关于群的一个应用

张海芳,费秀海
(云南省临沧师范高等专科学校 数学系,云南 临沧 677000)

【摘 要】首先介绍了半群中几个重要的概念,接着介绍了本文中重要的定理5.1,从而得到Zm={[0],[1],…[m-1]}关于二元运算[a][b]=[ab]形成幺半群,进而Z^+_m形成(m-1)阶群,最后得到推论6.1,最终完成该定理的证明。

【关键词】欧拉—费马;等价关系;模m同余
【中图分类号】O152.8 【文献标识码】A 【文章编号】1673-1891(2010)01-0034-04

引言

在数论中,有一个著名的定理,它有着极其广泛的应用,那就是欧拉——费马定理:

假设a为整数,p为素数且(a,p)≡1则$a(\mathrm{mod}\ p)$

(注:此定理也可写成:对任意素数p和任意整数a恒有$a^p\equiv a(\mathrm{mod}\ p)$)

为了以一种简捷的方式证明此定理,我们只需一些半群理论及群论的相关知识。

1 等价关系(equivalence relation)

(1)关系(relation)

定义1.1 如果X是一个非空集合,ρ是Cartesian积X×X的一个子集,即ρ⊆X×X那么ρ叫做X上的一个关系。

特别值得一提的关系是恒等关系$I_x=\{(x,x):x\in X\}$以及关系ρ的逆$\rho^{-1}=\{(x,y)\in X\times X:(y,x)\in\rho\}$。

(2)二元运算

定义1.2 如果G是一个非空集合,每个函数G×G→G叫做G上的一个二元运算。二元运算通常用符号o表示,(a,b)∈G×G在一个二元运算下的像常记作aob,本文中有的地方把aob写成ab(乘法记号)。

以B(X)表示集合X上所有关系的集合,那么B(X)上的一个二元运算,我们可如此

定义1.3 如果ρ,σ∈B(X)那么$\rho\circ\sigma=\{(x,y)\in X\times X:(\exists z\in X),(x,z)\in\rho$且$(z,y)\in\sigma\}$。

(3)等价关系

给定集合X上的一个关系ρ我们说:

(ⅰ)关系ρ是自反的(reflexive)如果$I_x\subseteq\rho$这就是说$(\forall x\in X)(x,x)\in\rho$

(ⅱ)关系ρ是对称的(symmetric)如果$\rho^{-1}=\rho$这就是说$(\forall x,y\in X)(x,y)\in\rho\Rightarrow(y,x)\in\rho$

(ⅲ)关系ρ是传递(Transitive)如果$\rho\circ\rho\subseteq\rho$这就是说$(\forall x,y,z\in X)[(x,y)\in\rho$且$(y,z)\in\rho]\Rightarrow(x,z)\in\rho$

定义1.4 如果非空集合X上的一个关系ρ同时满足(ⅰ)(ⅱ)(ⅲ)三条规律,那么我们便称关系ρ是非空集合X上的一个等价关系。

等价关系一般用符号~来表示,设ρ是非空集合X上的一个等价关系,若(a,b)∈ρ我们常常记为a~b,这种记法使用起来形象直观方便,于是等价关系中的三条规律可表示成:

I、Reflexive:$(\forall x\in X)x\sim x$

II、Symmetric:$(\forall x,y\in X)x\sim y\Rightarrow y\sim x$

III、Transitive:$(\forall x,y,z\in X)$(x~y且y~z⇒x~z)

2 集合的分类与集合上的等价关系

下面,我们给出关于一个集合的非常重要的概念

定义2.1 给定非空集合X上的一个子集族$\{A_i:i\in I\}$,我们说$\{A_i:i\in I\}$是集合X的一个分类,如果:

(ⅰ)$(\forall i\in I)A_i\neq\Phi$;

(ⅱ)$(\forall i,j\in I)A_i=A_j$或$A_i\cap A_j=\Phi$;

