信息安全数学基础

第三章 群

陈大江

信息与软件工程学院

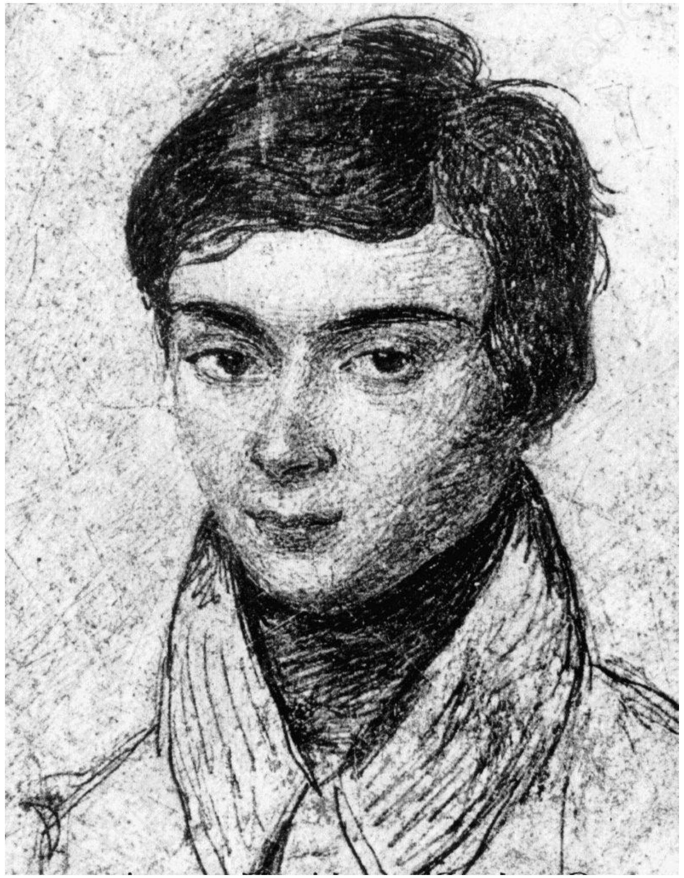
代数方程的解

两千多年之前古希腊时代数学家就能够利用开方法解二次方程 $ax^2+bx+c=0$ 。16世纪初欧洲文艺复兴时期之后，求解高次方程成为欧洲代数学研究的一个中心问题。1545年意大利数学家G. Cardano(1501-1576)在他的著作《大术》中给出了三、四项多项式的求根公式，此后的将近三个世纪中人们力图发现五次方程的一般求解方法，但都失败了。

直到1824年一位年青的挪威数学家 N.Abel (1802-1829)才证明五次和五次以上的一般代数方程没有求根公式。但是人们仍然不知道什么条件之下一个已知的多项式能借助加、减、乘、除有理运算以及开方的方法求出它的所有根,什么条件之下不能求根。

最终解决这一问题的是一位法国年青数学家E.Galois(1811—1832)，Galois引入了扩域以及群的概念，并采用了一种全新的理论方法发现了高次代数方程可解的法则。在Galois之后群与域的理论逐渐成为现代化数学研究的重要领域，这是近世代数产生的一个最重要的来源。

埃瓦里斯特·伽罗瓦



埃瓦里斯特·伽罗瓦(1811年10月25日—1832年5月31日)
法国著名数学家

1. 他的第一篇论文寄到法兰西科学院数学家柯西审稿,未能及时作出评价,以致连手稿也给遗失了;
2. 十八岁的伽罗瓦又取得了一些重要成果,再次写成论文寄交科学院,主持审稿傅立叶在举行主持审稿例会的前几天病世了;
3. 第三次写成论文,即《关于用根式解方程的可解性条件》。1831年,法兰西科学院第三次审查伽罗瓦的论文,主持这次审查的是科学院院士波松。最后一次得到波松草率的评语:“不可理解”而被否定了。

