

# 第一讲若干基本概念

陈建文

October 10, 2022

## 1 近世代数的起源

$$ax + b = 0$$

$$ax^2 + bx + c = 0$$

$$ax^3 + bx^2 + cx + d = 0$$

$$ax^4 + bx^3 + cx^2 + dx + e = 0$$

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

Abel(1802-1829):证明了一般的次数 $\geq 5$ 的一元方程没有用 $+$ ,  $-$ ,  $*$ ,  $/$ ,  $\sqrt{\quad}$ 表示的求根公式。

Crelle

Galois(1811-1832):

$$x^5 = 1$$

解决了哪些次数 $\geq 5$ 的一元方程有求根公式, 哪些没有的问题, 构思了群的概念

Liouville

群的概念来源于三个主要的数学领域: 代数方程论, 几何, 数论

Cantor(1845-1918):创立集合论

Noether(1882-1935):现代代数学之母

van der Waerden:Modern Algebra

Abstract Algebra

Basic Algebra

Algebra

## 2 运算

**定义1.** 设 $X$ 为一个非空集合, 一个从 $X \times X$ 到 $X$ 的映射 $\phi$ 称为集合 $X$ 上的一个二元代数运算。

注: 设 $X, Y, Z$ 为任意三个非空集合, 一个从 $X \times Y$ 到 $Z$ 的映射 $\phi$ 称为从 $X$ 与 $Y$ 到 $Z$ 的一个二元代数运算。

**定义2.** 设 $X$ 为一个非空集合, 一个从 $X$ 到 $X$ 的映射 $\phi$ 称为集合 $X$ 上的一个一元运算。

注：设 $X, Y$ 为任意两个非空集合，一个从 $X$ 到 $Y$ 的映射 $\phi$ 称为从 $X$ 到 $Y$ 的一个一元运算。

**定义3.** 设“ $\circ$ ”为非空集合 $S$ 上的一个二元代数运算，则称二元组 $(S, \circ)$ 为一个（有一个代数运算的）代数系。

类似的，可以定义具有两个代数运算的代数系 $(S, \circ, *)$ ，具有三个代数运算的代数系 $(S, \circ, *, +)$ ，等等。

我们熟知的实数集 $R$ ，与其上的加法运算“ $+$ ”和乘法运算“ $*$ ”一起构成了一个代数系，满足如下性质：

1. 对任意的 $x \in R, y \in R, z \in R, (x + y) + z = x + (y + z)$
2. 对任意的 $x \in R, 0 + x = x + 0 = x$
3. 对任意的 $x \in R, (-x) + x = x + (-x) = 0$
4. 对任意的 $x \in R, y \in R, x + y = y + x$
5. 对任意的 $x \in R, y \in R, z \in R, (x * y) * z = x * (y * z)$
6. 对任意的 $x \in R, 1 * x = x * 1 = x$
7. 对任意的 $x \in R, x \neq 0 \rightarrow x^{-1} * x = x * x^{-1} = 1$
8. 对任意的 $x \in R, y \in R, x * y = y * x$
9. 对任意的 $x \in R, y \in R, z \in R, x * (y + z) = x * y + x * z$
10. 对任意的 $x \in R, y \in R, z \in R, (y + z) * x = y * x + z * x$
11. 对任意的 $x \in R, x \leq x$ 。
12. 对任意的 $x \in R, y \in R$ ，如果 $x \leq y$ 并且 $y \leq x$ ，则 $x = y$ 。
13. 对任意的 $x \in R, y \in R, z \in R$ ，如果 $x \leq y$ 并且 $y \leq z$ ，则 $x \leq z$ 。
14. 对任意的 $x \in R, y \in R, x \leq y$ 和 $y \leq x$ 两者中必有其一成立。  
我们用 $x < y$ 表示 $x \leq y$ 并且 $x \neq y$ ， $x \geq y$ 表示 $y \leq x$ ， $x > y$ 表示 $x \geq y$ 并且 $x \neq y$ 。
15. 对任意的 $x \in R, y \in R, z \in R$ ，如果 $x < y$ ，则 $x + z < y + z$ 。
16. 对任意的 $x \in R, y \in R$ ，如果 $x > 0, y > 0$ ，则 $xy > 0$ 。
17. 设 $A_1, A_2, \dots, A_i, \dots$ 为实数集 $R$ 上的闭区间， $A_1 \supseteq A_2 \supseteq A_3 \supseteq \dots \supseteq A_i \supseteq \dots$ ，则 $\bigcap_{i=1}^{\infty} A_i$ 非空。

**定义4.** 设“ $\circ$ ”为集合 $S$ 上的一个二元代数运算。如果 $\forall a, b, c \in S, (a \circ b) \circ c = a \circ (b \circ c)$ ，则称二元代数运算“ $\circ$ ”满足结合律。

**定理1.** 设 $(S, \circ)$ 为一个代数系，如果二元代数运算“ $\circ$ ”满足结合律，则 $\forall a_i \in S, i = 1, 2, \dots, n, n$ 个元素 $a_1, a_2, \dots, a_n$ 的乘积由它们的次序唯一确定。