(ⅲ)$\bigcup_{i\in I}A_i=X$。

关于集合的分类与集合上的等价关系两者间的关系,本文只给出下面的

定理2.1 非空集合X的元间的一个等价关系~决定集合X的一个分类。

证明:给定X中的一个元a,记$[a]=\{b\in X\mid b\sim a\}$,称[a]为a所在的等价类。很明显,[a]是集合X的一个子集,我们说所有等价类子集构成X的一个分类。我们分三步来说明这一点。

(ⅰ)每个等价类$[a]\neq\Phi$,因为a~a,从而$a\in[a]$

(ⅱ)任意两个等价类[a]和[b],$[a]\cap[b]=\Phi$或[a]=[b]

首先,我们注意到这样一个事实:a~b⇔[a]=[b](本文限于篇幅证明留给读者)若$[a]\cap[b]\neq\Phi$则$\exists c\in X$,使得c∈[a]且c∈[b],从而c~a且c~b,即a~c且c~b,因此a~b,所以有[a]=[b]。

收稿日期:2010-02-15
作者简介:张海芳(1980-),女,云南保山人,基础数学硕士,研究方向:半群理论及代数理论。

(ⅲ)所有等价类的并显然是非空集合X。

3 半群及其上的同余关系

定义3.1一个半群是指一个非空集合G和G上满足(ⅰ)结合律:(ab)c=a(bc)(对所有的a,b,c∈G)的一个二元运算,常记作(G,o)。

定义3.2设ρ是半群(X,o)上的一个等价关系,如果(∀s,s',t,t'∈X)(s,s')∈ρ且(t,t')∈ρ有(st,s't')∈ρ,我们把等价关系ρ叫做同余关系。

如果把等价关系ρ表示成~,则等价关系~是同余关系,当且仅当(∀s,s',t,t'∈X)s~s'且t~t'有st~s't'(注意:同余关系中涉及到X中元素间的运算而等价关系则没说)。

4 模m同余

定义4.1假设m>0为固定的整数,如果a,b∈z且m|(a-b)那么我们说a与b模m同余,并且表示成a≡b(modm)

关于模m同余,很清楚它指出了整数集合Z中元间的一种关系,我们将会看到:

命题4.1模m同余是整数集合Z上的等价关系,并且Z恰好分成m个等价类

证明:(1)模m同余是整数集合Z上的等价关系,这是因为:

(ⅰ)(∀a∈Z)a≡a(modm)因为m|(a-a);

(ⅱ)(∀a,b∈Z)a≡b(modm)⇒b≡a(modm),因为m|(a-b)⇒m|(b-a);

(ⅲ)(∀a,b,c∈Z)[a≡b(modm)且b≡c(modm)]⇒a≡c(modm),因为[m|(a-b)且m|(b-c)]⇒m|[(a-b)+(b-c)]⇒m|(a-b);

注意:(∀a,b∈Z)a~b⇔a≡b(modm)⇔m|(a-b)

(2)Z被Z上的等价关系模m同余分成m个等价类,这是因为:

将整数a的等价类记为[a]。[a]=[b]⇔a~b⇔a≡b(modm)(*)给了任意整数a,由除法算式知道:存在唯一一对整数q和r,o≤r<m使得a=mq+r于是a-r=mq,从而m|(a-r)因此a≡r(modm)由式子(*)知[a]=[r]。由于a是任意整数而o≤r<m,从而每个等价类必为[o],[l],…,[m-1]中之一,但是这m个等价类是两两不同的:因为如果o≤i<j<m则o<j-i<m,从而m不整除(i-j)因此i≡j(modm)不成立。由式子(*)知[i]≠[j]这表明整数集Z上关于模m同余的等价类只有m个。进一步我们还有:

命题4.2模m同余是半群(Z,o)(其中o是普通乘法运算)上的同余关系。

证明:我们要证明:(∀a,a',b,b'∈Z)a~a'且b~b'有ab~a'b'

