网络安全数学基础(二)

沈佳辰
jcshen@sei.ecnu.edu.cn

网络安全数学基础

第八章 多项式环

- 定义8.1 设R是一个环，则系数都是R中元素的多项式，即给定多项式$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$，若对$i = 0,1,\ldots,n$，都有$a_i \in R$，且$a_n \neq 0_R$，则称$f(x)$是**$\boldsymbol{R}$上的多项式**，$a_n$称为$f(x)$的首项系数。

- 定义8.1 设R是一个环，则系数都是R中元素的多项式，即给定多项式$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$，若对$i = 0,1,\ldots,n$，都有$a_i \in R$，且$a_n \neq 0_R$，则称$f(x)$是$\boldsymbol{R}$**上的多项式**，$a_n$称为$f(x)$的首项系数。

- n称为$f(x)$的**次数**，记作$\deg f$。

- 定义8.1 设R是一个环，则系数都是R中元素的多项式，即给定多项式$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，若对$i=0,1,\ldots,n$，都有$a_i\in R$，且$a_n\neq 0_R$，则称$f(x)$是**$\boldsymbol{R}$上的多项式**，$a_n$称为$f(x)$的首项系数。

- n称为$f(x)$的**次数**，记作$\deg f$。

- 若$a_n=1_R$，则称$f(x)$为首一多项式。

- 定理8.1 设R是一个环，在R上的多项式全体组成的集合$R[x]$上定义加法和乘法：对任意$f(x)=\sum_{i=0}^{n}a_ix^i$,$g(x)=\sum_{i=0}^{m}b_ix^i$,,

$$(f+g)(x)=\sum_{i=0}^{\max(m,n)}(a_i+b_i)x^i,$$

$$(fg)(x)=\sum_{k=0}^{n+m}(\sum_{i+j=k}a_ib_j)x^k,$$

其中未定义的a_i和b_i都为0，即若$n>m$，则$b_{m+1}=b_{m+2}=\cdots=b_n=0$，若$n<m$，则$a_{n+1}=a_{n+2}=\cdots=a_m=0$，此时$R[x]$关于加法和乘法构成环。

华东师范大学 EAST CHINA NORMAL UNIVERSITY

证明：对任意$f(x), g(x) \in R[x]$，显然有$(f+g)(x), (fg)(x) \in R[x]$，因此$R[x]$对加法和乘法都封闭。对任意$f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i, h(x) = \sum_{i=0}^{l} c_i x^i \in R[x]$，因此$\big((f+g)+h\big)(x) = \left(\sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i\right) + \sum_{i=0}^{l} c_i x^i = \sum_{i=0}^{\max(n,m,l)} ((a_i+b_i)+c_i) x^i = \sum_{i=0}^{\max(n,m,l)} (a_i + (b_i + c_i)) x^i = \sum_{i=0}^{n} a_i x^i + \left(\sum_{i=0}^{\max(m,l)} (b_i + c_i) x^i\right) = (f + (g+h))(x)$，因此加法有结合律，类似可证乘法也有结合律，所以$R[x]$对加法和乘法都构成半群。

又因为$(f+g)(x)=\sum_{i=0}^{\max(m,n)}(a_i+b_i)x^i=\sum_{i=0}^{\max(m,n)}(b_i+a_i)x^i$ $=(g+f)(x)$，因此加法有交换律。显然$0(x)=0\in R[x]$，且$(0+f)(x)=(f+0)(x)=f(x)$，所以$0(x)$是$R[x]$的加法单位元，令$(-f)(x)=\sum_{i=0}^{n}(-a_i)x^i$，则有$\big(f+(-f)\big)(x)=\big((-f)+f\big)(x)$ $=0=0(x)$，因此$(-f)(x)$是$f(x)$的加法逆元，所以$R[x]$关于加法构成交换群。可验证$\big((f+g)h\big)(x)=(fh+gh)(x)$以及$\big(f(g+h)\big)(x)=(fg+fh)(x)$，所以$R[x]$关于加法和乘法满足分配律，因此$R[x]$关于这两种运算构成环。

