近世代数之三

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

1. 环的定义
2. 整环与域

环

1. 环=类似于$\mathbb{Z}$，带上加法、减法和乘法
2. 起源于D. Hilbert “Zahlring” 1897 (德语Ring意味an association；又指cyclical behaviour in $\mathbb{Z}[\alpha]$ or $\mathbb{Z}_n$)
3. 公理化定义A. Fraenkel 1914；M. Sono 1917; E. Noether 1921

Emmy Noether 1921, Ideal Theory in Ring Domains

Idealtheorie in Ringbereichen.

Von

Emmy Noether in Göttingen.

§ 1.

Ringbereich, Ideal, Endlichkeitsbedingung.

1. Der zugrunde gelegte Bereich Σ sei ein (kommutativer) *Ring* in abstrakter Definition[7]; d. h. Σ bestehe aus einem System von Elementen $a, b, c, \ldots, f, g, h, \ldots$, in dem eine den üblichen Bedingungen genügende Relation als *Gleichheit* definiert ist; und in dem durch zwei Operationen (Verknüpfungsarten), *Addition* und *Multiplikation*, aus je zwei Ringelementen a und b stets eindeutig je ein drittes als Summe $a + b$ und als Produkt $a \cdot b$ gewonnen wird. Der Ring und die sonst ganz willkürlichen Operationen müssen dabei den folgenden Gesetzen genügen:

1. *Dem assoziativen Gesetz der Addition*: $(a+b)+c = a+(b+c)$.
2. *Dem kommutativen Gesetz der Addition*: $a + b = b + a$.
3. *Dem assoziativen Gesetz der Multiplikation*: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
4. *Dem kommutativen Gesetz der Multiplikation*: $a \cdot b = b \cdot a$.
5. *Dem distributiven Gesetz*: $a \cdot (b + c) = a \cdot b + a \cdot c$.
6. *Dem Gesetz der unbeschränkten und eindeutigen Subtraktion.*

Es gibt in Σ ein einziges Element x, das die Gleichung $a + x = b$ befriedigt. (Man bezeichnet $x = b - a$.)

Aus diesen Eigenschaften folgt die Existenz der Null; ein Ring braucht aber keine Einheit zu besitzen; und es kann das Produkt zweier Elemente verschwinden, ohne daß ein Faktor verschwindet. Ringe, für die aus dem Verschwinden eines Produktes stets das Verschwinden eines Faktors folgt, und die außerdem eine Einheit besitzen, werden als *eigentliche Integritätsbereiche* bezeichnet. Für die endliche Summe $a + a \ldots + a$ führen wir die übliche abkürzende Bezeichnung na ein, wobei die ganzen Zahlen n lediglich als abkürzende Zeichen, nicht als Ringelemente zu betrachten sind, und durch $a = 1 \cdot a$, $na + a = (n+1)a$ rekurrierend definiert sind.

Emmy Noether

Noether Ring

环的定义

定义

环是指三元组$(R,+,\cdot)$：非空集合R、其上两个二元运算$+$以及$\cdot$，分别称为加法和乘法，使得下述八条公理成立：

(A1) $(a+b)+c=a+(b+c)$

(A2) $a+b=b+a$

(A3) 有零元素0_R

(A4) 有负元

(M1) $(a\cdot b)\cdot c=a\cdot(b\cdot c)$

(M2) 有幺元1_R（又称单位元）

(D1) 分配律

(D2) 分配律

定义的说明

1. 我们仅考虑含幺环
2. 约定：三元组$(R,+,\cdot)$简记为环R
3. **环相等**$(R,+,\cdot)=(R',+',\cdot')$当且仅当集合相等$R=R'$，且映射相等$+=+'$及$\cdot=\cdot'$
4. 环R中的**减法**运算: $a-b:=a+(-b)$, 加法的逆运算

基本例子

1. 整数环$\mathbb{Z} = (\mathbb{Z}, +, \cdot)$
2. Gauss整数环$\mathbb{Z}[\sqrt{-1}]$
3. 一元多项式环$\mathbb{Q}[x]$, x为字母（此处强调：x为符号、不取值的未定元）
4. 同余类环$\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$, $n \geq 2$
5. 矩阵环$M_n(\mathbb{C})$（表示论课程!）

环的基本性质

定义：求和符合$\sum_{i=1}^{n} a_i = a_1 + \cdots + a_n$

定义：定义$0a = 0_R$；$n \geq 1, a \in R$, a的n倍以及$-n$倍分别定义为

$$na = a + \cdots a, (-n)a = (-a) + \cdots + (-a)$$

WARNING:“倍乘”与R中乘法是完全不同的概念!