注意到命题4.1的证明过程中我们指出的:

a~b⇔a≡b(modm)⇔m|(a-b)(Δ)若a~a'且b~b'则m|(a-a')且m|(b-b')从而m|b(a-a')且m|a'(b-b')。因此m|[b(a-a')+a'(b-b')]即m|(ab-a'b')由式子(Δ)有ab~a'b'。

5 群论中的相关概念及一个重要定理

定义5.1如果一个半群G包含一个(ⅱ)(双侧)幺元素e∈G,使得ae=ea=a(对所有a∈G)便称G是一个幺半群;

如果幺半群G满足(ⅲ)对于每个a∈G,均存在(双侧)逆元素$a^{-1}\in G$使得$a^{-1}a=aa^{-1}=e$便称G是一个群;

如果半群G的二元运算满足(ⅳ)交换律:ab=ba(对所有的a,b∈G)便称G是交换幺半群或Abel半群;

定义5.2一个群G的元素的个数叫做这个群G的阶,常记作|G|

定义5.3若a是群G的一个元,能够使得$a^m=e$成立的最小的正整数m叫做元素a的阶,a的阶常记作|a|;若不存在正整数m使得$a^m=e$,我们说a的阶无限。

假设G是群,H是它的非空子集,如果对于每个a,b∈H均有ab∈H我们说H对于G中的二元运算是封闭的。

定义5.4假设G是群,H是它的非空子集,且H本身对于G中的二元运算是封闭的,如果H本身对于G中的二元运算是群,则称H为G的一个子群,记作H<G。值得指出的是,子群H中的幺元素e就是G中的幺元素,H中元素a在H中的逆元a^{-1}就是a在G中的逆元。

定义5.5设a是群G中的一个元素,且|a|=n,集合$S=\{a,a^2,\cdots a^n\}$对于G中的二元运算是G的一个子群,称作是由阶为n的元a生成的子群,记作〈a〉下面我们给出本文中的一个极其重要的

定理5.1设R(~)是幺半群G上的一个同余关系。幺半群G上的所有R等价类组成的集合G/R对于二元运算[a][b]=[ab]是幺半群(其中[x]表示x∈G的等价类),如果G为[Abel]群,则G/R亦然

证明:注意到[a][b]=[ab]是可以定义的,因为:如果[a]=[a'],[b]=[b']即a~a',b~b',从而ab~a'b'(~是同余关系)所以[ab]=[a'b']这就是说,两个等价类参与规定的二元运算的结果与等价类的代表元无关。

这个二元运算满足(ⅰ)结合律:([a][b])[c]=[a]

([b][c])(证明留给读者)(ⅱ)存在(双侧)幺元素[e],使得[a][e]=[ae]=[a]=[ea]=[e][a],于是G/R为幺半群。

如果G为群,则[a]∈G/R显然有逆元素[a^{-1}],因此G/R也是群。类似地,G的交换性导致G/R的交换性。

下面的事实很容易由定理5.1得出:交换幺半群(Z,o)(o是普通乘法运算)上的模m同余的所有等价类(由命题4.1事实上只有m个等价类)的集合记为Z_m={[0],[1],…[m-1]}规定二元运算[a][b]=[ab]则Z_m关于该二元运算是交换幺半群,其中[1]是幺元素。

命题5.1 如果m为素数,Z_m的非零元素组成的集合Z_m^+={[1],[2],…[m-1]}关于二元运算[a][b]=[ab]形成(m-1)阶群。

证明:Z_m^+关于二元运算[a][b]=[ab]是封闭的(证明留给读者)。∀[a]∈Z_m^+则[a]≠[0],即a≡0(modm)不成立。从而m不整除a,但m为素数,所以(m,a)=1,从而存在s,t∈Z使得ms+at=1(实际上,由于m是素数,t不是m的倍数,即[t]≠[o])于是at≡1(modm)从而由式子(*)知[at]=[1],即[a][t]=[t][a]=[1],即[a]∈Z_m^+中有逆元而Z_m^+显然满足结合律,而Z_m中的幺元素[1]也是Z_m^+中的幺元素,从而结论成立。

