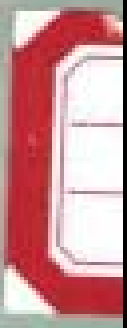
群与组合编码

樊恽 刘宏伟 编著

全国优秀出版社
武汉大学出版社

责任编辑：李汉保
责任校对：张　昕
版式设计：支　笛
封面设计：涂　驰



ISBN 7-307-03598-7/O·264
定价：12.50元

群与组合编码

樊 恽 刘宏伟 编著

武汉大学出版社

05
10
02

015

图书在版编目(CIP)数据

群与组合编码/樊恽,刘宏伟编著.--武汉:武汉大学出版社,2002.10

ISBN 7-307-03598-7

Ⅰ.群… Ⅱ.①樊… ②刘… Ⅲ.①群论 ②组合数学 ③编码 Ⅳ.O15

中国版本图书馆 CIP 数据核字(2002)第 029982 号

责任编辑:李汉保 责任校对:张 昕 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.whu.edu.cn)

印刷:湖北省荆州市今印印务有限公司

开本:850×1168 1/32 印张:7.625 字数:181 千字

版次:2002 年 10 月第 1 版 2002 年 10 月第 1 次印刷

ISBN 7-307-03598-7/O·264 定价:12.50 元

版权所有,不得翻印;凡购买我社的图书,如有缺页、倒页、脱页等质量问题者,请与当地图书销售部门联系调换。

内容简介

本书以群论、组合论、编码论的结合为切入点，通过对几个具体问题的解决，介绍这些领域的若干基本思想与知识以及它们的相互作用。本书只以初等线性代数为基础，可作为大学本科生选修课和硕士研究生课程教材。

前　言

本书是在作者近几年讲稿的基础上形成的教材. 这是一门为高年级本科生和硕士研究生开设的课程. 作者已在武汉大学为多届学生讲授过这门课程，初衷是想以群论与组合论、编码论的结合为切入点，通过几个具体问题的解决，向学生介绍群论、组合、编码的若干基本思想与知识及它们的相互作用与渗透

群论、组合论与编码理论具有各自的起源背景，在发展中相互影响、相互融合.

组合学既是一门古老的数学，又是一门年轻的数学. 组合学总是与实际问题相联系的，牛顿二项式定理、哥尼斯堡七桥问题、克格曼女生问题、地图着色问题等都是有名的老组合问题. 20 世纪中叶以来组合学迅速发展，一方面组合对象的重要性日益突出，使人们不得不把它们远置于数学游戏之上作为迫切问题予以研究；另一方面，一些成熟的数学理论与技术成功地应用到了组合学之中，并相互融合形成了重要的数学方向. 现在组合学已成为数学大树上的一大分枝. 广义地讲，组合学包括图论、组合分析等所有组合对象的研究理论；狭义地讲，组合学则是处理图论以外的组合对象.

任何组合结构，实际上任何结构，都有自己的自同构群；这个自同构群反映了该结构的对称性与匀称性. 分析群在结构上的作用既是解决问题的有效途径，也是产生新思想新研究问题的源泉.

然而群论起源于 19 世纪初 Galois 研究多项式方程的根式解

问题. 这是数学史上一块众所周知的里程碑. 人们在理解了Galois的思想之后，19 世纪中叶给出了抽象群的概念，以公理化的方式研究群. 群论的另一个应用范例是被用来刻画了自然界的晶体现象，人们发现所有的晶体点阵模式可以用 230 种结晶群来刻画. 这种重要的思想在本书介绍的 Pólya 定理中得到了体现.

编码理论则是由于近代通信科学技术的需要而产生于 20 世纪 40 年代的，它的孪生兄弟是信息论，但它们的数学性质和后来的发展都不尽相同. 编码理论和技术的目的是把信息编为符号序列，使得在信息传送中因各种原因产生错误后接收时仍然能获取正确的信息. 数学家们开始用一些组合技巧来达到部分目的；后来大量数学思想工具特别是代数思想工具成功地用到了编码中，使得编码发展成为一种数学思想与技术都很丰富的研究领域.

我们希望在大学基本课程主要是在线性代数的基础上展开本课程内容.

首先，我们需要介绍一些群论知识，但又不想把这事做得太抽象，所以在第 1 章里从变换开始引入群的基本概念，以初等数论方面的例子为主要素材演示了群论的作用，其中包括 RSA 密码系统的数论原理.

正如上面已经提到的，群常常是以作用的方式或者是自同构群的方式显示着自己的存在价值，不论是在理论上（甚至是数学自己的理论上）还是在应用上往往都是这样. 我们选择了以 Pólya 计数理论为应用实例来介绍群作用的思想，这就构成了第 2 章的内容.

群论特别是置换群论也有自己的组合问题，如对换的图的问题. 以此为契机，本书第 3 章介绍了图的有关常识，主要讨论了树、图的生成树等问题，包括以图的生成树为背景模型的拟阵概念及其在算法上的初步意义

第 4 章在介绍了码的一般情况后着重谈线性码. 这种码本身

就有一种交换群结构. 有限交换群上的 Fourier 变换在很多离散数学问题中有奇妙的应用，我们也以它为工具来介绍对偶码和对偶性质. 最后一节实际上是我们自己最近的研究工作，给出了极大投射码与等距线性码的关系.

循环码，特别是 BCH 码，结构并不很复杂但却很有效. 通常是从多项式环的角度讨论它，也可以归结到循环群的群代数的理想；这种群代数的理想又由特征标（character）完全决定. 在第 5 章中我们就以这种思路来介绍循环码及 BCH 码. 当然需要比较多的关于域的知识，特别是有限域的知识，对这些我们也都做了必要的准备.

每节后配备了习题，大致有三类题目：一类是基本练习题；另一类则是对正文的补充，这类题中的一部分还会在其他地方被引用；此外有少数稍微深一点的题目. 书末附有习题答案提示. 正如上所述，由于很多题目实际上是基本结论，所以答案提示做得还比较详细.

有些常共性的符号在全书中较多地方出现，为了阅读方便，把它们列在书末.

最后说明一下编写体例. 为了方便查找，定义、定理、命题等全书统一编号. 例如，“1.1.1 定义”是说第 1 章第 1 节第 1 个条目，它是一个定义，引用时就说“定义 1.1.1”. 又如“5.3.15 例子”是说第 5 章第 3 节第 15 个条目，它是一个例子，引用时就说“例 5.3.15”. 习题的引用稍微不一样：说“习题 2 (1)”是指本节编号 2 的习题的第(1)小题，而“习题 1.3.14”是说的第 1 章第 3 节习题 14.

以上就是本书的基本构思. 选材及处理等不当之处，还望读者斧正.

作　者

2002 年 4 月

目　录

第 1 章　群

§1.1　群

设 X 是一个非空集合. 在 X 的所有变换的集合 $T = \mathrm{Tran}(X) = \{\alpha : X \to X\}$ 上有合成运算，通常记作 $\circ$，即：对 $\alpha, \beta \in \mathrm{Tran}(X)$，$\alpha \circ \beta$ 定义为：$(\alpha \circ \beta)(x) = \alpha(\beta(x))$，$\forall x \in X$ 这个运算符合结合律，因为

$$((\alpha \circ \beta) \circ \gamma)(x) = (\alpha \circ \beta)(\gamma(x)) = \alpha(\beta(\gamma(x)))$$
$$= \alpha((\beta \circ \gamma)(x)) = (\alpha \circ (\beta \circ \gamma))(x)$$

一般地，我们有下述定义.

1.1.1 定义　集合 T 上的运算 $\circ$ 是指一个映射

$$\circ : T \times T \to T;$$

把 $(a, b) \in T \times T$ 的像记作 $a \circ b$. 我们称：

运算 $\circ$ 满足结合律，如果 $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$，$\forall \alpha, \beta, \gamma \in T$；

运算 $\circ$ 满足交换律，如果 $\alpha \circ \beta = \beta \circ \alpha$，$\forall \alpha, \beta \in T$.

进一步，设 $\oplus$ 也是 T 上的运算. 我们称：

运算 $\circ$ 对运算 $\oplus$ 满足左分配律，如果

$$\alpha \circ (\beta \oplus \gamma) = (\alpha \circ \beta) \oplus (\alpha \circ \gamma), \forall \alpha, \beta, \gamma \in T;$$

类似地，可定义一个运算对另一个运算的右分配律.

回到集合 $T = \mathrm{Tran}(X)$，它显然具备以下三条：

(1) 有运算 $\alpha \circ \beta$，为简单，记作 $\alpha \cdot \beta$ 或 $\alpha\beta$；

(2) 运算 $\alpha \circ \beta$ 满足结合律;

(3) 恒等映射 $\mathrm{id}_X \in T$,简记为 1,满足:$1 \circ \alpha = \alpha = \alpha \circ 1$, $\forall \alpha \in T$.

进一步,考虑 X 的所有可逆的变换,即双射变换的集合,

$\mathrm{Sym}(X) = \{\alpha \in \mathrm{Tran}(X) \mid \exists \alpha' \in \mathrm{Tran}(X)$ 使得 $\alpha\alpha' = 1 = \alpha'\alpha\}$,

按这个集合的定义就知道 $\mathrm{Sym}(X)$ 不仅具备上述(1)、(2)、(3)条,而且具备:

(4) $\forall \alpha \in \mathrm{Sym}(X) \exists \alpha' \in \mathrm{Sym}(X)$ 使得 $\alpha\alpha' = 1 = \alpha'\alpha$.

我们总用 $|X|$ 表示集合 X 中元素的个数,即集合 X 的基数. 如果 $|X| < \infty$,即 X 是有限集,则 $\mathrm{Sym}(X)$ 中的元称为 X 上的置换. 特别地,若 $X = \{1,2,\cdots,n\}$,则记 $\mathrm{Sym}(X)$ 为 S_n,其中元称为 n 次置换. n 次置换 α 可表示为

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}.$$

那么第二行显然是 $1,2,\cdots,n$ 的一个排列,即一个无重复的序列. 反过来,也只要第二行是 $1,2,\cdots,n$ 的一个排列,就给出了一个置换. 如

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$$

是把 1 置换为 4,把 2 置换为 1,等等. 故马上可得:

1.1.2 命题 $|S_n| = n!$. □

注意观察上面置换的例子,从 1 出发,1 被置换为 4,即到达 4;再从 4 到达 2,再从 2 到达 1,即回到了 1. 可以把这个圈写成(142),称为一个循环(cycle),或更准确地,称为一个 3- 循环. 在五个文字 1,2,3,4,5 中去掉 1,4,2 余下 3,5;随机取一个,如 3,重复这一过程,又得到一个循环(35). 因此可以写

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix} = (142)(35) = (35)(142)$$

但每次重复这个过程都可以从任一个文字出发. 比如,第一次从 4 出发,就得到(421),显然它与(142) 是同一个循环只是写法不一样,这容易理解. 因为"圈" 本来就是无头无尾的,但是写起来只能写成一行. 所以(142) = (421) = (214). 一个 3- 循环有 3 种写法. 显然,一般地,一个 k- 循环有 k 种写法. 另一方面,若第一次从 3 出发,则得到(35) = (53). 所以我们写(142)(35) = (35)(142).

实际上有一种更数学化的表述方式,可以把一个循环看做是一个置换:(142) 就是把 1 变为 4,把 4 变为 2,把 2 变为 1,使其他文字不变. 这样(142) 就是一个循环置换. 那么,由于(142) 与(35) 没有公共文字,容易看出置换(142) 与置换(35) 做乘法时可以交换,即(142)(35) = (35)(142).

从上述分析可以容易地证明下述命题.

1.1.3 命题　任何 n 次置换,可以写成彼此无公共文字从而彼此相乘可交换的循环置换之积,使得每个文字恰好出现一次;而且这种写法在不计循环因子的次序时是惟一的. □

例　$S_3 = \{(1),(12),(23),(31),(123),(132)\}$.

利用这种表达方式我们可以容易地列举出具备(1) ~ (4) 条的结构.

1.1.4 例　考虑平面上的一个正三角形(如图 1-1 所示),某些"刚体变换" 可把它变得重合于它自己,某些则不能. 当它重合于它自己时,它的三个顶点肯定重合于三个顶点. 我们用 1,2,3 来把它的三个顶点分别标上号,就可以把使得它变得重合于它自己的刚体变换表达为 3 次置换

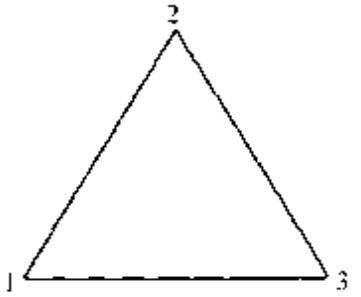


图 1-1

以这种方式容易看出,使此正三角形不变的全体变换是

$$S_3 = \{(1),(12),(13),(23),(123),(132)\}.$$

这正好是全体3次置换的集合，它显然满足(1) ~ (4)条.

1.1.5 例 考虑平面上用1,2,3,4标号的正方形(如图1-2所示)：

使它不变的全部"刚体变换"是(例如，逆时针旋转 $\pi/2$ 这个变换就是 $\begin{pmatrix}1234\\2341\end{pmatrix}=(1234)$)：

$$D_4=\{(1),(1234),(13)(24),(1432),$$
$$(12)(34),(14)(23),(13),(24)\}.$$

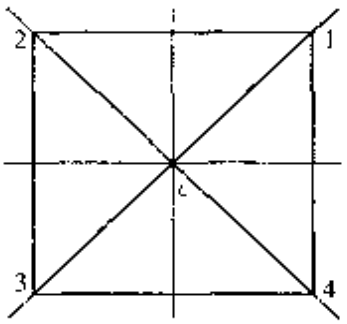


图 1-2

不用计算就可看出 $\alpha\beta\in D_4,\forall\alpha,\beta\in D_4$，因为使此正方形不变的合成变换显然还使此正方形不变；同样的道理，使此正方形不变的变换的逆变换显然还使此正方形不变，等等. 那么易见 D_4 满足(1) ~ (4)条.

可以想像，对任何一个几何体，使它不变的变换的集合恒满足(1) ~ (4)条；这样的数学结构可以刻画该几何体的对称性质 这可以说是群概念的直观来源.

1.1.6 定义 如果非空集合 G 具备下述四个条件：

(1) 在集合 G 上有一个运算(通常写作"·"，称作乘法)；

(2) 该运算满足结合律；

(3) 存在元素，通常记作1，使得 $1x=x=x1,\forall x\in G$；

(4) 对任意 $a\in G$ 存在 $a'\in G$ 使得 $aa'=1=a'a$；

则称 G 与(1)中的运算"·"一起构成一个群；此时(3)中的元素1称为群 G 的单位元，(4)中的元 a' 记作 a^{-1} 且称为 a 的逆元.

1.1.7 命题 在一个群中，单位元惟一，任一个元的逆元惟一.

证明 若 $1'$ 也是单位元，则 $1=11'=1'$ 若 a' 与 a'' 都是 a 的逆元，则 $a''=1a''=(a'a)a''=a'(aa'')=a'1=a'$. □

例 我们已经看到群的三个例子. 现在可以正式给它们命

名. 称 Sym(X) 是集合 X 的对称群(symmetry group). 当 $X = \{1,2,\cdots,n\}$ 时,称 $S_n = \mathrm{Sym}(X)$ 为 n 次对称群(symmetric group of degree n). 而例 1.1.4 中的 S_3,例 1.1.5 中的 D_4 可分别称为正三角形、正四边形的对称群.

为表明它们如何体现了几何体的对称,作为比较,看另一例子.

1.1.8 例　考虑边长不等的长方形(如图 1-3 所示),也用 1,2,3,4 给它的顶点标号:

那么我们得到的使它不变的"刚体变换群"是

$$K_4 = \{(1),(13)(24),(12)(34),(14)(23)\},$$

显然 K_4 是例 1.1.5 中的 D_4 的真子集,但它们的运算是一致的,单位元也是一样的. 直观来看,这就说明长方形确实比正方形的"对称"少了很多.

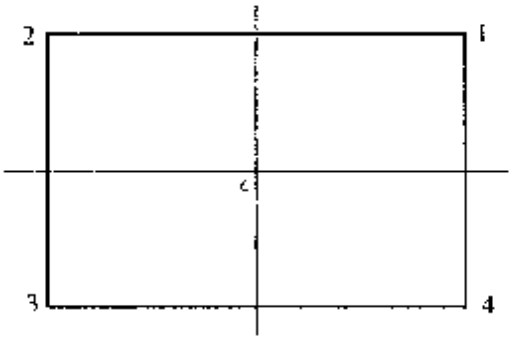


图 1-3

这个例子也导致下面的概念:

1.1.9 定义　设 G 是一个群,设 H 是 G 的非空子集. 如果 H 在 G 的运算之下封闭,而且在 G 的运算之下 H 也是一个群,则称 H 是 G 的子群,记作 $H \leqslant G$.

1.1.10 命题　如果 $H \leqslant G$,则 H 的单位元与 G 的单位元一致,即 $1_H = 1_G$;对任意 $h \in H$,h 在 H 中的逆元与它在 G 中的逆元一致.

证明　设 1_H 在 G 中的逆元是 $1_H'$,那么 $1_G = 1_H 1_H' = (1_H 1_H)1_H' = 1_H(1_H 1_H') = 1_H 1_G = 1_H$. 第二个结论可以从命题 1.1.7 直接得到(但是注意:第一个结论不能从单位元的惟一性得出,因为就是要证 $1_G \in H$),或者像上面那样证明也行. □

1.1.11 命题　设 G 是一个群,设 H 是 G 的非空子集. 则

(1) $H \leqslant G$ 当且仅当对于任意 $x, y \in H$ 有 $x^{-1} \in H$ 和 $xy \in H$.

(2) $H \leqslant G$ 当且仅当对于任意 $x, y \in H$ 有 $xy^{-1} \in H$.

(3) 进一步,设 G 是有限群,则 $H \leqslant G$ 当且仅当 H 在群运算之下封闭.

证明 (1) 类似于下述(2).

(2) 必要性显然是对的.反过来设条件成立.由于 $H \neq \emptyset$,取 $x \in H$ 得 $1 = xx^{-1} \in H$,从而,$x^{-1} = 1x^{-1} \in H$.那么对于任意 $x, y \in H$,就有 $y^{-1} \in H$;由条件 $xy = x(y^{-1})^{-1} \in H$,结合律在 H 中显然也成立.所以 H 在 G 的运算之下也是群.

(3) 由条件,G 的乘法运算可以限制成为 H 的运算.对于任意 $h, x, y \in H$,若 $hx = hy$,则两边同时左乘 h^{-1} 得 $x = y$.由本节习题 12 可知 H 在 G 的乘法下成为群. □

如同上面的例子所显示的,从几何角度来看群这个概念是比较直观的.然而历史上群的概念却首先产生于 19 世纪 Galois 研究代数方程的根式解.我们来看一下这样的代数例子 粗粗一想,代数例子应比几何例子抽象,但我们将会看到,它们与上述几何例子还真的类似.

1.1.12 例 考虑变元集合 $X = \{x_1, x_2, x_3\}$ 上的任意多项式 $f(X)$,例如 $h(X) = x_1 - x_2 - x_3$,$g(X) = x_1^2 + x_2^2 + x_3^2 - 3x_1x_2x_3$,等等.对于任一置换 $\alpha \in S_3$,令 α 置换变元如下:变 x_1 为 $x_{\alpha(1)}$,变 x_2 为 $x_{\alpha(2)}$,等等.则 α 把多项式 $f(X)$ 变为一个多项式,记作 $\alpha f(X)$.例如,若 $\gamma = (123)$ 而 $h(X)$ 如上,则 $\gamma h(X) = x_2 - x_3 - x_1$.如果 $\alpha f(X) = f(X)$,我们就说 α 使 $f(X)$ 不变 我们找出使 f 不变的所有置换的集合 G_f.与上述几何例子类似,使多项式 $f(X)$ 不变的变换的合成变换显然还使多项式 $f(X)$ 不变;使多项式 $f(X)$ 不变的变换的逆变换显然还使多项式 $f(X)$ 不变,等等.所以 G_f 是一个群而且它刻画了多项式 f 的对称性质.例如,对

上面的多项式 $h(X)$ 很容易找出

$$G_h = \{(1),(23)\}.$$

另一方面，对上面的多项式 $g(X)$ 则

$$G_g = \{(1),(123),(132),(12),(13),(23)\} = S_3.$$

容易看出，上面的多项式 $g(X)$ 真正是通常所说的“对称多项式”；而多项式 $h(X)$ 的“对称”就比 $g(X)$ 少很多，它只对变元 x_2 和 x_3 是对称的.

下面是一系列群的重要例子.

1.1.13 例　整数集$\mathbb{Z}$在加法运算下是一个无限群. 对于任意 $m \in \mathbb{Z}$，子集 $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$ 是一个子群.

1.1.14 例　设 m 为正整数，$\mathbb{Z}_m = \{[x] \mid x \in \mathbb{Z}\}$ 表示整数模 m 剩余类的集合，$[x]$ 表示整数 x 所在的剩余类；两个运算定义如下：

$$[x] + [y] = [x + y],$$
$$[x] \cdot [y] = [x \cdot y].$$

那么$\mathbb{Z}_m$在加法之下为群，称为整数模 m 剩余类加群. 显然 $|\mathbb{Z}_m| = m$

另一方面，令$\mathbb{Z}_m^* = \{[x] \in \mathbb{Z}_m \mid x$ 与 m 互素$\}$；按此集合的定义可验证它在乘法之下为群，见本节习题 11，称为整数模 m 剩余类乘群. 记

$$|\mathbb{Z}_m^*| = \varphi(m), \tag{1.1.15}$$

称式(1.1.15)为定义在正整数集上的 Euler 函数. 我们将对它进行一系列研究.

1.1.16 例　S_n 的任意子群称为 n 次置换群.

1.1.17 例　设 $M_n(\mathbb{C})$ 为所有 $n \times n$ 复矩阵的集合，则在矩阵加法之下为群. 另一方面，令 $GL_n(\mathbb{C})$ 为所有可逆的 $n \times n$ 复矩阵的集合，则 $GL_n(\mathbb{C})$ 在矩阵乘法之下为群，称为复数域上 n 级一般线性群. 而 $GL_n(\mathbb{C})$ 的任意子群称为复数域上 n 级线性群.

对有理数域$\mathbb{Q}$和实数域$\mathbb{R}$可以作出同样的群. 实际上本节习

题 4 是这个例子的特例.

习题 1.1

1. (1) 在 S_7 中, $\alpha = (1357)(246)$, $\beta = (25)(367)$. 求: $\alpha\beta$、$\beta\alpha$ 和 α^{-1}.

(2) 设 $|X| \geqslant 3$, 证明 $\mathrm{Tran}(X)$ 上的合成运算。不满足交换律.

2. 设 $|X| = n < \infty$. 计算 $|\mathrm{Tran}(X)|$.

3. 证明: 集合 X 的变换 α 可逆, 当且仅当 α 是 X 的双射变换.

4. (1) 全体有理数集合 $\mathbb{Q}$ 在有理数加法之下是一个群, 称为有理数加群. 全体非零有理数集合 $\mathbb{Q}^*$ 在有理数乘法之下是一个群, 称为有理数乘群.

(2) 对实数集 $\mathbb{R}$ 和复数集 $\mathbb{C}$ 同样分别有加群 $\mathbb{R}$ 和 $\mathbb{C}$, 乘群 $\mathbb{R}^*$ 和 $\mathbb{C}^*$.

5. 在群 G 中证明:

(1) $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$.

(2) 如果 $a^2 = a$ 则 $a = 1$.

(3) $a^2 = 1$ 当且仅当 $a = a^{-1}$.

(4) 如果 $ab = ba$ 则 $a^{-1}b = ba^{-1}$.

6. 证明群 G 是交换群, 当且仅当 $(xy)^2 = x^2y^2$, $\forall\, x, y \in G$.

7. 设 H_i, $i = 1, 2, \cdots$, 是群 G 的子群. 如果 $H_1 \subset H_2 \subset \cdots$, 则并集 $\bigcup_{i=1}^{\infty} H_i$ 是群 G 的子群.

8. 设 G 是一个群. 证明: $Z(G) = \{z \in G \mid zx = xz\ \forall\, x \in G\}$ 是一个交换子群(定义: $Z(G)$ 称为群 G 的中心).

9. 证明: 一个群不可能是它的两个真子群的并集. 它可以是三个真子群的并集吗?

10. 两个子群的交集仍是子群. 任意个子群的交集仍是子群.

11. 设 $\mathbb{Z}$ 是全体整数集合, m 是正整数. 证明:

(1) 如果 $m|(a-b)$ 则称 a 与 b 模 m 同余并记 $a \equiv b(\mathrm{mod}\ m)$. 那么 $\equiv(\mathrm{mod}\ m)$ 是 $\mathbb{Z}$ 的等价关系. $a \equiv b(\mathrm{mod}\ m)$ 当且仅当 $a-b \in m\mathbb{Z}$, 关于 $m\mathbb{Z}$ 见例 1.1.13.

(2) a 所在的等价类是 $a+m\mathbb{Z}=\{a+mx \mid x \in \mathbb{Z}\}$, 称为 a 所在的模 m 剩余类.

(3) 0 所在的模 m 剩余类 $m\mathbb{Z}$ 是 $\mathbb{Z}$ 的子群.

(4) $[a]+[b]=[a+b]$ 是合理定义的运算(即与代表元的选取无关).

(5) $[a]\cdot[b]=[a\cdot b]$ 是合理定义的运算.

(6) $[a] \in \mathbb{Z}_m^*$(即 $(a,m)=1$) 当且仅当存在 $[a'] \in \mathbb{Z}_m$ 使得 $[a][a']=[1]$

12. 设非空有限集合 X 上有满足结合律的运算"$\cdot$". 如果对于任意 $x,y,z \in X$, 只要 $xy=xz$ 就有 $y=z$, 且只要 $yx=zx$ 就有 $y=z$(这称为满足消去律(cancelation low)), 则在此运算之下 X 是一个群. 举例说明 X 的有限性条件不能去掉.

§1.2　群的基本性质

回顾整数模 m 剩余类集合 $\mathbb{Z}_m$. 由习题 1.1.11 知:

(1) 加群 $\mathbb{Z}$ 的子群 $m\mathbb{Z}$ 决定了一个等价关系:

$$a \equiv b(\mathrm{mod}\ m) \Leftrightarrow a-b \in m\mathbb{Z},$$

从而作出商集(等价类的集合) $\mathbb{Z}_m$, a 所在的等价类为 $[a]=a+m\mathbb{Z}$;

(2) 用代表元运算可以合理定义商集 $\mathbb{Z}_m$ 上的运算 $[a]+[b]=[a+b]$;

(3) 映射 $\sigma:\mathbb{Z}\to\mathbb{Z}_m$, $a\mapsto[a]$, 满足 $\sigma(a+b)=\sigma(a)+\sigma(b)$.

我们称满足这种条件的映射为同态映射.

我们沿此思路在一般群上展开讨论. 由于一般群的运算不一定交换, 遵循此思路, 第一步考虑如何由子群定义等价关系时就出

现了不同情况.

1.2.1 定义 设 G 为群,$H \leqslant G$. 对 $x, y \in G$,称 xy^{-1} 为右差,而称 $y^{-1}x$ 为左差.

如果 $xy^{-1} \in H$, 则称 x 与 y 模 H 右同余, 记作 $x \equiv y \pmod{H}$.

如果 $y^{-1}x \in H$, 则称 x 与 y 模 H 左同余, 记作 $x \equiv y \pmod{H}$.

1.2.2 命题 符号如上. 右同余 $x \equiv_r y \pmod{H}$(左同余 $x \equiv_l y \pmod{H}$)是等价关系;$y \in G$ 所在的等价类,称为模 H 右同余类(模 H 左同余类)为

$$Hy = \{hy \mid h \in H\} \quad (yH = \{yh \mid h \in H\}).$$

证明 $x \equiv_r y \pmod{H}$ 显然满足自反律. 如果 $x \equiv y \pmod{H}$,即 $xy^{-1} \in H$,因 H 是子群,故 $yx^{-1} = (xy^{-1})^{-1} \in H$,按定义,$y \equiv_r x \pmod{H}$. 这是对称律. 再设 $x \equiv_r y \pmod{H}$, $y \equiv_r z \pmod{H}$,那么 $xy^{-1} \in H$, $yz^{-1} \in H$,仍由 H 是子群,得 $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$. 即 $x \equiv_r z \pmod{H}$.

按等价类定义,$y \in G$ 所在的等价类是集合

$$\{x \in G \mid xy^{-1} \in H\} = \{x \in G \mid x \in Hy\} = Hy. \qquad \square$$

1.2.3 定义 $Hy(yH)$ 称为群 G 中关于子群 H 的一个右陪集(左陪集),y 为其代表元(显然 $y \in Hy$, $y \in yH$). H 的所有右陪集(左陪集)的集合,即对等价关系 $\equiv_r \pmod{H}$($\equiv_l \pmod{H}$)的商集,记作 $H \backslash G$ (G/H). 注意:该符号也常用来记右陪集(左陪集)的完全代表系.

1.2.4 引理 (1) 群 G 是其子群 H 的右陪集的不交并,也是 H 的左陪集的不交并.

(2) 任意两个右(左)陪集所含元素个数相等,它们都等于 H 的阶.

证明 (1) 因为右陪集是右同余关系的等价类.

(2) 考虑映射 $H \to Hy, h \mapsto hy$，映射 $Hy \to H, hy \mapsto h$，就是逆映射，所以这两个映射都是双射，故 $|H| = |Hy|$. □

1.2.5 Lagrange 定理　群 G 中子群 H 的右陪集个数与其左陪集个数相等，此个数称为 H 在 G 中的指数，记作 $|G:H|$，从而 $|G| = |G:H| \cdot |H|$.

证明　在两个陪集集合之间作映射 $G/H \to H\backslash G, yH \mapsto Hy^{-1}$；如果 $yH = y'H$，则 $y^{-1}y' \in H$ 也就是 $y^{-1}(y'^{-1})^{-1} \in H$；得 $Hy^{-1} = Hy'^{-1}$. 故这映射是合理定义的. 还易验证它是双射的，因为 $H\backslash G \to G/H$，$Hx \mapsto x^{-1}H$（与上相同这映射是合理定义的）就是它的逆映射. 此为第一个结论. 由引理 1.2.4(1)，$|G| = \sum_{yH \in G/H} |yH| = \sum_{yH \in G/H} |H| = |G:H| \cdot |H|$. □

进一步，考虑利用代表元运算定义商集上的运算时，我们发现不得不对子群加上进一步的条件才能使得定义不依赖于代表元的选取.

1.2.6 定义　群 G 的子群 H 称为正规子群，如果 H 的任一左陪集也是一个右陪集（等价于 $Hy = yH, \forall\, y \in G$，见本节习题 3），记作 $H \trianglelefteq G$.

