doi:10.13582/j.cnki.1674-5884.2017.04.011

近世代数教学中的问题解答

欧阳伦群,郑棵心
(湖南科技大学 数学与计算科学学院,湖南 湘潭 411201)

摘　要:对有限集合间映射的个数、n 个元素间加括号步骤的个数及等价关系中反射律条件是否多余等6类近世代数教学中学生普遍感到难以理解的问题,通过实例分别做出详尽解答。

关键词:映射;不变子群;二元运算
中图分类号:O151.2　　**文献标志码**:A　　**文章编号**:1674-5884(2017)04-0041-03

近世代数是大学本科数学专业主干课程之一。它一方面是高等代数知识的深化与继续;另一方面又为后续课程,如代数数论、代数几何和代数拓扑等重要基础课程的学习打下基础;同时又是一门应用性很强的基础学科,在计算机、电子科学和信息科学等诸多领域都有着非常广泛的应用,特别是在信息编码和信息安全方面更是应用广泛。但是由于近世代数具有高度抽象性和严密逻辑性的特点,学生学习起来往往困难重重。下面参照张禾瑞先生所编的《近世代数基础》教材[1],通过实例,对教材中学生普遍感到难以理解的问题,一一做出详尽解答。

1　有限集合间映射的个数问题

映射是近世代数核心定义之一,贯穿于整个近世代数始终。弄清有限集合间映射的个数问题,有助于深刻理解置换群和 Cayley 定理。许多同学不会计算有限集合间到底有多少不同性质的映射。下面通过一个例题给出计算有限集合间不同性质映射个数的方法。此例题来源于文献[2]。

例1:设 $\boldsymbol{A}$, $\boldsymbol{B}$ 是2个非空有限集合,那么,(1)从 $\boldsymbol{A}$ 到 $\boldsymbol{B}$ 可以建立多少个映射?(2)从 $\boldsymbol{A}$ 到 $\boldsymbol{B}$ 可以建立多少个单射?多少个满射?多少个一一映射?

解:设集合 $\boldsymbol{A}$ 中有 m 个元素,分别是 $a_1,a_2,\cdots,a_m$。集合 $\boldsymbol{B}$ 中有 n 个元素,分别是 $b_1,b_2,\cdots,b_n$。则

(1)要建立一个从 A 到 B 的映射 ψ,必须对集合 A 中每个元素 $a_i(1\leq i\leq m)$ 都唯一确定一个像 $\psi(a_i)$。由于对每个 $a_i,(1\leq i\leq m),\psi(a_i)$ 都有 n 种选法,故从 $\boldsymbol{A}$ 到 $\boldsymbol{B}$ 可建立 n^m 个映射。

(2)如果 $m>n$,则集合 $\boldsymbol{A}$ 中至少有2个元素具有相同的像,此时从 $\boldsymbol{A}$ 到 $\boldsymbol{B}$ 没有单射存在。下面考虑 $m\leq n$ 的情况。由于 $\psi(a_1)$ 有 n 种选法,$\psi(a_2)$ 有 $n-1$ 种选法,$\cdots$,$\psi(a_m)$ 有 $n-m+1$ 种选法,故从 $\boldsymbol{A}$ 到 $\boldsymbol{B}$ 可建立 $\mathrm{P}_n^m=n(n-1)\cdots(n-m+1)$ 个单射。

如果 $m<n$,则显然没有从 $\boldsymbol{A}$ 到 $\boldsymbol{B}$ 的满射存在。故只须考虑 $m\geq n$ 的情况。因为考虑的是满射,故 $\boldsymbol{B}$ 中每个元素都有原像。又由于 $\boldsymbol{B}$ 中元素 b_1 的原像有 m 种选法,b_2 的原像有 $m-1$ 种选法,$\cdots$,b_n 的原像有 $m-n+1$ 种选法,故共有 $m(m-1)\cdots(m-n+1)=P_m^n$ 种选法,则从 $\boldsymbol{A}$ 到 $\boldsymbol{B}$ 可建立 P_m^n 个满射。

