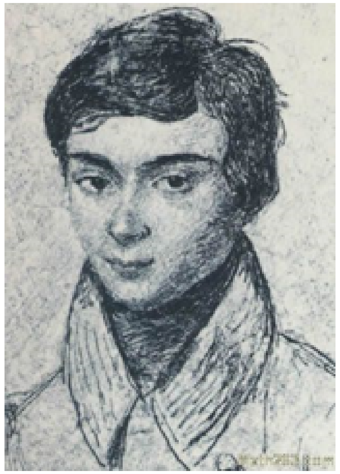
第三篇　代数系统

本篇用代数方法来研究数学结构, 故又叫代数结构或近世代数。它将用抽象的方法来研究集合上的关系和运算。

代数的概念和方法已经渗透到计算机科学的许多分支中，它对程序理论，数据结构，编码理论的研究和逻辑电路的设计已具有理论和实践的指导意义。本篇讨论一些典型的代数系统及其性质（包括格）。

第三篇　代数系统



Evariste Galois（**1811-1832**）

（伽罗瓦 法国人**)**

提出群论

第五章　　代数结构

§5-1 代数系统的引入

定义1 设A是一个集合，f是一个函数，f：$A^n \to A$，则称f为A上的**n元运算**，整数n称为运算的阶(元，次).

若n=1，则称f：$A \to A$为一元运算；

若n=2，则称f：$A^2 \to A$为二元运算。

若用运算符*表示二元运算f：$A^2 \to A$，则常用$x * y$表示$f(\langle x,y \rangle)$.

§5-1 代数系统的引入

例：（1）在整数集I和实数集R中，+，-，×均为二元运算.

（2）在集合Z的幂集$P(Z)$中，$\cap$,$\cup$均为二元运算，而“~”是一元运算.

（3）{命题公式}中，$\vee$,$\wedge$均为二元运算，而“$\neg$”为一元运算.

（4）{双射函数}中，函数的合成运算是二元运算.

（5）在正偶数集合中，×,+是二元运算；在正奇数集合中，×是二元运算，而+不是二元运算(正奇数集合对加法不封闭).

§5-1 代数系统的引入

定义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，…，f_k所组成的系统就称为一个代数系统（代数结构），记作<A, f_1, f_2, …, f_k>。

定义2’ 代数结构是由三个部分组成的数学结构：

（1）非空集合S，称为代数结构的载体。

（2）载体S上的若干运算。

（3）一组刻划载体上各运算所满足性质的公理。

§5-1 代数系统的引入

代数结构常用一个多元序组<S, *, Δ, … >来表示, 其中 S是载体，*，Δ，…为各种运算。有时为了强调S有某些元素地位特殊，也可将它们列入这种多元序组的末尾。

例：(1) 整数集合 I 上+，×：

$+\quad f:\ I^2 \to I$为二元运算

$\times\quad f:\ I^2 \to I$为二元运算

所以<I，+，×>是代数系统。

(2)< *P*(S)，∪，∩，~>是代数系统。

7

§5-1 代数系统的引入

例：<I，+>，对于二元运算“+”满足如下运算规律：

（1） $x+y=y+x$ 交换律

（2） $(x+y)+z=x+(y+z)$ 结合律

	$<I, \cdot>$	$<R, +>$	$<P(S), \cup>$	$<P(S), \cap>$
集合	整数	实数	S的幂集	S的幂集
运算	乘法	加法	集合的并	集合的交
交换律	$x\cdot y=y\cdot x$	$x+y=y+x$	$A\cup B=B\cup A$	$A\cap B=B\cap A$
结合律	$(x\cdot y)\cdot z=x\cdot(y\cdot z)$	$(x+y)+z=x+(y+z)$	$(A\cup B)\cup C=A\cup(B\cup C)$	$(A\cap B)\cap C=A\cap(B\cap C)$

§5-1 代数系统的引入

虽然集合不同，运算不同，但是它们是一些具有共同运算规律的运算.

