第五章 代数结构

5.1 代数系统的引入

集合上的运算

例如：

R上的1/a （a!=0） 一元的

R上的a+b 二元的

R上的if a=0 then b else c 三元的

共同的特征：运算结果也属于R——封闭性。

代数系统

定义5-1.1 对于集合A，一个从A^n到B的映射，称为集合A上的一个**n元运算**。如果B是A的子集，则称该n元运算是**封闭的**。

定义5-1.2 一个非空集合A连同若干个定义在该集合上的运算$f_1, f_2, \ldots, f_n$所组成的系统就称为一个**代数系统**，记作〈$A, f_1, f_2, \ldots, f_n$〉。

代数系统

注：代数系统是由一个集合和定义在集合上的若干运算构成。

①集合一般是非空的，

例：整数集，实数集，符号串集合等。

②定义在集合上的n元运算是一个从A^n到B的映射。

例：

$\langle N, + \rangle$，

$\langle \rho(S), \cup, \cap, \sim \rangle$**都是一个代数系统。**

5.2 运算及其性质

对于二元运算来说

定义5-2.1：*是定义在A上的二元运算，若$\forall x, y \in A$，有$x*y \in A$，　称*在A上是封闭的。

例：　$A=\{2^n \mid n \in N\}$，问<A，x>运算封闭否，

<A，+>，<A，/>呢?

解：$\forall 2^r, 2^s \in A$，$2^r \times 2^s = 2^{r+s} \in A$（$r+s \in N$），

∴<A，x>运算封闭。

又：$2, 4 \in A$，$2+4 \notin A$，∴<A，+>运算不封闭。

$2, 4 \in A$，$2/4 \notin A$，∴<A，/>运算不封闭。

交换律

定义5-2.2 *是定义在A上的二元运算，若∀x，y∈A，有 x*y=y*x，称*满足交换律。

例：设<有理数集，*>,*定义如下：

a*b=a+b-ab，问*满足交换律否？

证：∵∀a，b∈A，

a*b=a+b-ab=b+a-ba=b*a

∴*满足交换律。

结合律

定义5-2.3　*是定义在A上的二元运算，若∀x，y，z∈A，有x*（y*z）=（x*y）*z，称*满足结合律。

例：<A，*>，若∀a，b∈A，有a*b=b。

证明：*满足结合律

证：∀a，b，c∈A，

a*（b*c）=a*c=c

（a*b）*c=b*c=c

∴a*（b*c）=（a*b）*c

∴*满足结合律。　　#

分配律

定义5-2.4　设*和△是定义在A上的两个二元运算，若∀x，y，z∈A 都有：

$$x*(y\triangle z)=(x*y)\triangle(x*z)$$
$$(y\triangle z)*x=(y*x)\triangle(z*x)$$

