文章编号:1000-5471(2012)02-0131-03

关于近世代数中群论学习的探讨①

吕 恒, 徐海静

西南大学 数学与统计学院,重庆 400715

摘要:利用群的定义探讨了群与向量空间的联系,并用群的理论去证明欧拉定理和 Wilson 定理.

关 键 词:群;线性空间;欧拉定理;Wilson 定理

中图分类号:G420;O152 **文献标志码**:A

近世代数(亦称抽象代数)是本科数学系的专业基础课. 主要讲授群、环、域 3 个代数运算系统. 尽管近世代数与诸如晶体的对称性、三大几何作图难题的否定、编码、移位寄存器序列、同余方程组等问题有联系,但是当前大部分高校的数学系近世代数课程的课时都是 60~80 课时,一般的非数学专业近世代数的课时更少. 笔者在多年的教学中,接触了 3 类不同的教材(参见文献[1-3]),发现在这样少的时间内,老师只能按教材逻辑系统安排教学内容 ,依照定义——例子——定理这样的结构来展开教学,而没有时间与实际问题联系起来. 对于初学者来说,近世代数主要对代数系统进行研究,主要是符号的运算,抽象难懂. 近世代数对抽象群的研究[4-6]更是如此. 因此很多学生反映近世代数难学,而且学了没有多大用处,这让很多授课老师感到尴尬. 然而笔者在教学中发现,近世代数可以与高等代数、初等数论中的知识联系起来,使学生认为近世代数是有用、有趣且不是那么困难的.

下面从两个不同的方面,将近世代数中的群论知识与高等代数以及初等数论的知识联系起来.

1 群的定义与线性空间的定义之间的联系

群的定义是学习近世代数首先要遇到的. 关于群的等价定义很多,在教学中一般都会先给出下面的定义:

定义 1 设 G 是非空集合,"$\circ$"是它的一个代数运算,如果满足下面的条件:

(1) 结合律成立,即对 G 中的任意元 a,b,c,都有 $(a\circ b)\circ c=a\circ(b\circ c)$;

(2) G 中有左单位元 e,即对 G 中的任意元 a,都有 $e\circ a=a$;

(3) G 中任意元有左逆元,即对 G 中的任意元 a,都有 $a^{-1}\circ a=e$.

则称 G 在代数运算"$\circ$"下为一个群.

对于这样的群的抽象定义,一般会通过大量的例子来解释什么是群,如整数加群,实数域上的所有同阶可逆矩阵关于矩阵的乘法构成的群等. 这样的教学可以让学生明白什么是群,也能让他们掌握群的定义,但是这些例子过于简单,而一些抽象的例子让不少学生感觉理解困难,从而逐渐失去兴趣. 因此寻找合适的且能够加深学生印象的例子就显得比较关键了.

高等代数(或者线性代数)中讲述的线性空间的定义也是学生学习的一个难点,绝大部分同学是记不清楚的. 为了方便讨论,下面也给出线性空间的定义:

定义 2 设 V 是非空集合,P 是数域. 在 V 中定义一个二元运算"+",称为加法,对 V 中的任意元 α,β,存在 V 中的唯一元 γ,使得 $\gamma=\alpha+\beta$;在数域 P 与 V 之间定义一个数乘运算"$\cdot$",对 V 中的任意元 α,P 中

① 收稿日期:2011-09-07

基金项目:国家自然科学基金(11001226);重庆市教委科学技术研究项目(KJ111207);重庆市教育委员会科学技术研究项目(KJ091217).

作者简介:吕 恒(1976-),男,四川安岳人,副教授,主要从事群论的研究.

的任意元 k，有唯一的 V 中的元 β，使得 $\beta=k\cdot\alpha$. 同时加法与数乘满足下面的公理：

(1) 对 V 中的任意元 α,β，都有 $\alpha+\beta=\beta+\alpha$；

(2) 对 V 中的任意元 α,β,γ，都有 $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$；

(3) V 中有元 θ，对 V 中的任意元 α，都有 $\theta+\alpha=\alpha$；

(4) 对 V 中的任意元 α，V 中有负元 α_1，使得 $\alpha_1+\alpha=\theta$；

(5) 对 V 中的任意元 α，P 中的任意元 k,l，有 $k\cdot(l\cdot\alpha)=(k\cdot l)\cdot\alpha$；

(6) 对 V 中的任意元 α,β，P 中的任意元 k，有 $k\cdot(\alpha+\beta)=k\cdot\alpha+k\cdot\beta$；

(7) 对 V 中的任意元 α，P 中的任意元 k,l，有 $(k+l)\cdot\alpha=k\cdot\alpha+l\cdot\alpha$；

(8) 对 V 中的任意元 α，有 $1\cdot\alpha=\alpha$.