用代数的方法从不同的研究对象中概括出一般的数学模型并研究其规律、性质和结构。

抽象代数的研究对象是抽象的，它不是以某一具体对象为研究对象，而是以一大类具有某种共同性质的对象为研究对象，因此其研究成果适用于这一类对象中的每个对象，从而达到了事半功倍的效果。

9

第五章　代数结构

§5-2 运算及其性质

1 交换性

定义1 设*是集合A上的二元运算，若对任意x，$y \in A$，有 $x * y = y * x$，则称*运算在A上是可交换的（或者说*在A上满足交换律）。

例2：设Q是有理数集合，Δ是Q上的二元运算，对∀a，b∈Q，aΔb=a+b-a· b，问运算Δ是否可交换。

解：$a\Delta b = a+b-a\cdot b = b+a-b\cdot a = b\Delta a$

所以运算Δ是可交换的。

11

§5-2 运算及其性质

2 结合性

定义2 设*是集合A上的二元运算，若对任意x,y,z∈A都有$(x*y)*z = x*(y*z)$，则称*运算在A上是可结合的（或者说*在A上满足结合律）。

例如**R**上的加法运算和乘法运算都是可结合运算，

R上的减法运算和除法运算都是不可结合运算。

§5-2 运算及其性质

例3：设A是一个非空集合，★是A上的二元运算，对于任意a，b∈A，有a★b=b，证明★是可结合运算。

证明：因为对于∀a，b，c∈A，

$$(a\bigstar b)\bigstar c = b\bigstar c = c$$

而 $a\bigstar(b\bigstar c)=a\bigstar c=c$

所以$(a\bigstar b)\bigstar c=a\bigstar(b\bigstar c)$

3 分配律

定义3 设$*$和Δ是集合A上的两个二元运算，

若对任意$x,y,z \in A$，有 $x * (y\Delta z) = (x * y)\Delta(x * z)$；

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

则称运算$*$对Δ是可分配的（或称$*$对Δ满足分配律）。

§5-2 运算及其性质

例4：设集合A={α,β}，在A上定义两个二元运算*和Δ如表所示。运算Δ对于运算*可分配吗？运算*对于运算Δ呢？

*	α	β
α	α	β
β	β	α

Δ	α	β
α	α	α
β	α	β

解：因为$\beta*(\alpha\Delta\beta)=\beta*\alpha=\beta$，

而$(\beta*\alpha)\Delta(\beta*\beta)=\beta\Delta\alpha=\alpha$。

所以运算*对于运算Δ是不可分配的。

验证运算△对于运算*是可分配的。

从*和△的运算表中可以看出*和△两种运算都是可交换的。

故只须验证 $\alpha\triangle(\alpha*\alpha)=(\alpha\triangle\alpha)*(\alpha\triangle\alpha)$

$\alpha\triangle(\alpha*\beta)=(\alpha\triangle\alpha)*(\alpha\triangle\beta)$

$\alpha\triangle(\beta*\beta)=(\alpha\triangle\beta)*(\alpha\triangle\beta)$

$\beta\triangle(\alpha*\alpha)=(\beta\triangle\alpha)*(\beta\triangle\alpha)$

$\beta\triangle(\alpha*\beta)=(\beta\triangle\alpha)*(\beta\triangle\beta)$

$\beta\triangle(\beta*\beta)=(\beta\triangle\beta)*(\beta\triangle\beta)$

*	α	β
α	α	β
β	β	α

Δ	α	β
α	α	α
β	α	β

$\alpha\triangle(\alpha*\alpha)=\alpha\triangle\alpha=\alpha$ $\quad(\alpha\triangle\alpha)*(\alpha\triangle\alpha)=\alpha*\alpha=\alpha$

$\alpha\triangle(\alpha*\beta)=\alpha\triangle\beta=\alpha$ $\quad(\alpha\triangle\alpha)*(\alpha\triangle\beta)=\alpha*\alpha=\alpha$

