# 第6章 近世代数基础

# 引子

抽象代数亦称近世代数, 是在初等代数基础上的推广, 从18世纪末萌芽到20世纪30年代, 逐步形成现代数学的主要分支之一. 抽象代数作为数学的一门学科, 主要研究对象是代数结构, 比如群、环、域、模、向量空间和代数等.

这一章介绍的近世代数基础知识, 目标是本科学生能理解高级加密标准即AES算法. 在介绍相关知识时, 会尽量减少概念的引入, 比如关于群的半群、子群、陪集、商群等, 关于环的子环、理想甚至商环等, 有限域部分也仅仅是给出了概念.

# 6.1 群

群是一种代数系统, 对群的理论研究是由法国的数学家伽罗瓦开创的, 是为了解决一般的高次代数方程是否存在二次方程那样的求根公式, 即“为什么五次及更高次的代数方程没有一般的代数解法？ 也就是说, 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.”这个问题而产生的.

# 二元运算

【定义6.1.1】集合$G$中的**二元运算**是一个如下的函数:

$\mathrm{o}: G \times G \to G$

也就是说, 集合$G$中的二元运算, 就是为有序对$(a, b)$分配一个确定的元素$c$与之对应, 即: $a\mathrm{o}b = c$. 这里的o可以是数学运算中的加法、减法、乘法、除法或者异或等运算符号, 也可以是重新定义的运算符号.

# 结合律

【定义6.1.2】 设$\circ$是集合$G$中的二元运算，若对集合$G$中的任意元素$a, b, c$，都有$(a\circ b)\circ c = a\circ(b\circ c)$，则称二元运算$\circ$满足结合律.

通常意义上的加法和乘法满足结合律，减法和除法不满足结合律. 例如$(5+3)+7=5+(3+7)$，但$(5-3)-7\neq 5-(3-7)$.

# 交换律

【定义6.1.3】 设o是集合$G$中的二元运算，若对集合$G$中的任意元素a, b，都有$a\text{o}b = b\text{o}a$，则称二元运算o满足交换律.

通常意义上的加法和乘法满足结合律和交换律，减法和除法不满足结合律和交换律. 例如$5 + 3 = 3 + 5$，但$5 - 3 \neq 3 - 5$.

# 群的定义

设$G$为非空集合，在$G$内定义了一种代数运算为o，若满足下述公理：

（1）有封闭性．对任意$a, b \in G$，恒有$a\text{o}b \in G$.

（2）结合律成立．对任意$a, b, c \in G$，有$(a\text{o}b)\text{o}c = a\text{o}(b\text{o}c)$;

（3）$G$中有一恒等元$e$存在，对任意$a \in G$，有$e \in G$，使$a\text{o}e = e\text{o}a = a$;

（4）对任意$a \in G$，存在$a$的唯一逆元$a^{-1} \in G$，使$a\text{o}a^{-1} = a^{-1}\text{o}a = e$,

则$< G, \text{o} >$构成一个群.

# 交换群或者阿贝尔群.

在不引起混淆的情况下，也可以称$G$为群.

若群$G$满足交换律，则称群$G$为交换群或者阿贝尔群.

若群中的运算为加法，恒等元通常也称为零元；若群中的运算为乘法，恒等元通常也称为单位元、幺元.

# 伽罗瓦

【人物传记】 埃瓦里斯特·伽罗瓦（法语: Évariste Galois, 1811-1832），法国的数学家, 他发现了$n$次多项式可以用根式解的充要条件, 解决了长期困扰数学界的问题. 他的工作为伽罗瓦理论以及伽罗瓦连接领域的研究奠定了基石, 他是第一个使用群这一个数学术语来表示一组置换的人, 与阿贝尔并称为现代群论的创始人。

# 阿贝尔

【人物传记】尼尔斯·亨利克·阿贝尔（Niels Henrik Abel，1802－1829）, 挪威数学家, 以证明五次方程的根式解的不可能性和对椭圆函数论的研究而闻名. 跟同样早逝的伽罗华一同被奉为群论的先驱, 现代有以他名字命名的阿贝尔奖。

# 群-例题

【例6.1.1】 设$n$是一个正整数, 令

$Z=\{\dots,-n,\dots,-2,-1,0,1,2,\dots,n,\dots\}$, 即$Z$是所有整数的集合. 对于通常意义的加法(+), 集合$Z$满足:

（1）封闭性, 即整数与整数相加, 结果仍然是整数, 封闭性成立;

（2）结合律, 对于元素$a,b,c\in Z$, $(a+b)+c=a+(b+c)$, 结合律成立;

（3）存在零元0, 对于元素$a\in Z$, 有$a+0=0+a=a$;

（4）每个元素$a$的逆元为$-a$, $a+(-a)=0$.

