关于抽象代数中群定义理解

向建国，罗会亮
（黔南民族师范学院 数学与统计学院，贵州 都匀 558000）

摘 要：抽象代数是高校数学专业的基础课程，该课程概念抽象、概括性高、不易理解，尤其群论中群定义的理解较为困难，通过实例对群定义的内涵给予阐明。

关键词：二元运算；群；抽象代数；乘法
[中图分类号] O152 [文献标识码] A [文章编号] 1674-2389(2016)01-0113-03

Interpretation on Group Concept in Abstract Algebra

XIANG Jian-guo, LUO Hui-liang
(*School of Mathematics and Statistics, Qiannan Normal University for Nationalities, Duyun 558000, Guizhou, China*)

Abstract: Abstract algebra is the basic course of mathematics major. It has many features, such as abstract concepts, high degree in summarizing, difficult to understand, especially elusive to the concept of group in group theory. This paper illustrates the implication of the concept of group with concrete examples.

Key words: binary operation; group; abstract algebra; multiplication

社会生产力不断向前发展的要求是数学理论产生的动力之一，如欧氏几何、数理统计、微积分理论的建立。另一方面，由于数学本身发展的需要产生和建立了一些新的数学理论，如实数理论、n 维欧氏空间理论、量子群论、抽象群理论等。在理解和学习数学理论的过程中，不能脱离数学理论产生的来源背景，而是要将它们与实际联系起来，这样才能牢固地掌握理论知识，理解数学理论的内涵实质，不至于认识的只是抽象的纯粹数学概念。群论中群定义的灵魂是运算。[1](P14) 群定义是以运算为着重点，围绕着它把整个定义的要素组织起来。理解群定义时，要突出群定义的运算。这里具体谈谈对抽象代数中群论的群定义的理解。

1 关于二元运算和乘法

设 G 是一个非空的集合，所有集合 G 中的任意的两个元素 a, b 构成的序对 (a, b) 组成的集合叫作 G 的笛卡尔集，[2](P4) 记作 $G \times G$，即 $G \times G = \{(a, b) \mid a \in G, b \in G\}$。$\circ$ 是一个法则，它作用于 (a, b)，使得 G 中有唯一的元 d 与 (a, b) 对应，记 $\circ(a, b) = d$。此时称 $\circ$ 是 G 上的二元运算，[3](P11) 又称为 G 上的乘法，记为 $a \circ b = d$，简记为 $ab = d$.

可以看到，G 上的任意两个元素按照 G 上二元运算的运算的结果都在 G 集合中，它们都是集合 G 中的元素。由此知道，这个二元运算对集合 G 是封闭的。也就是说，对乘法运算是封闭的。

一般来说，序对 (a, b) 与 (b, a) 是不相同的，当集合 G 对其上的乘法不具有交换性时，一般有 $ab \neq ba$。

例1 G 包含模 n 的 n 个剩余类，$[a]$ 表示整数 a 所在的关于模 n 剩余类，

即 $[a] = \{x \mid x \equiv a(\mathrm{mod}n)\}$。规定 G 上的

收稿日期：2015-10-19
基金项目：2014年中央财政专项项目(2014ZCSX35)。
作者简介：向建国(1971-)，男，湖北黄梅人，讲师，硕士，研究方向：有限群。

运算为$[a]°[b]=[a+b]$，其中+是整数的普通加法。

设$[a']=[a]$，$[b']=[b]$，于是$a'\equiv a(\mathrm{mod}n)$，$b'\equiv b(\mathrm{mod}n)$，从而$n\mid a'-a$，$n\mid b'-b$，因而$n\mid(a'-a)+(b'-b)$，$n\mid(a'+b')-(a+b)$，所以$[a'+b']=[a+b]$，

即$[a']°[b']=[a]°[b]$，于是所规定的运算是G上的乘法。

而$[b+a]=[a+b]$，也就是$[b]°[a]=[a]°[b]$，说明所规定的运算乘法在G上的元之间具有交换的性质。

2 关于群的一般定义

设G是一个非空的集合，在G中定义了一个二元运算，叫做乘法，它满足

Ⅰ.结合律：$(ab)c=a(bc)$，$a,b,c\in G$；

Ⅱ.存在单位元素：G中存在一个元e，使得对任意的G中元a，都有$ea=ae=a$；称e其为G的单位元；

Ⅲ.存在逆元素：对于任意的G中元a，在G中存在一个元b，使得$ab=ba=e$，称b为a的逆元，且记其为a^{-1}；

则非空集合G对于其上的乘法作成一个群。[4](P1)

