Chapter 4

Algebra System

2015-12-29

本章概括

- 代数系统一般概念的引入
- 运算的概念
- 运算的性质
- 代数系统的形式定义
- 代数系统的特殊元素
- 同态与同构

§4.1 代数系统的引入 (1)

一个代数系统需要满足下面三个条件：

（1）有一个非空集合 S；

（2）有一些建立在 S 上的运算；

（3）这些运算在集合 S 上是封闭的。

§4.2 运算

4.2.1 运算的概念

定义

假设 A 是一个集合，A×A 到 A 的映射称为 A 上的二元运算。

一般地，A^n 到 A 的映射称为 A 上的 n 元运算。

§4.2 运算 (2)

4.2.1 运算的概念

$\circ$	a_1	a_2	…	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	…	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	…	$a_2 \circ a_n$
.		. . .		
.		. . .		
.		. . .		
a_n	$a_n \circ a_1$	$a_n \circ a_2$	…	$a_n \circ a_n$

	$\circ a_i$
a_1	$\circ a_1$
a_2	$\circ a_2$
.	.
.	.
.	.
a_n	$\circ a_n$

§4.2 运算 (3)

4.2.2 运算的性质

假设 $*, +$ 都是集合 A 上的运算

（1）封闭性

如果 $S \subseteq A$，对任意的 $a, b \in S$，有 $a*b \in S$，则称 S 对运算 * 是封闭的。

4.2.2 运算的性质

（2）交换律

如果对任意的 $a, b \in A$，都有 $a*b=b*a$，则称运算 * 是可交换的。

（3）结合律

如果对任意的 $a, b, c \in A$，都有 $(a*b)*c=a*(b*c)$，则称运算 * 是可结合的。

§4.2 运算

（4）分配律

如果对任意的 $a, b, c \in A$，都有 $a*(b+c)=(a*b)+(a*c)$

则称 * 对 + 运算满足左分配;

如果对任意的 $a, b, c \in A$，都有 $(b+c)*a=(b*a)+(c*a)$

则称 * 对 + 运算满足右分配。

如果运算 * 对 + 既满足左分配又满足右分配，

则称运算 * 对 + 满足分配律。

§4.2 运算

（5）消去律

如果对任意的 $a,b,c\in A$，当 $a*b=a*c$，必有 $b=c$，则称运算 $*$ 满足左消去律；

如果对任意的 $a,b,c\in A$，当 $b*a=c*a$，必有 $b=c$，则称运算 $*$ 满足右消去律；

如果运算 $*$ 既满足左消去律又满足右消去律，则称运算 $*$ 满足消去律。

（6）吸收律

如果对任意的 $a, b \in A$，都有 $a*(a+b)=a$，则称运算 * 关于运算 + 满足吸收律。

（7）等幂律

如果对任意的 $a \in A$，都有 $a*a=a$，则称运算 * 满足等幂律。

§4.2 运算

Δ	a	b	c
a	a	b	c
b	b	b	a
c	c	a	c

§4.3 代数系统 (1)

4.3.1 代数系统的概念

定义

假设 A 是一个非空集合，$f_1, f_2, \ldots, f_n$ 是 A 上的运算（运算的元数可以是不相同的），则称 A 在运算 $f_1, f_2, \ldots, f_n$ 下构成一个代数系统，记为：$<A, f_1, f_2, \ldots, f_n>$

§4.3 代数系统 (2)

4.3.1 代数系统的概念

定义

假设 $<A, *>$ 是一个代数系统，$S \subseteq A$，如果 S 对 * 是封闭的，则称 $<S, *>$ 为 $<A, *>$的子代数系统。

§4.3 代数系统 (3)

4.3.2 代数系统中的特殊元素

（1）单位元（幺元）

假设 $<A, *>$ 是一个代数系统，如果 $\exists e_L \in A$，对于任意元素 $x \in A$，都有 $e_L * x = x$，则称 e_L 为 A 中关于运算 * 的左单位元;

如果 $\exists e_r \in A$,对于任意元素 $x \in A$，都有 $x * e_r = x$，则称 e_r 为 A 中关于运算 * 的右单位元;

如果 A 中一个元素 e 既是左单位元又是右单位元，则称 e 为 A 中关于运算 * 的单位元。

§4.3 代数系统 (4)

A={a,b,c}

Δ	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

◊	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

•	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

<A,Δ>有左单位元：a,b,c

<A,◊>有右单位元：a,b,c

<A,•>有单位元：a

§4.3 代数系统 (5)

4.3.2 代数系统中的特殊元素

（1）单位元（幺元）

定理

假设 $<A, *>$ 是代数系统，并且 A 关于运算 * 有左单位元 e_L 和右单位元 e_r，则 $e_L = e_r = e$ 并且单位元唯一。

4.3.2 代数系统中的特殊元素

（2）零元

假设 $<A, *>$ 是一个代数系统，如果 $\exists\theta_L \in A$,对于任意元素 $x \in A$，都有 $\theta_L * x = \theta_L$，则称 θ_L为 A 中关于运算 * 的左零元;

如果 $\exists\theta_r \in A$，对于任意元素 $x \in A$，都有 $x * \theta_r = \theta_r$,则称 θ_r 为 A 中关于运算 * 的右零元;

如果 A 中一个元素 θ 既是左零元又是右零元，则称 θ 为 A 中关于运算 * 的零元。

§4.3 代数系统 (7)

A={a,b,c}

Δ	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

◊	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

•	a	b	c
a	a	b	c
b	b	b	b
c	c	b	b

<A,Δ>有右零元：a,b,c

<A,◊>有左零元：a,b,c

<A,•>有零元：b

4.3.2 代数系统中的特殊元素

（2）零元

定理

假设 <A, *> 是代数系统，并且 A 关于运算 * 有左零元 θ_L 和右零元 θ_r，则 $\theta_L=\theta_r=\theta$ 并且零元唯一。

4.3.2 代数系统中的特殊元素

（3）逆元

假设 <A, *> 是一个代数系统，e 是 <A, *>的单位元。对于元素 a∈A，如果存在 b∈A，使得 b*a=e，则称 a 为左可逆的，b 为 a 的左逆元；如果存在 c∈A，使得 a*c=e，则称元素 a 是右可逆的，c 为 a 的右逆元。如果存在 a' ∈A，使得 a'*a=a*a'=e，则称 a 是可逆的，a' 为 a 的逆元。a 的逆元记为：a^{-1}。

§4.3 代数系统

A={a,b,c}

•	a	b	c
a	a	b	c
b	b	c	c
c	c	a	b

•	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

4.3.2 代数系统中的特殊元素

（3）逆元

定理

设 <A, *> 是一个代数系统，且 A 中存在单位元 e，每个元素都存在左逆元。如果运算 * 是可结合的，那么，任何一个元素的左逆元也一定是该元素的右逆元，且每个元素的逆元唯一。

4.3.2 代数系统中的特殊元素

（4）幂等元

定义：

在代数系统<A, *>中，如果元素 a 满足 a*a=a，那么称 a 是 A 中的幂等元。

§4.3 代数系统

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

运算 1

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

运算 2

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

运算 3

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

运算 4

§4.4 同态与同构 (1)

