信息安全数学基础

第八章 群

中山大学 数据科学与计算机学院

抽象代数的基本概念

- 抽象代数（近世代数）的研究对象是代数系统,即集合以及定义在其上的一个或若干个代数运算构成的系统.
- 挪威数学家阿贝尔(Abell), 法国数学家伽罗瓦(Galois), 英国数学家摩根(Mogrgan)和布尔(Boole)等人都为抽象代数的开创做出了杰出贡献.
- 荷兰数学家范德瓦尔登(V • Derwaerden), 根据德国数学家诺特(Noether)和奥地利数学家阿廷(Artin)的讲稿, 于1930年和1931年分别出版了《近世代数学》一卷和二卷, 标志着抽象代数的成熟.
- 当今, 抽象代数已成为信息科学的最重要数学基础之一, 在信息论与编码, 以及密码学方面有广泛而深刻的应用.
- 基于抽象代数发展出来的其他数学分支, 例如, 代数数论和代数几何, 也在信息科学有深刻的应用.
- 另外, 抽象代数在近代物理和近代化学等许多自然科学领域都有重要应用, 因而它也是现代科学技术的数学基础之一, 许多非数学专业的科技研究人员也都需要用到它.

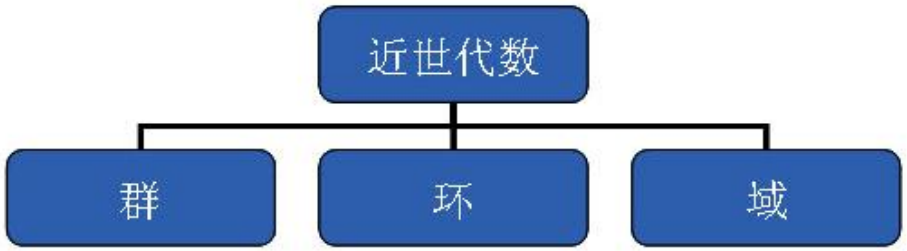
代数系统

整数集合$\mathbb{Z}$以及定义在这个集合上的整数加法$+$一起构成了一个代数系统$(\mathbb{Z}, +)$, 被称为一个群.

整数集合$\mathbb{Z}$以及定义在这个集合上的整数加法$+$和整数乘法$\times$一起构成了一个代数系统$(\mathbb{Z}, +, \times)$, 被称为一个环.

有理数集合$\mathbb{Q}$以及定义在这个集合上的整数加法$+$和整数乘法$\times$一起构成了一个代数系统$(\mathbb{Z}, +, \times)$, 被称为一个域.

抽象代数的最核心的内容包括: 群(group), 环(ring), 域(field)等代数系统.



2.1 集合的概念

- 若干固定事物的全体叫做集合, 用A, B, C, X等表示
- 固定事物称为元素, 用a, b, c, x, y等表示
- 有限集, 无限集
- 集合中元素个数用$|A|$表示
- 子集: 若集和A中的元素都为集合B中的元素, 则称集合A是集合B的一个子集. 记作: $A \subseteq B$
- 集合的运算: 相等, 交集, 并集, 差集

2.2 映射

- 映射
  设X与Y是两个集合, 如果有一个法则f, 它对于X中每一个元素x, 在Y中都有一个唯一确定的元素y与它对应, 则称f为X到Y的一个映射. 表示为

  $$f : x \to y,$$

  或着$y = f(x)$, 并且y叫做x在映射f下的像, 而x叫做y在映射f下的原像.

- 单射
  $f : A \to B$, 若任给$x_1, x_2 \in A, x_1 \neq x_2$则: $f(x_1) \neq f(x_2)$

- 满射$f : A \to B$, 若任给$y \in B$, 都有$x \in A$使$y = f(x)$

- 双射(一一映射)
  即为单射又为满射

2.3 笛卡尔乘积

- 序偶(ordered pair)
  由两个有固定次序的个体x, y组成的序列称为序偶, 记为$< x, y >$, x是序偶的第一个分量, y是序偶的第二个分量.
- 笛卡尔乘积
  给定两个集合A, B, 若序偶的第一个分量是A的一个元素,序偶的第二个分量是B的一个元素, 则所有这样的序偶的集合称为A与B的笛卡尔(乘)积, 简称卡氏积, 记为$A \times B$, 即$A \times B = \{< x, y > | x \in A \wedge y \in B\}$
- 卡氏阵
  若A, B为有限集, 比如$A = \{a_1, \cdots, a_m\}$, $B = \{b_1, \cdots, b_n\}$则$A \times B$的元素可排成一个矩阵(称为卡氏阵):

$$\begin{bmatrix} < a_1, b_1 > & < a_1, b_2 > & \cdots & < a_1, b_n > \\ < a_2, b_1 > & < a_2, b_2 > & \cdots & < a_2, b_n > \\ < a_3, b_1 > & < a_3, b_2 > & \cdots & < a_3, b_n > \\ & \cdots & & \\ < a_m, b_1 > & < a_m, b_2 > & \cdots & < a_m, b_n > \end{bmatrix}_{m \times n}$$

