

高等学校教学参考书

近世代数基础

(1978年修订本)

张禾瑞著

高等教育出版社

目 录

修订本说明	III
第一版序	IV
第一章 基本概念	1
§ 1. 集合	1
§ 2. 映射	4
§ 3. 代数运算	7
§ 4. 结合律	10
§ 5. 交换律	13
§ 6. 分配律	14
§ 7. 一一映射、变换	16
§ 8. 同态	19
§ 9. 同构、自同构	23
§ 10. 等价关系与集合的分类	27
第二章 群论	31
§ 1. 群的定义	31
§ 2. 单位元、逆元、消去律	35
§ 3. 有限群的另一定义	38
§ 4. 群的同态	40
§ 5. 变换群	44
§ 6. 置换群	50
§ 7. 循环群	56
§ 8. 子群	61
§ 9. 子群的陪集	65
§ 10. 不变子群、商群	70
§ 11. 同态与不变子群	75
第三章 环与域	80
§ 1. 加群、环的定义	80

§ 2. 交换律、单位元、零因子、整环	84
§ 3. 除环、域	89
§ 4. 无零因子环的特征	93
§ 5. 子环、环的同态	97
§ 6. 多项式环	101
§ 7. 理想	110
§ 8. 剩余类环、同态与理想	113
§ 9. 最大理想	116
§ 10. 商域	119
第四章 整环里的因子分解	125
§ 1. 素元、唯一分解	125
§ 2. 唯一分解环	130
§ 3. 主理想环	135
§ 4. 欧氏环	138
§ 5. 多项式环的因子分解	141
§ 6. 因子分解与多项式的根	148
第五章 扩域	151
§ 1. 扩域、素域	151
§ 2. 单扩域	154
§ 3. 代数扩域	160
§ 4. 多项式的分裂域	165
§ 5. 有限域	171
§ 6. *可离扩域	175
名词索引	182

第一章 基本概念

在普通代数里,我们计算的对象是数,计算的方法是加、减、乘、除. 数学渐渐进步,我们发现,可以对于若干不是数的事物,用类似普通计算的方法来加以计算. 这种例子我们在高等代数里已经看到很多,例如对于向量、矩阵、线性变换等就都可以进行运算. 近世代数(或抽象代数)的主要内容就是研究所谓代数系统,即带有运算的集合. 近世代数在数学的其他分支和自然科学的许多部门里都有重要的应用. 最近二十多年来,它的一些成果更被直接应用于某些新兴的技术.

我们在高等代数里已初步接触到的群、环、域是三个最基本的代数系统. 在本书里我们要对这三个代数系统做略进一步的介绍.

在这一章里,我们先把常要用到的基本概念介绍一下. 这些基本概念中的某一些,例如集合和映射,在高等代数里已经出现过. 但为了完整起见,我们不得不有所重复.

§ 1. 集 合

若干个(有限或无限多个)固定事物的全体叫做一个**集合**(简称**集**).

组成一个集合的事物叫做这个集合的**元素**(有时简称**元**).

关于集合,我们常用到几个名词和符号,现在把它们说明一下. 首先我们要规定空集合这一个概念.

定义 一个没有元素的集合叫做**空集合**.

空集合好象没有什么意义,但我们的确有用得到这个概念的

地方。这一点我们不久就会看到。

元素我们一般用小写拉丁字母 a, b, c, \dots 来表示, 集合用大写拉丁字母 A, B, C, \dots 来表示. 一个集合 A 若是由元素 a, b, c, \dots 作成的, 我们用符号

$$A = \{a, b, c, \dots\}$$

来表示.

若 a 是集合 A 的一个元素, 我们说, a 属于 A , 或是说, A 包含 a , 用符号

$$a \in A \quad \text{或是} \quad A \ni a$$

来表示.

若 a 不是集合 A 的元素, 我们说, a 不属于 A , 或是说, A 不包含 a , 用符号

$$a \notin A \quad \text{或是} \quad A \not\ni a$$

来表示.

定义 若集合 B 的每一个元都属于集合 A , 我们说, B 是 A 的**子集**; 不然的话, 我们说, B 不是 A 的子集.

