華東師範大學
EAST CHINA NORMAL UNIVERSITY

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

第七章 环和域

§7.1 环

- 第六章讨论了带一种运算的代数结构，并给出了群的概念，但是在日常生活中，我们接触到的代数结构通常都是带两种运算的，例如全体整数的集合Z上，我们定义了加法和乘法（减法和除法分别是加法和乘法的逆运算），再如在矩阵上，我们也定义了加法和乘法，类似群，我们在带两种运算的代数结构上给出环（和域）的概念。

- 定义7.1.1 设$(R,+,\cdot)$是定义了两种运算的代数结构，我们称它构成**环**，如果

  (i) $(R,+)$是交换群；

  (ii) $(R,\cdot)$是半群；

  (iii) R关于两种运算满足结合律，即对任意$a,b,c\in R$，都有$(a+b)c=ac+bc, a(b+c)=ab+ac$。

- 定义7.1.1 设$(R,+,\cdot)$是定义了两种运算的代数结构，我们称它构成**环**，如果

  (i) $(R,+)$是交换群；

  (ii) $(R,\cdot)$是半群；

  (iii) R关于两种运算满足结合律，即对任意$a,b,c\in R$，都有$(a+b)c=ac+bc, a(b+c)=ab+ac$。

- 类似于群和半群的定义，定义7.1.1隐含了$(R,+,\cdot)$关于两种运算都是封闭的。

- 例 全体整数集合Z是环，0是其加法单位元，一般称为整数环。

- 例 n阶方阵全体构成环，零矩阵是其加法单位元。

- 例 整系数多项式全体构成环，零多项式是其加法单位元。

- 定理7.1.1 设$(R,+,\cdot)$是一个环，0是其加法单位元，则对任意$a,b\in R, n\in Z$，都有

  (i) $0a=a0=0$；

  (ii) $(-a)b=a(-b)=-(ab)$；

  (iii) $(-a)(-b)=ab$；

  (iv) $(na)b=a(nb)=n(ab)$；

  (v) 对任意$a_1,a_2,\ldots,a_m\in R, b_1,b_2,\ldots,b_l\in R$，都有

$(\sum_{i=1}^{m} a_i)\left(\sum_{j=1}^{l} b_j\right)=\sum_{i=1}^{m}\sum_{j=1}^{l} a_i b_j$。

证明：(i) 因为$0a+0a=(0+0)a=0a$，因此$0a=0a+0=0a+0a-0a=0a-0a=0$，类似可得$a0=0$。

证明：(i) 因为$0a+0a=(0+0)a=0a$，因此$0a=0a+0=0a+0a-0a=0a-0a=0$，类似可得$a0=0$。

思考：不能用$0a+a=0a+1a=(0+1)a=a$进一步得$0a=0$，为什么？

证明：(i) 因为$0a+0a=(0+0)a=0a$，因此$0a=0a+0=0a+0a-0a=0a-0a=0$，类似可得$a0=0$。

(ii) 因为$(-a)b+ab=(-a+a)b=0b=0$，所以$(-a)b=-ab$，类似可得$a(-b)=-ab$。

证明：(i) 因为$0a+0a=(0+0)a=0a$，因此$0a=0a+0=0a+0a-0a=0a-0a=0$，类似可得$a0=0$。

(ii) 因为$(-a)b+ab=(-a+a)b=0b=0$，所以$(-a)b=-ab$，类似可得$a(-b)=-ab$。

(iii) 因为$(-a)b+(-a)(-b)=(-a)(b-b)=(-a)0=0$，所以$(-a)(-b)=-\left((-a)b\right)=-(-ab)=ab$。

華東師範大學
EAST CHINA NORMAL UNIVERSITY

证明：(i) 因为$0a+0a=(0+0)a=0a$，因此$0a=0a+0=0a+0a-0a=0a-0a=0$，类似可得$a0=0$。

(ii) 因为$(-a)b+ab=(-a+a)b=0b=0$，所以$(-a)b=-ab$，类似可得$a(-b)=-ab$。

(iii) 因为$(-a)b+(-a)(-b)=(-a)(b-b)=(-a)0=0$，所以$(-a)(-b)=-\big((-a)b\big)=-(-ab)=ab$。

(iv) $(na)b=\left(\underbrace{a+a+\cdots+a}_{n\text{个}}\right)b=\underbrace{ab+ab+\cdots+ab}_{n\text{个}}=nab$，类似可得$a(nb)=nab$。

$$(v)\ \sum_{i=1}^{m}\sum_{j=1}^{l} a_i b_j = \begin{array}{cccc} a_1 b_1 & +a_1 b_2 & \cdots & +a_1 b_l \\ +a_2 b_1 & +a_2 b_2 & \cdots & +a_2 b_l \\ \vdots & \vdots & & \vdots \\ +a_m b_1 & +a_m b_2 & \cdots & +a_m b_l \end{array} =$$

$a_1(b_1 + b_2 + \cdots + b_l) + a_2(b_1 + b_2 + \cdots + b_l) + \cdots + a_m(b_1 + b_2 + \cdots + b_l) = (a_1 + a_2 + \cdots + a_m)(b_1 + b_2 + \cdots + b_l) = (\sum_{i=1}^{m} a_i)\left(\sum_{j=1}^{l} b_j\right)$。

- 定义7.1.2 设$(R,+,\cdot)$是一个环，
  (i) 如果$(R,\cdot)$是含幺半群，那么$(R,+,\cdot)$称为含幺环；
  (ii)如果$(R,\cdot)$满足交换律，那么$(R,+,\cdot)$称为交换环。