第三章 群

3.1 二元运算

定义3.1.1 设A为集合，一个映射$f: A \times A \to A$称为集合A上的代数运算或二元运算。

一个集合A上的二元运算必须满足以下条件：

- 可运算性：即A中的任何两个元素都可以进行这种运算；
- 单值性：即A中的任何两个元素的运算结果是惟一的；
- 封闭性：即A中的任何两个元素运算的结果都属于A。

注：一个代数运算一般可用“$\circ$”、“$\cdot$”、“$+$”、“$\times$”符号来表示。

假设f是集合A上的一个代数运算，$f(x,y)=z$，则可写成$z=x\circ y$。

3.1 二元运算

例3.1.1

（1）整数集合Z上的加法运算是代数运算，满足代数运算的3个性质。

（2）自然数集合N上的减法运算不是代数运算，因为它不满足封闭性。

定义3.1.2 设“$\circ$”是A上的代数运算，如果对于A中的任意 三个元素a, b, c都有

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

则称“$\circ$”在集合A上满足结合律。

3.1 二元运算

定义3.1.3 设“$\circ$”是A上的代数运算，如果对于A中的任意两个元素a, b ,都有

$$a \circ b = b \circ a$$

则称“$\circ$”在集合A上满足交换律。

例3.1.2

整数集合Z上的加法运算满足结合律和交换律，同样，整数集合Z上的乘法运算也满足结合律和交换律。

定义3.1.4 设“$\circ$”和“$+$”是A上的两个代数运算，如果对于A中的任意三个元素a,b,c都有

$$a\circ(b+c)=a\circ b+a\circ c$$

$$(b+c)\circ a=b\circ a+c\circ a$$

则称“$\circ$”对“$+$”在集合A上满足分配律。

例3.1.3

整数集合Z上的乘法对加法满足分配律，而加法对乘法不满足分配律。

第三章 群

3.2 二元运算群的定义和简单性质

定义3.2.1 设G是一个具有代数运算$\circ$非空集合，并且满足：

（1）结合律：$\forall a, b, c \in G$，有

$$(a \circ b) \circ c = a \circ (b \circ c) \;;$$

（2）有单位元。即G中存在一个元素e :$\forall a \in G$，有

$$e \circ a = a \circ e = a$$

（3）有逆元。即对于任意$a \in G$，存在一个元素$a^{-1} \in G$，使得

$$a \circ a^{-1} = a^{-1} \circ a = e$$

称非空集合G关于代数运算$\circ$构成一个群。

例3.2.1

（1）全体整数 Z 对于通常的加法成一个群，这个群称为**整数加群**，在整数加群中，单位元是0，a 的逆元是 $-a$；同样全体有理数集合 Q，全体实数集合 R，全体复数集合 C 对加法也构成群。

（2）全体非零实数 R^* 对于通常的乘法构成一个群，全体正实数 R^+ 对于通常的乘法也构成一个群。

（3）模正整数 n 的最小非负完全剩余系 Z_n，对于模 n 的加法构成一个群，这个群称为**整数模 n 加群**，其单位元为0，a 的逆元是 $n-a$。

（4）元素在数域P中的全体n级**可逆矩阵对于矩阵的乘法**构成一个群，这个群记为 $GL_n(P)$，称为**n级一般线性群**。

群 G 的一些基本性质

1.单位元惟一：

G中存在唯一的元素e，使得对于所有的$a \in G$，有

$$e \circ a = a \circ e = a$$

证明：由群的定义可知，单位元e满足上述性质。假定还有另一个e'也满足上述性质，即

$$e'a = ae' = a$$

则有 $ee' = e = e'$

群G的一些基本性质。

2、逆元惟一:

