离散数学 II
Discrete Mathematics II

封筠

fengjun@stdu.edu.cn

20-11

课程回顾

半群：广群、半群、子半群、独异点、模m的同余类

5-4 群与子群

- 学习本节要熟悉如下术语（8个）：

  群、有限群、阶数、无限群、置换、等幂元、子群、平凡子群

- 要求：

掌握8个定理

一、群

1、定义5-4.1 称代数结构<G,*>为群(*groups*), 如果

（1） <G，*>中运算*是封闭的。

（2） <G，*>中运算*是可结合的。

（3） <G，*>中有么元e.

（4） <G，*>中每一元素x都有逆元x^{-1}。

例如，<R-{0}, ×>，$<\wp(S), \oplus>$等都是群。

例题1

设R={0°,60°,120°,180°,240°,300°}表示在平面上几何图形绕形心顺时针旋转角度的六种可能情况，设★是R上的二元运算，对于R中任意两个元素a和b，a★b表示平面图形连续旋转a和b得到的总旋转角度。并规定旋转360°等于原来的状态，就看作没有经过旋转。验证<R, ★>是一个群。

解 列运算表，可知运算★在R上是封闭的。

★	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°

对于任意的a,b,c∈R，(a★b)★c表示将图形依次旋转a,b和c,而a★(b★c)表示将图形依次旋转b,c和a,而总的旋转角度都等于

$a+b+c \pmod{360^\circ}$,

因此，(a★b)★c=a★(b★c)。

0°是幺元。

60°, 180°, 120°的逆元分别是300°, 180° , 240° 。因此<R, ★>是一个群。

2、定义5-4.2　设 <G,*>为一群。若 G为有限集，则称<G,*>为有限群（*finite group*）, 此时G的元素个数也称G的阶数(*order*),记为|G|；否则，称<G,*> 为无限群（*infinite group*）。