- 例 全体整数集合Z是含幺环，1是其乘法单位元，而且它是交换环。

- 例 n阶方阵全体构成含幺环，n阶单位阵是其乘法单位元，但它不是交换环。

- 例 整系数多项式全体构成含幺环，1是其乘法单位元，它也是交换环。

- 定义7.1.3 设 $(R,+,\cdot)$ 是一个环，如果存在 $a,b\in R, a,b\neq 0$，使得$ab=0$，那么称a是环R的**左零因子**，称b是环R的**右零因子**，如果a既是环R的左零因子，又是环R的右零因子，那么称它是环R的**零因子**。

- 定义7.1.3 设 $(R,+,\cdot)$ 是一个环，如果存在 $a,b\in R, a,b\neq 0$，使得$ab=0$，那么称a是环R的**左零因子**，称b是环R的**右零因子**，如果a既是环R的左零因子，又是环R的右零因子，那么称它是环R的**零因子**。

- 交换环的所有左（右）零因子都是零因子。

- 定义7.1.4 设$(R, +, \cdot)$是一个含幺交换环，如果它没有零因子，那么称它是一个**整环**。

- 例 整数环是整环。

- 例 整数环是整环。

- 例 整系数多项式环是整环。

- 例 整数环是整环。

- 例 整系数多项式环是整环。

- 例 n阶方阵全体构成的含幺环不是整环，它不仅是非交换环，它还含有零因子。

- 例 整数环是整环。

- 例 整系数多项式环是整环。

- 例 n阶方阵全体构成的含幺环不是整环，它不仅是非交换环，它还含有零因子。

- 例 $Z_6 = \{0,1,2,3,4,5\}$关于模6加法和模6乘法构成含幺交换环，但是它不是整环，因为$2 \cdot 3 = 0$，它包含零因子。

华东师范大学
EAST CHINA NORMAL UNIVERSITY

- 若R是整环，那么它关于乘法满足消去率，即对任意$a, b, c \in R, a \neq 0$，如果$ab = ac$，则有$b = c$。

- 设R是整环，那么它关于乘法满足消去率，即对任意$a, b, c \in R, a \neq 0$，如果$ab = ac$，则有$b = c$。

证明：因为$ab = ac$，所以$ab - ac = 0$，由分配律可知$a(b - c) = 0$，由于R是整环，因此它没有零因子，所以必有$a = 0$或$b - c = 0$，但题设$a \neq 0$，因此$b - c = 0$，即$b = c$。

- 定义7.1.5 设R是一个环，若存在$n \in Z^+$，使得对任意$a \in R$，都有$na = 0$，且对任意$n' \in Z^+, n' < n$，存在$a' \in R$，使得$n'a' \neq 0$（即n是使得对任意$a \in R$，$na = 0$都成立的最小正整数），则n称为R的**特征**，若不存在这样的n，则称R的**特征**为0。

- 例 全体整数集合Z是一个环，其特征为0，因为对任意$a \in Z, a \neq 0, n \in Z^{+}$，$na = 0$都不成立。
- $5Z$是Z的子环，其特征也为0。
- Z_5是一个环，其特征为5。

- 有限环的特征必不等于0。

- 有限环的特征必不等于0。

证明：对任意特征为0的有限环R，任意$a \in R$，都有$a, 2a, 3a, \ldots$两两不等，否则存在$k, m \in Z^{+}, k < m$，使得$ka = ma$，则有$(m-k)a = ma - ka = 0$，但$m - k \in Z^{+}$，与R的特征等于0矛盾，因此$a, 2a, 3a, \ldots$两两不等，又由R是环可知$(R, +)$是一个群，因为$a \in R$，所以$a, 2a, 3a, \ldots \in R$，与R是有限环矛盾，所以不存在特征为0的有限环。

- 定理7.1.2 设R是含幺环，且其特征c不为0，则c是使$n1_R = 0$成立的最小正整数，其中1_R是R的乘法单位元。

- 定理7.1.2 设R是含幺环，且其特征c不为0，则c是使$n1_R = 0$成立的最小正整数，其中1_R是R的乘法单位元。

证明：令c'是使$n1_R = 0$成立的最小正整数，因为R的特征c不为0，因此c'存在，显然有$c' \leq c$，仅需证明$c \leq c'$。事实上，对任意$a \in R$，由定理7.1.1 (iv)可知$c'a = c'(1_R a) = (c'1_R)a = 0a = 0$，因此$c \leq c'$。

- 定理7.1.3 设R是含幺环，且对$a, b \in R$，有$ab = ba$，则对任意$n \in Z^+$，有$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$。

证明：用数学归纳法，$n=1$时，$(a+b)^n=a+b=\binom{1}{0}a^0b^1+\binom{1}{1}a^1b^0=\sum_{i=0}^{n}\binom{n}{i}a^ib^{n-i}$成立，设$n=k$时结论成立，即$(a+b)^k=\sum_{i=0}^{k}\binom{k}{i}a^ib^{k-i}$成立，则$n=k+1$时，$(a+b)^{k+1}=$

$(a+b)^k(a+b)=\left(\sum_{i=0}^{k}\binom{k}{i}a^ib^{k-i}\right)(a+b)=$

$\sum_{i=0}^{k}\binom{k}{i}a^{i+1}b^{k-i}+\sum_{i=0}^{k}\binom{k}{i}a^ib^{k-i+1}=$