初学者学到这里一般会对群的定义都会感到疑惑：一是群定义中为什么要规定结合律，二是单位元、逆元是用什么样的方式来体现，三是单位元、逆元唯一性。

其实，这与规定在集合G上的乘法有关。实际上G上的乘法对于二个元相乘是有次序先后的约束。因此对于G中任意三个元a，b，c，它们的之间的三个元相乘有两种形式：a与b相乘所得的积再与c相乘，即$(ab)c$，另一种方式是a与b和c相乘后的积相乘，即$a(bc)$。这两种形式的积可能相等也有不相等。但是群所考虑的是相等的情形，即是要求G中的元满足结合律。

群的乘法具有封闭的性质，使得集合$aG=\{ax\mid x\in G\}$和$Ga=\{xa\mid x\in G\}$都包含在G内。那么元a有可能属于aG，也有可能不属于aG. 对于前者在aG中有元$x\in G$，使$ax=a$，更进一步，对G任意的元b，都有$bx=b$，此时元x称为G的单位元，并且有一个特称的符号e来表示它，即称e为单位元，满足$ea=ae=a$。

单位元e属于aG，则有元$t\in G$，使$at=e$，这样元t就是元a的逆元。

对于元a有可能属于Ga的情形，类似讨论。

设e'分别是群的单位元，满足$e'a=ae'=a$，那么取$a=e$，$e'e=ee'=e$，再由Ⅱ中，取$a=e'$，$ee'=e'e=e'$于是$e=e'$。因此群的单位元是唯一的。

设b，b'分别是元a逆元，满足$ab=ba=e$，$ab'=b'a=e$，于是$b=be=b(ab')=(ba)b'=eb'=b'$。因此元的逆元是唯一的。

例2 所有实数对(a,b)所作成的集合，规定两个元的乘法是$(a,b)°(c,d)=(a-c,b+d)$不能作成群，按此乘法不满足结合律。[5](P12)

事实上，取元$a=(0,0)$，$b=(0,0)$，$c=(1,0)$，则$a°(b°c)=(0,0)°(-1,0)=(1,0)$ $(a°b)°c=(0,0)°(1,0)=(-1,0)$ 即$a°(b°c)\neq(a°b)°c$

例3 对实数集R，规定两个元的乘法是$a°b=2(a-b)$，不能作成群，按此乘法没有单位元。

事实上，设R有单位元e，由于$0\in R$，得$e°0=2(e-0)=2e=0$，从而$e=0$。又由于$1\in R$，而$1°0=2(1-0)=2\neq1$，与$e=0$是R的单位元矛盾。

例4 非空集合M的所有子集作成集合$P(M)$，规定两个元的乘法是$AB=A\cap B$ $(A,B\subseteq M)$，此时$P(M)$不能作成群，因为按此乘法没有逆元。

事实上，集合M的任意真子集N，有$NM=N\cap M=N=M\cap N=MN$，故M是$P(M)$的单位元。但是，不存在$Y\in P(M)$，使得$NY=N\cap Y=M$，即N在$P(M)$中无逆元。

3 关于群的等价定义

设G是一个非空的集合，如果在G中定义了一个代数运算，叫做乘法，它满足

Ⅰ.G对乘法来说是封闭的；

Ⅱ.结合律：$(ab)c=a(bc)$，$a,b,c\in G$；

Ⅳ.对于任意的G中的两个元a，b，存在G中的两个元x，y，满足$ax=b$和$ya=b$。

则非空集合G对于其上的乘法作成一个群。[6](P31)

这里通常会有两个问题：一是两个方程$ax=b$和$ya=b$在群定义中表达了什么含义，二是如何体现单位元和逆元。

其实，仍然与定义中的代数运算有关。Ⅰ的乘法封闭性表明G上的任意两个元素的乘积结果都在G集合中，且它是集合G中的一个元。Ⅳ是从方程的角度来定义群，$ax=b$是一个在G中存在解的方程，它表达的含意是对集合G的任意一个元b来说，与集合G的任意一个元a，能够在集合G中找到一个元x，使得元a左乘元x的积与元b

相等(要注意的是这样的元 x 是唯一的),表明 G 包含在 $aG = \{ax \mid x \in G\}$ 内,即 $G \subset aG$。同样 $ya = b$ 也蕴含同样的含义,只不过它是元 a 右乘元 y 的积与元 b 相等(要注意这样的元 y 是唯一的),表明 G 包含在 $Ga = \{xa \mid x \in G\}$ 内,即 $G \subset Ga$。

对 aG,有元 $x \in G$,使 $ax = a$。此时 x 是 a 的单位元,还必须验证它是群的单位元。对群的任意元 b,由Ⅳ存在 G 中的元 y,有 $ya = b$,于是 $bx = yax = yb = b$,对 Ga 情形同样的讨论。由此群单位元是存在的,同时群的元的逆元自然也是存在的。

例5 设非零实数 R^*,按照乘法 $a \circ b = |ab|$ 不能构成一个群。

事实上,$1, -1 \in R^*$,但是方程 $1 \circ x = -1$ 即 $|x| = -1$ 在 R^* 中无解,从而不满足等价定义Ⅳ.