由上面的讨论可知,只有当 $m=n$ 时,方可从 A 到 B 建立一一映射,且建立一一映射的个数为 $m!$ 个。

收稿日期:20161205
基金项目:湖南省教改课题(G21316);湖南科技大学研究生精品课程(J52112)
作者简介:欧阳伦群(1967-),男,湖南洞口人,副教授,博士,主要从事同调代数与代数 K-理论研究。

2 n 个元素间加括号步骤的个数问题

设 $\boldsymbol{A}$ 是一个集合,$\circ$是集合 $\boldsymbol{A}$ 的二元运算,在集合 $\boldsymbol{A}$ 中任取 n 个元 $a_1,a_2,\cdots,a_n$, 符号 $a_1\circ a_2\circ\cdots\circ a_n$ 是没有意义的。但如果用一个加括号的步骤,当然会得到一个结果,加括号的步骤不止一种。由于 n 是一个有限整数,由文献[3]知这种加括号的步骤的个数也是一个有限整数,那么加括号的步骤到底有多少种呢?

我们用 $N(n)$ 表示 n 个元所有加括号的步骤的个数,则显然有 $N(1)=1,N(n)=N(n-1)N(1)+N(n-2)N(2)+\cdots+N(1)N(n-1)$。

为了得到 $N(n)$, 可引入幂级数

$y=N(1)x+N(2)x^2+\cdots+N(n)x^n+\cdots.$

由于

$y^2=N(1)N(1)x^2+[N(1)N(2)+N(2)N(1)]x^3+\cdots=N(2)x^2+N(3)x^3+\cdots,$

故 $y^2-y+x=0$。解此方程得

$$y=\frac{1-(1-4x)^{\frac{1}{2}}}{2}=\sum_{1}^{\infty}\frac{1\cdot3\cdots(2n-3)}{1\cdot2\cdots n}2^{n-1}x^n。$$

所以 $N(n)=\dfrac{1\cdot3\cdots(2n-3)}{1\cdot2\cdots n}2^{n-1}=\dfrac{(2n-2)!}{n!(n-1)!}$。

显然,当 $n=3$ 时, $a_1\circ a_2\circ a_3$ 有 $\dfrac{(2\times3-2)!}{3!(3-1)!}=2$ 种加括号的方法。

当 $n=4$ 时, $a_1\circ a_2\circ a_3\circ a_4$ 有 $\dfrac{(2\times4-2)!}{4!(4-1)!}=5$ 种加括号的方法。

3 等价关系中反射律条件是否多余

有人说:假如一个关系 $\boldsymbol{R}$ 适合对称律和推移律,那么它必适合反射律。其推论方法是:因为 R 适合对称律, $a\boldsymbol{R}b\Rightarrow b\boldsymbol{R}a$, 因为 $\boldsymbol{R}$ 适合推移律, $a\boldsymbol{R}b,b\boldsymbol{R}a\Rightarrow a\boldsymbol{R}a$。从而关系 $\boldsymbol{R}$ 必定适合反射律,故等价关系中反射律的条件是多余的。等价关系中反射律的条件真的是多余的吗?

我们的解答是:对集合中的任意元素 a, 如果集合中至少还存在一个元素 b, 使得 $a\boldsymbol{R}b$, 则由对称律和推移律,必有 $a\boldsymbol{R}a$; 如果集合中存在这样一个元素 a, 它与集合中所有元素都不满足关系 $\boldsymbol{R}$,则由对称律和推移律得不到 $a\boldsymbol{R}a$。此时一个关系 $\boldsymbol{R}$ 仅适合对称律和推移律,它就不一定适合反射律,从而关系就不一定是等价关系。例如:令 $\boldsymbol{A}$ 是整数集合,在集合 $\boldsymbol{A}$ 中定义关系 $\boldsymbol{R}$ 如下: $a\boldsymbol{R}b$ 当且仅当 $ab>0$。显然关系 $\boldsymbol{R}$ 适合对称律和推移律。但由于 0 与 $\boldsymbol{A}$ 中所有元素都不满足关系,故 $0\boldsymbol{R}0$ 不成立,$\boldsymbol{R}$ 不满足反射律。因而 $\boldsymbol{R}$ 不是等价关系。