$\sum_{i=1}^{k+1}\binom{k}{i-1}a^ib^{k-i+1}+\sum_{i=0}^{k}\binom{k}{i}a^ib^{k-i+1}=\binom{k}{k}a^{k+1}b^0+$

$\sum_{i=1}^{k}\binom{k}{i-1}a^ib^{k-i+1}+\sum_{i=1}^{k}\binom{k}{i}a^ib^{k-i+1}+\binom{k}{0}a^0b^{k+1}=$

$$\binom{k+1}{k+1}a^{k+1}b^0+\sum_{i=1}^{k}(\binom{k}{i-1}+\binom{k}{i})a^i b^{k-i+1}+\binom{k}{0}a^0 b^{k+1}=$$

$$\binom{k+1}{k+1}a^{k+1}b^0+\sum_{i=1}^{k}\binom{k+1}{i}a^i b^{k-i+1}+\binom{k}{0}a^0 b^{k+1}=$$

$\sum_{i=0}^{k+1}\binom{k+1}{i}a^i b^{k+1-i}$成立，得证。

$\binom{k+1}{k+1}a^{k+1}b^0+\sum_{i=1}^{k}(\binom{k}{i-1}+\binom{k}{i})a^ib^{k-i+1}+\binom{k}{0}a^0b^{k+1}=$
$\binom{k+1}{k+1}a^{k+1}b^0+\sum_{i=1}^{k}\binom{k+1}{i}a^ib^{k-i+1}+\binom{k}{0}a^0b^{k+1}=$
$\sum_{i=0}^{k+1}\binom{k+1}{i}a^ib^{k+1-i}$成立，其中$\binom{k}{i-1}+\binom{k}{i}=$
$\frac{k!}{(i-1)!(k-i+1)!}+\frac{k!}{i!(k-i)!}=\frac{k!}{(i)!(k-i+1)!}\big(i+(k-i+1)\big)=$
$\frac{k!}{(i)!(k-i+1)!}(k+1)=\frac{(k+1)!}{(i)!(k-i+1)!}=\binom{k+1}{i}$。

- 定理7.1.4 设含幺交换环R的特征是素数p，则对任意$a, b \in R$，有$(a+b)^p = a^p + b^p$。

- 定理7.1.4 设含幺交换环R的特征是素数p，则对任意$a,b\in R$，有$(a+b)^p = a^p + b^p$。

证明：由于对$i=1,2,\dots,p-1$，$\binom{p}{i}=\frac{p!}{i!(p-i)!}$，由于$p$是素数，因此$p\nmid 1,2,\dots,p-1$，所以$p\nmid i!,(p-i)!$，但显然有$p|p!$，所以$p|\binom{p}{i}$，所以存在$k_1,k_2,\dots,k_{p-1}\in Z^+$，使得$\binom{p}{i}=k_ip, i=1,2,\dots,p-1$，又由定理7.1.2可知$(a+b)^p = \sum_{i=0}^{p}\binom{p}{i}a^ib^{p-i}$
$= a^p+\sum_{i=1}^{p-1}\binom{p}{i}a^ib^{p-i}+b^p = a^p+\sum_{i=1}^{p-1}k_i(pa^i)b^{p-i}+b^p$
$=a^p+\sum_{i=1}^{p-1}k_i(0)b^{p-i}+b^p = a^p+0+b^p = a^p+b^p$。

§7.2 环同态和理想

- 第六章给出了群同态和群同构，类似地，也有环同态和环同构。

- 定义7.2.1 设$(R,+,\cdot)$和$(R',\oplus,\otimes)$是两个环，如果映射$f: R\rightarrow R'$满足对任意$a,b\in H$，都有$f(a)\oplus f(b)=f(a+b), f(a)\otimes f(b)=f(a\cdot b)$，那么称$f$是$R$到$R'$的一个**环同态**。当$f$是单射时，称它是**单同态**；当$f$是满射时，称它是**满同态**；当$f$是一一映射时，称它是**同构**，此时称$R$和$R'$**环同构**。

- 定义7.2.2 设$(R,+,\cdot)$是环，H是R的非空子集，如果$(H,+,\cdot)$也是环，那么称H是R的**子环**。

- 定义7.2.2 设$(R,+,\cdot)$是环，H是R的非空子集，如果$(H,+,\cdot)$也是环，那么称H是R的**子环**。

- 例 全体整数集合Z是一个环，它的子集$nZ,n\in Z$是它的子环。

- 定义7.2.2 设$(R,+,\cdot)$是环，H是R的非空子集，如果$(H,+,\cdot)$也是环，那么称H是R的**子环**。

- 例 全体整数集合Z是一个环，它的子集$nZ, n\in Z$是它的子环。

- 例 全体n阶方阵是一个环，全体n阶非奇异方阵是它的子集，且它关于矩阵的加法和乘法也构成一个环，因此全体n阶非奇异方阵是全体n阶方阵的子环。

- 定义7.2.3 设R是环，I是R的子环，如果对任意$a \in I, r \in R$，都有$ra \in I$，那么称I是R的**左理想**；如果对任意$a \in I, r \in R$，都有$ar \in I$，那么称I是R的**右理想**。如果R的子环I既是R的左理想，又是R的右理想，那么称它是R的**理想**。