B 是 A 的子集, 我们说, B 属于 A , 或是说, A 包含 B , 用符号

$$B \subset A \quad \text{或是} \quad A \supset B$$

来表示. B 不是 A 的子集, 我们说, B 不属于 A , 或是说, A 不包含 B , 用符号

$$B \not\subset A \quad \text{或是} \quad A \not\supset B$$

来表示.

注意: 空集合被认为是任何集合的子集.

定义 若集合 B 是集合 A 的子集, 而且至少有一个 A 的元不属于 B , 我们就说, B 是 A 的**真子集**; 不然的话, 我们说, B 不是 A 的真子集.

若集合 A 和集合 B 所包含的元完全一样, 那么 A 和 B 表示的

是同一集合,这时我们说, A 等于 B ,用符号

$$A=B$$

来表示. 显然

$$A=B \iff A \subset B, B \subset A$$

一个元 a 若同时属于 A 和 B 两个集合,我们说, a 是 A 和 B 的共同元.

定义 集合 A 和集合 B 的所有共同元所组成的集合叫做 A 和 B 的交集.

A 和 B 的交集我们用符号

$$A \cap B$$

来表示.

例 1 $A = \{1, 2, 3\}, B = \{2, 5, 6\}$. 那么

$$A \cap B = \{2\}$$

$A = \{1, 2, 3\}, B = \{4, 5, 6\}$. 那么

$$A \cap B = \text{空集合}$$

这里,我们看到空集合这个概念的用处.

定义 由至少属于集合 A 和 B 之一的一切元素组成的集合叫做 A 和 B 的并集.

A 和 B 的并集我们用符号

$$A \cup B$$

来表示.

例 2 $A = \{1, 2, 3\}, B = \{2, 4, 6\}$. 那么

$$A \cup B = \{1, 2, 3, 4, 6\}$$

$A = \{1, 2, 3\}, B = \{4, 5, 6\}$. 那么

$$A \cup B = \{1, 2, 3, 4, 5, 6\}$$

两个以上的集合 $A_1, A_2 \dots$ 的交集、并集的定义和上面完全类似.

定义 令 A_1, A_2, \dots, A_n 是 n 个集合. 由一切从 A_1, A_2, \dots, A_n 里顺序取出的元素组 (a_1, a_2, \dots, a_n) ($a_i \in A_i$) 所做成的集合叫做集合 A_1, A_2, \dots, A_n 的积, 记成

$$A_1 \times A_2 \times \dots \times A_n$$

习 题

1. $B \subset A$, 但 B 不是 A 的真子集, 这个情况什么时候才能出现?
2. 假定 $A \subset B$. $A \cap B = ?$ $A \cup B = ?$

§ 2. 映 射

在高等代数里已经看到映射这一概念的重要性. 现在我们给出这一概念的一个比较一般的定义.

我们看 n 个集合 A_1, A_2, \dots, A_n 和另外一个集合 D .

定义 假如通过一个法则 ϕ , 对于任何一个 $A_1 \times A_2 \times \dots \times A_n$ 的元 (a_1, a_2, \dots, a_n) ($a_i \in A_i$), 都能得到一个唯一的 D 的元 d , 那么这个法则 ϕ 叫做集合 $A_1 \times A_2 \times \dots \times A_n$ 到集合 D 的一个映射; 元 d 叫做元 (a_1, a_2, \dots, a_n) 在映射 ϕ 之下的象; 元 (a_1, a_2, \dots, a_n) 叫做元 d 在 ϕ 下的一个逆象.

一个映射我们常用以下符号来描写,

$$\phi: (a_1, a_2, \dots, a_n) \longrightarrow d = \phi(a_1, a_2, \dots, a_n)$$

这里, ϕ 代表所给的法则, 也就是所给的映射;

$$(a_1, a_2, \dots, a_n) \longrightarrow d$$

表示 ϕ 替 (a_1, a_2, \dots, a_n) 这个元规定的象是 d ; 至于 $\phi(a_1, a_2, \dots, a_n)$ 只是一个符号, 就是说, 我们有时把 d 这个元写成 $\phi(a_1, a_2, \dots, a_n)$. 但这个符号也不是毫无意义的. 这个符号暗示, d 是把 ϕ 应用到 (a_1, a_2, \dots, a_n) 上所得的结果.