可从另一角度来看条件 $Hy = yH$；显然它等价于

$$y^{-1}Hy = H.$$

对 $y \in G$ 可以定义映射

$$G \to G, x \mapsto y^{-1}xy \quad (\text{记 } y^{-1}xy = x^y);$$

称为由 y 给出的共轭映射；它显然是双射. 所以，正规子群就是在任何共轭之下不变的子群；另一个有用的刻画是 $H \trianglelefteq G$ 当且仅当 $y^{-1}xy \in H, \forall\, x \in H$ 和 $y \in G$（见本节习题 3）.

1.2.7 命题与定义　设 H 是群 G 的正规子群. 则在陪集集合 G/H 上如下定义的运算是合理的：

$$(xH)(yH) = (xy)H, \qquad \forall\, x, y \in G;$$

而且在此运算之下，商集 G/H 成为群，称为群 G 关于正规子群 H 的商群.

证明 如果 $x' \in xH, y' \in yH$（即 $x' \equiv_l x \pmod H$，$y' \equiv_l y \pmod H$），那么存在 $h, h' \in H$ 使得 $x' = xh, y' = yh'$；因 $H \trianglelefteq G$，故 $y^{-1}hy \in H$，则 $x'y' = xhyh' = xy(y^{-1}hyh') \in (xy)H$，即得 $(x'y')H = (xy)H$. 因此上述在商集 G/H 上的运算是合理定义的. 按这个定义，结合律显然满足；$1H = H$ 就是单位元；元素 xH 的逆元就是 $x^{-1}H$. 所以，商集 G/H 成为群. □

注解 对群 G 的子集合 S, T，可定义乘积：$ST = \{st \mid s \in S, t \in T\}$. 那么商群中的运算也可以从子集合的乘积的角度来讨论，见本节习题 5

现在按照本节开始时介绍的思路，讨论群同态和群同构.

1.2.8 定义 设 G, G' 是群（运算都写作乘法）. 映射 $f: G \to G'$ 称为群同态，如果以下条件成立

$$f(xy) = f(x)f(y), \qquad \forall x, y \in G.$$

进而，同态 f 称为单同态（全同态、同构）如果 f 还是单射（全射、双射）.

1.2.9 例 $G \to G', x \mapsto 1_G$. 零同态.

1.2.10 例 $\mathrm{id}_G: G \to G, x \mapsto x$. 恒等同态

1.2.11 例 设 $H \trianglelefteq G$ 是正规子群. 则容易验证 G 到商集 G/H 的自然映射 $\sigma: G \to G/H, x \mapsto xH$，是群的满同态，称为自然同态.

1.2.12 例 给定 $y \in G$. 共轭映射 $G \to G, x \mapsto x^y$，是 G 的自同构.

1.2.13 例 $\mathbb{Z} \to \mathbb{Z}_m, a \mapsto [a]$，是群的全同态.

1.2.14 命题与定义 设 $f: G \to G'$ 是群同态. 则

(1) $\mathrm{Ker}(f) = \{x \in G \mid f(x) = 1_G\}$ 是 G 的正规子群，称为

同态 f 的核.

(2) $\mathrm{Im}(f)=\{x'\in G'\mid \exists x\in G$ 使得 $f(x)=x'\}$ 是 G' 的子群,称为同态 f 的像.

证明　(1) 显然 $\mathrm{Ker}(f)\neq\varnothing$ 因为 $1\in\mathrm{Ker}(f)$,见本节习题 7. 对于任意 $x,y\in\mathrm{Ker}(f)$, 仍由本节习题 7 有 $f(x^{-1})=f(x)^{-1}=1_G$,从而还有 $f(x^{-1}y)=f(x^{-1})\cdot f(y)=1_G\cdot 1_G=1_G$. 所以 $\mathrm{Ker}(f)$ 是 G 的子群. 对于任意 $x\in\mathrm{Ker}(f)$ 和 $y\in G$,有 $f(y^{-1}xy)=f(y^{-1})f(x)f(y)=f(y)^{-1}\cdot 1_G\cdot f(y)=1_G$;所以 $y^{-1}xy\in H$ 即 $\mathrm{Ker}(f)\trianglelefteq G$.

(2) 类似于上证之. □

1.2.15 定理(同态基本定理)　设 $f:G\to G'$ 是群同态. 则存在惟一群同态 $\bar{f}:G/\mathrm{Ker}(f)\to G'$ 使得 $f=\bar{f}\circ\sigma$(即如图 1-4 所示交换),其中 $\sigma:G\to G/\mathrm{Ker}(f)$ 是自然同态;此时 $\bar{f}$ 必是单同态. 进一步,若 f 为全同态则 $\bar{f}$ 为群同构.

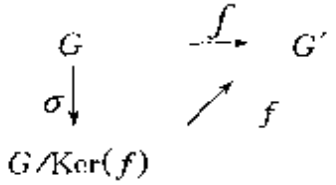


图 1-4

证明　对于任意陪集 $x\mathrm{Ker}(f)\in G/\mathrm{Ker}(f)$,我们证明:可以定义 $\bar{f}(x\mathrm{Ker}(f))=f(x)\in G'$. 若 $x'\equiv x\pmod{\mathrm{Ker}(f)}$ 即有 $h\in\mathrm{Ker}(f)$ 使得 $x'=xh$,则 $f(x')=f(xh)=f(x)f(h)=f(x)\cdot 1=f(x)$;所以我们合理地定义了映射 $\bar{f}:G/\mathrm{Ker}(f)\to G'$. 按定义对于任意 $x\in G$ 显然有 $\bar{f}\sigma(x)=\bar{f}(x\mathrm{Ker}(f))=f(x)$;即 $f=\bar{f}\sigma$. 而且按 $\bar{f}$ 的定义容易验证 $\bar{f}$ 是群同态.

又如果 $\bar{f}:G/\mathrm{Ker}(f)\to G'$ 使得 $f=\bar{f}\sigma$;则对于任意的 $x\mathrm{Ker}(f)\in G/\mathrm{Ker}(f)$ 有

$\bar{f}(x\mathrm{Ker}(f)) = \bar{f}\sigma(x) = f(x) = \bar{f}\sigma(x) = \bar{f}(x\mathrm{Ker}(f))$;
即得 $\bar{f} = \bar{f}$. □

集合的子集的包含关系显然是一个偏序关系,任何映射都保持这种偏序关系(包含关系),简单说成保序,即:$f: S \to S'$, $S_1 \subseteq S_2 \subseteq S$,则 $f(S_1) \subseteq f(S_2)$. 这对于群和群的同态当然也成立. 重要的是,对于群的满同态有非常强的结果.

1.2.16 定理(子群对应定理) 设 $f: G \to G'$ 是群的全同态,则下述子集的集合之间的映射

$$f^*: \{H \mid \mathrm{Ker}(f) \leqslant H \leqslant G\} \to \{H' \mid H' \leqslant G'\}, H \mapsto f(H)$$

是保序双射;且对 $\mathrm{Ker}(f) \leqslant H \leqslant G$ 有:

(1) $|G:H| = |G':f(H)|$.

(2) (第一同构定理) $H \trianglelefteq G$ 当且仅当 $f(H) \trianglelefteq G'$;而且在这种情形则有 $G/H \cong G'/f(H)$ 把 xH 映射为 $f(x)f(H)$.

证明 可以定义一个与 f^* 方向相反的映射

$$g^*: \{H' \mid H' \leqslant G'\} \to \{H \mid \mathrm{Ker}(f) \leqslant H \leqslant G\}, H' \mapsto f^{-1}(H')$$

这里 $f^{-1}(H') \subseteq G$ 表示 H' 在 G 中的完全原像,所以 $\mathrm{Ker}(f) \leqslant f^{-1}(H) \leqslant G$,见本节习题 7(3). 与命题 1.2.14 的证明类似地可以证明 $f^{-1}(H) \leqslant G$;而且当 $H' \trianglelefteq G'$ 时也与命题 1.2.14 的证明类似地可以证明 $f^{-1}(H) \trianglelefteq G$. 按 f^* 和 g^* 的定义,显然 $f^*g^*(H') = H', \forall H' \leqslant G'$;而且只要 $\mathrm{Ker}(f) \leqslant H \leqslant G$ 就有 $g^*f^*(H) = H$. 所以 f^* 和 g^* 正好是互逆的映射,即它们都是双射. 显然它们都是保序的. 下设对 $\mathrm{Ker}(f) \leqslant H \leqslant G$,记 $H' = f(H)$. 那么 H 就是 H' 的完全原像,见本节习题 7(3).

(1) 对于任意陪集 $xH \in G/H$,令 $f(x)H' \in G'/H'$ 与之对应. 如果 $yH = xH$,则 $y = xh$ 对于某 $h \in H$,故 $f(y) = f(xh) = f(x)f(h) \in f(x)H'$. 所以我们有合理定义的映射

$$\bar{f}: G/H \to G'/H', xH \mapsto f(x)H'.$$

这个映射显然是满射,因为 f 是满同态. 如果 $f(x)H' = f(y)H'$,

则 $f(y)^{-1}f(x)\in H'$,即 $f(y^{-1}x)\in H'$,那么 $y^{-1}x\in H$(因为 H 是 H' 的原像),故 $xH=yH$, $\bar{f}$ 是双射.即 $|G/H|=|G'/H'|$.这就是(1)所要证明的.

(2) 先证关于正规性的结论.由本节习题7(4),只剩下要证:如果 $\mathrm{Ker}(f)\leqslant H\lhd G$,则有 $f(H)\lhd G'$.这是因为对于任意 $x'\in G'$ 存在 $x\in G$ 使得 $f(x)=x'$,因而 $x'^{-1}f(H)x'=f(x^{-1}Hx)=f(H)$.再证关于商群同构的结论.在(1)的证明中我们已有了一个双射 $\bar{f}:G/H\to G'/H'$,现在只要证明它是群同态即可.按 $\bar{f}$ 的定义,注意到 H 和 H' 分别都是正规子群,对于任意 $xH,yH\in G/H$ 我们有

$$\begin{aligned}\bar{f}((xH)\cdot(yH))&=\bar{f}((xy)H))=f(xy)H'=f(x)f(y)H'\\&=f(x)H'\cdot f(y)H'=\bar{f}(xH)\cdot\bar{f}(yH).\end{aligned}$$

这就完成了全部证明. □

回到 $\mathbb{Z}$ 和 $\mathbb{Z}_m$.它们不仅有加法而且有乘法,$\mathbb{Z}_m$ 中的乘法同样是用代表元在 $\mathbb{Z}$ 中的乘法来定义(如同加法一样是合理定义的,见习题 1.1.11),而且乘法对加法满足分配律.

1.2.17 定义 如果非空集合 R 上有加法"+"和乘法"·"两种运算,且满足下述三条:

(1) $(R,+)$ 是一个加群(运算写作加法的交换群);

(2) 乘法满足结合律,乘法对加法满足左、右两个分配律;

(3) 有元素 $1\in R$ 使得 $x1=x=1x$, $\forall x\in R$,则称 $(R,+,\cdot)$ 是一个环;元素 1 称为环的单位元(unity).元素 $a\in R$ 称为可逆元(invertible element)(有的文献称单位(unit))如果存在 $a'\in R$ 使得 $aa'=1=a'a$,此时 a' 称为 a 的逆元,也可记作 a^{-1}(单位元、可逆元的逆元具有惟一性,见本节习题 11).记 $R^*=\{a\in R\mid a\text{ 可逆}\}$,易验证 R^* 在乘法下构成群(见本节习题 11),称 R^* 为环 R 的乘群.

如果环 R 的乘法还满足交换律,则称 R 为交换环.

进一步,如果交换环 F 的所有非零元都是可逆元,即 $F^*=F-\{0\}$,则称为域.

环 R 到环 R' 的映射 $f: R \to R'$ 称为环同态，如果 f 不仅是加群同态而且保持乘法，即

$$f(xy) = f(x)f(y), \forall\, x, y \in R.$$

环的单同态、全同态、环同构等意义自明，不再赘述.

很显然，$\mathbb{Z}$ 和 $\mathbb{Z}_m$ 都是交换环，而 $\mathbb{Z} \to \mathbb{Z}_m, x \mapsto [x]$，是环的全同态. 在习题 1.11(6) 中已有下述结论.

1.2.18 例 $\mathbb{Z}_m^* = \{[x] \in \mathbb{Z}_m \mid (x, m) = 1\}$；群阶 $|\mathbb{Z}_m^*| = \varphi(m)$，称为 Euler 函数，见式(1.1.15).

特别是，如果 $m = p$ 是一个素数，那么显然 $\varphi(p) = p - 1$，所以 $\mathbb{Z}_p$ 是一个域.

习题 1.2

1. 设 G 是一个群，$H \leqslant G, a, b \in G$. 证明以下条件彼此等价：

(1) $aH \cap bH \neq \varnothing$；

(2) $aH = bH$；

(3) $a^{-1}b \in H$；

(4) $b^{-1}a \in H$；

(5) $a \in bH$；

(6) $b \in aH$.

2. 设 $K \leqslant H \leqslant G$. 则 $|G:K| = |G:H| \cdot |H:K|$.

3. 设 G 是群，$H \leqslant G$. 则下述条件等价：

(1) H 的任一右陪集也是一个左陪集；

(2) $yH = Hy, \forall\, y \in G$；

(3) $yHy^{-1} = H, \forall\, y \in G$；

(4) $yhy^{-1} \in H, \forall\, y \in G$ 和 $h \in H$.

4. 任何群 G 的中心 $Z(G)$ 的任何子群是 G 的正规子群. 交换群的任何子群是正规子群.

5. 设 G 是一个群，S, T, W 是 G 的子集，令 $ST = \{st \mid s \in S,$

$t \in T\}$ 称 ST 为 S 与 T 之积，$S^{-1} = \{s^{-1} \mid s \in S\}$. 则：

(1) $(ST)W = S(TW)$；于是可写成 STW.

(2) $(ST)^{-1} = T^{-1}S^{-1}$.

(3) 若 $W \leqslant G$ 且 $1 \in S \subset W$，则 $WS = SW = W$.

(4) $W \leqslant G$ 当且仅当 $W^{-1} = W$ 且 $WW = W$.

(5) 设 H 是正规子群，则两个陪集之积仍是陪集，而商群中的乘法就是陪集相乘.

(6) 设 H 是正规子群，K 是子群；则 $HK = KH$，而且这个乘积是子群.

6. 两个正规子群之积仍然是正规子群. 两个正规子群之交仍然是正规子群

7. 设 $f: G \to G'$ 是群同态. 则：

(1) $f(1_G) = 1_{G'}$.

(2) 对于任意 $x \in G$ 有 $f(x^{-1}) = f(x)^{-1}$.

(3) 如果 $H \leqslant G$，则 $f(H)$ 在 G 中的原像是 $H \cdot \mathrm{Ker}(f)$.

(4) 如果 $H' \trianglelefteq G'$，则 H' 在 G 中的原像 $\trianglelefteq G$.

(5) 若 f 是同构，则 $f^{-1}: G' \to G$ 也是群同构.

8. 利用同态基本定理证明：$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$.

9. 设 G 是群，$H, K \leqslant G$. 如果 $\{h_i \mid i \in I\}$ 是 $H \cap K$ 在 H 中左陪集代表系，证明 $HK = \bigcup_{i \in I} h_i K$ 是不交并；推出：

$$|HK| = (|H| \cdot |K|)/|H \cap K|$$

$$|H : H \cap K| \leqslant |G : K|.$$

10. 记号同上题. 证明：

(1) $|G : H \cap K| \leqslant |G : H| \cdot |G : K|$.

(2) 若 $|G : H|$ 与 $|G : K|$ 都有限并互素，则上式中等号成立.

11　设 R 是一个环.

(1) 证明 R 的单位元是惟一的.

(2) 设 $a \in R$ 是可逆元，则 a 的逆元是惟一的.

(3) 证明 R^*(见定义 1.2.17)在乘法之下是一个群.

12. (1) 证明 Euler 定理:如果$(a,m)=1$,则 $a^{\varphi(m)} \equiv 1 \pmod{m}$.

(2) 证明 Fermat 小定理:设 p 是素数,则 $a^p \equiv a \pmod{p}$, $\forall a \in \mathbb{Z}$.

§1.3 循环子群 循环群

循环子群就是由一个元素生成的子群.我们从子集生成子群开始.

1.3.1 定义 若 S 为群 G 的子集,记

$$\langle S\rangle = \bigcap_{S\subset H\leqslant G} H;$$

由习题 1.1.10,$\langle S\rangle$ 是 G 的子群,称$\langle S\rangle$ 为 G 中由子集 S 生成的子群.另一方面,对于 $x \in G$ 和 $n \in \mathbb{Z}$,定义

$$x^n = \begin{cases} \overbrace{x\cdots x}^{n}, & \text{若 } n>0; \\ 1, & \text{若 } n=0; \\ \overbrace{x^{-1}\cdots x^{-1}}^{-n}, & \text{若 } n<0. \end{cases}$$

则指数律成立(见本节习题 1)

$$x^m x^n = x^{m+n}, \quad \forall m,n \in \mathbb{Z};$$

$$(x^m)^n = x^{mn}, \quad \forall m,n \in \mathbb{Z}.$$

那么(见本节习题 5)

$$\langle S\rangle = \{s_1^{n_1}\cdots s_k^{n_k} \mid s_i \in S, n_i \in \mathbb{Z}, k>0\}.$$

特别地,若 $S=\{a\}$ 由一个元构成,则记

$$\langle S\rangle = \langle a\rangle = \{a^n \mid n \in \mathbb{Z}\};$$

称$\langle S\rangle$ 为 G 中由元素 a 生成的循环子群.如果存在有限子集 S 使得 $G=\langle S\rangle$,则称 G 为有限生成的群.特别是,如果 $G=\langle a\rangle$ 由一个元生成,则称 G 为循环群,而 a 称为循环群 G 的一个生成元.显

然一个循环群可以有几个不同的生成元,见下面的例子.

注解　如果群 G 是交换群,那么群 G 中的运算也可记作加法"+",此时单位元改称零元,并改记作 0,此时 G 也可称作加群;那么上述定义有相应的加群表达方式,仅举一例如下:

$$mx + nx = (m + n)x, \qquad \forall\, m, n \in \mathbb{Z};$$
$$n(mx) = (nm)x, \qquad \forall\, m, n \in \mathbb{Z}.$$

1.3.2 例　整数加群$(\mathbb{Z}, +) = \langle 1\rangle = \langle -1\rangle$,而且只有这两个元可以是它的生成元(见下面 1.3.4 引理).

1.3.3 例　整数剩余类加群$(\mathbb{Z}_m, +) = \langle [1]\rangle$,而且$(\mathbb{Z}_m, +) = \langle [a]\rangle$ 当且仅当 $\gcd(a, m) = 1$(见本节习题 6). 从而加群 $\mathbb{Z}_m$ 的生成元恰好有$\varphi(m)$ 个(参见例 1.1.14).

1.3.4 引理　设 $H \leqslant \mathbb{Z}$, $|\mathbb{Z} : H| = m$. 则

$$H = \begin{cases} \langle m\rangle = m\mathbb{Z}, & \text{若 } m \text{ 有限;} \\ \langle 0\rangle = \{0\}, & \text{若 } m \text{ 无限.} \end{cases}$$

证明　如果 H 只含零,当然 $H = \{0\} = \langle 0\rangle$,此时$|\mathbb{Z} : H| = \infty$. 下设 H 含非零整数. 设 $m \in H$ 是 H 中绝对值最小的非零整数;由于 H 是子群,故 $-m \in H$,而 $|-m| = |m|$;所以还可设 m 是正的. 对于任意 $a \in H$,由带余除法,存在 $q, r \in \mathbb{Z}$ 使得 $0 \leqslant r < m$ 而 $a = qm + r$. 但由 H 是子群,得到 $r = a - qm \in H$,而 $|r| < m$;按照 m 的取法,只能是 $r = 0$. 所以 $a = qm \in \langle m\rangle$. 因此 $H = \langle m\rangle = m\mathbb{Z}$;而且此时我们已熟知$\mathbb{Z}/H = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$,即 $|\mathbb{Z} : H| = m$. 总而言之,恰好只有引理所说的两种情形. □

现在我们可以刻画所有的循环群了.

1.3.5 定理　设 $G = \langle a\rangle$ 是由 a 生成的循环群. 则映射 $f: \mathbb{Z} \to G, n \mapsto a^n$,是群的满同态,而且:

(1) 若 $|G| = m < \infty$,则 $\mathbb{Z}_m \to G, [n] \mapsto a^n$ 为同构;特别地,$a^h = a^k$ 当且仅当 $h \equiv k \pmod m$,从而 $1 = a^0, a^1, a^2, \cdots, a^{m-1}$ 是 G 的全部互不相同的元.

(2) 若$|G|=\infty$,则$\mathbb{Z}\to G, n\mapsto a^n$为同构;特别地,$a^h=a^k$当且仅当$h=k$,从而$\cdots,a^{-1},1=a^0,a^1,a^2,\cdots$是$G$的全部互不相同的元.

证明 容易验证定理所定义的f是群的满同态.根据同态基本定理,满同态f诱导同构$\bar{f}:\mathbb{Z}/\mathrm{Ker}(f)\cong G$,再由引理1.3.4,存在惟一非负整数$m'$使得$\mathrm{Ker}(f)=m'\mathbb{Z}$;而且有两种情况:

(1) 若$|G|=m<\infty$,则必须是$m=m'$,从而$\mathbb{Z}/\mathrm{Ker}(f)=\mathbb{Z}_m$,即$f:\mathbb{Z}_m\to G,[n]\mapsto a^n$,为同构.那么按剩余类的定义和由$f$诱导的同构$\bar{f}$的定义(参看同态基本定理),定理的情形(1)中后面的结论都是显然的了.

(2) 若$|G|=\infty$,则必须是$m'=0$,从而$\mathbb{Z}/\mathrm{Ker}(f)=\mathbb{Z}/\{0\}=\mathbb{Z}$;即上述同态$f$就是同构.那么定理的情形(2)中后面的结论就更是显然的了. □

1.3.6 定义 设G为群,$a\in G$.则循环子群$\langle a\rangle$的阶称为元素a的阶,记作$|a|$.

1.3.7 推论 设G为群,$a\in G$

(1) 元素a的阶是使得$a^m=1$的最小正整数m,若此正整数不存在,则$|a|=\infty$.

(2) 如果$|a|=m<\infty$,则$a^h=a^k$当且仅当$h\equiv k\pmod m$;特别地,$a^k=1$当且仅当$m|k$;又对任意整数k有$|a^k|=m/\gcd(k,m)$.

(3) 若$|a|=\infty$,则$a^h=a^k$当且仅当$h=k$;特别地,对于任意非零整数k有$|a^k|=\infty$.

证明 (1) 把定理1.3.5用到循环子群$\langle a\rangle$就得所求证结论.

(2) 前两个结论是定理1.3.5(1)的直接推论.第三个结论,对于任意整数n有$(a^k)^n=1$当且仅当$a^{kn}=1$当且仅当$m|(kn)$当且仅当$\dfrac{m}{\gcd(m,k)}\Big|\left(\dfrac{k}{\gcd(m,k)}n\right)$,因为$\dfrac{m}{\gcd(m,k)}$与

$\frac{k}{\gcd(m,k)}$ 互素，所以 $(a^k)^n = 1$ 当且仅当 $\frac{m}{\gcd(m,k)} \mid n$. 由上述已获证的(1) 知 $|a^k| = m/\gcd(k,m)$.

(3) 类似于(2) 的证明使用定理 1.3.5(2) 即可，而且这里更简单. □

1.3.8 推论　设 G 为有限群，$a \in G$. 则 $|a| \mid |G|$，特别有，$a^{|G|} = 1$.

证明　由 Lagrange 定理 1.2.5 和元素的阶的定义 1.3.6，立即得 $|a| \mid |G|$；后一结论由推论 1.3.7(2) 立即得出. □

1.3.9 定理　设 $G = \langle a \rangle$ 为 m 阶循环群 则对于任意 $d \mid m$，G 恰有一个 d 阶子群，它也是循环群由 $a^{m/d}$ 生成.

证明　由推论 1.3.7(2) 有 $|a^{m/d}| = \frac{m}{\gcd(m, m/d)} = d$；所以 $\langle a^{m/d} \rangle$ 是 G 的 d 阶子群. 再设 $H \leqslant G$ 且 $|H| = d$，证明 $H = \langle a^{m/d} \rangle$ 即可. 考虑定理 1.3.5 中的满同态 $f: \mathbb{Z} \to G, n \mapsto a^n$，显然 $\mathrm{Ker}(f) = m\mathbb{Z}$；由引理 1.3.4，$H$ 在 $\mathbb{Z}$ 中的原像是循环群 $m'\mathbb{Z} \supseteq m\mathbb{Z}$. 由子群对应定理 1.2.16(1)，我们有 $m' = |\mathbb{Z} : m'\mathbb{Z}| = |G : H| = m/d$. 因为 $m'\mathbb{Z}$ 由 m' 生成，由本节习题 4，H 由 $f(m') = a^{m'} = a^{m/d}$ 生成. □

现在考虑任意有限群 G，由推论 1.3.8，任意 $a \in G$ 的阶有限且为 $|G|$ 的因子. 对于正因子 $d \mid |G|$，令 $\psi_G(d)$ 表示 G 中阶为 d 的元素的个数. 则

$$|G| = \sum_{d \mid |G|} \psi_G(d). \qquad (1.3.10)$$

(d 跑遍 $|G|$ 的正因子.)

利用式(1.3.10) 可证明下述数论结果.

1.3.11 命题　设 m 为正整数，$\varphi(m)$ 记 Euler 函数. 则

$$m = \sum_{d \mid m} \varphi(d).$$

(d 跑遍 m 的正因子.)

证明 取群 G 为 m 阶的循环群. 对于任意正因子 $d|m$，若 $a \in G$ 是 d 阶元，则由定理1.3.9，$\langle a\rangle$ 是 G 的惟一一个 d 阶子群，所以 G 的任何 d 阶元都在 $\langle a\rangle$ 中. 但由本节习题6(3)，$\langle a\rangle$ 恰有 $\varphi(d)$ 个 d 阶元；所以 $\psi_G(d) = \varphi(d)$. 代入式(1.3.10)就得到本命题. □

1.3.12 命题 设有限群 G 的阶为 m. 如果对于任意 $d|m$，关于 λ 的方程 $\lambda^d = 1$ 在 G 中至多有 d 个解，则 G 是循环群.

证明 对于群 G 考虑式(1.3.10). 如果 $\psi_G(d) > 0$，则 G 有 d 阶元 a，于是 $\langle a\rangle$ 是 d 阶子群. 由推论 1.3.8，$\langle a\rangle$ 的所有元满足方程 $\lambda^d = 1$；那么由条件，$\langle a\rangle$ 以外的任何元不满足方程 $\lambda^d = 1$，特别是，$\langle a\rangle$ 以外没有 d 阶元. 但由本节习题6(3)，$\langle a\rangle$ 恰有 $\varphi(d)$ 个 d 阶元；即 $\psi_G(d) = \varphi(d)$. 所以对任意 $d|m$ 都有 $\psi_G(d) \leqslant \varphi(d)$. 但由式(1.3.10)和命题 1.3.11 我们有 $\sum\limits_{d|m}\psi_G(d) = \sum\limits_{d|m}\varphi_G(d)$. 因此只能是 $\psi_G(d) = \varphi(d)$，$\forall\, d|m$. 取 $d = m$，就得 $\psi_G(m) = \varphi(m) > 0$；亦即群 G 有 m 阶元，所以 G 是循环群. □

一个简单有用的推论是：

1.3.13 命题 域的乘群的有限子群是循环群

证明 在域中关于 λ 的方程 $\lambda^d = 1$ 至多有 d 个解. □

注解 显然，对于任意域上的多项式余式定理都成立. 那么作为余式定理的推论，任意域中的 d 次多项式至多有 d 个根.

习题 1.3

1. 证明群中指数律

$$a^m a^n = a^{m+n};$$
$$(a^m)^n = a^{mn}.$$

2. 设群 G 中元素 x, y 满足 $xy = yx$，则对于任意整数 n 有

$(xy)^n = x^n y^n$. 举例说明条件 $xy = yx$ 不可缺少.

3. (1) 证明: p 阶群是循环群,这里 p 为素数.

(2) 群 G 称为单群,如果只有 G 和 1 是 G 的正规子群. 证明:只有素数阶群是交换单群.

4. 设 $G = \langle a \rangle$ 是循环群,设 $f: G \to H$ 是群同态. 则 $f(G) = \langle f(a) \rangle$;即循环群的同态的像是由其生成元的像所生成的循环子群

5. 设 S 是群 G 的子集,令 $\bar{S} = S \cup S^{-1}$,参见习题 1.2.5. 则

$$\langle S \rangle = \{1\} \cup \bar{S} \cup \bar{S}\bar{S} \cup \bar{S}\bar{S}\bar{S} \cup \cdots.$$

6. (1) 证明 $|\mathbb{Z}_m : \langle [a] \rangle| = \gcd(a, m)$,这里 $[a] \in \mathbb{Z}_m$.

(2) $\mathbb{Z}_m = \langle [a] \rangle \Longleftrightarrow \gcd(a, m) = 1$.

(3) 证明 n 阶循环群中有 $\varphi(n)$ 个生成元,这里 $\varphi(n)$ 是数论 Euler 函数(见例 1.1.14 与例 1.2.18).

7. 设 G 为群, $a, b \in G$ 满足 $ab = ba$.

(1) 如果 a 与 b 的阶互素,则 $|ab| = |a| \cdot |b|$.

(2) 举例说明,即使 $ab = ba$,一般也不成立 $|ab| = |a| \cdot |b| / \gcd(|a|, |b|)$.

8. 设 G 是群, $a, b \in G$. 证明:

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

(2) $|a| = |bab^{-1}|$.

(3) $|ab| = |ba|$.

9. 设 $f: G \to H$ 是群同态, $x \in G$, $n \in \mathbb{Z}$. 则:

(1) $f(x^n) = f(x)^n$;

(2) 若 $|x| < \infty$,则 $|f(x)| < \infty$ 且 $|f(x)| \mid |x|$.

10. 设 G 和 H 都是循环群. 则存在从 G 到 H 的全同态当且仅当或者 $|G| = \infty$ 或者 $|G|, |H| < \infty$ 且 $|H| \mid |G|$.

11. 证明有理数加群 $\mathbb{Q}$ 的任一有限生成子群是循环子群;但 $\mathbb{Q}$ 不是循环群.

12. 证明：

(1) 有限群中阶大于 2 的元素的个数是偶数.

(2) 偶阶群中必有 2 阶元.

13. 设 $G=\langle a\rangle$ 是 m 阶循环群，ω 是一个本原 m 次单位根；若 $\chi: G\to\mathbb{C}^*$ 是群同态，这里 $\mathbb{C}^*$ 是复数域的乘群. 那么存在惟一整数 k 满足 $0\leqslant k<m$ 使得 $\chi(a)=\omega^k$. 特别是，G 到 $\mathbb{C}^*$ 的群同态有且只有 m 个.

14. 设 G 是群，$a\in G$，$|a|=m$.

