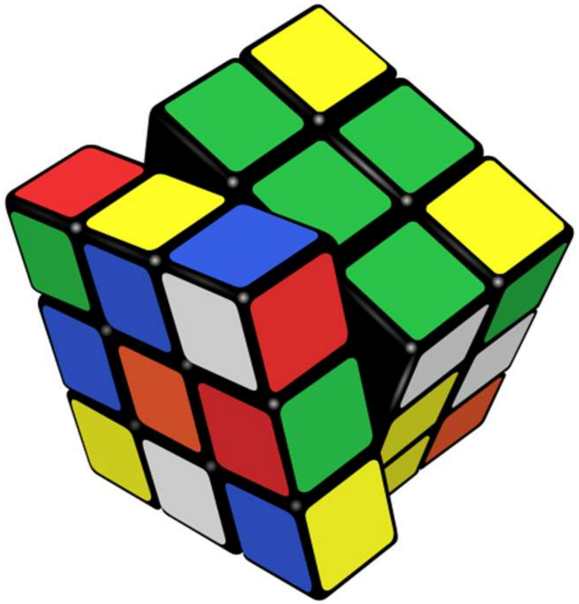
代数系统（二）

群论

南京大学计算机科学与技术系

内容提要

- 引言
- 半群
- 幺半群
- 群
- 群的性质
- 群的术语
- 群方程*

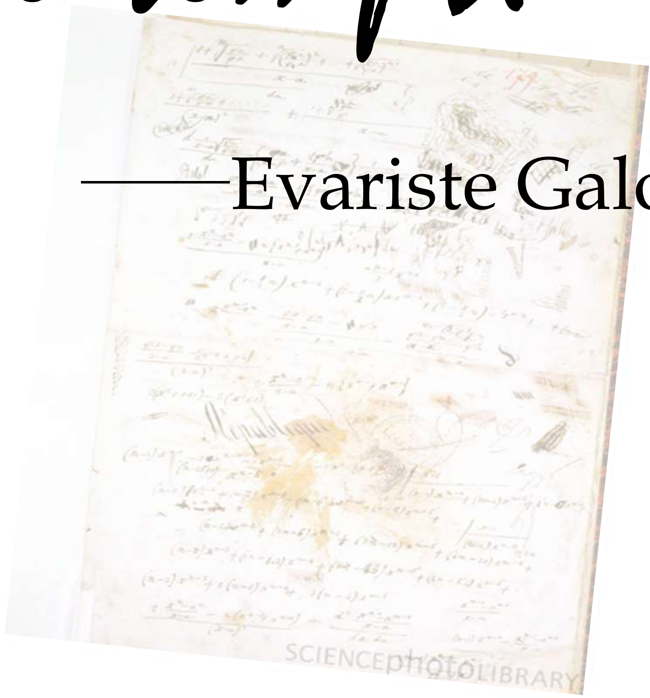


引言：一元多次方程的解

“为什么五次及更高次的代数方程没有一般的代数解法，即这样的方程不能由方程的系数经有限次四则运算和开方运算求根？”

群 论

Je n'ai pas le temps.



——Evariste Galois

半　群

定义　设$(S, *)$为代数系统，$(S, *)$为半群（Semigroup）指

(1) $(\forall x, y \in S)(x * y \in S)$

(2) $(\forall x, y, z \in S)((x * y) * z = x * (y * z))$

若$(\forall x, y \in S)(x * y = y * x)$则称$(S, x)$为交换半群（abelian半群）

- "代数系统" + "结合性" = "半群"
- 例：代数系统$\langle\{1,2\},*\rangle$为半群，其中$*$定义为

$\forall x, y \in \{1,2\}, x * y = y$

幺半群（Monoid）

定义 设$(S, *)$为代数系统，$(S, *)$为Monoid（Semigroup with unit）指

(1) $(\forall x, y \in S)(x * y \in S)$

(2) $(\forall x, y, z \in S)((x * y) * z = x * (y * z))$

(3) $(\exists e \in S)(\forall x \in S)(e * x = x * e = x)$

- “半群” + “单位元” = “**Monoid**”
- 注意：代数系统中左右单位元若存在则必相等且唯一

幺半群（续）

- 例1：$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$，$T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{R} \right\}$

