第一讲若干基本概念

陈建文

January 19, 2023

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≥ 5的一元方程没有用$+, -, *, /, \sqrt[n]{\ }$表示的求根公式。

Crelle

Galois(1811-1832):

$x^5 = 1$

解决了哪些次数≥ 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

群的概念主要来源于三个数学领域：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 基本概念

定义1. **设**X为一个非空集合，一个从$X \times X$到X的映射ϕ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ϕ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ϕ称为集合X上的一个一元代数运算。

注：设X,Y为任意两个非空集合，一个从X到Y的映射ϕ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$x\in R$，$x\neq 0\to x^{-1}*x=x*x^{-1}=1$
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，$\cdots$，A_i，$\cdots$为实数集R上的闭区间，$A_1\supseteq A_2\supseteq A_3\supseteq\cdots\supseteq A_i\supseteq\cdots$，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$\forall a_i\in S$，$i=1,2,\cdots,n$，n个元素$a_1,a_2,\cdots,a_n$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$e_l = e_r$，从而有单位元且单位元是唯一的。

证明. $e_r = e_l \circ e_r = e_l$。 □

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$\forall a_i \in S$，$i = 1, 2, \cdots, n$，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. 设π为任意一个从集合$\{1, 2, \cdots, n\}$到$\{1, 2, \cdots, n\}$的一个双射，以下用数学归纳法证明$a_{\pi(1)} \circ a_{\pi(2)} \circ \cdots \circ a_{\pi(n)} = (((a_1 \circ a_2) \circ a_3) \circ \cdots) \circ a_n$。

这里$a_{\pi(1)} \circ a_{\pi(2)} \circ \cdots \circ a_{\pi(n)}$表示按照$a_{\pi(1)}, a_{\pi(2)}, \cdots, a_{\pi(n)}$的次序进行"$\circ$"运算时任意加括号所得到的运算结果。

当$n = 1$时，结论显然成立。

假设当$n = k$时结论成立，往证当$n = k + 1$时，结论也成立。

设$\pi(i) = k + 1$，则

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

□