



网络空间安全学院

School of Cyberspace Security, BUPT

信息安全数学基础

—— 环 (2)

信数课题组

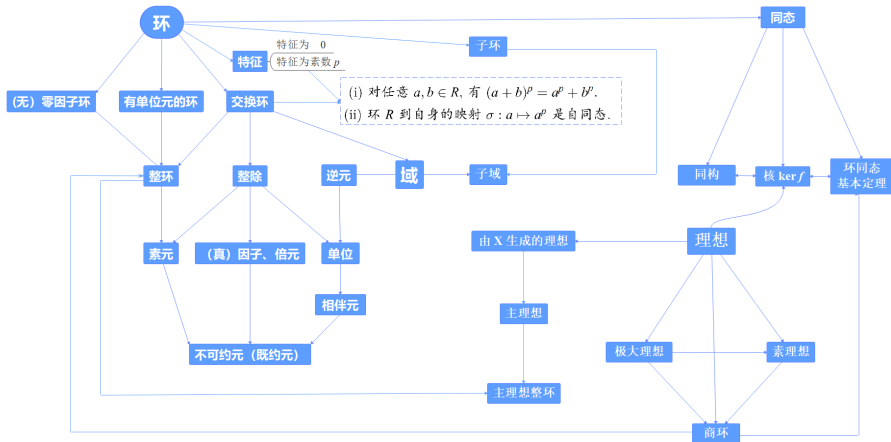
北京邮电大学

传邮万里

国脉所系



上次课回顾



目录

① 多项式整环

- 多项式整环与不可约多项式
- 多项式的欧几里德除法

目录

1 多项式整环

- 多项式整环与不可约多项式
- 多项式的欧几里德除法

定义 7.4.1

设 $(R, +, \cdot)$ 是整环, x 为变量, $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 其中 $a_i \in R$, 则称 $f(x)$ 为环 R 上的 (一元) 多项式. 此时,

- (i) a_i 称为多项式 $f(x)$ 的系数, $a_i \in R$.
- (ii) 若 $a_n \neq 0$, 则称多项式 $f(x)$ 的次数为 n , 记为 $\deg f = n$.

定义 7.4.1

设 $(R, +, \cdot)$ 是整环, x 为变量, $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 其中 $a_i \in R$, 则称 $f(x)$ 为环 R 上的 (一元) 多项式. 此时,

- (i) a_i 称为多项式 $f(x)$ 的系数, $a_i \in R$.
- (ii) 若 $a_n \neq 0$, 则称多项式 $f(x)$ 的次数为 n , 记为 $\deg f = n$.

我们考虑整环 R 上的全体多项式组成的集合 $R[x]$.

首先, 定义 $R[x]$ 上的加法. 设

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

定义 $f(x)$ 和 $g(x)$ 的加法为

$$(f+g)(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

则 $R[x]$ 中零元为 0, $f(x)$ 的负元为

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

其次, 定义 $R[x]$ 上的乘法. 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, a_n \neq 0,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0, b_m \neq 0,$$

定义 $f(x)$ 和 $g(x)$ 的乘法为

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

其中

$$c_k = \sum_{\substack{i+j=k, \\ 0 \leq i \leq n, \\ 0 \leq j \leq m}} a_i b_j = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k, 0 \leq k \leq n+m,$$

即

$$c_{n+m} = a_n b_m, c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m, \cdots, c_k = \sum_{i+j=k} a_i b_j, \cdots, c_0 = a_0 b_0,$$

则 $R[x]$ 中单位元为 1.

其次, 定义 $R[x]$ 上的乘法. 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, a_n \neq 0,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0, b_m \neq 0,$$

定义 $f(x)$ 和 $g(x)$ 的乘法为

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

其中

$$c_k = \sum_{\substack{i+j=k, \\ 0 \leq i \leq n, \\ 0 \leq j \leq m}} a_i b_j = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k, 0 \leq k \leq n+m,$$

即

$$c_{n+m} = a_n b_m, c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m, \cdots, c_k = \sum_{i+j=k} a_i b_j, \cdots, c_0 = a_0 b_0,$$

则 $R[x]$ 中单位元为 1.

