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

多项式整除和最大公因式

聂旭云
信息与软件工程学院
电子科技大学

多项式整除

- 定义5.2.1 设$f(x), g(x) \in F[x]$，如果存在$q(x) \in F[x]$，使得$f(x) = q(x)g(x)$，则称$g(x)$整除$f(x)$，记为$g(x)|f(x)$。记$g(x)\nmid f(x)$为$g(x)$不整除$f(x)$。当$g(x)|f(x)$时，称$g(x)$为$f(x)$的因式，而称$f(x)$为$g(x)$的倍式。

- 定理5.2.1 设$f(x), g(x) \in F[x]$，$g(x) \neq 0$，$g(x)$整除$f(x)$的充要条件是$g(x)$除$f(x)$的余式为零。

多项式整除的性质

- 定理5.2.2 设$\boldsymbol{F}[x]$是域$\boldsymbol{F}$上的多项式环。

（1）设$\boldsymbol{f(x), g(x) \in F}[x]$，若$\boldsymbol{f(x)|g(x)}$，$\boldsymbol{g(x)|f(x)}$，则有$\boldsymbol{f(x) = cg(x)}$，其中$\boldsymbol{c \in F}$。

（2）设$\boldsymbol{f(x), g(x), h(x) \in F}[x]$，若$\boldsymbol{f(x)|g(x)}$，$\boldsymbol{g(x)|h(x)}$，则有$\boldsymbol{f(x)|h(x)}$。

（3）设$\boldsymbol{f(x), g_i(x) \in F}[x]$，其中$\boldsymbol{i = 1, 2, \cdots, l}$，若对于所有的$\boldsymbol{i}$都有$\boldsymbol{f(x)|g_i(x)}$，则

$$\boldsymbol{f(x)|u_1(x)g_1(x) + \cdots + u_l(x)g_l(x)}$$

其中$\boldsymbol{u_i(x) \in F}[x]$是域$\boldsymbol{F}$上的任意多项式。

公因式

定义5.2.2 如果$h(x)$既是$f(x)$的因式，又是$g(x)$的因式，则称$h(x)$是$f(x)$和$g(x)$的公因式。

若$f(x)$和$g(x)$的公因式$d(x)$满足$f(x)$和$g(x)$的公因式都是$d(x)$的因式，则称$d(x)$是$f(x)$和$g(x)$的一个最大公因式。记首项系数为1的最大公因式为

$$\big(f(x), g(x)\big)$$

根据带余除法和多项式整除的性质，如果有等式

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

成立，那么$f(x), g(x)$和$g(x), r(x)$有相同的公因式，因此有

$$\big(f(x), g(x)\big) = (g(x), (r(x))$$

最大公因式

- 定理5.2.3 对于$F[x]$中的多项式$f(x)$和$g(x)$，一定存在最大公因式$d(x) \in F[x]$，且$d(x)$可以表示成$f(x)$和$g(x)$的一个组合，即存在$u(x), v(x) \in F[x]$，使得

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

证明思路：类似于最大公因数定理，利用辗转相除法，不断降低带余除法中余式的次数。

定理5.2.3的证明

- 证明：如果$f(x), g(x)$有一个为零，比如说$g(x)=0$，则$a_n^{-1}f(x)$就是一个最大公因式，其中a_n为$f(x)$的首项系数，且有

$$a_n^{-1}f(x)=a_n^{-1}f(x)+1\cdot 0。$$

结论成立。

设$g(x)\neq 0$。根据带余除法，用$g(x)$除$f(x)$，得到商$q_1(x)$和余式$r_1(x)$；如果$r_1(x)\neq 0$，就再用$r_1(x)$除$g(x)$，得到商$q_2(x)$和余式$r_2(x)$；如果$r_2(x)\neq 0$，就再用$r_2(x)$除$r_1(x)$，得到商$q_3(x)$和余式$r_3(x)$；依次下去，所得余式的次数不断降低，即