4 关于有限群

设 G 是一个群,如果群 G 的元的个数是一个有限的整数,则称 G 为有限群。

有限群的另一个定义是:

设 G 是一个有限的非空集合,如果在 G 中定义了一个代数运算,叫做乘法,它满足

Ⅰ. G 对乘法来说是封闭的;

Ⅱ. 结合律:$(ab)c = a(bc)$, $a, b, c \in G$;

Ⅵ. 存在消去律:对于 G 中的元 a, x, x', y, y',

如果 $ax = ax'$,那么 $x = x'$;

如果 $ya = y'a$,那么 $y = y'$

则有限的非空集合对于其上的乘法作成一个有限群。[6](P39)

这里有三方面的疑问:一是消去律在群定义中发挥了什么作用,二是群定义中的单位元,逆元通过什么方式来表现,三是集合的有限性在群的定义有什么作用。

其实,对于有限群来说,这两个定义是等价的。如果非空集合 G 是一个群,那么它是满足消去律的。对于群 G 的任意两个元 a, b,一定存在 G 中的两个元 x, y,满中 $ax = b$ 和 $ya = b$。这就意味着 $aG = G$ 以及 $Ga = G$。对于非空集合 G 来说,它满足乘法的封闭性,于是有 $aG \subset G$ 以及 $Ga \subset G$. 它满足消去律:对于 G 中的元 a,如果 $ax = ax'$,那么 $x = x'$。这里我们能够知道如果 $x \neq ax'$,会有 $ax \neq ax'$。也就是可以这样来理解 G 中的元的不同导致了 aG 的元也是不同,所以 aG 中元的个数与 G 中的元的个数一样多。

由此很容易找有限性在群的定义中发挥的作用,由于集合 G 是有限集合,由鸽笼原理,使得 $aG = G$ 成立,群 G 的任意两个元 a, b,存在 G 中的两个元 x 满足方程 $ax = b$。同样的原由 $Ga = G$ 成立,方程 $ya = b$ 按照乘法的规则也是满足的。

但是当 G 是无限集合时,仅仅满足消去律是不能保证群定义的成立。原因在于无限集合元素的个数与它的子集元素的个数一样多时,一般是不能保证群的等价定义中Ⅳ的成立。

例6 设 N 是非零偶数集,即 $N = \{2k \mid k \neq 0, k \in Z\}$,规定:两个元的乘法是普通整数的乘法。但是,$N$ 不能构成一个群。

事实上,非零偶数集有无限多个偶数,且它是满足消去律,但是,它没有单位元。如果元 e 是单位元,那么 $(2k)e = 2k$,由消去律,有 $e = 1$,这是个矛盾。非零偶数集 N 中找不到这样的元。

例7 设 N 是非零有理数集,即 $N = \{\frac{p}{q} \mid (p, q) = 1, p \neq 0, q > 0, p, q \in Z\}$,规定:两个元的乘法是普通有理数的乘法。但是,$N$ 构成一个群。

事实上,有理数集是无限集,且它是满足消去律,我们知道有理数的普通乘法是满足结合律,对于任意元 $\frac{p}{q}$,有逆元 $\frac{q}{p}$,使得 $\frac{p}{q}\frac{q}{p} = 1$,同时 1 是单位元。

例6,例7 所讨论的集合都是无限集,它们都满足消去律,结合律,但是例7 构成群,例6 则不然。说明无限集构成群的乘法复杂得多。

以上的讨论可以看出,在对数学知识的学习中,我们必须从定义的内涵出发,理解定义所表达出来的本质内容。这样既能够深刻理解数学理论,又可以起到事半功倍的学习效果。

参考文献

[1] 刘绍学. 近世代数基础[M]. 北京:高等教育出版社,1999.

[2] 盛德成. 抽象代数[M]. 北京:科学出版社,2001.

[3] 姚慕生. 抽象代数学[M]. 上海:复旦大学出版社. 1998.

[4] 徐明曜. 有限群导引(上)[M]. 北京:科学出版社,1999.

[5] 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,2003.

[6] 张禾瑞. 近世代数基础[M]. 北京:高等教育出版社,1978.

责任编辑:董宝平

责任校对:董宝平