$$b_m = b_{m-1} = \cdots = b_1 = b_0 = 0$$

- 即$g(x) = 0$。定理得证。

多项式带余除法

- 定理5.1.2（多项式的带余除法）设$f(x), g(x) \in F[x]$，$g(x) \neq 0$，则一定存在多项式$q(x), r(x) \in F[x]$，使得

$$f(x) = q(x)g(x) + r(x) \quad \text{（5-1）}$$

其中$\deg r(x) < \deg g(x)$或者$r(x) = 0$，而且$q(x), r(x)$是唯一的。$q(x)$称为$g(x)$除$f(x)$的商式，记为$f(x)\ div\ g(x)$，$r(x)$称为$g(x)$除$f(x)$的余式，记为$f(x)\ mod\ g(x)$。

证明思路：需要证明存在性和惟一性，注意利用条件$\deg r(x) < \deg g(x)$

多项式带余除法举例

- **例5.1.1** 在有理数域中取$f(x)=3x^3+4x^2-5x+6$，$g(x)=x^2-3x+1$，求$f(x)$除$g(x)$的商式和余式。

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

$$3x^3+4x^2-5x+6=(3x+13)(x^2-3x+1)+(31x-7)$$

多项式带余除法举例

- 例5.1.2 考虑$Z_2[x]$中多项式$f(x)=x^6+x^5+x^3+x^2+x+1$和$g(x)=x^4+x^3+1$，求$q(x),r(x)\in Z_2[x]$，使得$f(x)=q(x)g(x)+r(x)$其中$\deg r(x)<\deg g(x)$。

$$
\begin{array}{r|l}
 & x^2 \\
\cline{2-2}
x^4+x^3+1 & x^6+x^5+x^3+x^2+x+1 \\
 & x^6+x^5\qquad\quad +x^2 \\
\cline{2-2}
 & \qquad\qquad x^3\qquad\quad +x+1
\end{array}
$$

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

多项式带余除法举例

- 例5.1.3 在$Z_3[x]$中取$f(x) = x^5 + x^4 + x^2 + 1$，$g(x) = x^3 + x + 1$。
- 列竖式如下：

$$
\begin{array}{r|l}
 & x^2+x+2 \\
\hline
x^3+x+1 & x^5+x^4+x^2+1 \\
 & x^5+x^3+x^2 \\
\cline{2-2}
 & \quad x^4+2x^3+1 \\
 & \quad x^4+x^2+x \\
\cline{2-2}
 & \qquad 2x^3+2x^2+2x+1 \\
 & \qquad 2x^3\qquad +2x+2 \\
\cline{2-2}
 & \qquad\qquad 2x^2+2
\end{array}
$$

- 所以$f(x) = (x^2 + x + 2)g(x) + 2x^2 + 2$

感 谢 聆 听!

xynie@uestc.edu.cn