第三章 环与域

- 加群、环的定义
- 交换律、单位元、零因子、整环
- 除环、域
- 无零因子环的特征
- 子环、环的同态
- 多项式环
- 理想
- 剩余类环、同态与理想
- 最大理想
- 商域

§1. 环的定义

定义1.1. 对一个交换群, 若把这个群的代数运算叫做加法, 则称这个群为一个加群，并且用“+”来表示它的代数运算。

设$(G,+)$是一个加群，约定:

(i)$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n, \forall n \in \mathbb{Z}^+$, 以及$\forall a_1, a_2, \cdots, a_n \in G$;

(ii) 单位元记为0，称为零元;

(iii) $\forall a \in G$, a 的逆元用$-a$ 表示，并称之为a的负元;

$\forall a, b \in G$, 记$a + (-b) = a - b$;

(iv) $\forall a \in G, \forall n \in \mathbb{Z}^+$, 符号$na$表示$n$个$a$的和，并称之为$a$的$n$倍(简称$n$倍$a$); 即$na = \underbrace{a + a + \cdots + a}_{n个}$; 而记

(v) $(-n)a = -(na)$.规定$0a = 0$.

回忆：加群的一个非空子集 s 是一个子群的充分必要条件为：

$$\begin{cases} 1.\ \forall a, b \in \mathrm{S}, \text{有} a + b \in S; \\ 2.\ \forall a \in \mathrm{S}, \text{有} -a \in S. \end{cases}$$

或者，等价的有：

$\forall a, b \in \mathrm{S}$, 有 $a - b \in S$.

定义1.2. 称一个集合 R 为环(ring)，假如

1、 R是个加群；
2、 R 对于一个叫做乘法的运算来说是封闭的；
3、乘法满足结合律；即

$$\forall a, b, c \in R, 有 a(bc) = (ab)c;$$

4、乘法与加法满足分配律，即

$$\forall a, b, c \in R, 有 \begin{cases} a(b+c) = ab + ac; (左) \\ (b+c)a = ba + bc. (右) \end{cases}$$

例： $\mathbb{Z}$关于数的加法、乘法构成一个环.

$M_n(F)$关于矩阵的加法、乘法构成一个环，

但是$GL_n(F)$、$SL_n(F)$都不构成环.

在环R里，还有如下运算规则：即$\forall a, b, c \in R, m, n \in Z$,有：

7. $(a-b)c = ac - bc$;　　$c(a-b) = ca - cb$;

特别的，有$0a = a0 = 0$.（其中0为R中零元）

8. $(-a)b = a(-b) = -ab$;　$(-a)(-b) = ab$;

9. $\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = a_1b_1 + \cdots + a_1b_n + \cdots + a_mb_1 + \cdots + a_mb_n$

$$= \sum_{i=1}^{m}\sum_{j=1}^{n} a_ib_j$$

10. $(na)b = a(nb) = n(ab)$.

$\forall a \in R, m, n \in Z^+$，若规定：

$$a^n = \underbrace{aa\cdots a}_{n\text{个}}$$

则有：

$$a^m a^n = a^{m+n}$$
$$(a^m)^n = a^{mn}$$

定义1.3.　称一个环R为交换环，假如

$$\forall a, b \in R, 有 ab = ba.$$

注：此时$\forall a, b \in R,$ 有$a^n b^n = (ab)^n.$

定义1.4.　环R的一个元 e 叫做一个单位元，假如

$$\forall a \in R, 有 ea = ae = a.$$

注：不是所有环都有单位元，如下例:

例: R ＝｛所有偶数｝， R 对于普通数的加法和乘法作成一个环，但 R没有单位元。

注: (单位元的唯一性) 一个环R如果有单位元, 则其单位元是唯一的。

证明：设R有两个单位元 e 和 e', 则有

$$ee' = e = e',$$

所以性质成立。

注: 一个环R中的单位元用 1 (或者1_R)表示，
且规定： $a^0 = 1, \forall a \in R.$

定义1.5.设R是有单位元的环，$a \in R$. 如果$\exists b \in R$,满足：

$$ab = ba = 1,$$ 则称b为a的逆元.

注1：逆元不一定存在.

例如：整数环中除1和-1外，其余元都没有逆元.

注2：逆元唯一性, 即逆元如果存在，则必唯一.

证明：设a有两个逆元b和b'，则

$$b = 1b = (b'a)b = b'(ab) = b'1 = b'.$$

所以性质成立.

如果a 有逆元，则用a^{-1}表示它的逆元，且$\forall n \in N$, 规定：

$$a^{-n} = (a^{-1})^n.$$

此时，$\forall m, n \in Z$, 有

$$a^m a^n = a^{(m+n)}, \qquad (a^m)^n = a^{mn}.$$

定义1.6. 若在一个环R里，$\exists a \neq 0, b \neq 0$, 但$ab = 0$，则称 a 是环R的一个左零因子，b是环R的一个右零因子.
左、右零因子统称为零因子.

例：数域 F上全体n 阶方阵$\mathrm{M}_n(F)$对于矩阵的加法和乘法来说构成一个有单位元的环.

但当$n \geq 2$ 时, $\mathrm{M}_n(F)$有零因子。

如: $A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \neq 0, B = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \neq 0$

但　$AB=0$.

例: R={所有模n的剩余类}.
回忆: R 是一个加群.(关于加法:$[a]+[b]=[a+b]$)
规定: R 中的乘法如下：

$$[a][b]=[ab],$$ (这是定义合理的！)

则 R 是一个环，称之为模n的剩余类环，记作Z_n,或$(Z_n,+,\cdot)$.

若n 不是素数，设 $n=ab$,且$n\nmid a, n\nmid b$，则

$$[a]\neq 0,[b]\neq 0，\quad 但 \quad [a][b]=[ab]=[n]=[0]$$

所以n 的非平凡因子均为 R 的零因子.

定理1.6.　在一个没有零因子的环里，如下两个消去律成立;
反之，一个环里若有任一消去律成立，则这个环没有零因子.

$$\forall a \neq 0, ab = ac \Rightarrow b = c;$$
$$\forall a \neq 0, ba = ca \Rightarrow b = c.$$

证明：设环R没有零因子，则由 $a \neq 0$ 和 $ab = ac$,

知 $ab - ac = a(b - c) = 0$,

从而，得 $b - c = 0$，　即 $b = c$.