  则集合S与T关于矩阵的乘法皆构成Monoid
- 例2：$\langle \mathbb{Z}^+, + \rangle$为半群，但非Monoid
- 例3：$\langle \mathbb{Z}_n, \oplus_n \rangle$为Monoid，$\oplus_n$是模$n$加法
- 例4：$\langle A^A, \circ \rangle$ 为Monoid，$\circ$是函数复合运算
- 例5：$\langle \mathcal{P}(B), \oplus \rangle$为Monoid，$\oplus$为对称差运算

群（Group）

- $(G,*)$为群当且仅当有$e \in G$和G上的一元运算$^{-1}$使

$(0)\ G \neq \emptyset$

$(1)\ (\forall x, y \in G)(x * y \in G)$ ……代数系统

$(2)\ (\forall x, y, z \in G)(x * (y * z) = (x * y) * z)$ …半群

$(3)\ (\forall x \in G)(x * e = e * x = x)$ ……幺半群

$(4)\ (\forall x \in G)(x * x^{-1} = x^{-1} * x = e)$ ……群

$(1) \sim (4)$有时被称为群论公理

群 （续）

- 群的等价描述：
- 设G为非空集合，$*$为G上的二元运算，$\langle G,*\rangle$为群指

  $\langle G,*\rangle$为Monoid，其单位元为e，且满足：

$$(\forall \boldsymbol{x} \in \boldsymbol{G})(\exists \boldsymbol{y} \in \boldsymbol{G})(\boldsymbol{x} * \boldsymbol{y} = \boldsymbol{y} * \boldsymbol{x} = \boldsymbol{e})$$

- 注意：可结合的代数系统中逆元若存在则唯一

群（续）

命题 设$\langle G,*,e\rangle$为群，任何元素之逆是唯一的。

证：设y，z为x之逆，从而

$$x*y=y*x=e=x*z=z*x$$

$$\because x*y=e\rightarrow z*(x*y)=z*e$$

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

$$\rightarrow e*y=z$$

$$\rightarrow y=z$$

$\therefore y=z$ $\square$

群（续）

- 示例
  - $\langle \mathbb{R}, +\rangle, \langle \mathbb{Z}, +\rangle$为群，但$\langle \mathbb{N}, +\rangle$不为群（1无逆）
  - $\langle \mathbb{R}\text{-}\{0\}, *\rangle$，非零实数乘法群；$a$的逆元素为$1/a$
  - $\langle \mathbb{Z}_n, \oplus_n\rangle$为群，$i$之逆为$n-i$
  - 正方形的对称变换集与乘积构成群
  - $T_A = \{f: A \to A | f$为双射$\}$，单位元I_A，f的逆元f^{-1}
  - $A = \{f: \mathbb{R} \to \mathbb{R} |$呈形$f(x) = ax + b\}$，$\langle A, \circ\rangle$是群？

群（续）

设$f(x) = ax + b\ (a,\ b \in \mathbb{R})\ f \in A\ f$有逆吗?

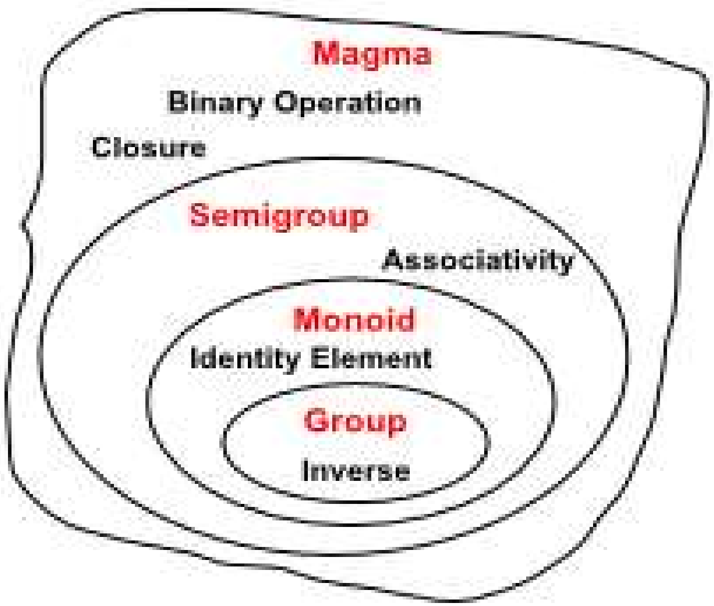
设$g(x) = cx + d\ (c,\ d \in \mathbb{R})$为$f$之逆，从而$f(g(x)) = g(f(x)) = x$。