，称运算*在△上**可分配**的。

例：设A={α，β}，二元运算*和△的**运算表**如右：

*	α	β
α	α	β
β	β	α

△	α	β
α	α	α
β	α	β

问分配律成立否？

*	α	β
α	α	β
β	β	α

△	α	β
α	α	α
β	α	β

解：验证_ △（_*_）组成的8个式子，看是否满足。

或者这样：

① 若能证x△(y*z)=(x△y)*(x△z)，则△对*可分配

证：当x=α：x△(y*z)=α；(x△y)*(x△z)=α

当x=β：x△(y*z)=y*z；(x△y)*(x△z)=y*z

②运算*对运算△不可分配（举一个反例即可）

证：∵β*（α△β）=β*α=β

（β*α）△（β*α）=β△α=α

吸收律

定义5-2.5　设*和△是定义在A上的两个可交换的二元运算，若∀x，y∈A有：

$x*(x \triangle y)=x$ ，$x \triangle (x * y)=x$，

称运算*和运算△满足**吸收律**。

例：N为自然数集，∀x,y∈N，x*y=max{x，y}，x△y=min{x，y}

试证：*和△满足吸收律。

证明：∀x，y∈N，

$x*(x \triangle y)=\max\{x, \min\{x, y\}\}=x$，

$x \triangle (x*y)=\min\{x, \max\{x, y\}\}=x$，

∴*和△满足吸收律。

#

等幂律

定义5-2.6 *是定义在A上的二元运算，若$\forall x \in A$，都有 x*x=x，则称*满足等幂律。

例：已知集合S，$\langle \rho(S), \cup, \cap \rangle$。

$\forall A, B \in \rho(S)$，$A \cup A = A$，$A \cap A = A$

$A \cap (A \cup B) = A$，$A \cup (A \cap B) = A$

则∪和∩满足吸收律，等幂律。

幺元和零元

定义5-2.7，5-2.8 设*是定义在A上二元运算，如果存在元素e_r，e_l，θ_r，θ_l，e，$\theta \in A$，有

①.若$\forall x \in A$，有$e_l * x = x$，称e_l为运算*的**左幺元**。

若$\forall x \in A$，有$x * e_r = x$，称e_r为运算*的**右幺元**。

②.若$\forall x \in A$，有$\theta_l * x = \theta_l$，称θ_l为运算*的**左零元**。

若$\forall x \in A$，有$x * \theta_r = \theta_r$，称θ_r为运算*的**右零元**。

③. 若$\forall x \in A$，有$e * x = x * e = x$，称e为运算*的**幺元**。**也叫单位元**

若$\forall x \in A$，有$\theta * x = x * \theta = \theta$，称$\theta$为运算*的**零元**。

么元和零元

例：

a) 〈I，×〉，I为整数集则么元为1，零元为0

b) 〈ρ(S),∪,∩〉

对运算∪，∅是么元，S是零元，

对运算∩，S是么元，∅是零元。

c) 〈N，+〉有么元0，无零元。

幺元和零元

例：代数系统A=〈{a，b，c}，∘〉，∘的运算表如下：

∘	a	b	c
a	a	b	b
b	a	b	c
c	a	b	a

则b是左幺元，无右幺元，

a是右零元，b是右零元，无左零元；

运算∘既无幺元，也无零元 。

幺元和零元

定理5-2.1: 设*是定义在 集合A上的二元运算，且在A中有关于*运算的左幺元e_l和右幺元e_r，则$e_l=e_r=e$，且幺元唯一。

证明：　　$e_r = e_l * e_r = e_l$

设有二个幺元e，e’；则e=e*e’=e’。

#

幺元和零元

定理5-2.2：设*是定义在集合A上的二元运算，且在A中有关于*运算的左零元θ_l，右零元θ_r，$\theta_l=\theta_r=\theta$，且零元唯一。

（证明与定理5-2.1类似）

定理5-2.2：设〈A，*〉是一个代数系统，且集合A中元素的个数大于1。如果该代数系统中存在幺元e和零元θ，则$\theta \neq e$。

证明：（反证法）设$\theta=e$，那么对于任意的$\forall x \in A$，必有

$x=e*x=\theta*x=\theta=e$，于是A中的所有元素都是相同的，这与A中含有多个元素相矛盾。

#

逆元

定义5-2.9 设*是定义在A上的二元运算，e是运算*的么元：

若对于元素a存在着元素b，使得b*a=e，那么称b为a的**左逆元**，如果a*b=e，则称b为a的**右逆元**。

如果一个元素b既是a的左逆元，又是a的右逆元，则称b是a的**逆元**。

显然，如果b是a的逆元，则a也是b的**逆元**，简称a与b互逆，a的逆元记作a^{-1}。

逆元

例1: 代数系统 〈R，×〉中，幺元为1，零元为0，除0外所有元素均有逆元。

例2：A= 〈{a，b，c}，*〉*运算表由下表定义：则指出每个元素的逆元?

*	a	b	c
a	a	a	b
b	a	b	c
c	a	c	c

解： a的右逆元为c，无左逆元，

b的逆元为b，

c无右逆元，左逆元为a 。

一般地，左、右逆元未必相等，左、右逆元未必存在，甚至不唯一。

逆元

定理5-2.4： 设代数系统<A,*>，*是定义在A上的二元运算，A中存在幺元e，且每个元素都有左逆元。如果*是可结合的，那么任何元素的左逆元必定也是该元素的右逆元，且**逆元唯一**。