所以，第一个消去律成立.

同理可证，第二个消去律也成立.

反之，不防设第一个消去律成立，此时若有 $ab=0,$

则有 $ab=a0.$

所以由第一条消去律知，若 $a\neq 0,$ 则 $b=0.$

因此，得到 $a=0,$或$b=0.$ 即该环没有零因子。

推论： 在一个环里，若有一个消去律成立，则另一个消去律也成立。

定义1.7.　称一个非零环R为整环，如果它满足：

1、乘法适合交换律：$\forall a, b \in R$, 有$ab = ba$;

2、R有单位元1；

3、R没有零因子：$\forall a, b \in R, ab = 0 \Rightarrow a = 0$或$b = 0$.

例如：整数环是一个整环.

§2. 除环、域

例1. 若环$R = \{a\}$，只含一个元 a，则它的加法和乘法必为：

$$a + a = a, \qquad aa = a.$$

因此，在该环中有a =0=1. 此时，0元可逆，且逆为其自身.

例2. 全体有理数作成的集合对于普通数的加法和乘法作成一个环，显然对于任意一个非 0 有理数 a，都有逆元a^{-1}。

例3. 若环 R中至少含两个元素，则$\exists 0 \neq a \in R$，从而 $0a = 0 \neq a = 1a$，这说明：在环R 中，0不是单位元.

再由$\forall x \in R$，有 $0x = x0 = 0 \neq 1$.因此，0不可逆.

定义2.1.　称一个环R 为除环，若

1、R 至少含有两个元；(即 R 至少含有一个不为零的元)；
2、R 有单位元；
3、R 中任一非零元都有逆元.

定义2.2. 交换除环称为域。

例：　Q, R, C都是域.

除环的性质：

1、除环无零因子。

因为若$a \neq 0, ab = 0 \Rightarrow b = a^{-1}ab = 0.$

2、除环R的全体非零元构成的集合，对于R的乘法来说构成一个群，记为$R^* = R - \{0\}$. 称之为除环 R 的乘法群.

验证： R^*关于乘法封闭，即$a \neq 0, b \neq 0,$则 $ab \neq 0.$

结合律(显然)、单位元($1 \in R^*$)、逆元($\forall a \in R^*,$有 $a^{-1} \in R^*$).

注1. 除环由两个群构成，分配律是联系这两个群的桥梁.

注2. 若R是有单位元的环，则其全体可逆元构成的集合，对于R的乘法构成一个群. 称之为R的单位群，其中的每个元素都称为一个单位.

在除环R中，$\forall a \neq 0, b \in R$，方程 $ax=b$ 和 $ya=b$ 有唯一解, 分别为 $a^{-1}b$ 和 ba^{-1}. 但是$a^{-1}b$不一定等于ba^{-1}.

如果 R 是域，则有 $a^{-1}b=ba^{-1}$, 所以在域中可以用 $\frac{b}{a}$ 表示 $a^{-1}b$ 和 ba^{-1}.

且此时，$\forall a, b, c, d \in R$，有以下结论：

1、$\frac{a}{b}=\frac{c}{d}$ 当且仅当 $ad=bc$ 时成立；

2、$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$

3、$\frac{a}{b}\frac{c}{d}=\frac{ac}{db}$

证明：显然.

例: (非交换除环)四元数环R ={所有复数对(α,β)}. 规定:

$$(\alpha_1,\beta_1)+(\alpha_2,\beta_2)=(\alpha_1+\alpha_2,\beta_1+\beta_2)$$

$$(\alpha_1,\beta_1)(\alpha_2,\beta_2)=(\alpha_1\alpha_2-\beta_1\overline{\beta_2},\alpha_1\beta_2+\beta_1\overline{\alpha_2})$$

则R是一个除环，但不是交换环。

因为对于非零元(α,β)，均有逆元$(\frac{\overline{\alpha}}{\alpha\overline{\alpha}+\beta\overline{\beta}},\frac{-\beta}{\alpha\overline{\alpha}+\beta\overline{\beta}})$.

但是$(i,0)(0,1)=(0,i),(0,1)(i,0)=(0,-i)$. 所以$(i,0)(0,1)\neq(0,1)(i,0)$.

这个环是非交换除环。

四元数环H:

$$令H=\left\{\begin{pmatrix}\alpha & \beta \\ -\overline{\beta} & \overline{\alpha}\end{pmatrix} \middle| \alpha,\beta\in C\right\}\subset M_2(\mathbb{C}),$$

则H关于矩阵的加法、乘法构成一个环，称之为四元数环.

注：1. H 中每个非零元素都有逆元.

2. H 是一个非交换除环，例如：

$$\begin{pmatrix} i & 0 \\ 0 & -i\end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}=\begin{pmatrix} 0 & i \\ i & 0\end{pmatrix}\neq\begin{pmatrix} 0 & -i \\ -i & 0\end{pmatrix}=\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i\end{pmatrix}.$$