(1) 如果 $m=m_1m_2$ 且 $\gcd(m_1,m_2)=1$，则存在 $a_1,a_2\in G$ 使得 $a=a_1a_2$ 且 $a_1a_2=a_2a_1$ 且 $|a_1|=m_1$ 而 $|a_2|=m_2$. 又若 $a_1',a_2'\in G$ 也使得这些成立则 $a_1'=a_1$ 且 $a_2'=a_2$.

(2) 如果 $m=m_1\cdots m_r$ 而 $m_1,\cdots,m_r$ 两两互素，则存在 $a_1,\cdots,a_r\in G$ 使得 $a=a_1\cdots a_r$ 且 $a_ia_j=a_ja_i$，$\forall\,1\leqslant i,j\leqslant r$，且 $|a_i|=m_i$，$i=1,\cdots,r$. 又若 $a_1',\cdots,a_r'\in G$ 也使得这些成立则 $a_i'=a_i$，$i=1,\cdots,r$.

§1.4 中国剩余定理

为介绍中国剩余定理，我们从直积概念开始.

1.4.1 定义 设 G_1 和 G_2 是群. 在集合 $G_1\times G_2$ 中定义：

$$(g_1,g_2)\cdot(h_1,h_2)=(g_1\cdot h_1,g_2\cdot h_2),$$
$$\forall\,(g_1,g_2),(h_1,h_2)\in G_1\times G_2.$$

则易验证在此运算之下集合 $G_1\times G_2$ 构成一个群，单位元是 $(1_{G_1},1_{G_2})$，元 (g_1,g_2) 的逆元是 (g_1^{-1},g_2^{-1}). 这个群称为群 G_1 和群 G_2 的直积. 定义 1.4.1 能以显然的方式推广到任意多个群的直积，而且“结合律”成立(见本节习题 1)

$$(G_1\times G_2)\times G_3\cong G_1\times G_2\times G_3\cong G_1\times(G_2\times G_3)$$

在直积 $G_1\times G_2$ 中有两个正规子群

$$G_1' = \{(x_1,1) \mid x_1 \in G_1\} \cong G_1,$$
$$G_2' = \{(1,x_2) \mid x_2 \in G_2\} \cong G_2.$$

它们满足：

条件：任一元 $g = (g_1,g_2) \in G_1 \times G_2$ 存在惟一的 $g_1' \in G_1'$ 和 $g_2' \in G_2'$ 使得 $g = g_1' \cdot g_2'$.

因此如果群 $G \cong G_1 \times G_2$，那么，令 G_1' 在 G 中的原像是 H_1，而 G_2' 在 G 中的原像是 H_2；则：

(1) H_1 和 H_2 都是 G 的正规子群(子群对应定理).

(2) 任一元 $g \in G$ 存在惟一的 $h_1 \in H_1$ 和 $h_2 \in H_2$ 使得 $g = h_1 \cdot h_2$.

换言之，G 就像是 H_1 与 H_2 的直积. 但此时 H_1 与 H_2 都在 G 之中，所以我们介绍如下定义：

1.4.2 定义　设 $H_1,H_2,\cdots,H_k$ 是群 G 的正规子群. 如果对于任意 $g \in G$ 存在 $h_1 \in H_1,h_2 \in H_2,\cdots,h_k \in H_k$ 使得 $g = h_1h_2\cdots h_k$；而且若 $h_1' \in H_1,h_2' \in H_2,\cdots,h_k' \in H_k$ 也使得 $g = h_1'h_2'\cdots h_k'$，则 $h_1' = h_1,h_2' = h_2,\cdots,h_k' = h_k$；则称群 G 是其正规子群 $H_1,H_2,\cdots,H_k$ 的内直积，记作 $G = H_1 \times H_2 \times \cdots \times H_k$.

注意：当考虑加群时当然就把运算写作加法，此时通常把直积称为直和，记作 $G_1 \oplus G_2$.

所以定义 1.4.1 中的直积理应称作“外直积”. 这里我们对外直积和内直积用了同样的记号，其实它们本质上也确实相同，因为在定义 1.4.2 中不仅群 G 的元素 g 写成 $g = h_1h_2\cdots h_k$ 的形式写法是惟一的，而且由本节习题 4(1)，运算也是按分量进行的：$g = h_1h_2\cdots h_k$，$g' = h_1'h_2'\cdots h_k'$，则 $gg' = h_1h_1' \cdot h_2h_2' \cdot \cdots \cdot h_kh_k'$. 所以我们把外直积和内直积统称直积. 在实际环境中可以从上下文区别究竟是内直积还是外直积.

1.4.3 引理　设 G 是群，$H_1 \trianglelefteq G$ 和 $H_2 \trianglelefteq G$. 则 $G = H_1 \times H_2$

当且仅当 $G = H_1H_2$ 和 $H_1 \cap H_2 = 1$.

证明 设 $G = H_1 \times H_2$,则当然 $G = H_1H_2$,而且对于任意 $x \in H_1 \cap H_2$ 可以写成 $x = x \cdot 1 = 1 \cdot x$,按直积的定义,元素的写法具有惟一性就必须有 $x = 1$;即 $H_1 \cap H_2 = 1$.

反之设这两条件成立.由 $G = H_1H_2$,对于任意 $g \in G$ 存在 $h_1 \in H_1$ 和 $h_2 \in H_2$ 使得 $g = h_1h_2$. 如果还有 $g = h_1'h_2'$ 其中 $h_1' \in H_1$ 和 $h_2' \in H_2$, 则 $h_1h_2 = h_1'h_2'$, 则有 $(h_1')^{-1}h_1 = h_2'(h_2)^{-1} \in H_1 \cap H_2 = 1$; 故 $(h_1')^{-1}h_1 = 1 = h_2'(h_2)^{-1}$;就是 $h_1' = h_1$ 和 $h_2' = h_2$. 所以 $G = H_1 \times H_2$. □

从两个整数开始引入本节主要定理.我们将看到,虽然是考虑两个整数,但是确实容易推到一般情形.

设 m_1 和 m_2 是两个整数.由于要同时考虑 $\mathbb{Z}_{m_1}$ 和 $\mathbb{Z}_{m_2}$,把它们的元素分别记作 $[x]_{m_1}$ 和 $[x]_{m_2}$. 它们都是循环群. 考虑直和 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 的两个元素.

$$a_1 = ([1]_{m_1}, [0]_{m_2}), \quad a_2 = ([0]_{m_1}, [1]_{m_2}).$$

对于任意 $([x]_{m_1}, [y]_{m_2}) \in \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$,按定义有

$$([x]_{m_1}, [y]_{m_2}) = x \cdot a_1 + y \cdot a_2.$$

设 $m = m_1m_2$. 显然下述映射是同态

$$\eta: \mathbb{Z} \to \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}, x \mapsto ([x]_{m_1}, [x]_{m_2}).$$

而且容易计算($\mathrm{lcm}(m_1, m_2)$ 记 m_1 和 m_2 的最小公倍数)

$$\begin{aligned}\mathrm{Ker}(\eta) &= \{x \in \mathbb{Z} \mid [x]_{m_1} = 0, [x]_{m_2} = 0\} \\ &= \{x \in \mathbb{Z} \mid m_1 \mid x, m_2 \mid x\} \\ &= \{x \in \mathbb{Z} \mid \mathrm{lcm}(m_1, m_2) \mid x\} \\ &= \mathrm{lcm}(m_1, m_2)\,\mathbb{Z}\end{aligned}$$

进一步,设 m_1 与 m_2 互素(更具体地,可以设想 $m_1 = 2, m_2 = 3$),即有 $k_1, k_2 \in \mathbb{Z}$ 使得

$$k_1 m_1 + k_2 m_2 = 1.$$

而且 $\operatorname{lcm}(m_1, m_2) = m_1 m_2 = m$ 从而

$$\operatorname{Ker}(\eta) = m\mathbb{Z}.$$

另一方面,显然

$$\eta(k_2 m_2) = a_1, \eta(k_1 m_1) = a_2;$$

所以

$$\begin{aligned}&\eta(x \cdot (k_2 m_2) + y \cdot (k_1 m_1))\\ &= x \cdot a_1 + y \cdot a_2 = ([x]_{m_1}, [y]_{m_2});\end{aligned}$$

即

$$\operatorname{Im}(\eta) = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}.$$

于是由同态基本定理立即得到同构

$$\begin{aligned}&\bar{\eta}: \mathbb{Z}_m \xrightarrow{\cong} \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2},\\ &[x]_m \mapsto ([x]_{m_1}, [x]_{m_2}).\end{aligned}$$

举一个具体例子,取 $m_1 = 2, m_2 = 3$,那么

$$2 \cdot 2 + (-1) \cdot 3 = 1$$

所以

$$\bar{\eta}([3]_6) = \bar{\eta}([(-1) \cdot 3]_6) = ([-3]_2, [-3]_3) = ([1]_2, [0]_3),$$

$$\bar{\eta}([4]_6) = \bar{\eta}([2 \cdot 2]_6) = ([4]_2, [4]_3) = ([0]_2, [1]_3).$$

而我们有内直和 $\mathbb{Z}_6 = H_1 \oplus H_2$,其中

$$\begin{aligned}H_1 &= \langle [3]_6 \rangle \cong \mathbb{Z}_2,\\ H_2 &= \langle [4]_6 \rangle = \langle [2]_6 \rangle \cong \mathbb{Z}_3.\end{aligned}$$

利用"结合律",由归纳法,容易把上述结论推广到有限个直和项的直和,这就是:

1.4.4 定理(中国剩余定理) 设 $m_1, m_2, \cdots, m_k$ 是两两互素的整数,$m = m_1 m_2 \cdots m_k$. 则有同构映射:

$$\begin{aligned}&\eta: \mathbb{Z}_m \xrightarrow{\cong} \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}\\ &[x]_m \mapsto ([x]_{m_1}, [x]_{m_2}, \cdots, [x]_{m_k})\end{aligned}$$ □

注解 实际上这个映射是环同构，即它还保持剩余类的乘法，当然这里右边的乘法也是按分量来做

$$\begin{aligned}\eta([x]_m[y]_m) &= \eta([xy]_m)\\ &= ([xy]_{m_1},[xy]_{m_2},\cdots,[xy]_{m_k})\\ &= ([x]_{m_1}[y]_{m_1},[x]_{m_2}[y]_{m_2},\cdots,[x]_{m_k}[y]_{m_k})\\ &= ([x]_{m_1},[x]_{m_2},\cdots,[x]_{m_k})\cdot([y]_{m_1},[y]_{m_2},\cdots,[y]_{m_k})\\ &= \eta([x]_m)\cdot\eta([y]_m).\end{aligned}$$

进一步，容易看出$\mathbb{Z}_{m_1}\oplus\cdots\oplus\mathbb{Z}_{m_k}$中的元素$([x_1]_{m_1},[x_2]_{m_2},\cdots,[x_k]_{m_k})$可逆当且仅当每个分量$[x_i]_{m_i}$在$\mathbb{Z}_{m_i}$中可逆；这是因为

$$([x_1]_{m_1},[x_2]_{m_2},\cdots,[x_k]_{m_k})\cdot([x_1']_{m_1},[x_2']_{m_2},\cdots,[x_k']_{m_k})=([1]_{m_1},[1]_{m_2},\cdots,[1]_{m_k})$$

当且仅当

$$[x_i]_{m_i}\cdot[x_i']_{m_i}=[1]_{m_i},\forall\, i=1,2,\cdots,k.$$

于是从定理 1.4.4 就可以得到以下推论.

1.4.5 推论 条件与定理 1.4.4 相同.对于乘法群则有群同构

$$\begin{aligned}\eta^*:\mathbb{Z}_m^*&\xrightarrow{\cong}\mathbb{Z}_{m_1}^*\times\mathbb{Z}_{m_2}^*\times\cdots\times\mathbb{Z}_{m_k}^*\\ [x]_m&\mapsto([x]_{m_1},[x]_{m_2},\cdots,[x]_{m_k})\end{aligned}$$

特别是，$|\mathbb{Z}_m^*|=|\mathbb{Z}_{m_1}^*|\cdot|\mathbb{Z}_{m_2}^*|\cdot\cdots\cdot|\mathbb{Z}_{m_k}^*|$；即

$$\varphi(m_1m_2\cdots m_k)=\varphi(m_1)\varphi(m_2)\cdots\varphi(m_k),$$

这里 $m_1,m_2,\cdots,m_k$ 是两两互素的整数，$\varphi(m)$ 是 Euler 函数.

□

1.4.6 推论 设 $p_1,p_2,\cdots,p_k$ 是两两互异的素数，$l_1,l_2,\cdots,l_k$ 是正整数.则

$$\varphi(p_1^{l_1}\cdots p_k^{l_k})=p_1^{l_1-1}(p_1-1)\cdots p_k^{l_k-1}(p_k-1).$$

证明 由上述推论及例 1.2.18，只需指出 $\varphi(p^l)=p^{l-1}(p-1)$.为此，直接计数0到 p^l 之间有多少个与 p 互素的整数，这样的数都

可写成 $r+kp, 1\leqslant r<p, 0\leqslant k<p^{t-1}$，恰好 $p^{t-1}(p-1)$ 个.

□

把上述结果与Fermat小定理(习题1.2.12)结合起来，提示我们考虑下面的情形.

1.4.7 命题 设 $p_1, p_2, \cdots, p_k$ 是两两互异的素数，$m=p_1p_2\cdots p_k$. 对于任意整数 e，构作 $\mathbb{Z}_m$ 的变换 τ_e 如下

$$\tau_e:\mathbb{Z}_m\to\mathbb{Z}_m, [a]\mapsto[a^e].$$

(1) 如果 $e\equiv e'\pmod{\varphi(m)}$，则 $\tau_e=\tau_{e'}$，从而任一 $[e]\in\mathbb{Z}_{\varphi(m)}$ 决定集合 $\mathbb{Z}_m$ 的一个变换 $\tau_{[e]}$ 使得 $\tau_{[e]}([a])=[a^e]=[a]^e$.

(2) 对于任意 $[e],[d]\in\mathbb{Z}_{\varphi(m)}$ 有 $\tau_{[e][d]}=\tau_{[e]}\tau_{[d]}$.

(3) $\tau_{[1]}=\mathrm{id}_{\mathbb{Z}_m}$.

证明 (1) 条件 $e\equiv e'\pmod{\varphi(m)}$ 是说有整数 t 使得 $e'=e+t\varphi(m)$. 现在先设 $k=1$ 即 $m=p_1$. 因为 $\mathbb{Z}_{p_1}-\{0\}=\mathbb{Z}_{p_1}^*$ 是阶为 $\varphi(p_1)$ 的群，所以当 $a\not\equiv 0\pmod{p_1}$ 时，有 $a^{\varphi(p_1)}\equiv 1\pmod{p_1}$，那么

$$a^{e'}=a^{e+t\varphi(m)}=a^e\cdot a^{t\varphi(m)}\equiv a^e\cdot 1\equiv a^e\pmod{p_1}.$$

而在 $a\equiv 0\pmod{p_1}$ 时当然也有 $a^{e'}\equiv a^e\pmod{p_1}$. 所以恒有 $a^{e'}\equiv a^e\pmod{p_1}$，即 $\tau_e=\tau_{e'}$.

对于一般情形，因为 $\varphi(m)=\varphi(p_1)\cdots\varphi(p_k)$，所以由条件 $e\equiv e'\pmod{\varphi(m)}$ 可得到

$$e\equiv e'\pmod{\varphi(p_i)},\quad \forall\, i=1,2,\cdots,k.$$

那么由上面已证明的情形，就有

$$a^e\equiv a^{e'}\pmod{p_i},\quad \forall\, i=1,2,\cdots,k.$$

但 $p_1, p_2, \cdots, p_k$ 两两互素，故 $a^e\equiv a^{e'}\pmod{m}$，即 $\tau_e=\tau_{e'}$.

(2) $\tau_{[e][d]}(a)=[a^{de}]=[a^d]^e=(\tau_{[d]}(a))^e=\tau_{[e]}(\tau_{[d]}(a))=(\tau_{[e]}\cdot\tau_{[d]})(a)$.

(3) 按 $\tau_{[e]}$ 的定义，显然 $\tau_{[1]}=\mathrm{id}_{\mathbb{Z}_m}$. □

命题1.4.7(3)可看做Fermat小定理(习题1.2.12)的一个推广形式.见下述推论.

推论 条件同命题1.4.7.如果 $e \equiv 1 \pmod{\varphi(m)}$,那么 $a^e \equiv a \pmod{m}$, $\forall\, a \in \mathbb{Z}$.

当然这里 $m = p_1 \cdots p_k$ 是彼此不同的素数之积.在 $k = 1$ 即 $m = p$ 是一个素数,而且取 $e = p$ 时,自然 $p \equiv 1 \pmod{\varphi(p)}$ 因 $\varphi(p) = p - 1$,则上述结论就是 $a^p \equiv a \pmod{p}$.这就是Fermat小定理(习题1.2.12).

下述推论是显然的,但该推论导致以上知识在密码方面的一个应用.

1.4.8 推论 记号如上.如果 $[e]_{\varphi(m)} \in \mathbb{Z}_{\varphi(m)}^*$,则 τ_e 是可逆变换,即是 $\mathbb{Z}_m$ 的置换.

证明 由条件,存在整数 d 使得 $ed \equiv 1 \pmod{\varphi(m)}$.由命题1.4.7(2)和(3)即知, $\tau_d\tau_e = \tau_{de} = \tau_1 = \mathrm{id}_{\mathbb{Z}_m} = \tau_e\tau_d$;即 τ_d 是 τ_e 的逆变换. □

1.4.9 例 (RSA公钥系统简介)取两个互异的素数 p 和 q,令 $m = pq$.取整数 e, d 使得 $ed \equiv 1 \pmod{\varphi(m)}$,这里 $\varphi(m) = (p-1)(q-1)$.那么变换 τ_e 把 $\mathbb{Z}_m$ 的元一一地变为 $\mathbb{Z}_m$ 的元: $a \mapsto a^e$.但如果不知道 d 而只是得到了经过变换的元,就无法知道它是从哪个元变来的.这就提供了一种设计密码的思路如下.

网络使用者A要求在必要时别人发送给他的信息须为密文,任何他人无法破译.于是需要一种公开的加密办法使任何人可以使用(称为公钥),然而解密办法却需要使任何他人无法获得(称为私钥).为此,A可取充分大的素数 p, q,令 $m = pq$;取整数 e, d 使 $ed \equiv 1 \pmod{\varphi(m)}$.将信息用模 m 的数 a 表示.加密办法为:

计算 a^e 模 m 的余数 r,发送 r 给A.

那么由推论1.4.8,A可将得到的信息 r 解密为 a

$$r^d \equiv a^{ed} \equiv a \pmod{m}$$

这里加密与解密方法都是公开的;关键数据(即所谓钥匙)m,e 与 d 中,m 与 e 是公开的(因而称为公钥),任何人可用它们将信息加密后通过网络发送给 A;然而 d 只有 A 自己知道(即所谓私钥 ,当然 p 与 q 也保密,但它们在加密、解密过程中不需要),他人不知,从而无法从 r 得到 a.

由于上述原理也是公开的,所以从理论上讲,根据 m,e 可以求出分解式 $m = pq$. 然后在剩余类乘群 $\mathbb{Z}^*_{(p-1)(q-1)}$ 中可求出 e 的逆元 d,也就是使得 $ed \equiv 1 \pmod{(p-1)(q-1)}$ 的 d. 换句话说,私钥 d 从理论上讲并非"私钥".

此系统之所以可以应用,是因为这种从公钥 e 求解私钥 d 的过程在实际上几乎无法实施. 这奠基在如下算法理论与实践之上. 已知确定的 m 与 e,计算 a^e 模 m 的余数 r(以及在解码时计算 r^d 模 m 的余数) 所需时间为 a 的多项式函数,尽管在实践中 m 取得很大,从而 a 也可很大,在现代计算机中仍可很快完成运算. 然而要破译,就得找出 d,于是如上所说就得对 m 做素分解(或在 $\mathbb{Z}_m$ 中求 r 的 e 次根,或其他做法等,其算法复杂程度也等价于分解 m);现在知道的最快素分解算法所需时间为 m 的指数函数,例如,m 为 100 位数时计算机分解 m 的时间约为 74 年,这在实际上几乎是不可能的!

习题 1.4

1. 设 G_1, G_2, G_3 是群,证明

$$(G_1 \times G_2) \times G_3 \cong G_1 \times G_2 \times G_3 \cong G_1 \times (G_2 \times G_3).$$

2. 设 G, G_1, G_2 是群,$f_1: G \to G_1$ 与 $f_2: G \to G_2$ 是群同态. 则映射

$$f = (f_1, f_2): G \to G_1 \times G_2, \quad f(x) = (f_1(x), f_2(x))$$

是群同态,且:

(1) $\mathrm{Ker}(f) = \mathrm{Ker}(f_1) \cap \mathrm{Ker}(f_2)$.

(2) $\mathrm{Im}(f) = G_1 \times G_2$ 当且仅当 $\mathrm{Ker}(f_1) \cdot \mathrm{Ker}(f_2) = G$.

(3) 举例说明:即使 f_1 和 f_2 都是全射,f 也不一定是全射.

3. 设 G_1, G_2 是群,设 $H_1 \leqslant G_1, H_2 \leqslant G_2$.

(1) $H_1 \times H_2 \leqslant G_1 \times G_2$,且

$$|G_1 \times G_2 : H_1 \times H_2| = |G_1 : H_1| \cdot |G_2 : H_2|.$$

(2) 如果 $H_1 \trianglelefteq G_1, H_2 \trianglelefteq G_2$;则 $H_1 \times H_2 \trianglelefteq G_1 \times G_2$,且

$$(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2).$$

4. 设 G 是其正规子群 H_1 和 H_2 的直积.

(1) 证明:$h_1 h_2 = h_2 h_1, \forall\, h_1 \in H_1, \forall\, h_2 \in H_2$.

(2) 如果 $h_1 \in H_1$ 和 $h_2 \in H_2$ 都是有限阶元,则 $h_1 h_2$ 是有限阶元且

$$|h_1 h_2| = |h_1| \cdot |h_2| / \gcd(|h_1|, |h_2|).$$

5. 设 p 是素数.有限群 P 称为 p- 群,如果 $|P| = p^l$,其中 l 是非负整数.证明:一个循环 p- 群不同构于两个非平凡的群的直积.

6. 设 $H_i \trianglelefteq G, i = 1,2,\cdots,k$.则 $G = H_1 \times H_2 \times \cdots \times H_k$ 当且仅当以下两条件成立:

(1) $G = H_1 H_2 \cdots H_k$;

(2) $H_{i+1} \cap (H_1 H_2 \cdots H_i) = 1, \forall\, i = 1,2,\cdots,k-1$.

7. 设 $n > 2$,证明:$2 \mid \varphi(n)$.

8. 证明:小于 m 且与 m 互素的 $\varphi(m)$ 个正整数之和为 $m\varphi(m)/2$.

9. 取 $p = 3, q = 11, m = pq = 33, e = 3$ 构作 RSA 系统(参见例 1.4.9),求私钥 d.

§1.5 有限交换群

除了循环群外,有限生成交换群是结构最清楚的一类群.但我们将只用到有限交换群.

首先我们给出所谓的 Sylow 分解. 下述定义是一般性的.

1.5.1 定义　设 p 是素数. 如果群的元素 x 的阶是 p 的幂,就说 x 是 p- 元. 如果群的子群 H 的每个元素的阶都是素数 p 的幂,就说 H 是 p- 子群. 极大的 p- 子群称为 Sylow p- 子群. 根据后面将要证的 Sylow 定理 2.3.3,有限的 p- 子群的阶显然也是 p 的幂. 所以这里的定义与习题 1.4.5 说的是一致的.

一个群的所有元素的阶的最小公倍数称为这个群的幂指数(exponent),记作 $\exp(G)$;如果有无限阶元或者这个最小公倍数不存在,则说 $\exp(G) = \infty$. 显然有限群的幂指数总有限;而且,如果这个群是有限交换群,则一定存在元素,它的阶就是这个群的幂指数. 见本节习题 2.

这一节讨论交换群时运算写作乘法.

1.5.2 引理　设 A 是有限交换群,$|A| = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$,其中 $p_1, p_2, \cdots, p_k$ 是互异的素数,$l_1, l_2, \cdots, l_k$ 是正整数. 设 $A_i = \{x \in A \mid x \text{ 是 } p_i\text{- 元}\}$,$i = 1, 2, \cdots, k$. 则每个 A_i 都是 A 的子群,且

$$A = A_1 \times A_2 \times \cdots \times A_k.$$

证明　由 A 的交换性,易验证 A_i 都是 A 的子群,从而是正规子群. 按照定义 1.4.2,剩下只要证明 A 的任一元惟一地写成 p_1- 元,p_2- 元,$\cdots$,p_k- 元之积,而这就是习题 1.3.14. □

下面着重讨论 p- 群,始终设 p 是一个素数.

1.5.3 引理　设 A 是有限交换 p- 群,设 a 是 A 中一个阶极大的元. 则存在子群 B 使得

$$A = \langle a \rangle \times B.$$

证明　按引理 1.4.3,就是要找一个子群 B 使得 $A = \langle a \rangle B$ 且 $\langle a \rangle \cap B = 1$. 设 B 是 A 中满足要求 $\langle a \rangle \cap B = 1$ 的阶最大的子群,那么乘积 $\langle a \rangle B$ 显然是子群,而且 $\langle a \rangle B = \langle a \rangle \times B$,见引理 1.4.3. 只要证明 $\langle a \rangle \times B = A$ 即可.

用反证法. 假设 $\langle a \rangle \times B \neq A$;则存在元素 $x \in A$ 但 $x \notin \langle a \rangle$

$\times B$. 那么存在 k 使得 $x^{p^k} \in \langle a\rangle \times B$ 但是 $x^{p^{k+1}} \in \langle a\rangle \times B$. 取 $y = x^{p^k}$; 则

$$y \in \langle a\rangle \times B \quad \text{但是} \quad y^p \in \langle a\rangle \times B.$$

特别是, 可以写 $y^p = a^i b_1$ 其中 $b_1 \in B$. 若 $|y^p| = p^s$ 即 $|y| = p^{s+1}$, 则 $a^{ip^s} \cdot b_1^{p^s} = (y^p)^{p^s} = 1$; 由于 $\langle a\rangle \times B$ 是直积, 由定义 1.4.2, $a^{ip^s} = 1$; 故 $|a| \mid (ip^s)$; 但 $|a| \geqslant |y| = p^{s+1}$; 所以 $p \mid i$; 可以写成 $i = jp$, 即 $y^p = a^{jp} b_1$. 令 $z = ya^{-j}$, 就有 $z^p = y^p a^{-jp} = b_1 \in B$. 因为 $y = za^j \in \langle a\rangle \times B$, 所以 $z \in \langle a\rangle \times B$. 总之, 我们得到: $z \in \langle a\rangle \times B$ 但是 $z^p = b_1 \in B$; 从而

$$\langle z\rangle \cap \big(\langle a\rangle \times B\big) = \langle z^p\rangle. \tag{1.5.3.1}$$

令 $B' = \langle B, z\rangle = \{bz^s \mid b \in B, s \in \mathbb{Z}\} \leqslant A$. 因 $z \notin B$ 所以 $|B'| > |B|$; 由 B 的极大性, $B' \cap \langle a\rangle \neq \{1\}$; 就有 $1 \neq w \in B' \cap \langle a\rangle$. 于是存在 $b \in B$ 及整数 s, t 使得 $w = a^t = bz^s$; 特别是 $z^s = b^{-1}a^t \in B \times \langle a\rangle$. 由式(1.5.3.1), $s = pr$ 从而 $z^s = (z^p)^r = b_1^r$. 那么 $w = a^t = bz^s = bb_1^r \in B \cap \langle a\rangle = \{1\}$; 得到 $w = 1$, 与 $w \neq 1$ 矛盾. □

1.5.4 推论 有限交换 p- 群可以写成循环 p- 子群的直积.

证明 对群阶使用归纳法. 由以上引理, $A = \langle a\rangle \times B$, 其中 $|a| = \exp(A)$, 见本节习题2. 那么 $|B| < |A|$; 所以按归纳法, B 可以写成循环 p- 子群的直积: $B = \langle a_2\rangle \times \langle a_3\rangle \times \cdots \times \langle a_r\rangle$. 于是 $A = \langle a\rangle \times \langle a_2\rangle \times \cdots \times \langle a_r\rangle$. □

结合引理 1.5.2 和推论 1.5.4, 立即得到结论:

1.5.5 引理 引理1.5.2中的有限交换群 A 可以写成一些循环 p_1- 子群, …, 一些 p_k- 子群的直积.

下面要证明在某种意义下这种写法是惟一的. 为此先考虑一种特殊的交换 p- 群: 称为初等交换 p- 群, 它的每个非单位元都是 p 阶元. 下面说的 $\mathbb{Z}_p$ 是域一事, 请见例 1.2.18; 为方便, 记 $F_p =$

$\mathbb{Z}_p$.

1.5.6 引理　初等交换 p- 群 A(这一次为方便把运算写作加法)可以下述方式作为域 $\boldsymbol{F}_p = \mathbb{Z}_p$ 上的向量空间:对 $[n] \in \boldsymbol{F}_p$, $a \in A$, 纯量积定义为 $[n] \cdot a = na$. 而作为向量空间 A 的 1 维子空间就是作为群 A 的 p 阶循环子群.

证明　如果 $[n'] = [n]$, 则 $n' = n + kp$, 故 $n'a = (n + kp)a = na + kpa = na$; 所以引理中的纯量积 $[n] \cdot a = na$ 是合理定义的. 很容易验证向量空间的所有定义条件在这里是满足的; 按纯量积的定义, 1 维子空间显然就是 p 阶循环子群. □

1.5.7 引理　设 A 是有限交换 p- 群. 对于任意 $i \geqslant 0$ 下述子集合

$$\Omega_i(A) = \{a \in A \mid |a| \mid p^i\} = \{a \in A \mid a^{p^i} = 1\}$$

是 A 的子群. 在 $A \neq \{0\}$ 时 $\Omega_1(A)$ 是 A 的极大的初等交换 p- 子群.

证明　对于任意 $a, b \in \Omega_i(A)$ 有 $a^{p^i} = 1 = b^{p^i}$, 那么 $(ab)^{p^i} = a^{p^i} b^{p^i} = 1$(习题 1.3.2); 即 $ab \in \Omega_i(A)$. 所以 $\Omega_i(A)$ 是子群, 见命题 1.1.11, 后一结论为显然. □

1.5.8 引理　设 A 是有限交换 p- 群. 如果

$$\begin{aligned} A &= \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_r \rangle \\ &= \langle a_1' \rangle \times \langle a_2' \rangle \times \cdots \times \langle a_r' \rangle; \end{aligned}$$

而各元素的阶为

$$|a_1| = p^{l_1}, |a_2| = p^{l_2}, \cdots, |a_r| = p^{l_r},$$
$$l_1 \geqslant l_2 \geqslant \cdots \geqslant l_r;$$
$$|a_1'| = p^{l_1'}, |a_2'| = p^{l_2'}, \cdots, |a_r'| = p^{l_r'}$$
$$l_1' \geqslant l_2' \geqslant \cdots \geqslant l_r';$$

那么 $r' = r$ 而且

$$l_1' = l_1, l_2' = l_2, \cdots, l_r' = l_r.$$

证明 令群 A 的幂指数 $\exp(A) = p^e$;对 e 进行归纳. $e = 1$ 时,引理中的分解就是 A 作为域 F_p 上的向量空间的 1- 维子空间分解,由线性代数得 $r' = r$;而此时所有 l_i 和 l_i' 都等于 1,所以引理成立.