4.4.1 基本概念

定义

设 $<A,*>$ 和 $<B,\circ>$ 是代数系统，$f:A\to B$，如果 f 保持运算，即对 $\forall x,y\in A$，有 $f(x*y)=f(x)\circ f(y)$。称 f 为代数系统 $<A,*>$ 到 $<B,\circ>$ 的同态映射，简称同态。也称为两代数系统同态。

§4.4 同态与同构 (2)

4.4.1 基本概念

定义

设 $<A,*>$ 和 $<B,\circ>$ 是代数系统，f 是 A 到 B 的同态。如果 f 是单射的，称 f 为单同态；如果 f 是满射的，称 f 为满同态；如果 f 是双射的，称 f 为同构映射，简称为同构。

§4.4 同态与同构 (3)

4.4.1 基本概念

定义

设 $<A,*>$ 是代数系统，若存在函数 $f:A\to A$，并且对 $\forall x,y\in A$,有 $f(x*y)=f(x)*f(y)$。称 f 为$<A,*>$ 的自同态；如果 f 是双射的，则称 f 为 $<A,*>$ 的自同构。

§4.4 同态与同构 (4)

4.4.2 同态、同构的性质

（1）如果两函数是同态、同构的，则复合函数也是同态、同构的。

定理

假设 f 是<A,*> 到 <B,°>的同态，g是<B,°>到<C,Δ> 的同态，则gof是<A,*> 到<C,Δ>的同态；如果 f 和 g 是单同态、满同态、同构时，则gof也是单同态、满同态和同构。

§4.4 同态与同构 (5)

4.4.2 同态、同构的性质

（2）满同态保持结合律

定理

假设 f 是<A,*> 到 <B,°>的满同态。如果 * 运算满足结合律，则 ° 运算也满足结合律，即满同态保持结合律。

（3）满同态保持交换律

4.4.2 同态、同构的性质

（4）满同态保持单位元

定理

假设 f 是<A,*> 到 <B,°>的满同态。e 是<A,*> 的单位元，则 f(e) 是<B,°>的单位元。

4.4.2 同态、同构的性质

（5）满同态保持逆元

定理

假设 f 是<A,*>到<B,°>的满同态。e_A 和 e_B 分别是<A,*>和<B,°>的单位元，如果 A 中元素 x 和 x' 互逆，则 B 中元素 f(x) 和 f(x')也互逆。

4.4.2 同态、同构的性质

（6）满同态保持零元

定理

假设 f 是<A,*> 到 <B,°>的满同态。θ是<A,*> 的零元，则 f(θ) 是<B,°>的零元。

4.4.2 同态、同构的性质

（7）满同态保持幂等元

定理

假设 f 是<A,*>到<B,°>的满同态。并且 x∈A是<A,*>的幂等元，则 f(x)∈B 是<B,°>的幂等元。

4.4.2 同态、同构的性质

（8）同构映射运算性质双向保持

定理

假设 f 是<A,*> 到 <B,°>的同构映射。则 f^{-1}是<B,°> 到 <A,*> 的同构映射。

§4.5 同余关系与商代数 (1)

4.5.1 同余关系

定义

假设 $<A,*>$ 是一个代数系统，E 是 A 上的等价关系。如果对 $\forall x_1,x_2,y_1,y_2 \in A$，当 $x_1 E x_2, y_1 E y_2$ 时，必有 $(x_1 * y_1) E (x_2 * y_2)$，则称 E 是 A 上的同余关系。

§4.5 同余关系与商代数 (2)

4.5.2 商代数 <A/E,°>

4.5.3 自然同态

定理：

假设 <A,*> 是一代数系统，E 是 A 上的同余关系，而 <A/E,°> 是 A 关于 E 的商代数系统。建立映射 g:A→A/E，定义为：对∀x∈A，有 g(x)=[x]，则 g 是 <A,*> 到 <A/E,°> 的满同态映射。

§4.5 同余关系与商代数 (3)

4.5.4 特殊的同余关系

假设两个代数系统 $<A,*>$ 与 $<B,\Delta>$ 同态，它们之间一定存在映射 $f:A\to B$。利用该映射在A 上建立一种关系 E_f，定义为：对

$\forall x,y\in A$，$E_f=\{<x,y>\mid f(x)=f(y)\}$，

即 $\forall x,y\in A$，如果 $f(x)=f(y)$，就有 $x\ E_f\ y$。

§4.5 同余关系与商代数 (4)

4.5.4 特殊的同余关系

定理：

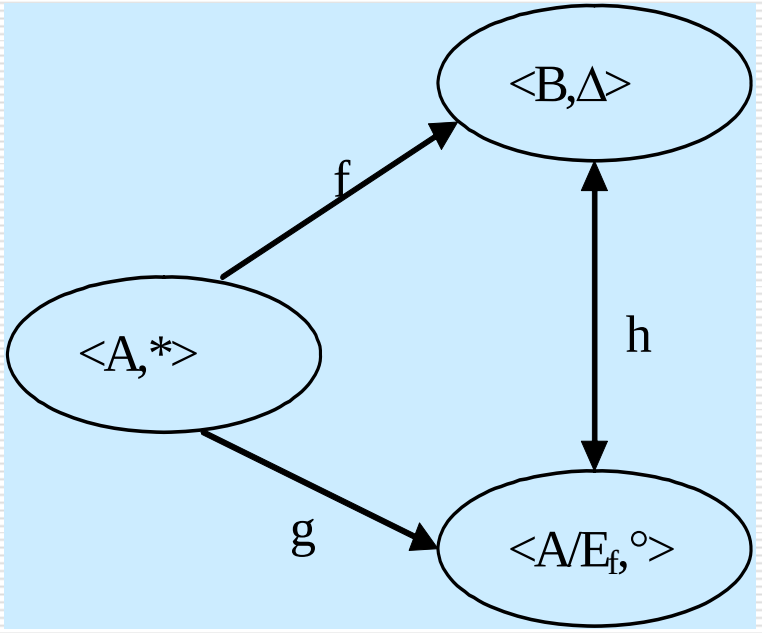
设 f 是代数系统 $<A,*>$ 到 $<B,\Delta>$ 的同态映射，则 A 上的关系 E_f 是一个同余关系。

§4.5 同余关系与商代数 (5)

4.5.5 同态基本定理

定理：

设 f 是 $<A,*>$ 到 $<B,\Delta>$ 满同态映射，E_f 是由 f 确定的 A 上的同余关系，A/E_f 为 A 关于 E_f 的商代数。则 $<A/E_f,\circ>$ 与 $<B,\Delta>$ 同构。



§4.6 直积

定义：

设 $<A,*>$ 和 $<B,\circ>$ 为两个代数系统，$<A\times B,\Delta>$ 称为两代数系统的直积。其中 $A\times B$ 是 A 和 B 的笛卡尔乘积，Δ 定义如下：对任意的 $<x,y>,<u,v>\in A\times B$，

$<x,y>\Delta<u,v>=<x*u,y\circ v>$。

§4.6 直积 (2)

定理：

假设 $<A,*>$ 和 $<B,\circ>$ 为两个代数系统，且分别有单位元 e_A,e_B，在两代数系统的直积$<A\times B,\Delta>$中存在子代数系统 S,T，使得