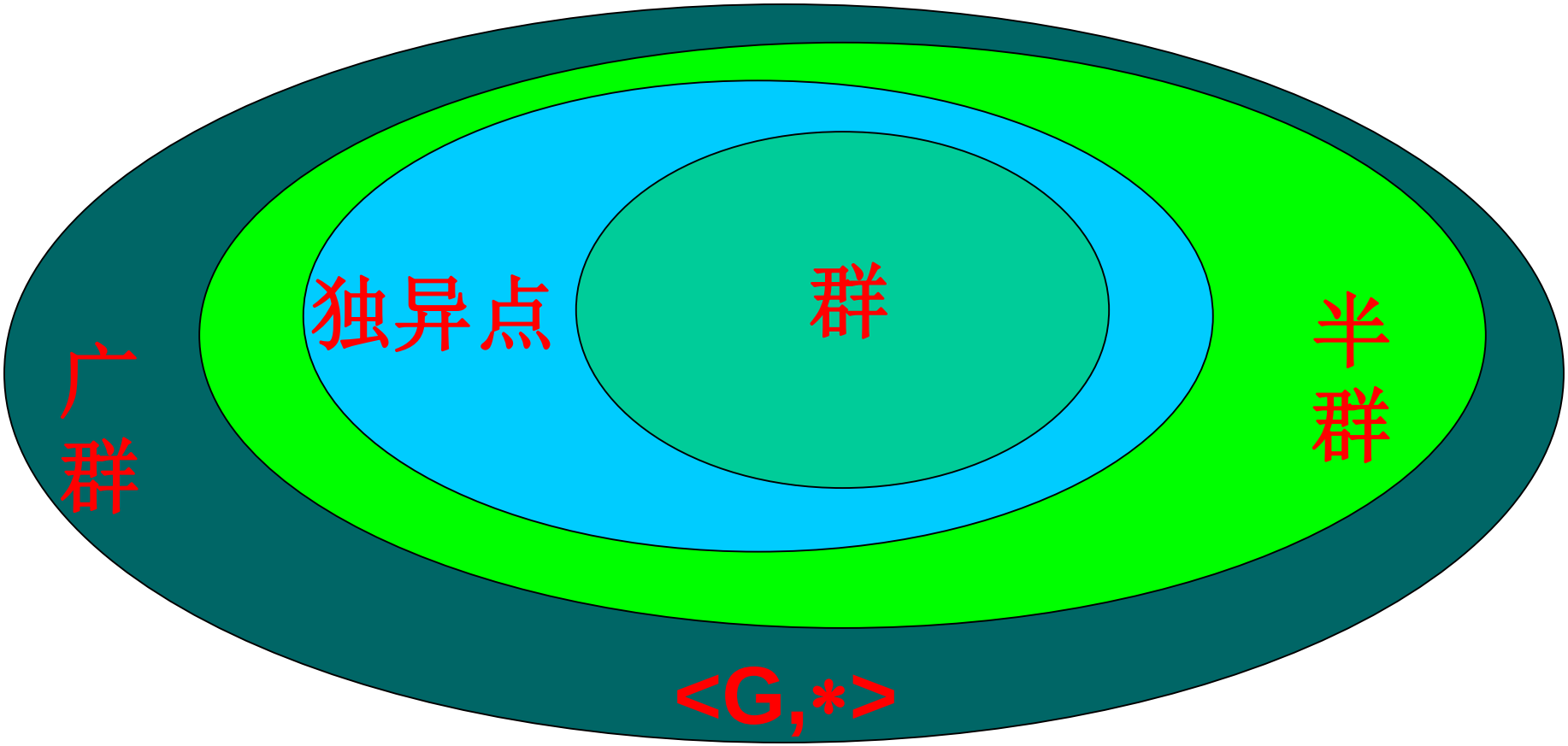
例题1中所述的<R, ★>就是一个有限群，且|R|=6。

例题2 试验证代数系统<I，+>是一个群，这里I是所有整数的集合，+是普通加法运算。

解 明显地，二元运算+在I上是封闭的且是可结合的。幺元是0。对于任一a∈A，它的逆元是-a。所以<I，+>是一个群，且是一个无限群。

代数结构小结

<G,*> —封闭→ 广群 —结合→ 半群 —含幺→ 独异点 —可逆→ 群



由定理5-2.4可知，群中任何一个元素的逆元必定是唯一的。由群中逆元的唯一性，我们可以有以下几个定理。

3、群的性质

定理5-4.1 设<G，*>为群，那么当$G \neq \{e\}$时，G无零元。即群中不可能有零元。

□ 证明：因当群的阶为1时，它的唯一元素是视作幺元e 。设|G|>1 且群有零元。那么群中任何元素$x \in G$，都有 $x * \theta = \theta * x = \theta \neq e$，所以，零元θ就不存在逆元。与G是群的假设矛盾

