抽象代数学

现在我们引入一种新的代数结构——环，它包含两种运算：加法、乘法．典型例子：$\mathbb{Z}$ 和 $\mathbb{F}[x]$

定义　设 R 是一个非空集合，有两种运算：加法和(记作 $a+b$) 乘法(记作 $a\cdot b$) 满足：

(1) $a+b=b+a$

(2) $(a+b)+c=a+(b+c)$

(3) 存在加法恒等元 0，$a+0=a$，$a+(-a)=0$

以上 $(R,+)$ 是 Abel 群，$\forall a,b,c\in R$

(4) $(a+b)\cdot c=a\cdot c+b\cdot c$，$c\cdot(a+b)=c\cdot a+c\cdot b$　分配律

(5) $(a\cdot b)c=a\cdot(b\cdot c)$

则 R 称为一个环(ring)

若 R 中存在 e，使得 $\forall a\in R$，$ae=ea=a$．则 e 称为(e 也记作 1)恒等元．一个环 = 乘法半群 + Abel 群 + 分配律．

例1．整数环 $\mathbb{Z}$，模 n 的整数环 $\mathbb{Z}_n$，有理数域 $\mathbb{Q}$

$\forall d\in\mathbb{Z}$，$d\mathbb{Z}$（无恒等元）

例2．$\mathbb{Z}(\sqrt{-3})=\{a+b\sqrt{-3}\mid a,b\in\mathbb{Z}\}$

例3　$\mathbb{F}[x]$　$\mathbb{F}$ 一个数域．

例4　$M_n(\mathbb{Z})$

有理数域 $\mathbb{Q}$ $\subset$ 实数域 $\mathbb{R}$ $\subset$ 复数域 $\mathbb{C}$ $\subset$ 四元数体 $\mathbb{H}$ $=\{a+bi+cj+dk\mid a,b,c,d\in\mathbb{R}\}$

基本性质 设R是一个环

(1) $a\cdot 0 = 0\cdot a = 0$;

(2) $a\cdot(-b) = (-a)\cdot b = -(ab)$;

(3) $(-a)\cdot(-b) = ab$; $\Rightarrow (na)\cdot b = a\cdot(nb) = n\cdot(a\cdot b)$. $n\in\mathbb{Z}$.

(4) $a(b-c) = ab-ac$, $(b-c)a = ba-ca$.

(5) 若$ab=ba$, 则$\forall n\in\mathbb{N}$, $(ab)^n = a^n b^n$ 且

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k \qquad C_n^k = \frac{n!}{i!(n-i)!}$$

(6) $$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j.$$

证明: (1) $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0 \Rightarrow a\cdot 0 = 0$.

(2) $a\cdot 0 = a\cdot[b+\cancel{(-1)\cdot b}\,(-b)] = ab + a\cdot\cancel{(-1)\cdot b}\,(-b) = 0 \Rightarrow \cancel{ab = -(1)(ab)}\ \cancel{[a\cdot(-b)]}$

$\cancel{*: (-1)\cdot b + b = 0 \Rightarrow (-1)b = -b}$ $\Rightarrow a\cdot(-b) = -(ab)$ 同理$(-a)\cdot b = -(ab)$

(3) $(-a)\cdot(-b) = -[a\cdot(-b)] = ab$

(6) 关于分配律作归纳法.

$$(na)\cdot b = (\underbrace{a+\cdots+a}_{n个})\cdot b = \underbrace{ab+\cdots+ab}_{n个} = n(ab)$$

$$a\cdot(nb) = a(\underbrace{b+\cdots+b}_{n个}) = ab+\cdots+ab = n(ab)$$

定义 设$a\neq 0\in R$, 若存在$b\neq 0\in R$, $ab=0$ 则a称为左零因子, b称为右零因子.

定义 设R是含幺环, $a\in R$ 称为左可逆, 若存在c, $ca=1$

c称为左逆. 类似地，可定义右可逆和右逆.

若a同时左可逆和右可逆，则a可逆，有唯一的乘法逆元素a^{-1}. 可逆元也称为R的单位.

例如. $M_n(\mathbb{C})$

定义 R一个环，若$\forall a,b\in R$, $ab=ba$，则R称为交换环

定义 R一个环，无零因子，则R称为一个整环

定义 R一个环，令$R^*=R\setminus\{0\}$，若R含1，且非零元均可逆，则R称为一个体(skew-field)，交换的体称为域(field)

例 $R=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,b\in\mathbb{F}\right\}$ 关于矩阵加法、乘法是一个环

$\forall\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ 有左幺元 $\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ $\forall c\in\mathbb{F}$.

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a & ac \\ 0 & 0 \end{pmatrix}.$$

设R是一个环. $M_n(R)=\{A=(a_{ij})_{n\times n}\mid a_{ij}\in R\}$是一个环，称为$R$上的$n$阶方阵环. 若$R$是含幺环，则$M_n(R)$有幺元 $I_n=\begin{pmatrix} 1_R & & \\ & \ddots & \\ & & 1_R \end{pmatrix}$ 1_R是R的幺元.