证：设a，b，c，b是a的左逆元，c是b的左逆元，因为

(b*a) *b=e*b=b

则 e=c*b = c*((b*a)*b)=(c*(b*a))*b=((c*b)*a)*b =(e*a)*b

=a*b，即 b也是a的右逆元。

设a有两个逆元b和c，则b=b*e=b*(a*c)=(b*a)*c=e*c=c

则a的逆元惟一。

从运算表中看二元运算的性质

1）运算 * 具有封闭性，当且仅当运算表中的每个元素都属于A。

2）运算 * 具有可交换性，当且仅当运算表关于主对角线是对称的。

3）运算 * 具有等幂性，当且仅当运算表的主对角线上的每一个元素与它所在的行（列）的表头元素相同。

4）A关于运算 * 有零元，当且仅当该元素所对应的行和列中的元素都与该元素相同。

5）A关于运算 * 有幺元，当且仅当该元素所对应的行和列依次与运算表的行和列相一致。

6）设A中有幺元，a和b互逆，当且仅当位于a所在行，b所在列的元素以及b所在行，a所在列的元素都是幺元。

5.3 半群

半群是一种特殊的代数系统，在计算机形式语言，自动机理论，编码理论等得到广泛应用。

广群和半群

定义5-3.1： 具有运算**封闭性**的代数系统〈S，*〉称为**广群**。

定义5-3.2： 满足**封闭性**、**结合律**的代数系统〈S，*〉，称为**半群**，即$\forall x, y, z \in S$满足

$$(x*y)*z=x*(y*z),$$

这里*是二元运算。

例1. a) 〈N，+〉 〈N，x〉是半群，

〈I_+，-〉 和 〈R，/〉？ 不是半群

b) 设s={a，b}，*定义如右表。

*	a	b
a	a	b
b	a	b

问：是半群吗？

∵∀x,y,z∈s

① x*y∈s ∴运算封闭

② x*（y*z）=x*z=z

（x*y）*z=z

∴结合律成立， ∴〈s，*〉是半群。

子半群

定理5-3.1 设〈S，*〉是半群，$B \subseteq S$且*在B上是封闭的，那么〈B，*〉也是一个半群。通常称〈B，*〉是半群〈S，*〉的**子半群**。

证明：

因为*在S上是可结合的，而$B \subseteq S$且*在B上是封闭的，所以*在B上也是可结合的，故〈B，*〉也是一个半群。 #

该定理提供了一种构造半群的方法。

等幂元

定理5-3.2　有限半群<S,*>,则必∃a∈s，有a*a=a。（这样的a叫等幂元）

证明：　∀b∈s，因为运算封闭，$b^2=b*b\in s$　b^3，b^4，…∈s

∵ s有限 ∴∃ i，$j(j>i)$ 有$b^i=b^j$。

∴ $b^i=b^j=b^{j-i}*b^i$。

∴令$p=j-i$ 当$q\geqslant i$,$b^q=b^p\cdot b^q$　（1）

又∵$p\geqslant 1$ ∴∃k 有$kp\geqslant i$，

由（1）$b^{kp}=b^p*b^{kp}=b^p*(b^p*b^{kp})=\ldots=b^{kp}*b^{kp}$,

∴令$a=b^{kp}\in s$ 则a*a=a ∴ b^{kp}是等幂元。#

逆元

定理5-2.4： 设代数系统<A,*>，*是定义在A上的二元运算，A中存在幺元e，且每个元素都有左逆元。如果*是可结合的，那么任何元素的左逆元必定也是该元素的右逆元，且**逆元唯一**。

证：设a，b，c，b是a的左逆元，c是b的左逆元，因为

(b*a) *b=e*b=b

则 e=c*b = c*((b*a)*b)=(c*(b*a))*b=((c*b)*a)*b =(e*a)*b

=a*b，即 b也是a的右逆元。

设a有两个逆元b和c，则b=b*e=b*(a*c)=(b*a)*c=e*c=c

则a的逆元惟一。

独异点

定义5-3.3：　含有幺元的半群称为独异点（也称含幺半群）。

例

<R,+><N, x >　都是独异点

<N-{0},+>　是半群，不是独异点，没有幺元

定理5-3.3 独异点<S,*>，则*运算表中任何两行或两列均不相同。

证明：设独异点的幺元为e，∀a，b∈s，a≠b

∵a*e≠b*e

∴<s，*>运算表中a，b两行不同。

由a，b任意性，运算表中任两行不同。

∵ e*a≠e*b

∴<s，*>运算表中a，b二列不同。

由a，b任意性，运算表中任两列不同。#

定理5-3.4 独异点$\langle S, * \rangle$，若$\forall a, b \in S$，a，b均有逆元，则 a) $(a^{-1})^{-1}=a$;