在以上的定义中, 有几点应该特别加以注意, 我们用下面的几

个例来说明一下。

例 1 $A_1 = A_2 = \dots = A_n = D =$ 所有实数作成的集合。

$\phi: (a_1, a_2, \dots, a_n) \longrightarrow a_1^2 + a_2^2 + \dots + a_n^2 = \phi(a_1, a_2, \dots, a_n)$

是一个 $A_1 \times A_2 \times \dots \times A_n$ 到 D 的映射。这里, A_i 和 D 都是相同的集合, 但这没有什么关系, 因为映射的定义并没有说, A_1, A_2, \dots, A_n, D 这几个集合中不许有相同的。

例 2 $A_1 = \{\text{东, 西}\}, A_2 = \{\text{南}\}, D = \{\text{高, 低}\}.$

$\phi_1: (\text{西, 南}) \longrightarrow \text{高} = \phi_1(\text{西, 南})$

不是一个 $A_1 \times A_2$ 到 D 的映射。因为, 这个 ϕ_1 只替(西, 南)这一个元规定了一个象; 但我们从 $A_1 \times A_2$ 里还可以取出另一个元来, 就是(东, 南), 替这一个元, ϕ_1 并没有规定什么象。这和定义中一个映射必须替每一个元规定一个象的要求不合。

假如 ϕ_2 是如下的一个法则

$\phi_2: (\text{西, 南}) \longrightarrow \text{高}, (\text{东, 南}) \longrightarrow \text{低}$

那么 ϕ_2 是一个 $A_1 \times A_2$ 到 D 的映射。

在例 1 里, $A_1 = A_2 = \dots = A_n$ 。对于那里的映射 ϕ 来说, A_i 的次序没有什么关系, 比方说, ϕ 也是 $A_2 \times A_1 \times \dots \times A_n$ 到 D 的映射。但对例 2 里的映射 ϕ_2 来说, A_1 和 A_2 的次序不能变动, ϕ_2 不是一个 $A_2 \times A_1$ 到 D 的映射。因为 ϕ_2 只替(西, 南)和(东, 南)各规定了一个象, 但并没有替(南, 西)和(南, 东)规定什么象。

例 3 $A_1 = D =$ 所有实数作成的集合。

$\phi: \begin{array}{ll} a \longrightarrow a, & \text{若是 } a \neq 1 \\ 1 \longrightarrow b, & \text{这里 } b^2 = 1 \end{array}$

不是一个 A_1 到 D 的映射。因为, 这个 ϕ 固然替每一个不等于 1 的 a 规定了一个唯一的象; 但通过这个 ϕ , 我们不能决定 b 是 1 还是 -1, 这就是说, ϕ 没有替 1 规定一个唯一的象: 这是与定义不合的。

例 4 $A_1 = D =$ 所有正整数作成的集合。

$$\phi: \quad a \longrightarrow a-1$$

不是一个 A_1 到 D 的映射。因为这个 ϕ 固然替每一个 $a \neq 1$ 规定了一个唯一的象 $a-1$ ；但当 $a=1$ 的时候， $a-1 \notin D$ ：这是与定义不合的。

总结起来说，我们对于映射的定义应当注意以下几点：

1. 集合 A_1, A_2, \dots, A_n, D 中可能有几个是相同的；
2. 一般， A_1, A_2, \dots, A_n 的次序不能掉换；
3. 映射 ϕ 一定要替每一个元 (a_1, a_2, \dots, a_n) 规定一个象 d ；
4. 一个元 (a_1, a_2, \dots, a_n) 只能有一个唯一的象；
5. 所有的象都必须是 D 的元。

给了集合 A_1, A_2, \dots, A_n, D ，一般来说，有各种不同的法则可以替每一个元 (a_1, a_2, \dots, a_n) 规定一个象。有时两个法则虽然不同，但它们替每一个元所规定的象却永远相同。

