近世代数

计算机科学与技术学院
唐琳琳

单选题 1分

设置

《近世代数》的研究对象是：（）

A 集合

B 映射

C 代数运算

D 代数系统

提交

内容

- 1. 集合
- 2. 映射与变换
- 3. 代数运算
- 4. 运算律
- 5. 同态与同构
- 6. 等价关系与集合的分类

代数运算

- 定义

➢集合 M 上的一个法则 $\circ$ ，如果对于集合上的每一组有序对 $a,b\in M$ ，总存在唯一的$d\in M$，使得 $a\circ b=d$ 。

那么，这样一个法则 $\circ$ 就被成为集合 M 上的代数运算。

代数运算

- 练习：

➢1. “+”, “-”, “×” 是 Z,Q,R,C 上的代数运算吗？

➢2. “-” 是否是自然数集 N 上的代数运算?

➢3. “÷” 是否是有理数集 Q 上的代数运算?

➢4. $a\circ b=\sqrt{a^2+b^2}$ 是否是整数集 Z 的代数运算?

➢5. $a\circ b=ab+1$ ， $a\circ b=a+b-10$ 是否是 Z 上的代数运算？

➢6. $A\circ B=|A|B$ 是否是集合$\left\{A_{n\times n}\,\middle|\,a_{ij}\in F,1\le i,j\le n\right\}$上的代数运算?

代数运算

- T(M)

➢记 $T(M)$ 为集合M上所有变换构成的集合,那么法则 “变换乘法或者说是变换合成” 将会是这个集合上的一个代数运算。

证明:

$\sigma,\tau\in T(M)$ ， $\forall x\in M$ $\sigma\tau(x)=\sigma(\tau(x))$

$\sigma\tau\in T(M)$

$$\sigma\circ\tau=\sigma\tau$$

代数运算

- 恒等变换

$$\sigma\varepsilon(x)=\varepsilon\sigma(x)=\sigma(x), \quad \forall x\in M \quad \text{for} \quad \forall\sigma\in T(M)$$

$$\sigma\varepsilon=\varepsilon\sigma=\sigma$$

- S(M)

$S(M)\subseteq T(M) \quad \forall\varphi\in S(M), \ \varphi$ 是一个双射变换

"变换乘法" 也是这个集合S(M)上的一个 代数运算

代数运算

- 例子

➢1.集合$M=\{1,2,3\}$的 双射变换集$S(M)=\{\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6\}$

$$\varphi_3\varphi_4(1)=\varphi_3(\varphi_4(1))=\varphi_3(2)=1$$

$$\varphi_3\varphi_4(2)=\varphi_3(\varphi_4(2))=\varphi_3(3)=3$$

$$\varphi_3\varphi_4(3)=\varphi_3(\varphi_4(3))=\varphi_3(1)=2$$

$$\varphi_3\varphi_4=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\varphi_2$$

代数运算

- “乘法表”——有限集上的代数运算的设计

$$M=\{a_1,a_2,\cdots,a_n\} \qquad a_i \circ a_j = a_{ij} \in M\ (i,j=1,2,\cdots,n)$$

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	a_{11}	a_{12}	$\cdots$	a_{1n}
a_2	a_{21}	a_{22}	$\cdots$	a_{2n}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	a_{n1}	a_{n2}	$\cdots$	a_{nn}

单选题 1分

设置

有限集M，若$|M|=n$ 则M上的代数运算有多少个?

A $n!$

B n^2

C n^n

D n^{n^2}

提交

代数运算

- “3元置换集S(M)的乘法表”

$$S(M)=\{\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6\},\qquad \circ$$

$$\varphi_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\varphi_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\varphi_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$\varphi_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\varphi_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\varphi_6=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

$\circ$	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_1	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_2	φ_2	φ_1	φ_5	φ_6	φ_3	φ_4
φ_3	φ_3	φ_4	φ_1	φ_2	φ_6	φ_5
φ_4	φ_4	φ_3	φ_6	φ_5	φ_1	φ_2
φ_5	φ_5	φ_6	φ_2	φ_1	φ_4	φ_3
φ_6	φ_6	φ_5	φ_4	φ_3	φ_2	φ_1