2.4 代数系统

- 运算
  A是集合,f是从A^2到A的一个函数: $f : A^2 \to A$, 则称f是集合A上的一个二元运算, 即自变量有2个.
- 代数系统
  A是集合, $f_1, f_2, \cdots, f_k$是若干定义在A上的运算, 则由A和$\{f_1, f_2, \cdots, f_k\}$组成的系统称为代数系统, 记为$< A, f_1, \cdots, f_k >$.

  例: 代数系统$< \mathbb{Z}, + >$, $< \mathbb{Z}, +, \times >$和$< \mathbb{Q}, +, \times >$.

3. 半群与群

- 半群
  设$\mathbb{G}$是一个非空集合, '$\bullet$'是$\mathbb{G}$上的一个二元运算, 即$\bullet : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$). 如果'$\bullet$'满足:
  结合律: 若对任意$x, y, z \in \mathbb{G}$, 均有$(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
  则称'$\bullet$'在$\mathbb{G}$上是可结合的, 则称$(\mathbb{G}, \cdot)$是一个半群, 简称$\mathbb{G}$是一个半群.

- 含么半群
  设$(\mathbb{G}, \cdot)$是一个半群, 如果对于'$\bullet$', 存在一个元素$e \in \mathbb{G}$, 使得对任意$x \in \mathbb{G}$, 均有

$$e \cdot x = x, x \cdot e = x,$$

  则称$(\mathbb{G}, \cdot)$是一个含么半群, 简称$\mathbb{G}$是一个含么半群.
  这个特殊的元素e称为单位元, 或么元.

- 群(Group)
  设$(\mathbb{G},\cdot)$是一个含么半群, 对于'$\bullet$', 如果对于所有$a\in\mathbb{G}$, 都存在元素$b\in\mathbb{G}$, 使得

$$a\cdot b=b\cdot a=e,$$

  则称$(\mathbb{G},\cdot)$是一个群, 简称$\mathbb{G}$是一个群. b称为a的逆元, 记作a^{-1}.

  可以看到如果b是a的逆元, 则a也是b的逆元, 即$b=a^{-1}, a=b^{-1}$; a与b互逆.

  可以看到, 群的定义包含4点: 封闭性,结合律,单位元,逆元.
  可以证明, 群具有消去率: $ax=ay\Rightarrow x=y$; $xa=ya\Rightarrow x=y$

- 群的两个性质:
  设$(\mathbb{G},\cdot)$是一个群, 则其单位元e是唯一的.
  设$(\mathbb{G},\cdot)$是一个群, 则对任意可逆元a，其逆元是唯一的.

- 交换群
  设$(\mathbb{G},\cdot)$是一个群, 对于'$\bullet$', 如果对于所有$a,b\in\mathbb{G}$, 都有$a\cdot b=b\cdot a$, 则称$(\mathbb{G},\cdot)$是一个交换群,简称$\mathbb{G}$是一个交换群(abel群).

线性群

设$M_n(F)$是数域F上的全体n阶矩阵的集合, 则$M_n(F)$对矩阵的加法构成群. 但对矩阵的乘法是半群而不是群.

设$GL_n(F)$是数域F上全体可逆矩阵的集合, 则$GL_n(F)$对矩阵的乘法构成群, 这个群称为F上的n次全线性群, 因为每个n阶可逆矩阵对应域n维线性空间中的一个可逆变换, 所以$GL_n(F)$可以看作是F上n维线性空间上全体可逆线性变换的集合

对称群

定义

设S是一个非空集合. $\mathbb{G}$是S到自身的所有双射f组成的集合. 对于$f, g \in \mathbb{G}$和任意的$x \in S$, 定义f和g的复合映射$g \circ f$ 为

$$(g \circ f)(x) = g(f(x)),$$

则$\mathbb{G}$对于映射的复合运算构成一个群, 叫做对称群. 恒等映射是单位元. $\mathbb{G}$中的元素叫做S的一个置换.

定义

当S是n元有限集合时, $\mathbb{G}$叫做n元对称群, 记作S_n.