综上, $R[x]$ 对上述加法和乘法运算构成一个整环, 称其为多项式整环.

例 7.4.1 设 $f(x) = x^6 + x^4 + x^2 + x + 1$, $g(x) = x^7 + x + 1 \in F_2[x]$, 则

$$f(x) + g(x) = x^7 + x^6 + x^4 + x^2.$$

$$f(x)g(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1.$$

事实上,

$$\begin{aligned} f(x)g(x) &= (x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) \\ &= x^{13} + x^{11} + x^9 + x^8 + x^7 \\ &\quad + x^5 + x^3 + x^2 + x \\ &\quad + x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1. \end{aligned}$$

例 7.4.2 设 R 是模 7 的剩余类环, 计算 $R[x]$ 中乘积
$$([3]x^3 + [5]x - [4])([4]x^2 - x + [3]).$$

例 7.4.2 设 R 是模 7 的剩余类环, 计算 $R[x]$ 中乘积

$$([3]x^3 + [5]x - [4])([4]x^2 - x + [3]).$$

解: 模 7 的剩余类环 $R = \{[0], [1], [2], [3], [4], [5], [6]\}$.

首先把负号变成正号, 然后有

$$\begin{aligned} \text{原式} &= ([3]x^3 + [5]x + [3])([4]x^2 + [6]x + [3]) \\ &= [3][4]x^5 + [3][6]x^4 + [3][3]x^3 \\ &\quad + [5][4]x^3 + [5][6]x^2 + [5][3]x \\ &\quad + [3][4]x^2 + [3][6]x + [3][3] \\ &= [5]x^5 + [4]x^4 + x^3 + [5]x + [2]. \end{aligned}$$

定义 7.4.2

设 $f(x), g(x)$ 是整环 R 上的任意两个多项式, 其中 $g(x) \neq 0$. 如果存在一个多项式 $q(x)$ 使得等式 $f(x) = q(x) \cdot g(x)$ 成立, 就称 $g(x)$ 整除 $f(x)$ 或者 $f(x)$ 被 $g(x)$ 整除, 记作 $g(x) \mid f(x)$.

这时, 把 $g(x)$ 叫作 $f(x)$ 的因式, 把 $f(x)$ 叫作 $g(x)$ 的倍式.

否则, 就称 $g(x)$ 不能整除 $f(x)$ 或者 $f(x)$ 不能被 $g(x)$ 整除, 记作 $g(x) \nmid f(x)$.

定义 7.4.2

设 $f(x), g(x)$ 是整环 R 上的任意两个多项式, 其中 $g(x) \neq 0$. 如果存在一个多项式 $q(x)$ 使得等式 $f(x) = q(x) \cdot g(x)$ 成立, 就称 $g(x)$ 整除 $f(x)$ 或者 $f(x)$ 被 $g(x)$ 整除, 记作 $g(x) | f(x)$.

这时, 把 $g(x)$ 叫作 $f(x)$ 的因式, 把 $f(x)$ 叫作 $g(x)$ 的倍式.

否则, 就称 $g(x)$ 不能整除 $f(x)$ 或者 $f(x)$ 不能被 $g(x)$ 整除, 记作 $g(x) \nmid f(x)$.

定义 7.4.3

设 $f(x)$ 是整环 R 上的非常数多项式. 若除因式 1 和 $f(x)$ 外, $f(x)$ 没有其他非常数因式, 那么 $f(x)$ 叫作不可约多项式; 否则, $f(x)$ 叫作合式.