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

证明：a) ∵$a*a^{-1}=e$ ∴a是a^{-1}的左逆元

$a^{-1}*a=e$ ∴a是a^{-1}的右逆元

∴$(a^{-1})^{-1}=a$

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

∴$b^{-1}*a^{-1}$是a*b的右逆元

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

∴$b^{-1}*a^{-1}$是a*b的左逆元 ∴$(a*b)^{-1}=b^{-1}*a^{-1}$。 #

5.4 群与子群

群论是抽象代数发展充分的一个分支，广泛应用于计算,通讯，计算机科学，是本章的重点。

群（Group）

定义5-4.1： 代数系统〈G，*〉，如果二元运算*满足：

1) 封闭性，即$\forall a,b,\in G$，$a*b \in G$。

2) 结合律，即$\forall a,b,c\in G$，$a*(b*c)=(a*b)*c$。

3) 存在幺元e，即$\forall a\in G$，$e*a=a*e=a$。

4) G中每个元素存在逆元，$\forall a\in G$，$\exists a^{-1}\in G$,使$a*a^{-1}=a^{-1}*a=e$。

则称〈G，*〉为群（Group）。

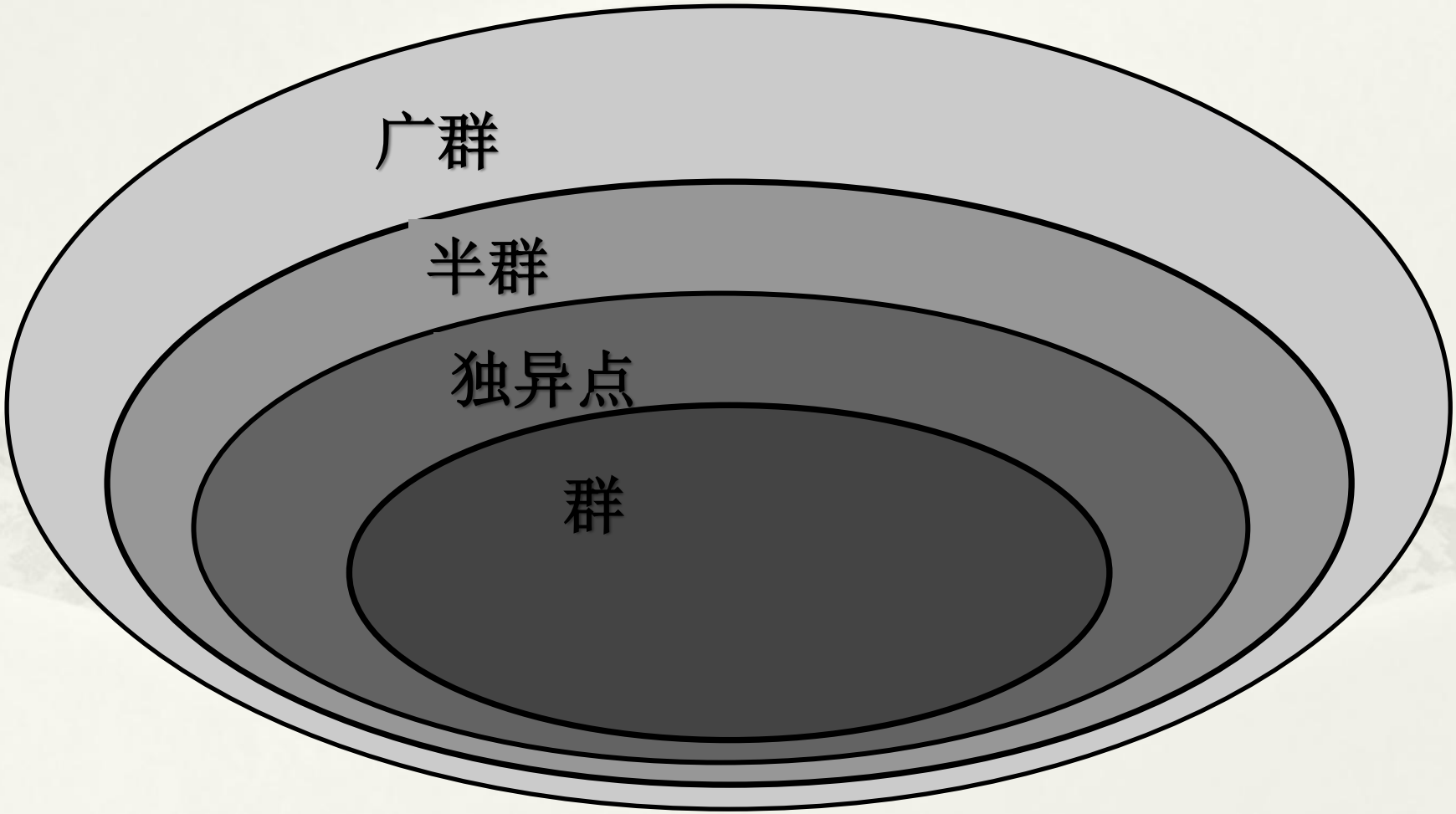
例： <R-{0}, x >是一个群。

阶数

定义5-4.2： 设〈G，*〉为群，若G是有限集，称〈G，*〉为**有限群**，|G|称为群的**阶数**，若G是无限集，称〈G，*〉为**无限群**。

例： <R-{0}, x >是一个无限群。

概念 汇总



群的性质

有关半群和独异点的性质在群中全部成立，

例如，$(a*b)^{-1}=b^{-1}*a^{-1}$

幺元和零元

定理5-2.2：设*是定义在集合A上的二元运算，且在A中有关于*运算的左零元θ_l，右零元θ_r，$\theta_l=\theta_r=\theta$，且零元唯一。

（证明与定理5-2.1类似）

定理5-2.2：设〈A，*〉是一个代数系统，且集合A中元素的个数大于1。如果该代数系统中存在幺元e和零元θ，则$\theta \neq e$。

证明：（反证法）设$\theta=e$，那么对于任意的$\forall x \in A$，必有

$x=e*x=\theta*x=\theta=e$，于是A中的所有元素都是相同的，这与A中含有多个元素相矛盾。

#

定理5-4.1 群中不可能有零元。

证：当 $|G|=1$，它的唯一元素视为么元。

当 $|G|>1$ 且 $\langle G, * \rangle$ 有零元 θ，则 $\forall x \in G$，都有 $x*\theta=\theta*x=\theta \neq e$。