$$deg(g(x))>deg(r_1(x))>deg(r_2(x))>\cdots$$

在有限次后，必然有余式为0。

定理5.2.3的证明（续）

- 于是有
- $$f(x)=q_1(x)g(x)+r_1(x), 0\le deg(r_1(x))<deg(g(x)),$$
$$g(x)=q_2(x)r_1(x)+r_2(x), 0\le deg(r_2(x))<deg(r_1(x)),$$
$$r_1(x)=q_3(x)r_2(x)+r_3(x), 0\le deg(r_3(x))<deg(r_2(x)),$$
$$\vdots$$
$$r_{l-2}(x)=q_l(x)r_{l-1}(x)+r_l(x), 0\le deg(r_l(x))<deg(r_{l-1}(x)),$$
$$r_{l-1}(x)=q_{l+1}(x)r_l(x)$$
- 根据定理前的说明，$r_l(x)$与0的最大公因式为$r_l(x)$；$r_l(x)$是$r_{l-1}(x)$和$r_l(x)$的最大公因式，同理以此类推，$r_l(x)$是$f(x)$和$g(x)$的最大公因式。

定理5.2.3的证明（续）

- 由上面的倒数第二个式子，可得

$$r_l(x)=r_{l-2}(x)-q_l(x)r_{l-1}(x)。$$

再由倒数第三个式子，可得$r_{l-1}(x)=r_{l-3}(x)-q_{l-1}(x)r_{l-2}(x)$，代入上式可得

$$r_l(x)=(1+q_l(x)q_{l-1}(x))r_{l-2}(x)-q_l(x)r_{l-3}(x)。$$

依次类推，可找到$u(x),v(x)\in F[x]$，使得

$$d(x)=r_l(x)=u(x)f(x)+v(x)g(x)。$$

定理中所使用的方法也称为辗转相除法。

求最大公因式例子

- **例5.2.1** 求$\mathbf{Z}_2[\mathbf{x}]$中的多项式$x^5+x^4+x^3+x^2+x+1$和x^4+x^2+x+1的最大公因式，并将最大公因式表示成这两个多项式的组合。

$q_2(x)=x^2+x$	$x^4 \quad +x^2+x+1$ x^4+x^3	$x^5+x^4+x^3+x^2+x+1$ $x^5 \quad +x^3+x^2+x$	$q_1(x)=x+1$
	x^3+x^2+x+1 x^3+x^2	$x^4 \quad +1$ $x^4 \quad +x^2+x+1$	
	$r_2(x)=x+1$	$r_1(x)=x^2+x$ x^2+x	$q_3(x)=x$
		0	

$$x+1=(x^5+x^4+x^3+x^2+x+1,x^4+x^2+x+1)$$

例5.2.1（续）

- 为了将**x+1**表示成$x^5+x^4+x^3+x^2+x+1$和x^4+x^2+x+1的组合，可将上述竖式写成横式：

$$
\begin{aligned}
&x^5+x^4+x^3+x^2+x+1=(x+1)(x^4+x^2+x+1)+x^2+x\\
&x^4+x^2+x+1=(x^2+x)(x^2+x)+x+1\\
&x^2+x=x(x+1).
\end{aligned}
$$

$$
\begin{aligned}
x+1&=x^4+x^2+x+1+(x^2+x)(x^2+x)\\
&=x^4+x^2+x+1+(x^2+x)[(x^5+x^4+x^3+x^2+x+1)+(x+1)(x^4+x^2+x\\
&=(x^2+x)(x^5+x^4+x^3+x^2+x+1)+(x^3+x+1)(x^4+x^2+x+1).
\end{aligned}
$$

多项式互素

- 定义5.2.3 如果**F[x]**中的多项式$f(x)$和$g(x)$满足$(f(x),g(x))=1$，则称$f(x)$与$g(x)$互素。

定理5.2.4 **F[x]**中的两个多项式$f(x)$和$g(x)$互素的充要条件是存在$u(x),v(x)\in F[x]$，使得

$$u(x)f(x)+v(x)g(x)=1。$$

定理5.2.5 （1）若$\boldsymbol{gcd(f(x),g(x))=1}$，且$\boldsymbol{f(x)|g(x)h(x)}$，则有$\boldsymbol{f(x)|h(x)}$。

