# 交换环

2023 年 9 月 12 日

## 目录

# 1 基本性质

在高校的代数中，普通实数的加法和乘法经常被赋予一些“规则”，这些规则总是很长的，大概有20多个页甚至更多，例如其中一个规则：**加法消去律**：

$$a+c=b+c, \text{ 则} a=b$$

一些其他例子，例如这个：涉及到减法的性质——仅仅只是在两边减去$c$。但这里有一些其他的规则涉及到两种运算，一个例子是分配律：

$$(a+b)c=ac+bc$$

当我们从左往右读，这是在说明$c$是可以被乘进$a+b$的，而当我们从右往左读，他又说$c$是可以为$ac+bc$的一个因子。

但现在还有一个神秘的法则：

$$(-1)\times(-1)=1$$

它包含乘法和减法两者。但其中有一些法则是可以通过删除一些来精简的。其中一个很好的理由是：精简这些规则得到一个较短的表格可以让我们容易看到彼此之间的差异，例如多项式和同余之间页是可以乘和加的，现在在我们探究这些相似点之前先解决上面对于$-1$这个法则的神秘之处。

## 1.1 引理

$$0\cdot a=0\text{对每个数}a\text{成立}$$

**证明：** 由于$0=0+0$，那么由分配律我们有

$$0\cdot a=(0+0)\cdot a=(0\cdot a)+(0\cdot a)$$

现在，我们只需要在等式两边同时减去$0\cdot a$就得到$0=0\cdot a$了。

我们顺便探讨一下，为什么0是不难当除数的。给定一个数$b$，它的倒数$1/b$一定满足$b(1/b)=1$的，特别的，我们也对$1/0$运用这个思路，那么就有$0(1/0)=1$，但利用引理1.1，我们知道$0(1/0)=0$，得到$1=0$，矛盾。

## 1.2 引理

若$-a$是一个数，当我们加上一个$a$后得到0，则$(-1)(-a)=a$

**证明：** 利用引理1.1和分配律有：

$$0 = 0 \cdot a = (-1+1)(-a) = (-1)(-a) + (-a)$$

现在只需要在两边同时加上$a$即可。

## 1.3 推论

$$(-1)a = -a\text{对每个数}a\text{成立}$$

**证明：** 利用引理1.2，则$(-1)(-a) = a$，现在只需要在两边乘上$-1$即有

$$(-1)(-1)(-a) = (-1)a$$

并且引理1.2给出$(-1)(-1) = 1$，证毕。

## 1.4 定义：交换环

一个交换环$R$指的是一个有两种运算的集合：加法和乘法，例如：

1. a+b = b+a 对所有$a, b \in R$成立
2. $a + (b + c) = (a + b) + c$对所有$a, b, c \in R$成立
3. 存在$0 \in R$且$0 + a = a$对所有$a \in R$成立。
4. 对每个$a \in R$，其中$a' \in R$使得$a + a' = 0$
5. $ab = ba$对所有数成立
6. $(ab)c = a(bc)$对每个数成立
7. 存在$1 \in R$，我们称为一，或者单位。且$1a = a$对所有$a \in R$成立。
8. $a(b + c) = ab + ac$对所有数成立。

当然，公理1到5说$R$在加法下构成阿贝尔群。环$R$中的加法和乘法是运算，所以我们可以构造函数

$$\alpha : R \times R \to R,\ \alpha(r, r') = r + r' \in R$$

和

$$\mu : R \times R \to R,\ \mu(r, r') = rr' \in R$$

对所有$r, r' \in R$，替换律在这里也是成立的。就像对其他任意运算那样：若$r = r'$和$s = s'$，则$r + s = r' + s'$和$rs = r's'$。

## 1.5 例子

1. 我们可以验证$Z, Q, R$和复数域$C$在加法和乘法下是交换环。

2. 令$Z[i]$是由形如$a + bi$的负数组成的集合。其中$a, b \in Z$，$i^2 = -1$。我们也可以检验这是一个环，而这个环也被叫做高斯整数。

## 1.6 命题

引理1.1,1.2和推论1.3对所有交换环成立。

**证明：** 对于这些命题都可以用公理证明，但这里我们要用一个非常挑剔的方法证明引理1.1。

因为$0 = 0 + 0$，则由分配律得到

$$0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a)$$

现在，我们在两边加上$-(0 \cdot a)$

$$-(0 \cdot a) + (0 \cdot a) = -(0 \cdot a) + [(0 \cdot a) + (0 \cdot a)]$$

由$-(0 \cdot a)$的定义可知左边是0，得到

$$0 = -(0 \cdot a) + [(0 \cdot a) + (0 \cdot a)]$$

在利用简单的结合律就得到右边

$$\begin{aligned} 0 =& -(0 \cdot a) + [(0 \cdot a) + (0 \cdot a)] \\ =& [-(0 \cdot a) + (0 \cdot a)] + (0 \cdot a) \\ =& 0 + (0 \cdot a) \\ =& 0 \cdot a \end{aligned}$$