$\alpha\triangle(\beta*\beta)=\alpha\triangle\alpha=\alpha$ $\quad(\alpha\triangle\beta)*(\alpha\triangle\beta)=\alpha*\alpha=\alpha$

$\beta\triangle(\alpha*\alpha)=\beta\triangle\alpha=\alpha$ $\quad(\beta\triangle\alpha)*(\beta\triangle\alpha)=\alpha*\alpha=\alpha$

$\beta\triangle(\alpha*\beta)=\beta\triangle\beta=\beta$ $\quad(\beta\triangle\alpha)*(\beta\triangle\beta)=\alpha*\beta=\beta$

$\beta\triangle(\beta*\beta)=\beta\triangle\alpha=\alpha$ $\quad(\beta\triangle\beta)*(\beta\triangle\beta)=\beta*\beta=\alpha$

4 吸收律

定义4 设*，Δ是定义在集合A上的两个**可交换**二元运算，若对于任意的x，y∈A，都有

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

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

则称运算*和运算Δ满足吸收律。

§5-2 运算及其性质

例5：设集合N为自然数全体，在N上定义两个二元运算 $*$ 和★，对于 $\forall x, y \in N$，有 $x * y = \max(x, y)$，$x ★ y = \min(x, y)$，验证运算 $*$ 和★满足吸收律。

解：对于 $\forall a, b \in N$，

$$a * (a ★ b) = \max(a, \min(a, b)) = a$$

$$a ★ (a * b) = \min(a, \max(a, b)) = a$$

因此，$*$ 和★满足吸收律。

18

§5-2 运算及其性质

5 幂等律

定义5 设$*$是A上的二元运算，若对任意$x \in A$有 $x * x = x$，则称$*$满足幂等律。

例6 设$P(S)$是集合S的幂集，在$P(S)$上定义的两个二元运算，请验证，集合的“并”运算$\cup$和集合的“交”运算$\cap$满足幂等律。

解： 对于任意的$A \in P(S)$，
有$A \cup A = A$和 $A \cap A = A$，
因此运算$\cup$和$\cap$都满足幂等律。

19

§5-2 运算及其性质

设$*$和Δ为集合A上的二元运算

若$\forall x \forall y(x,y \in A \rightarrow x*y= y*x)$,则称$*$满足交换律。

若$\forall x \forall y \forall z(x,y,z \in A \rightarrow x* (y* z) = (x*y) *z)$，则称$*$满足结合律。

若$\forall x \forall y \forall z(x,y,z \in A \rightarrow x*(y\Delta z)=(x*y)\Delta (x*z)$, $(y\Delta z)*x=(y*x)\Delta (z*x))$，则称$*$对$\Delta$满足分配律。

若$*$和Δ满足交换律，且有$\forall x \forall y(x,y \in A \rightarrow x*(x\Delta y)=x$, $x\Delta (x*y)=x)$，则称$*$和Δ满足吸收律。