证明. 用  $a_1 \circ a_2 \circ \cdots \circ a_n$  表示按照  $a_1, a_2, \cdots, a_n$  的次序进行“ $\circ$ ”运算时任意加括号所得到的运算结果。

以下用数学归纳法证明  $a_1 \circ a_2 \circ \cdots \circ a_n = (((a_1 \circ a_2) \circ a_3) \circ \cdots) \circ a_n$ 。

当  $n = 1$  时结论显然成立。

假设当  $n < k$  时结论成立, 往证当  $n = k$  时结论也成立。

对  $k$  个元素按  $a_1, a_2, \cdots, a_k$  的次序不论用什么方法加括号确定计算方案, 最后一步必是两个元素的乘积, 不妨设为  $b_1 \circ b_2$ , 这里  $b_1$  为前  $i$  个元素  $a_1, a_2, \cdots, a_i$  之积, 而  $b_2$  为后  $k - i$  个元素  $a_{i+1}, \cdots, a_k$  之积。

$$\begin{aligned} b_1 \circ b_2 &= (((((a_1 \circ a_2) \circ a_3) \circ \cdots) \circ a_i) \circ (((((a_{i+1} \circ a_{i+2}) \circ a_{i+3}) \circ \cdots) \circ a_k) \\ &= ((((((a_1 \circ a_2) \circ a_3) \circ \cdots) \circ a_i) \circ (((((a_{i+1} \circ a_{i+2}) \circ a_{i+3}) \circ \cdots) \circ a_{k-1})))) \circ a_k \\ &= (((((a_1 \circ a_2) \circ a_3) \circ \cdots) \circ a_{k-1}) \circ a_k \end{aligned}$$

□

Scala: Martin Ordersky

C++ STL: Alexander Stepanov

**定义5.** 设“ $\circ$ ”为集合  $S$  上的一个二元代数运算。如果  $\forall a, b \in S$ ,  $a \circ b = b \circ a$ , 则称二元代数运算“ $\circ$ ”满足交换律。

**定理2.** 设  $(S, \circ)$  为一个代数系, 如果二元代数运算“ $\circ$ ”满足结合律和交换律, 则  $\forall a_i \in S, i = 1, 2, \cdots, n$ ,  $n$  个元素  $a_1, a_2, \cdots, a_n$  的乘积仅与这  $n$  个元素有关而与它们的次序无关。

证明. 留作课后作业题。

□

**定义6.** 设“ $+$ ”与“ $\circ$ ”为集合  $S$  上的两个二元代数运算。如果  $\forall a, b, c \in S$ ,

$$a \circ (b + c) = a \circ b + a \circ c,$$

则称二元代数运算“ $\circ$ ”对“ $+$ ”满足左分配律。如果  $\forall a, b, c \in S$ ,

$$(b + c) \circ a = b \circ a + c \circ a,$$

则称二元代数运算“ $\circ$ ”对“ $+$ ”满足右分配律。

**定理3.** 设  $(S, +, \circ)$  为具有两个二元代数运算的代数系, “ $+$ ”满足结合律。如果“ $\circ$ ”对“ $+$ ”满足左分配律, 则对任意的  $a, a_i \in S, i = 1, 2, \cdots, n$ , 有

$$a \circ (a_1 + a_2 + \cdots + a_n) = a \circ a_1 + a \circ a_2 + \cdots + a \circ a_n$$

如果“ $\circ$ ”对“ $+$ ”满足右分配律, 则对任意的  $a, a_i \in S, i = 1, 2, \cdots, n$ , 有

$$(a_1 + a_2 + \cdots + a_n) \circ a = a_1 \circ a + a_2 \circ a + \cdots + a_n \circ a$$

**定义7.** 设 $(S, \circ)$ 为一个代数系。如果存在一个元素 $e_l \in S$ , 使得 $\forall a \in S$ ,

$$e_l \circ a = a$$

则称 $e_l$ 为“ $\circ$ ”运算的左单位元素；如果存在一个元素 $e_r \in S$ , 使得 $\forall a \in S$ ,

$$a \circ e_r = a$$

则称 $e_r$ 为“ $\circ$ ”运算的右单位元素；如果存在一个元素 $e \in S$ , 使得 $\forall a \in S$ ,

$$e \circ a = a \circ e = a$$

则称 $e$ 为“ $\circ$ ”运算的单位元素。

**定理4.** 设 $(S, \circ)$ 为一个代数系, 如果二元代数运算 $\circ$ 既有左单位元 $e_l$ , 又有右单位元 $e_r$ , 则 $e_l = e_r$ , 从而有单位元。

证明.  $e_r = e_l \circ e_r = e_l$

□

### 3 课后作业题

**练习1.** 设 $(S, \circ)$ 为一个代数系, 如果二元代数运算“ $\circ$ ”满足结合律和交换律, 则 $\forall a_i \in S, i = 1, 2, \dots, n$ ,  $n$ 个元素 $a_1, a_2, \dots, a_n$ 的乘积仅与这 $n$ 个元素有关而与它们的次序无关。