4 环定义中加法必须满足交换律的条件是否多余

有人说环的定义中加法运算必须适合交换律的条件是多余的,因为由两个分配律成立可以得到环中的加法运算肯定是适合交换律的,其证明方法如下:对任意 $a,b\in\boldsymbol{R}$, 由于分配律成立,有下列式子成立:

$(a+b)(1+1)=(a+b)\times1+(a+b)\times1=a+b+a+b,$

$(a+b)(1+1)=a(1+1)+b(1+1)=a+a+b+b$。

有 $a+b+a+b=a+a+b+b$ 得 $a+b=b+a$, 再由 a,b 的任意性知加法适合交换律。故环的定义中加法运算必须适合交换律的条件是多余的。这种说法是否正确呢?

我们的解答是:如果环 $\boldsymbol{R}$ 是有单位元 1 的环,上述说法是正确的。在有单位元 1 的环中,加法适合交换律的确是环中乘法对加法适合分配律这个条件的结果。但是如果环 $\boldsymbol{R}$ 中没有单位元 1,则由乘法对加法满足分配律的条件得不到加法满足交换律的结论。实际上没有单位元 1 的环很多,故作为一般

环的定义,加法满足交换律这个条件是必不可少的,并不多余。

5　半群中单位元与逆元素不同边是否还构成群

设$\{\boldsymbol{G},\circ\}$是一个半群,$\circ$是$\boldsymbol{G}$的代数运算。如果半群$\{\boldsymbol{G},\circ\}$中有左单位元且每个元素有左逆元,或半群$\{\boldsymbol{G},\circ\}$中有右单位元且每个元素有右逆元,则由近世代数中的相关知识,半群$\{\boldsymbol{G},\circ\}$是一个群。教学中学生往往会问到另一个问题,如果半群$\{\boldsymbol{G},\circ\}$中单位元和逆元素出现在不同的边,譬如:半群$\{\boldsymbol{G},\circ\}$中有左单位元,每个元素有右逆元,那么半群$\{\boldsymbol{G},\circ\}$是否也能构成一个群呢?

对于这个问题,我们的解答是:如果半群$\{\boldsymbol{G},\circ\}$中单位元与逆元素不同边,则半群$\{\boldsymbol{G},\circ\}$不一定是群。

例如:设$\boldsymbol{F}$是一个数域,$\boldsymbol{G}=\left\{\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\middle|\ a,b\in\boldsymbol{F},\text{且}\ a\neq 0\right\}$,集合$G$中的代数运算$\circ$为普通的矩阵乘法。则(1)$G$对运算$\circ$来说满足封闭性;(2)结合律成立;(3)$\boldsymbol{e}=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$是$\boldsymbol{G}$的一个左单位元;(4)对$\boldsymbol{G}$的每一个元$\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\in\boldsymbol{G}$,$\begin{pmatrix}a^{-1} & 0\\ 0 & 0\end{pmatrix}$是$\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}$的右逆元。但$\{\boldsymbol{G},\circ\}$不是一个群,因为由群的定义,群的左单位元必是右单位元,而上述代数系统$\{\boldsymbol{G},\circ\}$中,$\boldsymbol{e}$是左单位元,但不是右单位元。故$\{\boldsymbol{G},\circ\}$不是一个群。