现在假设R是含幺交换环，定义置换阵P_σ. $\sigma\in S_n$

定义 $\det(P_\sigma)=\begin{cases}1 & \sigma\text{偶置换}\\ -1 & \sigma\text{奇置换}\end{cases}$

$\det(A)=\sum_{\sigma\in S_n}\det(P_\sigma)a_{1\sigma(1)}\cdots a_{n\sigma(n)}$，可验证

$\det: M_n(R)\longrightarrow R$ 多重线性交错函数.

性质：(1) $\det(AB)=\det(A)\cdot\det(B)$

(2) $A\cdot\operatorname{adj}A=\operatorname{adj}A\cdot A=\det(A)\cdot I_n$

} 基于R的交换和det的性质.

定理 R 含幺交换环，$A\in M_n(R)$ A有逆$\Longleftrightarrow$ $\det(A)$ 在R中有逆

证明：若$\det(A)\in R$有逆，记作$\det(A)^{-1}\in R$，则

$\det(A)^{-1}\cdot\operatorname{adj}A\in M_n(R)$

$$\left(\det(A)^{-1}\cdot\operatorname{adj}A\right)\cdot A=A\cdot\left(\det(A)^{-1}\cdot\operatorname{adj}A\right)=I_n$$

即A有逆 $\det(A)^{-1}\cdot\operatorname{adj}A$

反之，若A有逆$A^{-1}\in M_n(R)$ 则 $AA^{-1}=I_n$

$\det(AA^{-1})=1_R=\det(A)\cdot\det(A^{-1})$ 即$\det(A^{-1})$是$\det(A)$的逆

群环. 设G是一个群，R一个环，定义RG是如下元素集合

$$\alpha=\sum_{g\in G}a_g g,\quad a_g\in R，只有有限个a_g\neq 0.$$

加法：$\alpha+\beta=\left(\sum_{g\in G}a_g g\right)+\left(\sum_{g\in G}b_g g\right)=\sum_{g\in G}(a_g+b_g)g$

乘法 $\alpha\beta=\left(\sum_{g\in G}a_g g\right)\left(\sum_{h\in G}b_h h\right)=\sum_{g,h\in G}a_g b_h gh$

RG称为群环 (group ring)

例如 $R=\mathbb{R}$. $G=\mathbb{Z}_2$ $\mathbb{R}\mathbb{Z}_2\cong\mathbb{R}^3$ (作为向量空间)

形式幂级数环 (The ring of formal power series in x)

设R一个环，$R[[x]]=\{f(x)=a_0+a_1x+a_2x^2+\cdots \mid a_i\in R,\ i\in\mathbb{N}\}$

定理 设R交换环，含幺元. 设 $f(x)=\sum_{i=0}^{\infty}a_ix^i\in R[[x]]$

则 $f(x)$ 可逆（在 $R[[x]]$ 中）$\Leftrightarrow a_0\in R$ 可逆.

证明：设 $g(x)=\sum_{j=0}^{\infty}b_jx^j$

$$f(x)g(x)=\sum_{k=0}^{\infty}\left(\sum_{i=0}^{k}a_ib_{k-i}\right)x^k$$

$f(x)g(x)=1\Leftrightarrow a_0b_0=1,\ \sum_{i=0}^{k}a_ib_{k-i}=0\quad\forall k\geq 1$

若 a_0 可逆，则 $b_0=a^{-1}$，$b_1=-b_0(a_1a_0^{-1})=-b_0(a_1b_0),\cdots$

$b_k=-b_0\sum_{i=1}^{k}a_ib_{k-i}\Rightarrow$ 存在 $g(x)$; $f(x)g(x)=1_R$.

注：形式幂级数环 $\xrightarrow{\text{推广}}$ 形式Laurent级数环 $R((x))$
$=\left\{f_r(x)=\sum_{i=0}^{\infty}a_{r+i}x^{r+i} \,\middle|\, \begin{matrix} r\in\mathbb{Z} \\ a_{r+i}\in R\end{matrix}\right\}$ 当 R 是一个域时，
$R((x))$ 也是一个域.

例 有限环若存在非零元不是零因子，则有幺元，且每个非零因子均可逆. 作为一个推论，阶数 >1 的有限环若无零因子，则是除环.

证明：设 $a\neq 0\in R$ 且 a 非零因子 $|R|<\infty$. 则 $a,a^2,a^3,\cdots$ 必有相等 设 $a^m=a^n$ $1\leq m<n$.

$a^{m-1}(a-a^{n-m+1})=0 \Rightarrow a=a^{n-m+1}=a^{n-m}\cdot a$

$\forall x\in R$, $ax=a^{n-m+1}x \Rightarrow a(x-a^{n-m}x)=0 \Rightarrow x=a^{n-m}x$

同理 $x=xa^{n-m}$. $\Rightarrow a^{n-m}=1_R$

$a\cdot a^{n-m-1}=a^{n-m} \Rightarrow a^{n-m-1}$ 是 a 的逆元

作业：Page 84，1，2，3，4，6，8，10

（注：第10题中 $\overline{x}\,\overline{y}=\overline{y}\,\overline{x}$ 应为 $\overline{xy}=\overline{y}\cdot\overline{x}$