代数运算

- 练习

➢1. 判断$a \circ b = a^b$，$a \circ b = a+b-2$ $a \circ b = a$ 是否是N 上的代数运算？

➢2. 设计出集合$M=\{a,b,c\}$上的两种不同的代数运算，共有几个？

➢3. $\circ$ 和 $\bar{\circ}$ 是集合M上的两个代数运算, 如果

$\exists a,b \in M, \quad s.t. \ \ a \circ b \neq a \,\bar{\circ}\, b$，那么他们为$M$ 上的不同代数运算。

如果$|M|=n$，则 M 上的代数运算有多少个？

➢4. 给出集合$\{A_{n\times n} | a_{ij} \in F, 1 \le i,j \le n\}$ 上的两个不同与矩阵基本运算的代数运算。

(1) $A \circ B = AB - A - B$ (2) $A \circ B = E$

代数运算

- 练习

➢5. $M=\{1,2,3\}$ $\quad |T(M)|=?$ $\quad |S(M)|=?$

➢6. 给出自然数集 N 上的两个不同的双射变换 σ， τ ,

s.t. $\sigma\tau\neq\tau\sigma$

σ: $1\to 2$， $2\to 1$ $\quad x\to x$

τ: $1\to 3$， $3\to 1$ $\quad x\to x$

运算律

- 结合律

➢ 集合M 上的代数运算 $\circ$ ，对集合上任意三个元素$\forall a,b,c \in M$，都有以下等式成立：

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

那么，我们称此代数运算$\circ$满足结合律。

是不是所有的代数运算都满足结合律??

单选题 1分

设置

是不是所有的代数运算都满足结合律??

A 是

B 否

提交

运算律

- 例子

➢1. 自然数集N 上的代数运算 $a \circ b = ab+1$，是否满足结合律??

$$(a \circ b) \circ c = abc + c + 1$$

$$a \circ (b \circ c) = abc + a + 1$$

$$abc + c + 1 \neq abc + a + 1 \qquad (a \circ b) \circ c \neq a \circ (b \circ c)$$

$$(a \circ b) \circ c = 5$$

$$a = 1, b = 1, c = 2$$

$$a \circ (b \circ c) = 4$$

运算律

- 例子

➢2. 变换乘法 满足结合律

$\forall \sigma,\tau,\varphi \in T(M)$ ， $\forall x \in M$

$$[(\sigma\tau)\varphi](x)=(\sigma\tau)(\varphi(x))=\sigma[\tau(\varphi(x))]$$

$$[\sigma(\tau\varphi)](x)=\sigma[(\tau\varphi)(x)]=\sigma[\tau(\varphi(x))]$$

$$[(\sigma\tau)\varphi](x)=[\sigma(\tau\varphi)](x)$$

$$(\sigma\tau)\varphi=\sigma(\tau\varphi)$$

运算律

- 结合律的意义

集合 M上的代数运算 $\circ$，那么对于$\forall a,b,c,d \in M$

$$a \circ b \circ c \circ d$$

$$[(a \circ b) \circ c] \circ d \qquad a \circ [(b \circ c) \circ d]$$

$$[a \circ (b \circ c)] \circ d \qquad a \circ [b \circ (c \circ d)]$$

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

当 $\circ$ 满足结合律的时候, 上面的几个式子是相等的。

$$|M| = n \qquad a_1, a_2, \cdots, a_n \qquad s = \frac{(2n-2)!}{n!(n-1)!} \qquad \Pi_1(a_1 \circ a_2 \circ \cdots \circ a_n) \quad \Pi_2(a_1 \circ a_2 \circ \cdots \circ a_n)$$

$$\Pi_s(a_1 \circ a_2 \circ \cdots \circ a_n)$$

运算律

- 定理1

➢集合M，如果其上的代数运算 $\circ$ 满足结合律，则对M上任意 $n(n\geq 3)$ 个元素只要顺序一定，无论如何加括号，其结果都一样。

数学归纳法

$n=3$ √

$\leq n-1$ √

$\Pi_j\left(a_1\circ a_2\circ\cdots\circ a_n\right),\quad 1\leq j\leq s$

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

$b_1 \quad\rightarrow\quad a_1,a_2,\cdots,a_k$

$b_2 \quad\rightarrow\quad a_{k+1},a_{k+2},\cdots,a_n$

$$\begin{aligned}\Pi_j\left(a_1\circ a_2\circ\cdots\circ a_n\right)&=b_1\circ b_2\\&=\left(a_1\circ a_2\circ\cdots\circ a_k\right)\circ\left(a_{k+1}\circ\cdots\circ a_n\right)\\&=a_1\circ\left[\left(a_2\circ\cdots\circ a_k\right)\circ\left(a_{k+1}\circ\cdots\circ a_n\right)\right]\\&=a_1\circ\left(a_2\circ\cdots\circ a_n\right)\end{aligned}$$

$$\Pi_1\left(a_1\circ a_2\circ\cdots\circ a_n\right)=\cdots=\Pi_s\left(a_1\circ a_2\circ\cdots\circ a_n\right)$$