则我们称 V 为数域 P 上的一个线性空间，V 中的元素称为向量.

这个时候需要引入交换群的定义. 对交换群 G 中的任意元 a,b 都满足 $a\circ b=b\circ a$. 一般情况下，称运算“$\circ$”是乘法运算. 而对于交换群，则通常称运算“$\circ$”是加法运算，记为“$+$”. 此时左单位元 e 用零元 0 表示，a 在 G 中的左逆元 a^{-1} 就用负元 $-a$ 表示. 利用定义 1 容易得到下面交换群的定义：

定义 3 设 G 是非空集合，“$+$”是 G 的一个代数运算，如果满足下面的条件：

(1) 交换律成立，即对 G 中的任意元 a,b，都有 $a+b=b+a$；

(2) 结合律成立，即对 G 中的任意元 a,b,c，都有 $(a+b)+c=a+(b+c)$；

(3) G 中有零元 0，即对 G 中的任意元 a，都有 $0+a=a$；

(4) G 中任意元有负元，即对 G 中的任意元 a，都有 $-a+a=0$.

则称 G 在代数运算“$+$”下为一个交换群.

现在回头看，容易发现 V 中二元运算“$+$”实际就是 V 的一个代数运算. 定义 2(1)－(4) 的本质意思就是使得 V 关于二元运算“$+$”作成一个交换群. 掌握了群的定义后，线性空间的定义就变得容易理解和记忆了. 因此在讲解群的定义时，适当结合线性空间的定义，学生在学习中就会觉得群是有意义的，同时加深对群与线性空间定义的理解.

有很多关于线性空间中各个公理的独立性或者等价公理的讨论，如文献[7－8]，很多教师在讲授线性空间定义的时候会一句带过，不加以详谈. 下面就利用群的定义给出定义 3 的一个等价定义：

定义 4 设 G 是非空集合，“$+$”是 G 的一个代数运算，如果满足下面的条件：

(1) 交换律成立，即对 G 中的任意元 a,b，都有 $a+b=b+a$；

(2) 结合律成立，即对 G 中的任意元 a,b,c，都有 $(a+b)+c=a+(b+c)$；

(3) 对 G 中的任意元 a,b，$a+x=b$ 在 G 中有解.

则称 G 在代数运算“$+$”下为一个交换群.

由于定义 2(1)－(4) 的本质意思就是使得 V 关于二元运算“$+$”作成一个交换群，因此可把定义 2 的公理(3),(4) 换成：(3″) 对 V 中的任意元 α,β，$\alpha+x=\beta$ 在 V 中有解.

故定义 2 中的 8 条公理只需要改为(1),(2),(3″),(5),(6),(7),(8) 这 7 条，V 同样是一个线性空间. 这样的讨论学生很容易懂，又加深了他们对群的定义以及线性空间定义的理解.

另外，如果我们在上课时花几分钟谈谈群起源于伽罗瓦解决五次以上的代数方程是否存在根式解的问题，那么学生就会发现群是挺有意思的，居然与以前大的数学问题联系起来了. 在讲完定义后，同时布置一个课后作业，提供相关资料，要求学生查伽罗瓦解决五次以上的代数方程问题的相关资料，并作一个简单笔记介绍什么是五次以上的代数方程，以及伽罗瓦解决五次以上的代数方程的相关历史，并回答什么是对称群、置换群，举出一些对称群的例子. 如果学生按照上述步骤去完成课后作业，在花不了多长时间的同时，既能加深对群的定义的理解，又提高了学习积极性.

2 群与欧拉定理、Wilson 定理

著名的欧拉定理是学习初等数论必须掌握的内容. 然而，欧拉定理也可以利用群的理论来证明，证明很简单易懂.