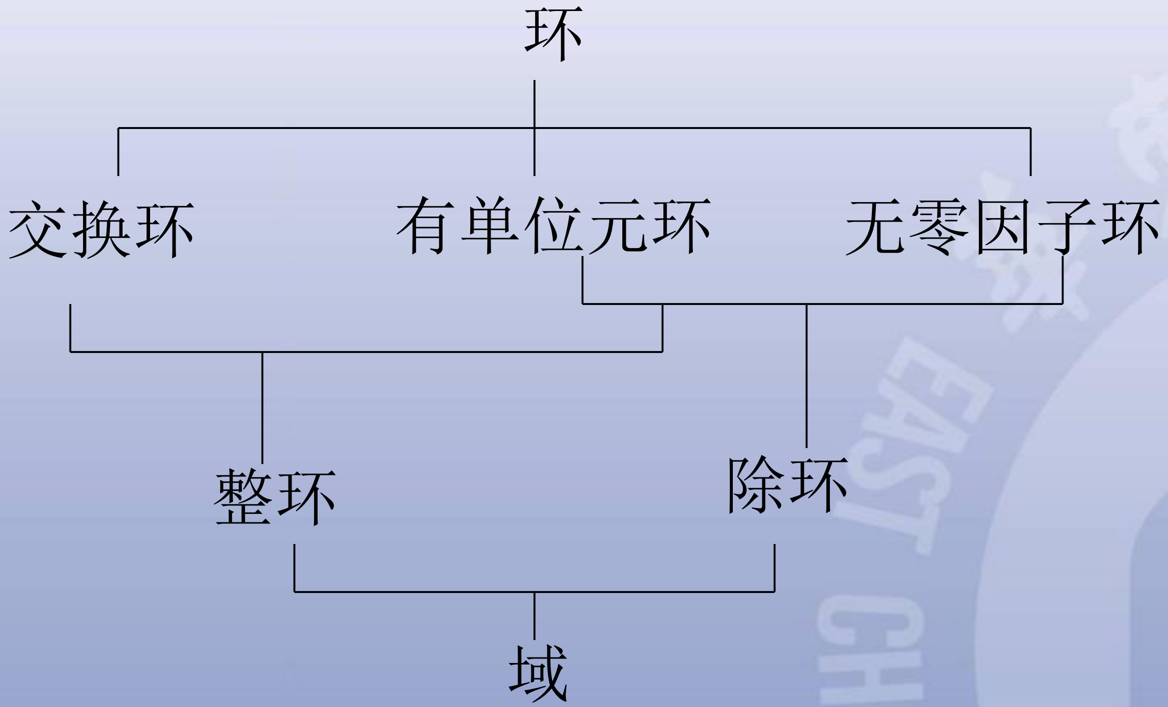
3. H是$\mathbb{R}$上的四维线性空间.

事实上，H有一组基 $\left\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix},\begin{pmatrix}i & 0\\0 & -i\end{pmatrix},\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix},\begin{pmatrix}0 & i\\i & 0\end{pmatrix}\right\}$.

若记$E=\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, I=\begin{pmatrix}i & 0\\0 & -i\end{pmatrix}, J=\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}, K=\begin{pmatrix}0 & i\\i & 0\end{pmatrix}$,

则$I^2=J^2=K^2=-E$,且$IJ=K=-JI$, $JK=I=-KJ$, $KI=J=-IK$.

环的分类：



§3. 无零因子环的特征

讨论问题：$a \neq 0 \overset{?}{\Rightarrow} ma = \overbrace{a + a + \cdots + a}^{m个} \neq 0$

例：设 p 是一个素数，则模 p 的剩余类环$Z_p = {}^{Z}/_{pZ}$ 是一个域 (记作F_p).

证明：首先Z_p 是一个有单位元[1] 的交换环.

因此，只需证明Z_p的任一非零元都有逆元。

$\forall 0 \neq [a] \in Z_p$, 由于$p$不整除 a，且p是素数, 故 p与a互素,

于是，$\exists x, y \in Z$, 使得 $px+ay=1$.

因此，在Z_p中，有$[px] + [ay] = [1]$.

即 $[a][y] = [1]$.

注：对该域中的任一非零元a，都有$p[a]=[0]$.

证明：因为$p[a]=[a]+[a]+\ldots+[a]=[pa]=[0]$.

回忆：对环中的一个非零元 a 而言，

若它关于加法的阶为∞，则$\forall m \in Z, ma \neq 0$.

若它关于加法的阶为有限数n，则 $na=0$.

例：设$G_1=\langle b\rangle, G_2=\langle c\rangle$都是循环群，$b, c$ 分别是它们的生成元，且b 的阶为∞, c 的阶是有限数n.

此时，可分别记$G_1=\{hb|\forall h\in Z\}, G_2=\{kc|\forall k\in Z\}$.

令$R=\{(hb，kc)\}=G_1\times \mathrm{G}_2$, 并定义如下运算：

加法：$(h_1b，k_1c)+(h_2b，k_2c)=((h_1+h_2)b，(k_1+k_2)c)$;

乘法：$(h_1b，k_1c)(h_2b，k_2c)=(0，0)$;

则，易知R 是一个环，且$(b, 0)$的阶为∞, $(0，c)$ 的阶为n.

定理2.3. 设R 是一个无零因子环，则R 中所有非零元的阶（对于加法来说）都相等。

证明：若每个非零元的阶都是无限大，则结论成立。

因此，不防设R中存在一个非零元 a ，且它的阶是正整数n，

则$\forall 0 \neq b \in R$,有：$0=(na)b=a(nb)$.

再由R是无零因子环，知nb=0. 所以b的阶不超过a的阶.

同理可证 a 的阶不超过 b 的阶，所以a的阶＝b的阶.

注：上述定理条件中的“无零因子”不能去掉.

例如：在环 $^{Z}/_{6Z}$ 中， [2] 的阶为3 ，而[3] 的阶为2.

定义2.4.　若一个无零子环R的非零元（关于加法）的阶为∞，则称R的特征为0；若阶为n，则称R的特征为n.

定理2.5. 若无零因子环R的特征是一个有限数n，则n一定是素数.

证明：假如n不是素数，设$n=n_1n_2$，其中$1< n_1, n_2< n$,那么，

$$\forall 0 \neq a \in R, 有 (n_1a)(n_2a) = (n_1n_2)a^2 = na^2 = 0$$

但是$n_1a \neq 0, n_2a \neq 0$.

这与R是无零因子环矛盾，所以n是素数。

推论2.6· 整环、除环、域的特征或是0，或是一个素数。

例： $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$的特征都为0.

$F_p = {}^{Z}/_{pZ}$， $M_n(F_p)$的特征都为p.

结论：在一个特征为 p 的交换环中, 有:

$$(a+b)^p = a^p + b^p.$$

§4. 子环、环的同态

定义4.1. 环R 的一个子集 S 叫做R的一个子环，如果S本身对于R的代数运算也构成一个环。

注：同样地，可以定义子除环、子整环、子域概念。

结论：1.一个环的非空子集S构成子环的充要条件是：

$$\forall a,b\in S,\text{有}a-b\in S,\text{且}ab\in S.$$

2.一个除环的非空子集S作成子除环的充要条件是：

(1). S至少含有一个非零元；

(2). $\forall a,b\in S$，有$a-b\in S$；

(3). $\forall a,b\in S$，且$b\neq 0,$有$ab^{-1}\in S.$

例: R本身是环R的子环。由0一个元作成的集合$\{0\}$也是R的子环。

例: 一个环R的中心 $C(R)=\{x\in R\mid xr=rx,\forall r\in R\}$ 是R的一个子环.