定义 我们说， $A_1 \times A_2 \times \dots \times A_n$ 到 D 的两个映射 ϕ_1 和 ϕ_2 是相同的，假如对于任何一个元 (a_1, a_2, \dots, a_n) 来说，

$$\phi_1(a_1, a_2, \dots, a_n) = \phi_2(a_1, a_2, \dots, a_n)$$

我们所以这样规定的原因是，两个映射本身是不是相同对于我们并不重要，重要的是它们的效果是不是相同。

例 5 $A = D =$ 所有正整数的集合。

$$\phi_1: \quad a \longrightarrow 1 = \phi_1(a)$$

$$\phi_2: \quad a \longrightarrow a^0 = \phi_2(a)$$

这里替每一个 a 规定象的法则，换一句话说，我们的映射，本身并不相同。但照我们的定义这两个映射是相同的。

习 题

1. $A = \{1, 2, 3, \dots, 100\}$ 。找一个 $A \times A$ 到 A 的映射。

2. 在你为习题 1 所找到的映射之下, 是不是 A 的每一个元都是 $A \times A$ 的一个元的象?

§ 3. 代数运算

在本章开头已经说过, 我们要研究带有运算的集合. 现在我们利用映射的概念, 来定义代数运算这一个概念. 我们看两个集合 A, B 和另一个集合 D .

定义 一个 $A \times B$ 到 D 的映射叫做一个 $A \times B$ 到 D 的**代数运算**.

按照我们的定义, 一个代数运算只是一种特殊的映射. 在一般映射的定义里, 一方面有 n 个集合 A_1, A_2, \dots, A_n 出现, 另一方面有一个集合 D 出现, 这里 n 可以是任何正整数. 假如我们有一个特殊的映射, 它一方面只和两个集合 A, B , 另一方面和一个集合 D 发生关系, 就把它叫做一个代数运算. 让我们看一看, 为什么把这样的一个特殊映射叫做代数运算. 假定我们有一个 $A \times B$ 到 D 的代数运算, 按照定义, 给了一个 A 的任意元 a 和一个 B 的任意元 b , 就可以通过这个代数运算, 得到一个 D 的元 d . 我们也可以说, 所给代数运算能够对 a 和 b 进行运算, 而得到一个结果 d . 这正是普通的计算法的特征, 比方说, 普通加法也不过是能够把任意两个数加起来, 而得到另一个数.

代数运算既是一种特殊的映射, 描写它的符号, 也可以特殊一点. 一个代数运算我们用 \circ 来表示, 用以前的符号, 就可以写

$$\circ: \quad (a, b) \longrightarrow d = \circ(a, b)$$

我们说过, $\circ(a, b)$ 完全是一个符号, 现在为方便起见, 不写 $\circ(a, b)$, 而写 $a \circ b$. 这样, 我们描写代数运算的符号, 就变成

$$\circ: \quad (a, b) \longrightarrow d = a \circ b$$

我们举几个例.

例 1 $A = \{\text{所有整数}\}$, $B = \{\text{所有不等于零的整数}\}$, $D = \{\text{所有有理数}\}$.

$$\circ: (a, b) \longrightarrow \frac{a}{b} = a \circ b$$

是一个 $A \times B$ 到 D 的代数运算, 也就是普通的除法.

例 2 令 V 是数域 F 上一个向量空间. 那么 F 的数与 V 的向量间的乘法是一个 $F \times V$ 到 V 的代数运算.

例 3 $A = \{1\}$, $B = \{2\}$, $D = \{\text{奇, 偶}\}$.

$$\circ: (1, 2) \longrightarrow \text{奇} = 1 \circ 2$$

是一个 $A \times B$ 到 D 的代数运算.

例 4 $A = \{1, 2\}$, $B = \{1, 2\}$, $D = \{\text{奇, 偶}\}$.

$$\circ: (1, 1) \longrightarrow \text{奇}, (2, 2) \longrightarrow \text{奇}$$

$$(1, 2) \longrightarrow \text{奇}, (2, 1) \longrightarrow \text{偶}$$

是一个 $A \times B$ 到 D 的代数运算.