再设 $e > 1$. 由本节习题 3(1) 知 $\exp(A) = p^{l_1} = p^{l_1'}$. 则不妨设

$$l_t = e \text{ 但 } l_{t+1} < e$$

$$l_t' = e \text{ 但 } l_{t+1}' < e$$

那么由本节习题 3(2) 和本节习题 4,知道

$$\begin{aligned}\Omega_{e-1}(A) &= \langle a_1^p\rangle \times \cdots \times \langle a_t^p\rangle \times \langle a_{t+1}\rangle \times \cdots \times \langle a_r\rangle \\ &= \langle a_1'^p\rangle \times \cdots \times \langle a_t'^p\rangle \times \langle a_{t+1}'\rangle \times \cdots \times \langle a_r'\rangle\end{aligned}$$

仍由本节习题 3(1) 知 $\exp(\Omega_{e-1}(A)) = e - 1$;按归纳假设,$r' = r$,而且上述 $\Omega_{e-1}(A)$ 的两个分解中各生成元的阶对应相等. 特别是,这两个分解中阶为 p^{e-1} 的直积项的个数相等,阶小于 p^{e-1} 的各元素的阶对应相等. 所以原来引理中的 A 的两个分解中阶小于 p^{e-1} 的各元素的阶对应相等;剩下只要证明引理中的 A 的两个分解中阶为 p^e 的直积项个数相等,即要证 $t' = t$.

A 的这两个分解中阶为 p^e 的直积项个数 t 和 t' 可利用习题 1.4.3(2) 来计算. 按 A 的第一个分解我们有 $|A/\Omega_{e-1}(A)| = p^t$;按第二个分解又有 $|A/\Omega_{e-1}(A)| = p^{t'}$,所以 $t' = t$. □

把引理 1.5.2、推论 1.5.4 和引理 1.5.8 结合起来,就得到本节的主要定理.

1.5.9 定理 设有限交换群 A 如引理 1.5.2 所述,则 A 可分解为循环 p_i- 群 C_{ij}, $i = 1,2,\cdots,k$ 的直积

$$A = C_{11} \times C_{12} \times \cdots \times C_{1r_1} \times \cdots \times C_{k1} \times C_{k2} \times \cdots \times C_{kr_k}$$

又若 A 还有循环 p_i- 群 C_{ij}', $i = 1,2,\cdots,k$,使得

$$A = C_{11}' \times C_{12}' \times \cdots \times C_{1r_1}' \times \cdots \times C_{k1}' \times C_{k2}' \times \cdots \times C_{kr_k'}'$$

则 $r_i' = r_i, i = 1,2,\cdots,k$;且适当重排直积因子顺序后有

$$|C_{ij}'| = |C_{ij}|, \forall\, i = 1,2,\cdots,k, \forall\, j = 1,2,\cdots,r_i.$$

1.5.10 定义　定理 1.5.9 中 A 的循环分解的各直积项的阶的全体称为有限交换群 A 的初等因子,其属于素数 p_i 的初等因子称为 p_i- 初等因子.

习题 1.5

1. 设 $U \subseteq \mathbb{C}^*$是所有单位根(即存在正整数 n 使得$\lambda^n = 1$ 的复数 λ, n 称为此单位根的次数) 的集合.

(1) 证明:U 是$\mathbb{C}^*$的子群, U 的每个元素阶有限,但 $\exp(U) = \infty$.

(2) $\mathbb{C}^*$的任何有限子群包含在 U 中.

2. 设 A 是有限交换群. 证明存在 $a \in A$ 使得$|a| = \exp(A)$.

3. 设 A, B 是有限交换 p- 群. 则

(1) $\exp(A \times B) = \max\{\exp(A), \exp(B)\}$.

(2) $\Omega_i(A \times B) = \Omega_i(A) \times \Omega_i(B)$.

4. 设 $A = \langle a \rangle$ 是有限循环 p- 群, $|a| = p^l$. 则

$$\Omega_i(A) = \begin{cases} \langle a^{p^{l-i}} \rangle, & \text{若 } 0 \leqslant i \leqslant l; \\ \langle a \rangle, & \text{若 } l < i. \end{cases}$$

5. 找出所有的 8 阶交换群.

6. 设有限交换群 A 可以写成两个子群之积$A = A_1A_2$. 则 $A = A_1 \times A_2$ 当且仅当$|A| = |A_1| \cdot |A_2|$.

7. 设 A 是初等交换 p- 群,设$|A| = p^n$, $0 \leqslant k \leqslant n$. A 的 p^k 阶子群有多少个?

8. 设 A 是有限交换群, $|A| = n$. 证明:对于任意 $d \mid n$, A 有阶 d 的子群.

9. 设 A 是有限交换 p- 群. 则 A 是循环群当且仅当 A 只有一个 p 阶子群.

10. 设 A 是有限交换群.

(1) A 有非平凡循环子群 $A_1, A_2, \cdots, A_r$ 使得 $A = A_1 \times A_2 \times \cdots \times A_r$ 而且 $|A_{i+1}| \mid |A_i|$ 对于所有 $1 \leqslant i < r$.

(2) 如果非平凡循环子群 $B_1, B_2, \cdots, B_{r'}$ 也使得(1)成立,则 $r' = r$ 而且 $|B_i| = |A_i|$ 对于所有 $1 \leqslant i < r$(这些子群的阶的序列 $|A_1|, |A_2|, \cdots, |A_r|$ 称为 A 的不变因子).

11. 设有限交换群 A 是它的子群的直积 $A = A_1 \times A_2 \times \cdots \times A_k$. 设 B 是交换群.

(1) 如果对于每个 $i = 1, 2, \cdots, k$ 有群同态 $f: A_i \to B$,则可定义映射 $f = f_1 \times f_2 \times \cdots \times f_k : A \to B$ 为:对于任意 $a \in A$ 写 $a = a_1 a_2 \cdots a_k$,其中 $a_i \in A_i$,令 $f(a) = f_1(a_1) f_2(a_2) \cdots f_k(a_k)$,而且 f 是群同态.

(2) 如果 $f: A \to B$ 是群同态,则限制映射 $f_i = f|_{A_i} : A_i \to B$, $i = 1, 2, \cdots, k$,都是群同态,而且 $f = f_1 \times f_2 \times \cdots \times f_k$.

12. 设有限交换群 A 是它的循环子群的直积 $A = A_1 \times A_2 \times \cdots \times A_r$.

(1) 如果 $\chi_i : A_i \to \mathbb{C}^*, i = 1, 2, \cdots, r$,是群同态,这里 $\mathbb{C}^*$ 是复数域的乘群,则 $\chi_1 \times \chi_2 \times \cdots \times \chi_r : A \to \mathbb{C}^*$ 是群同态.

(2) A 到 $\mathbb{C}^*$ 的所有同态都可以按(1)的方式构造出来.

(3) A 到 $\mathbb{C}^*$ 共有多少个互不相同的同态?

第 2 章　群 作 用

§2.1　置换的分解

我们已知道，有限集合 X 的所有双射变换的集合 $\mathrm{Sym}(X)$ 在变换的乘法运算（即合成运算）之下是一个群，称为 X 的对称群. 但我们又常常把 X 取为 n 个文字的集合 $\{1,2,\cdots,n\}$，其对称群称为 n 次对称群，记作 S_n. 实际上，从数学结构来说它们本质上是一样的.

2.1.1 引理　设 X 与 Y 是两个基数相等的有限集合. 则对于任意一双射 $f: X \to Y$，映射

$$\bar{f}:\ \mathrm{Sym}(X) \xrightarrow{\cong} \mathrm{Sym}(Y), \alpha \mapsto f \cdot \alpha \cdot f^{-1}$$

是群同构并使得

$$(f \cdot \alpha)(x) = \bar{f}(\alpha) \cdot f(x), \forall\, \alpha \in \mathrm{Sym}(X)\ \forall\, x \in X.$$

证明　按照 $\bar{f}$ 的定义可以容易地直接验证它是群同态. 再从 f 的逆映射 $f^{-1}: Y \to X$ 也可诱导

$$\widetilde{f^{-1}}: \mathrm{Sym}(Y) \xrightarrow{\cong} \mathrm{Sym}(X), \beta \mapsto f^{-1} \cdot \beta \cdot f$$

那么显然容易验证 $\bar{f}$ 与 $\widetilde{f^{-1}}$ 正好互为逆映射. 所以 $\bar{f}$ 是群同构. 最后的等式从计算来看是显然的：$f \cdot \alpha = f \cdot \alpha \cdot f^{-1} \cdot f = \bar{f}(\alpha) \cdot f$. 从下面的交换图图 2-1 更容易理解它.

所以考虑置换群时，集合中的元素是什么并不重要；一般情况下讨论 S_n 就足够了.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ a\downarrow & & \downarrow faf^{-1}=\tilde{f} \\ X & \xrightarrow[f]{} & Y \end{array}$$ □

图 2-1

在命题 1.1.3 中我们已叙述了下述结论.

2.1.2 引理 (1) 任意二个彼此无公共文字的循环置换相乘可交换.

(2) 任一置换在不计乘积顺序的意义下可以惟一地写成彼此无公共文字的循环置换之积使得每个文字恰出现一次,称为置换的循环分解. □

把 n 次置换 α 的循环分解

$$\alpha=(a_{11}a_{12}\cdots a_{1t})(a_{21}a_{22}\cdots a_{2j})\cdots(a_{r1}a_{r2}\cdots a_{rk})$$

中的括号去掉,就是 $1,2,\cdots,n$ 的一个排列. 如(264)(13)(5),去掉括号就是 264135.

反之,对于 $1,2,\cdots,n$ 的任意一个排列加上括号就可以是一个 n 次置换的循环分解.

2.1.3 引理 设 $\alpha=(a_{11}a_{12}\cdots a_{1t})(a_{21}a_{22}\cdots a_{2j})\cdots(a_{r1}a_{r2}\cdots a_{rk})$ 是 n 次置换 α 的循环分解,$\gamma\in S_n$. 则

$$\gamma\alpha\gamma^{-1}=(\gamma(a_{11})\gamma(a_{12})\cdots\gamma(a_{1t}))(\gamma(a_{21})\gamma(a_{22})\cdots\gamma(a_{2j}))\cdots$$
$$(\gamma(a_{r1})\gamma(a_{r2})\cdots\gamma(a_{rk}))$$

证明 $a_{11},\cdots,a_{1t},\cdots,a_{r1},\cdots,a_{rk}$ 是 $1,2,\cdots,n$ 的一个置换,所以

$$\gamma(a_{11}),\cdots,\gamma(a_{1t}),\cdots,\gamma(a_{r1}),\cdots,\gamma(a_{rk})$$

也是 $1,2,\cdots,n$ 的一个置换,因而上式右端是一个循环置换分解. 那么只要证明

$$\gamma\alpha\gamma^{-1}(\gamma(a_{11}))=\gamma(a_{12}),\gamma\alpha\gamma^{-1}(\gamma(a_{12}))=\gamma(a_{13}),\cdots$$

即可;而这些式子是显然成立的. □

2.1.4 定义 设 n 次置换 α 的循环分解中长度 l 的循环有 $\lambda_l(\alpha)$ 个，则 λ_l 是置换 α 的非负整函数，称为置换的第 l 个型函数；在 α 确定时，简记为 λ_l. 序列 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 称为该 n 次置换 α 的型；型有时也形式地记作 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$.

一个 n 次置换 α 的型显然满足 $\lambda_1+2\lambda_2+\cdots+n\lambda_n=n$；反之，关于变元 $x_1,x_2,\cdots,x_n$ 的方程 $x_1+2x_2+\cdots+nx_n=n$ 的任何非负整数解 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 是某些 n 次置换的型.

2.1.5 命题 对称群 S_n 中两置换 α 与 β 共轭当且仅当 α 与 β 的型相同，即 $\lambda_l(\alpha)=\lambda_l(\beta)$, $\forall\, l=1,2,\cdots,n$.

证明 必要性，若 $\gamma\alpha\gamma^{-1}=\beta$，由引理2.1.3及定义2.1.4，它们的型相同. 充分性，假设它们的型相同，那么可以把它们的循环分解按循环长度排列使得对应的循环的长度相等

$$\alpha=(a_{11}a_{12}\cdots a_{1r})(a_{21}a_{22}\cdots a_{2r})\cdots(a_{r1}a_{r2}\cdots a_{rk}),$$

$$\beta=(b_{11}b_{12}\cdots b_{1r})(b_{21}b_{22}\cdots b_{2r})\cdots(b_{r1}b_{r2}\cdots b_{rk});$$

那么 $a_{11}a_{12}\cdots a_{1r}\cdots a_{r1}a_{r2}\cdots a_{rk}$ 与 $b_{11}b_{12}\cdots b_{1r}\cdots b_{r1}b_{r2}\cdots b_{rk}$ 都是 $1,2,\cdots,n$ 的排列，所以

$$\gamma=\begin{pmatrix}a_{11}a_{12}\cdots a_{1r}a_{21}a_{22}\cdots a_{2r}\cdots a_{r1}a_{r2}\cdots a_{rk}\\ b_{11}b_{12}\cdots b_{1r}b_{21}b_{22}\cdots b_{2r}\cdots b_{r1}b_{r2}\cdots b_{rk}\end{pmatrix}$$

是一个 n 次置换；由引理2.1.3就得 $\gamma\alpha\gamma^{-1}=\beta$. □

2.1.6 Cauchy公式 型为 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 的 n 次置换个数是

$$\frac{n!}{\lambda_1!\lambda_2!\cdots\lambda_n!\cdot 1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}}.$$

证明 考虑填空模型

$$\overbrace{(\ *\ )\cdots(\ *\ )}^{\lambda_1}\ \overbrace{(\ **\ )\cdots(\ **\ )}^{\lambda_2}\cdots.$$

把 $1,2,\cdots,n$ 填入各 $*$ 位置处，共有 $n!$ 种填法；这样就给出了全部型为 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 的 n 次置换. 但同一个 n 次置换在此过程中重复得出多次：前 λ_1 个括号的任意排列得出同一个置换，这种

重复有 $\lambda_1!$次;类似地,λ_2 个(* *)型括号给出 $\lambda_2!$次重复,等等.又,同一个 k-循环可以有 k 种不同写法(循环中任一文字可以放在首位),而 k-循环有 λ_k 个,就得到 k^{λ_k} 个重复;这里 $k=1,2,\cdots,n$.综合起来,同一个 n 次置换在上述填空过程中重复得出的次数是 $\lambda_1!\lambda_2!\cdots\lambda_n!\cdot 1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$.这样就得到了 Cauchy 公式. □

例 S_3 中型为 $1^1 2^1 3^0$ 的置换有 $3!/(1!1!0!1^1 2^1 3^0)=3$ 个,即有 3 个对换.

注意到一个简单的事实,任意 l-循环可以写成2-循环也就是对换之积

$$(a_1 a_2\cdots a_l)=(a_1 a_l)\cdots(a_1 a_3)(a_1 a_2),$$

对换个数 $l-1$ 是循环长度减 1.那么任意置换 α 就可以写成对换之积.而且有一种写法的对换因子个数是 α 的循环分解中各循环长度减 1 之和,即

$$T(\alpha)=\sum_{l=1}^{n}(l-1)\lambda_l(\alpha)=\sum_{l=1}^{n}(1-\lambda_l(\alpha)). \tag{2.1.7}$$

但把置换写成对换之积的写法肯定不是惟一的,比如,即使一个对换就还可以写成三个对换之积的形式:

$$(ab)=(1a)(1b)(1a).$$

但我们有下述结论(可称为置换的对换分解定理).

2.1.8 定理(置换的对换分解定理) 任意 n 次置换 α 可以写成有限个对换的乘积,其对换因子的个数 $\equiv T(\alpha)\pmod 2$.

证明 这里给出一个代数风格的证明.在第三章中我们还将对此分解的对换因子个数做更多的组合分析.令 $X=\{x_1,x_2,\cdots,x_n\}$ 是 n 个变元的集合;考虑 X 上的多项式

$$f(X)=\prod_{1\leqslant i<j\leqslant n}(x_i-x_j);$$

即任意一对互异的脚标 $i<j$ 恰对应于一个因式.由例 1.1.12 知,对于任意 $\alpha\in S_n$,按对变元脚标的置换使 $f(X)$ 变成多项式 $\alpha f(X)$,那么任意一对互异的脚标 $i<j$ 也恰对应于 $\alpha f(X)$ 的一个

因式,它要么是 $x_i - x_j$ 即与 $f(X)$ 的对应因式相同,要么是 $x_j - x_i = -(x_i - x_j)$. 所以 $\alpha f(X) = \pm f(X)$. 需要确定这个符号.

首先设 $\tau \in S_n$ 是对换. 如果 $\tau = (k, k+1)$ 是相邻对换,显然它仅仅使 $x_k - x_{k+1}$ 变成 $x_{k+1} - x_k = -(x_k - x_{k+1})$,而不改变 $f(X)$ 的其他因式的符号,即 $\tau f(X) = -f(X)$. 对不相邻的对换 (ij),则可分解为 $2(j-i-1)+1$ 个,即奇数个相邻对换之积

$$(ij) = \overbrace{(j-1,j)(j-2,j-1)\cdots(i+1,i+2)}^{j-i-1} \cdot (i,i+1) \cdot \overbrace{(i+1,i+2)\cdots(j-2,j-1)(j-1,j)}^{j-i-1}.$$

所以对于任意对换 $\tau \in S_n$ 我们有 $\tau f(X) = -f(X)$.

回到一般的置换 α,把它写成 $\alpha = \tau_1 \tau_2 \cdots \tau_k$,每个 τ_i 是对换,则 $\alpha f(X) = (-1)^k f(X)$. 但是由式(2.1.7)我们已经知道有一种写法 $\alpha = \tau_1' \tau_2' \cdots \tau_{T(\alpha)}'$;所以 $\alpha f(X) = (-1)^{T(\alpha)} f(X)$. 故得 $(-1)^k = (-1)^{T(\alpha)}$;即是 $k \equiv T(\alpha) \pmod 2$. □

2.1.9 定义 置换 α 称为偶置换,如果 α 可写成偶数个对换之积;否则称 α 为奇置换.

从定理2.1.8立即可以得到下述推论,注意其中 $\{\pm 1\}$ 在乘法之下构成2阶群.

2.1.10 推论 映射 $\sigma: S_n \to \{\pm 1\}$, $\sigma(\alpha) = \begin{cases} 1, & \text{若 } \alpha \text{ 是偶置换,} \\ -1, & \text{若 } \alpha \text{ 是奇置换.} \end{cases}$ 是群同态,特别地,S_n 中所有偶置换的集合 A_n 是 S_n 的正规子群,称为 n 次交错群;且 $|S_n : A_n| = 2$.

习题 2.1

1. 求 S_4 有多少个共轭类.

2. (1) l- 循环置换的阶为 l.

(2) 设 α 和 β 是两个无公共文字的循环置换. 证明: $|\alpha\beta| = |\alpha| \cdot |\beta| / \gcd(|\alpha|, |\beta|)$.

(3) 任一置换 α 的阶是它的循环分解中各循环的长度的最小公倍数.

3. (1) 如果 n 次置换 α 的型是 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$,则 $\lambda_1+2\lambda_2+\cdots+n\lambda_n=n$.

(2) 如果 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 是关于变元 $(x_1,x_2,\cdots,x_n)$ 的方程 $x_1+2x_2+\cdots+nx_n=n$ 的非负整数解,则存在 n 次置换 α,它的型是 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$.

4. 设 n 是自然数.证明:

$$\sum_{(\lambda_1,\lambda_2,\cdots,\lambda_n)}\frac{1}{\lambda_1!\lambda_2!\cdots\lambda_n!\cdot 1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}}=1;$$

其中 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 跑遍方程 $x_1+2x_2+\cdots+nx_n=n$ 的非负整数解.

5. 偶置换与偶置换之积为偶置换;奇置换与奇置换之积为偶置换;奇置换与偶置换之积为奇置换.

6. (1) 对于任意置换 α,平方 α^2 是偶置换.

(2) 奇阶的置换必为偶置换.

7. 设 n 次置换 $\alpha=\begin{pmatrix}1 & 2 & \cdots & n\\ a_1 & a_2 & \cdots & a_n\end{pmatrix}$;对于任意 $i<j$,若 $a_i>a_j$ 就说 (a_ia_j) 是一个逆序对,所有逆序对的个数称为 α 的逆序数,记作 $N(\alpha)$.证明:$N(\alpha)\equiv T(\alpha)\pmod 2$.

8. 证明:S_n 可以由子集 $\{(1\ 2),(1\ 3),\cdots,(1\ n)\}$ 生成.

9. 证明:A_n 可以由子集 $\{(1\ 2\ 3),(1\ 2\ 4),\cdots,(1\ 2\ n)\}$ 生成.

10. 设 G 是一个 n 次置换群,即 $G\leqslant S_n$.证明:如果 G 有奇置换,则奇置换的个数与偶置换的个数相等.

§2.2 群作用

我们在命题1.4.7和推论1.4.8中看到,设 $m=p_1p_2\cdots p_k$ 是

彼此不同的素数之积，对应于乘群$\mathbb{Z}_{\varphi(m)}^*$的任意元$[e]$有集合$\mathbb{Z}_m$上的置换

$$\tau_{[e]}:\mathbb{Z}_m\to\mathbb{Z}_m,[a]\mapsto[a^e];$$

而且$\tau_{[e][d]}=\tau_{[e]}\tau_{[d]}$. 这成为RSA密码系统(见例1.4.9)的数学基础. 群在很多地方以这种形式出现，并成为极有用的工具. 我们把它一般化如下.

2.2.1 定义　设X是集合，G是群. 群G在集合X上的一个作用是说有一个群同态

$$\tau:G\to\mathrm{Sym}(X),g\mapsto\tau(g)(=\tilde{g})$$

(在τ给定不致混淆时，简记$\tau(g)$为$\tilde{g}$) 换言之，每个$g\in G$对应X的一个可逆变换$\tilde{g}$并且$\widetilde{g_1g_2}=\tilde{g}_1\tilde{g}_2,\forall\, g_1,g_2\in G$. 群同态的核$\mathrm{Ker}(\tau)$也称为该作用的核. 这个作用称为忠实的(faithful)如果$\mathrm{Ker}(\tau)=1$，即τ为单同态.

群G在集合X上的一个作用$\tau:G\to\mathrm{Sym}(X)$也称为群G在集合X上的一个变换表示，或者称为置换表示如果X是有限集.

我们用另一个等价的方式来刻画群作用，这种方式在线性代数中已出现.

2.2.2 命题　设X是集合，G是群. 以下两条件等价：

(1) 群G作用在集合X上；

(2) 有一个映射$G\times X\to X,(g,x)\mapsto gx$(为简便，记$(g,x)$的像为$gx$)，满足：

(a) $(g_1g_2)x=g_1(g_2x),\forall\, g_1,g_2\in G,\forall\, x\in X$；

(b) $1_Gx=x,\forall\, x\in X$.

证明　(1)⇒(2). 设$G\to\mathrm{Sym}(X),g\mapsto\tilde{g}$，是按定义2.2.1给的一个群作用. 作映射$G\times X\to X,(g,x)\mapsto\tilde{g}(x)$，即令$gx=\tilde{g}(x)$. 那么

$$(g_1g_2)x=\widetilde{g_1g_2}(x)=(\tilde{g}_1\tilde{g}_2)x=\tilde{g}_1(\tilde{g}_2(x))=g_1(g_2x);$$

即(a)成立.而 $\widetilde{1}_G = \mathrm{id}_X$,(b)显然成立.

(2)⇒(1).从映射 $G\times X\to X,(g,x)\mapsto gx$,任意 $g\in G$ 对应 X 的一个变换 $\tilde{g}:X\to X,\tilde{g}(x)=gx$.由(b)知单位元 1_G 对应恒等变换 $\widetilde{1}_G=\mathrm{id}_X$.再由(a),

$$\widetilde{g_1g_2}(x)=(g_1g_2)x=g_1(g_2x)=\tilde{g}_1(\tilde{g}_2(x))=(\tilde{g}_1\tilde{g}_2)x;$$

即 $\widetilde{g_1g_2}=\tilde{g}_1\tilde{g}_2,\forall g_1,g_2\in G$.特别是,$\tilde{g}\,\widetilde{g^{-1}}=\widetilde{gg^{-1}}=\widetilde{1}_G=\mathrm{id}_X$;同样有,$\widetilde{g^{-1}}\,\tilde{g}=\mathrm{id}_X$;所以 $\tilde{g}\in\mathrm{Sym}(X)$ 是可逆变换.这样就得到一个映射 $G\to\mathrm{Sym}(X),g\mapsto\tilde{g}$;而且这个映射满足:$\widetilde{g_1g_2}=\tilde{g}_1\tilde{g}_2$,$\forall g_1,g_2\in G$;即,这个映射是群同态.得到(1). □

评注 以上证明同时告诉我们群作用的两种表达形式是如何互相转化的.

例 用我们现在的语言,命题 1.4.7 就是说群 $\mathbb{Z}^*_{\varphi(m)}$ 作用在集合 $\mathbb{Z}_m$ 上;RSA 密码系统能保密的关键是:按算法的理论和实践从 $\mathbb{Z}_m$ 很难找到群 $\mathbb{Z}^*_{\varphi(m)}$ 因而很难从变换 τ_e 找到它的逆变换.

2.2.3 例 如果 $G\leqslant\mathrm{Sym}(X)$ 是集合 X 的变换群(置换群,若 X 是有限集),则包含同态 $G\to\mathrm{Sym}(X)$ 给出 G 在 X 的作用,这时 G 的元就是 X 的双射变换(X 的置换若 X 是有限集).所以,群作用是变换群(置换群)的推广;而忠实作用就可等同于变换群(置换群).特别地,关于群作用的结论对于置换群都成立.反过来,关于置换群成立的结论,用到群作用时则需要根据作用的核的情况作适当修正.

例 对于任意 $g\in G$ 令 $\tilde{g}=\mathrm{id}_X$,即作用的核是 G,则这个作用称为平凡作用.

2.2.4 例 设群 G 作用在集合 X 上.令 $P(X)=\{Y\mid Y\text{ 是 }X\text{ 的子集}\}$,即 $P(X)$ 是 X 的幂集.那么对于任意 $g\in G$,$Y\in P(X),\tilde{g}(Y)\in P(X)$;以这种方式,群 G 作用在集合 $P(X)$

上.还可以做得更细致一点.为方便,把 X 的基数为 k 的子集称为 k- 子集.以 $P_k(X)$ 表示 X 的所有 k- 子集的集合.显然,$\bar{g}$ 把 k- 子集变为 k- 子集,所以 G 作用在 $P_k(X)$ 上.G 在 $P_1(X)$ 上的作用就是 G 在 X 上的作用.

下述例子对我们后面的应用有特殊重要性.设群 G 作用在集合 X 上.设 C 是集合,令

$$\mathrm{Hom}(X,C)=\{\varphi\mid\varphi \text{ 是 } X \text{ 到 } C \text{ 的函数}\}.$$

任意 $g\in G$ 对应 X 的可逆变换 $\bar{g}$.对于 $\varphi\in\mathrm{Hom}(X,C)$,显然合成映射 $\varphi\bar{g}$ 仍是从 X 到 C 的函数,即 $\varphi\bar{g}\in\mathrm{Hom}(X,C)$.那么 $\varphi\mapsto\varphi\bar{g}$ 就是集合 $\mathrm{Hom}(X,C)$ 的变换,记作

$$g^*:\mathrm{Hom}(X,C)\to\mathrm{Hom}(X,C),\varphi\mapsto\varphi\bar{g}.$$

于是得到 G 到变换集合 $\mathrm{Tran}(\mathrm{Hom}(X,C))$ 的映射

$$\tau^*:G\to\mathrm{Tran}(\mathrm{Hom}(X,C)),g\mapsto g^*.$$

显然 $\tau^*(1_G)=1_C^*=\mathrm{id}_{\mathrm{Hom}(X,C)}$.对于 $g_1,g_2\in G$,和任意 $\varphi\in\mathrm{Hom}(X,C)$,我们有

$$\begin{aligned}\tau^*(g_1g_2)(\varphi)&=\varphi(g_1g_2)=(\varphi\ g_1)g_2=(\tau^*(g_1)(\varphi))g_2\\&=\tau^*(g_2)(\tau^*(g_1)(\varphi))=(\tau^*(g_2)\tau^*(g_1))(\varphi).\end{aligned}$$

所以

$$\tau^*(g_1g_2)=\tau^*(g_2)\tau^*(g_1),\quad\forall\, g_1,g_2\in G. \tag{2.2.5}$$

那么

$$g^*(g^{-1})^*=(g^{-1}g)^*=1_C^*=\mathrm{id}_{\mathrm{Hom}(X,C)}.$$

特别是,$\mathrm{Im}(\tau^*)\subset\mathrm{Sym}(\mathrm{Hom}(X,C))$,即我们得到映射

$$\tau^*:G\to\mathrm{Sym}(\mathrm{Hom}(X,C)),g\mapsto g^*$$

它满足式(2.2.5).虽然 τ^* 很像群同态,但它不是群同态,因为群同态的要求是 $\tau^*(g_1g_2)=\tau^*(g_1)\tau^*(g_2)$,而式(2.2.5)中的顺序刚好反了.有两种处理办法.一种再简单不过的办法是,就称这种满足式(2.2.5)的 τ^* 为群的反同态.那么我们也可说群 G 反作

用在集合 $\mathrm{Hom}(X,C)$ 上.

另一种是先对群作定义:

2.2.6 定义 设 G 是群,运算写作乘法"·".在集合 G 上定义运算"∘"为 $g_1 \circ g_2 = g_2 \cdot g_1$.则在运算"∘"之下 G 也是一个群,称为原来的群$(G,\cdot)$ 的反群(opposite group).为了与原来的群相区别,记作 G^0.

再回头看 τ^*,它定义在集合 G 上;当然也可把定义域看做反群 G^0:

$$\tau^* : G^0 \to \mathrm{Sym}(\mathrm{Hom}(X,C)), g \mapsto g^*.$$

那么就有

$$\tau^*(g_1 \circ g_2) = \tau^*(g_1)\tau^*(g_2),\ \forall g_1, g_2 \in G \forall \varphi \in \mathrm{Hom}(X,C);$$

所以 τ^* 作为定义在反群 G^0 上的映射是群同态.因此有以下结论.

