A Concrete Introduction to Number Theory and Algebra–多项式与有限域

Libin Wang

School of Computer Science, South China Normal University

April 19, 2021

Table of contents

多项式.

Definition

多项式通常表达为如下形式:

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{1}$$

其中，所有的 a_i 称为多项式的系数（coefficient），n 是使得 $a_n \neq 0$ 的最大非负整数，称为多项式的次数，记为 $deg\ f(x) = n$，而系数 a_n 就称为首项系数。首项系数为 1 的多项式称为首一多项式（monic）。如果多项式所有的系数都是 0，即多项式 $f(x) = 0$，称为零多项式，其次数定义为 $-\infty$。如果多项式的所有系数除了 a_0 之外都是 0，即 $f(x) = a_0$，$a_0 \neq 0$，此多项式称为常数多项式。多项式中的占位符 x 称为不定元（indeterminate）。

多项式的加法.

Definition

设 R 为交换环，$a(x), b(x) \in R[x]$，且

$$a(x) = \sum_{i=0}^{n} a_i x^i, \qquad b(x) = \sum_{i=0}^{m} b_i x^i, \quad n \geq m.$$

加法定义为:

$$a(x) + b(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

其中，当 $i > m$ 时，b_i 视为 0。

多项式的乘法.

Definition

设 R 为交换环，$a(x), b(x) \in R[x]$，且

$$a(x) = \sum_{i=0}^{n} a_i x^i, \qquad b(x) = \sum_{i=0}^{m} b_i x^i, \quad n \geq m.$$

乘法定义为:

$$a(x) * b(x) = \sum_{i=0}^{n+m} c_i x^i$$

其中，对所有的 i，$c_i = \sum_{k=0}^{i} a_k b_{i-k}$。

多项式环.

Proposition

设 R 为交换环，x 为不定元，环 R 上的多项式 $R[x]$ 在加法、乘法下形成交换环，并称之为多项式环。

命题的证明留给读者。

多项式环–实例.

Example

1. $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 分别是整数上的多项式环和有理数上的多项式环。
2. 设 p 为素数，$\mathbb{Z}_p[x]$ 是域 $\mathbb{Z}_p$ 上的多项式环。
3. $\mathbb{Z}_2[x]$ 是域 $\mathbb{Z}_2$ 上的多项式环。如果大家没有忘记二进制的位置计数法的话，应该知道 $\mathbb{Z}_2[x]$ 中每一个多项式都代表了一个二进制数字。

多项式环的除法算法.

Theorem

设 $\mathbb{F}$ 为域，$a(x), b(x) \in \mathbb{F}[x]$，且 $b(x)$ 不为零多项式。那么，存在唯一的多项式对 $q(x), r(x) \in \mathbb{F}[x]$ 使得，

$$a(x) = q(x)b(x) + r(x)$$

其中，$deg\ r(x) < deg\ b(x)$ 或者 $r(x)$ 为零多项式。

多项式环的除法算法–证明.

Proof.

使用归纳法证明。

1. 归纳起始步，如果 $a(x)$ 是零多项式，则
$$0 = 0b(x) + 0$$
因此，$q(x)$ 和 $r(x)$ 都是零多项式。
2. 归纳假设，假设次数小于 n 的多项式 $a(x)$ 都满足定理要求。

$\square$

多项式环的除法算法–证明 (续 1).

Proof.

使用归纳法证明。

- 归纳步，假设 $a(x)$ 为非零多项式，且 $\deg a(x) = n$，$\deg b(x) = m$。如果 $m > n$，则令 $q(x) = 0$，$r(x) = a(x)$，证完。所以，可以假设 $m \le n$，对 $a(x)$ 的次数 n 进行归纳。现在，

$$a(x) = \sum_{i=0}^{n} a_i x^i, \qquad b(x) = \sum_{i=0}^{m} b_i x^i, \quad n \ge m.$$

用 $a(x)$ 除 $b(x)$，除法第一步的结果是多项式

$$a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$$

并且，$a'(x)$ 的次数小于 n 或者为 0。

多项式环的除法算法–证明 (续 2).