对于群G中的任意一元素a，存在唯一元素$b \in G$，使得

$$ab = ba = e$$

证明：由群的定义可知，对于任意一元素$a \in G$，存在G中的一个元素是a的逆元，不妨设为b。假定再有一个元素c也具有性质

$$ca = ac = e$$

则有

$$c = ce = c(ab) = (ca)b = eb = b$$

3.2 二元运算群的定义和简单性质

3、消去律成立：

设a, b, c是群G中的任意三个元素，则

（1） 若$ab = ac$，则$b = c$；

（2） 若$ba = ca$，则$b = c$。

证明：假定$ab = ac$ ，那么

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

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

$$eb = ec$$

$$b = c$$

同理，由 $ba = ca$ 可得$b = c$。

4. 一次方程解惟一：

对于群G中的任意元素a,b，方程

$$ax = b和xa = b$$

在群G中有唯一解。

证明：显然，$x = a^{-1}b$是方程 的解，因而有解。假设x_1, x_2是方程的两个解，则有

$$ax_1 = ax_2$$

根据消去律即可得$x_1 = x_2$ 。这就证明了唯一性。

同理可证，方程$xa = b$在G中有唯一解。

5、对于群G中的任意元素a,b，都有

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

证明：由于

$$abb^{-1}a^{-1}=b^{-1}a^{-1}ab=e$$

所以

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

3.2 二元运算群的定义和简单性质

定理3.2.1 设G为一非空集合，G上乘法封闭且满足结合律。若对于任意$a,b\in G$，方程

$$ax=b \text{ 和 } ya=b$$

在G中有解，则G是群。

证明：

(1) 有单位元：对G中任意一个固定元素b设方程$yb=b$在G中的解用e表示，即有$eb=b$。

再任取$a\in G$, 设方程$bx=a$在G中的解为c，即有

$$bc=a$$

于是

$$ea=e(bc)=(eb)c=bc=a,$$

（即e是左单位元）

同理可证：G 存在右单位元e'，即：$\forall a \in G$ 有$ae' = a$。
因此，$e = ee' = e'$
即e 是G 的单位元。
（2）逆元： 对G中任意元素a，由于方程

$$ya = e$$

在G中有解a'，即a在G 中有左逆元a'。
同理可证：$\forall a \in G$存在右逆元a''
又 $a'' = ea'' = (a'a)a'' = a'(aa'') = a'e = a'$
因此，$\forall a \in G$有逆元。（证毕）

3.2 二元运算群的定义和简单性质

有限群和无限群

定义3.2.2 若群G中只含有有限个元素，则称群G为有限群；若群G中含有无限多个元素，则称群G为无限群。一个有限群G中的元素个数称为群的阶，记为$|G|$。

例3.2.1中的（1）（2）都是无限群，而整数模n加群Z_n为有限群，且$|Z_n| = n$。

有限群的判定

定理3.2.2 一个有乘法的有限集合G，若其乘法在G中封闭，且满足结合律和消去律，则G是群。

证明思路：（定理3.2.1）对于G中的任意元素$a,b\in G$，方程

$$ax=b \text{ 和 } xa=b$$

在G中有解，则G是群。

证明：假定G中有n个元素，不妨设这n个元素为$a_1,a_2,\cdots,a_n$

用a左乘所有的a_i，可做成集合$G'=\{aa_1,aa_2,\cdots,aa_n\}$

有限群的判定

定理3.2.2 的证明（续）：

由于乘法在G上封闭，所以$G' \subseteq G$。

但当$i \neq j$的时候，$aa_i \neq aa_j$。不然的话，由消去律可知，$a_i = a_j$与假定不合。因此G'有n个不同的元素，所以有$G' = G$。

这样，对于方程中的b，必然存在某个k，使得$b = aa_k$，
也就是说方程$ax = b$在G中有解。

同理可证，方程$xa = b$在G中也有解。

根据定理3.2.1，G是群。

例3.2.2 取模m的最小非负简化剩余系，记为Z_m^*，其中元素个数为$\varphi(m)$个，定义其上的乘法为模m的乘法。显然其乘法在Z_m^*上封闭，且满足结合律。由定理2.2.7可知，Z_m^*中的元素均存在模m的乘法逆元。对于任意$a, b, c \in Z_m^*$，若

$$ab \equiv ac(\mathrm{mod} m)$$

则有

$$a^{-1}ab \equiv a^{-1}ac(\mathrm{mod} m)$$

即$b \equiv c(\mathrm{mod} m)$。因此，模$m$的乘法在$Z_m^*$上满足消去律。根据定理3.2.2，$Z_m^*$是群。