运算律

- 交换律

➢集合M上的代数运算 $\circ$, 如果对于$\forall a,b\in M$,都有

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

那么, 就称这个代数运算满足交换律。

是否每一个代数运算都会满足交换律呢??

运算律

- 意义和定理2

➢ 集合*M*上的代数运算 $\circ$，若它既满足结合律又满足交换律，那么任意的*n*个集合中的元素任意的结合（加括号）和交换位置的前后顺序，其所得的结果都一样。

➢ 数学归纳法 $n=2$ ∨ ， $\leq n\text{-}1$ ∨

n ?

$$a_1, a_2, \cdots, a_n \qquad a_{i_1}, a_{i_2}, \cdots, a_{i_n}$$

Let $a_{i_k} = a_1$, then

$$\begin{aligned}
a_{i_1} \circ a_{i_2} \circ \cdots a_{i_n} &= \left[\left(a_{i_1} \circ \cdots \circ a_{i_{k-1}}\right) \circ a_1\right] \circ \left(a_{i_{k+1}} \circ \cdots \circ a_{i_n}\right) \\
&= \left[a_1 \circ \left(a_{i_1} \circ \cdots \circ a_{i_{k-1}}\right)\right] \circ \left(a_{i_{k+1}} \circ \cdots \circ a_n\right) \\
&= a_1 \circ \left[\left(a_{i_1} \circ \cdots \circ a_{i_{k-1}}\right) \circ \left(a_{i_{k+1}} \circ \cdots \circ a_n\right)\right] \\
&= a_1 \circ \left(a_2 \circ \cdots \circ a_n\right) \\
&= a_1 \circ a_2 \circ \cdots \circ a_n
\end{aligned}$$

运算算律

- 分配律

➢ 集合M上两个代数运算 $\circ$ 和 $\oplus$, 如果对 $\forall a,b,c \in M$, 总有

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

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

那么, 我们称代数运算 $\circ$ 关于代数运算 $\oplus$ 分别满足左分配律和右分配律。

运算律

- 定理3

➢集合M上的两个代数运算$\circ$ 和$\oplus$ ，若$\oplus$ 满足结合律$\circ$，关于$\oplus$满足分配律。那么，对$\forall a \in M$ 和 $\forall b_1, b_2, \ldots, b_n \in M$ ，那么就有下式成立：

$$a \circ \left(b_1 \oplus b_2 \oplus \cdots \oplus b_n\right) = \left(a \circ b_1\right) \oplus \left(a \circ b_2\right) \oplus \cdots \oplus \left(a \circ b_n\right)$$

数学归纳法

运算律

- 练习

➢1.M=R其上代数运算 $a \circ b = 2a + 3b \quad (a, b \in M)$，是否满足结合律和交换律？

➢结合律 No

$$(a \circ b) \circ c = 2(a \circ b) + 3c = 2(2a + 3b) + 3c = 4a + 6b + 3c$$

$$a \circ (b \circ c) = 2a + 3(b \circ c) = 2a + 3(2b + 3c) = 2a + 6b + 9c$$

➢交换律 No

$$a \circ b = 2a + 3b \qquad b \circ a = 2b + 3a$$

运算律

- 练习

➢2.给出集合$M=\{1,2,3\}$上既满足结合律又满足交换律的一个代数运算；再给出其上满足交换律但不满足结合律的一个代数运算。

(1) 交换律 √　　　　　　　　　　　　　　结合律 √

$a\circ b=\max(a,b)$　　　　　　$a\circ b=\min(a,b)$

(2) 交换律 √　　　　　　　　　　　　　　结合律 ×

$\circ$	1	2	3
1	2	1	1
2	1	2	1
3	1	1	2

运算律

- 练习

➢3.若$f(x)\circ g(x)=(f(x),g(x))$表示求取首席数为1的最大公因式，其中$f(x),g(x)$ 是数域F上的多项式；问代数运算$\circ$是否满足结合律？是否满足交换律？