- 定义7.2.3 设R是环，I是R的子环，如果对任意$a \in I, r \in R$，都有$ra \in I$，那么称I是R的**左理想**；如果对任意$a \in I, r \in R$，都有$ar \in I$，那么称I是R的**右理想**。如果R的子环I既是R的左理想，又是R的右理想，那么称它是R的**理想**。

- 例 $\{0\}$和R显然都是R的子环，也是R的理想，它们称为**平凡理想**。

- 定理7.2.1 设R是环，I是R的非空子集，则I是R的左（右）理想的充要条件是
  (i) 对任意$a, b \in I$，都有$a - b \in I$；
  (ii) 对任意$r \in R, a \in I$，都有$ra \in I$（$ar \in I$）。

证明：必要性显然，下面证明充分性，我们只证明左理想的情形，类似可得右理想的情形。

由 (i) 和定理6.1.6可知，$(I,+)$ 是 $(R,+)$ 的子群，即 $(I,+)$ 是群；由(ii)可知，对任意$a\in I, b\in I\subseteq R$，有$ba\in I$，因此$I$关于运算$\cdot$封闭，因为$(R,+,\cdot)$是环，因此$R$关于$\cdot$有结合律，因此$I$关于$\cdot$有结合律，所以$(I,\cdot)$是半群；又因为$(R,+,\cdot)$是环，因此$R$关于$+$和$\cdot$有分配律，因此$I$关于$+$和$\cdot$有分配律，所以$(I,+,\cdot)$是环，因此$I$是$R$的子环，再结合$(ii)$可知，$I$是$R$的左理想。

- 定理7.2.2 设R是环，$A_1, A_2, \ldots, A_n$是R的左（右）理想，则$\bigcap_{i=1}^{n} A_i$也是R的左（右）理想。

- 定理7.2.2 设R是环，$A_1, A_2, \dots, A_n$是R的左（右）理想，则$\bigcap_{i=1}^{n} A_i$也是R的左（右）理想。

证明：我们只证明左理想的情形。

对任意$a, b \in \bigcap_{i=1}^{n} A_i, r \in R$，则对任意$i = 1,2, \dots n$，都有$a, b \in A_i$，因为$A_i$是$R$的左理想，则由定理7.2.1可知$a - b \in A_i, ra \in A_i$，所以$a - b \in \bigcap_{i=1}^{n} A_i, ra \in \bigcap_{i=1}^{n} A_i$，再由定理7.2.1，我们有$\bigcap_{i=1}^{n} A_i$是$R$的左理想。

- 定义7.2.4 设R是环，X是R的非空子集，设$\{H_i | i \in I\}$是R的所有包含X的理想，则$\bigcap_{i \in I} H_i$称为X**生成的理想**，记为(X)。如果$|X|$有限，则称(X)是**有限生成**的，特别的，如果$X = \{x\}$，则称$\bigcap_{i \in I} H_i$ 为R的**主理想**。如果R的所有理想都是主理想，那么称R为**主理想环**。

- 例 所有整数集合Z是一个主理想环，因为它的所有子环$nZ, n \in Z$，都是主理想，事实上$nZ = (n)$。

- 定理7.2.3 设R是环，$a \in R$，则

(i) $(a) = \{ra + ar' + na + \sum_{i=1}^{m} r_i a s_i \,|r, r', r_i, s_i \in R, n \in Z, m \in Z^+\}$

(ii) 如果R是含幺环，则$(a) = \{\sum_{i=1}^{m} r_i a s_i \,|r_i, s_i \in R, m \in Z^+\}$

(iii) 如果$a \in C(R) = \{r \in R|$对任意$x \in R$，都有$xr = rx\}$则 $(a) = \{ra + na|r \in R, n \in Z\}$

(iv) Ra（aR）是R的左（右）理想。

证明：仅需证明$I=\{ra+ar'+na+\sum_{i=1}^{m}r_i as_i \mid r,r',r_i,s_i\in R,n\in Z,m\in Z^+\}$是包含$a$的理想，且任意包含$a$的理想$A$，都有$I\subseteq A$。

令$r=r'=r_i=s_i=0_R,m=1,n=1$，则有$a\in I$。对任意$x\in R$，有$x(ra+ar'+na+\sum_{i=1}^{m}r_i as_i)=(xr)a+xar'+(nx)a+\sum_{i=1}^{m}(xr_i)as_i=r^{(1)}a+ar'^{(1)}+n^{(1)}a+\sum_{i=1}^{m^{(1)}}r_i^{(1)}as_i^{(1)}\in R$，其中$r^{(1)}=xr+nx\in R,r'^{(1)}=0_R\in R,n^{(1)}=0\in Z,m^{(1)}=m+1\in Z^+,r_{m+1}^{(1)}=x,s_{m+1}^{(1)}=r',r_i^{(1)}=xr_i,s_i^{(1)}=s_i,i=1,2,\dots,m$，所以$I$是$R$的左理想，类似可证$I$是$R$的右理想，因此$I$是$R$的包含$a$的理想。

因为A是包含a的理想，因此对任意$r, s \in R$，都有$ra, as \in A$，又因为A是R的理想，所以A是R的子环，因此A关于$+$和$\cdot$都是封闭的，由此可得$I \subseteq A$。因此$I = (a)$。

因为A是包含a的理想，因此对任意$r, s \in R$，都有$ra, as \in A$，又因为A是R的理想，所以A是R的子环，因此A关于$+$和$\cdot$都是封闭的，由此可得$I \subseteq A$。因此$I = (a)$。