注意: 跟一般映射的情形一样, 当 $A = B$ 的时候, A, B 的次序对于一个 $A \times B$ 到 D 的代数运算来说没有什么关系, 一个 $A \times B$ 到 D 的代数运算也是一个 $B \times A$ 到 D 的代数运算. 但 A 和 B 的次序可以掉换并不是说, 对于 A 的任意元 a, B 的任意元 b , 有

$$a \circ b = b \circ a$$

因为 A 和 B 的次序可以掉换只是说, $a \circ b$ 和 $b \circ a$ 都有意义, 并不是说, $a \circ b = b \circ a$. 比方说, 例 4 的 A, B 就是相等的集合, 但

$$1 \circ 2 = \text{奇}$$

$$2 \circ 1 = \text{偶}$$

在 A 和 B 都是有限集合的时候, 一个 $A \times B$ 到 D 的代数运算, 我们常用一个表, 叫做运算表来说明. 假定 A 有 n 个元 a_1, \dots, a_n , B 有 m 个元 b_1, \dots, b_m ,

$$\circ: (a_i, b_j) \longrightarrow d_{ij}$$

是所给的代数运算. 我们先画一垂线, 在这垂线上端画一向右的

横线. 把 A 的元 a_1, a_2, \dots, a_n 依次写在垂线的左边, 把 B 的元 b_1, b_2, \dots, b_m 依次写在横线的上边, 然后把对 a_i 和 b_j 进行运算后所得结果 d_{ij} 写在从 a_i 右行的横线和从 b_j 下行的垂线的交点上:

	b_1	b_2	\dots	b_m
a_1	d_{11}	d_{12}	\dots	d_{1m}
a_2	d_{21}	d_{22}	\dots	d_{2m}
\vdots	\dots	\dots	\dots	\dots
a_n	d_{n1}	d_{n2}	\dots	d_{nm}

比方说, 例 4 的代数运算的运算表是

	1	2
1	奇	奇
2	偶	奇

用运算表来说明一个代数运算, 常比用箭头或用等式的方法省事, 并且清楚.

$A \times B$ 到 D 的一般代数运算用到的时候比较少. 最常用的代数运算是 $A \times A$ 到 A 的代数运算. 在这样的一个代数运算之下, 可以对 A 的任意两个元加以运算, 而且所得结果还是在 A 里面. 所以我们有

定义 假如 \circ 是一个 $A \times A$ 到 A 的代数运算, 我们就说, 集合 A 对于代数运算 \circ 来说是闭的, 也说, \circ 是 A 的代数运算或二元运算.

习 题

1. $A = \{\text{所有不等于零的偶数}\}$. 找一个集合 D , 使得普通除法是 $A \times A$ 到 D 的代数运算. 是不是找得到一个以上的这样的 D ?
2. $A = \{a, b, c\}$. 规定 A 的两个不同的代数运算.

§ 4. 结 合 律

从上一节的 3, 4 两例, 我们可以看出, 一个代数运算是可以相当任意规定的, 并不一定有多大意义. 假如我们任意取几个集合, 任意给它们规定几个代数运算, 我们很难希望, 可以由此算出什么好的结果来. 所以以下将遇到的代数运算都适合某些从实际中来的规律. 常见的这种规律的第一个, 就是结合律.

我们看一个集合 A , 一个 $A \times A$ 到 A 的代数运算 \circ .

在 A 里任意取出三个元 a, b, c 来, 假如我们写下符号

$$a \circ b \circ c$$

那么这个符号没有什么意义, 因为代数运算只能对两个元进行运算. 但是我们可以先对 a 和 b 进行运算, 而得到 $a \circ b$, 因为 \circ 是 $A \times A$ 到 A 的代数运算, $a \circ b \in A$, 所以我们又可以把这个元同 c 来进行运算, 而得到一个结果. 这样得来的结果, 普通用加括号的方法来表示, 所用的步骤也就叫做加括号的步骤. 由上面所描写的步骤得来的结果, 用加括号的方法写出来, 就是

$$(a \circ b) \circ c$$

但我们还有另外一种加括号的步骤, 它的结果用加括号的方法写出来是

$$a \circ (b \circ c)$$

在一般情形之下, 由这两个不同的步骤所得的结果也未必相同. 我们举一个例.

例 $A = \{\text{所有整数}\}$. 代数运算是普通减法. 那么

$$(a - b) - c \neq a - (b - c), \quad \text{除非 } c = 0$$

现在我们下一个

定义 我们说, 一个集合 A 的代数运算 \circ 适合结合律, 假如对于 A 的任何三个元 a, b, c 来说, 都有

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

(注意: a, b, c 不一定是不相同的元.)