交换律 √

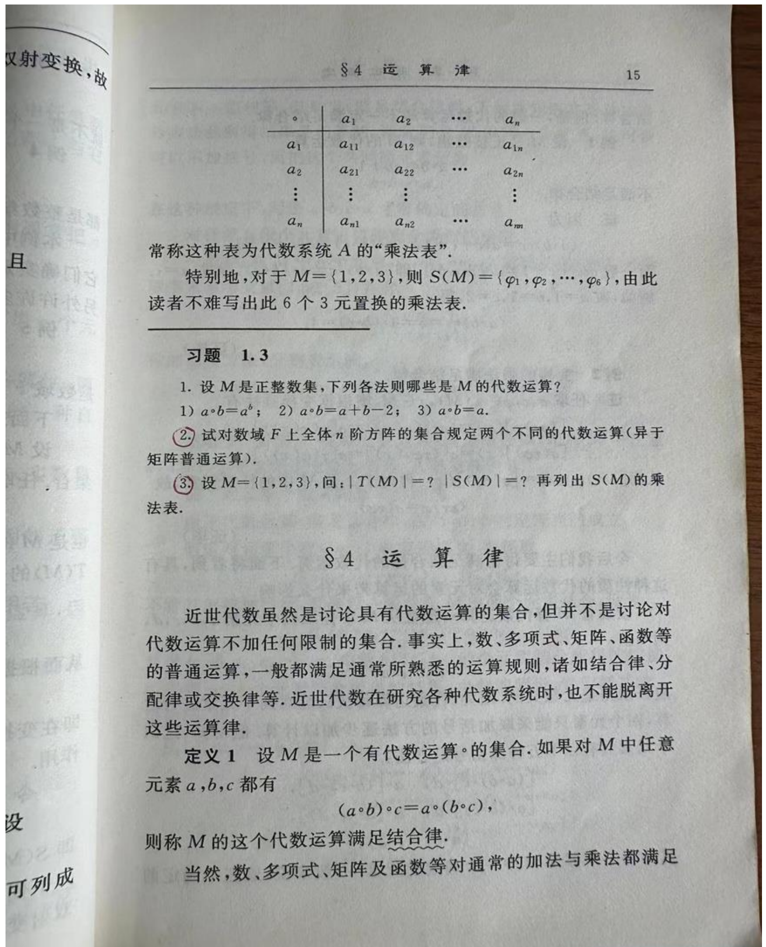
结合律 √

由最大公因式的定义和性质不难得到

$$(f\circ g)\circ h=((f,g),h)=(f,(g,h))=f\circ(g\circ h)$$

作业

- P15：2、3
- P19：2



$\circ$	a_1	a_2	$\cdots$	a_n
a_1	a_{11}	a_{12}	$\cdots$	a_{1n}
a_2	a_{21}	a_{22}	$\cdots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	a_{n1}	a_{n2}	$\cdots$	a_{nn}

常称这种表为代数系统 A 的“乘法表”.

特别地，对于 $M=\{1,2,3\}$，则 $S(M)=\{\varphi_1,\varphi_2,\cdots,\varphi_6\}$，由此读者不难写出此 6 个 3 元置换的乘法表.

习题 1.3

1. 设 M 是正整数集，下列各法则哪些是 M 的代数运算？
   1) $a\circ b=a^b$； 2) $a\circ b=a+b-2$； 3) $a\circ b=a$.
2. 试对数域 F 上全体 n 阶方阵的集合规定两个不同的代数运算(异于矩阵普通运算).
3. 设 $M=\{1,2,3\}$，问：$|T(M)|=$？ $|S(M)|=$？ 再列出 $S(M)$ 的乘法表.

