抽象代数学

子环：定义 设R一个环，$S\subseteq R$，若S关于R的加法和乘法是一个环，则S是R的子环(subring)

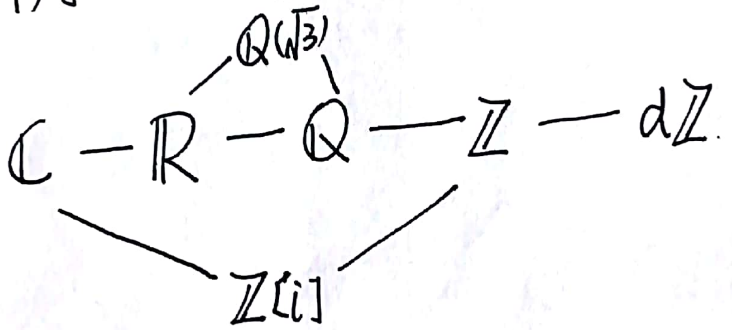
判别法：$S\subseteq R$，S是子环$\Leftrightarrow$ S关于R的加减法、乘法封闭、加法逆元封闭 $\Leftrightarrow$ $\forall a,b\in S$，$a-b\in S$，$ab\in S$.

例 $\mathbb{H}=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{R}\}$ 四元数环

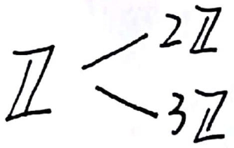
$\mathbb{R}$，$\mathbb{R}(i)=\{a+bi \mid a,b\in\mathbb{R}\}\cong\mathbb{C}$ 均是子环

$\{bi \mid b\in\mathbb{R}\}$ 不是子环，因为 $i\cdot i=-1\notin\{bi \mid b\in\mathbb{R}\}$

例 $\mathbb{C}$的子环



性质：(1)子环的交是子环 (2)子环的并未必是子环，例如



$2\mathbb{Z}\cup 3\mathbb{Z}$

例 R是一个环，$C=\{c\in R \mid cr=rc, \forall r\in R\}$，$C$是一个环

C称为R的中心.

例 R一个环, $X\subseteq R$, 令 $\langle X\rangle = \bigcap\limits_{\substack{X\subseteq S \\ S\text{是子环}}} S$, 则 $\langle X\rangle$ 是包含X的最小子环.

例 $\mathbb{Q}$中包含 $\frac{2}{3}$ 的最小子环 $\langle \frac{2}{3}\rangle = \left\{ \sum\limits_{i=1}^{n} a_i \left(\frac{2}{3}\right)^i \,\middle|\, \begin{matrix} n\in\mathbb{N} \\ a_i\in\mathbb{Z} \end{matrix} \right\}$

理想和商环 (ideals and quotient rings)

回忆 G是一个群, $H\leq G$, G/H 是群 $\Leftrightarrow H\lhd G$.

问题 R是一个环, I是子环, R/I 是环 $\Leftrightarrow$ I满足什么条件?

例 $R=\mathbb{Z}\times\mathbb{Z}$ $S=\{(x,x)\mid x\in\mathbb{Z}\}$ 是子环

$(0,1)+S=(-1,0)+S$, 但是

$((0,1)+S)((0,1)+S)=(0,1)+S$

$((0,1)+S)((-1,0)+S)=(0,0)+S$

不能定义 well-defined 的乘法!

定义 设R一个环, $I\subseteq R$, 若I满足

(1) $I\leq(R,+)$

(2) $\forall r\in R, a\in I$, 有 $ar\in I$, $ra\in I$, 则I称为R的一个理想 (ideal)

任一环R有两个平凡理想: $R, \{0\}$

性质 R 一个环，$I \subseteq R$，则 I 是一个理想 $\Leftrightarrow$

(1) $\forall a, b \in I$，　$a-b \in I$

(2) 若 $a \in I, r \in R$，则 $ra, ar \in I$.

例1. $\mathbb{Z}$，$n\mathbb{Z}$ 是一个理想　　$\mathbb{Z}/n\mathbb{Z}$ 是一个环

例2. R 含幺交换环，$a_1, \cdots, a_n \in R$. $I = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$ 是 R 的一个理想（被 $a_1, \cdots, a_n$ 生成）

定理 R 是一个环，I 是 R 的子环，定义 $R/I = \{r+I \mid r \in R\}$ 上加法、乘法：

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

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

R/I 关于以上定义成为一个环 $\Longleftrightarrow$ I 是 R 的一个理想.

证明: "$\Leftarrow$" (1) 乘法是 well-defined

设 $a+I=a'+I$，$b+I=b'+I$，则 $\exists s, t \in I$，使得 $a=s+a'$，$b=t+b'$，$ab=st+sb'+a't+a'b'$

$(a+I)(b+I)=ab+I=(st+sb'+a't+a'b')+I$

但 I 是理想，$st, sb', a't \in I$，上式 $=a'b'+I$.

"$\Rightarrow$" 设 I 不是 R 的理想，则存在 $a \in I$，$r \in R$，$ar \notin I$ 或 $ra \notin I$. 不妨设 $ar \notin I$，则 $(a+I)(r+I)=ar+I$

但 $a+I=0+I$. 矛盾!