定义 7.4.2

设 $f(x), g(x)$ 是整环 R 上的任意两个多项式, 其中 $g(x) \neq 0$. 如果存在一个多项式 $q(x)$ 使得等式 $f(x) = q(x) \cdot g(x)$ 成立, 就称 $g(x)$ 整除 $f(x)$ 或者 $f(x)$ 被 $g(x)$ 整除, 记作 $g(x) \mid f(x)$.

这时, 把 $g(x)$ 叫作 $f(x)$ 的因式, 把 $f(x)$ 叫作 $g(x)$ 的倍式.

否则, 就称 $g(x)$ 不能整除 $f(x)$ 或者 $f(x)$ 不能被 $g(x)$ 整除, 记作 $g(x) \nmid f(x)$.

定义 7.4.3

设 $f(x)$ 是整环 R 上的非常数多项式. 若除因式 1 和 $f(x)$ 外, $f(x)$ 没有其他非常数因式, 那么 $f(x)$ 叫作不可约多项式; 否则, $f(x)$ 叫作合式.

例 7.4.3 在 $\mathbb{Z}[x]$ 中, 多项式 $x^2 + 1$ 不可约.

目录

① 多项式整环

- 多项式整环与不可约多项式
- 多项式的欧几里德除法

定理 7.4.1

设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, a_n \neq 0$,
 $g(x) = x^m + \cdots + b_1 x + b_0, m \geq 1$, 是整环 R 上的两个多项式, 则一定存在多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x) = q(x) \cdot g(x) + r(x), \deg r < \deg g.$$

定理 7.4.1

设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, a_n \neq 0$,
 $g(x) = x^m + \cdots + b_1 x + b_0, m \geq 1$, 是整环 R 上的两个多项式, 则一定存在多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x) = q(x) \cdot g(x) + r(x), \deg r < \deg g.$$

证: 对 $f(x)$ 的次数 $\deg f = n$ 作数学归纳法.

(i) 如果 $\deg f < \deg g$, 则取 $q(x) = 0, r(x) = f(x)$. 结论成立.

定理 7.4.1

设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, a_n \neq 0$,
 $g(x) = x^m + \cdots + b_1 x + b_0, m \geq 1$, 是整环 R 上的两个多项式, 则一定存在多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x) = q(x) \cdot g(x) + r(x), \deg r < \deg g.$$

证: 对 $f(x)$ 的次数 $\deg f = n$ 作数学归纳法.

(i) 如果 $\deg f < \deg g$, 则取 $q(x) = 0, r(x) = f(x)$. 结论成立.

(ii) 设 $\deg f \geq \deg g$. 假设结论对 $\deg f < n$ 的多项式成立.

对于 $\deg f = n \geq \deg g$, 有 $f(x) - a_n x^{n-m} \cdot g(x)$

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

这说明 $f(x) - a_n x^{n-m} \cdot g(x)$ 是次数 $\leq n-1$ 的多项式. 对其运用归纳假设或情形 (i), 存在整系数多项式 $q_1(x)$ 和 $r_1(x)$ 使得

$$f(x) - a_n x^{n-m} \cdot g(x) = q_1(x) \cdot g(x) + r_1(x), \deg r_1(x) < \deg g(x).$$

注：此过程称为多项式欧几里德除法，上式中的 $q(x)$ 叫作 $f(x)$ 被 $g(x)$ 除所得的不完全商， $r(x)$ 叫作 $f(x)$ 被 $g(x)$ 除所得的余式.

注：此过程称为多项式欧几里德除法，上式中的 $q(x)$ 叫作 $f(x)$ 被 $g(x)$ 除所得的不完全商， $r(x)$ 叫作 $f(x)$ 被 $g(x)$ 除所得的余式。

例 7.4.4 设 $f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$,
 $g(x) = x^8 + x^4 + x^3 + x + 1 \in F_2[x]$, 求 $q_1(x)$ 和 $r_1(x)$ 使得
 $f(x) = q_1(x) \cdot g(x) + r_1(x)$, $\deg r_1 < \deg g$.