1. 加法消去律$a + b = a + c \Rightarrow a = c$
2. $(n + m)a = na + ma$，任意$n, m \in \mathbb{Z}$
3. $na = (n1_R) \cdot a$，特别地，$0_R \cdot a = 0_R$

零环

命题

设R为环。则以下断言等价：

1. $0_R = 1_R$;
2. $R = \{0_R\}$;
3. R仅含有一个元素。

此类环称为**零环**. 我们只考虑非零环。

二元环

例子

抽象定义**二元环**$X = \{x_0, x_1\}$

加法表

$+$	x_0	x_1
x_0	x_0	x_1
x_1	x_1	x_0

乘法表

$\cdot$	x_0	x_1
x_0	x_0	x_0
x_1	x_0	x_1

尝试：如何验证X是环？

思考：环X“本质上”是模2同余类环$\mathbb{Z}_2$

记号：均记为$\mathbb{F}_2$，称**二元域**

二项式定理

称R为**交换环**，若$a \cdot b = b \cdot a$。

约定：以后，我们仅考虑含幺交换环R。

定义幂$a^n = a \cdot a \cdots a$，以及$a^0 = 1_R$。

验证：$a^n \cdot a^m = a^{m+n}$

定理 (I. Newton 1665)

设$a, b \in R$为环，$n \geq 1$。则有

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

可逆元

1. $a \in R$ 称为乘法可逆元（或单位），若存在b满足$a \cdot b = 1_R$.
2. 记号$b = a^{-1}$，进而有a^n，任意$n \in \mathbb{Z}$
3. 除法运算$c \div a := c \cdot a^{-1}$，即为乘法的逆运算

命题

设$a \in R$可逆。则有

1. $a^n \cdot a^m = a^{m+n}$
2. 乘法消去率：$a \cdot x = a \cdot y \Rightarrow x = y$

单位群

1. $U(R) = \{a \in R \mid a\text{可逆}\}$
2. 验证：$U(R)$自然成为群，称为环R的**单位群**
3. 试刻画$U(\mathbb{Z}), U(\mathbb{Z}[\sqrt{-1}]), U(\mathbb{Q}), U(\mathbb{Z}_8)$

设$u \in U(R)$。定义新的环$R_u = (R, +, \circ)$，其中新乘法为

$$a \circ b = u^{-1} \cdot a \cdot b$$

思考：R_u与R“本质”一样么？

整环与域

约定：乘法$a \cdot b$(有时)简记为ab!

定义

非零环R称为**整环**，若$ab = 0_R$蕴含$a = 0_R$或$b = 0_R$；非零换R称为**域**，若非零元均可逆。

1. 整环中满足乘法消去率
2. 域是整环
3. 域是可以做“四则运算”的环，也为解方程的操作区域!

例子

1. $\mathbb{Z}, \mathbb{Z}[\sqrt{-1}]$是整环，不是域
2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$为域
3. 同余类环$\mathbb{Z}_n$为整环 $\Leftrightarrow$ 其为域 $\Leftrightarrow$ $n = p$为素数。此时，记为$\mathbb{F}_p$
4. $U(\mathbb{Z}_n) = \{[m] \mid \gcd(m, n) = 1\}$，其阶为$\phi(n)$, Euler函数

试证明：有限环R是整环 $\Leftrightarrow$ R是域。

子环和子域

定义

(1) 设R为环。子集$S \subseteq R$称为**子环**，若满足$1_R \in S$，S对加法、减法以及乘法封闭。

(2) 设K为域。子环$S \subseteq K$称为**子域**，若满足$0_R \neq a \in S$，则$a^{-1} \in S$，即，对除法也封闭。

1. 子环自然成为环；子域自身作为环是域。
2. 这里的子环与课本上可能不同，我们强烈要求$1_R \in S$。
3. 平凡子环$R \subseteq R$
4. 整环的子环是整环。
5. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ 子环链

思考题：子环与子域

1. $\mathbb{Z}$以及$\mathbb{Z}_n$均没有真子环
2. $\mathbb{Q}$以及$\mathbb{F}_p$均没有真子域
3. 分类$\mathbb{Z}[\sqrt{-1}]$的子环。（定义：两子环$X, Y \subseteq \mathbb{Z}[\sqrt{-1}]$相等，若作为子集$X = Y$。分类=完全列出）
4. 分类$\mathbb{Q}$的子环。
5. 证明$\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$是子域，并分类$\mathbb{Q}(\sqrt{-1})$ 的子域。

部分练习

1. 环R中，证明: $na = (n1_R) \cdot a$; $(na) \cdot b = n(a \cdot b) = a \cdot (nb)$
2. 广义分配率的证明。
3. 证明：交换环的二项式定理。
4. 证明：有限整环是域。
5. $\mathbb{Q}(\sqrt{-1})$的子域分类（补充细节）。