例1 $\mathbb{Z}_4=\{0+\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}=\mathbb{Z}/4\mathbb{Z}$

$(2+4\mathbb{Z})+(3+4\mathbb{Z})=5+4\mathbb{Z}=1+4\mathbb{Z}$.

$(2+4\mathbb{Z})(3+4\mathbb{Z})=6+4\mathbb{Z}=2+4\mathbb{Z}$

例2. $R=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d\in\mathbb{Z}\right\}$ $I=\left\{\begin{pmatrix} x & y \\ z & w \end{pmatrix} \middle| x,y,z,w \in 2\mathbb{Z}\right\}$

$I\subseteq R$ 是一个理想.

$R/I=\left\{\begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}+I \middle| u_i=0\text{或}1,\ i=1,2,3,4\right\}$

例3. 设 R 含幺环, I 是 R 的理想, 则 $M_n(I)$ 是 $M_n(R)$ 的理想.

证明: $0_R\in I \Rightarrow$ 零阵 $\in M_n(I)$, $\forall A,B\in M_n(I)$ $A-B\in M_n(I)$. 设 $C\in M_n(R)$, $A\in M_n(I)$ CA 的元素形如 $\sum_j c_{ij}a_{jk}$ $c_{ij}\in R$, $a_{jk}\in I \Rightarrow \sum_j c_{ij}a_{jk}\in I \Rightarrow CA\in M_n(I)$

注: 反面也对, 即: 若 J 是 $M_n(R)$ 的理想, 则存在 I 是 R 的理想, $J=M_n(I)$. 实际上 $I=\{r\in R \mid r$ 是 J 中的矩阵的某一项$\}$ 设 $A=(a_{ij})\in J$, 则 $E_{ki}AE_{jl}=a_{ij}E_{kl}$

由此得 I 是理想和 $J=M_n(I)$.

推论: 若 R 是除环, 则 $M_n(R)$ 无非平凡理想.

例4. $R=\mathbb{Q}[x]$ $\quad I=(x^2-2)=\{f(x)(x^2-2)\mid f(x)\in\mathbb{Q}[x]\}$

$$\frac{\mathbb{Q}[x]}{(x^2-2)}=\{f(x)+(x^2-2)\mid f(x)\in\mathbb{Q}[x]\}$$
$$=\{a\bar{x}+b\mid a,b\in\mathbb{Q},\ \bar{x}=x+(x^2-2)\}$$

例5. $\mathbb{R}[x]$ 给一个新不定元 ε $\Rightarrow (\mathbb{R}[x])[\varepsilon]=\mathbb{R}[x,\varepsilon]$

$(\varepsilon^2)=I$ 令 $\bar{R}=\dfrac{\mathbb{R}[x,\varepsilon]}{(\varepsilon^2)}=\{f(x,\varepsilon)+(\varepsilon^2)\}$

$(x+\varepsilon)^3=x^3+3x^2\varepsilon+3x\varepsilon^2+\varepsilon^3$ 在 $\bar{R}$ 中，它等于

$x^3+3x^2\varepsilon=x^3+(x^3)'\varepsilon$

$\forall f(x)\in\mathbb{R}[x]$ $\quad\boxed{f(x+\varepsilon)+(\varepsilon^2)=f(x)+f'(x)\varepsilon+(\varepsilon^2)}$.

理想的性质：R 一个环

(1) 设 I, J 均为 R 的理想，$I+J$ 也是理想.

$IJ=\{\sum_{i,j}a_ib_j\mid a_i\in I,\ b_j\in J\}$ 也是理想.

(2) 设 $x\in R$，x 生成的理想，记作 (x) 称为主理想.

(3) 若 R 没有非平凡理想，则 R 称为单环. 例如：除环和域.

定理. 设 R 含幺交换环. R 是域 $\Leftrightarrow$ R 是单环.

证明："$\Rightarrow$" 显然，因为任意元素可逆

"$\Leftarrow$" 设 R 是单环，$\forall a\in R$，$a\neq 0$　$(a)=\{ra \mid r\in R\}$

是一个理想，则 $(a)=R$　即 $\exists r_0\in R$，$r_0a=1=ar_0$

$\Rightarrow a$ 可逆 $\Rightarrow R\setminus\{0\}$ 是一个交换群，$\Rightarrow R$ 是一个域.

左理想/右理想

定义 R 一个环，$I\subseteq R$，若有 (1) $I\leqslant(R,+)$，(2) $\forall a\in I, r\in R$，$ra\in I$，则 I 称为左理想. 同理可定义右理想.

例 $I=\left\{\begin{pmatrix} a & 0 \\ b & 0\end{pmatrix} \middle| a,b\in\mathbb{R}\right\}$ 是 $M_2(\mathbb{R})$ 的左理想.

性质：I, J 是 R 的左理想，则 $I+J$，$I\cap J$，IJ 均为 R 的左理想

注：设 $a\in R$.

(1) a 生成的理想 $(a)=\{x_1ay_1+\cdots+x_kay_k+xa+ay+na \mid x_i, y_i, x, y\in R, n\in\mathbb{Z}\}$

(2) R 交换，$(a)=\{ra+na \mid r\in R, n\in\mathbb{Z}\}$

(3) R 含幺交换 $(a)=\{ra \mid r\in R\}$

作业：Page 89，1, 2, 5, 8, 12, 13, 14