$<A,*> \cong <S,\Delta>$，$<B,\circ> \cong <T,\Delta>$。

Chapter 5

Group theory

2015-12-29

§5.1 半群

5.1.1 半群的定义

定义：

设 <S,*> 是一个代数系统，如果 * 运算满足结合律，则称 <S,*> 是一个半群。

§5.1 半群

例：假设S={a,b,c}，在S上定义运算Δ，如运算表给出。证明<S,Δ>是半群。

Δ	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

§5.1 半群

5.1.1 半群的定义

定义：

假设 <S,*> 是一个半群，a∈S，n 是正整数，则 a^n 表示 n 个 a 的计算结果，即 $a^n = a*a*...*a$。

对任意的正整数 m,n，

$a^m * a^n = a^{m+n}$，$(a^m)^n = a^{mn}$。

§5.1 半群

5.1.2 交换半群

定义：

如果半群 <S,*> 中的 * 运算满足交换律，则称 <S,*> 为交换半群。

在交换半群 <S,*> 中，若a,b∈S，n是任意正整数，则 $(a*b)^n = a^n * b^n$

5.1.3 独异点（含幺半群）

定义：

假设 <S,*> 是一个半群，如果 <S,*> 中有单位元，则称 <S,*> 是独异点，或含幺半群。

5.1.3 独异点（含幺半群）

定理：

假设 $<S,*>$ 是独异点，如果$a,b\in S$，并且 a,b 有逆元 a^{-1},b^{-1}存在，则：

（1）$(a^{-1})^{-1} = a$;

（2）$(a*b)^{-1} = b^{-1} * a^{-1}$。

5.1.4 子半群

定义：

假设 $<S,*>$ 是一个半群，若 $T \subseteq S$，且在 $*$ 运算下也构成半群，则称 $<T,*>$ 是 $<S,*>$ 的子半群。

§5.1 半群

假设A={a,b}，<P(A),∩>是一个含幺半群。

若B={a}

则P(B)⊆P(A)

并且<P(B),∩>构成半群，是<P(A),∩>的子半群。

∩	∅	{a}	{b}	{a,b}
∅	∅	∅	∅	∅
{a}	∅	{a}	∅	{a}
{b}	∅	∅	{b}	{b}
{a,b}	∅	{a}	{b}	{a,b}

5.1.4 子半群

定义：

设 <S,*> 是含幺半群，若 <T,*> 是它的子半群，并且 <S,*> 的单位元 e 也是 <T,*>单位元，则称 <T,*> 是 <S,*> 的子含幺半群。

§5.1 半群

例：设<S,*>是可交换的含幺半群，T={a|a∈S，且a*a=a}，则<T,*>是<S,*>的子含幺半群。

§5.1 半群

例：设<A,*>是一半群，对任意的a,b∈A，如果有 a≠b 必有 a*b ≠ b*a。

证明：

（1）对任意的a∈A，有a*a = a;

（2）对任意的a,b∈A，有a*b*a = a;

（3）对任意的a,b,c∈A，有a*b*c = a*c。

§5.2 群的概念及其性质 (1)

5.2.1 群的基本概念

定义：

设 <G,*> 是一代数系统，如果满足以下几点：

(1) 运算是可结合的;

(2) 存在单位元 e;

(3) 对任意元素 a 都存在逆元 a^{-1};

则称 <G,*> 是一个群。

§5.2 群的概念及其性质 (2)

例：假设R={0,60,120,180,240,300}表示平面几何上图形绕形心顺时针旋转的角度集合。*是定义在R上的运算。定义如下：对任意的a,b∈R，a*b表示图形顺时针旋转a角度，再顺时针旋转b角度得到的总旋转度数。并规定旋转360度等于原来的状态，即该运算是模360的。整个运算可以用运算表表示。

§5.2 群的概念及其性质 (3)

*	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

§5.2 群的概念及其性质 (4)

5.2.1 群的基本概念

一个群如果运算满足交换律，则称该群为交换群，或Abel群。

§5.2 群的概念及其性质 (5)

5.2.2 群的性质

(1) 任何阶大于 1 的群都没有零元。

(2) 设 <G,*> 是群，则 G 中消去律成立。

(3) 设 <G,*> 是群，单位元是 G 中的唯一等幂元。

5.2.2 群的性质

(4) 设<G,*>,<H,Δ>是群，f是 G 到 H 的同态，若 e 为<G,*>的单位元，则 f(e) 是<H,Δ> 的单位元，并且对任意 $a\in G$，有 $f(a^{-1})= f(a)^{-1}$。

(5) 设<G,*>是群，<H,Δ>是任意代数系统，若存在 G 到 H 的满同态映射，则<H,Δ>必是群。

§5.2 群的概念及其性质 (7)

5.2.3 半群与群

(1) 假设<G,*>是半群，并且

① <G,*>中有一左单位元 e，使得对任意的 $a \in G$，有 $e * a = a$;

② <G,*>中任意元素 a 都有“左逆元”a^{-1}，使得 $a^{-1} * a = e$。

则 <G,*> 是群。

5.2.3 半群与群

(2) 假设 <G,*> 是半群，对任意的 a,b∈G，方程 a*x = b，y*a = b 都在 G 中有解。则 <G,*> 是群。

(3) 有限半群，如果消去律成立，则必为群。

5.2.4 有限群的性质

定理：

设 <G,*> 是一个 n 阶有限群，它的运算表中的每一行（每一列）都是 G 中元素的一个全排列。

§5.2 群的概念及其性质

5.2.4 有限群的性质

*	e
e	e

*	e	a
e	e	a
a	a	e

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

§5.2 群的概念及其性质

5.2.4 有限群的性质

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

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

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

§5.2 群的概念及其性质 (12)

例：假设<G,*>是一个二阶群，则<G×G,*>是一个Klein群。

*	<e,e>	<e,a>	<a,e>	<a,a>
<e,e>	<e,e>	<e,a>	<a,e>	<a,a>
<e,a>	<e,a>	<e,e>	<a,a>	<a,e>
<a,e>	<a,e>	<a,a>	<e,e>	<e,a>
<a,a>	<a,a>	<a,e>	<e,a>	<e,e>