注：此过程称为多项式欧几里德除法，上式中的 $q(x)$ 叫作 $f(x)$ 被 $g(x)$ 除所得的不完全商， $r(x)$ 叫作 $f(x)$ 被 $g(x)$ 除所得的余式。

例 7.4.4 设 $f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$,

$g(x) = x^8 + x^4 + x^3 + x + 1 \in F_2[x]$, 求 $q_1(x)$ 和 $r_1(x)$ 使得

$f(x) = q_1(x) \cdot g(x) + r_1(x)$, $\deg r_1 < \deg g$.

解：逐次消除最高次项

$$\begin{aligned} & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 - x^5(x^8 + x^4 + x^3 + x + 1) \\ &= x^{11} + x^4 + x^3 + 1. \end{aligned}$$

$$\begin{aligned} & x^{11} + x^4 + x^3 + 1 - x^3(x^8 + x^4 + x^3 + x + 1) \\ &= x^7 + x^6 + 1. \end{aligned}$$

因此, $q_1(x) = x^5 + x^3$ 和 $r_1(x) = x^7 + x^6 + 1$.

类似于整数中的最大公因数和最小公倍数, 我们可以给出多项式环 $R[x]$ 中的最大公因式和最小公倍式.

类似于整数中的最大公因数和最小公倍数, 我们可以给出多项式环 $R[x]$ 中的最大公因式和最小公倍式.

定义 7.4.4

设 $f(x), g(x) \in R[x]$, 如果 $d(x) \in R[x]$ 满足

(1) $d(x) \mid f(x), d(x) \mid g(x)$.

(2) 若 $h(x) \mid f(x), h(x) \mid g(x)$, 则 $h(x) \mid d(x)$.

则称 $d(x)$ 为 $f(x), g(x)$ 的最大公因式, 记作 $(f(x), g(x))$.

类似于整数中的最大公因数和最小公倍数, 我们可以给出多项式环 $R[x]$ 中的最大公因式和最小公倍式.

定义 7.4.4

设 $f(x), g(x) \in R[x]$, 如果 $d(x) \in R[x]$ 满足

- (1) $d(x) \mid f(x), d(x) \mid g(x)$.
- (2) 若 $h(x) \mid f(x), h(x) \mid g(x)$, 则 $h(x) \mid d(x)$.

则称 $d(x)$ 为 $f(x), g(x)$ 的最大公因式, 记作 $(f(x), g(x))$.

定义 7.4.5

设 $f(x), g(x) \in R[x]$, 如果 $D(x) \in R[x]$ 满足

- (1) $f(x) \mid D(x), g(x) \mid D(x)$.
- (2) 若 $f(x) \mid h(x), g(x) \mid h(x)$, 则 $D(x) \mid h(x)$.

则称 $D(x)$ 为 $f(x), g(x)$ 的最小公倍式, 记作 $[f(x), g(x)]$.

如何求 $(f(x), g(x))$?

设 $f(x), g(x)$ 是域 K 上的多项式, $\deg g \geq 1$.

记 $r_0(x) = f(x)$, $r_1(x) = g(x)$. 反复运用多项式欧几里德除法, 有

$$r_0(x) = q_1(x) \cdot r_1(x) + r_2(x), \quad 0 \leq \deg r_2 < \deg r_1,$$

$$r_1(x) = q_2(x) \cdot r_2(x) + r_3(x), \quad 0 \leq \deg r_3 < \deg r_2,$$

$$\vdots$$

$$r_{k-2}(x) = q_{k-1}(x) \cdot r_{k-1}(x) + r_k(x), \quad 0 \leq \deg r_k < \deg r_{k-1},$$

$$r_{k-1}(x) = q_k(x) \cdot r_k(x) + r_{k+1}(x), \quad \deg r_{k+1} = 0.$$

如何求 $(f(x), g(x))$?

设 $f(x), g(x)$ 是域 K 上的多项式, $\deg g \geq 1$.