思考: 一个域的子集构成一个子域的充要条件是什么？

回答：同子除环的条件.

定理4.2. 设R是一个环R' 是一个非空集，且R' 有两个代数运算：加法和乘法。若存在一个R到R' 的满射，使得R与R'对于一对加法和一对乘法来说都是同态，则R'也是一个环。

证明：利用群里的类似结果.(如教材P40，定理1)

环同态 (环同构) 是指两个环之间的一个映射，且它对加法和乘法都是同态(同构).

定理4.3. 设R和R' 都是环，$\varphi: R \to R'$是一个满的环同态，则:

(1). R 的零元的象是R'的零元; 即 $\varphi(0_R) = 0_{R'}$.

(2). R中元a的负元的象是a的象的负元, 即

$$\forall a \in R, \varphi(-a) = -\varphi(a).$$

(3). 若R是交换环，则R'也是交换环；

(4). 若R有单位元1_R，则R'也有单位元$1_{R'}$， 而且$1_{R'} = \varphi(1_R)$.

注： 环的满同态不保持环的“无零因子”性质.

例： 设 Z 是整数环，$Z_n = {}^{Z}/_{nZ}$ 是模n的剩余类环，则

$$\phi: Z \to Z_n$$

$$a \to [a]$$

显然是Z到Z_n的一个同态满射。

但Z是无零因子环；而当 n 不是素数时，Z_n是有零因子环。

例: 令$R=Z\times Z=$\{所有整数对(a,b)\}，定义代数运算:

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$$
$$(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2).$$

则R是一个环.

下面考虑映射： $\phi\colon R\to Z$

$$(a,b)\mapsto a$$

显然它是一个环的满同态。
但是，$(a,0)(0,b)=(0,0)\in R$.

从而R是有零因子环，Z是一个无零因子环。

定理4.4. 假设环 R与环R'同构，即$R \cong R'$. 则：

1. 若R是整环，则R'也是整环；
2. 若R是除环，则 R'也是除环；
3. 若R是域，则R'也是域。

证明：显然.

引理4.5. 设集合A与A'之间有一个一一映射．若A有加法、乘法，则A'上也存在代数运算：加法、乘法，使得A与A'对于这两个代数运算而言都是同构.

证明: 设$\varphi: A \to A'$是一个一一映射，则$\forall a', b' \in A'$,

分别存在唯一的$a, b \in A$, 使得

$$a' = \varphi(a),\ b' = \varphi(b).$$

定义：$a' + b' = \varphi(a) + \varphi(b) := \varphi(a + b);$

$$a'b' = \varphi(a)\varphi(b) := \varphi(ab);$$

易知A与A'对于这两个代数运算而言都是同构.

定理4.6.（挖补定理）设S是环R的一个子环, 环S'与 S 同构(即$S' \cong S$)，且$S' \cap (R-S) = \emptyset$. 则存在一个与$R$同构的环$R'$，使得$S'$是$R'$的子环。

证明：令
$$S = \{a_s, b_s, \cdots\}$$
$$S' = \{a_{s'}, b_{s'}, \cdots\}$$

同构映射 $\varphi: S \to S'$
$$x_s \mapsto \phi(x_s) = x_{s'}$$

R中不属于S的元为$a,b,c,\ldots$

则 $R=\{a_s,b_s,\cdots|a,b,\cdots\}$.

令 $R'=\{a_{s'},b_{s'},\cdots|a,b,\cdots\}$,

规定一个映射$\psi: R\rightarrow R'$, 使得$\forall x\in R$,

$$\psi(x)=\begin{cases} x, & \text{如果} x\in R-S; \\ \varphi(x), & \text{如果} x\in S; \end{cases}$$

则由$S'\cap(R-S)=\emptyset$，可知: ψ是一一映射。

从而，由前面的定理知R'上存在加法、乘法，且ψ对于这两个运算而言，都是同构。

故，R'也是环，且有环同构$R\cong R'$.

注意到：$S' \subset R'$，若记S', R'上的运算分别为$(S', +, \cdot)$和$(R', \oplus, \odot)$, 则 $\forall x_{s'}, y_{s'} \in S'$, 有:

$$x_{s'} + y_{s'} = \varphi(x_s) + \varphi(y_s) = \varphi(x_s + y_s);$$

$$x_{s'} \oplus y_{s'} = \psi(x_s + y_s) = \varphi(x_s + y_s)\,,$$

即 $x_{s'} + y_{s'} = x_{s'} \oplus y_{s'}$.

同理可证: $\cdot = \odot$.

因此，S'是R' 的子环.

§5. 多项式环

设R_0是有单位元的交换环，R是包含1的子环.

定义5.1. 设$\alpha \in R_0$，称元$a_0 + a_1\alpha + \cdots + a_n\alpha^n$ $(a_i \in R, n \in Z_{\geq 0})$ 为一个系数在R中的α的多项式(或α在R上的多项式)，a_i 称为该多项式的系数.

记：$R[\alpha]$ ={所有系数在 R中的α的多项式}

由于$R[\alpha] \subset R_0$, 容易验证：

加法：$(a_0 + a_1\alpha + \cdots + a_m\alpha^m) + (b_0 + b_1\alpha + \cdots + b_n\alpha^n) \in R[\alpha]$;

乘法：$(a_0+a_1\alpha+\cdots+a_m\alpha^m)(b_0+b_1\alpha+\cdots+b_n\alpha^n)$
$=c_0+c_1\alpha+\cdots+c_{n+m}\alpha^{n+m}$,
其中 $c_k=\sum_{i+j=k}a_ib_j$.

结论：1、加法与乘法封闭。

2、$R[\alpha]$是R_0的一个子环，且是包含R和α的最小子环。

定义：$R[\alpha]$称为R上α的多项式环。

例：Z上i 的多项式环$Z[i]=\{a+bi|\forall a,b\in Z\}\subset\mathbb{C}$.