故$Z$是一个群.

由于通常意义的加法(+)满足交换律, 故该群是一个交换群.

# 群-例题

【例6.1.2】 非零集合$Z^* = Z\backslash\{0\}$对于通常意义的乘法($\times$)满足封闭性、结合律, 存在单位元1, 但不是每个元素都有逆元, 例如找不到元素$a \in Z$, 使得$2 \times a = a \times 2 = 1$, 也即2的逆元不存在. 故$Z^*$不是一个群.

【例6.1.3】 设$n$是一个正整数, 令$Z/nZ = \{0,1,2,3, \ldots, n-1\}$, 也即模$n$的最小非负完全剩余系, 则集合$Z/nZ$对于加法:

$$a \oplus b = a + b \pmod n$$构成一个交换群.

例如, $n=11$时, 令$G=Z/nZ=\{0,1,2,3,4,5,6,7,8,9,10\}$, 对于集合中的元素$a,b$, 定义加法运算为:

$$a \oplus b = a + b (\operatorname{mod} n)$$

则$< G,\oplus >$构成一个群, 且是交换群. 下面看看$< G,\oplus >$满足公理的情况.

（1）封闭性. 对任意$a,b \in G$, 恒有$a \oplus b (\operatorname{mod} 11) \in G$. 例如, $8 \oplus 9 = 17 \equiv 6 (\operatorname{mod} 11) \in G$, 满足封闭性性质.

（2）结合律成立. 对任意$a,b,c \in G$, 有$(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

（3）恒等元存在, $G$中恒等元$e=0$, 对任意$a \in G$, 有$e \in G$, 使$a+e=e+a=a$.

（4）对任意$a \in G$,存在$a$的唯一逆元$a^{-1} \in G$, 使$a+a^{-1}=a^{-1}+a=e$. 例如, 7在集合中的逆元为4, 因$7 \oplus 4 (\operatorname{mod} 11) \equiv 0$.

显然, 加法满足交换律, 故该群是交换群.

特别地, 当n=2时, $<Z_2,\oplus>$也是一个交换群.

# 群-例题

【例6.1.4】 设$p$是一个素数, $F_p = Z/pZ = \{0,1,2,3,\ldots,p-1\}$, $F^* = F_p \backslash \{0\}$, $F^*$是模$n$的最小非负简化剩余系. 则集合$F^*$对于乘法:

$$a \otimes b = a \times b (\bmod n)$$

构成一个交换群.

例如$p=11$时, $F^*$={ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}, , 定义该集合中的运算为:

$$a \otimes b = a \times b (\bmod 11)$$

其中$a, b$为集合中的元素. 则$F^*$是一个群, 且是交换群. 下面看看{ $F^*$,$\otimes$}满足公理的情况.

(1) 封闭性. 对任意$a, b \in F^*$, 恒有$a \otimes b (\bmod 11) \in F^*$. 例如$8 \otimes 9 = 72 \equiv 6 (\bmod 11) \in F^*$.

(2) 结合律成立. 对任意$a, b, c \in G$, 有

$$(a \otimes b) \otimes c = a \otimes (b \otimes c).$$

(3) 恒等元存在, 恒等元$e=1$. 即对任意$a \in F^*$, 有$e \in F^*$, 使

$$a \otimes e = e \otimes a = a.$$

(4)对任意$a \in F^*$, 存在$a$的逆元$a^{-1} \in F^*$, 使$a \otimes a^{-1} = a^{-1} \otimes a = e$. 例如: 7在集合中的逆元为8, 因$7 \otimes 8 (\bmod 11) \equiv 1$.

显然, 乘法满足交换律, 故该群是交换群.

特别地, 当$n=2$时, <$Z_2^*$,$\otimes$>也是一个交换群. 实际上, $Z_2^* = \{1\}$, 该集合中只有一个元素1.

# 群-例题

【例6.1.5】 设$n$是一个正合数，$Z_n = \{0,1,2,3,\dots,n-1\}$，则集合$Z_n\backslash\{0\}$对于乘法：

$$a \otimes b = a \times b (\bmod n)$$

不构成一个交换群，因为$n$的真因数没有逆元.

例如，$n = 10$，则$2^{-1} (\bmod 10)$不存在，因2与10不互素.

# 群-例题

【例6.1.6】设$n$是一个正合数，$Z_n = \{0,1,2,3,\ldots,n-1\}$，令$Z_n^* = (Z/nZ)^* = \{a|a \in Z_n, (a,n) = 1\}$，也即模$n$的最小非负简化剩余系. 则集合$Z_n^*$对于乘法:

$$a \otimes b = a \times b(mod n)$$

构成一个交换群.