记 $r_0(x) = f(x)$, $r_1(x) = g(x)$. 反复运用多项式欧几里德除法, 有

$$r_0(x) = q_1(x) \cdot r_1(x) + r_2(x), \quad 0 \leq \deg r_2 < \deg r_1,$$

$$r_1(x) = q_2(x) \cdot r_2(x) + r_3(x), \quad 0 \leq \deg r_3 < \deg r_2,$$

$$\vdots$$

$$r_{k-2}(x) = q_{k-1}(x) \cdot r_{k-1}(x) + r_k(x), \quad 0 \leq \deg r_k < \deg r_{k-1},$$

$$r_{k-1}(x) = q_k(x) \cdot r_k(x) + r_{k+1}(x), \quad \deg r_{k+1} = 0.$$

经过有限步骤, 必然存在 k 使得 $r_{k+1}(x) = 0$, 这是因为

$$0 = \deg r_{k+1} < \deg r_k < \deg r_{k-1} < \cdots < \deg r_2 < \deg r_1 = \deg g,$$

且 $\deg g$ 是有限正整数.

定理 7.4.2

设 $f(x), g(x)$ 是域 K 上的多项式, $\deg g \geq 1$, 则

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

其中 $r_k(x)$ 是多项式广义欧几里得除法中最后一个非零余式.

定理 7.4.2

设 $f(x), g(x)$ 是域 K 上的多项式, $\deg g \geq 1$, 则

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

其中 $r_k(x)$ 是多项式广义欧几里德除法中最后一个非零余式.

从多项式广义欧几里德除法中逐次消去 $r_{k-1}(x), r_{k-2}(x), \dots, r_3(x), r_2(x)$ 我们可找到多项式 $s(x), t(x)$ 使得

$$s(x) \cdot f(x) + t(x) \cdot g(x) = (f(x), g(x)).$$

定理 7.4.2

设 $f(x), g(x)$ 是域 K 上的多项式, $\deg g \geq 1$, 则

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

其中 $r_k(x)$ 是多项式广义欧几里德除法中最后一个非零余式.

从多项式广义欧几里德除法中逐次消去 $r_{k-1}(x), r_{k-2}(x), \dots, r_3(x), r_2(x)$ 我们可找到多项式 $s(x), t(x)$ 使得

$$s(x) \cdot f(x) + t(x) \cdot g(x) = (f(x), g(x)).$$

定理 7.4.3

设 $f(x), g(x)$ 是域 K 上的多项式, 则存在多项式 $s(x), t(x)$ 使得

$$s(x) \cdot f(x) + t(x) \cdot g(x) = (f(x), g(x)).$$

定理 7.4.2

设 $f(x), g(x)$ 是域 K 上的多项式, $\deg g \geq 1$, 则

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

其中 $r_k(x)$ 是多项式广义欧几里德除法中最后一个非零余式.

从多项式广义欧几里德除法中逐次消去 $r_{k-1}(x), r_{k-2}(x), \dots, r_3(x), r_2(x)$ 我们可找到多项式 $s(x), t(x)$ 使得

$$s(x) \cdot f(x) + t(x) \cdot g(x) = (f(x), g(x)).$$

定理 7.4.3

设 $f(x), g(x)$ 是域 K 上的多项式, 则存在多项式 $s(x), t(x)$ 使得

$$s(x) \cdot f(x) + t(x) \cdot g(x) = (f(x), g(x)).$$

注: 如果 $f(x)$ 与 $g(x)$ 的最大公因式 $(f(x), g(x)) = 1$, 则称它们是 **互素** (或**互质**) 的.

例 7.4.5 设 $f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \in \mathbb{F}_2[x]$,
 $g(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$,
求多项式 $s(x), t(x)$ 使得 $s(x) \cdot f(x) + t(x) \cdot g(x) = (f(x), g(x))$.