Proof.

使用归纳法证明。

- 根据归纳假设，存在多项式 $q'(x)$ 和 $r(x)$ 使得

$$a'(x) = q'(x)b(x) + r(x)$$

且 $r(x)$ 的次数小于 $b(x)$ 的次数或者为 0。令

$$q(x) = q'(x) + \frac{a_n}{b_m}x^{n-m}$$

则 $a(x) = q(x)b(x) + r(x)$。唯一性的证明留给读者，提示：用反证法。

□

多项式环的若干定义.

Definition

设 $\mathbb{F}$ 为域，$a(x), b(x) \in \mathbb{F}[x]$.

- 如果存在 $q(x) \in \mathbb{F}[x]$ 使得 $a(x) = q(x)b(x)$，则称 $a(x)$ 可被 $b(x)$ 整除，记为 $b(x) \mid a(x)$，此时也称 $b(x)$ 是 $a(x)$ 的一个*因子*。
- 如果多项式 $d(x) \in \mathbb{F}[x]$ 满足 $d(x) \mid a(x)$ 且 $d(x) \mid b(x)$，则称 $d(x)$ 为 $a(x)$ 和 $b(x)$ 的公因子。如果*首一多项式* $d(x)$ 是 $a(x)$ 和 $b(x)$ 的公因子，且对 $a(x)$ 和 $b(x)$ 的其他公因子 $d'(x)$ 都有 $d'(x) \mid d(x)$，则称 $d(x)$ 是 $a(x)$ 和 $b(x)$ 的*最大公因子*，记为 $d(x) = gcd(a(x), b(x))$。

多项式环的若干定义.

Definition

设 $\mathbb{F}$ 为域，$a(x), b(x) \in \mathbb{F}[x]$.

- 如果 $gcd(a(x), b(x)) = 1$，则称 $a(x)$ 和 $b(x)$ *互素*。如果非常数多项式 $a(x) \in \mathbb{F}[x]$ 不能表达为任意两个非常数多项式 $b(x), c(x) \in \mathbb{F}[x]$ 的乘积，且 $b(x)$ 和 $c(x)$ 的次数都比 $a(x)$ 的次数要小，则称 $a(x)$ 为 *不可约多项式*（*irreducible polynomial*）。不可约多项式类似整数中的素数，它是多项式环中的*素多项式*。

整除性–多项式环版本.

Proposition

设 F 为域，$a(x), b(x), c(x) \in F[x]$，则有以下结论：

1. 如果 $a(x) \mid b(x)$，$b(x) \mid c(x)$，则 $a(x) \mid c(x)$。
2. 如果 $c(x) \mid a(x)$，$c(x) \mid b(x)$，则对任意 $m(x), n(x) \in F[x]$，有 $c(x) \mid (m(x)a(x) + n(x)b(x))$。

整除性–多项式环版本–证明.

Proof.

1. 因为 $a(x) \mid b(x)$，$b(x) \mid c(x)$，则存在 $u(x), v(x) \in F[x]$ 使得 $b(x) = u(x)a(x)$ 和 $c(x) = v(x)b(x)$，所以 $c(x) = v(x)(u(x)a(x)) = (v(x)u(x))a(x)$，即 $a(x) \mid c(x)$。
2. 因为 $c(x) \mid a(x)$，$c(x) \mid b(x)$，则存在 $u(x), v(x) \in F[x]$ 使得 $a(x) = u(x)c(x)$，$b(x) = v(x)c(x)$。对任意 $m(x), n(x) \in F[x]$，有

$$
\begin{aligned}
(m(x)a(x) + n(x)b(x)) &= m(x)u(x)c(x) + n(x)v(x)c(x) \\
&= (m(x)u(x) + n(x)v(x))c(x)
\end{aligned}
$$

所以，$c(x) \mid (m(x)a(x) + n(x)b(x))$。

$\square$

欧几里德算法–多项式环版本.