让我们看一看, 结合律有什么作用.

在 A 里任意取出 n 个元 a_1, a_2, \dots, a_n 来, 假如我们写下符号

$$a_1 \circ a_2 \circ \dots \circ a_n$$

这个符号当然也没有意义. 但是假如我们用一个加括号的步骤, 当然也会得到一个结果. 加括号的步骤自然不止一种, 但因为 n 是一个有限整数, 这种步骤的个数总是一个有限整数. 假定它是 N , 我们把由这 N 个步骤所得的结果用

$$\pi_1(a_1 \circ a_2 \circ \dots \circ a_n), \pi_2(a_1 \circ a_2 \circ \dots \circ a_n), \dots, \pi_N(a_1 \circ a_2 \circ \dots \circ a_n)$$

来表示. 比方说, 在上面 $n=3$ 的时候, $N=2$, 我们就可以叫

$$\pi_1(a \circ b \circ c) = (a \circ b) \circ c, \pi_2(a \circ b \circ c) = a \circ (b \circ c)$$

这样得来的 N 个 $\pi(a_1 \circ a_2 \circ \dots \circ a_n)$ 当然未必相等, 但是它们也都相等. 我们规定:

定义 假如对于 A 的 n ($n \geq 2$) 个固定的元 a_1, a_2, \dots, a_n 来说, 所有的 $\pi(a_1 \circ a_2 \circ \dots \circ a_n)$ 都相等, 我们就把由这些步骤可以得到的唯一的结果, 用 $a_1 \circ a_2 \circ \dots \circ a_n$ 来表示.

现在我们证明

定理 假如一个集合 A 的代数运算 \circ 适合结合律, 那么对于 A 的任意 n ($n \geq 2$) 个元 a_1, a_2, \dots, a_n 来说, 所有的 $\pi(a_1 \circ a_2 \circ \dots \circ a_n)$ 都相等; 因此符号 $a_1 \circ a_2 \circ \dots \circ a_n$ 也就总有意义.

证明 用数学归纳法.

我们知道, 若是只看两个或三个元, 定理是对的.

假定, 若是元的个数 $\leq n-1$, 定理是对的. 我们说, 在这个假定之下, 对于一个任意的 $\pi(a_1 \circ a_2 \circ \dots \circ a_n)$ 来说

$$(1) \quad \pi(a_1 \circ a_2 \circ \dots \circ a_n) = a_1 \circ (a_2 \circ a_3 \circ \dots \circ a_n)$$

这一步能够证明, 我们的定理也就证明了.

这一个 $\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$ 是经过一种加括号的步骤所得来的结果,这个步骤的最后一步总是对两个元进行运算:

$$\pi(a_1 \circ a_2 \circ \cdots \circ a_n) = b_1 \circ b_2$$

这里, b_1 是前面的若干个,假定是*i*个元 a_1, a_2, \dots, a_i 经过一个加括号的步骤所得的结果, b_2 是其余的*n-i*个元 $a_{i+1}, a_{i+2}, \dots, a_n$ 经过一个加括号的步骤所得的结果.因为*i*和*n-i*都 $\leq n-1$,由归纳法的假定,

$$b_1 = a_1 \circ a_2 \circ \cdots \circ a_i, \quad b_2 = a_{i+1} \circ a_{i+2} \circ \cdots \circ a_n$$

$$\pi(a_1 \circ a_2 \circ \cdots \circ a_n) = (a_1 \circ a_2 \circ \cdots \circ a_i) \circ (a_{i+1} \circ a_{i+2} \circ \cdots \circ a_n)$$

假如*i*=1,那么上式就是(1)式,我们用不着再证明什么.假定*i*>1,那么

$$\begin{aligned} \pi(a_1 \circ a_2 \circ \cdots \circ a_n) &= [a_1 \circ (a_2 \circ \cdots \circ a_i)] \circ (a_{i+1} \circ a_{i+2} \circ \cdots \circ a_n) \\ &= a_1 \circ [(a_2 \circ \cdots \circ a_i) \circ (a_{i+1} \circ a_{i+2} \circ \cdots \circ a_n)] \\ &= a_1 \circ (a_2 \circ a_3 \circ \cdots \circ a_n) \end{aligned}$$

即(1)式仍然成立.证完.