例如$n = 10$，则$(Z/nZ)^* = \{1,3,7,9\}$，即模10的最小非负简化剩余系，运算封闭，满足结合律，单位元为1，每个元素存在逆元.

可以看出，群和群的例子，就犹如面向对象编程中的类和类的实例.

# 6.1.2 循环群

【定义6.1.5】 设<$G$, o>是群, $a \in G, n \in Z$, 则$a$的幂定义为:

$a^n = a \circ a \circ \ldots \circ a$;

$a^{-n} = a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1}$;

$a^0 = e$.

例如, 在群$< Z_3, \oplus >$中, 定义$a \oplus b = a + b \pmod 3$, 则

$2^0 = 0$,

$2^3 = 2 \oplus 2 \oplus 2 = 2 + 2 + 2 \pmod 3 \equiv 0$,

$2^{-3} = (2^{-1})^3 = 1^3 = 1 + 1 + 1 \pmod 3 \equiv 0$.

# 阶

【定义6.1.6】 设$<G, \circ>$是群, $a \in G$, 使得等式$a^k = e$成立的最小正整数$k$称为$a$的阶, 记作$|a| = k$, 也称$a$为$k$阶元. 若不存在这样的正整数$k$使得$a^k = e$成立, 则称$a$为无限阶元. 若集合$G$的元素个数有限, 则其元素个数称为群$G$的阶.

# 阶-例题

【例6.1.7】 在$<Z_6, \oplus>$中，该群有6个元素，故群的阶为6.

2和4是3阶元，因为

$$2^3 = 2 \oplus 2 \oplus 2 = 2 + 2 + 2 \pmod 6 \equiv 0$$

$$4^3 = 4 \oplus 4 \oplus 4 = 4 + 4 + 4 \pmod 6 \equiv 0$$

3是2阶元，因为$3^2 = 3 \oplus 3 = 3 + 3 \pmod 6 \equiv 0$.

1和5是6阶元，例如

$$5^6 = 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5$$
$$= 5 + 5 + 5 + 5 + 5 + 5 \pmod 6 \equiv 0$$

0是1阶元.

# 阶-例题

【例6.1.8】 在$<Z_{11}^*, \otimes>$中，该群有10个元素，故群的阶为10.

由第5章的知识易得，2是模11的生成元，故 $2^3=8$, $2^7\equiv7$, $2^9\equiv6 \pmod{11}$也为模11的生成元，它们都是10阶元.

由【定理5.1.4】，$2^2=4$, $2^4\equiv5$, $2^6\equiv9$, $2^8\equiv3 \pmod{11}$模11的指数为5，它们是模11的5阶元.

$2^5\equiv10 \pmod{11}$ 模11的指数为2，它是模11的2阶元.

# 阶-例题

【定理6.1.1】 设<$G$, o>为群, 则群中任何元素$a$与其逆元$a^{-1}$具有相同的阶.

例如【例6.1.7】中, 2和4互为逆元, 它们的阶都为3. 1和5互为逆元, 它们的阶都为6. 3和3互为逆元, 阶都为2.

例如【例6.1.8】中, 2和6互为逆元, 它们的阶都为10. 7和8互为逆元, 它们的阶都为10. 3和4互为逆元, 它们的阶都为5. 5和9互为逆元, 它们的阶都为5. 10的逆元为自身, 它的阶为2.

在【性质5.1.1】中描述为：$\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$.

# 生成元

【定义6.1.7】 设$<G, \circ>$为群, 如果存在一个元素$a \in G$, 使$G = \{a^k | k \in Z\}$, 则称$G$为循环群, 记作$G =< a >$, 称$a$是$G$的生成元.

也就是说, 群$G$的每一个元素都能表示为元素$a$的幂.

循环群都是交换群, 循环群的生成元也可以不止一个.

如果$a$的阶为$n$, 即$a^n = e$, 那么这时$G =< a >=< 1, a, a^2, \ldots\ldots, a^{n-1} >$, 则$G$称为由$a$所生成的$n$阶循环群, 注意此时$1, a, a^2, \ldots\ldots, a^{n-1}$两两不同.

群和循环群，就如同面向对象编程中的父类和派生类.

# 生成元-例题

【例6.1.9】 循环群的生成元举例.

（1）<$Z$, ＋>是一个循环群, 1或-1是生成元, 1与-1互为逆元.

（2）<$Z_6$, ⊕>是循环群, 其生成元为1或5.