## 1.7 定义：减法

若$R$是交换环且$a, b \in R$，则减法被定义为：

$$a - b = a + (-b)$$

### 1.8 定义：零元

令$R$是交换环，且$a \in R$和$n \in \mathbf{N}$，定义$0a = 0$，和定义$(n+1)a = na + a$，定义$(-n)a = -(na)$

### 1.9 命题：二项式定理

若$a, b \in R$，其中$R$是交换环，则对所有$n \geq 0$

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$$

**证明：** 我们需要定义$a^0 = 1$和$a = 0$对每个$a \in R$成立。由于交换环中没清楚的定义$1 \neq 0$。所以必须非常小心。

### 1.10 命题：零环

若$R$是交换环且其中$1 = 0$，则$R$只有唯一的一个元素$R = \{0\}$，我们也把这个$R$叫做**零环**

**证明：** 通过命题1.6，若$r \in R$，则$r = 1r = 0r = 0$

### 1.11 定义：整环

一个整环指的是满足额外的公理$1 \neq 0$和乘法消去律的交换环$R$:

$$ca = cb, c \neq 0 \Rightarrow a = b$$

我们也可以把这个定义给简记为**域**

我们熟悉的一些交换环$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$都是域，接下来我们展示一些不是域的交换环。

### 1.12 命题

一个交换环$R$是域当且仅当它不是零环且对于任意两个非零元素的乘积是非零的。

**证明：** 我们假设$R$是域，那么它满足消去律，我们通过矛盾的方法设这里存在非零元素$a, b \in R$使得$ab = 0$，利用引理1.1，有$0 \cdot b = 0$，那么存在$ab = 0 \cdot b$最后利用消去律就得到$a = 0$得到矛盾。

反过来，我们假设非零元素的乘积在$R$中永远不等于0。若$ca - cb$其中$c \neq 0$，则$0 = ca - cb = c(a - b)$，由于$c \neq 0$，利用非零假设我们得到$a - b = 0$。因此$a = b$。

## 1.13 定义：子环

一个交换环$R$的子集$S$称作$R$的子环，若其：

1. $1 \in S$
2. 若$a, b \in S$，则$a - b \in S$
3. 若$a, b \in S$则$ab \in S$

就像子群也是群一样，一个子环也是一个环。

## 1.14 命题：

一个交换环$R$的子环$S$自身也是交换环。

**证明：** 由假设我们知道存在$1 \in S$，现在有$1s = s, s \in S$，现在我们证明其对加法封闭，即$s, s' \in S$，则$s + s' \in S$。利用子环的公理2我们可以得到$1 - 1 = 0 \in S$，并且还可以得到$0 - b = -b \in S$。最后，若$a, b \in S$，利用推论1.3可以有

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

因此，$S$在加法和乘法下封闭。并且也包含$1, 0$且对任意$s$存在$-s \in S$，并且$S$也继承了其他交换环的性质，例如分配律对$S$也成立。

就像我们验证一个群需要验证很多个性质一样，验证一个环也需要验证很多性质，不同的是，我们可以像验证子群一样验证一个交换群，可以省很多麻烦。

例如，我们可以很简单的看出高斯整数是一个环：

$$Z[i] = \{z \in C : z = a + ib : a, b \in Z\}$$

且是数域$C$中的子环。

### 1.14.1 例子

若$n \neq 3$是整数，令$\zeta_n = e^{2\pi i/n}$是$n$次单位根，并定义

$$Z[\zeta_n] = \{z \in C : z = a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}, a_i \in Z\}$$

当$n = 4$的时候，它就是高斯整数$Z[i]$[1]，并且也是$C$的子环。且对乘法封闭，注意：若$m \geq n$，则$m = qn + r$，其中$0 \leq r < n$并且$\zeta_n^m = \zeta_n^r$

## 1.15 命题

1. 模$m$整数类$I_m$是交换环

2. 交换环$I_m$是一个域当且仅当$m$是素数。

**证明：** 我们之前在同余类上定义过加法和乘法，即$[a] + [b] = [a + b]$，它满足公理1，乘法如下：$[a][b] = [ab]$满足公理$5, 7$，最后之u需要验证分配律对$Z$成立即可。

$$\begin{aligned}[a]([b] + [c]) =& [a][b + c] \\ =& [a(b + c)] \\ =& [ab + ac] \\ =& [ab] + [ac] = \quad [a][b] + [a][c]\end{aligned}$$