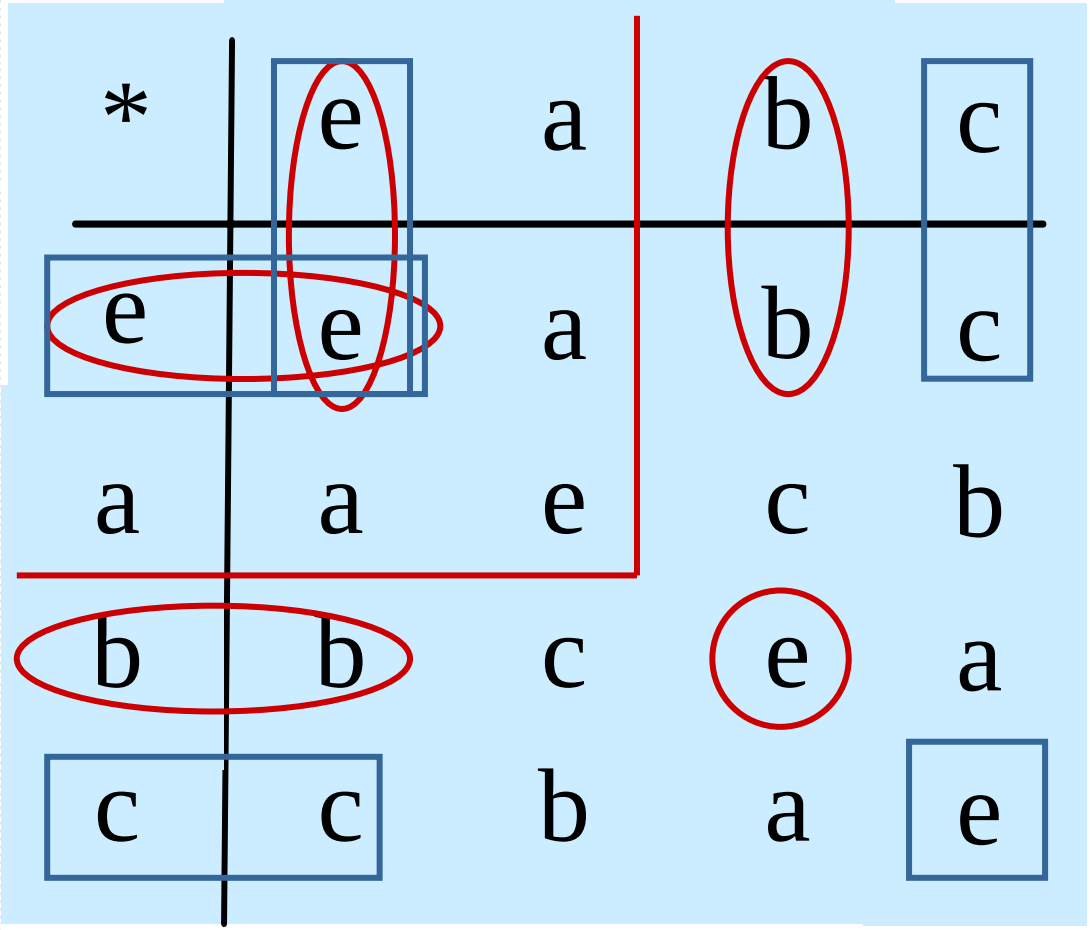
§5.3 子群与元素周期 (1)

5.3.1 子群

定义：

设 $<G,*>$ 是一个群，非空集合 $H \subseteq G$。如果 H 在 G 的运算下也构成群，则称 $<H,*>$ 是 $<G,*>$ 的子群。

§5.3 子群与元素周期



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

§5.3 子群与元素周期 (3)

5.3.1 子群

定理：

设 <H,*> 是 <G,*> 的子群，则

(1) <H,*> 的单位元 e_H 一定是 <G,*> 的单位元，即 $e_H = e_G$。

(2) 对 $a \in H$，a 在 H 中的逆元 a'，一定是 a 在 G 中的逆元。

§5.3 子群与元素周期 (4)

5.3.2 由子集构成子群的条件

(1) 设 H 是群 $<G,*>$ 中 G 的非空子集，则 H构成 $<G,*>$ 子群的充要条件是:

① 对 $\forall a,b\in H$，有 $a*b\in H$;

② 对 $\forall a\in H$，有$a^{-1}\in H$。

§5.3 子群与元素周期 (5)

5.3.2 由子集构成子群的条件

(2) 推论

假设 $<G,*>$ 是群，H 是 G 的非空子集，则 $<H,*>$ 是 $<G,*>$ 子群的充要条件是:

对 $\forall a,b \in H$，有 $a*b^{-1} \in H$。

§5.3 子群与元素周期

5.3.2 由子集构成子群的条件

(3) 假设 $<G,*>$ 是一个群，H 是 G 的非空有限子集，则 $<H,*>$ 是 $<G,*>$ 子群的充要条件是：

对 $\forall a,b\in H$，有 $a*b\in H$。

§5.3 子群与元素周期

5.3.3 元素的周期

（1）群中元素的幂运算

假设 $<G,*>$ 是一个群，$a \in G$。

则 $a^0 = e$； $a^{i+1} = a^i * a$;

$a^{-i} = (a^{-1})^i \quad (i \geq 0)$;

$a^m * a^n = a^{m+n}$;

$(a^m)^n = a^{mn}$（m,n为整数）。

§5.3 子群与元素周期

5.3.3 元素的周期

（2）元素的周期

定义：设<G,*>是一个群，a∈G。若存在正整数 n，使得$a^n = e$，则将满足该条件的最小正整数 n 称为元素 a 的周期或阶。若这样的 n 不存在，则称元素 a 的周期无限。元素 a 的周期记为：|a|。

§5.3 子群与元素周期

例3: $<Z_4, +_4>$是一个群，其中

$Z_4 = \{[0],[1],[2],[3]\}$，其运算表如右图。

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$[0]=[0]$ $|[0]|=1$

$[1]^4=[0]$ $|[1]|=4$

$[2]^2=[0]$ $|[2]|=2$

$[3]^4=[0]$ $|[3]|=4$

§5.3 子群与元素周期

5.3.3 元素的周期

（3）元素周期的性质

设<G,*>是一个群，a∈G。

① a 的周期等于 a 生成的循环子群(a)的阶。

即 |a| = |(a)|;

② 若 a 的周期为 n，则 $a^m = e$ 的充分必要条件是 n|m。

§5.3 子群与元素周期

5.3.3 元素的周期

（3）元素周期的性质

推论：

设 $<G,*>$ 是一个群，$a \in G$。若 a 的周期为 n，则

$(a)=\{a^0,a^1,\ldots,a^{n-1}\}$。

§5.4 循环群 (1)

5.4.1 定义

设 $<G,*>$ 是一个群，若在 G 中存在一个元素 a，使得 G 中任意元素都由 a 的幂组成，即 $G = (a) = \{a^i \mid i \in Z\}$，则称该群为循环群，元素 a 称为循环群的生成元。

§5.4 循环群 (2)

5.4.2 循环群的性质

（1）设 $\langle G, * \rangle$ 是一个循环群。

① 若 $\langle G, * \rangle$ 是 n 阶有限群，则 $\langle G, * \rangle \cong \langle Z_n, +_n \rangle$；

② 若 $\langle G, * \rangle$ 是无限群，则 $\langle G, * \rangle \cong \langle Z, + \rangle$。

§5.4 循环群 (3)

5.4.2 循环群的性质

（2）循环群的子群必为循环群

（3）设 $\langle G,*\rangle$ 是 n 阶循环群，m 是正整数，并且 $m|n$，则 G 中存在唯一一个 m 阶子群。

§5.4 循环群 (4)

5.4.2 循环群的性质

例如：$<Z_4, +_4>$是一个群，其中

$Z_4 = \{[0],[1],[2],[3]\}$，其运算表如右图。

[1]、[3] 是生成元。

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

§5.5 置换群 (1)