由于这个定理,假如结合律成立,我们就随时都可以应用 $a_1 \circ a_2 \circ \cdots \circ a_n$ 这个符号,这对于我们当然是一件极方便的事.结合律的重要也就在此.

习 题

1. $A = \{\text{所有不等于零的实数}\}$. \circ 是普通除法: $a \circ b = \frac{a}{b}$. 这个代数运算适合不适合结合律?

2. $A = \{\text{所有实数}\}$.

\circ :

$$(a, b) \longrightarrow a + 2b = a \circ b$$

这个代数运算适合不适合结合律?

3. $A = \{a, b, c\}$. 由表

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

所给的代数运算适合不适合结合律?

§ 5. 交 换 律

一个代数运算常适合的另一规律,就是交换律.

我们知道,在一个 $A \times A$ 到 D 的代数运算 \circ 之下, $a \circ b$ 未必等于 $b \circ a$. 但是凑巧 $a \circ b$ 也可以等于 $b \circ a$.

定义 我们说,一个 $A \times A$ 到 D 的代数运算 \circ 适合交换律,假如对于 A 的任何两个元 a, b 来说,都有

$$a \circ b = b \circ a$$

我们有一个与上节的定理类似的

定理 假如一个集合 A 的代数运算 \circ 同时适合结合律与交换律,那么在 $a_1 \circ a_2 \circ \cdots \circ a_n$ 里,元的次序可以掉换.

证明 我们用归纳法.

当我们只看一个或两个元的时候,定理是对的.

假定,当元的个数 $= n - 1$ 时,定理成立. 在这个假定之下,我们证明,若是把 a_i 的次序任意颠倒一下,而作成

$$a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n}$$

这里 i_1, i_2, \dots, i_n 还是 $1, 2, \dots, n$ 这 n 个整数,不过次序不同,那么

$$a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n} = a_1 \circ a_2 \circ \cdots \circ a_n$$

i_1, i_2, \dots, i_n 中一定有一个等于 n , 假定是 i_k . 那么,由于结合律,交换律以及归纳法假定,

$$\begin{aligned} a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n} &= (a_{i_1} \circ \cdots \circ a_{i_{k-1}}) \circ [a_n \circ (a_{i_{k+1}} \circ \cdots \circ a_{i_n})] \\ &= (a_{i_1} \circ \cdots \circ a_{i_{k-1}}) \circ [(a_{i_{k+1}} \circ \cdots \circ a_{i_n}) \circ a_n] \end{aligned}$$

$$\begin{aligned}
&= [(a_{i_1} \circ \cdots \circ a_{i_{k-1}}) \circ (a_{i_k} \circ \cdots \circ a_{i_n})] \circ a_n \\
&= (a_1 \circ a_2 \circ \cdots \circ a_{n-1}) \circ a_n \\
&= a_1 \circ a_2 \circ \cdots \circ a_n
\end{aligned}$$

证完

我们普通所习知的重要代数运算，都是适合交换律的。但也碰到过一些不适合交换律的代数运算，例如， n 阶矩阵以及线性变换的乘法。所以交换律也是一个极重要的规律。

习 题

1. $A = \{\text{所有实数}\}$ ， \circ 是普通减法： $a \circ b = a - b$ 。这个代数运算适合不适合交换律？

2. $A = \{a, b, c, d\}$ ，由表

	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	b	d
d	d	c	a	b

所给的代数运算适合不适合交换律？

§ 6. 分配律

结合律和交换律都只同一种代数运算发生关系。现在要讨论同两种代数运算发生关系的一种规律，就是分配律。我们看两种代数运算 \odot 和 \oplus ：

\odot 是一个 $B \times A$ 到 A 的代数运算。|

\oplus 是一个 A 的代数运算，

那么，对于任意的 B 的 b 和 A 的 a_1, a_2 来说，

$$b \odot (a_1 \oplus a_2) \text{ 和 } (b \odot a_1) \oplus (b \odot a_2)$$

都有意义，都是 A 的元。但这两个元未必相等。

定义 我们说，代数运算 \odot ， \oplus 适合第一个分配律，假如对于