定理 1 (欧拉定理) 设 m 是大于 1 的整数，$(a,m)=1$，则 $a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m)$，其中 $\varphi(m)$ 是欧拉函数. 用 $M=\{[0],[1],[2],\cdots,[m-1]\}$ 表示模 m 的剩余类. 集合 $N=\{[a_1],[a_2],\cdots,[a_{\varphi(m)}]\}\subset M$ 是

模 m 的一个简化剩余类，其中$[a_1]=[1]$. 现在规定 M 的一个二元运算“$\cdot$”，即$[a]\cdot[b]=[ab]$. 对任意整数 a_1,b_1，若 $a_1\in[a]$，$b_1\in[b]$，则 $a_1=a+km$，$b_1=b+lm$，其中 k,l 是整数，因此 $a_1b_1=ab+(kb+la+klm)m\in[ab]$，即有$[a_1]\cdot[b_1]=[a]\cdot[b]$. 从而 M 的二元运算“$\cdot$”与剩余类代表元的选取无关，因此二元运算“$\cdot$”是 M 的一个代数运算，易得“$\cdot$”也是 M 的子集 N 的一个代数运算. 这时候容易验证 N 关于二元运算“$\cdot$”是一个阶为 $\varphi(m)$ 的有限群.

下面用群的理论给出欧拉定理的证明.

定理 1 的证明　考虑集合$N=\{[a_1],[a_2],\cdots,[a_{\varphi(m)}]\}$. 由于 N 关于二元运算“$\cdot$”是一个群，其中$[1]$是单位元，对任意整数 a，若$(a,m)=1$，则$[a]\in N$. 用$[a]^k$ 表示 k 个$[a]$连续做运算. 由于 N 含有 $\varphi(m)$ 个元，即群 N 的阶为 $\varphi(m)$，于是$[a]^{\varphi(m)}=[a^{\varphi(m)}]=[1]$. 从而得到 $a^{\varphi(m)}=1+sm$，故 $a^{\varphi(m)}\equiv1(\mathrm{mod}\ m)$ 成立.

同样地用群的理论可以证明初等数论中的著名的 Wilson 定理.

定理 2（Wilson 定理）　设 p 是素数，则$(p-1)!\equiv-1(\mathrm{mod}\ p)$.

证　考虑集合 $N=\{[1],[2],\cdots,[p-1]\}$. 由于 p 是素数，因此 N 关于二元运算“$\cdot$”是一个阶为 $p-1$的群. 对于任意$[x]\in N$，若$[x]\cdot[x]=[x^2]=[1]$，即 $x^2-1\equiv0(\mathrm{mod}\ p)$，从而易得 $x\equiv-1(\mathrm{mod}\ p)$ 或者 $x\equiv1(\mathrm{mod}\ p)$. 因此$[x]=1$ 或者$[x]=[p-1]$. 这表明 N 只有$[1]$和$[p-1]$的可逆元是自身，其他的元与逆元互不相同. 于是

$$[1]\cdot[2]\cdot[3]\cdot\cdots\cdot[p-1]=[1]\cdot[p-1]=[p-1]$$

即$[(p-1)!\,]=[p-1]$. 从而有$(p-1)!\equiv p-1\equiv-1(\mathrm{mod}\ p)$.

定理 1 和定理 2 只需要花很少时间学习，甚至可以布置为课后作业. 学科之间的紧密联系可以让学生觉得近世代数的学习不仅有意义，而且有趣，由此激发学生的学习积极性，使得学生在学习近世代数时不会感觉那么困难.

参考文献：

[1] 张禾瑞. 近世代数基础 [M]. 北京：高等教育出版社，1978.

[2] 张广祥. 抽象代数 [M]. 北京：科学出版社，2005.

[3] 杨子胥. 近世代数基础 [M]. 北京：高等教育出版社，2003.

[4] 龚　律，曹洪平. 恰有 7 个非正规子群的有限群 [J]. 西南大学学报：自然科学版，2010，32(2)：104－108.

[5] 裴　俊. 能够表示成真正规子集并的完全单半群 [J]. 西南大学学报：自然科学版，2010，32(2)：109－112.

[6] 薛海波，吕　恒. 所有无限真子群是阿贝尔群的局部幂零 p-群 [J]. 西南师范大学学报：自然科学版，2010，35(2)：6－8.

[7] 王凯宇. 关于线性空间的定义 [J]. 数学通报，1980(11)：20－21.

[8] 袁振邦. 关于向量空间的定义 [J]. 西南师范大学学报：自然科学版，1982(3)：37－42.

On How to Study Group Theory in Modern Algebra

LÜ　Heng，　XU Hai-jing

School of Mathematics and statistics，Southwest University，Chongqing 400715，China

Abstract：In this paper，the definition of group is used to study the relation of group with vector space and the theory of group is used to prove the Euler theorem and the Wilson theorem.

Key words：group；linear space；Euler theorem；Wilson theorem

责任编辑　廖　坤