2.2.7 命题 设群 G 作用在集合 X 上:$g \in G$ 对应为 X 的可逆变换 $\tilde{g}$;设 C 是集合.则 G 在 X 上的作用诱导它的反群 G^0 在集合 $\mathrm{Hom}(X,C)$ 上的作用:$g \in G$ 对应为 $\mathrm{Hom}(X,C)$ 的可逆变换 g^* 使得 $g^*(\varphi) = \varphi\tilde{g}$, $\forall \varphi \in \mathrm{Hom}(X,C)$. □

回想置换的循环分解:设 n 次置换

$$\alpha = (a_{11}a_{12}\cdots a_{1i})(a_{21}a_{22}\cdots a_{2j})\cdots(a_{r1}a_{r2}\cdots a_{rk}).$$

从群作用的角度来看,α 生成的子群$\langle\alpha\rangle$ 可以把文字 a_{11} 变成任一 a_{1t},但不能变为任一 a_{2t},不能变为任一 a_{rt} 等.

这种直观图形(见图 2-2)可以作为下述定义的原始模型.

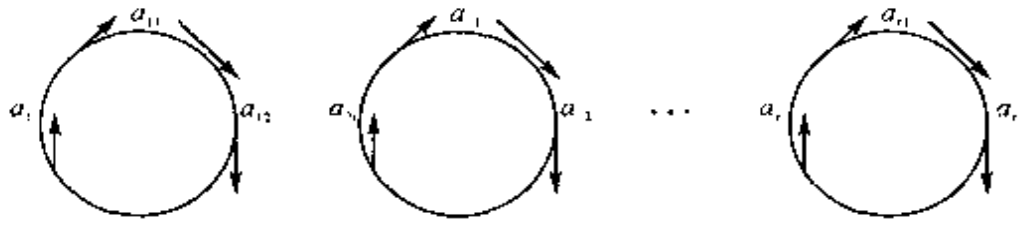


图 2-2

2.2.8 命题与定义　设群 G 作用在集合 X 上. 在 X 上定义关系：对于任意 $x,y\in X$，称 x 被 G- 可迁到 y，记作 $x\sim_G y$，如果存在 $g\in G$ 使得 $\tilde{g}(x)=y$. 则 G- 可迁关系“$\sim_G$”是 X 上的等价关系. 称 X 中关于此关系的等价类为 G- 轨道，简称轨道. 如果 X 的 G- 轨道只有一个，则说 G 在 X 上的作用是可迁的.

证明　自反性显然成立. 若 $\tilde{g}(x)=y$，则 $\widetilde{g^{-1}}(y)=x$，此即对称性. 若 $\tilde{g}_1(x)=y\,\tilde{g}_2(y)=z$，则 $\widetilde{g_2g_1}(x)=z$，传递性成立. □

2.2.9 例　上面说的 a 生成的子群 $\langle a\rangle$ 的轨道就是

$$\Omega_1=\{a_{11},a_{12},\cdots,a_{1t}\},\Omega_2=\{a_{21},a_{22},\cdots,a_{2t}\},\cdots,\Omega_r=\{a_{r1},a_{r2},\cdots,a_{rt}\}$$

设群 G 作用在有限集 X 上，设 $X_1,X_2,\cdots,X_r$ 是全部轨道. 由于 X 必为其轨道的不交并 $X=\bigcup_{i=1}^{r}X_i$，当然有

$$|X|=\sum_{i=1}^{r}|X_i|. \tag{2.2.10}$$

这样一个看起来简单的公式，称为轨道方程，它有时很有用. 其中每轨道的长度 $|X_i|$（即轨道 X_i 中元素个数）可如下计算.

2.2.11 命题　设群 G 作用在集合 X 上. 对于 $x\in X$，记 $\Omega_x=\{\tilde{g}(x)\mid g\in G\}$ 是 x 所在的 G- 轨道；再记 $G_x=\{g\in G\mid\tilde{g}(x)=x\}$. 则：

(1) $G_x\leqslant G$（从而称 G_x 为 x 的稳定子群）；

(2) $|\Omega_x|=|G:G_x|$（称为轨道长公式）.

证明　(1) 显然 $1_G\in G_x$. 设 $g,h\in G_x$；则 $h(x)=x$ 从而 $h^{-1}(x)=x$，那么 $h^{-1}g(x)=x$；得 $h^{-1}g\in G_x$. 于是 G_x 是子群.

(2) 对左陪集 $gG_x\in G/G_x$，令 $\tilde{g}(x)\in X$ 与之对应；按轨道的定义 $\tilde{g}(x)\in\Omega_x$. 若 $g'\in gG_x$，则有 $s\in G_x$ 使得 $g'=gs$，那么 $\tilde{g}'(x)=\tilde{g}\,\tilde{s}(x)=\tilde{g}(x)$. 这样从子群 G_x 的左陪集的集合 G/G_x 到 x 的轨道 Ω_x，我们给出了一个合理定义的映射

$$G/G_x \to \Omega_x, gG_x \mapsto \tilde{g}(x).$$

这显然是满射.另一方面,如果 $gG_x \in G/G_x$ 与 $hG_x \in G/G_x$ 对应的像相等,即 $\tilde{h}(x) = \tilde{g}(x)$,则 $\tilde{h}^{-1}\tilde{g}(x) = x$,从而 $h^{-1}g \in G_x$,也就是 $gG_x = hG_x$ 是同一陪集.故上述映射又是单射.因此上述映射是双射. □

关于群作用时轨道的个数计数则有以下引理:

2.2.12 引理(Burnside 轨道计数公式) 设有限群 G 作用在有限集 X 上.对 $g \in G$ 令 $\mathrm{Fix}(g) = \{x \in X \mid \tilde{g}(x) = x\}$(称为 g 在 X 上的不动点集),则 X 的 G- 轨道的个数 t 为

$$t = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|.$$

注解 容易看出 $|\mathrm{Fix}(g)|$ 就是 g 对应的置换 $\tilde{g}$ 的型 $(\lambda_1(\tilde{g}), \lambda_2(\tilde{g}), \cdots, \lambda_n(\tilde{g}))$ 中的第一个型函数 $\lambda_1(\tilde{g})$ 值;参看定义 2.1.4.

证明 考虑集合 $S = \{(g,x) \mid g \in G, x \in X, \tilde{g}(x) = x\}$ 的计数,有两种途径来计算它.一方面,对于任意一个固定的 $g \in G$,按照 $\mathrm{Fix}(g)$ 的定义这种偶对 (g,x) 的个数是 $|\mathrm{Fix}(g)|$;所以

$$|S| = \sum_{g\in G}|\mathrm{Fix}(g)|. \tag{2.2.12.1}$$

另一方面,对于任意一个固定的 $x \in X$,按照 G_x 的定义这种偶对 (g,x) 的个数是 $|G_x|$,所以

$$|S| = \sum_{x\in X}|G_x|.$$

将 X 划分为轨道的不交并 $X = X_1 \cup X_2 \cup \cdots \cup X_t$.对同一轨道的 $x \in X_i$ 根据轨道长公式 $|G_x| = |G|/|X_i|$.因而

$$\begin{aligned}|S| &= \sum_{i=1}^{t}\sum_{x\in X_i}|G|/|X_i| = |G|\sum_{i=1}^{t}\sum_{x\in X_i}1/|X_i| \\ &= |G|\sum_{i=1}^{t}|X_i|/|X_i| = |G|\cdot t.\end{aligned} \tag{2.2.12.2}$$

比较式(2.2.12.2)与式(2.2.12.1),就得到所要求证的公式. □

2.2.13 注解　在讨论群 G 作用在集合 X 上时,这里为了区别,把群 G 的元素 g 对应的 X 的变换记作 $\tilde{g}$,在 $x \in X$ 上映射的像就是 $\tilde{g}(x)$. 以后,在不致混淆的情况下,为简单计,可把 g 对应的变换也记作 g,作用于 $x \in X$ 的像可简记为 $g(x)$,或更简单地,记作 gx. 比如,上述注解中的 $\lambda_t(\tilde{g})$ 就可写作 $\lambda_t(g)$.

习题 2.2

1. 设 G 是群,X 是集合. 如果映射 $\tau: G \to \mathrm{Tran}(X)$ 满足:

(1) $\tau(g_1 g_2) = \tau(g_1)\tau(g_2), \forall\, g_1, g_2 \in G$;

(2) $\tau(1_G) = \mathrm{id}_X$.

则 τ 是群 G 在集合 X 上的一个作用.

2. 设群 G 作用在集合 X 上,对 $x \in X$,记 G_x 是 x 的稳定子群,见命题 2.2.11. 设 $g \in G$. 证明:$gG_xg^{-1} = G_{\tilde{g}(x)}$.

3. 设群 G 作用在集合 X 上. 证明:群 G 在集合 X 上可迁,当且仅当对于任意 $x, y \in X$,存在 $g \in G$,使得 $\tilde{g}(x) = y$.

4. (1) 设 $\alpha \in S_n$ 为 n- 循环,则 $\langle \alpha \rangle$ 在 $\{1,2,\cdots,n\}$ 上可迁. 特别是,S_n 在 $\{1,2,\cdots,n\}$ 上是可迁作用.

(2) 当 $n > 2$ 时,A_n 在 $\{1,2,\cdots,n\}$ 上是可迁作用.

5. 设群 G 可迁的作用在集合 X 上. 问:G 在 X 的幂集 $P(X)$ 上的作用是否也可迁?

6. 设 G 是群. 证明:映射 $G \to G, g \mapsto g^{-1}$,是群的反同构.

7. 设群 G 作用在集合 X 上,设 C 是集合,而 $\mathrm{Hom}(X,C)$ 如同命题 2.2.7 所定义. 将 $g \in G$ 对应为 $\mathrm{Hom}(X,C)$ 的这样的变换 g^*:对于 $\varphi \in \mathrm{Hom}(X,C)$ 令 $g^*(\varphi) = \varphi\tilde{g}^{-1}$. 证明:群 G 以这一方式作用在集合 $\mathrm{Hom}(X,C)$ 上.

8. 设群 G 既作用在集合 X 上也作用在集合 Y 上. 对于任意 $g \in G$ 和任意 $(x,y) \in X \times Y$,令 $\hat{g}(x,y) = (\tilde{g}(x), \tilde{g}(y))$. 证明:

群 G 作用在集合 $X \times Y$ 上. 如果 G 在集合 X 和集合 Y 上的作用都是可迁的,群 G 在 $X \times Y$ 上的作用可迁吗?考虑 $X = Y$ 的情况

9. 设 X 是 n 次单位根的集合,γ 是复共轭,即 $\gamma(x) = \bar{x}$, $\forall x \in X$.

(1) $G = \{\mathrm{id}_X, \gamma\}$ 是群,且它作用于 X;

(2) 用 Burnside 引理计算 G 在 X 上的轨道个数;

(3) X 正好是复平面上单位圆的等分点的集合,从几何直观观察 G 在 X 上的轨道,与(2) 的结果对照.

10. 设 G 为有限群,取集合 $X = G$,令 $H \leqslant G$. 证明:

(1) H 以下述方式作用于 X:对于 $h \in H$ 和 $x \in X(= G)$, $h(x) = hx$;

(2) 对于 $x \in X$,x 所在的 H- 轨道正好是 H 的右陪集 Hx;

(3) 用轨道长公式证明 $|Hx| = |H|$;

(4) 用 Burnside 引理证明 Lagrange 定理(此仅为练习,因为在 Burnside 引理的证明中引用了 Lagrange 定理).

§2.3 Sylow 定理

这一节我们把群作用思想用到考虑群自己的结构.

在定义 1.2.6 中我们已经看到任意 $a \in G$ 决定 G 的一个自同构 $\tau_a: G \to G, g \mapsto aga^{-1}$,这就给出了群 G 在集合 G 上的一个作用,称为共轭作用. 由于 τ_a 不仅仅是集合 G 的可逆变换,而且实际上是群 G 的自同构,所以我们实际上称 τ 给出了群 G 在群 G 上的作用. 再设 $X \subset G$,那么 X 在 G 中的稳定子群(参见命题 2.2.11) 记作 $N_G(X) = \{g \in G \mid gXg^{-1} = X\}$ 称为 X 在 G 中的正规化子;另一方面,$C_G(X) = \{g \in G \mid gxg^{-1} = x, \forall x \in X\}$ 则称为 X 在 G 中的中心化子. 显然 $C_G(X) \subset N_G(X)$;进一步,实际上 $C_G(X) \trianglelefteq N_G(X)$,而且 $N_G(X)/C_G(X)$ 同构于 X 的一个变换群. 当 $X \leqslant$

G 是子群时，$g \in N_G(X)$ 的共轭变换实际是群 X 的自同构，$N_G(X)/C_G(X)$ 同构于群 X 的一个自同构群(见本节习题 1).

看一个特殊情况. 取 $X = G$，则 $C_G(G) = Z(G)$ 就是群 G 的中心；而 $N_G(G) = G$，$G/Z(G)$ 对应的群 G 的自同构群被称为是群 G 的内自同构群.

2.3.1 引理　设 P 是有限 p- 群，这里 p 是一个素数. 设 P 作用在有限集合 X 上. 令 $\mathrm{Fix}(P) = \{x \in X \mid \bar{g}(x) = x, \forall g \in P\}$，参看 2.2.12 中的记号. 则

$$|X| \equiv |\mathrm{Fix}(P)| \pmod{p}.$$

证明　显然 $x \in \mathrm{Fix}(P)$ 当且仅当 x 的轨道就是 $\{x\}$ 只含一个点. 所以轨道方程(2.2.10) 可写成

$$|X| = |\mathrm{Fix}(P)| + \sum_{|\Omega|>1} |\Omega|, \quad (\Omega \text{ 跑遍基数大于 1 的轨道})$$

若轨道 Ω 长度大于 1，由命题 2.2.11 轨道长公式，$|\Omega| = |P:P_x| > 1$，其中 $x \in \Omega$；但 P 是 p- 群即 $|P| = p^n$ 而 P_x 是 P 的真子群，根据 Lagrange 定理 1.2.5，就得到 $p \mid |P:P_x| = |\Omega|$. 这对于任何长度大于 1 的轨道成立，故 $\sum_{|\Omega|>1} |\Omega|$ 能被 p 整除. 于是就得到所求证同余式. □

将这一公式用到上面分析的群的中心. 对于有限 p- 群 P 在它自己的集合 P 上的共轭作用来说，显然 $\mathrm{Fix}(P) = \{a \in P \mid yay^{-1} = a, \forall y \in P\} = Z(P)$. 即有 $|P| \equiv |Z(P)| \pmod{p}$；特别是，$|Z(P)| \equiv 0 \pmod{p}$. 所以我们得到如下推论.

2.3.2 推论　非平凡有限 p- 群有非平凡的中心. □

仍设 p 是素数；设 G 是任意有限群，可以用上面的思想方法来考虑 G 的“p- 部分”. 设 $|G| = p^a n$，其中 $p \nmid n$，即 p^a 是群阶 $|G|$ 的 p- 部分. 按照 Lagrange 定理，对 G 的任意 p- 子群 P 有 $|P| \mid p^a$；一个基本的定理则说存在 p- 子群使得这成为等号. 为此，考虑 G 的这种子集的集合：$\mathscr{X} = \{S \subset G \mid |S| = p^a\}$. 那么群 G

以“左平移”方式作用在集合 $\mathscr{X}$ 上：对于 $g \in G$ 令

$$\tilde{g}: \mathscr{X} \to \mathscr{X}, S \mapsto gS.$$

显然

$$|\mathscr{X}| = \binom{p^a n}{p^a} = \frac{p^a n(p^a n-1)(p^a n-2)\cdots(p^a n-p^a+1)}{1\cdot 2\cdot 3\cdots(p^a-1)p^a}$$

$$= n \cdot \frac{(p^a n-1)}{1} \cdot \frac{(p^a n-2)}{2} \cdots \frac{(p^a n-p^a+1)}{p^a-1}$$

我们这样写是为了便于考虑分子和分母中所含的 p 的最高次幂. 考虑 $p^a n - r$ 与 r 时，令 r 中所含的 p 的最高次幂是 p^e，记作 $p^e \| r$，因为 $0 < r < p^a$，所以，$e < a$；即 $p^e | p^a$. 因而 $p^e \| (p^a n - r)$；换言之，$p^a n - r$ 与 r 所含的 p 的最高次幂是相等的. 那么由 $|\mathscr{X}|$ 上述表达式知道 $p \nmid |\mathscr{X}|$. 因此，集合 $\mathscr{X}$ 的 G- 轨道中至少有一个轨道长度不被 p 整除. 设轨道 Ω 使得 $p \nmid |\Omega|$；再取 $S \in \Omega$. 按照轨道长公式 2.2.11，$|\Omega| = |G:G_S|$，其中 $G_S = \{g \in G \mid gS = S\}$ 是 S 的稳定子群. 但由 Lagrange 定理 1.2.5，$|G:G_S| |G_S| = |G| = p^a n$，而 $p \nmid |G:G_S|$，所以 $p^a \| |G_S|$. 另一方面，取 $s \in S$，按 G_S 的定义有 $gs \in S, \forall g \in G_S$；因此有映射 $G_S \to S, g \mapsto gs$. 如果 $gs = g's$ 则显然 $g = g'$. 所以这个映射是单射；故 $|G_S| < |S| = p^a$. 于是我们得到 $|G_S| = p^a$.

我们已经证明了下述定理的一部分.

2.3.3 Sylow 定理 设 p 是素数，G 是有限群，$|G| = p^a n$ 而 $p \nmid n$. 则

(1) G 有子群 P 使得 $|P| = p^a$，这种子群称为 G 的 Sylow p- 子群.

(2) 对于 G 的任意 p- 子群 Q 存在 $g \in G$ 使得 $g^{-1}Qg \subset P$；特别是，G 的任意两个 Sylow p- 子群彼此共轭.

(3) G 的 sylow p- 子群的个数 $\equiv 1 \pmod{p}$.

证明 (1) 已证明如上.

(2) 令 C 是 G 中 Sylow p- 子群 P 的左陪集的集合. 让群 Q 以左平移方式作用在集合 C 上:对于 $u \in Q$

$$\tilde{u}: C \to C, gP \mapsto ugP.$$

由于 Q 是 p- 群,由引理 2.3.1

$$|C| \equiv |\mathrm{Fix}(Q)| \pmod{p}.$$

按 Sylow p- 子群的定义,$|P| = p^{\alpha}$;故 $|C| = |G:P| = n$ 与 p 互素;即是说 $|C| \not\equiv 0 \pmod{p}$;从而 $|\mathrm{Fix}(Q)| \neq 0$. 所以有 gP 使得 $ugP = gP, \forall u \in Q$;即 $g^{-1}ugP = P$,从而 $g^{-1}ug \in P, \forall u \in Q$. 换言之,$g^{-1}Qg \subset P$.

(3) 根据(2),知道 $S = \{gPg^{-1} \mid g \in G\}$ 是 G 的所有 Sylow p- 子群的集合 那么群 P 就可以按共轭方式作用在集合 S 上:即对于 $y \in P$

$$\hat{y}: S \to S, gPg^{-1} \mapsto ygPg^{-1}y^{-1}.$$

因而由引理 2.3.1

$$|S| \equiv |\mathrm{Fix}(P)| \pmod{p}.$$

因此只要能证明 $|\mathrm{Fix}(P)| = 1$ 就行了. 设 $Q \in \mathrm{Fix}(P)$,即 $uQu^{-1} = Q, \forall u \in P$,故 $P \subset N_G(Q)$. 那么在群 $N_G(Q)$ 中,$Q \trianglelefteq N_G(Q)$,$P \leqslant N_G(Q)$ 利用第二同构定理(见本节习题 7),子群的乘积 PQ 是一个子群,而且 $|PQ| = |Q| \cdot |P:P \cap Q|$;特别地,$PQ$ 是 p- 子群. 但 Q 是 Sylow p- 子群,PQ 不能比 Q 真大;所以 $P \cap Q = P$,即 $P \subset Q$;而它们的阶相等,故 $Q = P$. 换言之,$\mathrm{Fix}(P) = \{P\}$ 只有一个成员.

至此,Sylow 定理全部证明完毕. □

习题 2.3

1. (1) 设 G 是群,$X \subset G$. 证明:$C_G(X) \trianglelefteq N_G(X)$ 而且 $N_G(X)/C_G(X)$ 同构于 X 的一个变换群.

(2) 进一步设 $X \leqslant G$,证明 $N_G(X)/C_G(X)$ 同构于群 X 的一个自同构群.

2. 设 G 是群，素数 $p \mid |G|$. 考虑 p 元序列的集合

$$\mathscr{S} = \{(g_1, g_2, \cdots, g_p) \mid g_i \in G, g_1 g_2 \cdots g_p = 1\};$$

令 $\alpha = (1\ 2 \cdots p)$ 是 p- 循环置换并令 $Z = \langle \alpha \rangle$，则 p 阶循环群 Z 作用在集合 $\mathscr{S}$ 上：$\tilde{\alpha}(g_1, g_2, \cdots, g_p) = (g_{\alpha(1)}, g_{\alpha(2)}, \cdots, g_{\alpha(p)})$. 利用引理 2.3.1 证明群 G 有 p 阶元素（这结果有时被称为 Cauchy 定理，它显然是 Sylow 定理的简单推论；但也可先证明它，然后从它出发利用简单的群论推理去证明 Sylow 定理）.

3. 设 P 是有限群 G 的一个 Sylow p- 子群. 证明：有限群 G 中 Sylow p- 子群的个数为 $|G : N_G(P)| \mid |G : P|$.

4. 证明：10 阶群只有一个 Sylow 5- 子群从而它一定是正规子群；而它的 Sylow 2- 子群要么是 1 个要么是 5 个. 进一步：

(1) 如果 10 阶群 G 只有一个 Sylow 2- 子群，则 G 是循环群.

(2) 如果 10 阶群 G 有 5 个 Sylow 2- 子群，则 G 由一个 5 阶元 a 和一个 2 阶元 b 生成，而且满足等式 $a^5 = 1 = b^2, bab^{-1} = a^{-1}$. 证明 G 与正五边形的自同构群同构.

(3) 如果群 G 有两个元素 a 和 b 生成，而且满足等式 $a^5 = 1 = b^2$（表示 a 和 b 分别是 5 阶元和 2 阶元），$bab^{-1} = a^{-1}$，则 G 是 10 阶非交换群（群论中称群 G 由生成集 $\{a, b\}$ 按关系 $a^5 = 1 = b^2$，$bab^{-1} = a^{-1}$ 生成）.

5. 证明：在同构意义下，6 阶群只有两个：6 阶循环群，3 次对称群 S_3.

6. 设 P 是有限群 G 的一个 Sylow p- 子群，设 $H \trianglelefteq G$. 证明：$P \cap H$ 是 H 的 Sylow p- 子群，PH/H 是 G/H 的 Sylow p- 子群.

7. （第二同构定理）设 G 是群，$H, K \leqslant G$. 如果 $H \trianglelefteq G$，则：

(1) $HK \leqslant G$；

(2) $H \trianglelefteq HK$ 且 $K \cap H \trianglelefteq K$；

(3) $HK/H \cong K/(H \cap K)$；特别是

$$|HK| = |H| \cdot |K : H \cap K|.$$

8 (Frattini 推理 - 群作用形式) 设群 G 可迁地作用在集合 X 上,设 $H \leqslant G$ 而且 H 在 X 上的作用也是可迁的. 任取 $x \in X$. 证明: $G = HG_x$.

9. (Frattini 推理 - 群论形式) 设 G 是有限群, $H \trianglelefteq G$ 而 $p \nmid |G:H|$. 证明: G 的任何 Sylow p- 子群 P 包含在 H 中;从而 $G = HN_G(P)$.

10. 设 G 是有限群, p 是一个素数而且 $p^r \mid |G|$, 则 G 有 p^r 阶子群.

§2.4 Pólya 计数

首先我们来看一个实际问题,从它引进数学模型.

2.4.1 问题 要设计 n 个珠子的项链,珠子的颜色有红、黄、蓝三种,问共可设计出多少种项链?

如果把珠子标上号 $1,2,\cdots,n$, 则每标号 i 有 3 种选择,故共有 3^n 种颜色配置(见图 2-3); 令 $V = \{1,2,\cdots,n\}$, $C = \{R,Y,B\}$, 则任一映射 $\varphi: V \to C$ 恰是一种颜色配置; 记 $\mathrm{Hom}(V,C) = \{\varphi: V \to C\}$ 是所有 V 到 C 的映射的集合; 则它即为颜色配置的数学模型.

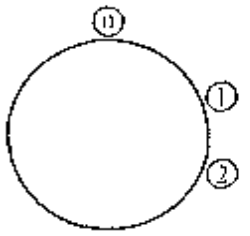


图 2-3

然而,实际上珠子并未标号,例如下述两配置实际上是一样的(见图 2-4):

其原因在于:将左边的配置通过置换 $g = \begin{pmatrix}123\\312\end{pmatrix}$ 后就得到右边的配置,而这个置换并未改变各珠子的位置关系. 进一步观察,置换 g 是 V 的双射;在图 2-4 中,若记图(a) 颜色配置对应的映射是 $\varphi \in \mathrm{Hom}(V,C)$, 则合成映射 $\varphi g \in \mathrm{Hom}(V,C)$ 恰好是图(b) 颜色配置对应的映射. 由此得到直观结论如下:

图 2-4

2.4.2 结论 如果 $\varphi \in \mathrm{Hom}(V,C)$ 是一个颜色配置，而 g 是 V 的一个置换使得珠子之间的位置关系不变，那么合成映射 $\varphi g \in \mathrm{Hom}(V,C)$ 给出的颜色配置在实际观感上是一样的.

这种认识将导致我们建立问题的数学模型.步骤如下：

第一步.考虑 V 的哪些置换不改变珠子的位置关系以及它们有哪些性质？

n 个珠子的项链的框架恰相当于正 n 边形，使它不变的全体空间变换有 $2n$ 个：n 个旋转，n 个反射，它们构成一个群；这 $2n$ 个变换恰对应于 $V=\{1,2,\cdots,n\}$ 的 $2n$ 个置换，例如 $(12\cdots n)$ 是一个旋转，而 $(2,n)(3,n-1)(4,n-2)\cdots$ 是一个反射；这 $2n$ 个置换构成 V 的一个置换群，我们把它记作 G.与 §1.1 的例 1.1.5、例 1.1.8 比较，可以看到，这里的 V 从数学的角度来说不仅仅是集合而且具有某些结构，比如本问题中的 V 不是 n 个点的集合而是正 n 边形，所以结论是：

结论 所考虑的变换的集合 G 在变换乘法之下是结构 V 的自同构群.

第二步.考虑颜色配置所对应的数学对象.

由上述分析我们看到，$\forall\, \varphi \in \mathrm{Hom}(V,C)$ 与 $g \in G$，合成映射 $\varphi g \in \mathrm{Hom}(V,C)$；换言之，$g$ 给出集合 $\mathrm{Hom}(V,C)$ 的一个自映射：$g^{*}:\mathrm{Hom}(V,C)\to \mathrm{Hom}(V,C)$，$\varphi \mapsto \varphi g$；而且

$$P(G;m,m,\cdots,m)=\frac{1}{|G|}\sum_{g\in G}m^{\lambda_1(g)}m^{\lambda_2(g)}\cdots m^{\lambda_n(g)}.$$

证明 由引理 2.2.12,所求轨道数为

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g^*)|$$

其中 $|\mathrm{Fix}(g^*)|$ 为 g^* 在 $\mathrm{Hom}(V,C)$ 上的不动点的集合. 而 $\varphi\in\mathrm{Fix}(g^*)$ 当且仅当 $\varphi g(v)=\varphi(v)\forall v\in V$,当且仅当 $\varphi g^i(v)=\varphi(v),\forall i>0,\forall v\in V$;所以有以下结论.

2.4.7 结论 $\varphi\in\mathrm{Fix}(g^*)$ 当且仅当 φ 在 V 的同一$\langle g\rangle$-轨道上取同一值,即 φ 是$\langle g\rangle$-轨道函数. 换言之,$\mathrm{Fix}(g^*)=\{V$ 的$\langle g\rangle$-轨道集合到 C 的函数$\}$.

长 l 的$\langle g\rangle$-轨道有$\lambda_l(g)$个,取值 C 中的轨道函数在这$\lambda_l(g)$个轨道上可以取值的方式有 $m^{\lambda_l(g)}$ 种. 那么容易算出

$$|\mathrm{Fix}(g^*)|=m^{\lambda_1(g)}m^{\lambda_2(g)}\cdots m^{\lambda_n(g)}.$$

把它代入上面的 Burnside 轨道计数公式即得到本定理. □

2.4.8 例 回到实际问题 2.4.1:$V=\{1,2,\cdots,n\}$,$C=\{\mathrm{R},\mathrm{Y},\mathrm{B}\}$,即 $m=3$;$G=\{n$ 个旋转,n 个反射$\}$. 为简单,取 $n=4$;则 G 的全部元为 (1)(2)(3)(4), (1234), (1432), (13)(24), (12)(34), (14)(23), (1)(3)(24), (2)(4)(13);算出循环指标多项式

$$(2.4.9)\quad P(G;x_1,x_2,x_3,x_4)=\frac{1}{8}(x_1^4+2x_1^2x_2+3x_2^2+2x_4).$$

将 $x_1=x_2=x_3=m=3$ 代入得

$$P(G;3,3,3,3)=\frac{1}{8}(3^4+2\cdot3^2\cdot3+3\cdot3^2+2\cdot3)=21,$$

即得项链种类数为 21. 又,若 $C=\{\mathrm{R},\mathrm{Y}\}$,则 $m=2$;则算出项链种类数为

$$P(G;2,2,2,2)=\frac{1}{8}(2^4+2\cdot2^2\cdot2+3\cdot2^2+2\cdot2)=6,$$

共 6 种,图式如下:

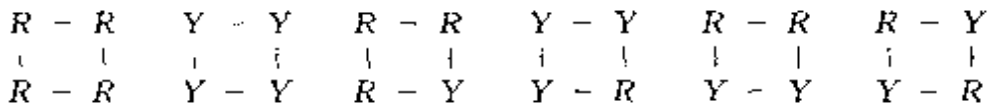


图 2-5

习题 2.4

1. 一木棒等分为四段，每段涂上红、黄、蓝三种颜色之一，有多少种涂法？

2 考虑所有八位 2- 进制数的集合 为某种需要，两个数若仅相差循环置换就被认为是等价的，如：01100111 与 11001110 被看做一样. 问有多少个等价类？

3. 将一个 8×8 的方形方格棋盘的每格涂上黑、白二色之一，有多少种方式？

4. 试求正 n 边形的对称群的循环指标多项式.

5 设群 G 作用在集合 X 上，群 H 作用在集合 Y 上.