回看第190页5-3习题（3）

定理5-4.2 设$<G, *>$为群，对于$a,b \in G$，必存在$x \in G$，使得关于x的方程$a*x=b$有唯一解。

□ 证明：1）先证解存在性

设a的逆元a^{-1}，令

$x = a^{-1} * b$ （构造一个解）

$a*x = a*(a^{-1}*b)$

$=(a*a^{-1})*b$

$=e*b=b$

2）再证解唯一性

若另有解x_1满足$a*x_1 = b$，则

$a^{-1}*(a*x_1) = a^{-1}*b$

$x_1 = a^{-1}*b$ □

定理5-4.3 设<G，*>为群，那么，对任意a,b,c∈ G

$a*b = a*c$ 蕴涵 $b = c$

$b*a = c*a$ 蕴涵 $b = c$

G的所有元素都是可约的。因此，群中消去律成立。

□ 证明：设$a*b=a*c$,且a的逆元a^{-1}，则有

$$a^{-1}*(a*b) = a^{-1}*(a*c)$$

$$e*b = e*c$$

$$b = c$$

同理可证第二式。□

4、定义5-4.3 设S是一个非空集合，从集合S到S的一个双射称为S的一个置换。

譬如，对于集合S={a,b,c,d}，将a映射到b，b映射到d，c映射到a，d映射到c是一个从S到S上的一个一对一映射，这个置换可以表示为

$$\begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$$

即上一行中按任何次序写出集合中的全部元素，而在下一行中写每个对应元素的象。

定理5-4.4 设<G，*>为群，那么，运算表中的每一行或每一列都是群G的元素的置换。

□ 证明：先证G中每一个元素只出现一次

用反证法：设a对应行有两个元素b_1、b_2对应的都是c，　即$a*b_1=a*b_2=c$,且$b_1\neq b_2$

由可约性得$b_1=b_2$

与假设矛盾。

再证G中每一个元素必出现一次

对于元素$a\in G$的那一行，设b是G中的任意一个元素，由于$b=a*(a^{-1}*b)$，所以b必定出现在对应于a的那一行。

再由运算表中任何两行或两列都是不相同的。得出要证的结论。对列的证明过程类似。□

5、定义5-4.4设<G，＊>为代数结构，如果存在a∈G，有a＊a= a，则称 a为等幂元。

定理5-4.5 在群<G，＊>中，除幺元e之外，不可能有任何别的等幂元。

□ 证明: 因为e＊e = e，所以e是等幂元。

现设 a∈G， a≠e 且 a＊a= a

则有

回看第185页5-2习题（2）

二、子群

1、定义5-4.5 设<G，*>为群，S为G的非空子集，如果<S，*>为一群，则称<S，*>为G的子群(*subgroups*)。

2、定义5-4.6 设<G,*>为群，<S,*>为G的子群，如果，S ={e}或S =G，那么称<S,*>为<G,*>的平凡子群。

3、基本定理

定理5-4.6 设<G,*>为群，<S,*>为G的子群，那么，<G,*>中的幺元e必定也是<S,*>中的幺元 。

□ 证明: 设<S,*>中的幺元为e_1，对于任意一个元素 $x \in S \subseteq G$, 必有

$$e_1 * x = x = e * x$$

则有 $e_1 = e$ □

例题3 $<I,+>$是一个群，设$I_E=\{x|x=2n,n\in I\}$，证明$<I_E,+>$是$<I,+>$的一个子群。

证明 (1)对于任意的$x,y\in I_E$，不妨设

$x=2n_1,y=2n_2,n_1,n_2\in I$,则

$$x+y=2n_1+2n_2=2(n_1+n_2)$$

而 $n_1+n_2\in I$

所以 $x+y\in I_E$

即+在I_E上封闭。

(2)运算+在I_E上保持可结合性。

(3)<I，+>中的幺元0也在I_E中。

(4)对于任意的$x\in I_E$，必有n使得x=2n，而

$$-x=-2n=2(-n)，-n\in I$$

所以$-x\in I_E$，而x+(-x)=0，因此，$< I_E$,+>是<I,+>的一个子群。

定理5-4.7 设<G,*>[illegible]
如果B是一个有限集[illegible]
< B,*>必定是 <G,*>的子群。

第195页例题 4

□ 证明：设任意元素$b \in B$，若*在B上封闭，则元素 $b^2=b*b$, $b^3= b^2*b$, $b^4= b^3*b$,...,都在B中。由于是有限集，所以必存在正整数i和j(i<j)，使得

$$b^i=b^j$$

必有 $b^i=b^i * b^{j-i}$

即 b^{j-i} 是<G,*>中的幺元。且该幺元也在子集B中。

如果j-i>1，则由$b^{j-i} =b*b^{j-i-1}$可知b^{j-i-1}是b的逆元，且$b^{j-i-1} \in B$；如果j-i=1，则由$b^i=b^i*b$可知b是幺元，而幺元是以自身为逆元的。

因此，< B,*>必定是 <G,*>的子群。□

定理5-4.8 设$<G,\triangle>$为群,S为G的非空子集,如果对于任意元素$a,b\in S$有$a\triangle b^{-1}\in S$,那么, $<S,\triangle>$必定是 $<G, \triangle>$的子群。

□分四步证明：1）先证G中的幺元e也是S中的幺元

对任意元素$a\in S\subseteq G$, $e=a\triangle a^{-1}\in S$

且 $a\triangle e=e\triangle a=a$，即$e$也是$S$中的幺元。

2）再证S中的每一个元素逆元均在集合中

对任意元素$a\in S$中， 因为$e\in S$,

所以 $e\triangle a^{-1}\in S$ ，即$a^{-1}\in S$ 。

3）最后证明$\triangle$在S中是封闭的

对任意元素$a,b\in S$, $b^{-1}\in S$, 而$b=(b^{-1})^{-1}$

所以 $a\triangle b=a\triangle(b^{-1})^{-1}\in S$ 。

4） 结合律是保持的 □

例题5 设<H,*>和<K,*>都是群<G,*>的子群，试证明<H∩K,*>也是<G,*>的子群。

证明 设任意的$a,b\in H\cap K$，因为<H,*>和<K,*>都是子群，所以$b^{-1}\in H\cap K$，由于*在H和K中的封闭性，
所以$a*b^{-1}\in H\cap K$，由定理5-4.8即得<H∩K,*>也是<G,*>的子群。

作业：

P197 (1)、 (2)、 (3) 、(4)

The End