信道编码理论中用到的代数基础

zcl.space

目录

本章的内容是信道编码理论中用到的最基本的抽象代数的汇总。林舒也无意让读者通过本章的学习掌握抽象代数。更详细的抽象学习推荐其他教材，当然在本章结尾本书作者也推荐了一些经典老教材。此处，我推荐Michael Artin的《代数》和Harvard大学与此书配套的公开课。

当然本章也并不是没有存在必要。本章以较快的节奏给出了信道编码理论中涉及的代数理论，便于有一定基础的专业人士快速复习和进入编码世界。

1 群

群是抽象代数中最基本的概念。假设 G是一个集合，在G上，我们定义一个二元运算规则 $*$。通过这个二元运算规则和 G中的任意两个元素 a和b，我们可以定义第三个元素 $c = a * b$. 当$c \in G$，我们称 $*$在 G上是封闭的。比如，假设G是所有整数的集合，二元运算是加法，则对于 G中的任意整数 i和j，有$(i + j) \in G$。我们称所有整数组成的集合在加法下是封闭的。二元运算 $*$满足结合律，当且仅当 $\forall a, b, c \in G$:

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

现在我们给出群的完整定义：

在一个集合G上定义二元运算，当满足以下条件时我们称G是一个群：

1. 二元运算满足结合律;
2. G中有一个元素 e, $\forall a \in G$满足：
$$a * e = e * a = a$$
我们称e是单位元素。
3. $\forall a \in G$, G中有一个元素$a^{'}$ 满足:
$$a * a^{'} = a^{'} * a = e$$
我们称$a^{'}$是逆元。

群G是交换群，当且仅当对于任何两个元素 $a, b \in G$，有

$$a * b = b * a$$

对于群G，单位元素e和逆元都是唯一存在的。对于整数加法群，单位元是0，$-i$是i的逆元。所有除0以外的有理数构成一个乘法交换群：单位元是1，b/a是a/b的逆元。无论是整数加法群还是除零外的有理数乘法群，其元素个数都是无穷多个。当然，只有有限个元素的群也是存在的，我们称这样的群为有限群。

接下来考虑一个集合 $G = \{0, 1\}$，这个集合只有两个元素，并定义一个二元运算：

$$0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$$

我们称这样的二元运算为模二加。显然，定义了$\oplus$运算的集合G是一个交换群。

群中元素的个数叫做群的阶数。具有有限阶的群叫做有限群。接下来我们来阐述一个事实：对于任何的正整数m，我们都有可能定义一个有限群，群上的二元运算与实数加法非常相似。考虑一个整数集合$G=\{0,1,2,\ldots,m-1\}$ 定义$+$是实数加法，定义$\boxplus$是G上的二元运算满足

$$i \boxplus j = r$$

其中 $r = i + j \mod (m)$, 我们称其为模m加。显然$0 \le r \le (m-1)$ 并且$r \in G$.因此在二元运算符号$\boxplus$运算下G是封闭的。对于 $0 < i < m$ ， i和$m-i$都在G中. 因为

$$i + (m-i) = (m-i) + i = m$$

所以有

$$i \boxplus (m-i) = (m-i) \boxplus i = 0$$

因此，i和$m-i$在$\boxplus$运算下互逆。0的逆是它本身。另外我们还可以证明模m加满足结合律，即

$$(i \boxplus j) \boxplus k = i \boxplus (j \boxplus k)$$

综上，我们可以说集合$G=\{0,1,2,\ldots,m-1\}$在模m加运算下是一个群。我们称这样的群为加法群。我们给出一个模4加群计算中的模4加表如下所示：

表 1: 模4加法表

$\boxplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

接下来我们看一个乘法交换群的例子。假设p是一个素数，考虑集合$G=\{1,2,3,\ldots,p-1\}$。我们定义$\cdot$为乘法，定义$\boxdot$ 为模p乘，具体表示为

$$i \boxdot j = r, r = i \cdot j \mod p$$

首先我们知道$i \cdot j$不能被p整除，因此 $0 < r < p$ 且r是G中的一个元素。进而得出，r是G中的一个元素。可以证明在模p乘运算下，G是一个交换群。

显然1是单位元素。接下来我们证明对于每一个元素i都有且只有一个逆元存在。由于p是一个素数，$i < p$，i和p之间没有任何大于1的公约数。另外根据欧几里德定理存在两个整数满足

$$a \cdot i + b \cdot p = 1$$

其中a, p之间没有除1之外的最大公约数。把上式重排，我们有

$$a \cdot i = -b \cdot p + 1$$

这说明a是 i在G中模p乘的逆。值得一提的是当p不是质数时，G不是群。

接下来我们定义子群的概念。假定H是群G的一个子集，那么H是群G的一个子群当且仅当H在群G中的运算下是封闭的。

定理 假设G是二元运算$*$下的群。H是G的一个子集，那么H是一个子群，当且仅当：

1. H在二元运算$*$ 下封闭；
2. 对于H中的任何一个元素a，其逆也在H中。

接下来我们顶一个非常重要的概念：陪集。假设H是G的一个子群，二元运算为$*$，假设a是G中的任何一个元素。那么集合 $a*H \triangleq \{a*h : h \in H\}$叫做 H的左陪集；集合 $H*a \triangleq \{h*a : h \in H\}$叫做 H的右陪集。显然，当G是交换群的时候，左陪集等于右陪集。

