群与半群

陶先平 赵建华

内容

- 系统公理与公理化系统
- 半群
- 独异点（单元半群）
- 群公理
- 群方程及解
- 群与消去律
- 群表

半群与群

- 半群(Semigroup)
  - 代数系统$< S,\circ >$，其中$\circ$满足结合律
- 单元半群(Monoid)
  - 具有单位元素的半群
- 群（Group）
  - 所有元素可逆的单元半群

半群

- 系统公理：结合律
- 例子

  $(\{1,2\},*)$, 对任意 $x,y\in\{1,2\}$, $x*y=y$
- 证明：

  $(x*y)*z = z = x*z = x*(y*z)$
- 满足交换律的半群称为“可换半群”

独异点（单元半群）

- 系统公理：
  - 结合律
  - 有单位元素
  - 即有单位元的半群
- 例子：

$$S=\left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| a,d \in R\right\} \qquad T=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in R\right\}$$

- S与矩阵乘法构成独异点，T与矩阵乘法也构成独异点。T是S的**子半群**，但不是**子独异点**。

例子

- (A,*)是半群，且 $\forall a,b(\mathrm{a} \neq b \Rightarrow a * b \neq b * a)$，或者说$\forall a,b(\mathrm{a} * \mathrm{b} = b * a \Rightarrow \mathrm{a} = \mathrm{b})$。有如下性质
  - a*a = a

    简证：(a*a)*a = a*(a*a)
  - a*b*a = a

    (a*b*a)*a=(a*b)*(a*a)=a*b*a，且a*(a*b*a)=a*b*a
  - a*b*c = a*c

    (a*b*c)*(a*c)=(a*b)*(c*a*c)=a*b*c,

    (a*c)*(a*b*c)=a*b*c

例子：寻找单位元素

- (A,*)是半群，假设存在元素a, 满足：对任意x, 总存在u,v, 使得a*u=v*a=x。证明：A含单位元素。
- 证明：
  - 对于a本身，存在u_a,v_a, 满足：$a*u_a=a$; $v_a*a=a$。
  - 则对任意x, $x*u_a=(v*a)*u_a=v*a=x$, 即u_a是右单位元素。同理可证v_a是左单位元素。
  - 则：$u_a=v_a$是单位元素。

乘幂

- 如果运算 满足结合律，则如下定义的乘幂有意义：

  $x^1 = x$

  $x^{n+1} = x^n \quad x$ (n是正整数)

- 如果运算 另外还满足有单位元，则如下定义的乘幂有意义：

  $x^0 = e$ (e是单位元素)

  $x^{n+1} = x^n \quad x$ (n是非负整数)

  $x^n \quad x^m = x^{n+m}$

  $(x^n)^m = x^{nm}$

群公理

- 结合律
  - 因此：群也是半群
- 有单位元素
  - 因此：群也是独异点
- 每个元素均有逆元素
  - 将元素a的逆元素记为a^{-1}
  - 幂的扩展：定义$a^{-k} = (a^{-1})^k$ (k为正整数)

- 如果还满足交换律：可交换群(阿贝尔群)

群的例子

- 整数加群: $(Z,+)$
  - 加法可结合；单位元素0；a的逆元素为$(-a)$
- 剩余加群: $(Z_n, +_n)$ (其实这一类群，含无穷多个群)
  - $Z_n=\{0,1,2,\ldots,n-1\}$, $a+_n b=$<$a+b$除以n的余数>
  - 剩余加可结合；单位元素0；a的逆元素为$n-a$
- 非零实数乘法群: $(R-\{0\},\bullet)$
  - 乘法可结合；单位元素1；x的逆元素为$1/x$
  - 注意：实数集与乘法**不**构成群
- 每行每列恰好有一个1，其它元素均为0的所有$n\times n$阶矩阵 以及 矩阵乘法构成群
  - 矩阵乘法可结合；单位元是主对角元素全为1而其它元素全为0的矩阵；根据线性代数知识可知这样的矩阵是可逆矩阵。