5.5.1 置换及其运算

（1）有限集 S 到其自身的双射称为 S 上的一个置换。当 |S| = n 时，S 上的置换称为 n 次置换。

例如：S={a, b, c, d} 并且f (a)=b, f (b)=c, f (c)=d, f (d)=a

$$f=\begin{pmatrix} a & b & c & d \\ f(a) & f(b) & f(c) & f(d) \end{pmatrix}=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$$

§5.5 置换群 (2)

5.5.1 置换及其运算

$$f_1=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} \qquad f_2=\begin{pmatrix} a & b & c & d \\ c & d & b & a \end{pmatrix}$$

$$f_1 \circ f_2=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ c & d & b & a \end{pmatrix}=\begin{pmatrix} a & b & c & d \\ d & a & c & b \end{pmatrix}$$

§5.5 置换群 (3)

5.5.1 置换及其运算

$$f_1=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} \qquad f_2=\begin{pmatrix} a & b & c & d \\ c & d & b & a \end{pmatrix}$$

$$f_1^{-1}=\begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix} \qquad f_2^{-1}=\begin{pmatrix} a & b & c & d \\ d & c & a & b \end{pmatrix}$$

§5.5 置换群 (4)

5.5.1 置换及其运算

（2）定义：设 S 上有如下置换

$$f=\begin{pmatrix} a_1 & a_2 & \dots & a_{i-1} & a_i & a_{i+1} & \dots & a_n \\ a_2 & a_3 & \dots & a_i & a_1 & a_{i+1} & \dots & a_n \end{pmatrix}$$

称该置换为循环置换，记为$(a_1,a_2,\dots,a_i)$，i为循环长度。当i=2 时称为对换。单位置换，即恒等映射也视为循环置换，记为（1）或（n）。

§5.5 置换群

5.5.1 置换及其运算

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (2,3);$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1,3,4)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1) = (4)$$

§5.5 置换群

5.5.2 置换群

（1）定义：

称 $<S_n,\circ>$ 为 n 次对称群，而 $<S_n,\circ>$ 的任意子群称为 n 次置换群。

5.5.2 置换群

例1：假设 S={1,2,3}，写出 S 的 3 次对称群和所有的 3 次置换群。

解：$S_3=\{f_1,f_2,f_3,f_4,f_5,f_6\}$，并且

$f_1=(1),f_2=(1,2),f_3=(1,3),f_4=(2,3),$

$f_5=(1,2,3),f_6=(1,3,2)$

$$f_1 = (1) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad f_2 = (1,2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$f_3 = (1,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad f_4 = (2,3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$f_5 = (1,2,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_6 = (1,3,2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

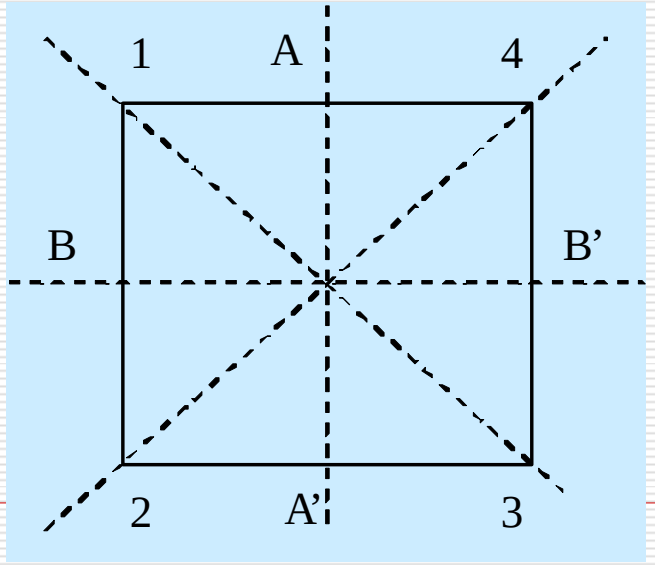
§5.5 置换群 (8)

5.5.2 置换群

（2）性质：

任意 n 阶群必同构于一个 n 次置换群。

例2：给定一个正四边形，如图所示。四个顶点的集合为 S={1,2,3,4}。



§5.6 陪集 (1)

5.6.1 左同余关系（左陪集关系）

定义：

设$<G,*>$是一个群，$<H,*>$是其子群。利用 H 在 G 上定义关系：

$$R_H=\{<a,b>|a,b\in G,b^{-1}*a\in H\}$$

$$R'_H=\{<a,b>|a,b\in G,a*b^{-1}\in H\}$$

则称 R_H 为 G 上的模 H 左同余关系（左陪集关系）；R'_H为 G 上的模 H 右同余关系（右陪集关系）。

§5.6 陪集 (2)

5.6.1 左同余关系（左陪集关系）

定理：

设 <H,*> 是 <G,*> 的一个子群，则 G 中模 H 左同余关系是等价关系。

§5.6 陪集 (3)

5.6.2 左陪集

定义：

设 $<H,*>$ 是 $<G,*>$ 的一个子群，则 $a\in G$ 为代表元的模 H 左同余关系的等价类 $[a]_{R_H}=\{a*h|h\in H\}$，称为 H 在 G 内由 a 确定的左陪集。简记为：$aH=[a]_{R_H}$。

§5.6 陪集 (4)

5.6.2 左陪集

定理：

设 $<H,*>$ 是 $<G,*>$ 的一个子群，则：

(1) $eH = H$;

(2) 对$\forall a,b \in H$，$aH = bH \Leftrightarrow b^{-1}*a \in H$

(3) 对$\forall a \in H$，$aH = H \Leftrightarrow a \in H$

§5.6 陪集 (5)

5.6.2 左陪集

例：设$<Z_6,+_6>$是一个群，$Z_6=\{[0],[1],[2],[3],[4],[5]\}$，试写出$<Z_6,+_6>$中每个子群及相应的左陪集。

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

群$<Z_6,+_6>$的子群：

$<\{[0]\},+_6>$

$<\{[0][3]\},+_6>$

$<\{[0][2][4]\},+_6>$

$<Z_6,+_6>$

§5.6 陪集 (6)

子群: $<\{[0]\},+_6>=<H_1,+_6>$确定的左陪集

$[0]H_1=\{[0]\}$，$[1]H_1=\{[1]\}$，…，$[5]H_1=\{[5]\}$

子群: $<\{[0],[3]\},+_6>=<H_2,+_6>$确定的左陪集

$[0]H_2=\{[0],[3]\}=[3]H_2$　$[1]H_2=\{[1],[4]\}=[4]H_2$

$[2]H_2=\{[2],[5]\}=[5]H_2$

子群: $<\{[0],[2],[4]\},+_6>=<H_3,+_6>$确定的左陪集

$[0]H_3=\{[0],[2],[4]\}=[2]H_3=[4]H_3$

$[1]H_2=\{[1],[3],[5]\}=[3]H_3=[5]H_2$

§5.6 陪集

5.6.3 左商集和右商集

定义：

设 <H,*> 是 <G,*> 的一个子群，由 H 所确定的 G 上所有元素的左陪集构成的集合称为 G 对 H 的左商集，记为：$S_L=\{ aH|a\in G \}$；所有右陪集构成的集合称为 G 对 H 的右商集，记为：$S_R=\{ Ha|a\in G \}$。