§4 运 算 律

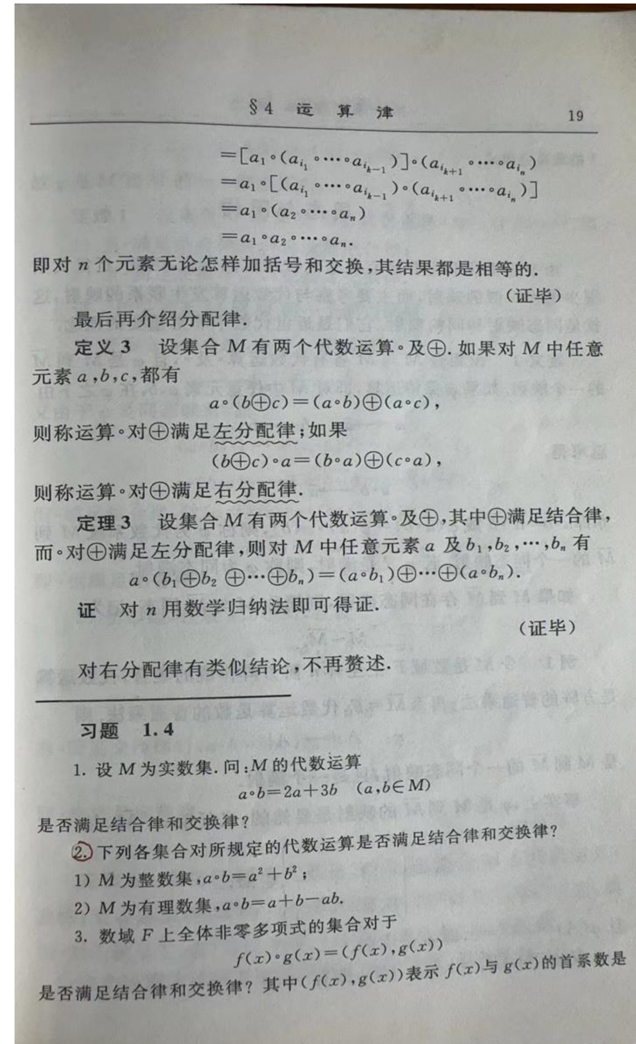
近世代数虽然是讨论具有代数运算的集合，但并不是讨论对代数运算不加任何限制的集合. 事实上，数、多项式、矩阵、函数等的普通运算，一般都满足通常所熟悉的运算规则，诸如结合律、分配律或交换律等. 近世代数在研究各种代数系统时，也不能脱离开这些运算律.

定义 1 设 M 是一个有代数运算$\circ$的集合. 如果对 M 中任意元素 a,b,c 都有

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

则称 M 的这个代数运算满足结合律.

当然，数、多项式、矩阵及函数等对通常的加法与乘法都满足



$$=[a_1\circ(a_{i_1}\circ\cdots\circ a_{i_{k-1}})]\circ(a_{i_{k+1}}\circ\cdots\circ a_{i_n})$$
$$=a_1\circ[(a_{i_1}\circ\cdots\circ a_{i_{k-1}})\circ(a_{i_{k+1}}\circ\cdots\circ a_{i_n})]$$
$$=a_1\circ(a_2\circ\cdots\circ a_n)$$
$$=a_1\circ a_2\circ\cdots\circ a_n.$$

即对 n 个元素无论怎样加括号和交换，其结果都是相等的.

(证毕)

最后再介绍分配律.

定义 3 设集合 M 有两个代数运算$\circ$及$\oplus$. 如果对 M 中任意元素 a,b,c，都有

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

则称运算$\circ$对$\oplus$满足左分配律；如果

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

则称运算$\circ$对$\oplus$满足右分配律.

定理 3 设集合 M 有两个代数运算$\circ$及$\oplus$，其中$\oplus$满足结合律，而$\circ$对$\oplus$满足左分配律，则对 M 中任意元素 a 及 $b_1,b_2,\cdots,b_n$ 有

$$a\circ(b_1\oplus b_2\oplus\cdots\oplus b_n)=(a\circ b_1)\oplus\cdots\oplus(a\circ b_n).$$

证 对 n 用数学归纳法即可得证.

(证毕)

对右分配律有类似结论，不再赘述.

习题 1.4

1. 设 M 为实数集. 问：M 的代数运算
   $$a\circ b=2a+3b\quad(a,b\in M)$$
   是否满足结合律和交换律？
2. 下列各集合对所规定的代数运算是否满足结合律和交换律？
   1) M 为整数集，$a\circ b=a^2+b^2$；
   2) M 为有理数集，$a\circ b=a+b-ab$.
3. 数域 F 上全体非零多项式的集合对于
   $$f(x)\circ g(x)=(f(x),g(x))$$
   是否满足结合律和交换律？其中$(f(x),g(x))$表示 $f(x)$与 $g(x)$的首系数是