例 7.4.5 设 $f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \in \mathbb{F}_2[x]$,
 $g(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$,

求多项式 $s(x), t(x)$ 使得 $s(x) \cdot f(x) + t(x) \cdot g(x) = (f(x), g(x))$.

解: 在例 7.4.4 的基础上, 反复运用广义多项式欧几里德除法, 我们有

$$f(x) = q_1(x) \cdot g(x) + r_1(x), \quad q_1(x) = x^5 + x^3, \quad r_1(x) = x^7 + x^6 + 1,$$

$$g(x) = q_2(x) \cdot r_1(x) + r_2(x), \quad q_2(x) = x + 1, \quad r_2(x) = x^6 + x^4 + x^3,$$

$$r_1(x) = q_3(x) \cdot r_2(x) + r_3(x), \quad q_3(x) = x + 1, \quad r_3(x) = x^5 + x^3 + 1,$$

$$r_2(x) = q_4(x) \cdot r_3(x) + r_4(x), \quad q_4(x) = x, \quad r_4(x) = x^3 + x,$$

$$r_3(x) = q_5(x) \cdot r_4(x) + r_5(x), \quad q_5(x) = x^2, \quad r_5(x) = 1.$$

$$r_4(x) = q_6(x) \cdot r_5(x) + r_6(x), \quad q_6(x) = x^3 + x, \quad r_6(x) = 0.$$

从而,

$$\begin{aligned}r_5(x) &= q_5(x) \cdot (q_4(x) \cdot r_3(x) + r_2(x)) + r_3(x) \\&= (q_5(x) \cdot q_4(x) + 1) \cdot r_3(x) + q_5(x) \cdot r_2(x) \\&= (x^3 + 1) \cdot (q_3(x) \cdot r_2(x) + r_1(x)) + x^2 \cdot r_2(x) \\&= (x^4 + x^3 + x^2 + x + 1) \cdot (q_2(x) \cdot r_1(x) + g(x)) + (x^3 + 1) \cdot r_1(x) \\&= (x^5 + x^3) \cdot (q_1(x) \cdot g(x) + f(x)) + (x^4 + x^3 + x^2 + x + 1) \cdot g(x) \\&= (x^5 + x^3) \cdot f(x) + (x^{10} + x^6 + x^4 + x^3 + x^2 + x + 1) \cdot g(x)\end{aligned}$$

从而,

$$\begin{aligned}r_5(x) &= q_5(x) \cdot (q_4(x) \cdot r_3(x) + r_2(x)) + r_3(x) \\&= (q_5(x) \cdot q_4(x) + 1) \cdot r_3(x) + q_5(x) \cdot r_2(x) \\&= (x^3 + 1) \cdot (q_3(x) \cdot r_2(x) + r_1(x)) + x^2 \cdot r_2(x) \\&= (x^4 + x^3 + x^2 + x + 1) \cdot (q_2(x) \cdot r_1(x) + g(x)) + (x^3 + 1) \cdot r_1(x) \\&= (x^5 + x^3) \cdot (q_1(x) \cdot g(x) + f(x)) + (x^4 + x^3 + x^2 + x + 1) \cdot g(x) \\&= (x^5 + x^3) \cdot f(x) + (x^{10} + x^6 + x^4 + x^3 + x^2 + x + 1) \cdot g(x)\end{aligned}$$

故 $s(x) = x^5 + x^3, t(x) = x^{10} + x^6 + x^4 + x^3 + x^2 + x + 1$.

对应的, 也可以给出多项式同余的概念.

定义 7.4.6

给定 $R[x]$ 中的首一多项式 $m(x)$. 如果 $R[x]$ 中的两个多项式 $f(x), g(x)$ 满足 $m(x) \mid f(x) - g(x)$, 则称多项式 $f(x)$ 与 $g(x)$ 模 $m(x)$ 同余, 记作 $f(x) \equiv g(x) \pmod{m(x)}$. 否则, 称 $f(x)$ 与 $g(x)$ 模 $m(x)$ 不同余, 记作 $f(x) \not\equiv g(x) \pmod{m(x)}$.