定义5.2. R_0的一个元x叫做R上的一个未定元，若$\forall n$,
不存在不全为零的元$a_0, a_1, \cdots, a_n \in R$, 使得

$$a_0 + a_1 x + \cdots a_n x^n = 0.$$

注1. 在R_0中，不是每个元都是未定元（比如R中元）；

2. 对于一个未定元的多项式，它的系数是唯一确定的.

定义5.3. 对环R上未定元 x 的一个多项式

$$a_0 + a_1 x + \cdots a_n x^n, \text{其中} a_n \neq 0,$$

称n为该多项式的次数.

规定0多项式没有次数，通常也记它的次数为∞.

注：环R_0不一定有R上的未定元.

例如：Z上i 的多项式环$Z[i]=\{a+bi|\forall a,b\in Z\}$.

$$\forall\alpha=a+bi\in Z[i], \text{有}$$

$$(a^2+b^2)+(-2a)\alpha+\alpha^2=0\in Z[i].$$

因此，$Z[i]$中的每个元都不是Z上的未定元.

定理5.4. 设 R 是有单位元1的交换环，则必存在R上的一个未定元 x. 从而，R上的多项式环$R[x]$存在。

证明：1、利用交换环R构造环P' .

令$P' = \{(a_0, a_1, \cdots) | \forall a_i \in R,$ 且只有有限多个$a_i \neq 0\}$.

不妨将$(a_0, a_1, \cdots)$记为$(a_i)_{i\in N}$，

规定：$(a_i)_{i\in N} = (b_i)_{i\in N} \Leftrightarrow \forall i \in N, a_i = b_i$.

加法：$(a_i)_{i\in N} + (b_i)_{i\in N} = (a_i + b_i)_{i\in N}$;

乘法：$(a_i)_{i\in N}(b_i)_{i\in N} = (c_i)_{i\in N}$ 其中$c_i = \sum_{i=k+j} a_k b_j$.

则可验证P'为交换环，其零元为$(0,0,\cdots)$，且

$$(a_0, 0, \cdots)\ (b_0, b_1, \cdots) = (a_0 b_0, a_0 b_1, \cdots).$$

2、利用P'可以得到一个包含R的环P.

首先，注意到P'是一个有单位元$(1,0,\cdots)$的环。

其次，考虑P'的子集$R' = \{(a,0,0,\cdots)|\forall a \in R\}$.

则R'是P'的一个(含单位元的)子环，且映射

$$\begin{aligned} R' &\to R \\ (a,0,0,\cdots) &\mapsto a \end{aligned}$$

是一个环同构，即$R' \cong R$.

最后，注意到$R \cap (P' - R') = \emptyset$.

综上，存在一个环P，使得$P \cong P'$以及R是它的一个子环.

事实上，P也是一个有单位元的交换环，其单位元为1，且作为集合来说，$P = R \cup (P' - R')$.

3、证明P中含有R上的未定元 $x=(0,1,0,\cdots)$.

首先，用数学归纳法可以证明：

$$\forall k \in N, 有 x^k = (\underbrace{0,0,\cdots,0,}_{k个}1,0,\cdots).$$

其次，若有$n \in N$, 以及 $a_0, a_1, \cdots, a_n \in R$, 使得

$$a_0 + a_1 x + \cdots a_n x^n = 0 \in P,$$

则在P'中，有：

$$(a_0,0,0,\cdots) + (a_1,0,0,\cdots)x + \cdots + (a_n,0,0,\cdots)x^n$$
$$= (a_0,a_1,a_2,\cdots,a_n,0,0,\cdots)$$
$$= (0,0,\cdots).$$

故，$a_0 = a_1 = \cdots = a_n = 0.$

设R_0是有单位元的交换环，R是包含1_R的子环.

任取$\alpha_1,\alpha_2,\cdots,\alpha_n\in R_0$,可以作$R$上$\alpha_1$的多项式环$R[\alpha_1]$,
然后作$R[\alpha_1]$上α_2的多项式环$R[\alpha_1][\alpha_2]$. 依次下去，
可以得到：

$$R[\alpha_1][\alpha_2]\cdots[\alpha_n]=\left\{\sum_{i_1i_2\cdots i_n}a_{i_1i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}\;\middle|\;\begin{array}{c}a_{i_1i_2\cdots i_n}\in R,\\ \text{且只有有限个非零.}\end{array}\right\},$$

称之为R上的$\alpha_1,\alpha_2,\cdots,\alpha_n$的多项式环，记作$R[\alpha_1,\alpha_2,\cdots,\alpha_n]$,
其中的每个元叫做R上的$\alpha_1,\alpha_2,\cdots,\alpha_n$的一个多项式。

定义5.5. R_0的n个元$x_1,x_2,\cdots,x_n$称为R上的无关未定元,

如果任何一个R上的$x_1,x_2,\cdots,x_n$的多项式都不等于0,

除非系数全为零.

定理5.6. 设R是一个交换环，n为一个正整数，则一定有R上的无关未定元 $x_1,x_2,\cdots,x_n$存在. 因此，也就有R上的多项式环$R[x_1,x_2,\cdots,x_n]$.

证明：由于R上存在未定元, 记为 x_1, 然后考虑环$R[x_1]$, 及其上的一个未定元，记为 x_2. 依次下去，最后考虑$R[x_1,x_2,\cdots,x_{n-1}]$，及其上的一个未定元，记为$x_n$.

利用数学归纳法，证明$x_1,x_2,\cdots,x_n$ 是R上的无关未定元.

假设$x_1,x_2,\cdots,x_{n-1}$ 是R上的无关未定元，若存在

$$\sum_{i_1,i_2,\cdots,i_n} a_{i_1 i_2\cdots i_n} {x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n} = 0,$$

$$\sum_{i_1,i_2,\cdots,i_n} a_{i_1 i_2 \cdots i_n} {x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n} = 0\,,$$

则 $$\sum_{i_1,i_2,\cdots,i_n} (a_{i_1 i_2 \cdots i_n} {x_1}^{i_1} {x_2}^{i_2} \cdots {x_{n-1}}^{i_{n-1}}) {x_n}^{i_n} = 0\,.$$

将上式左边进行整理，可写成$R[x_1 ,x_2,\cdots ,x_{n-1}]$上未定元$x_n$的多项式，故系数全为0. 注意到每项系数又都是$R$上未定元$x_1 ,x_2,\cdots ,x_{n-1}$的多项式，因此由归纳假设，得证.