$\therefore \theta$ 无逆元，这与G是群矛盾。 #

定理5-4.2： 若〈G，*〉是一个群，则∀a，b∈G

a）存在唯一的x，使得a*x=b，

b）存在唯一的y，使得y*a=b。

证：a）存在性：

令$x=a^{-1}*b$，则$a*(a^{-1}*b)=a*a^{-1}*b=e*b=b$。

唯一性：

若$a*x'=b$，则$a^{-1}*a*x'=a^{-1}*b$，$\therefore x'=a^{-1}*b=x$。

b）略

定理5-4.3　若〈G，*〉是一个群，

则∀a，b，c∈G，有

(a) a*b=a*c　⇒ b=c

(b) b*a= c *a　⇒ b=c

证：∵ a*b=a*c

⇒ a^{-1}*（a*b）=a^{-1}*（a*c）

⇒ b=c　#

（群满足消去律）

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**。

例如，S={a,b,c,d}，一个置换为

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

定理5-4.4：群〈G，*〉的运算表中的每一行或每一列是G中元素的一个置换。

证：① 先证运算表中每一行(列)中的元素不能出现二次(单射)。

∵若$a*b_1=a*b_2=k$，且$b_1\neq b_2$，与可约性矛盾。

② 再证G中任一元素在任一行（列）中均出现（满射）。

∵考察对应于a的那一行，$\forall b\in G$，则$b=a*(a^{-1}*b)$，

∴b出现在a那一行，由 a， b 任意性得证.

③因〈G，*〉中有么元，

∴任二行（列）均不相同（即各个置换均不相同）。

例

① 一阶群仅有1个

*	e
e	e

② 二阶群仅有1个

*	e	a
e	e	a
a	a	e

③ 三阶群仅有1个

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

④ 四阶群仅有2个

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

* ⑤ 五阶群仅有1个

*	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

* ⑥ 六阶群仅有2个

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	b	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

定理5-4.5：么元是群中唯一的等幂元。

证：若x是等幂元素，

则：$x=e*x=(x^{-1}*x)*x=x^{-1}*(x*x)$

$=x^{-1}*x=e$ #

从运算表中看二元运算的性质

1）运算 * 具有封闭性，当且仅当运算表中的每个元素都属于A。

2）运算 * 具有可交换性，当且仅当运算表关于主对角线是对称的。

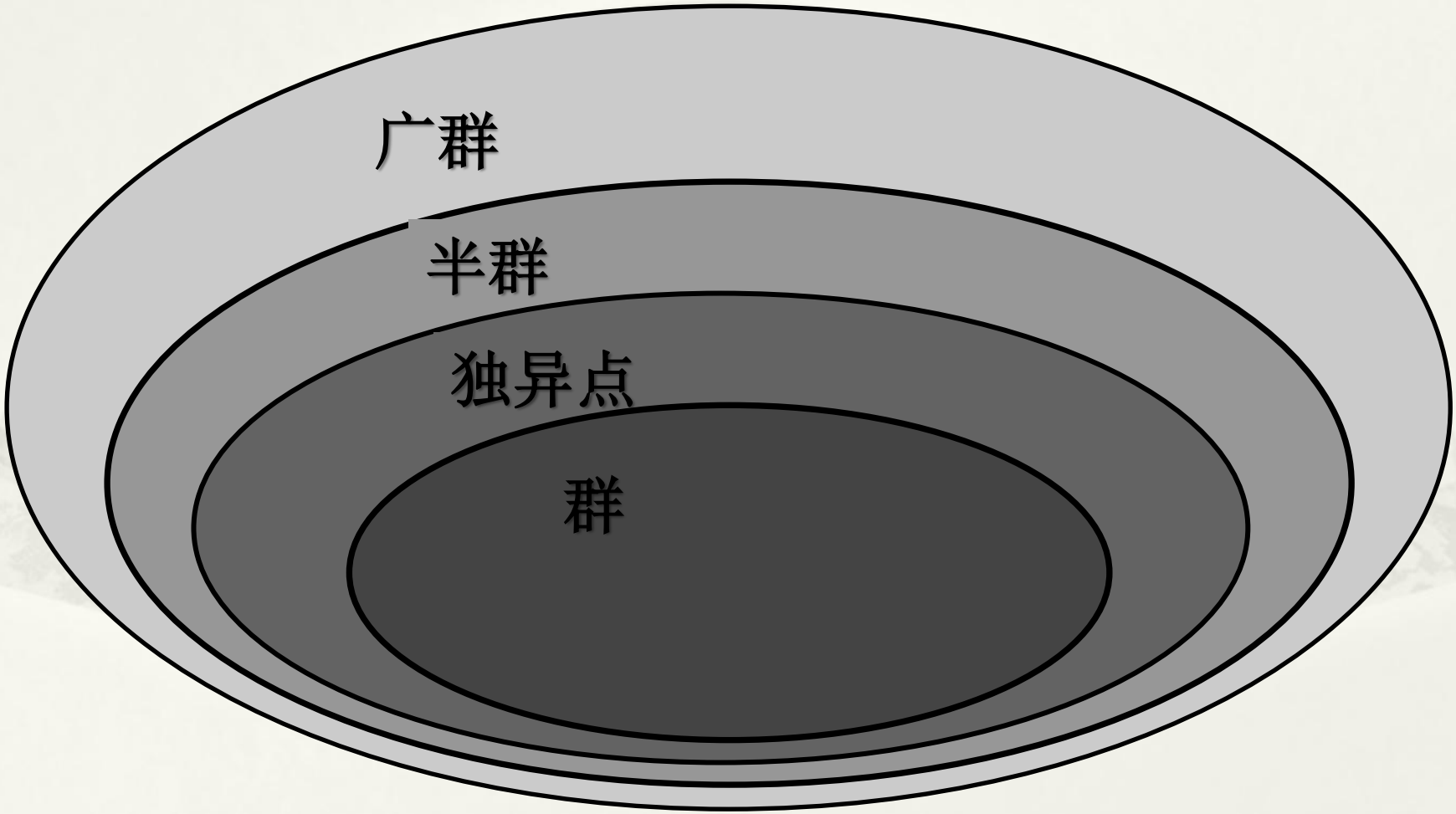
3）运算 * 具有等幂性，当且仅当运算表的主对角线上的每一个元素与它所在的行（列）的表头元素相同。