(1) 证明群 $G\times H$ 以下述方式作用于不交并集合 $X\cup Y$：$\forall (g,h)\in G\times H$ 与 $z\in X\cup Y$

$$(g,h)^*(z)=\begin{cases} g^*(z), & \text{若 } z\in X;\\ h^*(z), & \text{若 } z\in Y.\end{cases}$$

(2) 证明群 $G^0\times H$ 以下述方式作用于映射集合 $\mathrm{Hom}(X,Y)$：$\forall (g,h)\in G\times H$ 与 $\varphi\in \mathrm{Hom}(X,Y)$，$(g,h)^*(\varphi)=h^*\varphi g^*$；即，$\forall x\in X$，$(g,h)^*(\varphi)(x)=h^*\varphi g^*(x)$.

6. 设有限群 G 作用在 n- 元集合 X 上，有限群 H 作用在 m- 元集合 Y 上. 令

$P(G;x_1,x_2,\cdots,x_n)$ 是群 G 在集合 X 上的循环指标多项式，

$P(H;x_1,x_2,\cdots,x_m)$ 是群 H 在集合 Y 上的循环指标多项式.

证明：群 $G\times H$ 在不交并集合 $X\cup Y$ 上的循环指标多项式是乘积

多项式

$$P(G;x_1,x_2,\cdots,x_n)\cdot P(H;x_1,x_2,\cdots,x_m).$$

§2.5 Pólya 计数 进一步的问题

我们继续讨论上一节的问题，所有的符号术语与上节相同. 还是从一个具体问题出发，看看面对具体的进一步的要求该如何处理.

2.5.1 问题 还考虑问题 2.4.1，但是有进一步的要求：红、黄、蓝三种颜色的珠子各至少要一个，怎么办？或者，指定蓝色珠子恰好用两个，又怎么办？

这一类问题的实质在于，在计算群 G^0 作用于集合 $\mathrm{Hom}(V,C)$ 的轨道时，要设法区分 C 中的元素. 有效办法之一是所谓“加权”：即赋予 C 中的元素以不同的重量. 由于 Burnside 轨道计数公式是我们思考这类问题的基础，所以我们首先考虑 Burnside 轨道计数公式的加权形式. 表达重量的恰当形式是所谓实数域 $\mathbb{R}$ 上的代数，简称 $\mathbb{R}$- 代数，我们就从它开始.

2.5.2 定义 设 $\mathbb{R}$ 是实数域. W 称为一个 $\mathbb{R}$- 代数（实数域上的代数）如果 W 既是一个 $\mathbb{R}$- 向量空间也是一个环（见定义 1.2.17），并且下列两条命题成立：

(1) 环的加法运算与向量加法运算一致；

(2) $a(w_1w_2)=(aw_1)w_2=w_1(aw_2)$ 对于所有 $w_1,w_2\in W$ 与 $a\in\mathbb{R}$ 成立.

如果 W 还是交换环，就称为交换 $\mathbb{R}$- 代数.

换言之，一个 $\mathbb{R}$- 代数 W 有三个运算：加法，乘法，系数乘法（即纯量乘法）. 加法与乘法构成环，加法与系数乘法构成向量空间，这两种结构彼此相容（即上述命题(2)）.

例 $\mathbb{R}$ 是一个 $\mathbb{R}$- 代数. 这个例子是下面两个例子的特例.

例 设 $M_n(\mathbb{R})$ 是所有 $n\times n$- 实矩阵的集合，则 $M_n(\mathbb{R})$ 是

一个 $\mathbb{R}$- 代数.

2.5.3 例 设 $X=\{x_1,x_2,\cdots,x_n\}$ 是 n 个不定元的集合,令

$$\mathbb{R}[X]=\{f(X)\mid f(X)\text{ 是 }X\text{ 上 }\mathbb{R}\text{- 系数多项式}\},$$

则在多项式加法、多项式乘法和实数乘多项式三种运算之下,$\mathbb{R}[X]$ 是一个 $\mathbb{R}$- 代数.

2.5.4 定义 设 V 是一个非空集合,W 是一个 $\mathbb{R}$- 代数. 如果有一个映射 $\omega:V\to W$,则称 V 是一个 W- 值的加权集合(W-valued weighted set),称 ω 是 V 的加权(weighting);进一步,若 $U\subseteq V$ 是 V 的非空有限子集,则称 $\omega(U)=\sum\limits_{u\in U}\omega(u)$ 为子集 U 的总权(total weight),而称 $\overline{\omega(U)}=\omega(U)/|U|$ 为非空有限子集 U 的平均权.

直观注解 V 的加权 ω 就是给 V 的每个元 v 赋予一个重量 $\omega(v)\in W$,称为 v 的权值;这样,适当选择加权 ω,就可以按需要把各个元素区别开. 通常的集合 V 可以看做是具有平凡加权 $\tau:V\to\mathbb{R},v\mapsto 1$ 的加权集合.

2.5.5 Burnside 轨道计数公式(加权形式)

设有限群 G 作用于有限加权集合 V,这里 V 的加权是 $\omega:V\to W$,W 是一个 $\mathbb{R}$- 代数. 设 $V_1,V_2,\cdots,V_t$ 是 V 的所有 G- 轨道. 则 G- 轨道的平均权之和为

$$\sum_{i=1}^{t}\overline{\omega(V_i)}=\frac{1}{|G|}\sum_{g\in G}\omega(\mathrm{Fix}(g)).$$

注 若 ω 是平凡加权,则 $\overline{\omega(V_i)}=1$ 而 $\omega(\mathrm{Fix}(g))=|\mathrm{Fix}(g)|$,就得到通常的 Burnside 轨道计数公式 2.2.12.

证明 以下证明就是把通常的 Burnside 公式(见引理 2.2.12)的证明稍加改造得来的.

考虑集合 $S=\{(g,x)\mid g\in G,x\in V,\tilde{g}(x)=x\}$;给它也赋予加权 $\omega(g,x)=\omega(x)$. 我们计算它的总权 $\omega(S)$ 有两种途径. 一方面,对于任意一个固定的 $g\in G$,按照 $\mathrm{Fix}(g)$ 的定义这种

偶对 (g,x) 中的 x 跑遍 $\mathrm{Fix}(g)$；即 S 是这些集合 $\{(g,x)\mid x\in \mathrm{Fix}(g)\}, g\in G$ 的不交并. 所以

$$\omega(S)=\sum_{g\in G}\omega(\mathrm{Fix}(g)). \tag{2.5.5.1}$$

另一方面，对于任意一个固定的 $x\in V$，按照 G_x 的定义这种偶对 (g,x) 中的 g 跑遍 $|G_x|$，即 S 是这些集合 $\{(g,x)\mid g\in G_x\}$，$x\in V$ 的不交并. 所以

$$\omega(S)=\sum_{x\in V}|G_x|\cdot\omega(x).$$

而 V 是它的轨道的不交并 $V=V_1\cup V_2\cup\cdots\cup V_t$. 对于 $x\in V_i$，由轨道长公式有 $|V_i|=|G|/|G_x|$，即 $|G_x|=|G|/|V_i|$. 因此

$$\begin{aligned}\omega(S)&=|G|\sum_{i=1}^{t}\sum_{x\in V_i}\omega(x)/|V_i|\\&=|G|\sum_{i=1}^{t}\Big(\sum_{x\in V_i}\omega(x)\Big)/|V_i|\\&=|G|\sum_{i=1}^{t}\overline{\omega(V_i)}.\end{aligned}$$

把此式与式(2.5.5.1)相比较，就得到所要求的公式. □

回到问题 2.5.1，我们来讨论加权形式的 Pólya 计数方法. 对应于 $C=\{R,Y,B\}$，令 $X=\{r,y,b\}$ 是不定元的集合，而 $W=\mathbb{R}[r,y,b]$ 是关于 r,y,b 的实系数多项式代数，见定义 2.5.2 及例 2.5.3. 再令 $\omega: C\to W$ 是 C 的加权，它使 $\omega(R)=r,\omega(Y)=y,\omega(B)=b$. 那么 ω 自然地诱导 $\mathrm{Hom}(V,C)$ 的一个(乘法)加权

$$\omega^*:\mathrm{Hom}(V,C)\to W,\varphi\mapsto\prod_{v\in V}\omega(\varphi(v)). \tag{2.5.6}$$

因 $\varphi(v)\in C$，显然 $\omega(\varphi(v))\in X=\{r,y,b\}$. 于是 $\omega^*(\varphi)$ 是 r,y,b 的单项式. 对于任意 $\varphi\in\mathrm{Hom}(V,C)$ 与 $g\in G$ 有 $w^*(g^*(\varphi))=\prod_{v\in V}w(\varphi g(v))$，而当 v 跑遍 V 时 $g(v)$ 也跑遍 V，

所以 $w^*(g^*(\varphi)) = w^*(\varphi)$;即是说,在 $\mathrm{Hom}(V,C)$ 的一个 G^0-轨道 Ω_i^* 中的所有元素(即映射)的权都相同;特别地,有以下结论:

2.5.7 引理 $\mathrm{Hom}(V,C)$ 的一个 G^0- 轨道 Ω_i^* 的平均权 $\overline{w^*(\Omega_i^*)}$ 等于该轨道中的任一元素 $\varphi \in \Omega^*$ 的权,即:$\overline{w^*(\Omega_i^*)} = w^*(\varphi), \forall \varphi \in \Omega^*$.

根据 $\mathrm{Hom}(V,C)$ 上的加权的定义(2.5.6),可以从这个加权来判断相应颜色配置中各个颜色出现的情况;例如,针对问题2.5.1,我们就有以下判别办法:

判别办法:在 G^0- 轨道 Ω_i^* 给出的颜色配置中(其中 $\varphi \in \Omega^*$):

(1) 红、黄、蓝三种颜色的珠子各至少出现一次当且仅当单项式 $w^*(\varphi) = ar^iy^jb^k$ 满足 $i>0, j>0, k>0$,即 r,y,b 的次数都大于0;

(2) 蓝色珠子恰好两个当且仅当单项式 $w^*(\varphi) = ar^iy^jb^2$,即 b 的幂次数恰好为2.

因此我们可以得出以下结论:

2.5.8 结论 只要计算出集合 $\mathrm{Hom}(V,C)$ 上的所有 G^0- 轨道的平均权之和(它是 r,y,b 的多项式),问题2.5.1就可以解决.

现在我们用更数学化的形式来叙述.

2.5.9 一般问题 (1) 设 $V = \{1,2,\cdots,n\}$,C 是有限集,记 $\mathrm{Hom}(V,C) = \{\varphi: V \to C\}$ 是所有 V 到 C 的映射的集合;设群 G 作用于集合 V,而 $P(G;x_1,x_2,\cdots,x_n)$ 如定义2.4.5所定义的是 G 在 V 上的循环指标多项式;由引理2.2.7,群 G^0 作用于集合 $\mathrm{Hom}(V,C)$;设 $\Omega_1^*,\Omega_2^*,\cdots,\Omega_t^*$ 是 $\mathrm{Hom}(V,C)$ 的全部 G^0- 轨道.这些与上节2.4.4是一样的;

(2) 再设 W 是实数域 $\mathbf{R}$ 上的一个代数,设 $\omega: G \to W$ 是 C 到 W 的一个加权.称下述 ω^* 是由 ω 诱导的 $\mathrm{Hom}(V,C)$ 的乘法加权:

(2.5.10) $\omega^*: \mathrm{Hom}(V,C) \to W, \varphi \mapsto \prod_{v\in V}\omega(\varphi(v))$;

(3) 目的:求集合 $\mathrm{Hom}(V,C)$ 上的所有 G^0- 轨道的平均权之和 $\sum_{i=1}^{t}\overline{\omega^*(\Omega_i^*)}$.

注意,显然引理 2.5.7 一般是成立的,这里我们把它重述如下.

$\mathrm{Hom}(V,C)$ 的一个 G^0- 轨道 Ω_i^* 中的所有元素(即映射)的权都相同.特别地,Ω_i^* 的平均权 $\overline{w^*(\Omega_i^*)}$ 等于该轨道中的任一元素 $\varphi \in \Omega^*$ 的权 $w^*(\varphi)$.

2.5.11 Pólya 计数定理 记号如上.令 $p_i = \sum_{c\in C} w(c)^i$, $i = 1,2,\cdots,n$. 则 $\mathrm{Hom}(V,C)$ 的所有 G^0- 轨道的平均权之和等于

$$P(G;p_1,p_2,\cdots,p_n) = \frac{1}{|G|}\sum_{g\in G} p_1^{\lambda_1(g)} p_2^{\lambda_2(g)}\cdots p_n^{\lambda_n(g)}$$

证明 根据加权的 Burnside 计数公式 2.5.5,所求平均权之和为

$$(2.5.11.1)\qquad \sum_{k=1}^{t}\overline{w^*(\Omega_k^*)} = \frac{1}{|G|}\sum_{g\in G}\sum_{\varphi\in \mathrm{Fix}(g^*)} w^*(\varphi)$$

其中 $\mathrm{Fix}(g^*)$ 为 g^* 在 $\mathrm{Hom}(V,C)$ 上的不动点的集合.由结论 2.4.7,有

$$\mathrm{Fix}(g^*) = \{V \text{ 的}\langle g\rangle\text{- 轨道集合到 } C \text{ 的函数}\}.$$

回想 g 的型为 $(\lambda_1(g),\lambda_2(g),\cdots,\lambda_n(g))$,即 V 的长为 i 的 $\langle g\rangle$- 轨道有 $\lambda_i(g)$ 个:$V_{i1},V_{i2},\cdots,V_{i\lambda_i(g)}$;设 $\varphi \in \mathrm{Fix}(g^*)$ 在 V_{ij} 上取值 c_{ij},其中 c_{ij} 可跑遍 C,按定义 2.5.10 有(这里规定 $\lambda_i(g)=0$ 时 $\prod_{j=1}^{\lambda_i(g)} w(c_{ij})^i = 1$):

$$(2.5.11.2)\qquad w^*(\varphi) = \prod_{i=1}^{n}\prod_{j=1}^{\lambda_i(g)} w(c_{ij})^i$$

它正好是下式

$$p_1^{\lambda_1(g)}p_2^{\lambda_2(g)}\cdots p_n^{\lambda_n(g)}=\prod_{i=1}^{n}\Big(\sum_{c\in C}w(c)^i\Big)^{\lambda_i(g)} \tag{2.5.11.3}$$

的展开式中的一项. 反之, 易见(2.5.11.3) 的展开式中的一项也正好是某个 $\varphi\in \mathrm{Fix}(g^*)$ 给出的 $w^*(\varphi)$ 的值(2.5.11.2). 因此式(2.5.11.1) 右边的

$$\sum_{\varphi\in \mathrm{Fix}(g^*)} w^*(\varphi)=p_1^{\lambda_1(g)}p_2^{\lambda_2(g)}\cdots p_n^{\lambda_n(g)}.$$

这就得到了定理所求证的等式. □

2.5.12 例　回到问题2.5.1, 按照结论2.5.8来做它. 为简单计, 设 $n=4, C=\{\mathrm{R},\mathrm{Y}\}$; 令 W 是代数 $\mathbb{R}[r,y]$, 加权 $\omega: C\to W$ 是 $\omega(\mathrm{R})=r, \omega(\mathrm{Y})=y$. 那么由式(2.4.9) 有

$$\begin{aligned}P(G;p_1,p_2,p_3,p_4)&=\frac{1}{8}\left((r+y)^4+2(r+y)^2(r^2+y^2)+3(r^2+y^2)^2+2(r^4+y^4)\right)\\&=r^4+r^3y+2r^2y^2+ry^3+y^4.\end{aligned}$$

即是说项链种类共 6 种, 分类如下:

4 红珠的 1 种;

3 红珠 1 黄珠的 1 种;

2 红珠 2 黄珠的 2 种;

1 红珠 3 黄珠的 1 种;

4 黄珠的 1 种

与例 2.4.8 的结果比较, 可见加权形式的 Pólya 计数方法能给出更多的信息.

习题 2.5

1. 用红、黄两种颜色的珠子穿成五珠项圈, 可穿制出几种项圈? 又, 若要求项圈为三个红珠两个黄珠, 则有几种?

2. 用两颗红珠、两颗黄珠、两颗蓝珠穿成一个手链, 共有多少种穿法?

3. 有 5 本书, 其中 3 本是同种书 A, 另 2 本是同种书 B, 现把它

们分给 3 个人,要求其中二人各得 2 本,另一人得 1 本,有多少种分法?

4. 令 $P(S_n;x_1,x_2,\cdots,x_n)$ 是 n 次对称群 S_n 的循环指标多项式. 证明:

$$P(S_n;1+x,1+x^2,\cdots,1+x^n)=1+x+x^2+\cdots+x^n.$$

5. 设有限群 G 作用在 n 元集合 X 上,即有同态 $\tau:G\to \mathrm{Sym}(X)$. 令 $H=\mathrm{Im}(\tau)$,那么 H 是 X 的置换群. 考虑 G 在 X 上的作用,有循环指标多项式 $P(G;x_1,x_2,\cdots,x_n)$;考虑 H 在 X 上的作用,又有循环指标多项式 $P(H;x_1,x_2,\cdots,x_n)$. 证明:

$$P(G;x_1,x_2,\cdots,x_n)=P(H;x_1,x_2,\cdots,x_n).$$

6. 设 G 是有限群. 以集合 G 为基作 $\mathbb{R}$- 向量空间,记作 $\mathbb{R}G$;那么 $\mathbb{R}G$ 的任意元是 G 的元的线性组合 $\sum_{g\in G}a_g g$. 在 $\mathbb{R}G$ 中定义乘法如下:

$$\Big(\sum_{g\in G}a_g g\Big)\Big(\sum_{g\in G}a'_g g\Big)=\sum_{g\in G}\Big(\sum_{uv=g}a_u a'_v\Big)g;$$

即把 G 的乘法运算线性扩张(或者说按分配律扩张)成为整个 $\mathbb{R}G$ 上的乘法运算. 证明:$\mathbb{R}G$ 是一个 $\mathbb{R}$- 代数.

7. 实数区间 $[0,1]$ 上的所有实连续函数的集合 $\mathbb{R}[0,1]$ 是一个 $\mathbb{R}$ - 代数.

思考题:Pólya 计数定理的推广

考虑这样的问题:

有 5 本书,其中 3 本是同种书 A,另 2 本是同种书 B;现把它们分装进 3 个箱子,其中 2 个箱子是一样的而另一个不同,有多少种装法?

令 V 是书的集合,而 C 是箱子的集合;则要考虑映射集合 $\mathrm{Hom}(V,C)$;由条件,群 $S_3\times S_2$ 作用于书的集合 V,参看习题 2.4.5(1);群 S_2 作用于箱子的集合 C;从而群直积 $(S_3\times S_2)^e\times S_2$ 作用于集合 $\mathrm{Hom}(V,C)$,见习题 2.2.4(2);所述问题的解答就是这

个作用下集合 $\mathrm{Hom}(V,C)$ 所分的轨道的个数. 因此,Pólya 计数问题的推广形式之一如下:

设有限群 G 作用于有限集 V,有限群 H 作用于有限集 C;则有限群 $G^0\times H$ 作用于映射集合 $\mathrm{Hom}(V,C)$;如何计算 $G^0\times H$ 在集合 $\mathrm{Hom}(V,C)$ 上的轨道个数?

按 Burnside 引理,所求个数等于

$$\frac{1}{|G||H|}\sum_{(g,h)\in G\times H}|\mathrm{Fix}((g,h)^*)|.$$

因此,关键是要计算 $|\mathrm{Fix}((g,h)^*)|$. 然而它比原来的形式要复杂一些. 加权的形式就更复杂了. 不妨一试.

另一种推广思路. 在问题 2.4.1 的基础上进一步考虑问题:

设计三种颜色珠子的项链,要求红、黄、蓝三色珠子搭配匀称;即,将任二种颜色互换,项链的样式仍然不变.

设 V,C,G 如同 §2.4. 这个进一步的要求用数学方式来表达就是:设有群 S_3 作用在集合 $C=\{\mathrm{R},\mathrm{Y},\mathrm{B}\}$ 上,容易证明对 G^0 在 $\mathrm{Hom}(V,C)$ 上的任一轨道 Ω^* 与任意 $\alpha\in S_3$,若有 $\varphi\in\mathrm{Hom}(V,C)$ 使 $\alpha\varphi\in\mathrm{Hom}(V,C)$,则对任意 $\varphi'\in\mathrm{Hom}(V,C)$ 都有 $\alpha\varphi'\in\mathrm{Hom}(V,C)$;换言之,$\alpha$ 使轨道 Ω^* 不变. 我们的数学问题就是:

求在 $\mathrm{Hom}(V,C)$ 上使得在 S_3 的所有置换之下都不变的 G^0-轨道的个数.

可阅参考文献[6].

第 3 章　图

§3.1　图 与 树

图(graph)实际上是一个非常直观的概念,比如街道图,流程图等,表达了一个有限集合的元素之间的某些关联配置.从数学的角度,我们需要一个数学化的定义,但是显然下面的形式定义有非常直观的图示

3.1.1 定义　一个图 $X=(V,E,\alpha)$ 是由两个集合 V 和 E 以及一个映射 $\alpha:E\to V^{(2)}\cup V^{(1)}$ 构成,这里 $V^{(2)}$ 与 $V^{(1)}$ 分别是 V 的所有 2- 子集的集合与所有 1- 子集的集合;V 称为图 X 的顶点集(vertex set),其元素称为顶点(vertex)或简称点;E 称为图 X 的边集(edge set).其元素称为边(edge).基数 $|V|$ 称为图 X 的阶.$|V|$ 和 $|E|$ 都有限的图称为有限图.

如果 $e\in E$ 的像 $\alpha(e)=\{v_0\}\in V^{(1)}$,则称 e 为环(loop);如下图的 e_0.如果 V 的 2- 子集 $\{v_1,v_2\}\in V^{(2)}$ 在 E 中的原像 $\{e\in E|\alpha(e)=\{v_1,v_2\}\}$ 含成员个数多于一个,则称 $\{e\in E|\alpha(e)=\{v_1,v_2\}\}$ 为重边(multiedge);如图 3-1 中的 e_1 和 e_2.

既无环也无重边的图称为简单图(sample graph),带重边的图称为重图(multigraph).

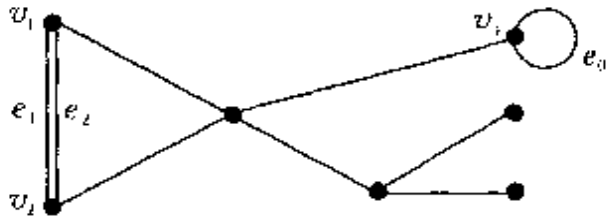


图 3-1

3.1.2 注解　(1) 在上述图的定义中，若将 $V^{(2)}$ 换为 $V^2 = V \times V$，即 V 的 2 元有序对的集合，则所定义的结构称为有向图 (oriented graph)；这时直观图示中的每条边是有方向的. 另一方面，若把图的每个顶点都标上号予以区别，则称为标号图 (labeled graph).

(2) 通常不带定语的"图"是指无向简单图；我们以下也将采用这种约定 对无向简单图，映射 $\alpha: E \to V^{(2)}$ 是单射，我们干脆把 E 等同于它的像

$$\{\{u,v\} \in V^{(2)} \mid \text{存在 } e \in E, \text{ 使得 } \alpha(e) = \{u,v\}\},$$

就把边 $e \mapsto \{u,v\}$ 简单说成"边 $\{u,v\}$"，或更简单地说成边 (uv)，但要注意这样说时，$(uv) = (vu)$ 是不讲顺序的. 换句话说，对无向简单图就认为 E 是所有这些边 (uv) (即 $\{u,v\}$) 的集合；对顶点 $u,v \in V$，若 $\{u,v\} \in E$ (即 $(uv) \in E$) 则说 u 和 v 之间有条边；因此，我们可以简记无向简单图为 $X = (V,E)$. 另一方面，有向简单图的边则形象地简记为 $(u \to v)$.

(3) 我们约定，下文中的图若无特定定语均指有限无向简单图.

3.1.3 定义　图 $X = (V,E)$ 中连接顶点 v_1, v_2 的一条道 (walk) 是指点的序列 $W = (u_1, u_2, \cdots, u_n)$ 使得 $u_1 = v_1$ 而 $u_n = v_2$，而且 $(u_i u_{i+1}) \in E$ 对于任意 $i = 1,2,\cdots,n-1$. 如果 $u_1 = u_n$，则称此道为闭道 (closed walk). 使得 $u_1, u_2, \cdots, u_{n-1}$ 无重复的道

$W=(u_1,u_2,\cdots,u_n)$ 称为路(path). 闭路称为圈(cycle).

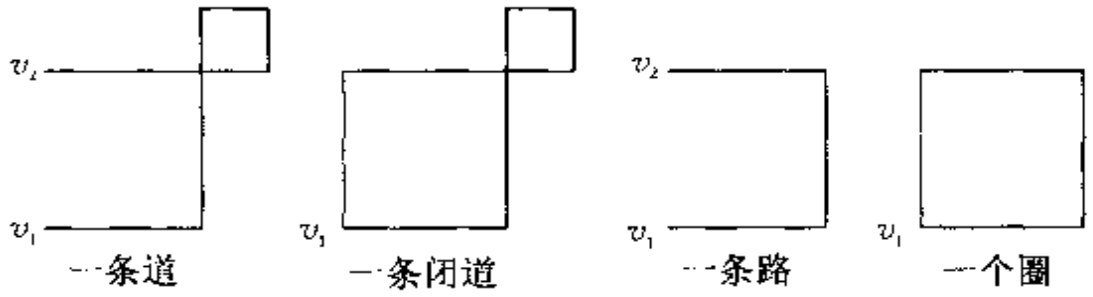


图 3-2

3.1.4 命题 图 $X=(V,E)$ 中

(1) 顶点 v_1,v_2 之间若有道则必有路.

(2) 顶点 v 到 v 若有闭道则必有含 v 的圈.

证明 去掉重复点的中间部分. □

3.1.5 定义 在图 $X=(V,E)$ 中如果顶点 u 与 v 之间有一条边即 $(uv)\in E$,则称点 u 与 v 相邻(adjacent).

顶点 v 的邻域(neighbor) 记作 $N(v)$, 定义为 $N(v)=\{u\in V|(vu)\in E\}$.

顶点 v 的次数(degree)或称度数,记作 $d(v)$,定义为 $d(v)=|N(v)|$.

顶点 v 称为孤立点(isolated vertex) 如果 $d(v)=0$;顶点 v 称为端点(endpoint) 如果 $d(v)=1$.

3.1.6 命题 在图 $X=(V,E)$ 中,$\sum_{v\in V}d(v)=2\cdot|E|$.

证明 在计算 V 的所有顶点的次数之和时每条边 $e\in E$ 恰好用了两次. □

3.1.7 定义 设 $X=(V,E)$ 是一个图. 图 $X'=(V',E')$ 称为图 $X=(V,E)$ 的子图(subgraph),如果 $V'\subset V$ 而且 $E'\subset E$.

对 $S\subset V$,以 S 为顶点集的 X 的最大子图称为 S 的导出子图

(induced subgraph),记作$\langle S\rangle$.

如果 X 的子图 $X'=(V',E')$ 使得 $V'=V$,则称 X' 是图 X 的生成子图(spanning subgraph).

3.1.8 定义 设 $X=(V,E)$ 是一个图.

(1) $v_1,v_2\in V$ 在 X 中称为连通的(connected)如果 $v_1=v_2$ 或者 v_1 到 v_2 之间有一条道.

(2) 连通关系是 V 的等价关系(见本节习题1),任一个等价类的导出子图称为图 X 的连通分支(connected component).

(3) 如果 X 只有一个连通分支,则称 X 为连通图(connected graph).

(4) 如果 X 的任意两点之间都有一条边,则称 X 为完全图(complete graph);n 阶完全图常记作 K_n.

完全图显然是同阶图中边数最多的图,而且下述结论是显然的.

3.1.9 引理 设 $X=(V,E)$ 是图.则 $|E|\leqslant|V|(|V|-1)/2$;而且,等号成立当且仅当 X 是完全图.

证明 简单的计数公式. □

我们再来看同阶图中边数最少的连通图.

3.1.10 引理 设 $X=(V,E)$ 是一个连通图.则 $|E|\geqslant|V|-1$.

证明 对 $|E|$ 进行归纳.当 $|E|=0$ 时,X 只能是一个点的图或者是空图,命题显然成立.

再设 $|E|=n>1$.任取 $(uv)\in E$.令 $X'=(V,E')$ 是从图 X 中去掉一条边 (uv) 后所得到的图,即 $E'=E-\{(uv)\}$.对于任意 $w\in V$,我们证明在图 X' 中 w 或者与 u 连通或者与 v 连通.若 $w=u$ 则 w 与 u 连通.再设 $w\neq u$.在图 X 中从 w 到 u 有一条开路 $w=v_1,v_2,\cdots,v_l=u$.若任意 $v_i\neq v$,则边 (uv) 不在这条路中出现,所以 w 与 u 在图 X' 中也连通.否则,存在 $0<j<l$ 使得

$v_j = v$；而且，因为路中无重复点，u 不在路 $w = v_1, v_2, \cdots, v_j = v$ 中出现，故 w 与 v 在图 X' 中连通.

如果 X' 是连通的，因 $|E'| = n - 1 < |E|$，由归纳法，得 $|E| > |E'| \geqslant |V| - 1$. 如果 X' 不是连通的，由上段论证，图 X' 中 u 所在的连通分支 $X'_u = (V'_u, E'_u)$，与 v 所在的连通分支 $X'_v = (V'_v, E'_v)$，满足 $V'_u \cup V'_v = V$（即包含了 X 的所有顶点）和 $E'_u \cup E'_v = E'$，那么可对连通图 X'_u 和 X'_v 分别使用归纳法，得

$$|E'_u| \geqslant |V'_u| - 1 \text{ 和 } |E'_v| \geqslant |V'_v| - 1;$$

所以

$$\begin{aligned} |E| &= |E'_u| + |E'_v| + 1 \geqslant (|V'_u| - 1) + (|V'_v| - 1) + 1 \\ &= |V| - 1. \end{aligned}$$

□

使得上述命题中的等号成立的图显然存在，如图 3-3 所示：

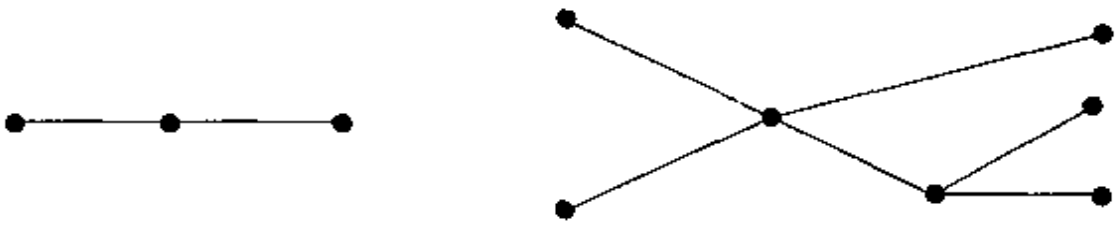


图 3-3

它们实际上是一类重要的特殊的图.