注： $x_1,x_2,\cdots ,x_n$的一个多项式通常用$f\,(x_1,x_2,\cdots ,x_n)$ 来表示.

定理5.7. 设R是有单位元的交换环,$R[x_1, x_2, \cdots, x_n]$和$R[\alpha_1, \alpha_2, \cdots, \alpha_n]$都是$R$上的多项式环，且 $x_1,x_2,\cdots,x_n$是R上的无关未定元，$\alpha_1, \alpha_2, \cdots, \alpha_n$ 是R上的任意元。则存在一个满同态：$R[x_1, x_2, \cdots, x_n] \to R[\alpha_1, \alpha_2, \cdots, \alpha_n]$.

证明：定义映射 ϕ: $R[x_1, x_2, \cdots, x_n] \to R[\alpha_1, \alpha_2, \cdots, \alpha_n]$.

$$f(x_1, x_2, \cdots, x_n) \mapsto f(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

即将$f(x_1, x_2, \cdots, x_n) = \sum_{i_1 i_2 \cdots i_n} a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$映为$f(\alpha_1, \alpha_2, \cdots, \alpha_n) = \sum_{i_1 i_2 \cdots i_n} a_{i_1 i_2 \cdots i_n} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}$.
容易验证这是一个映射、满射、环同态.

注：上述映射 $\phi: R[x_1, x_2, \cdots, x_n] \to R[\alpha_1, \alpha_2, \cdots, \alpha_n]$.

$$f(x_1, x_2, \cdots, x_n) \mapsto f(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

称为代入映射.

特殊情况：$R[x] \to R[\alpha]$

$$f(x) \mapsto f(\alpha)$$

§ 6. 理想

定义6.1.环R的一个非空子集 I 叫做R的一个理想(子环)，若I 满足：

1、$\forall a, b \in I \Rightarrow a - b \in I$;

2、$\forall a \in I, r \in R \Rightarrow ra, ar \in I$.

显然：只包含零元的集合{0}，是R的理想，称为R的零理想。R自己也是R的理想，称之为R的单位理想。

零理想和单位理想统称为平凡理想。

定理6.2. 一个除环R只有平凡理想。

证明：设 I 是R的一个理想，且不是零理想，则

$$\exists a \in I, \text{且} a \neq 0, \text{从而} a^{-1}a = 1 \in I.$$

因此，对任意$b \in R, b \cdot 1 = b \in I.$

所以$R = I.$

注：理想对除环和域没有用处。

例: 设Z是整数环，n是一个整数，则它的所有倍数 rn 构成的集合是Z的一个理想，即$\{rn|\forall r \in Z\}$, 记作nZ.

且Z的每一个理想都是nZ的形式.

例: 环R上的一元多项式环$R[x]$中所有常数项为0的多项式构成的集合

$\{a_1x + a_2x^2 + \cdots + a_nx^n|\forall a_1, a_2 \cdots a_n \in R, \forall n \in Z^+\}$

是$R[x]$的一个理想。

设R一个环，$a \in R$，则集合

$$\{(x_1 a y_1 + \cdots + x_m a y_m) + sa + at + na \mid \forall x_i, y_i, s, t \in R, \forall n \in Z)\}$$

是R的一个理想，记为(a).

结论：(a)是包含a的最小理想．称之为由a生成的主理想.

当R为交换环时，$(a) = \{ra + na \mid \forall r \in R, \forall n \in Z\}$;

当R有单位元时，$(a) = \{\Sigma x_i a y_i \mid \forall x_i, y_i \in R\}$;

当R有单位元且为交换环时，$(a) = \{ra \mid \forall r \in R\}$.

设R是一个环，若$a_1, a_2, \cdots, a_m$是R的m个元，则集合

$$I = \{s_1 + s_2 + \cdots + s_m | \forall s_i \in (a_i)\}$$

是R的一个理想。

证明：因为$\forall a, a' \in I,$

设$a = s_1 + s_2 + \cdots + s_m$, $a' = s_1' + s_2' + \cdots + s_m'$, 则

$$a - a' = s_1 - s_1{}' + \cdots + s_m - s_m{}' \in I;$$
$$ra = rs_1 + rs_2 + \cdots + rs_m \in I;$$
$$ar = s_1 r + s_2 r + \cdots + s_m r \in I.$$

所以是R的理想。

注：$I=\{s_1+s_2+\cdots+s_m|\forall s_i\in(a_i)\}$

是包含$a_1,a_2,\cdots,a_m$的最小理想。称为由$a_1,a_2,\cdots,a_m$生成的理想。记作$(a_1,a_2,\cdots,a_m)$.

注： $(a_1,a_2,\cdots,a_m)=(a_1)+(a_2)+\cdots+(a_m)$.

例 设Z[x]是整数环Z上的一元多项式环，则

$$(2,x)=\{2p_1(x)+xp_2(x)\mid \forall p_1(x),p_2(x)\in Z[x]\}.$$

不是主理想。

证明：首先，可以验证

$$(2,x)=\{2a_0+a_1x+\cdots+a_nx^n\mid \forall a_i\in Z,n\in Z^+\}$$

其次，采用反证法。假设它是主理想，设

$(2,x)=(p(x))$,则$2\in(p(x)),x\in(p(x))$.

由$2=q(x)p(x)\Rightarrow p(x)=a$;

再由$x=h(x)p(x)\Rightarrow x=ah(x)\Rightarrow a=\pm1$,

则$\pm1=p(x)\notin(2,x)$,矛盾。

§ 7. 剩余类环、同态与理想

设R为一个环，I 为其一个理想，则对加法运算而言，I是R的一个正规子群，所以 I 的陪集：

$$[a],[b],[c],\cdots$$

是R的一个分类，称为R的模 I 的剩余类。

显然：$[a]=a+I=\{a+u|u\in I\}.$

$$[a]=[b]\Leftrightarrow a-b\in I.$$

把R 的所有剩余类作成的集合, 记作$\overline{R}$, (注：$\overline{R} = {}^{R}/_{I}$),
并在其上规定:

$$\text{加法：} [a] + [b] = [a + b]$$
$$\text{乘法：} [a][b] = [ab]$$

$$\text{乘法：} \overline{R} \times \overline{R} \to \overline{R}$$
$$([a], [b]) \mapsto [ab]$$

若$[a] = [a'], [b] = [b']$, 则$\exists u, v \in I$, 使得$a = a' + u, b = b' + v$,

$$\text{从而:} ab - a'b' = ab - a'b + a'b - a'b'$$
$$= (a - a')b + a'(b - b')$$
$$= ub + a'v \in I,$$

即$[ab] = [a'b']$.