4）A关于运算 * 有零元，当且仅当该元素所对应的行和列中的元素都与该元素相同。

5）A关于运算 * 有幺元，当且仅当该元素所对应的行和列依次与运算表的行和列相一致。

6）设A中有幺元，a和b互逆，当且仅当位于a所在行，b所在列的元素以及b所在行，a所在列的元素都是幺元。

概念 汇总



回顾

* 定理5-4.1 群中不可能有零元。
* 方程解唯一性
* 消去律
* 置换
* 定理5-4.5：么元是群中唯一的等幂元。

子群

定义5-4.5 设<G,*>为群，S⊆G，若<S,*>也构成群，则称(S,*)为(G,*)的**子群**(Subgroup)。

定义5-4.6 如果S = {e}或者S = G，则称<S，*>是<G，*>的**平凡子群**。

定理5－4.6 设<G，*>是一个群，<S，*>是<G，*>的一个子群，那么<G，*>的幺元e必定也是<S，*>的幺元。

证：设＜G，＊＞的幺元为e’，则对于任意S中的元素x，都有x＊e’＝e’＊x＝x，则e’＝e。 #

子群的判定方法 1

* **定理 5 – 4.7：** $<G,*>$是群，$B \subseteq G$且非空，如果B有限且*运算在B上封闭，那么$<B,*>$必定是$<G,*>$的子群。

任取$a \in B$ 若$a=e$，则$a^{-1}=e^{-1}=e \in B$

若$a \neq e$,令 $S=\{a,a^2,...\}$，因为运算*封闭，所以$S \subseteq B$

由于B是有穷集，必有$a^i=a^j$ $(i<j)$，即$a^i=a^i*a^{j-i}$。

根据G中的消去律得： $a^{j-i}=e$（B中存在幺元）

由$a \neq e$可知，$j-i \neq 0$，$j-i \geq 1$，

$j-i>1$时，由$a^{j-i-1}*a=e$ 和 $a*a^{j-i-1}=e$可知a^{j-i-1}为a的逆元；

$j-i=1$时，由$a^i=a^i*a^{j-i}$可知a即为幺元，幺元以自身为逆元；

从而证明了 $a^{-1}=a^{j-i-1} \in B$ （B中每个元素存在逆元）。

学生解题

例1.

a) $<\{3n|n\in I\},+>$是$<I,+>$的子群，

其中I为整数集。

子群的判定方法2

定理5-4.8： $<G,*>$是群，$S \subseteq G$且非空，若$\forall a,b \in S$，有$a*b^{-1} \in S$，则$<S,*>$是$<G,*>$的子群。