Theorem

设 $\mathbb{F}$ 是域，给定两个多项式 $a, b \in \mathbb{F}[x]$，设 $deg\ a(x) \geq deg\ b(x)$，则 $a(x)$ 和 $b(x)$ 的最大公因子等于 $b(x)$ 和 $a(x) \bmod b(x)$ 的最大公因子。即

$$gcd(a(x), b(x)) = gcd(b(x), a(x) \bmod b(x))$$

其中，$a(x) \bmod b(x)$ 表示用 $a(x)$ 除以 $b(x)$ 所得到的余数 $r(x)$。

欧几里德算法–多项式环版本.

Example

计算有理数域 $\mathbb{Q}$ 上多项式 $a(x) = x^5 + x^4 + x + 1$ 和 $b(x) = x^4 + x^3 + x + 1$ 的最大公因子。

$$
\begin{aligned}
gcd(a(x), b(x)) &= gcd(b(x), -x^2 + 1) \\
&= gcd(-x^2 + 1, 2x + 2) \\
&= gcd(2x + 2, x + 1) \\
&= gcd(x + 1, 0) = x + 1
\end{aligned}
$$

欧几里德算法–多项式环版本–代码.

Listing 1: 欧几里德算法–多项式环版本

```
#Input: 多项式f和g
#Output: f和g的最大公因子
def poly_gcd(f, g):
    while g != 0:
        r = f % g #求f除g得到的余数
        f = g
        g = r
    return f
```

扩展欧几里德算法–多项式环版本.

Theorem

设 F 是域，设 $d(x)$ 是两个多项式 $a, b \in \mathbb{F}[x]$ 的最大公因子，则存在 $r(x), s(x) \in \mathbb{F}[x]$ 使得：

$$d(x) = r(x)a(x) + s(x)b(x)。$$

不可约多项式.

Proposition

设 $\mathbb{F}$ *为域，* $p(x) \in \mathbb{F}[x]$ *是不可约多项式，则对任意* $f(x) \in \mathbb{F}[x]$ *且* $p(x) \nmid f(x)$*，有：*

$$gcd(p(x), f(x)) = 1$$

不可约多项式–证明.

Proof.

设 $d(x) = gcd(p(x), f(x))$，则 d 或者是一个非零常量，或者是一个 $\mathbb{F}[x]$ 中非零多项式。如果是前者，则 $d(x)$ 只能是 1，因为最大公因子必须是首一多项式。如果是后者，因为 $p(x)$ 是不可约多项式，且 $d(x) \mid p(x)$，则存在某个常量 $a \in \mathbb{F}$，使得 $d(x) = ap(x)$。但是，同时 $d(x) \mid f(x)$，则存在某个 $g(x) \in \mathbb{F}[x]$，使得 $f(x) = d(x)g(x) = ap(x)g(x)$，说明 $p(x) \mid f(x)$，与条件假设矛盾。 □ □

有限域.

准确来说，本节并不打算深入讨论有限域的理论。而是通过构造出一种特殊的有限域，让读者先建立起对有限域的认识。实在是入门之入门。
域 $\mathbb{F}$ 是一种特殊的环，它在加法上是阿贝尔群，$\mathbb{F}^*$ 在乘法上是阿贝尔群。有限域则是具有有限个元素的域。先归纳以上章节中关于有限域的几点结论：

1. 有限域的特征必为素数。
2. 如果有限域 $\mathbb{F}$ 的特征是素数 p，则 $\mathbb{F}$ 的阶是 p^n，n 是某个正整数。
3. 对任意的素数 p 和正整数 n，存在阶为 p^n 的有限域。
4. R 是交换环，R/M 是域当且仅当 M 是 R 的极大理想。