为了完成欧拉——费马定理的证明,我们还需要群论中的一些知识。

6 陪集与指数

我们看一个群G和G的一个子群H,我们规定一个G上元间的关系R:

(∀a,b∈G),(a,b)∈R⇔ab^{-1}∈H读者很容易证明关系R是G上的一个等价关系。由定理2.1知G上的等价关系R决定了G上的一个分类

定义6.1 由上面规定的群G上的等价关系R所决定的类叫做子群的H右陪集。包含元a的右陪集用符号Ha来表示(实际上,Ha={ha | h∈H},这个事实读者容易证明)。

类似地,我们如果这样规定一个G上元间的关系L:(∀a,b∈G)(a,b)∈L⇔a^{-1}b∈H,它也是G上的一个等价关系。利用这个等价关系,我们可以得到G的另一个分类。

定义6.2 由上面规定的群G上的等价关系L所决定的类叫做子群H的左陪集。包含元a的左陪集用符号aH来表示(其中aH={ah | h∈H})。值得提醒读者的是,H的右陪集和左陪集一般情况下是不相同的,但它们之间有一个共同点。

定理6.1 一个子群H的右陪集的个数和左陪集的个数相等,它们或者都是无限大或者都是有限并且相等。

证明:我们把H的所有右陪集作成的集合记为s_r,H的所有左陪集作成的集合记为s_l。建立对应Φ:s_r→s_l,Ha ↦ a^{-1}H,事实上Φ是一个s_r到s_l的一个一一对应。因为:

(i)Ha=Hb⇒ab^{-1}∈H⇒ba^{-1}=$(ab^{-1})^{-1}$∈H⇒$(b^{-1})^{-1}$$(a^{-1})$∈H⇒$a^{-1}$H=$b^{-1}$H,所以右陪集Ha的像与a的选择无关,Φ是$s_r$到$s_l$的一个映射;

(ⅱ)s_l的任意元aH是s_r的元Ha^{-1}的像,所以Φ是满射;

(ⅲ)a^{-1}H=b^{-1}H⇒ab^{-1}=$(a^{-1})^{-1}$$(b^{-1})$∈H⇒Ha=Hb,所以Φ是单射。于是我们有下面的

定义6.3 一个群G的一个子群H的右陪集(或者左陪集)的个数叫做H在G中的指数,记为[G:H]

关于子群H和它的每一个右陪集Ha,我们有如下的

引理6.1 一个子群H与H的每一个右陪集Ha之间都存一个一一映射。

证明:建立对应Φ:H→Ha,h ↦ ha,我们说Φ实际上是H与Ha间的一个一一映射,因为:

(ⅰ)H的每个元H都有一个唯一的像ha,Φ是映射;

(ⅱ)Ha的每个元ha都是H中h的像,Φ是满射;

(ⅲ)若h_1a=h_2a则h_1=h_2,Φ是单射。

由这个引理,我们可以得到极其重要的定理6.2和定理6.3

定理6.2 假定H是一个有限群G的一个子群,且|H|=n,[G:H]=j,|G|=N则有N=nj

证明:G的阶N阶是有限的,那么H的阶n和指数j都是有限正整数。G的N个元被分成j个右陪集,而由引理6.1,每一个右陪集都有n个元,从而N=nj。

定理6.3 一个有限群G的任一元a的阶n都整除G的阶N

证明:a生成一个阶是n的子群〈a〉,由定理6.2知n | N。

推论6.1 设群G的阶为N,a是G中的任意元,则有a^N=e。

证明:设|a|=n,由定理6.3知n | N,即N=nq(q是整数)。但a^n=e从而a^N=$(a^n)^q$=e^q=e。

7 Proof of Euler-Fermat Theorem

考察Z_p(P是素数)的非零元素组成的集合Z_p^+={[1],[2],…[p-1]}

Proof:(i)由命题5.1知:Z_p^+关于二元运算[a][b]=[ab]形成(p-1)阶群;