由(i)易证(ii)、(iii)成立。

因为A是包含a的理想，因此对任意$r, s \in R$，都有$ra, as \in A$，又因为A是R的理想，所以A是R的子环，因此A关于$+$和$\cdot$都是封闭的，由此可得$I \subseteq A$。因此$I = (a)$。

由(i)易证(ii)、(iii)成立。

(iv) 仍然只证左理想的情形。对任意$b, c \in Ra$，则存在$b', c' \in R$，使得$b = b'a, c = c'a$，由于R关于$+$构成一个群，所以$b' - c' \in R$，因此$b - c = b'a - c'a = (b' - c')a \in Ra$；对任意$b \in Ra$，则存在$b' \in R$，使得$b = b'a$，因此对任意$r \in R$，由于$R$关于$\cdot$封闭，所以$rb' \in R$，因此$rb = r(b'a) = (rb')a \in Ra$，由定理7.2.1可知$Ra$是$R$的左理想。

- 设R是环，则$(R,+)$是交换群，因此R的所有理想I关于$+$都是它的正规子群，由定理6.3.4可知，关于运算$+$的商集R/I关于运算$(a+I)+(b+I)=(a+b)+I$构成一个群，进一步由于$(R,+)$是交换群可知$(R/I,+)$也是交换群。再定义R/I上的$\cdot$后，我们发现理想的性质保证了R/I关于$\cdot$构成半群，并进一步可知R/I也是一个环。

- 定理7.2.4 设R是环，I是R的理想，在商集R/I上定义运算

$$(a+I)+(b+I)=(a+b)+I$$

$$(a+I)(b+I)=ab+I$$

则R/I构成一个环，称其为**商环**。如果R是含幺环（交换环），则R/I也是含幺环（交换环）。

证明：由定理6.3.4和R关于$+$的交换律可知$(R/I,+)$是交换群。接下来我们先证明R/I上这样定义的$\cdot$是一个映射，即对任意$a,b \in R, a' \in a+I, b' \in b+I$，都有$a'b' \in ab+I$。

证明：由定理6.3.4和R关于$+$的交换律可知$(R/I,+)$是交换群。接下来我们先证明R/I上这样定义的$\cdot$是一个映射，即对任意$a,b\in R, a'\in a+I, b'\in b+I$，都有$a'b'\in ab+I$。事实上，因为$a'\in a+I, b'\in b+I$，所以存在$x,y\in I$，使得$a'=a+x, b'=b+y$，因为$I$是$R$的理想，所以$xb, ay, xy\in R$，所以$a'b'=(a+x)(b+y)=ab+xb+ay+xy\in ab+I$。

证明：由定理6.3.4和R关于$+$的交换律可知$(R/I,+)$是交换群。接下来我们先证明R/I上这样定义的$\cdot$是一个映射，即对任意$a,b\in R,a'\in a+I,b'\in b+I$，都有$a'b'\in ab+I$。事实上，因为$a'\in a+I,b'\in b+I$，所以存在$x,y\in I$，使得$a'=a+x,b'=b+y$，因为$I$是$R$的理想，所以$xb,ay,xy\in R$，所以$a'b'=(a+x)(b+y)=ab+xb+ay+xy\in ab+I$。显然$R/I$关于运算$\cdot$是封闭的，我们再证明$R/I$关于运算$\cdot$满足结合律，对任意$a,b,c\in R$，$\big((a+I)(b+I)\big)(c+I)=(ab+I)(c+I)=(ab)c+I=a(bc)+I=(a+I)(bc+I)=(a+I)\big((b+I)(c+I)\big)$成立，因此$(R/I,\cdot)$是一个半群。

最后我们来证明R/I关于运算$+$和$\cdot$满足分配律，事实上，对任意$a,b,c\in R$，都有$\big((a+I)+(b+I)\big)(c+I)=\big((a+b)+I\big)(c+I)=(a+b)c+I=(ac+bc)+I=(ac+I)+(bc+I)=(a+I)(c+I)+(b+I)(c+I)$，类似可得$(a+I)\big((b+I)+(c+I)\big)=(a+I)(b+I)+(a+I)(c+I)$，因此分配律成立。所以$R/I$关于运算$+$和$\cdot$构成一个环。

华东师范大学 EAST CHINA NORMAL UNIVERSITY

最后我们来证明R/I关于运算$+$和$\cdot$满足分配律，事实上，对任意$a,b,c\in R$，都有$\big((a+I)+(b+I)\big)(c+I)=\big((a+b)+I\big)(c+I)=(a+b)c+I=(ac+bc)+I=(ac+I)+(bc+I)=(a+I)(c+I)+(b+I)(c+I)$，类似可得$(a+I)\big((b+I)+(c+I)\big)=(a+I)(b+I)+(a+I)(c+I)$，因此分配律成立。所以$R/I$关于运算$+$和$\cdot$构成一个环。

由R的含幺性和交换律易证R/I的含幺性和交换律，令1表示R的单位元，则易知$1+R$是R/I的单位元。

- 定理7.2.5（环同态基本定理）设R和R'是环，f是R到R'的环同态，则$\ker(f) = \{a \in R | f(a) = 0\}$是$R$的理想，且$R/\ker(f)$和$f(R)$同构。反之，若$I$是$R$的理想，则映射

$$
\begin{array}{llll}
s: & R & \to & R/I \\
 & a & \mapsto & a+I
\end{array}
$$

是R到R/I的同态映射，且$I = \ker(s)$，s称为R到R/I的**自然同态**。

证明：令$I' = \ker(f)$，定义映射$f' : \begin{array}{ccc} R/I' & \to & f(R) \\ a+I' & \mapsto & f(a) \end{array}$，则 $f\big((a+I')+(b+I')\big) = f'\big((a+b)+I'\big) = f(a+b) = f(a)+f(b) = f'(a+I')+f'(b+I')$，$f'((a+I')(b+I')) = f'(ab+I') = f(ab) = f(a)f(b) = f'(a+I')f'(b+I')$，因此$f'$是一个同态映射。