置换群

设有限集合$A=\{1,2,\cdots,n\}$, 则A上的置换可以表示为:

$$f=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix},$$

其中$i_1,i_2,\cdots,i_n$是一个n级全排列, 这样的所有置换构成一个n次对称群, 记作S_n.
由n级全排列的个数知$|S_n|=n!$

例如, S_3共有$3!=6$个元素, 它们是:

$$\sigma_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}\sigma_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\sigma_3=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

$$\sigma_4=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\sigma_5=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\sigma_6=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

二面体群

设X为正$n(n \geq 3)$边形的顶点集合, 且按照逆时针方向排列. 将正多边形绕中心o逆时针方向旋转

$$2\pi/n$$

角度, 则顶点i变为顶点$(i+1) \bmod n$的位置, 这个旋转是X上的一个置换, 记作ρ_1, 可以表示为:

$$\rho_1 = \begin{pmatrix} 0 & 1 & 2 & \cdots & n-1 \\ 1 & 2 & 3 & \cdots & 0 \end{pmatrix}.$$

逆时针方向旋转$2k\pi/n$角度, 记作ρ_k, 可以表示为:

$$\rho_k = \begin{pmatrix} 0 & 1 & 2 & \cdots & n-1 \\ k & k+1 & k+2 & \cdots & k+n-1 \end{pmatrix}$$

其中$k = 0, 1, 2, \cdots, n-1$.

此外, 逆时针方向旋转0角度ρ_0为单位变换, ρ_k还可以表示为:

$$\rho_k(i) = (k+i), \quad i = 0, 1, \cdots, n-1$$

在X为正$n(n \geq 3)$边形的顶点集合中, 一个重要的变换(映射)是绕对称轴翻转π角度, 这类变换为反射变换.

这样的对称轴一共有n个. 记过顶点0的轴为l_0, 过边$(0,1)$中点的轴为l_1, 过顶点1的轴为l_2, 过边$(1,2)$中点的轴为$l_3, \cdots$, 直到l_{n-1}. 相应的反射变换记作$\pi_0, \pi_1, \cdots, \pi_{n-1}$. 例如:

$$\pi_0 = \begin{pmatrix} 0 & 1 & \cdots & n-1 \\ 0 & n-1 & \cdots & 1 \end{pmatrix}.$$

不难证明:

$$\pi_k(i) = k + n - i.$$

由此还可以证明如下的运算关系:

$$\rho_k = \rho_1^k, \pi_k^2 = \rho_0, \rho_k^{-1} = \rho_{n-k}$$

$$\pi_k^{-1} = \pi_k, \rho_k \rho_l = \rho_{k+l}, \rho_k \pi_l = \pi_{k+l}$$

$$\pi_k \rho_l = \pi_{k-l}, \pi_k \pi_l = \rho_{k-l}$$

令$D_n = \{\rho_k, \pi_k : k = 0, 1, 2, \cdots, n-1\}$, 则$D_n$对变换的复合是封闭的,有单位元$\rho_0$, 每个元素都有逆元. 所以$D_n$是群, 称为二面体群.

剩余类群

$$\mathbb{Z}_n = \{C_0, C_1, C_2, \cdots, C_{n-1}\},$$

即模n的剩余类构成的集合,在该集合上定义加法(模n加法):

$$C_a + C_b = C_{a+b}.$$

模n剩余类的加法满足

- 封闭性
- 结合律
- 有单位元C_0
- 所以每个元素都有逆元, $C_a + C_{n-a} = C_0$,
- 可交换

于是, $(\mathbb{Z}_n, +)$是交换群.

一般直接写$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$, 对应的加法则写为$a + b \triangleq (a + b \bmod n)$.
这样的$(\mathbb{Z}_n, +)$与上意义相同, 且$(\mathbb{Z}_n, +)$一般直接写为$\mathbb{Z}_n$.

剩余类群

考虑模n的简化剩余系

$$\mathbb{Z}_n^* = \{C_k : C_k \in \mathbb{Z}_n, (k,n) = 1\},$$

以及在其上定义的乘法$C_a \times C_b \triangleq C_{ab}$.

模n简化剩余系的乘法满足

- 封闭性: $C_a, C_b \in \mathbb{Z}_n^+ \Rightarrow C_{ab} \in \mathbb{Z}_n^+$
- 结合律:
  $C_a \times (C_b \times C_c) = C_a \times C_{bc} = C_{a(bc)} = C_{(ab)c} = C_{ab} \times C_c = (C_a \times C_b) \times C_c$
- 有单位元C_1
- 有逆元, $\forall C_a \in \mathbb{Z}_n^+ \Rightarrow (a,n) = 1 \Rightarrow \exists (b,n) = 1 : ab \equiv 1 \bmod n \Rightarrow C_{ab} = C_1 \Rightarrow C_a \times C_b = C_1$
- 可交换: $C_a \times C_b = C_{ab} = C_{ba} = C_b \times C_a$

类似地, $\mathbb{Z}_n^*$一般直接写成$\{k : k \in \mathbb{Z}, (k,n) = 1\}$, 而$C_a \times C_b$写成$a \times b \triangleq (ab \bmod n)$.
这个群中元素个数显然为$\varphi(n)$.