若$\forall x (x \in A \rightarrow x*x=x)$，则称$*$满足幂等律。

§5-2 运算及其性质

二、特殊元素——幺元，零元和逆元

1 幺元（单位元）

设<A，*>是代数系统，*是集合A上的二元运算，

(1) 若$\exists e_l \in A$，对$\forall x \in A$ 有$e_l * x = x$；则称e_l为A中关于*的**左幺元**；

(2) 若$\exists e_r \in A$，对$\forall x \in A$ 有$x * e_r = x$；则称e_r为A中关于*的**右幺元**；

(3)若$\exists e \in A$，既是左幺元又是右幺元，则称e为A中关于*的**幺元**。 $e * x = x * e = x$

§5-2 运算及其性质

例7：设集合S={α，β，γ，δ}，在S上定义的两个二元运算*和★如表示。试指出左幺元或右幺元。

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

★	α	β	γ	δ
α	α	β	δ	γ
β	β	α	γ	δ
γ	γ	δ	α	β
δ	δ	δ	β	γ

解：由表可知β， δ都是S中关于运算*的左幺元，没有右幺元。

α是S中关于运算★的右幺元，没有左幺元。

§5-2 运算及其性质

定理1： 设*是集合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A中的幺元是唯一的。

证明：先证左幺元e_l=右幺元e_r=e

$\because\ e_l * e_r = e_r = e_l$

$\therefore$ 有$e_l = e_r = e$成立。

再证幺元e是唯一的

设另有一幺元$e_1 \in A$，则$e_1= e_1 * e= e$，

$\therefore$ 若存在幺元，一定是唯一的。

§5-2 运算及其性质

例：

（1）在实数集合R中，对$+$而言，$e=0$；

对$\times$而言，$e=1$；

（2）在$P(S)$中，对$\cap$而言，$e=S$（全集合）；

对$\cup$而言，$e=\Phi$（空集）；

（3）{命题逻辑}中，对$\vee$而言，$e=F$（永假式）；

对$\wedge$而言，$e=T$（永真式）。

24

§5-2 运算及其性质

2 零元

设<A，*>是代数系统，*是集合A上的二元运算，

（1）若$\exists\theta_l\in A$，且对$\forall x\in A$有$\theta_l * x=\theta_l$，则称θ_l为A中关于*的左零元；

（2）若$\exists\theta_r\in A$，且对$\forall x\in A$有$x*\theta_r=\theta_r$，则称θ_r为A中关于*的右零元。

（3）若$\exists\theta\in A$，既是左零元又是右零元，则称θ为A中关于*的零元。$\theta * x=x*\theta=\theta$

25

§5-2 运算及其性质

例8：设集合S={浅色，深色}，

定义在S上的二元运算*如表，试指出零元和幺元。

*	浅色	深色
浅色	浅色	深色
深色	深色	深色

解：深色是S中关于运算*的零元，

浅色是S中关于运算*的幺元。

§5-2 运算及其性质

定理2 设*是集合A上的二元运算，且在A中有关于* 运算的左零元θ_l和右零元θ_r，则$\theta_l = \theta_r = \theta$，且A中的零元是唯一的。

证明：先证左零元θ_l=右零元θ_r=θ

$$\theta_l = \theta_l * \theta_r = \theta_r = \theta$$

再证零元θ是唯一的

设另有一零元$\theta_1 \in A$，则$\theta_1 = \theta_1 * \theta = \theta$，

∴若存在零元，一定是唯一的。

§5-2　运算及其性质

例：

（1）在实数集合R中，对$\times$而言，$\theta=0$

对+ 而言，没有零元.

（2）在$P(S)$中，对$\cap$而言，$\theta=\Phi$；

对$\cup$而言，$\theta=S$；

（3）{命题逻辑}中，对$\vee$而言，$\theta=T$；

对$\wedge$而言，$\theta=F$.

§5-2 运算及其性质

定理3 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：用反证法

设$\theta = e$，对$\forall x \in A$ 有

$$x = e * x = \theta * x = \theta = e$$

则A中的所有元素都相同。与|A|>1矛盾。

§5-2 运算及其性质

3 逆元

设<A，*>是代数系统， *是A上的二元运算

(1) 若对某个$a \in A$，$\exists b \in A$，使$b * a = e$，称b是a的左逆元；

(2) 若对某个$a \in A$，$\exists b \in A$，使$a * b = e$，称b是a的右逆元；

(3) 若元素b既是a的左逆元，又是右逆元，则称b是a的一个逆元。

30

§5-2 运算及其性质

讨论：

（1）若b是a的逆元，那么a也是b的逆元，称a与b互为逆元。

（2）x的逆元通常记为x^{-1};