证明：令$I' = \ker(f)$，定义映射$\begin{array}{cccc} f': & R/I' & \to & f(R) \\ & a+I' & \mapsto & f(a) \end{array}$，则$f\big((a+I')+(b+I')\big) = f'\big((a+b)+I'\big) = f(a+b) = f(a)+f(b) = f'(a+I')+f'(b+I')$，$f'((a+I')(b+I')) = f'(ab+I') = f(ab) = f(a)f(b) = f'(a+I')f'(b+I')$，因此$f'$是一个同态映射。$f'$是满射显然，下面证明$f'$是单射，若存在$a, b \in R/I'$，使得$f'(a) = f'(b)$，则存在$a', b' \in R$，使得$a = a'+I', b = b'+I'$，且$f(a') = f(b')$，因此$f(a'-b') = f(a')-f(b') = 0$，因此$a'-b' \in \ker(f) = I'$，由定理6.3.1 (iii)可知$a'+I' = b'+I'$，即$a = b$，因此f'是单射，所以f'是同构映射。

对任意$a, b \in R$，有$s(a+b) = (a+b) + I = (a+I) + (b+I) = s(a) + s(b)$以及$s(ab) = ab + I = (a+I)(b+I) = s(a)s(b)$，因此$s$是同态映射。

对任意$a, b \in R$，有$s(a+b) = (a+b) + I = (a+I) + (b+I) = s(a) + s(b)$以及$s(ab) = ab + I = (a+I)(b+I) = s(a)s(b)$，因此$s$是同态映射。而$\ker(s) = \{a \in R | s(a) = 0\}$，对任意$x \in \ker(s)$，因为$s(x) = 0$，所以$x + I = 0 + I = I$，所以$x \in I$，因此$\ker(s) \subseteq I$；对任意$x \in I$，显然$x + I = I = 0 + I$，因此$s(x) = x + I = 0 + I = 0$，所以$I \subseteq \ker(s)$，所以$I = \ker(s)$。

华东师范大学 EAST CHINA NORMAL UNIVERSITY

- 例 nZ是Z的理想（也是Z的主理想），则映射

$$\begin{aligned} f:\quad Z &\rightarrow \quad Z \\ a &\mapsto \ a \bmod n \end{aligned}$$

是R到R/I的同态映射，且$nZ = \ker(f)$，再由定理7.2.5可知Z/nZ同构于$f(Z) = \{0,1,\dots,n-1\} = Z_n$，一般我们写成$Z/nZ = Z_n$，并由定理7.2.4可知$Z_n$也是一个含幺交换环。

§7.3 域

- 定义7.3.1 设F是环，如果$(F\backslash\{0\},\cdot)$也构成一个交换群，那么F称为**域**，$|F|$称为F的阶。

§7.3 域

- 定义7.3.1 设F是环，如果$(F\setminus\{0\},\cdot)$也构成一个交换群，那么F称为**域**，$|F|$称为F的阶。

- 显然域必是含幺环、交换环、整环。

- 例 全体整数集合Z不是域，事实上，除了1和-1之外，$Z\backslash\{0\}$中其它元素都没有乘法逆元。

- 例 全体整数集合Z不是域，事实上，除了1和-1之外，$Z\backslash\{0\}$中其它元素都没有乘法逆元。

- 例 Z_n是域当且仅当n是素数，当n是合数时，Z_n包含零因子，因此它不是域。

- 例 全体整数集合Z不是域，事实上，除了1和-1之外，$Z\backslash\{0\}$中其它元素都没有乘法逆元。

- 例 Z_n是域当且仅当n是素数，当n是合数时，Z_n包含零因子，因此它不是域。

- 例 全体实数集合R是域，它是一个无限域；全体有理数集合Q也是一个无限域。

- 定理7.3.1 设F是域，则其特征必为素数或0。

- 定理7.3.1 设F是域，则其特征必为素数或0。

证明：仅需证明若F的特征不为0，则必为素数。设F的特征为$c \neq 0$，由定理7.1.2可知c是使$n1_F = 0$成立的最小正整数，若其为合数，则存在$m, l \in Z^+, 0 < m, l < c$，使得$c = ml$，则由定理7.1.1$(iv)$可知$0 = c1_F = (ml)(1_F \cdot 1_F) = m\big(l(1_F \cdot 1_F)\big) = m\big(1_F \cdot (l1_F)\big) = (m1_F)(l1_F)$，由于$c$是使$n1_F = 0$成立的最小正整数，因此$m1_F, l1_F \neq 0$，所以$F$有零因子，与$F$是域矛盾，所以$c$不是合数，所以$c$是素数。