因此$I_m$是交换环。

对第二个命题，若$m$不是素数，则$m = ab$，其中$0 < a, b < m$，那么$[a], [b] \neq [0] \in I_m$，由于$m$整除$a$或者$b$，那么$[a][b] = [m] = [0]$，因此$I_m$不是域。

反过来，假设$m$是素数，因此$m \geq 2$，我们有$[1] \neq [0]$，若$[a][b] = [0]$，则$ab \equiv 0 \mod m$，那么$m \mid ab$，由于$m$是素数，由欧拉定理我们有$m \mid a$或者$m \mid b$，因此$a \equiv 0 \mod m$或者$b \equiv 0 \mod m$，得到$[a] = [0]$或者$[b] = [0]$，所以$I_m$是域。

例如$I_6$就不是域，因为$[2] \neq 0, [3] \neq 0$，但$[2][3] = [0]$。

[1] 当n=4，则单位根只有$-1, i$两种结果，所以是高斯整数。

## 1.16 定义：除法

令$a, b \in R$，其中$R$是交换环。那么$R$中的$a$除$b$指的是若存在一个$c \in R$使得$b = ca$，我们把$a$除$b$记作

$$a \mid b$$

例如一个极端的例子，若$0 \mid a$，则$a = 0 \cdot b$对某个$b \in R$成立。由于$0 \cdot b = a$，那么必须有$a = 0$。因此$0 \mid a$当且仅当$a = 0$

注意的是，$a \mid b$不仅取决于元素$a$和$b$，还取决于交换环$R$。例如：3在$Q$中可以除2，因为$2 = 3 \times \frac{2}{3}$，其中$\frac{2}{3} \in Q$。另一方面3在整数集中并不能除2，因为不存在一个数$c \in Z$使得$3c = 2$

## 1.17 引理

令$R$是一个交换环，并令$a, b, c \in R$

1. 若$a \mid b, b \mid c$则$a \mid c$
2. 若$a \mid b, a \mid c$，则$a$可除任意$sb + tc$的组合，其中$s, t \in R$

**证明：** 对于命题1，若$a \mid b, b \mid c$，那么有$b = ac$和$c = db$，我们有$c = d(ac)$可知$a \mid c$

对于第二个命题，由于$a \mid b, a \mid c$，那么就存在$d, e \in R$使得$b = da$和$c = ea$，利用贝祖定理可知存在一些数$s, t \in R$使得

$$sb + tc = a$$

那么我们就得到

$$s(da) + t(ea) = a$$

得到$a \mid sb + tc$

## 1.18 定义：线性组合

若$R$是交换环且$a, b \in R$，则$R$的一些元素的线性组合形如$sa + tb$，其中$s, t \in R$

## 1.19 定义：单位，逆，相伴

我们说$R$中的元$u$是单位元，那么$u \mid 1$，那么就存在$v \in R$使得$uv = 1$，而$v$被称为$u$的逆，并记作$u^{-1}$。若存在单位$u \in R$使得$a = ur$，则$a$称为$r$的相伴元

### 1.19.1 例子

$Z$中的单位元只有$\pm 1$，且对于$n \in Z$它的相伴元是$\pm n$

## 1.20 命题

若$a$是整数，则$[a]$是$I_m$的单位元当且仅当$a, m$互素，实际上，若$sa + tm = 1$，则$[a]^{-1} = [s]$

**证明：** 若$[a]$是$I_m$中的单位元，那么$[s] \in I_m$使得$[s][a] = [1]$，因此$sa \equiv 1 \mod m$，那么就有$sa - 1 = tm$得到$sa - tm = 1$可知$a, m$互素。

反过来，若$a, m$互素，则存在一些整数$s, t$使得$1 = sa + tm$，因此$sa - 1 = -tm$就有$sa \equiv 1 \mod m$所以$[s][a] = [1]$。说明$[a]$是$I_m$中的单位元。

## 1.21 引理

若$p$是素数，则每个非零的$[a] \in I_p$都是单位元。

**证明：** 若$[a] \neq [0]$，那么$a \equiv 0 \mod p$可知$p \nmid a$，因此$a, p$是互素的因为$p$是素数。

## 1.22 定义：单位群

若$R$是交换环，则$R$的单位群指的是

$$U(R) = \{\text{all unit s in R}\}$$

简单的验证一下可以发现$U(R)$是乘法群，例如$U(I_m)$

当我们引入交换环$I_m$的时候它使得我们解决同余方程组的问题变得自然。例如$Z$中的同余方程$ax \equiv b \mod m$变成$I_m$的方程$[a][x] = [b]$，那么这种解就是$[x] = [a]^{-1}[b] = [s][b] = [sb]$。换句话说，若普通的线性方程$ax = \beta$在$R$中的解$x = a^{-1}\beta$得到了，那么我们就找到了同余方程的解。