离散数学 II
Discrete Mathematics II

封筠

fengjun@stdu.edu.cn

20-11

课程回顾

群与子群：群的定义、群的性质（5个）、群的阶数、子群的定义、子群的性质（3个）

5-5 阿贝尔群和循环群

●学习本节要熟悉如下术语（4个）：

阿贝尔群、循环群、生成元、阶

●要求：

掌握3个定理

一、阿贝尔群（Abel 群）

1、定义 5-5.1 设 **<G,*>**为一群,若 * 运算满足交换律,则称G为交换群或阿贝尔群(***Abel group***)。阿贝尔群又称加群，常表示为**<G，+ >**（这里的 + 不是数加，而泛指可交换二元运算）。加群的幺元常用**0**来表示， 元素**x**的逆元常用**-x**来表示。

例题1 设S={a,b,c,d}，在S上定义一个双射函数 f: f(a)=b,f(b)=c,f(c)=d,f(d)=a,

对于任一x∈S，构造复合函数

$f^2(x)=f \circ f(x)=f(f(x))$

$f^3(x)=f \circ f^2(x)=f(f^2(x))$

$f^4(x)=f \circ f^3(x)=f(f^3(x))$

如果用f^0表示S上的恒等映射，即$f^0(x)=x \quad x\in S$

很明显地有$f^4(x)=f^0(x)$，记$f^1=f$，构造集合

$F=\{f^0, f^1, f^2, f^3\}$，那么<F，o>是一个阿贝尔群。

解 对于F中任意两个函数的复合，可以由下表给出

o	f^0	f^1	f^2	f^3
f^0	f^0	f^1	f^2	f^3
f^1	f^1	f^2	f^3	f^0
f^2	f^2	f^3	f^0	f^1
f^3	f^3	f^0	f^1	f^2

可见，复合运算o关于F是封闭的，并且是可结合的。

f^0的逆元就是它本身， f^1和f^3互为逆元， f^2的逆元也是它本身。

由表的对称性，可知复合运算o是可交换的。

因此<F，o>是一个阿贝尔群。

再看5-4节P191例题1

★	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

已经验证了<R，★>是群。

由运算表的对称性知运算★是可交换的，因此<R，★>是阿贝尔群。

练习 P200（1）

设<G，*>是一个独异点，并且对于G中的每一个x都有x*x=e，其中e是幺元，证明<G，*>是一个阿贝尔群。

证明　x*x=e说明G中的每一个元素x都是自身的逆元，所以<G，*>是一个群。

任取x，y∈G，则x*y∈G

因为$x*y=(x*y)^{-1}=y^{-1}*x^{-1}=y*x$

所以<G，*>是一个阿贝尔群。

此题的推论：若群中每个元素的逆元都是它自己，则该群必是可交换群。

例题2 设G为所有n阶非奇（满秩）矩阵的集合，矩阵乘法运算 o 作为定义在集合G上的二元运算，则<G, o >是一个不可交换群。

解 任意两个n阶非奇矩阵相乘后，仍是一个非奇矩阵，所以运算 o 是封闭的。

矩阵乘法运算 o 是可结合的。

n阶单位阵E是G中的幺元。

任意一个非奇矩阵A存在唯一的逆阵A^{-1}，使$A^{-1}oA=AoA^{-1}=E$。

但矩阵乘法运算 o 是不可交换的，因此<G, o >是一个不可交换群。

2、**定理 5-5.1** 设 <G,*>为一群, <G,*>是阿贝尔群的充要条件是对任意的a,b∈G，有

$$(a*b)*(a*b)=(a*a)*(b*b)$$

□ 证明：1）先证充分性

从条件“（a*b）*（a*b）=（a*a）*（b*b）”出发，推出“<G,*>是阿贝尔群”的结论：

对于元素a,b∈G，有(a*b)*(a*b)=(a*a)*(b*b)

因为 a*(a*b)*b=(a*a)*(b*b)=(a*b)*(a*b)