§5.6 陪集

$<\{[0]\},+_6>$, $H_1=\{[0]\}$,

$S_L=\{[0]H_1, [1]H_1, [2]H_1, [3]H_1, [4]H_1, [5]H_1\}$

$S_R=\{H_1[0], H_1[1], H_1[2], H_1[3], H_1[4], H_1[5]\}$

$<\{[0],[3]\},+_6>$, $H_2=\{[0],[3]\}$,

$S_L=\{[0]H_2, [1]H_2, [2]H_2\}$

$S_R=\{H_2[0], H_2[1], H_2[2]\}$

S_L与S_R等势

5.6.3 左商集和右商集

定理：

设 $<H,*>$ 是任意群 $<G,*>$ 的子群，则 G 关于 H 的左、右商集必等势。

定义映射 $f:S_L \to S_R$，

对 $\forall a \in G$，$f(aH)=Ha^{-1}$

§5.6 陪集

5.6.3 左商集和右商集

定理：

设 <H,*> 是群 <G,*> 的子群，H 的任意左陪集（右陪集）与 H 等势。

§5.6 陪集

5.6.3 左商集和右商集

定义：

设 <H,*> 是群 <G,*> 的子群，S_L的基数称为 H 在G 内的指数。记为：$[G:H]=|S_L|$。

5.6.4 Lagrange 定理

定理：

假设 <G,*> 是有限群，<H,*> 是 <G, *> 的子群，则子群（H）的阶必整除群（G）的阶，并且

$$|G| = [G:H]|H|。$$

§5.6 陪集

5.6.4 Lagrange 定理

（1）任何素数阶的群不可能有非平凡的子群。

（2）素数阶的群必为循环群 。

（3）假设<G,*>是 n 阶有限群，则对 $\forall a \in G, |a| | n$。

（4）假设<G,*>是 n 阶有限群，则对 $\forall a \in G, a^n = e$。

§5.7 正规子群 (1)

5.7.1 正规子群的定义

设 <H,*> 是群 <G,*> 的子群，如果对 $\forall a \in G$ 有 $aH = Ha$，则称 <H,*> 是<G,*> 的正规子群（不变子群）。

§5.7 正规子群 (2)

例：假设 $S=\{1,2,3\}, S_3=\{f_1,f_2,..,f_6\}$

$$f_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, f_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$f_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, f_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},$$

$$f_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, f_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

∘	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

§5.7 正规子群 (3)

$$f_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},f_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},f_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$f_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},f_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},f_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$<\{f_1\}, o>, <\{f_1,f_2\},o>,$
$<\{f_1,f_3\},o>, <\{f_1,f_4\},o>,$
$<\{f_1,f_5,f_6\},o>, <S_3, o>$

$f_1\{f_1,f_2\}=\{f_1,f_2\}=f_2\{f_1,f_2\}, \{f_1,f_2\}f_1=\{f_1,f_2\}=\{f_1,f_2\}f_2$

$f_3\{f_1,f_2\}=\{f_3,f_5\}=f_5\{f_1,f_2\}, \{f_1,f_2\}f_3=\{f_3,f_6\}=\{f_1,f_2\}f_6$

$f_4\{f_1,f_2\}=\{f_4,f_6\}=f_6\{f_1,f_2\}, \{f_1,f_2\}f_4=\{f_4,f_5\}=\{f_1,f_2\}f_5$

§5.7 正规子群 (4)

5.7.2 判定正规子群的条件

定理：

设 <H,*>是群<G,*>的一个子群，则以下各条件等价。

(1) 对$\forall a \in G$, $aH=Ha$

(2) 对$\forall a \in G, h \in H$,必存在$h' \in H$,使

$h*a=a*h'$

(3) 对$\forall a \in G, h \in H$, 有 $a^{-1}*h*a \in H$。

§5.7 正规子群 (5)

5.7.3 商群

设<H,*>是群<G,*>的一个正规子群。

则商集为：$G/H=\{aH|a\in G\}=\{Ha|a\in G\}$

在商集G/H上定义运算Δ如下：

对$\forall aH, bH\in G/H$，$aH\ \Delta\ bH=(a*b)H$

则<G/H,Δ>构成商群。

§5.7 正规子群 (6)

5.7.3 商群

例：三次置换群$<\{f_1,f_5,f_6\},\circ>$所产生的商集 $S_3/H_3=\{f_1H_3, f_2H_3\}$ 关于运算 Δ 构成一个商群。

$$f_1H_3=\{f_1,f_5,f_6\}=f_5H_3=f_6H_3$$
$$f_2H_3=\{f_2,f_3,f_4\}=f_3H_3=f_4H_3$$

§5.7 正规子群 (7)

5.7.3 商群

在S_3/H_3上所定义的运算如下所示：

对任意的$aH,bH\in S_3/H_3$，$aH\Delta bH=(a\circ b)H$

运算定义如右表所示：

Δ	f_1H_3	f_2H_3
f_1H_3	f_1H_3	f_2H_3
f_2H_3	f_2H_3	f_1H_3

§5.7 正规子群

5.7.4 子集的乘积

（1）定义

假设 <G,*> 是一个群，A,B 是 G的子集，集合

{a*b| a∈A,b∈B}或者{ab| a∈A,b∈B}

称为A,B的乘积，记为A*B 或 AB。

§5.7 正规子群

5.7.4 子集的乘积

（2）性质

（I）子集的乘积满足结合律。即

$$(A*B)*C=A*(B*C)$$

（II）在子集的运算下，任何子群都为幂等元，即$HH=H$。

§5.7 正规子群

5.7.4 子集的乘积

定理：

设<H,*>是群<G,*>的正规子群，

则对$\forall a,b\in G$，$aH*bH=(a*b)H$

Chapter 6

Ring and Fields

2015-12-29

§6.1 定义及基本性质 (1)

6.1.1 环

假设 <A,★,*> 是一个代数系统，其中，★和 * 都是集合 A 上的二元运算，如果满足:

（1）<A,★> 是交换群（Abel群）;

（2）<A,*> 是半群;

（3） * 对★ 是可分配的;

则称 <A,★,*> 是一个环。

§6.1 定义及基本性质 (2)

6.1.1 环

例：试证明<Z,⊕,⊗>是环。

其中，Z是整数集合，⊕,⊗定义如下：

对∀a,b∈Z， $a \oplus b = a+b-1$

$a \otimes b = a+b-a\times b$

§6.1 定义及基本性质 (3)

6.1.2 环的性质

假设 <A,★,*> 是一个环。

（1）因为<A,★>是Abel群，所以★满足结合律、交换律、消去律，<A,★>中有单位元。

§6.1 定义及基本性质 (4)

6.1.2 环的性质

约定：$a^n = a\star a\star\ldots\star a = na$;

对$\forall a,b\in A$, $(a\star b)^n = na\star nb$;

$a^{m+n} = a^m\star a^n = (m+n)a$;

$a^{mn} = (a^m)^n = n(ma)$。

§6.1 定义及基本性质 (5)

6.1.2 环的性质

(2) 假设 e 是<A,★>的单位元，对∀a,b,c∈A有:

① $e * a = a * e = e$

② $a * b^{-1} = a^{-1} * b = (a*b)^{-1}$

③ $a^{-1} * b^{-1} = a * b$

④ $a*(b★c^{-1}) = (a*b)★(a*c)^{-1}$

⑤ $(b★ c^{-1}) * a = (b*a)★(c*a)^{-1}$

§6.1 定义及基本性质 (6)

6.1.3 由 * 运算确定的几种环

（1）在环 <A,★,*> 中，如果 <A,*> 是含幺半群，并且 e' 是单位元，则称 e' 为环的单位元。这时称 A 为有单位元的环（有 1 环）。如果元素 a 在 <A,*> 中有逆元，则在含有单位元的环中，该元素的逆也称为环中元素的逆。

§6.1 定义及基本性质 (7)

6.1.3 由 * 运算确定的几种环

（2）如果环中只含有一个元素，此时该元素应该是 <A,★> 中的单位元，当然也是 <A,*> 中的单位元和零元，所以这种环称为零环。

（3）设 <A,★,*> 是环，当 <A,*> 是可交换半群时，称 <A,★,*> 是可交换环。

§6.2 整环、除环和域 (1)

6.2.1 零因子

设 $<A,\star,*>$ 是环，如果存在 $a,b\in A$，这里 $a\neq e$，$b\neq e$，但 $a * b = e$，则称 a 为 A 中的左零因子，b 为 A 中的右零因子，左、右零因子统称为零因子。

其中，e 是$<A,\star>$的单位元。

§6.2 整环、除环和域 (2)

6.2.1 零因子

例如：$<Z_4, +_4, \times_4>$是一个环。其中，$+_4, \times_4$的运算表如下：

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\times_4$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

§6.2 整环、除环和域 (3)

6.2.1 零因子

当一个环中不含有零因子时，称它为无零因子环。即对任意的 a,b∈A，若 a * b = e，则必有 a = e 或 b = e。

定理：

设 <A,★,*> 是无零因子的环，则 * 在 A 上消去律成立。反之亦然。

§6.2 整环、除环和域 (4)

6.2.2 整环

设 $<A,\bigstar,*>$ 是无零因子环，并且是可交换的含幺环，则称它为整环。

即 $<A,\bigstar,*>$ 是环，并且 $<A,*>$ 有单位元，$*$ 运算可交换，对 $\forall a,b\in A$，若 $a*b=e$，则必有 $a=e$ 或 $b=e$。

§6.2 整环、除环和域

6.2.3 除环、域

设 <A,★,*> 是一个含幺环，其单位元是e'，如果A-{e}≠∅，并且<A-{e},*>是一个群，则称它为除环，可交换的除环是域。

§6.2 整环、除环和域 (6)

6.2.3 除环、域

域一定是整环，但整环不一定是域。

有限整环必为域。

假设 $<A,\bigstar,*>$是一个无零因子的有限环，并且$|A| \geq 2$，则$<A,\bigstar,*>$ 一定是除环。

Chapter 7

Lattices and Boolean Algebra

2015-12-29

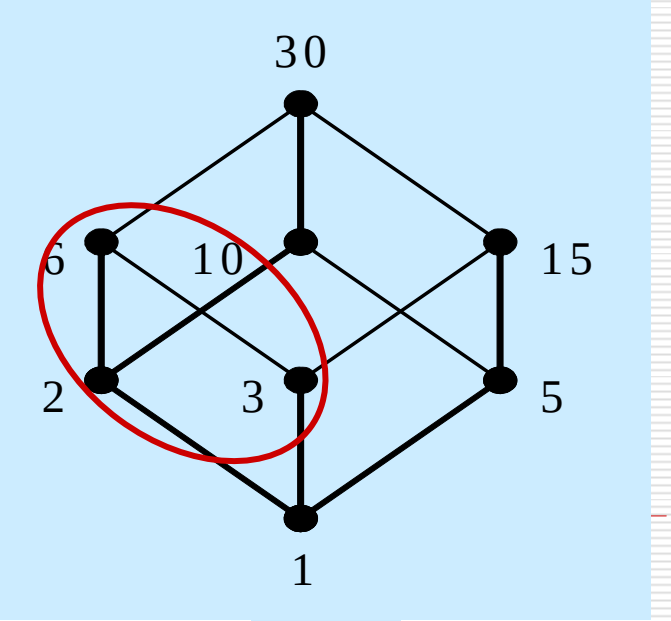
§ 7.1 Lattices (1)

7.1.1 Posets and Lattices

Exam 1: $S_{30} = \{1,2,3,5,6,10,15,30\}$

$| = \{<x,y> \mid x,y \in S_{30} \text{ and } x|y\}$

$S = \{2,3,6\} \subseteq S_{30}$

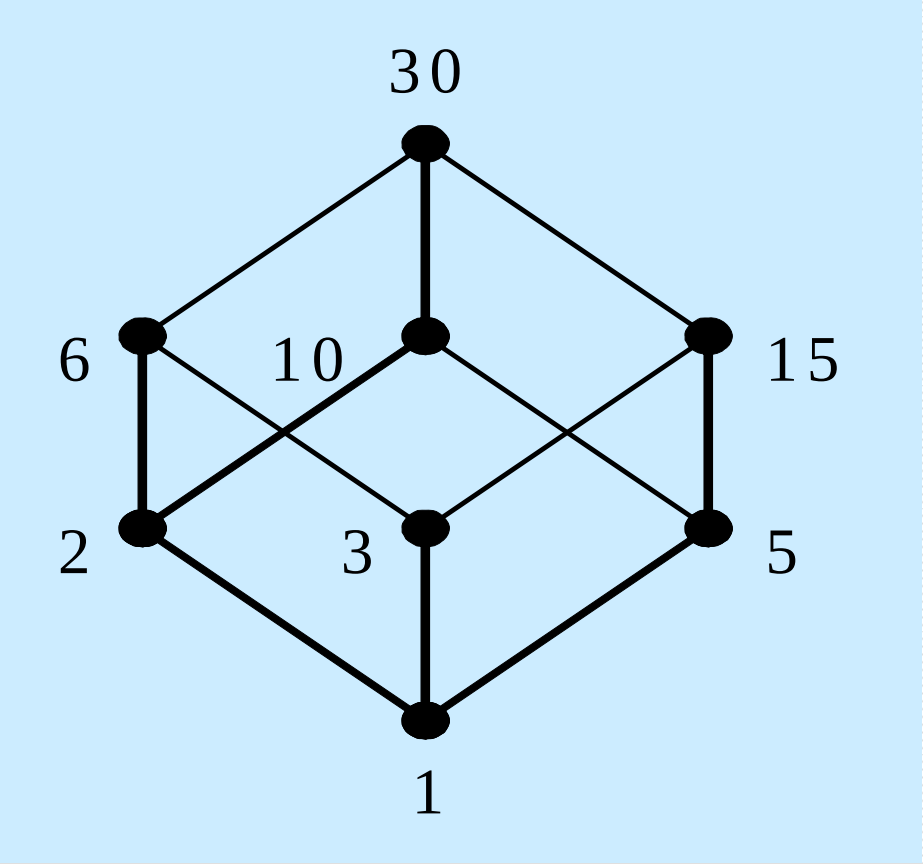


§ 7.1 Lattices (2)