考虑一个模16加法群$G=\{0,1,2,\ldots,15\}$。可以检验$H=\{0,4,8,12\}$是一个子群。对于这个子群有陪集:

$$
\begin{aligned}
0 \boxplus H &= \{0,4,8,12\} \\
1 \boxplus H &= \{1,5,9,13\} \\
2 \boxplus H &= \{2,6,10,14\} \\
3 \boxplus H &= \{3,7,11,15\}
\end{aligned}
$$

事实上，我们可以检验对于H只有这4个陪集。这4个陪集是互斥的，他们的并集构成了G.

定理 子群H的任意两个陪集的交集是空集。

假设$a*H$和$b*H$是H的两个不同的陪集，且$a*h$和$b*h^{'}$是$a*H$和$b*H$中的两个元素。假设$a*h=b*h^{'}$，h^{-1}是h的逆。则有：

$$
\begin{aligned}
(a*h)*h^{-1} &= (b*h^{'})*h^{-1} \\
a*(h*h^{-1}) &= b*(h^{'}*h^{-1}) \\
a*e &= b*h^{''} \\
a &= b*h^{''}
\end{aligned}
$$

其中 $h^{''}=h^{'}*h^{-1}$ 是H中的一个元素。 $a=b*h^{''}$意味着：

$$
\begin{aligned}
a*H &= (b*h^{'})*H \\
&= \{(b*h^{''})*h : h \in H\} \\
&= \{b*(h^{''}*h) : h \in H\} \\
&= \{b*h^{''''}, h^{'''} \in H\} \quad = \\
b*H
\end{aligned}
$$

此时，$a*H$和$b*H$是两个相同的陪集，与假设矛盾。

通过以上几个定理，我们发现群G的子集H的陪集具有以下性质：

1. 每一个G中的元素只出现在H的一个陪集中。
2. H的所有陪集是互斥的，即没有相同的元素。
3. H的所有陪集构成群G，即H的所有陪集是群G的一个划分我们用G/H来表示。

定理 (**朗格朗日定理**) 假设G是一个阶数为n的群，H是其阶数为m的子群。那么m可以整除n，并且G/H有n/m个H的陪集。

2 域

现在基于群的概念，我们引入抽象代数的另一个概念：域。粗略来讲，域是一些元素的集合，在这个集合中加减乘除都是封闭的。并且加法，乘法满足交换律，结合律和分配率。域的正式定义如下：

定义 (**域**) 令F是一个集合，在该集合上定义两个双目运算：加法+和乘法$\cdot$. 定义了加法和乘法运算的集合F是一个域，当且仅当：

1. F是一个加法交换群。零元是0；
2. F中除0以外的元素是一个乘法交换群。乘法单位元用1表示。

3. F乘法满足分配率，即对F中的三个元素 a, b, c满足 $a \cdot (b + c) = a \cdot b + a \cdot c$

通过以上定义，我们知道域中必须包含两个元素：加法零元和乘法单位元。域的元素个数叫做域的阶数。如果一个域中元素个数是有限的，我们称这个域是有限域。在一个域中，定义元素a的加法逆元为$-a$;乘法逆元为$a^{-1}, a \neq 0$。从一个域元a中减去另一个元素b定义为a加上b的逆元 $-b$。如果b是一个非零元，则定义a除以b为a乘以b的逆元b^{-1}。

从域的定义中可以推导出域的一些基本性质：

1. 对于域中每一个元素a， $a \cdot 0 = 0 \cdot a = 0$

2. 对于域中任何两个非零元素a和b，有$a \cdot b \neq 0$

3. $a \cdot b = 0 a \neq 0$意味着：$b \neq 0$

4. 对于域中任何两个元素 a和b，有$-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

5. 对于$a \neq 0, a \cdot b = a \cdot c$，有$b = c$

易得，实数在实数加法和乘法下是一个域。这个域有无穷多个元素。接下来我们给一个有限域的例子。

考虑带有模2加法和乘法的集合$\{0, 1\}$

表 2: 模2加法表

$+$	0	1
0	0	1
1	1	0

表 3: 模2乘法表

$\cdot$	0	1
0	0	0
1	0	1

我们知道$\{0, 1\}$是一个模2加交换群，$\{1\}$是一个模2乘群。同样我们可以很容易的验证模2乘在模2乘下满足分配率。

上面例子中的群我们成为二进制域，用$GF(2)$表示。$GF(2)$是一个非常重要的二进制域，这个域在编码理论，计算机理论和通信与存储系统中有广泛的应用。

接下来我们再给一个质数域的例子。假设p是一个素数了，那么$\{0, 1, 2, \ldots, p-1\}$是一个模p加下的交换群，同样我们也知道$\{1, 2, \ldots, p-1\}$形成了模p的乘法交换群。根据模p加法和乘法定义，结合实数乘法在模p加法下满足乘法分配率。所以，$\{0, 1, 2, \ldots, p-1\}$是一个p阶域。由于这个域是从质数构造而来的所以这个域也叫作质数域。特别的当$p = 2$时，我们有$GF(2)$。