- 事实上，还可验证$1(x) = 1 \in R[x]$是$R[x]$的乘法单位元，因此$R[x]$是含幺环。

- 事实上，还可验证$1(x) = 1 \in R[x]$是$R[x]$的乘法单位元，因此$R[x]$是含幺环。

- 若R是交换环，则$R[x]$也是交换环。

- 事实上，还可验证$1(x) = 1 \in R[x]$是$R[x]$的乘法单位元，因此$R[x]$是含幺环。

- 若R是交换环，则$R[x]$也是交换环。

- 若R无零因子，则$R[x]$也没有零因子。因此若R是整环，则$R[x]$也是整环。

- 定义8.2 设R是一个整环，$f(x), g(x) \in R[x], g(x) \neq 0$，若存在$q(x) \in R[x]$，使得$f(x) = g(x)q(x)$，则称$f(x)$**能被**$g(x)$**整除**，或者$g(x)$**能整除**$f(x)$，记作$g(x) | f(x)$，否则称$f(x)$**不能被**$g(x)$**整除**，或者$g(x)$**不能整除**$f(x)$，记作$g(x) \nmid f(x)$。

- 定义8.2 设R是一个整环，$f(x), g(x) \in R[x], g(x) \neq 0$，若存在$q(x) \in R[x]$，使得$f(x) = g(x)q(x)$，则称$f(x)$**能被**$g(x)$**整除**，或者$g(x)$**能整除**$f(x)$，记作$g(x)|f(x)$，否则称$f(x)$**不能被**$g(x)$**整除**，或者$g(x)$**不能整除**$f(x)$，记作$g(x) \nmid f(x)$。

- 若$g(x)|f(x)$，称$f(x)$为$g(x)$的**倍式**，$g(x)$为$f(x)$的**因式**。

- 定义8.3 给定$f(x) \in R[x]$，若存在$g(x) \in R[x]$，使得$g(x)|f(x)$，则称$f(x)$是**合式**，若不存在这样的多项式，则称$f(x)$是**既约多项式**。

- 例 因为$x^3 - 1 = (x-1)(x^2 + x + 1)$，所以$(x-1)|(x^3 - 1)$，$x-1$是$x^3-1$的因式。

- 例 因为$x^3-1=(x-1)(x^2+x+1)$，所以$(x-1)|(x^3-1)$，$x-1$是x^3-1的因式。

- 例 在Z_2上，$x^2+1=(x+1)^2$，所以$(x+1)|(x^2+1)$，x^2+1是$x+1$的倍式，因此x^2+1在Z_2上不是既约多项式。

- 例 因为$x^3-1=(x-1)(x^2+x+1)$，所以$(x-1)|(x^3-1)$，$x-1$是x^3-1的因式。
- 例 在Z_2上，$x^2+1=(x+1)^2$，所以$(x+1)|(x^2+1)$，x^2+1是$x+1$的倍式，因此x^2+1在Z_2上不是既约多项式。
- x^2+1不可用于从F_2生成F_4。

- 定理8.2 对任意域F上两个多项式$f(x), g(x)$，$g(x) \neq 0$，则存在唯一$q(x), r(x) \in F[x], \deg r < \deg g$, 使得$f(x) = q(x)g(x) + r(x)$。$q(x)$称为$f(x)$被$g(x)$除所得的**不完全商**，$r(x)$称为$f(x)$被$g(x)$除所得的**余式**。

证明：若$\deg f < \deg g$，令$r(x) = f(x), g(x) = 0 \in F[x]$，则有$f(x) = q(x)g(x) + r(x)$且$\deg r < \deg g$，因此这样的$q(x), r(x)$存在。

华东师范大学
EAST CHINA NORMAL UNIVERSITY

证明：若$\deg f<\deg g$，令$r(x)=f(x), g(x)=0\in F[x]$，则有$f(x)=q(x)g(x)+r(x)$且$\deg r<\deg g$，因此这样的$q(x), r(x)$存在。若$\deg f\geq\deg g$，令$n=\deg f-\deg g\geq 0, q(x)=ab^{-1}x^n, r(x)=f(x)-q(x)g(x)$，其中$a, b$分别为$f(x), g(x)$的首项系数，则$\deg(qg)=\deg q+\deg g=\deg f-\deg g+\deg g=\deg f$，观察$qg$的首项系数为$ab^{-1}b=a$，因此$\deg r=\deg(f-qg)<\deg f$，因此存在这样的$q(x), r(x)$。