定理7.1：设R是一个环，I 是它的一个理想，则$\overline{R}$按照上述加法和乘法构成一个环，且R到$\overline{R}$有一个自然的满同态。

证明：映射 $\pi: R \to \overline{R}$ 是一个满同态，

$$a \mapsto [a]$$

所以$\overline{R}$是一个环。

注：$\overline{R}$ 中的元$[a]$通常用$\bar{a}$来表示.

定义：$\overline{R}$称为R模I的商环，或者剩余类环，记作${}^{R}/_{I}$.

定理7.2 设R与R'是两个环，并且$\varphi: R \to R'$是一个环的满同态，则同态的核

$$\ker\varphi = \{x \in R | \varphi(x) = 0_{R'}\}$$

是R的一个理想，并且${}^{R}/_{\ker\varphi} \cong R'$.

证明：1、证明$\ker\varphi$是 R 的一个理想。

由于φ是加群同态，故$\ker\varphi$是R的子群.

因此，只需验证：

$$\forall r \in R, a \in \ker\varphi, \Rightarrow ra \in \ker\varphi, ar \in \ker\varphi.$$

直接计算得：$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0;$

同理得：$\varphi(ar) = 0.$

2、证明:$R/_{\ker\varphi} \cong R'$.

由于 $\psi: R/_{\ker\varphi} \to R'$ 是一个加群同构,

$$\bar{a} = [a] \mapsto \varphi(a)$$

故只需验证 ψ 是一个环同态，即：

$$\forall \bar{a}, \bar{b} \in R/_{\ker\varphi}, \psi(\bar{a}\bar{b}) = \psi(\bar{a})\psi(\bar{b}).$$

验证得：

$$\psi(\bar{a}\bar{b}) = \psi(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(\bar{a})\psi(\bar{b}),$$

即证.

例：在环$Z_n = {}^{Z}/_{nZ} = \{[0],[1],\cdots,[n-1]\}$中，

$$\forall [a],[b] \in Z_n, 有 [a]+[b]=[a+b];$$

$$[a][b]=[ab].$$

上式也写作：

$$\bar{a}+\bar{b}=\overline{a+b};$$

$$\bar{a}\bar{b}=\overline{ab}.$$

定理7.3：设映射f：$R \to R'$是一个环同态，则：

1. R 的一个子环 S 在 f 下的象是R'的一个子环；
2. R 的一个理想 I 在 f 下的象是 $f(R)$ 的一个理想；
3. R'的一个子环S'在 f 下的逆象是 R 的一个子环；
4. R'的一个理想I'在 f 下的逆象是 R 的一个理想。

§8. 极大理想

定义8.1. 环R的一个理想 I 称为R的极大理想，如果：

1. $I \neq R$;
2. 任一包含 I 的理想，或者是 I 本身，或者是R.

例：整数环Z的全部理想：$nZ=(n)$, 对正整数n有：
n是素数 $\Leftrightarrow (n)$是Z的极大理想.

证明：$\Rightarrow$ 若J是一个理想，满足$(n) \subset J, (n) \neq J$,

则 $\exists q \in J \subset Z$, 使得$n \nmid q$. 因此, $(n,q) = 1$.

从而 $\exists u, v \in Z$, 使得$nu + qv = 1$.

再由J是理想, 且$n, q \in J$, 得$1 \in J$. 即$J = Z$.

$\Leftarrow$ 设n有因子p, 则$(n) \subseteq (p)$

由(n)是极大理想，故(p)=Z, 或$(p) = (n)$, 且$n \neq 1$.

从而p= 1或$n = p$.

定理8.2. 设 I 是环 R的一个理想，且 $I\neq R$. 则 I 是极大理想当且仅当商环R/I是单环(即:没有非平凡理想).

证明：$\Rightarrow$考虑自然的环的满同态$\pi: R \to R/I$.

$$a \mapsto \bar{a}$$

若I 是极大理想，则对商环R/I的任一非零理想$\overline{I_1}$, 有：它的逆象$\pi^{-1}(\overline{I_1})$是 R 的一个理想。

由于$\overline{0} \in \overline{I_1}$, 故$I \subset \pi^{-1}(\overline{I_1})$; 而由$\overline{I_1} \neq \{\overline{0}\}$, 知$\pi^{-1}(\overline{I_1}) \neq I$.

由条件 I 是极大理想，得$\pi^{-1}(\overline{I_1}) = R$.

因此： $R/I = \pi(R) = \pi\left(\pi^{-1}(\overline{I_1})\right) \subset \overline{I_1} \subset R/I$,

从而得$\overline{I_1} = R/I$, 即 R/I 只有平凡理想.

$\Leftarrow$ 若${}^{R}/_{I}$是单环，即只有平凡理想.

设I_1是R的一个理想，使得$I_1 \supset I, I_1 \neq I$.

由于π 是环的满同态，则$\pi(I_1)$ 是${}^{R}/_{I}$的一个理想，并且非零，即 $\pi(I_1) \neq \{\bar{0}\}$.

再由条件${}^{R}/_{I}$是单环，故：$\pi(I_1) = {}^{R}/_{I}$.

$\forall r \in R, \exists a \in I_1,$ 使得$\bar{r} = \bar{a} \in {}^{R}/_{I}$, 即$r - a \in I$.

从而，

$$r \in I_1, \text{即} R = I_1.$$

因此，I 是极大理想.

定理8.3. 设环 R 是一个有单位元1 (1≠0)的交换环.则 R 是单环当且仅当R是域.

证明: ⇒只需证明 R 中每个非零元都可逆.

$\forall a \in R, a \neq 0,$ 则$(a) \neq \{0\}.$

由条件R是单环, 得$(a)=R$.