=a*(b*a)*b

即 a*(a*b)*b=a*(b*a)*b

由可约性得，用a^{-1}左*上式，再用b^{-1}右*上式，

(a*b)=(b*a)

2）再证必要性

从“<G,*>是阿贝尔群”的结论出发，推出

“(a*b)*(a*b)=(a*a)*(b*b)”条件：略□

二、循环群

1、定义5-5.2 设<G,*>为群，如果在G中存在元素 a ,使 G以{a}为生成集，即G的任何元素都可表示为 a 的幂（约定$e=a^0$）,称<G,*>为循环群(*cyclic group*)，这时a称为循环群G的生成元（*generater*）。

例如，60°就是群

<{0° ,60° ,120° ,180° ,240° ,300°}, ★>的生成元，因此，该群是循环群。

2、定理 5-5.2 设任何一个循环群必定是阿贝尔群。

□ 证明思路:循环群⇒是阿贝尔群

设 $<G,*>$是一个循环群， a是该群的生成元，则对于任意的$x,y\in G$ ，必有$r,s\in I$，使得

$$x= a^r \text{ 和 } y = a^s$$

而且 $$x*y=a^r*a^s=a^{r+s}=a^{s+r}=a^s*a^r=y*x$$

因此，运算*可交换，是阿贝尔群。 □

3、定义5-5.3 设<G,*>为群，$a \in G$，

如果$a^n = e$, 且n为满足此式的最小正整数,则称a 的阶(*order*)为n，如果上述n不存在时,则称a有无限阶.

练习 每个元素的阶是多少？

★	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

4、定理 5-5.3 设$<G,*>$为有限循环群，$a \in G$是该群的生成元，如果G的阶数是n，即$|G|=n$，则$a^n=e$,且

$$G=\{a, a^2, a^3,..., a^{n-2}, a^{n-1}, a^n=e\}$$

其中，e是群$<G,*>$的幺元。n是使$a^n=e$的最小正整数。

证明思路:先证a的阶为n

设对于某个正整数m,m<n,有$a^m=e$。那么，由于<G,*>是一个循环群，所以对于G中任意的元素都能写为a^k ($k\in I$),而且k=mq+r,其中q是某个整数,0≤r<m,则有

$$a^k=a^{mq+r}=(a^m)^q*a^r=(e)^q*a^r=a^r$$

因此，G中每一元素都可写成$a^r(0\leqslant r<m)$，G中最多有m个元素。与 |G|= n矛盾。所以$a^m=e$是不可能的。

再用反证法证明a， a^2，...， a^n互不相同。

设$a^i=a^j$，其中$1\leqslant i<j\leqslant n$，就有$a^{j-i}=e$，而且$1\leqslant j-i<n$，这已经有上面证明是不可能的。 所以 a，$a^2$，...， a^n都不相同。

因此$G=\{a, a^2, a^3,..., a^{n-2}, a^{n-1}, a^n=e\}$

练习 < Zm , +m >生成元是什么？每个元素的阶是多少？

表 5-3.2

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

例题3 设集合G={α，β，γ，δ}，在G上定义二元运算*如下表所示。试说明<G, * >是一个循环群。

*	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β

解 由上表可知运算*是封闭的，α是幺元。

β，γ 和 δ 的逆元分别是β, δ和γ。可以验证运算*是可结合的。所以<G, * >是一个群。在这个群中，由于

$$\gamma^* \gamma = \gamma^2 = \beta,\quad \gamma^3 = \delta,\quad \gamma^4 = \alpha$$

以及$\delta * \delta = \delta^2 = \beta,\quad \delta^3 = \gamma,\quad \delta^4 = \alpha$

故群<G, * >是由γ或δ生成的，因此<G, * >是一个循环群。

从上例可知：一个循环群的生成元可以不是唯一的。

作业：P200 (2)只做阿贝尔群证明、(4)还要给出每个元素的阶

The End