若存在$q'(x), r'(x) \in F[x], \deg r' < \deg g$，使得$f(x) = q'(x)g(x) + r'(x)$，则有$q'(x) = q(x), r'(x) = r(x)$。事实上若$q'(x) \neq q(x)$，则$\deg((q'-q)g) = \deg(q'-q) + \deg g \geq 0 + \deg g = \deg g$，而$\deg(r - r') \leq \max(\deg r, \deg r') < \deg g$，因此$\deg(r - r') < \deg((q'-q)g)$，但由$q'(x)g(x) + r'(x) = q(x)g(x) + r'(x)$可知$(q'-q)(x)g(x) = (r - r')(x)$，矛盾，所以$q'(x) = q(x)$，由此可得$r'(x) = f(x) - q'(x)g(x) = f(x) - q(x)g(x) = r(x)$，唯一性得证。

- 定义8.4 给定环R上两个多项式$f(x), g(x)$，若$d(x) \in R[x]$满足$d(x)|f(x), d(x)|g(x)$，且对任意$h(x) \in R[x]$，若$h(x)|f(x), h(x)|g(x)$，则有$h(x)|d(x)$，那么称$d(x)$为$f(x)$和$g(x)$的**最大公因式**。

- 定义8.4 给定环R上两个多项式$f(x), g(x)$，若$d(x) \in R[x]$满足$d(x)|f(x), d(x)|g(x)$，且对任意$h(x) \in R[x]$，若$h(x)|f(x), h(x)|g(x)$，则有$h(x)|d(x)$，那么称$d(x)$为$f(x)$和$g(x)$的**最大公因式**。

- 若$d(x)$和$d'(x)$都是$f(x), g(x)$的最大公因式，则显然$d(x)|d'(x)$且$d'(x)|d(x)$。

- 若R是域，设a和a'分别为$d(x)$和$d'(x)$的首项系数，则显然$a^{-1}d(x)$也是$f(x),g(x)$的最大公因式，且$a'a^{-1}d(x)=d'(x)$，所以$f(x),g(x)$的最大公因式在忽略非零常数因子的意义下是唯一的，一般将这些最大公因式中首项系数为1的作为它们的代表，记作$(f(x),g(x))$。

- 定义8.5 给定域F上两个多项式$f(x), g(x)$，若$\big(f(x), g(x)\big) = 1$，则称$f(x)$和$g(x)$互素。

- 例 取F_2上多项式$f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1, g(x) = x^8 + x^4 + x^3 + x + 1$，由辗转相除法可求得$\left(f(x), g(x)\right) = 1$。

- 辗转相除法

  对任意域F上多项式$f(x), g(x), \deg g \geq 1$，令$r_0 = f(x), r_1 = g(x)$，反复使用带余除法，则有

$$
\begin{aligned}
r_0(x) &= r_1(x)q_1(x) + r_2(x), && 0 \leq \deg r_2 < \deg r_1 \\
r_1(x) &= r_2(x)q_2(x) + r_3(x), && 0 \leq \deg r_3 < \deg r_2 \\
&\vdots \\
r_{n-2}(x) &= r_{n-1}(x)q_{n-1}(x) + r_n(x), && 0 \leq \deg r_n < \deg r_{n-1} \\
r_{n-1}(x) &= r_n(x)q_n(x) + r_{n+1}(x), && r_{n+1}(x) = 0
\end{aligned}
$$

  经过有限次带余除法后，必然可得$r_{n+1}(x) = 0$，则$\big(f(x), g(x)\big) = a^{-1}r_n(x)$，其中$a$为$r_n(x)$的首项系数。

- 类似于整数上的辗转相除法，我们有

- 定理8.3 对任意域F上多项式$f(x), g(x), \deg g \geq 1$，存在$s(x), t(x) \in F[x]$，使得
$$s(x)f(x) + t(x)g(x) = (f(x), g(x))$$

- 例 上例中，对F_2上多项式$f(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1, g(x)=x^8+x^4+x^3+x+1$，已求得$\left(f(x),g(x)\right)=1$，由辗转相除法进一步可求得$s(x)=x^5+x^3, t(x)=x^{10}+x^6+x^4+x^3+x^2+x+1$，使得$s(x)f(x)+t(x)g(x)=\left(f(x),g(x)\right)=1$。

实验4

- 有限域的构造
  - 随机取10以内的素数p和3至10之间的正整数n。
  - 搜索F_p上的一个n次极小多项式$p(x)$。
  - 基于$p(x)$构造有限域F_{p^n}，并找出它的一个生成元α。
  - 将F_{p^n}所有非零元都分别用α的幂和F_p上次数不超过n的多项式的形式。
- 要求：输出$p(x), \alpha, \alpha$的幂与多项式的对应表
- 语言：C/C++或Python
- 使用头歌平台搭建环境并提交作业