群的基本概念小结

- 半群: 封闭性, 结合律.
- 含么半群: 含单位元的半群.
- 群: 封闭性, 结合律, 单位元, 逆元.
- 交换群: 群运算具有交换律.
- 线性群: 群元素是矩阵, 群运算是矩阵乘.
- 对称群: 群元素是非空集合S中的双射, 群运算是映射的复合.

群的阶，加法群中的零元和负元，群元素的幂

- 群的阶
  设$(\mathbb{G},\cdot)$是一个群. 如果$\mathbb{G}$是一个有限集合, 则称$\mathbb{G}$为有限群, 否则成为无限群. $\mathbb{G}$中的元素个数$|\mathbb{G}|$称为该群的阶.
- 群中特殊元素
  经常把交换群中的运算称为加法运算, 所以交换群又称为加群. 其中的单位元被称为零元, 记作0, 其中任意元素x的逆元x^{-1}被称为负元, 记作$-x$.
- 元素的幂(对应地,倍数)
  在一个代数系统(一般讨论的是群)$(\mathbb{G},\cdot)$中, 元素a的幂a^n(n为正整数)定义为

$$a^n = \underbrace{a\cdot a\cdot a\cdot a\cdots a}_{n}$$

  约定: $a^0 = e$,
  特别地, 如果某两个元素a,b满足$ab=ba$,则$(ab)^n = a^n b^n$

有限群举例

- 集合$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$关于模5的加法构成了一个有限群, 并且除去元素0后关于模5的乘法也构成一个有限群.

有限群举例

- 集合$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$关于模5的加法构成了一个有限群, 并且除去元素0后关于模5的乘法也构成一个有限群.
- 集合$\mathbb{Z}_{26} = \{0, 1, 2, \cdots, 25\}$关于模26的加法构成了一个有限群, 而除去元素0后关于模26的乘法不构成一个群.

有限群举例

- 集合$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$关于模5的加法构成了一个有限群, 并且除去元素0后关于模5的乘法也构成一个有限群.
- 集合$\mathbb{Z}_{26} = \{0, 1, 2, \cdots, 25\}$关于模26的加法构成了一个有限群, 而除去元素0后关于模26的乘法不构成一个群.
- 如果p是素数, 那么集合$\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$关于模$p$的加法构成了一个有限群, 并且除去元素0后关于模$p$的乘法也构成一个群.

有限群举例

- 集合$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$关于模5的加法构成了一个有限群, 并且除去元素0后关于模5的乘法也构成一个有限群.
- 集合$\mathbb{Z}_{26} = \{0, 1, 2, \cdots, 25\}$关于模26的加法构成了一个有限群, 而除去元素0后关于模26的乘法不构成一个群.
- 如果p是素数, 那么集合$\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$关于模$p$的加法构成了一个有限群, 并且除去元素0后关于模$p$的乘法也构成一个群.
- 如果$n = pq$, 那么集合$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$关于模$n$的加法构成了一个有限群, 而除去元素0后关于模$p$的乘法不构成一个群.

4. 逆元的简单性质

在一个群$(\mathbb{G}, \cdot)$中,

- $(a^{-1})^{-1} = a$
- $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
  因为$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$
- $(a^n)^{-1} = (a^{-1})^n$
  这是因为
  $a^n \cdot (a^{-1})^n$
  $= (\underbrace{a \cdot a \cdot a \cdot a \cdots a}_{n}) \cdot (\underbrace{a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n})$
  $= (\underbrace{a \cdot a \cdot a \cdot a \cdots a}_{n-1}) \cdot (a \cdot a^{-1}) \cdot (\underbrace{a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n-1})$
  $= (\underbrace{a \cdot a \cdot a \cdot a \cdots a}_{n-1}) \cdot e \cdot (\underbrace{a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n-1})$
  $= (\underbrace{a \cdot a \cdot a \cdot a \cdots a}_{n-1}) \cdot (\underbrace{a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n-1})$
  $= e$
- $(a^{-1})^n$经常记作a^{-n}.

4. 逆元的简单性质

定理

G是一个非空集合,定义了有结合律的二元运算, a, b是G中任意两个元素. 如果G是一个群, 则方程

$$ax = b, ya = b$$

有解. 反之,如果上述方程在G中有解, 则G是一个群.

证明: 设G是一个群, 则

$$a^{-1}ax = a^{-1}b \to x = a^{-1}b.$$

设上述方程有解. 则方程$ax = a$有解, 从而有单位元. 同时, 方程$ax = e$也有解. 所以G中有单位元, 每个元素都有逆元, 所以G是一个群.