3.1.11 定义 没有圈的图称为林(forest)，连通的林称为树(tree)

注解 有的文献称“林”为“树”，而称上述定义的树为“连通树”

3.1.12 定理 设 $X = (V, E)$ 为图. 则以下三条件彼此等价：

(1) X 是一棵树；

(2) X 的任意两不同点间恰好有一条路相连；

(3) X 连通而且 $|E| = |V| - 1$.

证明　(1)$\Longrightarrow$(2). 如果两点 $u \neq v \in V$ 之间有两条不同的路相连,则这两条路形成闭道;由命题 3.1.4, X 有圈.

(2) $\Longrightarrow$(3). 由(2)已知 X 连通,而且任意去掉一条边 (uv) 后得到的图 X' 不再连通(否则此二点在图 X 中有两条路相连);根据本节习题 4, X' 恰有两个连通分支 $X_1' = (V_1', E_1')$ 和 $X_2' = (V_2', E_2')$ 使得 $V = V_1' \cup V_2'$(不交并)且 $E = E_1' \cup E_2' \cup \{(uv)\}$(不交并);而且图 X_1' 和 X_2' 显然都满足(2);可对图的阶 $|V|$ 采用归纳法;于是 $|E_i| = |V_i| - 1, i = 1,2$;那么

$$\begin{aligned} |E| &= |E_1| + |E_2| + 1 \\ &= (|V_1| - 1) + (|V_2| - 1) + 1 \\ &= |V| - 1. \end{aligned}$$

(3) $\Longrightarrow$(1). 由于 X 连通. 若 X 有圈,则根据本节习题 5,可从 X 中去掉一条边使得所得图 $X' = (V, E')$ 仍然连通,但由(3),得到 $|E'| = |V| - 2$,按照引理 3.1.10,这是不可能的. 所以 X 没有圈,即 X 是一座林. 而 X 是连通的,故得到(1). □

此定理有一些明显的但有用的推论,这里只叙述一个,另两个放在本节习题 6 和习题 7,请读者自行证明.

3.1.13 推论　一棵阶大于 1 的树至少有两个端点.

证明　设 $T = (V, E)$ 是一棵树. 由命题 3.1.6 和定理 3.1.12 知道 $\sum_{v \in V} d(v) = 2|E| = 2|V| - 2$,而每个 $d(v) \geqslant 1$(因 T 没有孤立点),所以至少有两个点 v_1, v_2 使得 $d(v_i) = 1, i = 1,2$. □

3.1.14 定义　m 阶图(m 阶连通图)的任一 m 阶子林(m 阶子树)称为该图的生成林(spanning forest)(生成树(spanning tree)).

例　四边形的图有四棵生成树:

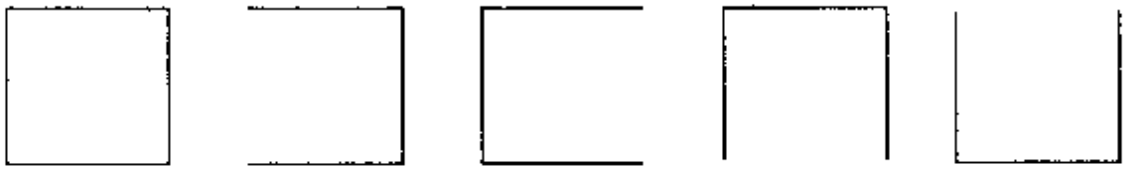


图 3-4

3.1.15 命题 连通图的任意一棵子树可以扩充为一棵生成树.

证明 设 $X=(V,E)$ 为连通图,设 $T_0=(V_0,E_0)$ 是 X 的一棵子树.扩充步骤如下.

(1) 若 $V_0=V$,则已完成. 否则:

(2) 可断言 $N(T_0)=\{u\in V\mid u\notin V_0$,但有 $v_0\in V_0$ 使得 $(v_0u)\in E\}\neq\varnothing$.

这是因为有 $u\in V-V_0$,任取 $v_0\in V_0$,由连通性,有路 $W=(v_0=u_0,u_1,\cdots,u_n=u)$ 连接 v_0 与 u,则存在 $0<i\leqslant n$ 使得 $u_i\notin V_0$ 但 $u_{i-1}\in V_0$;于是 $u_i\in N(T_0)$.

(3) 取 $v_1\in N(T_0)$,则还可取 $v_0\in V_0$ 使得 $(v_0v_1)\in E$;令 $T_1=(V_1,E_1)$,其中 $V_1=V_0\cup\{v_1\}$ 而 $E_1=E_0\cup\{(v_0v_1)\}$.

用 T_1 代替 T_0,回到(1);因 X 是有限图,重复此过程,经有限步以后,必达到生成树. □

注解 上述证明中的步骤(1)~(3)实际上给出了搜索生成树的一种具体算法:可以从任意一棵 2 阶子树即一条边开始,如果图的阶是 n,则经过 $n-2$ 次循环可得到生成树.即使对非连通图,此办法亦可搜索出生成林.特别地,下述推论是显然的.更重要的是此方法可稍加发展成为搜索所谓"极小生成树(林)"的算法,见 §3.5.

3.1.16 推论　图(连通图)的生成林(生成树)存在.

3.1.17 推论　连通图只有一棵生成树当且仅当它是一棵树.

证明见本节习题 8. □

在 §3.3 中我们将进一步讨论生成树的棵数.

习题 3.1

1. 证明:在一个图中顶点集的连通关系是等价关系.

2. 一个图中奇次数的顶点的个数必为偶数.

3. 如果图 X 中有一条道包含图的每条边恰好一次,则 X 称为 Euler 图,这种道称为 Euler 道. 证明:连通图 X 是 Euler 图当且仅当它的奇次数的顶点个数不大于 2

4. 设图 $X=(V,E)$ 有 r 个连通分支,$(uv)\in E$. 证明:图 $X'=(V,E')$,其中 $E'=E-\{(uv)\}$ 的连通分支个数或者是 r 或者是 $r+1$.

5. 设 $X=(V,E)$ 是连通图. 则图 X 有圈当且仅当可以从图 X 中去掉一条边使得所得图仍然连通.

6. 设 $X=(V,E)$ 为图,且 $|V|>2$. 证明:X 是树当且仅当 X 是一座林而且任意添加一条边后就形成一个圈.

7. 设 $X=(V,E)$ 为图,且 $|E|=|V|-1$ 则 X 是树当且仅当 X 连通.

8. 证明推论 3.1.17.

9. 连通分支个数为 t 的图为林当且仅当 $|E|=|V|-t$.

§3.2　对换的图

这一节从图的角度考虑若干有关置换的问题.

3.2.1 定义 设 $V=\{1,2,\cdots,n\}$；$E=\{\tau_1,\tau_2,\cdots,\tau_m\}\subset S_n$，每个 τ_i 是对换.则可构作标号图 $X=(V,E)$，即以 V 为顶点集，E 为边集的图(如果 $\tau=(ij)\in E$ 则(ij)为一条边)；该图称为对换集合 E 的图.

例 $V=\{1,2,3,4\}$，$E=\{(12),(13),(24)\}$；则图 $X=(V,E)$ 如下面的图 3-5 中左边所示.

注意：为说明标号图与无标号图的差别，见注解 3.1.2，再举一例：$X'=(V,E')$，其中 V 同上，但 $E'=\{(12),(23),(34)\}$.若把它们作为无标号图，则此图为图 3-5(b) 所示，与图 3-5(a) 完全相同，这只要作顶点之间的双射即可看出：$1\mapsto 3,2\mapsto 1,3\mapsto 2,4\mapsto 4$ 但它们作为标号图则是不一样的.由此可见使用标号图完全可以区别不同的对换集合.

图 3-5

使用这种图的语言我们讨论三个问题.

3.2.2 问题 (1) 什么样的对换集合可以生成对称群 S_n？

(2) 我们已经看到一个循环可写成对换之积.现在的问题是：什么样的对换集合 $E=\{\tau_1,\tau_2,\cdots,\tau_m\}$ 可使得 $\alpha=\tau_1\tau_2\cdots\tau_m$ 是一个循环？

(3) 进一步，一个 m- 循环可写成 $m-1$ 个对换之积，问题：一

个 m- 循环写成 $m-1$ 个对换之积的方式有多少种?

先研究第一个问题.

3.2.3 引理.　设 $V=\{1,2,\cdots,n\}$, E 为集合 V 的一些对换的集合.则下述三条件等价:

(1) $\langle E\rangle = S_n$,即 E 生成对称群 S_n;

(2) E 生成的子群在 V 上可迁;

(3) 图 $X=(V,E)$ 连通.

证明　(1) $\Longrightarrow$ (2).显然.

(2) $\Longrightarrow$ (3). 反证之. 若图 $X=(V,E)$ 不连通,则 X 可分为子图 $X_1=(V_1,E_1)$ 和 $X_2=(V_2,E_2)$ 使得 $V=V_1\cup V_2$(不交并) 和 $E=E_1\cup E_2$(不交并),而它们二者不连通.特别是,E_1 的任何对换不会把 V_1 的点变到 V_2 的点,也不会把 V_2 的点变到 V_1 的点;E_2 的任何对换也是这样.对于任意 $\alpha=\tau_1\tau_2\cdots\tau_k\in\langle E\rangle$,每个 $\tau_i\in E$,则 α 也不会把 V_1 的点变到 V_2 的点,等等.总之,$\langle E\rangle$ 在 V 上不可迁;这与(2) 矛盾.

(3) $\Longrightarrow$ (1). 要证明(1),由定理 2.1.8,只要证明任意对换 $(ij)\in\langle E\rangle$.但由(3),图 $X=(V,E)$ 是连通的,即有路

$$i=i_1,i_2,\cdots,i_k=j$$

使得每对换 $(i_ti_{t+1})\in E$.那么

$$(ij)=(i_1i_2)(i_2i_3)\cdots(i_{k-1}i_k)(i_{k-2}i_{k-1})\cdots(i_2i_3)(i_1i_2)\in\langle E\rangle.$$

□

由此立即可得如下定理.

3.2.4 定理　(Pólya定理) 至少要 $n-1$ 个对换才能生成 n 次对称群 S_n.而 $n-1$ 个对换生成对称群 S_n 当且仅当它们的图是一棵树(这里说的树是连通树).

证明　由引理3.2.3, m 个 n 次对换生成 S_n 当且仅当它们的

图连通;那么由引理3.1.10,$m \geqslant n-1$.此即第一个结论.再由习题3.1.7,$n-1$个对换的图连通当且仅当它是一棵树.这就是第二个结论 □

再研究第二个问题.下面的引理在很多场合有用.

3.2.5 引理 设 $\alpha \in S_n$,(ij) 为 n 次对换.

(1) 如果 i 和 j 分别属于 α 的循环分解中的不同循环,即 α 的循环分解可写为 $\alpha=(i\cdots h)(j\cdots k)(l\cdots)\cdots$,则 $\alpha\cdot(ij)$ 的循环分解为:$(i,\alpha(j),\cdots,k,j,\alpha(i),\cdots,h)(l\cdots)\cdots$;就是 α 的分含 i 和 j 的两个循环合成了一个循环而其他循环不变.

(2) 如果 i 和 j 属于 α 的同一个循环,即 α 的循环分解可写为 $\alpha=(ih\cdots jk\cdots)(l\cdots)\cdots$.则 $\alpha\cdot(ij)$ 的循环分解为:$(ik\cdots)(jh\cdots)(l\cdots)\cdots$;$\alpha$ 含 i 和 j 的那个循环分成了两个循环而其他循环不变.

证明 直接验算即可得结论,两种情况可分别直观图示如下:

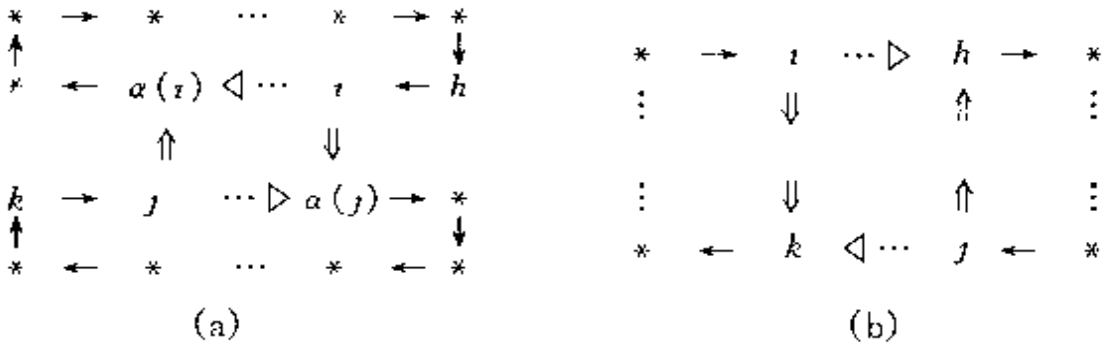


图 3-6 □

3.2.6 命题 设 $V=\{1,2,\cdots,n\}$ 而 $E=\{\tau_1,\tau_2\cdots,\tau_m\}\subset S_n$ 是一些对换的集合.如果图 $X=(V,E)$ 是一座林,则 $\alpha=\tau_1\tau_2\cdots\tau_m$ 的循环分解的各循环圈恰对应于图 X 的各连通分支,使

得 X 的每棵阶为 $k+1$ 的分支树 $\{\tau_{i_1}, \tau_{i_2}, \cdots, \tau_{i_k}\}$ 恰好给出 α 的一个长 $k+1$ 的循环圈(孤立点给出 1- 循环).

证明　对 m 进行归纳. 当 $m=1$ 时结论显然是对的.

再设 $m>1, \alpha=\tau_1\tau_2\cdots\tau_{m-1}\tau_m$. 令 $\alpha'=\tau_1\tau_2\cdots\tau_{m-1}$. 按归纳法, α' 的循环分解恰对应于图 $X'=(V, E-\{\tau_m\})$ 的连通分支. 设 $\tau_m=(ij)$; 分两种情况对 $\alpha=\alpha'\tau_m=\alpha'\cdot(ij)$ 进行讨论.

情形 1: i 和 j 分别属于 α' 的两个不同的循环圈 $(i\cdots h)$ 和 $(j\cdots k)$. 由归纳法, 这两个循环圈对应于图 X' 的两个不同的连通分支树 T_i 和 T_j. 那么, 一方面, 图 X 恰好就是在图 X' 的这两个连通分支 T_i 和 T_j 之间加上一条边 (ij) 而连成了一个连通树以后得到的图, 此时 X' 的其他连通分支均未改变. 另一方面, 由引理 3.2.5, $\alpha=\alpha'\cdot(ij)$ 的循环分解也恰好就是在 α' 的循环分解这两个循环圈 $(i\cdots h)$ 和 $(j\cdots k)$ 被对换 (ij) 连成了一个循环圈以后得到的循环乘积, 此时 α' 的其他循环圈均未改变. 所以结论对 m 成立. 如图 3-7 所示:

$$(i\cdots h)(j\cdots k)\cdot(ij)=(i\cdots kj\cdots h)$$

图 3-7

情形 2: i 和 j 属于 α' 的同一个循环圈 $(i\cdots j\cdots)$. 然而, 按归纳法, α' 的循环分解的循环圈对应于图 X' 的连通分支树, 即是说, 点 i 和点 j 属于图 X' 的同一个连通分支树 T'; 而图 X 是在图 X' 上加一条边 (ij) 后得到, 此时原图 X' 的连通分支树 T' 被加上了一条边 (ij), 得到的就不再是连通树(见习题 3.1.6); 这与假设 X 是一座林相矛盾. 所以这种情况是不可能发生的. 如图 3-8 所示:

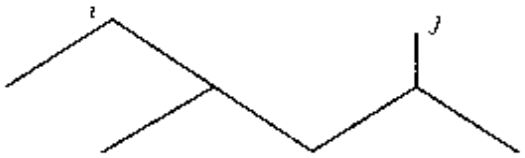


图 3-8 □

3.2.7 定理 设 $V=\{1,2,\cdots,n\}$ 为点集，$E=\{\tau_1,\tau_2,\cdots,\tau_{n-1}\}\subset S_n$ 为一些对换的集合，则 $\alpha=\tau_1\tau_2\cdots\tau_{n-1}$ 为一个 n- 循环置换当且仅当图 $X=(V,E)$ 是一棵 n 阶树.

证明 充分性：可由命题 3.2.6 立即推出.

必要性：设 α 为 n 循环，则 $\langle\alpha\rangle$ 在 V 上可迁(见习题2.2.4). 但是 $\langle E\rangle\supset\langle\alpha\rangle$，所以 $\langle E\rangle$ 在 V 上也可迁；那么由引理 3.2.3，图 X 是连通的；再由定理 3.1.12，图 X 是 n 阶连通树. □

下面研究第三个问题. 我们把它与另一个计数问题联系起来.

回想，任二点都相邻的图称为完全图，n 阶完全图 K_n 的边共有 $n(n-1)/2$ 条；见定义 3.1.8 和引理 3.1.9.

3.2.8 定理 一个 n 循环置换表写成 $n-1$ 个对换之积的方式个数 $d(n)$ 与 n 循环的选取无关，只是 n 的函数；它等于 n 阶完全图 K_n 的生成树的棵数 $T(n)$.

证明 设 α 与 β 都是 n 循环置换；那么 α 与 β 的型相同，因此有置换 γ 使得 $\beta=\gamma\alpha\gamma^{-1}$，见命题 2.1.5. 如果 α 有对换分解 $\alpha=\tau_1\tau_2\cdots\tau_{n-1}$，则

$$\begin{aligned}\beta=\gamma\alpha\gamma^{-1}&=\gamma\cdot\tau_1\cdots\tau_{n-1}\cdot\gamma^{-1}\\&=(\gamma\tau_1\gamma^{-1})\cdot\gamma\cdots\gamma^{-1}\cdot(\gamma\tau_{n-1}\gamma^{-1})\end{aligned}$$

就是 β 的一个对换分解，因为每个 $\gamma\tau_i\gamma^{-1}$ 都是对换. 容易看出，完全类似地，β 的一个对换分解通过 $\alpha=\gamma^{-1}\beta\gamma$ 就得到 α 的一个对换

分解. 所以,按照这种方式,α 的表写成 $n-1$ 个对换之积的方式与 β 的表写成 $n-1$ 个对换之积的方式之间一一对应. 因此 n 循环置换表写成 $n-1$ 个对换之积的方式个数 $d(n)$ 与 n 循环的选取无关.

现在考虑对换序列的集合 $\tau=\{(\tau_1,\tau_2,\cdots,\tau_{n-1})\mid(V,\{\tau_1,\tau_2,\cdots,\tau_{n-1}\})$ 为树$\}$. 我们可以用两种方法来计数 $|\tau|$.

一方面,对 S_n 的任意一个 n 循环,注意到表写成 $n-1$ 个对换之积的顺序问题,它的任意一个长 $n-1$ 的对换分解对应于 τ 的一个序列. 反之,由定理 3.2.7 可知,τ 的一个序列也对应于一个 n 循环的一个长 $n-1$ 的对换分解. 但是,S_n 中的所有 n 循环,由 Cauchy 公式 2.1.6,共有 $n!/n=(n-1)!$ 个. 所以,所有的 n 循环表写成 $n-1$ 个对换之积的所有方式之个数总和为 $|\tau|=(n-1)!\cdot d(n)$.

另一方面,τ 的一个序列对应于 n 阶完全图 K_n 的一棵生成树的 $n-1$ 条边的一个排列. 反之,K_n 的一棵生成树的 $n-1$ 条边的一个排列给出 τ 中的一个序列. 而 K_n 的一棵生成树的 $n-1$ 条边的排列方式有 $(n-1)!$ 种;所以,K_n 的所有生成树的边集的所有排列方式的总和数为 $|\tau|=(n-1)!\cdot T(n)$.

把上述两段论证结果结合起来就得到:

$$(n-1)!\cdot d(n)=(n-1)!\cdot T(n);$$

即 $d(n)=T(n)$. □

下一节我们将计算出:$T(n)=n^{n-2}$;见推论 3.3.10. 所以这里作为推论可对第三个问题回答如下.

3.2.9 推论　一个 n 循环置换表写成 $n-1$ 个对换之积的方式共有 n^{n-2} 种. □

习题 3.2

1. 利用引理 3.2.5 证明定理 2.1.8 中的惟一性部分.

2. 设 $V=\{1,2,\cdots,n\}$；$E=\{\tau_1,\tau_2,\cdots,\tau_m\}\subset S_n$，每个 τ_i 是对换；设 $\alpha=\tau_1\tau_2\cdots\tau_m$.

(1) 如果 α 是一个循环置换，证明循环长度不大于 $m+1$.

(2) 举例说明上述 α 可以是一个长度小于 $m+1$ 的循环置换.

(3) 如果上述 α 是一个长度 $m+1$ 的循环置换，证明：图 $X=(V,E)$ 是一座这样的林，它的一棵分支树为 $m+1$ 阶，其他分支全为孤立点.

3. 设 $\tau_1,\tau_2,\cdots,\tau_m$ 都是 S_n 中的对换. 如果其积 $\tau_1\tau_2\cdots\tau_m$ 是一个长度小于 $m+1$ 的循环置换，则要么对换 $\tau_1\tau_2,\cdots,\tau_m$ 之中有彼此相同的，要么由这些对换构成的图不是林.

4 证明：n 阶标号树的棵数等于 n 阶完全图 K_n 的生成树的棵数.

§3.3 矩阵—树定理

我们将把生成树的问题与一个矩阵问题联系起来，这就是本节标题的来历. 对于任意一个图都可以构造两个矩阵.

3.3.1 定义 设图 $X=(V,E)$，其中 $V=\{v_1,v_2,\cdots,v_n\}$ 而 $E=\{e_1,e_2,\cdots,e_m\}$. 由它定义 $n\times n$ 矩阵

$$A(X)=(a_{ij})_{n\times n},\text{其中 } a_{ij}=\begin{cases}1, & \text{若}(v_iv_j)\in E;\\ 0, & \text{否则.}\end{cases}$$

称为图 X 的邻接矩阵(adjacency matrix). 再定义 $n\times m$ 矩阵

$$B(X)=(b_{ij})_{n\times m},\text{其中 } b_{ij}=\begin{cases}1, & \text{若 } v_i\in e_j;\\ 0, & \text{否则.}\end{cases}$$

称为图 X 的关联矩阵(incidence matrix)，因为若 $v_i\in e_j$，则说点 v_i 与边 e_j 关联. 图的每条边恰与两个点关联，所以矩阵 $B(X)$ 的每

列恰含两个1,其余都是0.将 $B(X)$ 的每列中的一个1改为 -1,另一个 1 不动,得到的矩阵记作

$$E(X) = (e_{ij})_{n\times m}, \quad e_{ij} = \pm b_{ij};$$

称 $E(X)$ 为图 X 的交错关联矩阵(alternative incidence matrix).最后令

$$M(X) = E(X) \cdot E(X)^{\mathrm{T}};$$

其中 $E(X)^{\mathrm{T}}$ 为矩阵 $E(X)$ 的转置矩阵(transposed matrix).

列出明显的性质如下.

3.3.2 引理　(1) $A(X)$ 的对角线元素均为零;它的第 i 行元素之和与第 i 列元素之和都是图的顶点 v_i 的次数 $d(v_i)$.

(2) $B(X)$ 的每列恰好两个 1;它的第 i 行元素之和为 $d(v_i)$.

(3) $E(X)$ 的每列恰好 1 与 -1 各一个,其余为 0.　□

3.3.3 引理　$M(X) = -A(X) + \begin{pmatrix} d(v_1) & & & \\ & d(v_2) & & \\ & & \ddots & \\ & & & d(v_n) \end{pmatrix}$.

证明　令 $M(X) = (m_{ij})_{n\times n}$,按定义有 $m_{ij} = \sum_{k=1}^{m} e_{ik}e_{jk}$. 当 $i = j$ 时,有

$$e_{ik}e_{ik} = b_{ik}^2 = \begin{cases} 1, & \text{若 } v_i \in e_k; \\ 0, & \text{否则.} \end{cases}$$

所以 $m_{ii} = |N(v_i)| = d(v_i)$. 再设 $i \neq j$,那么 $e_{ik} \neq 0 \neq e_{jk} \Longleftrightarrow v_i \in e_k$ 且 $v_j \in e_k \Longleftrightarrow (v_iv_j) = e_k \in E \Longleftrightarrow a_{ij} \neq 0$,而在此时 e_{ik} 与 e_{jk} 恰好是 $E(X)$ 的第 k 列的仅有的两个非零元,故正好一个是 1 另一个是 -1.所以当 $i \neq j$ 时,有

$$e_{ik}e_{jk} = -1 = -a_{ij}.$$

最后，注意到 $a_{nn}=0$；就得到所求证的等式. □

3.3.4 推论 $M(X)$ 的每行元素之和与每列元素之和都为零.

证明 结合引理 3.3.2(1) 和引理 3.3.3 即得. □

以下是本节主要定理.

3.3.5 定理 设 $X=(V,E)$ 是连通图. 则矩阵 $M(X)$ 的所有元素的代数余子式彼此相等，它等于图 X 的生成树的棵数

证明分为几个步骤. 首先，定理的第一个结论直接从推论 3.3.4 以及下述线性代数引理推出.

3.3.6 引理 如果一个 $n\times n$ 矩阵的每行元素之和与每列元素之和都为零，则它的所有元素的代数余子式彼此相等.

证明 令 A 是如引理所设矩阵；设 $A(ij)$ 是从 A 中去掉第 i 行与第 j 列后得到的 $(n-1)\times(n-1)$ 矩阵. 注意到 $A(ij)$ 与 $A(1j)$ 有 $n-2$ 行相同(但位置可能不完全相同)，通过以下三组初等变换可把 $A(ij)$ 变换到 $A(1j)$：

(1) 从 $A(ij)$ 开始：把所有行加到第 1 行；

(2) 第 1 行乘以 -1，此时第 1 行等于 $A(1j)$ 的第 $i-1$ 行即 A 的第 i 行去掉第 j 个元；

(3) 把第 1 行与第 2 行对换，第 2 行与第 3 行对换，等等；经过 $i-2$ 个相邻行的对换把原第 1 行换到第 $i-1$ 行，故所得矩阵等于 $A(1j)$. 所以行列式 $(-1)^{i-1}\det A(ij)=\det A(1j)$；从而

$$(-1)^{i+j}\det A(ij)=(-1)^{i+j+i-1}A(1j)=(-1)^{1+j}A(1j).$$

即任意 (i,j)- 代数余子式等于 $(1,j)$- 代数余子式. 同理可证，任意 $(1,j)$- 代数余子式等于 $(1,1)$- 代数余子式. 故所有代数余子式彼此相等. □

为证定理 3.3.5，现在只需证明 $M(X)$ 的 (n,n)- 代数余子式，记作 D_n，等于 X 的生成树的棵数，这里 $n=|V|$ 是图 X 的阶.

考虑 $M(X)=E(X)\cdot E(X)^{\mathrm{T}}$. 去掉矩阵 $E(X)$ 的最后一行，所得 $(n-1)\times n$ 矩阵记作 E_1. 那么直接的矩阵运算告诉我们

(3.3.7)　$D_n = M(X)$ 的 (n,n)- 代数余子式 $=\det(E_1\cdot E_1^{\mathrm{T}})$.

现在需要另一个线性代数引理.

3.3.8 引理　设矩阵 $A=(a_{ij})_{n\times m}$，$B=(b_{ij})_{m\times n}$，其中 $m\geqslant n$. 则

$$\det(AB)=\sum_{\substack{(j_1,j_2,\cdots,j_n)\\ 1\leqslant j_1<\cdots<j_n\leqslant n}}\det A\begin{pmatrix}1&\cdots&n\\ j_1&\cdots&j_n\end{pmatrix}\cdot\det B\begin{pmatrix}j_1&\cdots&j_n\\ 1&\cdots&n\end{pmatrix}$$

其中 $A\begin{pmatrix}1&\cdots&n\\ j_1&\cdots&j_n\end{pmatrix}$ 是由 A 的第 j_1 列，第 j_2 列，…，第 j_n 列构成的 $n\times n$ 矩阵；$B\begin{pmatrix}j_1&\cdots&j_n\\ 1&\cdots&n\end{pmatrix}$ 的意义类似.

证明　以下总用 $(c_{ij})_{1\leqslant i,j\leqslant n}$ 其中 c_{ij} 是数，表示矩阵. 则

$$\begin{aligned}
&\det(AB)\\
&=\det\Big(\sum_{k=1}^{m}a_{ik}b_{kj}\Big)_{1\leqslant i,j\leqslant n}\\
&=\sum_{(k_1,\cdots,k_n)}\det\big(a_{ik_j}b_{k_jj}\big)_{1\leqslant i,j\leqslant n}\qquad(\text{各 } k_j \text{ 均跑遍 } 1,2,\cdots,m)\\
&=\sum_{(k_1,\cdots,k_n)}\det\big(a_{ik_j}\big)_{1\leqslant i,j\leqslant n}\cdot b_{k_1 1}b_{k_2 2}\cdots b_{k_n n}\\
&\qquad\qquad(\text{第 } j \text{ 列提出公因子 } b_{k_j j})\\
&=\sum_{\substack{(k_1,\cdots,k_n)\\ k_\alpha\neq k_\beta\ \text{当}\ \alpha\neq\beta}}\det\big(a_{ik_j}\big)_{1\leqslant i,j\leqslant n}\cdot b_{k_1 1}b_{k_2 2}\cdots b_{k_n n}\\
&\qquad\qquad(\text{两列相等的行列式为 } 0)\\
&=\sum_{1\leqslant j_1<\cdots<j_n\leqslant m}\ \sum_{\substack{(k_1,\cdots,k_n)\text{跑遍}\\ j_1,\cdots,j_n\text{的排列}}}\det A\begin{pmatrix}1&\cdots&n\\ j_1&\cdots&j_n\end{pmatrix}
\end{aligned}$$

$$\cdot(-1)^{\sigma(k_1,\cdots,k_n)}b_{k_1 1}b_{k_2 2}\cdots b_{k_n n}$$

$$=\sum_{1\leqslant j_1<\cdots<j_n\leqslant m}\det A\begin{pmatrix}1 & \cdots & n\\ j_1 & \cdots & j_n\end{pmatrix}\det B\begin{pmatrix}j_1 & \cdots & j_n\\ 1 & \cdots & n\end{pmatrix}$$

其中 $\sigma(k_1,\cdots,k_n)$ 记排列 $(k_1,\cdots,k_n)$ 的逆序数. □

回到定理 3.3.5 的证明. 把引理 3.3.8 用到式(3.3.7),得到

$$D_n=\det(E_1\cdot E_1^{\mathrm{T}})=\sum_{S_1}\det(S_1\cdot S_1^{\mathrm{T}}),$$

其中 S_1 跑遍 E_1 的 $n-1$ 阶子矩阵.