从而，$1 \in (a)$，故$\exists b \in R,$ 使得$ba = ab = 1.$

⇐显然。因为域的零理想是极大理想。

定理8.4. 设 R 是一个有单位元1 (1≠0)的交换环, I 是R的一个理想. 则R/I是域当且仅当 I 是极大理想.

证明：显然。

定义8.5. 设 R 是有单位元的交换环，R的一个理想 P ($P\neq R$) 称为素理想，如果$\forall a, b\in R, ab\in P \Longrightarrow a\in P$,或者$b\in P$.

定理8.6. 设 R 是一个有单位元的交换环, P 是R的一个理想. 则$R/_P$是整环当且仅当 P是素理想.

证明：只需要说明$R/_P$ 无零因子当且仅当P是素理想.

$$\forall a,b \in R,\quad \bar{a}\,\bar{b} = \bar{0} \Leftrightarrow ab \in P.$$

故得证.

推论8.7　极大理想一定是素理想.

§9. 商域

定理9.1. 任一无零因子的交换环都是某个域的子环.

证明：不妨设R是一无零因子的交换环，且至少含有两个元素.

令$A=R\times R^* = \{(a,b)|\forall a,b\in R, b\neq 0\}$,

在A上定义如下关系：$\forall (a,b),(a',b')\in A$,

$$(a,b)\sim(a',b')\Leftrightarrow ab'=ba'.$$

则这是A上的一个等价关系。

1.反身性：显然

2.对称性：显然

3.传递性：若$(a,b)\sim(a',b'),(a',b')\sim(a'',b'')$,则

$$ab''b'=ab''b'=ab'b''=ba'b''=bb'a''=ba''b'.$$

将A中每个元(a,b) 所在的等价类记为 $[\frac{a}{b}]$.

令$Q_0 = \left\{所有等价类[\frac{a}{b}] | \forall (a,b) \in A\right\}$.

在Q_0上定义如下运算：$\forall [\frac{a}{b}], [\frac{c}{d}] \in Q_0$,

加法: $[\frac{a}{b}] + [\frac{c}{d}] = [\frac{ad+bc}{bd}]$;

乘法: $[\frac{a}{b}] \cdot [\frac{c}{d}] = [\frac{ac}{bd}]$,

下面验证：这两个运算是定义合理的，且

加法满足：交换律、结合律、零元为$[\frac{0}{b}]$、$[\frac{a}{b}]$的负元为$[\frac{-a}{b}]$;

乘法满足：交换律、结合律、单位元$[\frac{b}{b}]$、非零元$[\frac{a}{b}]$可逆，

且其逆元为$[\frac{b}{a}]$.

分配律成立，从而Q_0是一个域。

1. 首先注意到：若$b \neq 0, d \neq 0$, 则$bd \neq 0$.

2. 其次，若$[\frac{a}{b}] = [\frac{a'}{b'}], [\frac{c}{d}] = [\frac{c'}{d'}]$，则$ab' = ba', cd' = dc'$.

从而，
$$
\begin{aligned}
(ad + bc)b'd' &= adb'd' + bcb'd' \\
&= ba'dd' + bb'dc' \\
&= bd(a'd' + b'c').
\end{aligned}
$$

即 $[\frac{a}{b}] + [\frac{c}{d}] = [\frac{a'}{b'}] + [\frac{c'}{d'}]$.

因此，加法是定义合理的运算。

3. 最后，$[\frac{a}{b}] \cdot [\frac{c}{d}] = [\frac{ac}{bd}] = [\frac{a'c'}{b'd'}] = [\frac{a'}{b'}] \cdot [\frac{c'}{d'}]$,

因此，乘法是定义合理的运算。

4. 其它直接验证即可，并且 Q_0 上的运算由R上的运算确定。

任意固定一个$q \in R^*$, 令$R_0 = \{[\frac{qa}{q}] | \forall a \in R\} \subset Q_0$,

则映射 $\quad i: R \to R_0 \quad$ 是一个环同构.

$$a \mapsto [\frac{qa}{q}]$$

事实上：$\forall a, b \in R$,

$$i(a+b) = \left[\frac{q(a+b)}{q}\right] = [\frac{q^2(a+b)}{q^2}] = i(a) + i(b);$$

$$i(ab) = \left[\frac{q(ab)}{q}\right] = [\frac{q^2(ab)}{q^2}] = i(a)i(b);$$

此外，i 是单射、满射.

再由$R \cap (Q_0 - R_0) = \emptyset$，故存在一个域$Q$，使得$R$是$Q$的子环.

定理9.2. 上述Q 恰好由形如$[\frac{a}{b}](=ab^{-1})$ $(\forall a,b\in R, b\neq 0)$ 的元素构成.

证明：对 Q_0 中的任一元$[\frac{a}{b}]$,有

$$[\frac{a}{b}]=\left[\frac{q^2a}{q^2b}\right]=\left[\frac{qa}{q}\right]\cdot[\frac{q}{qb}]=[\frac{qa}{q}]\cdot[\left(\frac{qb}{q}\right)]^{-1}.$$

故在Q 中， $[\frac{a}{b}]=ab^{-1}$, $a=(qa)q^{-1}$.

注：在Q 中，$\forall ab^{-1},cd^{-1}\in Q$, 有:

$ab^{-1}=cd^{-1}$ 当且仅当 $ad=bc$.

$ab^{-1}+cd^{-1}=(ad+bc)(bd)^{-1}$,

$ab^{-1}\cdot cd^{-1}=(ac)(bd)^{-1}$.

定义9.3. 上述域Q称为R的商域(或者分式域).

注：对任一无零因子的交换环R，一定存在一个域Q，使得R是Q的子环。从而，$\forall 0 \neq a \in R, a$ 在Q中可逆。

定理9.4. 同构的环具有同构的分式域，即在同构的意义下，分式域是唯一存在的.

证明：环R的分式域的运算完全由R决定。

定理9.5. 若R是一个非零环，F是包含R的一个域，则F包含R的一个分式域.

证明：$\forall a, 0 \neq b \in R$, 有$ab^{-1} \in F$.

分式域$Q = \{ab^{-1} | \forall a, b \in R, b \neq 0\}$,

故 $Q \subset F$.