以$p = 7$为例，集合$0, 1, 2, 3, 4, 5, 6$是一个模7加法和乘法下的7阶域，用$GF(7)$表示。加法表对减法也适用。比如，如果我们要计算$3 - 6$，首先我们找到-6的加法逆1。然后，把1和3相加，既得4。对于除法，我们使用乘法表。假设要计算$\frac{3}{2}$，则我们首先找到2^{-1}的逆$3 \cdot 4 = 5$。综上，我们验证了在一个有限域中，加法减法乘法除法可以像普通的代数运算一样进行计算。

我们知道对于任何的质数p，存在一个p阶的有限域。事实上，对于任何的正整数m，可以扩展质数域$GF(p)$到p^m个元素。更进一步，已经证明任何有限域的阶数是质数的幂次方。有限域也叫伽罗华域，这是为了纪念有限域的发明者：法国数学家伽罗华。很大一部分的代数编码理论，码的构建和译码都是基于有限域展开的。在接下来的几个章节，我们会考察有限域的几个基本性质：包括他们的代数结构，质数扩展域的构造。

考虑一个q阶有限域，$GF(q)$，让我们做以下加法：

$$\begin{aligned}\sum_{i=1}^{1} 1 &= 1\\ \sum_{i=1}^{2} 1 &= 1+1\\ \sum_{i=1}^{3} 1 &= 1+1+1\\ \ldots &= \ldots\\ \sum_{i=1}^{k} 1 &= \underbrace{1+1+\ldots+1}_{k}\end{aligned}$$

因为有限域在加法下是封闭的，这些和一定在有限域中；又由于有限域中的元素个数是有限的，这些和不可能无限的加下去而不出现重复。因此在些和组成的序列中一定存在重复，即一定存在两个正整数m和$n, m < n$ 且满足

$$\sum_{i=1}^{m} 1 = \sum_{i=1}^{n} 1$$

这意味着$\sum_{i=1}^{n-m} 1 = 0$。因此一定存在一个最小的正整数λ满足$\sum_{i=1}^{\lambda} 1 = 0$，我们称$\lambda$为$GF(q)$的特征值。二进制域$GF(2)$的特征值是2，因为$1+1=0$。更进一步，质数域$GF(p)$的特征值是$p$。因为$\sum_{i=1}^{k} 1 = k \neq 0, \forall 1 \leq k < p$ 并且 $\sum_{i=1}^{p} 1 = 0$

定理 有限域的特征值λ是一个质数。假设λ不是一个质数，那么λ可以表示成两个整数的乘积$\lambda = km$，由于域在乘法下是封闭的，则有

$$\left(\sum_{i=1}^{k} 1\right) \cdot \left(\sum_{i}^{m} 1\right)$$

也是域中的一个元素利用分配率，有

$$\left(\sum_{i=1}^{k} 1\right) \cdot \left(\sum_{i}^{m} 1\right) = \sum_{i}^{km} 1$$

由于$\sum_{i}^{km} 1 = 0$ 则，$\sum_{i}^{k} 1$或者$\sum_{i}^{m} 1$中至少有一个为0；然而这是不可能的，因为λ是满足$\sum_{i}^{\lambda} 1 = 0$的最小整数。矛盾产生，因此λ是一个质数。

因此，我们可以进一步推论，对于$GF(p)$中的任何两个小鱼λ的正整数k, m，有

$$\sum_{i}^{k} 1 \neq \sum_{i}^{k} 1 \neq 0$$

同样我们可以用反证法来证明，假设

$$\sum_{i}^{k} 1 \neq \sum_{i}^{k} 1$$

则有

$$\sum_{i}^{k-m} 1 = 0$$

, 不失一般性我们假设$k > m$. 然而这是不可能的，因为$k - m < \lambda$

接下来我们有λ个不相同的数：

$$1 = \sum_{i}^{1} 1, \sum_{i}^{2} 1, \sum_{i}^{3} 1, \ldots, \sum_{i}^{\lambda-1} 1, \sum_{i}^{\lambda} 1 = 0$$

. 事实上，这个求和集合本上构成了加法和乘法下阶数为λ的域。由于$GF(\lambda)$是$GF(q)$的一个子集，我们称$GF(\lambda)$是$GF(q)$的一个子域. 因此，我们可以说任何特征为λ 的