但当运算被称为“加法运算”（记为+）时，x的逆元可记为$-x$ 。

（3）一个元素的左逆元不一定等于它的右逆元。

一个元素可以有左逆元而没有右逆元。

一个元素的左（右）逆元不一定是唯一的。

例9：设集合S={α，β，γ，δ，ζ}，定义在S上的一个二元运算*如表所示。指出代数系统<S，*>中各个元素的左、右逆元情况。

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

解： α是幺元；

β的左逆元和右逆元都是γ；即β和γ互为逆元；

δ的左逆元是γ而右逆元是β；β有两个左逆元γ和δ；

ζ的右逆元是γ，但ζ没有左逆元。

§5-2 运算及其性质

定理(补充) 设<A, *>是一个代数系统， *是A上**可结合**的二元运算，且A中存在幺元e，若A中元素a关于*运算存在左逆元b和右逆元c，则必有 $b=c$，即元素a关于*运算存在逆元，且逆元**是唯一**的.

请补充证明过程.

33

§5-2 运算及其性质

定理4 设<A, *>是代数系统， *是A上的二元运算，A中存在幺元e，且每个元素都有左逆元。若*是可结合的，则该代数系统中任何一个元素的左逆元必定是该元素的右逆元，且每个元素的逆元是唯一的。

§5-2 运算及其性质

证明：先证左逆元=右逆元

设$a, b, c \in$ A，且b是a的左逆元，c是b的左逆元

$\because (b * a) * b = e * b = b$

$\therefore e = c * b = c * ((b * a) * b)$

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

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

$= (e * a) * b$

$= a * b$

$\therefore$ b也是a的右逆元

35

再证逆元是唯一的

设a有两个逆元b和c，那么

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

$\therefore$ a的逆元是唯一的。

§5-2 运算及其性质

《推论》 $(x^{-1})^{-1}=x$， $e^{-1}=e$

X是x^{-1}的右逆元　　X是x^{-1}的左逆元

证明：$\because x^{-1} * x = x * x^{-1} = e$

$\therefore (x^{-1})^{-1}=x$

$\because e^{-1} = e^{-1} * e = e$

即 $e^{-1}=e$

37

§5-2 运算及其性质

例：（1）在实数集合R中，

对“+”运算，加法幺元e是0

$\forall x \in R$ $\because x+(-x)=0$ $\therefore x^{-1}=-x$，

对“×”运算，乘法幺元e是1；

$\forall x \in R$ $(x \neq 0)$，$\because x \times 1/x=1$，$\therefore x^{-1}=1/x$

（2）在函数的合成运算中，每一个双射函数都是可逆的，f^{-1}（f的逆关系）；

（3）在所有的二元运算中，零元一定不存在逆元，

$\because \theta * x = x * \theta = \theta$。

§5-2 运算及其性质

例9：试构造一个代数系统，使得其中只有一个元素具有逆元。

解：设m，$n \in I$，$T=\{x|x \in I, m \leq x \leq n\}$，

那么，代数系统 $<T, max>$ 中有一个幺元是m，且只有m有逆元，

因为$m=max(m, m)$。

§5-2 运算及其性质

例10：对于代数系统<N_k，$+_k$>，这里N_k={0,1,2,…,k-1}，$+_k$是定义在N_k上的模k加法运算，定义如下：对于任意$\forall x$，$y \in N_k$

$$x +_k y = \begin{cases} x+y & \text{若} x+y<k \\ x+y-k & \text{若} x+y \geq k \end{cases}$$

问是否每个元素都有逆元。

解：可以验证，$+_k$是一个可结合的二元运算，N_k中关于 运算$+_k$的幺元是0，N_k中的每一个元素都有唯一的逆元，即0的逆元是0，每个非零元素x的逆元是k-x。

40

§5-2 运算及其性质

二元运算的性质与运算表的关系

<A， *>是一个代数系统， *是A上的一个二元运算。

（1）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。

（2）运算*具有幂等性，当且仅当运算表的主对角线上的每一元素与它所在行（列）的表头元素相同。

41

§5-2 运算及其性质

（3）A关于*有零元，当且仅当该元素所对应的行和列中元素都与该元素相同。

（4）A关于*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。

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

42