集合上的置换

- 在集合$\{1,2,3\}$上可以定义6个一一对应的函数：

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\quad \alpha=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad \beta=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$\gamma=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\quad \delta=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\quad \varepsilon=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

有限集合上的一一对应的函数称为置换。

群S_3

- $(\{e,\alpha,\beta,\gamma,\delta,\varepsilon\}，\quad)$构成群，其中，　是函数复合运算。

	e	α	β	γ	δ	ε
e	e	α	β	γ	δ	ε
α	α	β	e	δ	ε	γ
β	β	e	α	ε	γ	δ
γ	γ	ε	δ	e	β	α
δ	δ	γ	ε	α	e	β
ε	ε	δ	γ	β	α	e

运算表

例如：

$$\delta\quad\gamma(1)=\gamma(\delta(1))=\gamma(3)=2$$

$$\delta\quad\gamma(2)=\gamma(\delta(2))=\gamma(2)=3$$

$$\delta\quad\gamma(3)=\gamma(\delta(3))=\gamma(1)=1$$

即：$\delta\quad\gamma=\alpha$

群的直积

- 给定两个群: $(S,\ )$, $(T,*)$, 定义笛卡儿乘积 $S\times T$上的运算$\otimes$如下：

  $\langle s_1,t_1\rangle \otimes \langle s_2,t_2\rangle = \langle s_1\quad s_2,\ t_1*t_2\rangle$

- $(S\times T,\ \otimes)$是群
  - 结合律： $\langle (r_1\quad s_1)\quad t_1,\ (r_2*s_2)*t_2\rangle$

    $= \ \langle r_1\quad (s_1\quad t_1),\ r_2*(s_2*t_2)\rangle$
  - 单位元素： $\langle 1_S,\ 1_T\rangle$
  - 逆元素： $\langle s,\ t\rangle$ 的逆元素是 $\langle s^{-1},\ t^{-1}\rangle$
    - (其中： $s,\ s^{-1}\in S,\ \ t,\ t^{-1}\in T$)

又一个群的例子

- 已知(S,)是群， u是S中一个特定的元素， 定义S上一个新运算*如下：
  - $a*b = a\ \ u^{-1}\ \ b$
- (S, *)是群：
  - 结合律：
    - $(a*b)*c = a*(b*c) = a\ \ u^{-1}\ \ b\ \ u^{-1}\ \ c$
  - 单位元素：
    - 对任意x, $x*u = x\ \ u^{-1}\ \ u = x$, 而$u*x = u\ \ u^{-1}\ \ x = x$
  - 逆元素：
    - 对任意x, $x*(u\ \ x^{-1}\ \ u) = x\ \ u^{-1}\ \ (u\ \ x^{-1}\ \ u)$

      其中x^{-1}是(S,)中x的逆元素

考察函数$f(x) = x\ \ u$

群方程及其解

- 群方程：
  - $a\ \ x=b$ 和 $y\ \ a=b$ 称为群方程
- 群方程的解：
  - $a\ \ x=b \rightarrow a\ \ (a^{-1}\ \ b)=b$
  - $y\ \ a=b \rightarrow (b\ \ a^{-1})\ \ a=b$
- 群方程的解是唯一的
  - 假设$a\ \ x_1=b=a\ \ x_2$, 等号两边同时左乘a^{-1},
    有： $x_1=a^{-1}\ \ b=x_2$,

群的第二定义

- 代数系统(G,)满足结合律，且形如a x=b 和 y a=b 的方程均有唯一解，则(G ,)是群
- 证明

(1) y b=b 有唯一解，设为e, 证明e是**左单位元素**:

(2) b y=b 有唯一解，设为e’, 证明e’是**右单位元素**:

(3) 证明e=e’就是单位元。

(4) 对于任意元素a，y a=e和a y=e各自有唯一解，设为a’和a’’。证明a’=a’’，即知a’是a的逆元。

群与消去律

- 群满足消去律：
  - 设$(G,\ )$是群，对任意$a,b,c\in G$

    若$a\ \ b=a\ \ c$, 则$b=c$

    若$b\ \ a=c\ \ a$, 则$b=c$

- 正整数集与普通乘法构成的代数系统满足结合律和消去律，但它**不是**群。

有限群与消去律

- 设G是有限集合，代数系统(G,)满足结合律和消去律，则(G,)是群
- 证明要点

设$G=\{a_1,a_2,a_3,\ldots,a_n\}$，对G中任意给定的元素$a_i$,考虑集合$a_iG=\{a_i\ \ a_1, a_i\ \ a_2, a_i\ \ a_3, \ldots, a_i\ \ a_n\}$。注意$a_iG$是G的子集(运算封闭)，同时又与G等势(消去律)，所以：$a_iG=G$。这意味着方程a x=b 有唯一解。(***Why?***)

类似地可证方程y a=b也有唯一解。

因此：(G,)是群

“单侧”消去律

- 设$(S,\ \ )$是有限半群，$\forall a,b,c\in S$, 若$ba=ca$, 则$b=c$ (这称为右消去律)，且S中存在左单位元，证明: $(S,\ \ )$是群。
  - 设$S=\{a_1,a_2,a_3,\ldots,a_n\}$，对$S$中任意给定的元素$a_i$,考虑集合$Sa_i=\{a_1\ a_i,\ a_2\ a_i, a_3\ a_i, \ldots, a_n\ a_i\}$。注意$Sa_i$是$S$的子集(运算封闭)，同时又与$S$等势(右消去律)，所以： $Sa_i=S$。因此对任意a,b, 方程$y\ a=b$也有唯一解。
  - 于是，$y\ a=e_{左}$有唯一解a^*。$\forall a,b,c\in S$, 若$ab=ac$, 则$a^*ab= a^*ac$, 即$b=c$, 即$(S,\ )$也满足左消去律，它是群。
- 给出反例证明：若上述条件中删除“有左单位元”，则结论不成立。

群元素的阶

- 定义：
  - 设G是群，a是G中元素。使得等式$a^k = e$成立的最小正整数K称为a的阶（周期），记为$|a|=k$.
    - 如果这样的K不存在，a为无限阶元
- 性质：
  - 有限群不存在无限阶元。
  - 群中元素及其逆阶相同
  - 有限群中阶大于2的元素有偶数个
  - 偶数群中阶为2的元素有奇数个

群表

- 群方程有唯一解在群表中的体现
  - 设G={$a_1,a_2,\ldots,a_n$}

    假设第i行上有两个相同元素a_j，分别在第k, l列，则意味着$a_i*x=a_j$有两个不同的解。矛盾。

    同样可以讨论一列上有两个相同元素的情况。

这就意味着：群表中的每一行或每一列均为群中所有元素的一种排列，因此行和列也不可能出现同样的排列。

习题

- p.202-204
  - 2
  - 4
  - 5
  - 11
  - 15-19

Niels Abel(1802-1829):天才与贫困

- 阿贝尔的第一个抱负不凡的冒险，是试图解决一般的五次方程。…失败给了他一个非常有益的打击；它把他推上了正确的途径，使他怀疑一个代数解是否是可能的。他***证明了不可解***。那时他大约十九岁。
- 阿贝尔的《关于非常广泛的一类超越函数的一般性质的论文》呈交给巴黎科学院。这就是勒让德后来用贺拉斯的话描述为“永恒的纪念碑”的工作，埃尔米特说：“***他给数学家们留下了够他们忙上五百年的东西。***”它是现代数学的一项登峰造极的成就。(摘自贝尔：《数学精英》)
  - 这篇论文的一个评阅人勒让德74岁，发现这篇论文很难辨认，而另一位评阅人，39岁的柯西正处于自我中心的顶峰，把论文带回家，不知放在何处，完全忘了。4年后，当柯西终于将它翻出来时，阿贝尔已经不在人世。作为赔偿，科学院让阿贝尔和雅可比一起获得1830年的数学大奖。

- 伽罗华
  - Galois，公元1811年~公元1832年
  - 群论的创始人
  - 法国对函数论、方程式论和数论作出重要贡献的数学家
  - 数学史上最“悲剧”的数学家