（3）<$Z_{11}^*$, ⊗>循环群, 其生成元有2, 6, 7和8.

# 循环群-阶

【定义6.1.8】 设$<G, \circ>$为循环群，$a$是$G$的生成元，若$G$的阶为$n$，则称$G$为$n$阶循环群，此时$G=\{e, a, a^2, \cdots, a^{n-1}\}$；若$a$是无限阶元，则称$G$为无限循环群.

# 循环群-生成元

对于一个循环群$G=\langle a\rangle$, 它的生成元可能不止一个, 如何求出它的所有生成元呢?

【定理6.1.2】 设$G=\langle a\rangle$是循环群.

(1) 若$G=\langle a\rangle$是无限循环群, 则$G$只有两个生成元, 即$a$和$a^{-1}$.

(2) 若$G=\langle a\rangle$是$n$阶循环群, 即$G=\{e,a,a^2,\cdots,a^{n-1}\}$, $G$的生成元是$a^t$当且仅当$t$与$n$是互质的. 易知$n$阶循环群的生成元的个数为$\varphi(n)$.

# 群-生成元

【例6.1.10】 设$<Z_9, \oplus>$是模9的整数加法群, 求其生成元.

解: 小于等于9并与9互素的正整数为1, 2, 4, 5, 7和8, 所以其生成元为1, 2, 4, 5, 7和8.

# 群-生成元

【例6.1.11】 设$<Z_{17}^*, \otimes>$是模17的整数乘法群，求其生成元.

解: 由【例5.1.4】知, 5是群$Z_{17}^* = \{1, 5, 5^2, \cdots, 5^{16-1} = 5^{15}\}$的生成元, 故$Z_{17}^* =< 5 >$, 故该群有8个生成元, 即

$Z_{17}^* =< 5 >=< 5^3 >=< 5^5 >=< 5^7 >=< 5^9 >=< 5^{11} >=< 5^{13} >=< 5^{15} >$.

# 6.1.3 同态与同构

【定义6.1.9】 设$(G,\cdot,1)$与$(H,*,1)$为群, $\eta: G \to H$为$G$到$H$的映射, 其满足
$\eta(g_1 \cdot g_2) = \eta(g_1) * \eta(g_2), (\forall g_1, g_2 \in G)$, 则$\eta$为$G$到$H$的群同态;

若有$\eta$是满射$(\eta(G) = H)$, 则称$G$与$H$同态, 记为$G \sim H$;

若$\eta$为双射(单射+满射), 则称$G$与$H$同构, 并记为$G \cong H$.

# 同态-例题

【例6.1.12】 设$G_1 = \{Z, +\}$是整数加群，$G_2 = \{Z_n, \oplus\}$是模$n$整数加群. 令$\eta: Z \rightarrow Z_n$，$\eta\,(x) = x \pmod n$. 则称$\eta$是群$G_1$到$G_2$的同态, 因为有$\forall x, y \in Z$,

$$\eta\,(x+y) = (x+y) \pmod n$$
$$= (x) \pmod n \oplus (y) \pmod n = \eta\,(x) \oplus \eta\,(y)$$

# 同态-例题

【例6.1.13】 群$(Z,+)$与群$(R-\{0\},\times)$同态, 且是单同态, 因为存在一个从$Z$到$R-\{0\}$的同态映射$f(x)=e^x$,对任意$x,y\in Z$, 有

$$f(x+y)=e^{x+y}=e^x\times e^y=f(x)\times f(y).$$

# 同构-例题

【例6.1.14】 设$R$为全体实数组成的加法群(+), $R^+$表示全体正实数组成的乘法群(·), 则群$R$与$R^+$同构.

证明: （1）对任意的$x \in R$, 令 $\eta(x) = e^x$, 则$\eta$是$R$到$R^+$的映射.

（2）设$x, y \in R$, 如果$\eta(x) = \eta(y)$, 即$e^x = e^y$, 所以$\eta$是$R$到$R^+$的单映射.

（3）对任意的$r \in R^+$, 令$x = log_e r$, 则$x \in R, \eta(x) = e^x = e^{log_e r} = r$. 所以$\eta$是$R$到$R^+$的满射.

（4）对$x, y \in R, \eta(x+y) = e^{x+y} = e^x \cdot e^y = \eta(x) \cdot \eta(y)$.

这就证明了$\eta$是$(R, +)$到$(\mathrm{R}^+, \cdot)$的同构映射.

# 循环群-性质

【定理6.1.3】 每个无限循环群同构于整数加法群$(Z,+)$，每个阶为$m$的有限循环群同构于$(m/mZ,\oplus)$.

# 作业