6　群为何只对不变子群才能做商群

令$\boldsymbol{N}$是$\boldsymbol{G}$的子群,把$\boldsymbol{N}$的所有右陪集做成一个集合$\boldsymbol{S}_r=\{\boldsymbol{N}a,\boldsymbol{N}b,\boldsymbol{N}c,\cdots\}$,在$\boldsymbol{S}_r$中定义运算:$(\boldsymbol{N}x)(\boldsymbol{N}y)=\boldsymbol{N}(xy)$。我们知道如果$\boldsymbol{N}$是$\boldsymbol{G}$的不变子群,则$\boldsymbol{S}_r$对此运算做成群,称之为群$\boldsymbol{G}$对不变子群$\boldsymbol{N}$的商群,并记做$\boldsymbol{G}/\boldsymbol{N}$。现在的问题是:如果$\boldsymbol{N}$是$\boldsymbol{G}$的一般子群,$\boldsymbol{S}_r$对此运算是否一定做成群?

我们的解答是:$\boldsymbol{S}_r$对上述运算不一定做成群。因为$\boldsymbol{S}_r$对上述运算做成一个群,则运算必须满足封闭性,即两个右陪集$\boldsymbol{N}a$与$\boldsymbol{N}b$运算的结果还必须是一个右陪集$\boldsymbol{N}c$。下面我们证明对任意$\boldsymbol{N}a,\boldsymbol{N}b\in\boldsymbol{S}_r$,它们的积$\boldsymbol{N}a\boldsymbol{N}b$仍是$\boldsymbol{N}$的右陪集的充要条件是对任意$x\in\boldsymbol{G}$,有$x\boldsymbol{N}=\boldsymbol{N}x$,即$\boldsymbol{N}$必为不变子群。

充分性:如果$\boldsymbol{N}$为不变子群,则对任意$\boldsymbol{N}a,\boldsymbol{N}b\in\boldsymbol{S}_r$,有

$\boldsymbol{N}a\boldsymbol{N}b=\boldsymbol{N}(a\boldsymbol{N})b=\boldsymbol{N}(\boldsymbol{N}a)b=\boldsymbol{N}\boldsymbol{N}ab=\boldsymbol{N}(ab)$,所以$\boldsymbol{N}a\boldsymbol{N}b=\boldsymbol{N}(ab)$是以$ab$为代表元的右陪集。

必要性:对任意$x\in\boldsymbol{G}$,对$y\in\boldsymbol{G}$,由条件知$\boldsymbol{N}x\boldsymbol{N}y$仍是一个右陪集$\boldsymbol{N}a$。但$xy=exey\in\boldsymbol{N}x\boldsymbol{N}y=\boldsymbol{N}a$,所以$\boldsymbol{N}xy=\boldsymbol{N}a=\boldsymbol{N}x\boldsymbol{N}y$。令$y=e$,我们有$\boldsymbol{N}x=\boldsymbol{N}x\boldsymbol{N}$。任取$xn\in x\boldsymbol{N}$,由式子$\boldsymbol{N}x=\boldsymbol{N}x\boldsymbol{N}$知,存在$n_1$,$n_2\in\boldsymbol{N}$使得$n_1x=n_2xn$,于是有$n_2^{-1}n_1x=xn$,所以$xn\in\boldsymbol{N}x$。由$xn$的任意性知$x\boldsymbol{N}\subseteq\boldsymbol{N}x$。再由$x$的任意性有$x^{-1}\boldsymbol{N}\subseteq\boldsymbol{N}x^{-1}$,从而有$x(x^{-1}\boldsymbol{N})x\subseteq x(\boldsymbol{N}x^{-1})x$,即$\boldsymbol{N}x\subseteq x\boldsymbol{N}$,于是证明了$x\boldsymbol{N}=\boldsymbol{N}x$.

参考文献:

[1] 张禾瑞.近世代数基础[M].北京:高等教育出版社,2012.

[2] 杨子胥,宋宝和.近世代数习题解[M].济南:山东科学技术出版社,2002.

[3] 贾柯勃逊 N.抽象代数学[M].北京:科学出版社,1960.

(责任校对　谢宜辰)