因此，$a(cx + d) + b = x$，$c(ax + b) + d = x$；$acx + ad + b = x$，$acx + cb + d = x$；$ac = 1$，$ad + b = cb + d = 0$；$c = 1/a$，$d = -b/a$。

故当$a = 0$时f无逆，当$a \neq 0$时f的逆为$g(x) = x/a - b/a$。

然而令$A' = \{f : \mathbb{R} \to \mathbb{R} | f$呈形$f(x) = ax + b$且$a \neq 0\}$，$(A', \circ)$为群。

群 （续）


Magma
Binary Operation
Closure
Semigroup
Associativity
Monoid
Identity Element
Group
Inverse

群的性质

定理 设$(G, *, e, ^{-1})$为群

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

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

(3) $ab = ac \rightarrow b = c$（左消去律）

(4) $ba = ca \rightarrow b = c$（右消去律）

(5) 方程$ax = b$和$ya = b$在G中对x，y有唯一解

有限群的运算表中每行（列）均为群中所有元素的一种排列，不同行（列）也不可能出现同样的排列。

群的术语：元素的乘幂（次方）

- 定义

  $a^0 = e$ （e是单位元素）

  $a^{n+1} = a^n \circ a$ (n是非负整数)

  $a^{-k} = (a^{-1})^k$ (k为正整数)

- 性质

  $a^n \circ a^m = a^{n+m}$

  $(a^n)^m = a^{nm}$

群的术语：元素的阶

- 设G是群，$a \in$G， a的阶（周期）定义如下：
  - $|a| = \min\{k \in \mathbb{Z}^+ \mid a^k = e\}$
  - 如果这样的k不存在，a为无限阶元
- 性质
  - 有限群不存在无限阶元
  - 群中元素及其逆元具有相同的阶
  - 有限群中阶大于2的元素有偶数个
  - 偶数群中阶为2的元素有奇数个 $(a = a^{-1})$

群的术语：群的阶

(1) 若G为有穷集，则称$(G,*)$为有限群。当$|G|=n$时称$(G,*)$之阶为n且称G为n阶群

(2) 若G为无穷集，则称$(G,*)$为无限群

(3) 若群$(G,*)$满足$(\forall x,y\in G)(xy=yx)$，则称$G$为交换群(abelian群)

下面我们给出1，2，3，4阶全部不同构的群

(1) 若$(G,*)$为1阶群，从而设$G=\{e\}$有$ee=e$。故1阶群在同构意义下只有一个。

(2) 若$(G,*)$为2阶群，从而设$G=\{e,a\}(a\neq e)$，易见$ea=ae=a$，$ee=e$但aa呢？

若$aa=a$则$a=e$矛盾，故$aa=e$。故2阶群在同构意义下只有一个。

乘法表见下:

$*$	e	a
e	e	a
a	a	e

有关群的术语（续）

(3) 若$\langle G,*\rangle$为3阶群，从而可设$G=\{e,a,b\}$，e,a,b互异。若$a*a=e$,则$a*b=b$, 矛盾，故$a*a=b$。运算表唯一。因此，3阶群在同构意义下只有一个。

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

有关群的术语（续）

- **证明：** 四阶群皆为Abel群

证：设$G=\{e,a,b,c\}$，e为幺。现证$ab=ba$

情况1. $ab=e$从而ba只能为e或c，若$ba=c$则$aba=ac$，从而$ea=ac$，从而$c=e$矛盾，故$ba=e$。

情况2. $ab=c$，同理$ba=c$

同理$bc=cb$，$ac=ca$。 □

- **证明：** 四阶群中元素的阶为1、2或者4（不为3）.

假设有个元素a的阶为3，$\{e, a, a^2, b\}, ab=$?（矛盾）

有关群的术语（续）

(4) 只有两种四阶群

- 有个元素的阶为4：

  $\{e, a, a^2, a^3\}$

  与$\langle \mathbb{Z}_4, \oplus_4 \rangle$同构

- 元素的阶均不为4：

  Klein四元群

$*$	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