证明：首先证明G中的幺元也是S中的幺元

1）$\forall a$，$a \in S$，有$a*a^{-1}=e \in S$。

其次证明，S中的每一元素都有逆元

2）$\forall a \in S$，由于$e \in S$，则有$e*a^{-1}=a^{-1} \in S$。

最后证明封闭性

3）$\forall a,b \in S$，由2）可知$b^{-1} \in S$，

又因为$b=(b^{-1})^{-1}$，所以$a*(b^{-1})^{-1}= a*b \in S$。

故$<S,*>$是$<G,*>$的子群。 #

例2. 若$<H,*>$，$<K,*>$是群$<G,*>$的子群，则$<H\cap K,*>$是$<G,*>$的子群。

证明：

设$\forall a,b\in H\cap K$，则$a,b\in H,a,b\in K$，

又因为$<H,*>$，$<K,*>$是群$<G,*>$的子群。

所以，$b^{-1}\in H\cap K$。

根据封闭性，$\therefore a*b^{-1}\in H$，$a*b^{-1}\in K$。即$a*b^{-1}\in H\cap K$。

由子群判别法2知：$<H\cap K,*>$是$<G,*>$的子群。

5.5 阿贝尔群与循环群

定义5-5.1： 设〈G，*〉为群，若*满足交换律，称〈G，*〉为阿贝尔群(或可交换群)。

例1、 $\langle I, + \rangle$ 是一个群，且为阿贝尔群，

证： ① $\langle I, + \rangle$ 运算封闭。

② 普通加法满足结合律。

③ 0为么元。

④ $\forall a \in I$，$-a$是a的逆元。

⑤普通加法满足交换律。

例 2 $\langle Q_+, \times \rangle$ 是阿贝尔群

定理5-5.1　设〈G，x〉是一个群，则〈G，*〉是阿贝尔群的充要条件是:∀a，b∈G，有（a*b）*（a*b）=（a*a）*（b*b）。

证：充分性：若∀a，b∈G,有(a*b)*(a*b)=(a*a)*(b*b)。

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

∴ b*a=a*b，∴〈G，*〉是阿贝尔群。

必要性：若〈G，*〉是阿贝尔群，则∀a，b∈G，a*b=b*a。

∴a*（a*b）*b=a*（b*a）*b,

∴（a*a）*（b*b）=（a*b）*（a*b）。 #

循环群

定义5-5.2 设<G,*>是一个群，若在G中存在元素a，使得G中任意元素都由a的幂组成，则称<G,*>是一个**循环群**，元素a称为循环群<G,*>的**生成元**。