（2）若$\boldsymbol{f(x)|h(x)}$，$\boldsymbol{g(x)|h(x)}$，且$\boldsymbol{gcd(f(x),g(x))=1}$，则有$\boldsymbol{f(x)g(x)|h(x)}$。

不可约多项式

- 定义5.2.4 如果域F上的次数大于等于1的多项式p(x)不能分解为域F上的两个次数比p(x)低的多项式的乘积，则称p(x)为域F上的不可约多项式。换句话说，如果p(x)在F[x]中只有F中不等于0的元素c和cp(x)为因式，则称p(x)为域上的不可约多项式。
- 注：n次多项式p(x)为域上的不可约多项式当且仅当p(x)与次数比n小的多项式都互素。
- 定理5.2.6 设$p(x)$为域F上的不可约多项式，对于任意两个多项式$f(x),g(x)\in F[x]$，若$p(x)|f(x)g(x)$，则有

$$p(x)|f(x)\text{或}p(x)|g(x)。$$

不可约多项式

表1　$GF(2)[x]$五次以内的不可约多项式

0	1
1	x，$x+1$
2	x^2+x+1
3	x^3+x^2+1，x^3+x+1
4	$x^4+x^3+x^2+x+1$，x^4+x^3+1，x^4+x+1
5	$x^5+x^3+x^2+x+1$，$x^5+x^4+x^2+x+1$，$x^5+x^4+x^3+x+1$，$x^5+x^4+x^3+x^2+1$，x^5+x^3+1，x^5+x^2+1

因式分解唯一性定理

定理5.2.7（因式分解唯一性定理）域F上的任意次数大于等于1的多项式$f(x)$都可以表示成$F[x]$中一些不可约多项式的乘积。更进一步，若

$$f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_l(x)$$

是将$f(x)$分解成不可约多项式的积的两种形式，则一定有$s=l$且适当排序后有$p_i(x)=c_iq_i(x)$，其中$c_i(1\le i\le s)$是域F中不等于零的元素。

由因式分解唯一性定理，$F[x]$中的任何一个多项式$f(x)$都可以分解成如下形式

$$f(x)=cp_1^{r_1}(x)p_2^{r_2}(x)\cdots p_m^{r_m}(x),$$

其中c是$f(x)$的首项系数，$p_1(x),p_2(x),\cdots,p_m(x)$是不同的首项系数为1的不可约多项式，$r_1,r_2,\cdots,r_m$是正整数。该分解式称为$f(x)$的标准分解式。

多项式的分解

- 例5.2.2　分解$GF(2)[x]$上多项式：

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

- 由于$f(1)=0$，所以$f(x)$有因式$x+1$．运用多项式除法得

$$f(x) = (x+1)(x^4+x^2+1).$$

- 通过试探得

$$(x^4+x^2+1) = (x^2+x+1)^2.$$

- 故

$$f(x) = (x+1)(x^2+x+1)^2.$$

- 实际上在$GF(2)[x]$上有

$$(f(x)+g(x))^2 = (f(x))^2+(g(x))^2.$$

因此x^4+x^2+1也可这样分解：

$$x^4+x^2+1 = (x^2+x)^2+1 = (x^2+x)^2+1^2 = (x^2+x+1)^2.$$

多项式的根

定义5.2.5 设$f(x) \in F[x]$，且$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$，设$\alpha \in F$。在$f(x)$的表达式中用$\alpha$替代未定元$x$所得到的域$F$中的元素

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

称为$f(x)$当$x = \alpha$时的值，记为$f(\alpha)$。若$f(\alpha) = 0$，则称α是$f(x)$在域F中的一个根。

定理5.2.8（余元定理）设$f(x) \in F[x]$，$\alpha \in F$，则用一次多项式$x - \alpha$去除$f(x)$所得余式是域F中的元素$f(\alpha)$。

推论5.2.1 设$f(x) \in F[x]$，$\alpha \in F$，则α是$f(x)$的根的充要条件是$x - \alpha | f(x)$。

推论5.2.2 设$f(x) \in F[x]$，$deg(f(x)) = n$，则$f(x)$在F中最多n个两两相异的根。

感 谢 聆 听！

xynie@uestc.edu.cn