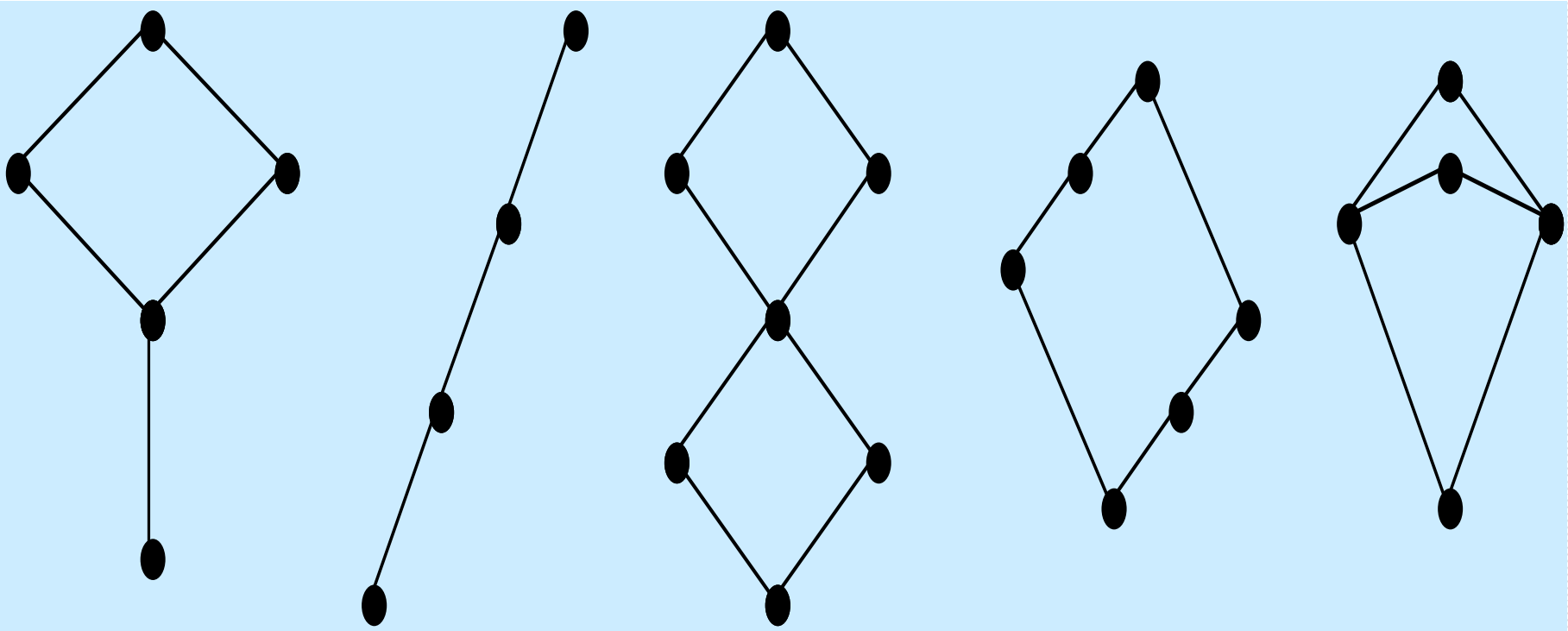
7.1.2 The concept of lattices and their properties

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a lattices.

§ 7.1 Lattices



§ 7.1 Lattices



§7.1 Lattices

⊕, * 运算性质：

（1）Idempotent laws（幂等律）

（2）Commutative laws（交换律）

（3）Associative laws（结合律）

（4）Absorptions（吸收律）

§7.2 Lattices - algebra system (1)

$$< P, \leq > \Leftrightarrow <P, \oplus, * >$$

定理

假设$< P, \leq >$是一个格，则对$\forall a,b \in P$，有 $a \leq b \Leftrightarrow a*b=a \Leftrightarrow a \oplus b=b$。

引理

设$<P, \oplus, *>$是一个代数系统，如果运算$\oplus, *$满足等幂、结合、交换、吸收律，那么

$$a * b = a \Leftrightarrow a \oplus b = b。$$

§7.2 Lattices - algebra system (2)

定理

假设<P, ⊕, * >是一个代数系统，其中的运算⊕, * 满足等幂、结合、交换、吸收律，定义 P 上的关系为：对∀a,b∈P，a ≤ b ⇔ a * b = a，则 ≤ 是偏序关系，并且对 ∀a,b∈P，a * b 和 a ⊕ b 分别表示为 a,b 在<P, ≤>中的最大下界和最小上界，从而，<P, ≤>是一个格。

§7.2 Lattices - algebra system (3)

定义

设<P, ⊕, * >是一个代数系统，如果运算 ⊕, * 满足等幂、结合、交换、吸收律，那么<P, ⊕, * >就是一个格。

§7.3 Several different types of lattices (1)

① Complete lattice

A complete lattice is a partially ordered set in which all subsets have both a supremum and an infimum.

§ 7.3 Several different types of lattices (2)

② Bounded lattice

A bounded lattice is a lattice $<P,\leq>$ and $\exists a,b\in P$ satisfy the following:

1. for all $x\in P$, $a\leq x$, that a is called the lower bound;

2. for all $x\in P$, $x\leq b$, that b is called the upper bound.

§ 7.3 Several different types of lattices (3)

③ Complemented lattice

A complemented lattice is a bounded lattice (that is it has a least element 0 and a greatest element 1), in which each element x has a complement.

§ 7.3 Several different types of lattices (4)

④ Distributive lattice

A lattice is said to be distributive if it satisifes either (and therefore both) of the distributive laws:

$$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$$

$$a * (b \oplus c) = (a * b) \oplus (a * c)$$

§ 7.3 Several different types of lattices

⑤ Modular lattice

A modular lattice P is a lattice that satisfies the following self-dual condition:

Modular law

$a \leqslant c$ implies

$a \oplus (b * c) = (a \oplus b) * c$

for all $a,b,c \in P$.

§ 7.4 Boolean algebra

Boolean lattice

A Boolean lattice B is a distributive lattice in which for each element $x \in B$ there exists a complement $x' \in B$.

§7.5 Boolean expressions (1)

Boolean expressions

定义：假设 B 是一个布尔代数，$x_1,x_2,\ldots,x_n$是 B 上的变量，B上由$x_1,x_2,\ldots,x_n$生成的布尔表达式归纳定义如下：

(1) B中的元素是B上由$x_1,x_2,\ldots,x_n$生成的布尔表达式；

(2) B上任意变量x_i（i=1,2,…,n）是B上由$x_1,x_2,\ldots,x_n$生成的布尔表达式；

(3)如果α，β是B上由$x_1,x_2,\ldots,x_n$生成的布尔表达式，则α⊕β，α*β，α'（α的补元）是B上由$x_1,x_2,\ldots,x_n$生成的布尔表达式；

(4)只有通过有限次使用(1),(2),(3)得到的符号串是B上由$x_1,x_2,\ldots,x_n$生成的布尔表达式。