信息安全数学基础 第十次作业

BY 18340087 李晨曦

(1)

由于$*$在$\mathbf{R}$上是结合的，$\boldsymbol{R}^* \subset \boldsymbol{R}$， 显然$*$在$\boldsymbol{R}^*$也是结合的；

由题意， 存在e使得$e \cdot e = e \cdot e$成立， 所以$e \in \boldsymbol{R}^*$；

由题意， 如果$a \in \boldsymbol{R}^*$， 那么存在$a^{-1} \in \boldsymbol{R}$. 而$a^{-1}$也有逆元$a \in \boldsymbol{R}$， 故$a^{-1} \in \boldsymbol{R}^*$. 这样一来$\boldsymbol{R}^*$中的所有元素都有逆元；

对于$a \in \boldsymbol{R}^*, b \in \boldsymbol{R}^*$,

$$(ab)^{-1} = b^{-1} a^{-1}$$

而$b^{-1} \in \boldsymbol{R}, a^{-1} \in \boldsymbol{R}$， 由群的封闭性可知$b^{-1} a^{-1} \in \boldsymbol{R}$. 而这会得出$ab \in \boldsymbol{R}^*$， 封闭性得证；

综上所述，$\boldsymbol{R}^*$对于乘法运算构成一个群。

(2)

假设R中的可逆元a， 一个任意元b， 满足$a \neq 0, b \neq 0, ab = 0$， 即是说$a$是左零因子，$b$是右零因子。由于$a$可逆， 我们有：

$$\begin{aligned} a^{-1} ab &= a^{-1} \cdot 0 \\ b &= 0 \end{aligned}$$

矛盾， 所以不成立。也就是说a不可能是左零因子，a自然不可能是零因子。

(3)

考虑$\boldsymbol{R}$中的两个任意元素a, b， 有：

$$\begin{aligned} (x+y)^2 &= x^2 + xy + yx + y^2 \\ &= x + y + xy + yx \\ &= x + y \end{aligned}$$

这得到：

$$\begin{aligned} xy + yx &= 0 \\ xy &= -yx \\ &= (xy)^2 \\ &= yx \end{aligned}$$

所以布尔环R是交换环。

(4)

如果一个环G是非零有限整环， 也就是说，$0 \notin G$， 那么对于任意的$a \in G$， 集合

$$A = \{aa_i \mid a_i \in G\}$$

有

$$|A|=|G| \tag{1}$$

这是因为

- $1\leqslant i\leqslant |G|$
- 对于$\forall i,j,(i\neq j)\rightarrow aa_i\neq aa_j$. 这是因为若$aa_i=aa_j$， 则有

  $$a\left(a_i-a_j\right)=0$$

  因为$a\neq 0$， 所以必有$a_i=a_j$，$i=j$.

由环对乘法封闭， 我们有:

$$A\subset G \tag{2}$$

结合(1) (2)， 可知

$$A=G$$

这说明

$$e\in A$$

也即是说，$\exists i,a_i\in G,aa_i=e$， 由交换性得到$a_i a=e$， 所以$a_i$是$a$的逆元。这样一来， 环$G$内的任何元素都有逆元， 结合环$G$是一个整环， 可以得到环$G$是一个域。