(ii)∀a∈Z且(p,a)从而a≡0(modp)不成立,即[a]≠[0],从而[a]∈Z_p^+;

(iii)由推论6.1知:$[a]^{p-1}$=[1],从而$[a^{p-1}]$=[1],因此$a^{p-1}\equiv 1(\mathrm{mod}p)$。

最后指出,欧拉——费马定理常表现为:(a是任意整数,p是素数)$a^p\equiv a(\mathrm{mod}p)$。

注释及参考文献:

[1]J.M.HOWIE. An introduction to Semigroup theory[M].London;New York:Academic Press,1976.

[2]Thomas.W.Hungerford .Algebra[M].1982.

[3]聂灵沼,丁石孙著.代数学引论[M].北京:高等教育出版社,2000.

[4]张禾瑞著.近世代数基础[M].北京:人民教育出版社,1979.

One Application about Rough Algebra

ZHANG Hai-fang, FEI Xiu-hai

(Department of Math, Junior College Level Normal School, Lincang, Yunnan 677000)

Abstract: In this paper, we introduced some basic conceptions of semi-group and the important theorem5.1 firstly. And then, we proved that $Z_m=\{[0],[1],\cdots[m-1]\}$ is a monoid semi-group in the binary Operation [a][b]=[ab], consequently, Z_m^+ is a group of (m-1) order. Finally, we obtained the inference 6.1, and finished this proof.

Key words: Euler-Fermat; Equivalence relation; M-congruence modulo

(上接33页)

[5]Browder F E. Nonlinear mappings of nonexpansive and accretive type in Banach spaces[J]. Bull Amer Math Soc,1967,73:875-882.

[6]L.S.LIU, Ishikawa and Mann. Iterative process with errors for nonlionear strongly accretive mappings in Banach spaces[J]. Math.Anal.,1995,194:114-125.

[7]谷峰.赋范空间中渐进一致 φ-为压缩型映象不动点的迭代逼近[J].数学实践与认识.2006,37(3):282-287.

[8]刘桂霞,姚力. Banach空间中两类压缩映射的迭代逼近[J].大学数学,2006,22(6):48-52.

[9]王兵. 赋范空间中有限个渐进一致 φ-伪压缩型映象公共不动点的迭代逼近[J].重庆工商大学学报(自然科学版),2009(5):434-436.

The Iterative Approximation of Limited Cluster Quasi-Contractive Mapping in Banach Space

A Li Fei-ri, HE Zhong-quan*

(School of Mathematics and Information, ChinaWest Normal University, Nanchong, Sichuan 637009)

Abstract: In a solid Banach space, the introduction of a revised limited cluster $T_1, T_2, \cdots, T_m$ quasi-contractive mapping was done, and proved that under certain conditions, on the $\{x_n\}$ of iterations: $x_{n+1}=(1-\alpha_{1n})x_n+\alpha_{1n}T_1y_{1n}+u_{1n}$, $y_{1n}=(1-\alpha_{2n})x_n+\alpha_{2n}T_2y_{2n}+u_{2n}\cdots$, $y_{(m-1)n}=(1-\alpha_{mn})x_n+\alpha_{mn}T_mx_n+u_{mn}$, $(m\geq 2)$ strong convergence in a finite number of clusters to be compression of the common fixed point of $T_1, T_2, \cdots, T_m$. The results of this paper improve and generalize of the latest results of the literature.

Key words: Quasi-contractive mapping; Consistent smooth Banach space; An error of Ishikawa iterations; Normalized duality mapping; Fixed point