例，群{<0°,60°,120°,180°,240°,360° >，★}

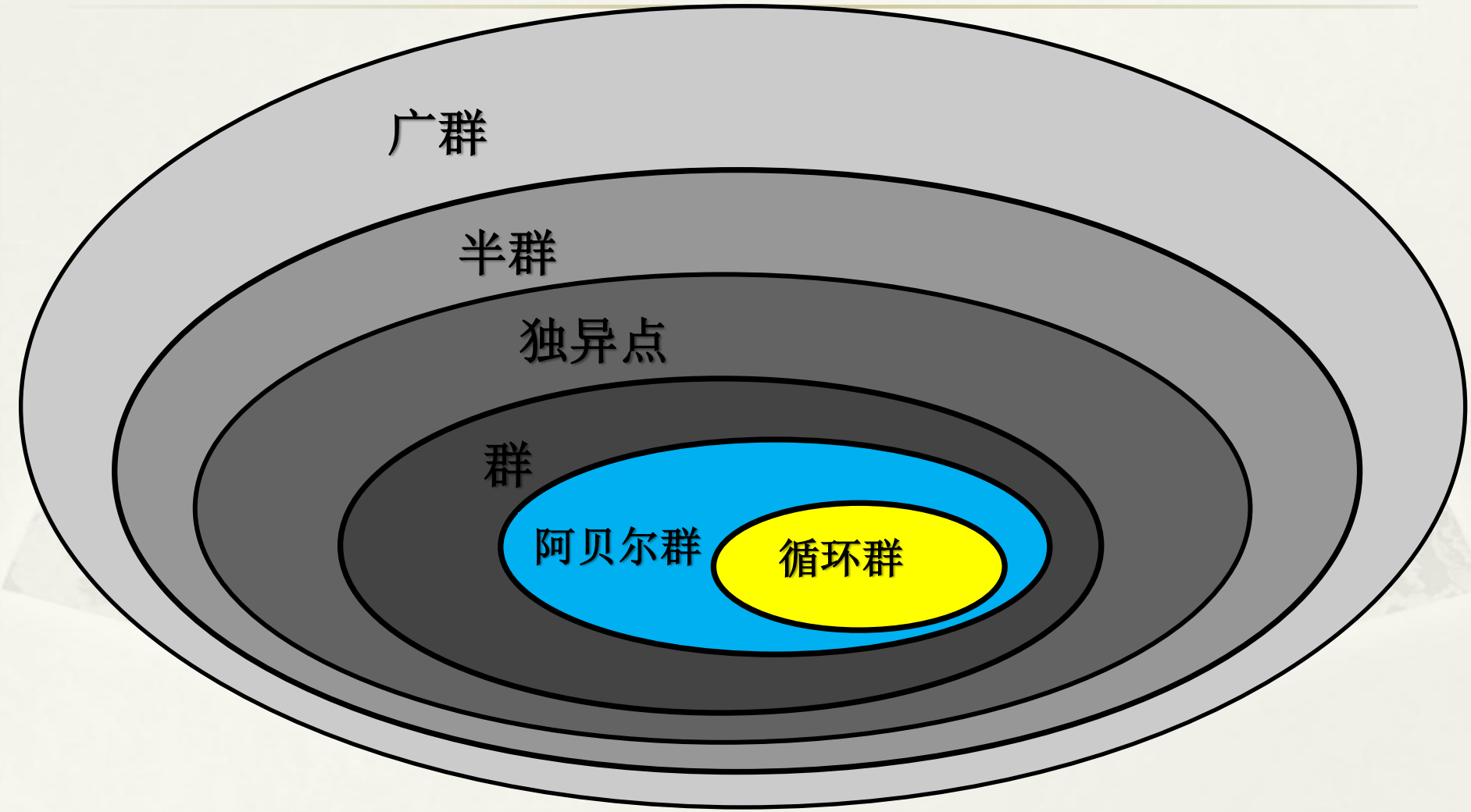
其中，★是两个角度连续旋转，即mod 360加，

该群是一个循环群，其生成元是60°。

学生解题

定理5-5.2 任何循环群必定是阿贝尔群。

概念 汇总



元素的阶

- 定义： 设a是G中的一个元素，若$\exists k \in I^+$，使得$a^k=e$，则**使得$a^k=e$的最小正整数k称为元素a的阶**（或称“a的周期”），记为O(a)，并称a是有限阶的元素。

定理5-5.3： 设$<G,*>$是由a生成的有限循环群，若G的阶为n，即$|G|=n$，则$G=\{a^1, a^2, \ldots, a^n = e\}$。其中$e$是幺元，$n$是$a^n = e$最小正整数。

证： a) 证a的阶为n。先证：若$m<n$，则$a^m \neq e$。

（反证法） 若$m<n$，且$a^m=e$，$\forall a^k \in G$，$k=mq+r$，$0 \leqslant r<m$，

$\therefore a^k = a^{mq+r} = a^{mq} \cdot a^r = (a^m)^q \cdot a^r = (e)^q \cdot a^r = a^r$，

$\therefore$G中最多有m个不同元素，这与$|G|=n$矛盾，所以a阶为n。

b)证G中的元素全不相同。

若$a^i = a^j (1 \leqslant i<j \leqslant n)$，$a^{j-i}=e$。

$\because 0 \leqslant j-i<n$ $\therefore$这与a)矛盾。

c) $\because a^i \in G$且$|G|=n (1 \leqslant i \leqslant n)$，$\therefore G=\{a^1, \ldots, a^n\}$，

$\because <G,*>$是一个群，故必有幺元，$\therefore a^n=e$

$G=\{a^1, a^2, \ldots, a^n\}$。

例1. a)<I,+>是无限循环群,其中-1,1均是生成元。

(生成元不唯一)

b)<{5j|j∈I},+>是无限循环群,其中-5,5均是生成元。

例2. 设$G=\{\alpha,\beta,\gamma,\delta\}$，$G$上二元运算$*$如下右表所示。 证明$<G,*>$是循环群。

证：$\because \gamma^2=\beta,\ \gamma^3=\delta,\ \gamma^4=\alpha$ $\therefore$运算表可改写如下：

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

$*$	γ^4	γ^2	γ	γ^3
γ^4	γ^4	γ^2	γ	γ^3
γ^2	γ^2	γ^4	γ^3	γ
γ	γ	γ^3	γ^2	γ^4
γ^3	γ^3	γ	γ^4	γ^2

$*$	γ^4	γ	γ^2	γ^3
γ^4	γ^4	γ	γ^2	γ^3
γ	γ	γ^2	γ^3	γ^4
γ^2	γ^2	γ^3	γ^4	γ
γ^3	γ^3	γ^4	γ	γ^2

由上表看出$<G,*>$是一个循环群.

学生解题

例1.

a) $\langle\{3n \mid n \in I\}, +\rangle$是$\langle I, +\rangle$的子群，

其中I为整数集。

答案：p.194 例题3

学生解题

定理5-5.2　任何循环群必定是阿贝尔群。

证：设g是<G,*>的生成元，

则$\forall a,b\in G$, $a=g^r$, $b=g^s(r,s\in I)$,

$a*b=g^r*g^s=g^{r+s}=g^{s+r}=g^s*g^r=b*a$。　#