- 定理7.3.1 设F是域，则其特征必为素数或0。

证明：仅需证明若F的特征不为0，则必为素数。设F的特征为$c \neq 0$，由定理7.1.2可知c是使$n1_F = 0_F$成立的最小正整数，若其为合数，则存在$m, l \in Z^+, 0 < m, l < c$，使得$c = ml$，则由定理7.1.1$(iv)$可知$0_F = c1_F = (ml)(1_F \cdot 1_F) = m\big(l(1_F \cdot 1_F)\big) = m\big(1_F \cdot (l1_F)\big) = (m1_F)(l1_F)$，由于$c$是使$n1_F = 0_F$成立的最小正整数，因此$m1_F, l1_F \neq 0_F$，所以$F$有零因子，与$F$是域矛盾，所以$c$不是合数，所以$c$是素数。

。

- 定理7.3.1 设F是域，则其特征必为素数或0。

证明：仅需证明若F的特征不为0，则必为素数。设F的特征为$c \neq 0$，由定理7.1.2可知c是使$n1_F = 0_F$成立的最小正整数，若其为合数，则存在$m, l \in Z^+, 0 < m, l < c$，使得$c = ml$，则由定理7.1.1$(iv)$可知$0_F = c1_F = (ml)(1_F \cdot 1_F) = m\big(l(1_F \cdot 1_F)\big) = m\big(1_F \cdot (l1_F)\big) = (m1_F)(l1_F)$，由于$c$是使$n1_F = 0_F$成立的最小正整数，因此$m1_F, l1_F \neq 0_F$，所以$F$有零因子，与$F$是域矛盾，所以$c$不是合数；若$c = 1$，则有$1_F = 1 \cdot 1_F = 0_F$，矛盾；所以$c$是大于1的非合数，即$c$是素数。

- 定理7.3.2 设域F的特征为p，则对任意$a \in F, a \neq 0_F, m \in Z^+$，$ma = 0_F$当且仅当$p|m$。

- 定理7.3.2 设域F的特征为p，则对任意$a \in F, a \neq 0_F, m \in Z^+$，$ma = 0_F$当且仅当$p|m$。

证明：充分性显然，现证必要性。

存在$q, r \in Z^+, 0 \leq r < p$，使得$m = qp + r$因为$0_F = ma = m(1_F a) = (m1_F)a$，由于$F$是域，$a \neq 0_F$，所以$m1_F = 0_F$，所以$r1_F = (m - qp)1_F = m1_F - qp1_F = 0_F - q(p1_F) = 0_F - q0_F = 0_F$，又因为$p$是$F$的特征，由定理7.1.2可知$p$是使$n1_F = 0_F$成立的最小正整数，但$0 \leq r < p$，所以$r = 0$，即$p|m$。

- 定理7.3.3 设$q \in Z^+$，则阶为q的域都同构。数学上认为同构的域本质上是一样的，因此我们认为阶为q的域只有一个，记作$GF(q)$或F_q，我们也称有限域为**伽罗华域**（Galois field）。

- 例 设p为素数，则Z_p是一个域。由定理7.3.3可知，阶为p的域都与Z_p同构，我们一般写作$GF(p)=Z_p$。

- 定理7.3.4 有限域的阶必为素数幂，反之，任意素数幂阶的域都存在。

- 定理7.3.4 设F是一个域，F'是F的非空子集，若F'也是域，则称F'是F的**子域**，F是F'的**扩域**。

- 定义7.3.2 设F是一个域，F'是F的非空子集，若F'也是域，则称F'是F的**子域**，F是F'的**扩域**。

- 例 全体有理数集合Q是实数域R的非空子集，且Q也是域，因此Q是R的子域，R是Q的扩域。

- 定理7.3.5 设F是一个域，F'是它的扩域，则两者的特征相等。

- 定理7.3.5 设F是一个域，F'是它的扩域，则两者的特征相等。

证明：因为F是F'的子域，因此$(F,+)$是$(F',+)$的子群，则由定理6.1.5可知$0_F = 0_{F'}$，再由F是F'的子域可知$(F\backslash\{0_F\},\cdot)$是$(F'\backslash\{0_{F'}\},\cdot)$的子群，仍由定理6.1.5可知$1_F = 1_{F'}$，所以$n1_{F'} = 0_{F'}$和$n1_F = 0_F$解的情况相同，令$c'$为$F'$的特征，$c$为$F$的特征，由定理7.1.2可知$c' = c$。

- 定理7.3.6 设F是一个域，F'是它的扩域，则$0_F=0_{F'},1_F=1_{F'}$，且F可看作F'上的线性空间，该空间的维数记作$[F':F]$，如果$[F':F]$有限，则称F'是F的**有限扩张**，如果$[F':F]$无限，则称F'是F的**无限扩张**。

- 定理7.3.6 设F是一个域，F'是它的扩域，则$0_F = 0_{F'}, 1_F = 1_{F'}$，且$F$可看作$F'$上的线性空间，该空间的维数记作$[F':F]$，如果$[F':F]$有限，则称$F'$是$F$的**有限扩张**，如果$[F':F]$无限，则称$F'$是$F$的**无限扩张**。

- 例 复数域C是实数域R的扩域，且$[C:R] = 2$，因此C是R的有限扩张。

§7.4 有限域的构造

- 由定理7.3.4可知若$n \in Z^+, p$是素数，$q = p^n$是一个素数幂，则$GF(q)$存在，且所有有限域都可以写成$GF(q)$的形式，但是我们知道$n > 1$时，$Z_q = Z_{p^n}$不是域，那么$GF(q)$的结构是怎样的？