对应的, 也可以给出多项式同余的概念.

定义 7.4.6

给定 $R[x]$ 中的首一多项式 $m(x)$. 如果 $R[x]$ 中的两个多项式 $f(x), g(x)$ 满足 $m(x) \mid f(x) - g(x)$, 则称多项式 $f(x)$ 与 $g(x)$ 模 $m(x)$ 同余, 记作 $f(x) \equiv g(x) \pmod{m(x)}$. 否则, 称 $f(x)$ 与 $g(x)$ 模 $m(x)$ 不同余, 记作 $f(x) \not\equiv g(x) \pmod{m(x)}$.

定义 7.4.7

设 $p(x)$ 是 $R[x]$ 中的多项式, 则称 $(p(x)) = \{f(x) \in R[x] \mid p(x) \mid f(x)\}$ 为 $R[x]$ 中的多项式理想.

注：设 $R[x]$ 是整环，由此可得到商环 $R[x]/(p(x))$ 。其中商环 $R[x]/(p(x))$ 上的运算法则是：

加法：
$$f(x) + g(x) = (f + g)(x) \mod p(x).$$

乘法：
$$f(x) \cdot g(x) = (f \cdot g)(x) \mod p(x).$$

注：设 $R[x]$ 是整环，由此可得到商环 $R[x]/(p(x))$ 。其中商环 $R[x]/(p(x))$ 上的运算法则是：

加法：
$$f(x) + g(x) = (f + g)(x) \mod p(x).$$

乘法：
$$f(x) \cdot g(x) = (f \cdot g)(x) \mod p(x).$$

进一步，可以得到：

定理 7.4.4

设 K 是一个域， $p(x)$ 是 $K[x]$ 中的不可约多项式，则商环 $R[x]/(p(x))$ 对于上述运算法则构成一个域。

注：设 $R[x]$ 是整环，由此可得到商环 $R[x]/(p(x))$ 。其中商环 $R[x]/(p(x))$ 上的运算法则是：

加法：
$$f(x) + g(x) = (f + g)(x) \mod p(x).$$

乘法：
$$f(x) \cdot g(x) = (f \cdot g)(x) \mod p(x).$$

进一步，可以得到：

定理 7.4.4

设 K 是一个域， $p(x)$ 是 $K[x]$ 中的不可约多项式，则商环 $R[x]/(p(x))$ 对于上述运算法则构成一个域。

证：只需证明 $R[x]/(p(x))$ 中的非零元 $f(x) \mod p(x)$ 为可逆元。

事实上，对于 $f(x) \not\equiv 0 \mod p(x)$ ，有 $(f(x), p(x)) = 1$ 。

根据多项式广义欧几里德除法，存在多项式 $s(x), t(x)$

使得 $s(x) \cdot f(x) + t(x) \cdot p(x) = 1$ 。从而 $s(x)f(x) \equiv 1 \mod p(x)$ 。

这说明 $f(x) \mod p(x)$ 为可逆元， $s(x) \mod p(x)$ 为其逆元。

本课作业

1. 设 $a(x), b(x)$ 是如下所示的多项式,

$$a(x) = x^6 + 5x^5 + 4x^4 + 3x^3 + x + 3,$$

$$b(x) = x^6 + 3x^5 + 5x^4 + 6x^3 + 2x + 1.$$

试计算 $a(x) + b(x)$ 和 $a(x) \cdot b(x)$ 在数域 F_5 上的结果.

2. 设 R 是整环. 证明: 对 R 上的任何非零多项式 $f(x), g(x)$, 有

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

如果 R 不是整环, 这一结论还成立吗?

交流与讨论



电子邮箱:

陈秀波: xb_chen@bupt.edu.cn

徐国胜: guoshengxu@bupt.edu.cn

金正平: zhpjin@bupt.edu.cn