- 定理7.4.1 设$\boldsymbol{F}_q$是q元有限域，其特征p为素数，则$\boldsymbol{F}_q$是域$\boldsymbol{F}_p = \mathbf{Z}/p\mathbf{Z}$的扩域，设$n = [\boldsymbol{F}_q : \boldsymbol{F}_p]$，则$q = p^n$,即$q$是其特征$p$的幂。

- 定理7.4.2 设$\boldsymbol{F}_q$是q元有限域，则$\boldsymbol{F}_q^* = \boldsymbol{F}_q \backslash \{0\}$关于乘法是$q-1$阶循环群。

- 定义7.4.1 设$\boldsymbol{F}_q$是q元有限域，$g \in \boldsymbol{F}_q$，如果g是乘群$\boldsymbol{F}_q^*$的生成元，则称g为域$\boldsymbol{F}_q$的生成元。

- 定义7.4.1 设$\boldsymbol{F}_q$是q元有限域，$g \in \boldsymbol{F}_q$，如果g是乘群$\boldsymbol{F}_q^*$的生成元，则称g为域$\boldsymbol{F}_q$的生成元。

- 若g是有限域$\boldsymbol{F}_q$的生成元，则有$\boldsymbol{F}_q = \{0, g^0 = 1, g, \ldots, g^{q-2}\}$。

- 定义7.4.2 设F是一个域，F'是它的扩域，$a \in F'$，若存在F上的多项式$f(x)$，使得$f(a) = 0$，则称a是F上的**代数数**，若不存在这样的多项式，则称a是F上的**超越数**。

- 定义7.4.2 设F是一个域，F'是它的扩域，若对任意$a \in F'$，a都是F上的代数数，则称F'是F的**代数扩张**，若存在$a \in F'$，a是F上的超越数，则称F'是F的**超越扩张**。

- 定义7.4.2 设F是一个域，F'是它的扩域，若对任意$a \in F'$，a都是F上的代数数，则称F'是F的**代数扩张**，若存在$a \in F'$，a是F上的超越数，则称F'是F的**超越扩张**。

- 例 复数域C是实数域R的代数扩张，因为任意$c = a + bi \in C$，其中$a, b \in R$，c是$f(x) = (x - a)^2 + b^2 \in R[x]$的根，即$c$是$R$上的代数数。

- 定义7.4.2 设F是一个域，F'是它的扩域，若对任意$a \in F'$，a都是F上的代数数，则称F'是F的**代数扩张**，若存在$a \in F'$，a是F上的超越数，则称F'是F的**超越扩张**。

- 例 复数域C是实数域R的代数扩张，因为任意$c = a + bi \in C$，其中$a, b \in R$，c是$f(x) = (x - a)^2+b^2 \in R[x]$的根，即$c$是$R$上的代数数。

- 例 实数域R是有理数域Q的超越扩张，因为无理数（π, e等）是Q上的超越数。

- 定理7.4.3 设F是一个域，F'是它的扩域，$a \in F'$，若a是F上的代数数，则存在唯一F上的首一不可约多项式$f(x)$，使得$f(a) = 0$ 。$f(x)$称为a的**极小多项式**。

- 给定有限域F_p，有限域F_{p^n}的构造如下（p和q都是素数幂）：
  - 取F_p上的n次首一不可约多项式$p(x)$，则$p(x) \in F_p[x], \deg p = n$，$(p(x))$是$F_p[x]$的理想，在商环$F_p[x]/(p(x))$上定义加法和乘法：
$$(f+g)(x) = f(x) + g(x)\ mod\ p(x)$$
$$(fg)(x) = f(x)g(x)\ mod\ p(x)$$
  - 则$F_p[x]/(p(x))$关于这两种运算构成一个域，其阶为p^n。由定理7.3.4可知阶为p^n的域在同构的意义下有且仅有一个，即为F_{p^n}。

- 例 我们知道Z_2是一个域，容易验证$p(x) = x^3 + x + 1$是Z_2上的3次不可约多项式，因此$Z_2[x]/(x^3 + x + 1)$是8元域F_8。

- 例 我们知道Z_2是一个域，容易验证$p(x)=x^3+x+1$是Z_2上的3次不可约多项式，因此$Z_2[x]/(x^3+x+1)$是8元域F_8。具体来说，由定理7.4.2可知，$F_8\backslash\{0\}$关于乘法是一个循环群，因此若设$p(x)$是$\alpha\in F_8$的极小多项式，则

n	$\alpha^n \bmod p(\alpha)$
0	1
1	α
2	α^2
3	$\alpha+1$
4	$\alpha^2+\alpha$
5	$\alpha^2+\alpha+1$
6	α^2+1

华东师范大学 EAST CHINA NORMAL UNIVERSITY

- 例 我们知道Z_2是一个域，容易验证$p(x) = x^3 + x + 1$是Z_2上的3次不可约多项式，因此$Z_2[x]/(x^3 + x + 1)$是8元域F_8。具体来说，由定理7.4.2可知，$F_8\backslash\{0\}$关于乘法是一个循环群，因此若设$p(x)$是$\alpha \in F_8$的极小多项式，则

n	$\alpha^n \bmod p(\alpha)$
0	1
1	α
2	α^2
3	$\alpha + 1$
4	$\alpha^2 + \alpha$
5	$\alpha^2 + \alpha + 1$
6	$\alpha^2 + 1$

因此$F_8 = \{0,1,\alpha,\alpha^2,\alpha + 1\,, \alpha^2 + \alpha,\alpha^2 + \alpha + 1,\alpha^2 + 1\} \cong Z_2[x]/(x^3 + x + 1)$。