那么,任一 S_1 是从 $E(X)$ 取 $n-1$ 列再去掉最后一行得到的 $(n-1)\times(n-1)$ 矩阵. $E(X)$ 是由关联矩阵 $B(X)$ 的每列改变一个符号得来的,见定义 3.3.1. 按照关联矩阵 $B(X)$ 的定义,从 $E(X)$ 构作 S_1 时取的 $n-1$ 列对应于图 X 的 $n-1$ 条边,这 $n-1$ 条边与顶点集 V 一起构成了 X 的一个子图,记作 Y;而 Y 的交错关联矩阵 $E(Y)$ 按照定义就是 $E(X)$ 中构作 S_1 时取出的 $n-1$ 列. 所以按照式(3.3.7),$\det(S_1\cdot S_1^{\mathrm{T}})$ 就是 $M(Y)=E(Y)\cdot E(Y)^{\mathrm{T}}$ 的 (n,n)- 代数余子式. 另一方面,注意到 X 的任意一个带 $n-1$ 条边的子图 Y 对应于 $E(X)$ 的 $n-1$ 列,所以对应于一个这样的 S_1;特别是,生成树一定对应于这样一个 $n-1$ 阶子矩阵 S_1. 因此下面的结论可以完成整个定理 3.3.5 的证明.

3.3.9 引理 设图 $Y=(V,E)$, $V=\{v_1,v_2,\cdots,v_n\}$, $E=\{e_1,e_2,\cdots,e_{n-1}\}$. 则

$$M(Y)\text{ 任一代数余子式}=\begin{cases}1, & \text{当 } Y \text{ 连通即为树;}\\ 0, & \text{否则.}\end{cases}$$

(注:由于定理 3.3.5 的第一个结论已证,$M(Y)$ 的所有代数余子式相同.)

证明 $M(Y)$ 的 (n,n)- 代数余子式为

$$\det(S_1 \cdot S_1^{\mathrm{T}}) = (\det S_1)^2,$$

其中 S_1 是从 $E(Y)$ 去掉最后一行得到的 $(n-1)\times(n-1)$ 矩阵. 以下分两种情形讨论.

情形 1：Y 不连通. 则有一连通分支 Y_1 不含 v_n，此连通分支的阶 $k < n$. 由关联矩阵的定义，v_n 对应 $E(Y)$ 的最后一行；那么连通分支 Y_1 的顶点对应的 $E(Y)$ 的行全部在 S_1 中，不妨设是 S_1 的前 k 行. 对于任意 $e_j \in E$，若 e_j 在 Y_1 中，则 $E(Y)$ 的第 j 列的两个非零元 ± 1 在前 k 行中；否则第 j 列的前 k 个元全是零. 特别是，S_1 的前 k 行之和为零，所以 $\det S_1 = 0$，从而 $\det(S_1 \cdot S_1^{\mathrm{T}}) = 0$.

情形 2：Y 连通. 那么 Y 是树，从而 Y 有端点，见推论 3.1.13. 适当重编号：先令 v_1 是端点；则 v_1 与惟一一条边关联，再令 e_1 是这惟一与 v_1 关联的边. 那么 $E(Y)$ 的第 1 行是 $(\pm 1,0,\cdots,0)$. 从 X 中去掉点 v_1 和边 e_1 得到阶 $n-1$ 的树 Y_1；同样地，Y_1 有端点编号为 v_2，与之关联的惟一边编号为 e_2；则 $E(Y_1)$ 的第 1 行是 $(\pm 1,0,\cdots,0)$；因而 $E(Y)$ 的前 2 行是 $\begin{pmatrix} \pm 1 & 0 & 0 & \cdots & 0 \\ * & \pm 1 & 0 & \cdots & 0 \end{pmatrix}$. 如此做下去，最后得到的 $E(Y)$ 就是对角线元素为 ± 1 的三角矩阵：

$$E(Y) = \begin{pmatrix} \pm 1 & 0 & 0 & \cdots & 0 \\ * & \pm 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ * & * & * & \cdots & \pm 1 \\ * & * & * & \cdots & * \end{pmatrix}$$

所以 $\det S_1 = \pm 1$，因而 $\det(S_1 \cdot S_1^{\mathrm{T}}) = 1$. □

至此，定理 3.3.5 全部证毕. 作为应用，我们计算 n 阶完全图 K_n 的生成树的棵树 $T(n)$.

3.3.10 推论 $T(n) = n^{n-2}$.

证明 对于 n 阶完全图 K_n 容易算出

$$A(K_n) = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{pmatrix}, d(v_i) = n - 1.$$

于是由引理 3.3.3 知道

$$M(K_n) = \begin{pmatrix} n-1 & -1 & -1 & \cdots & -1 \\ -1 & n-1 & -1 & \cdots & -1 \\ \vdots & \vdots & \vdots & & \vdots \\ -1 & -1 & -1 & \cdots & n-1 \end{pmatrix}_{n\times n}$$

它的 (n,n)- 代数余子式为

$$\det\begin{pmatrix} n-1 & -1 & -1 & \cdots & -1 \\ -1 & n-1 & -1 & \cdots & -1 \\ \vdots & \vdots & \vdots & & \vdots \\ -1 & -1 & -1 & \cdots & n-1 \end{pmatrix}_{(n-1)\times(n-1)}$$

为计算此行列式,把所有列加到第 1 列,第 1 列全变为 1;再把全为 1 的第 1 列分别加到第 $2,3,\cdots,n-1$ 列,得三角形行列式

$$\det\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & n & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & \cdots & n \end{pmatrix}_{(n-1)\times(n-1)} = n^{n-2}. \qquad \square$$

习题 3.3

1. 设 $X = (V,E)$ 为图,$A(X)$ 是它的邻接矩阵,$k \geqslant 1$. 证明:$A(X)^k$ 中的 (i,j)- 元等于从顶点 v_i 到 v_j 的长度为 k 的道的

条数.

2. 图 $X=(V,E)$ 称为二部图(bipartite graph),如果 $V=V_1 \cup V_2$ 为不交并,使得 V_1 的任意二点不相邻,V_2 的任意二点也不相邻.

(1) 给出二部图的邻接矩阵的特征.

(2) X 为二部图当且仅当对于任意奇数 k 有 $A(X)^k$ 的对角线元全为零.

§3.4　Greedy 算法和拟阵

假设某地区有 n 个地点需供水,可能铺设的管线用两点间的连线表示就得到一个图,但这种图的每条边有自己的长度. 如图 3-9 所示.

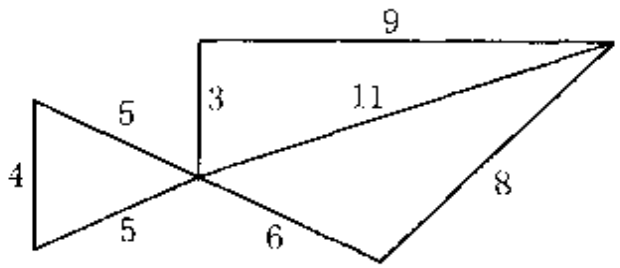


图 3-9

我们的问题是:如何选择一个最经济的铺设管线的方案?很简单的直观分析是:一个管线方案应该是一个子图,而且:(1) 它应该是连通的,否则不是一个供水系统;(2) 它应该是生成子图(见定义 3.1.7),因为所有地点都要供到水;(3) 它不应该有圈,因为有圈时就可去掉一条边使得(1)、(2) 两条仍然可以办到. 综上所述,问题是要找一棵生成树. 这由命题 3.1.15 即可以做到. 但这里有进一步的要求:要使得生成树的边长之和最小. 不过,这也只要把命题 3.1.15 的方法稍加改进就可以办到.

现在我们更数学化地来叙述.

3.4.1 定义 图 $X=(V,E)$ 称为一个边加权图(edge-weighted graph)如果它赋有一个函数 $w:E\to\mathbb{R}^+$,这里$\mathbb{R}^+$表示非负实数的集合,w 称为它的加权函数,或简称 w 为加权.类似地可以定义点加权图(point-weighted graph). 以下若非声明,"加权图"均指边加权图赋有加权函数 w.

设 $X=(V,E)$ 是一个加权图 设 $Y=(V_1,E_1)$ 是 X 的子图.则称 $w(Y)=\sum_{e_1\in E_1} w(e_1)$ 为 Y 的权或重量(weight).

加权图(连通加权图)$X=(V,E)$ 的重量极小的生成林(生成树)称为 X 的极小生成林(minimal spanning forest)(极小生成树(minimal spanning tree)). 类似地,可以定义极大生成林(maximal spanning forest)(极大生成树(maximal spanning tree)).

搜索极小生成林问题:设 $X=(V,E)$ 是一个加权图.如何最快地搜索出 X 的一座极小生成林?

一个很自然的也是很直观的想法是,首先找一条重量最小的边,即是一棵 2 阶子树;然后再加入使得能构成林而且重量最小的边,如此继续下去;最后一定达到一座生成林.下面形式化地写出这一过程.设 $X=(V,E)$ 是带权函数 w 的加权图.注意,由习题 3.1.9,X 的生成林的边数总是常数 $r=|V|-t$ 其中 t 是连通分支数.

3.4.2 搜索极小生成林算法. 在主算法之前需要做:

P1 定义存放加权边集的数据结构;

(注:随机存放有序结构,算法需要对它做搜索和逐个检验操作.)

P2 子算法 1. 检验一个图是否为林;

子算法 2. 搜索一个加权边集合中的重量最小边;

主算法的主体是一个检验循环.

A1　输入图 $X=(V,E)$;给 F,D 赋值空集;

(注:即初始化 X,F,D)

A2　只要(V,F) 不是 X 的生成林就做;

开始:　　(注:调用子算法 1)

A2.1　取所有不在 F 中的边放在 D 中;

(即赋值 $D:=E-F$)

A2.2　逐个检验 D 中的边e:如果$(V,F\cup\{e\})$不是林就从 D 中删去e;

A2.3　搜索 D 中重量最小的边e;　(注:调用子算法 2)

A2.4　把 e 加入F.　(注:即赋值 $F:=F\cup\{e\}$)

结束.

上述算法的另一种写法如下.

```
STRUCTURE weightedset;
int FUNCTION isforest (STRUCTURE weightedset);
    {Remark: return 1 if it is a forest, 0 otherwise}
weightedset FUNCTION miniedge(STRUCTURE weightedset);
    {Remark: return a minimal edge}
BEGIN
  VAR E,F,D: weightedset; VAR V:set;
  V:= input;E:= input;F:= ∅;D:= ∅;
  WHILE|F|< r DO
    BEGIN
      D:= E - F; i:= 1; k = |D|;{Remark:D = {d1,
      d2,⋯,dk}}
       WHILE i ≤ k DO
         BEGIN
           IF isforest (F ∪ {di}) = 0 DO
              BEGIN
```

FOR j = i TO k-1 DO $d_i := d_{i+1}$;

$k := k - 1$;

END

ELSE $i := i + 1$;

END

$D := \{d_1, d_2, \cdots, d_k\}$; $e :=$ miniedge(D); $F := F \cup \{e\}$;

END

END

这种做法的基本点是：每一步都是在符合基本要求的那些对象中(如上述问题中符合基本要求的就是这种边把它加入到已获得的子图后要构成林)选取最好的(如对上述问题而言"重量最小"就是最好). 因为每一步都"吃进"最好的，所以它被称为Greedy 算法.

然而问题是，每一步都"吃进"最好的，最后得到的从总体上来说确实是最好的吗?

对上述问题而言就是：最后输出的 F 确实是极小生成林吗?为回答此问题，先看看图的一个性质. 在叙述这性质之前，注意一个关键点，在上述问题以及上述算法的数据中，起主要作用的是加权边集.

3.4.3 引理 设 $X = (V, E)$ 是一个图(不必连通). 令

$$M = \{F \subset E \mid (V, F) \text{ 构成 } X \text{ 的子林}\}.$$

那么以下三条结论成立：

(1) $\varnothing \in M$;

(2) 若 $F \subset F'$ 而 $F' \in M$，则 $F \in M$;

(3) 若 $F, F' \in M$ 而 $|F| < |F'|$，则有 $e \in F' - F$ 使得 $F \cup \{e'\} \in M$. 而且 M 中的极大成员是图 X 的生成林.

证明 结论(1) 和(2) 都是显然的.

(3) 由于 $Y = (V, F)$ 和 $Y' = (V, F')$ 都是林，所以

$$t = |V| - |F|,\ t' = |V| - |F'|$$

分别是林 Y 和 Y' 的连通分支个数，见习题 3.1.9；而 $|F| < |F'|$，即 $t > t'$. 因此 Y' 至少有一个连通分支 T' 不被 Y 的任意一个连通分支完全包含(注意孤立点也是连通分支)；那么在 T' 中存在一条边 $e' \in F'$，它的两个端点属于 Y 的不同的连通分支，从而 $(V, F \cup \{e'\})$ 是图 X 的子林，即 $F \cup \{e'\} \in M$.

最后一个结论由命题 3.1.15 得出. □

3.4.4 定理 设 $X = (V, E)$ 为加权图. 则算法 3.4.2 经过有限步后停机，输出的 $T = (V, F)$ 是 X 的极小生成林.

证明 如同上述算法之前说明的，我们仍假设 r 是 X 的生成林的边数. 如果检验操作 $A2$ 的回答是“(V, F) 不是 X 的生成林”，就进入操作 A2.1 ~ A2.4；由命题 3.1.15，存在边 e 加到 F 后构成林，换言之，在操作 A2.3 中的 D 不是空集；因此在操作 A2.4 得到的 F 所含的边数增大了 1 个. 由于 X 的边数有限，经有限 m 步后在检验操作 A2 时会得到回答“(V, F) 是 X 的生成林”，从而停机，以下要证明此时的生成林 F 是极小的.

为了数学论证方便，设各步后得到的子林分别是

$$T_1 = (V, F_1), T_2 = (V, F_2), \cdots, T_r = (V, F_r),$$

其中 $F_i = F_{i-1} \cup \{e_i\}$，$T_r$ 是最后得到的生成林. 由此假设有

$$F_1 = \{e_1\}, F_2 = \{e_1, e_2\}, \cdots, F_r = \{e_1, e_2, \cdots, e_r\}.$$

使用引理 3.4.3 的记号，每个 $F_i \in M, i = 1, \cdots, r$；而且 F_r 是 M 的极大成员. 而且由习题 3.1.9 知 M 的极大成员都是含 r 条边.

注意 X 是加权图，我们用 w 表示 X 的加权. 于是可以断言

$$w(e_1) \leqslant w(e_2) \leqslant \cdots \leqslant w(e_r). \tag{3.4.4.1}$$

这是因为从算法过程可知 $F_{i-1} \cup \{e_i\}$ 与 $F_{i-1} \cup \{e_{i+1}\}$ 都是林，换言之，在从 F_{i-1} 往下算时，e_i 和 e_{i+1} 都在操作 A2.3 的集合 D 中；而从 F_{i-1} 构造 F_i 即操作 A2.4 时 e_i 是 D 中重量最小的边，即是说 $w(e_i) \leqslant w(e_{i+1})$.

如果 $T_r=(V,F_r)$ 不是极小生成林,则有 $T'=(V,F')$ 使得 $F'\in M$ 是 M 的极大成员而且 $w(F')<w(F_r)$;特别还有 $|F'|=r$,那么可设 $F'=\{e_1',e_2',\cdots,e_r'\}$,还不妨设

(3.4.4.2) $\quad w(e_1')\leqslant w(e_2')\leqslant\cdots\leqslant w(e_r')$.

比较(3.4.4.1)与(3.4.4.2).由于 e_1 是整个 E 中重量最小的边,故当然 $w(e_1)\leqslant w(e_1')$;但另一方面,$w(F_r)>w(F')$,即(3.4.4.1)的各项之和又大于(3.4.4.2)的各项之和,所以在把它们的对应项相比较时,就一定存在 $1<k\leqslant r$ 使得 $w(e_k)>w(e_k')$;由(3.4.4.1)和(3.4.4.2)就有

(3.4.4.3) $\quad w(e_1')\leqslant w(e_2')\leqslant\cdots\leqslant w(e_k')<w(e_k)$.

由于 $|\{e_1',e_2',\cdots,e_k'\}|=k>k-1=|F_{k-1}|$,按引理3.4.3(3),存在 e_j',$1\leqslant j\leqslant k$,使得 $F_{k-1}\cup\{e_j'\}\in M$.这就是说,在从 F_{k-1} 构造 F_k 时的操作A2.3中,e_j' 和 e_k 都属于 D,但按假设,操作A2.3选取了 e_k 是 D 中重量最小的边;所以 $w(e_j')\geqslant w(e_k)$.然而因为 $j\leqslant k$,根据(3.4.4.3)就有 $w(e_j')<w(e_k)$.这相互矛盾的结论表明本段开始的假设"T_r 不是极小生成林"不能成立.这就完成了整个证明. □

我们现在把这些研究做得更一般化.

3.4.5 定义 设 S 为有限集合,设 $M\subset P(S)$(S 的幂集).我们称 (S,M) 是一个拟阵(matroid)如果以下三条件成立:

(1) $\varnothing\in M$;

(2) 若 $F\subset F'$ 而 $F'\in M$,则 $F\in M$;

(3) 若 $F,F'\in M$ 而 $|F|<|F'|$,则有 $e'\in F'-F$ 使得 $F\cup\{e'\}\in M$.

进一步,如果对拟阵 (S,M) 有函数 $w:S\to\mathbb{R}^+$,这里 $\mathbb{R}^+$ 是非负实数的集合,则称 M 是加权拟阵(weighted matroid),称 w 是它的加权(weighting)或称权函数(weight function).此时,对于任意

$F \in M, w(F) = \sum_{e \in F} w(e)$ 称为 F 的重量(weight)(显然,重量可对 S 的任意子集定义).

例 拟阵的典型例子之一就是我们上面讨论的一个图的子林的集合;如果这个图是加权图,则得到的拟阵也是加权拟阵.

3.4.6 例 另一个典型例子是:设 S 是一个向量空间中的有限个向量的集合,令 M 是 S 的所有线性无关子集的集合,则 (S, M) 是一个拟阵;这时定义 3.4.5 的条件(3) 实际上相当于替换引理(参见本节习题 1). 正是因为这个例子,下面我们把拟阵 M 中的成员称为 S 的无关集,而 M 中的极大成员称为生成无关集.

3.4.7 注解 容易证明,一个拟阵 (S, M) 的 M 中的所有生成集(极大成员) 的基数彼此相等,这个基数称为该拟阵的秩(rank)(这也是从上一个例子借来的名词). 但对加权拟阵来说,生成集的重量不一定相等,见本节习题 2.

对加权拟阵,与算法 3.4.2 相同,我们同样有搜索极小生成无关集的算法 但是容易看出,对实际问题来说,有时候需要极小,有时候需要极大;对这两个不同目的可用同样的搜索算法. 前面已经有了一个"搜索极小" 的算法,所以下面我们列出"搜索极大" 的算法,其中 (S, M) 是带权函数 w 的加权拟阵,r 是它的秩.

3.4.8 搜索最大重量的极大成员的 Greedy 算法

P1 定义存放加权集的数据结构. (注:随机存放有序结构,算法需要对它做搜索和逐个检验操作.)

P2 子算法 1. 检验一个集合是否为给定集合组 M 的极大成员;

子算法 2. 搜索一个加权集中的重量最大元.

主算法

A1 输入 (S, M);给 F, D 赋值空集;

(注:M 是一组加权集)

A2 只要 F 不是 M 的极大成员就做

开始: (注:调用子算法 1)

A2.1 取 S 的所有不在 F 中的元素放在 D 中;(即赋值 $D:=S-F$)

A2.2 逐个检验 D 中的元素 e:如果 $F\cup\{e\}\in M$ 就从 D 中删去 e;

A2.3 搜索 D 中重量最大的元素 e; (注:调用子算法 2)

A2.4 把 e 加入 F. (注:即赋值 $F:=F\cup\{e\}$)

结束.

3.4.9 定理 设 (S,M) 是加权拟阵.则算法 3.4.8 经有限步后停机,输出的 F 是 M 的重量最大的极大成员.

证明 类似于定理 3.4.4 的证明,详情作为习题. □

3.4.10 注解 (1) 算法 3.4.8 本身并不局限于拟阵,它对于任意加权集 S 和它的子集组 $M\subset P(S)$ 都可以做,而且容易看出它一定经有限步停机给出 M 中的极大成员.

(2) 对拟阵 (S,M),上述定理已说它一定给出 M 中的重量最大的极大成员.但是 M 中的重量最大的极大成员可以有多个,算法所得结果与算法执行过程有关,因为在步骤 A2.3 中的 D 中的重量最大元不惟一,搜索过程可能取出不同的重量最大元.对此本节习题 5 是个有意思的结果.

(3) 现实告诉我们,每次都"吃进"最好的,总体结果不一定是最好的.下述结论确切地回答了这一点:从某种意义来说,Greedy 算法也只对拟阵起作用,即是说,它只对拟阵能保证给出最优解.

3.4.11 定理 设 S 是有限集,$M\subset P(S)$ 满足两条件:

(1) $\varnothing\in M$;

(2) 若 $F\subset F'$ 而 $F'\in M$,则 $F\in M$.

如果对于 S 的任意加权 $w:S\to\mathbb{R}^+$,算法 3.4.8 恒经有限步停机给出 M 中的重量最大的极大成员,则 (S,M) 是拟阵(即

3.4.5(3) 也满足).

证明 假定(S,M)不是拟阵,则有$E,F\in M$使得$|E'|>|E|$但是对于任意$e'\in E'$有$E\cup\{e'\}\in M$.取正实数ϵ,定义加权函数为

$$w:S\to\mathbb{R}^+,w(s)=\begin{cases}1+\epsilon, & \text{若 } s\in E;\\ 1, & \text{若 } s\in E'-E;\\ 0, & \text{否则.}\end{cases}\tag{3.4.11.1}$$

对这个加权,搜索"最大"的算法3.4.8从空集F开始每步都取得E中元,直到得到$F=E$;因为$E\cup\{e'\}\in M,\forall e'\in E'$,所以此后只会加入$S-E'$的元,决不会加入$E'$的元.这样,停机时输出的$F$不会包含$E'-E$的元.因而

$$\begin{aligned}w(F)&=w(E)=|E|+\epsilon\cdot|E|\\ w(E')&=|E'-E|+(1+\epsilon)\cdot|E'\cap E|\\ &=|E'|+\epsilon\cdot|E'\cap E|\end{aligned}\tag{3.4.11.2}$$

由于$|E'|>|E|$而$|E|-|E'\cap E|\geqslant 0$,满足下述条件的正实数$\epsilon$存在

$$\epsilon\cdot(|E|-|E'\cap E|)<|E'|-|E|$$

取这样的ϵ给出加权(3.4.11.1),那么由(3.4.11.2)就有:$w(E')>w(F)$,然而$E'\in M$;即是说,F不是M中重量最大的极大成员. □

习题 3.4

1. 设S是一个向量空间中的有限个向量的集合,令M是S的所有线性无关子集的集合,则(S,M)是一个拟阵.这样产生的拟阵称为线性拟阵(linear matroid).

2. (1) 拟阵(S,M)的M中的极大成员有相同的基数,这个基数称为该拟阵的秩(rank).

(2) 举例说明加权拟阵(S,M)的M中的极大成员的重量不一定相等.

3. 设(S,M)是拟阵，$T\subset S$. 令$N=\{F\cap T\mid F\in M\}$. 则(T,N)也是拟阵.

4. 证明定理 3.4.9.

5. 设(S,M)是拟阵，F是M的一个极大成员，$E\in M$. 证明：存在$E'\subset F-E$使得$E\cup E'$是M的极大成员.

6. 设(S,M)是带权函数w的加权拟阵. $\{e_1,e_2,\cdots,e_r\}\in M$是$M$的一个重量最大的极大成员且$w(e_1)\geqslant w(e_2)\geqslant\cdots\geqslant w(e_r)$. 再设$\{e_1',e_2',\cdots,e_r'\}\in M$，且$w(e_1')\geqslant w(e_2')\geqslant\cdots\geqslant w(e_r')$. 证明：

(1) $w(e_i)\geqslant w(e_i'),i=1,2,\cdots,r$.

(2) 进一步，如$\{e_1',e_2',\cdots,e_r'\}$也是$M$的重量最大的极大成员，则$w(e_i)=w(e_i'),i=1,2,\cdots,r$

(3) e_1是S中的重量最大的元素.

7. 设(S,M)是加权拟阵. 则对于M的任意一个重量最大的极大成员F，存在算法 3.4.8 的一个执行过程使得输出结果恰为F.

§3.5 循环赛图

设有n个篮球队$v_1,v_2,\cdots,v_n$进行循环赛，亦即每个队v_i与任一其他队v_j恰进行一场比赛(无平局比赛). 全部共$n(n-1)/2$场比赛；赛完后就可以得到一个有向完全图$D=(V,E)$：点集当然是$V=\{v_1,v_2,\cdots,v_n\}$，而边集是

$$E=\{(v_i\to v_j)\mid(v_i,v_j)\text{ 跑遍 }V^{(2)},v_i\text{ 胜 }v_j\}$$

3.5.1 定义 n阶有向完全图称为n-循环赛图(tournament graph). 以下为简单把顶点集记作$V=\{1,2,\cdots,n\}$.

例 从图的角度来说，图 3-10 中图(a)和图(b)是一样的：

因为在图(a)中只要将 2 和 3 对换就得到图(b). 但图(a)与图(c)却不一样，无法从顶点置换从图(a)得到图(c). 直观来说，图

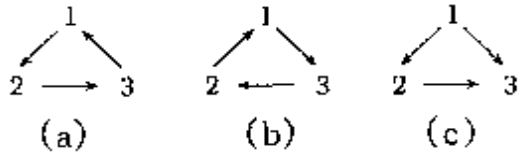


图 3-10

(a) 和图(b) 所表达的结果确实是类似的:每队胜负各一场. 但图(c) 则不一样,有一队两场全胜. 由此导致以下数学定义.

3.5.2 定义　称两个循环赛图 $D_1=(V_1,E_1)$ 和 $D_2=(V_2,E_2)$ 是同构的,记作 $D_1\cong D_2$,如果有一个双射 $\alpha:V_1\to V_2$ 使得对于任意 $(i\to j)\in E_1$ 有 $(\alpha(i)\to\alpha(j))\in E_2$(实际上,这也是一般图同构的定义).

从总体上考察 n 阶循环赛图,把所有以 $V=\{1,2,\cdots,n\}$ 为顶点集的循环赛图的集合记作 $\tau(n)$. 显然有以下引理.

3.5.3 引理　$|\mathscr{T}(n)|=2^{n(n-1)/2}$. □

任意 $\alpha\in S_n$ 对应一个 $\tilde{\alpha}\in \mathrm{Tran}(\mathscr{T}(n))$ 它把任意 $D\in\mathscr{T}(n)$ 变为图 $\tilde{\alpha}(D)=(V,\alpha(E))$,其中

$$\alpha(E)=\{(\alpha(i)\to\alpha(j))\mid(i\to j)\in E\}$$

3.5.4 引理　记号如上. 群 S_n 以上述方式忠实地作用在 n-循环赛图的集合 $\mathscr{T}(n)$ 上:$S_n\to \mathrm{Sym}(\tau(n)),\alpha\mapsto\tilde{\alpha}$.

证明见本节习题 2. □

那么,$\tau(n)$ 就被划分为 S_n- 轨道,就是 n- 循环赛图的同构类,见本节习题2. 与上面的分析相同,一个 S_n- 轨道就是 n 个队进行循环赛的结局的一种模式,属于同一轨道的循环赛图表示的结局虽然对各队来说不一样,但结局的形式或者说模式是一样的,只是各队的位置不一样. 如图 3-11 所示. 这样自然地就产生了下述数学问题.

问题:$\mathscr{T}(n)$ 的 S_n- 轨道有多少个?实际意义是:n 个球队进行

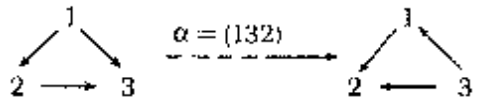


图 3-11

循环赛的结局有多少种模式?

因为我们有 Burnside 轨道计数公式,引理 2.2.12,集合 $\mathcal{T}(n)$ 上 S_n- 轨道个数是

$$t = \frac{1}{n!}\sum_{\alpha\in S_n} |\mathrm{Fix}(\alpha)|, \tag{3.5.5}$$

这里 $\mathrm{Fix}(\alpha) = \{D \in \mathcal{T}(n) \mid \tilde{\alpha}(D) = D\}$ 是 α 的不动点的集合. 因此,为解决上述问题,只要计算出 $|\mathrm{Fix}(\alpha)|$ 即可

为此作为准备,我们先研究一下无向图的两个情形,都涉及完全性;第一个是完全图.

3.5.6 引理 设 $\alpha = (12\cdots m)$ 是一个 m- 循环置换. 设 K_m 是点集 $V = \{1,2,\cdots,m\}$ 上的完全图 则群 $\langle\alpha\rangle$ 作用在 K_m 的边集 E 上(见例 2.2.4).

(1) 若 $m = 2k$ 是偶数,则 $(1,k+1) \in E$ 在 $\langle\alpha\rangle$ 中的稳定子群是 $\langle\alpha^k\rangle \leqslant \langle\alpha\rangle$ 且 $\alpha^k(1,k+1) = (k+1,1)$;特别是,$(1,k+1)$ 所在的 $\langle\alpha\rangle$- 轨道长 k.

(2) 若 m 是奇数,则 E 的每个 $\langle\alpha\rangle$- 轨道长 m.

证明 (1) 直接计算即可知,边 $(1,k+1)$ 所在的 $\langle\alpha\rangle$- 轨道为 $(1,k+1),\alpha(1,k+1) = (2,k+2),\cdots,\alpha^{k-1}(1,k+1) = (k,2k)$.

(2) 设边 $e = (ij)$. 若 $\alpha^k \in \langle\alpha\rangle$ 稳定 e,即 $\alpha^k(ij) = (ij)$;则

$$\begin{cases}\alpha^k(i) = i\\ \alpha^k(j) = j\end{cases} \text{ 或者 } \begin{cases}\alpha^k(i) = j\\ \alpha^k(j) = i\end{cases}$$

但马上可看出后一情形不可能发生:因为若如此,则 α^k 的循环分解中有 2- 循环,从而 $|\alpha^k|$ 是偶数,由 Lagrange 定理,$|\alpha^k| \mid |\alpha|$,这与假设矛盾,所以只能是 $\alpha^k(i) = i$. 然而 $\alpha^k(i) \equiv i +$

$k(\mathrm{mod}\ m)$，见本节习题 3；那么 $i \equiv i + k(\mathrm{mod}\ m)$，即是 $k \equiv 0\ (\mathrm{mod}\ m)$；也就是 $\alpha^k = 1$. 可见，$e = (ij)$ 在 $\alpha^k \in \langle\alpha\rangle$ 中的稳定子群是 1. 故 e 所在的 $\langle\alpha\rangle$- 轨道长 m. □

在下一个引理中将用到二部图的概念，见习题 3.3.2. 图 $B = (V, E)$ 称为二部图，如果 $V = V_1 \cup V_2$ 为不交并，使得 V_1 的任二点不相邻，V_2 的任二点也不相邻；换言之，只在 V_1 与 V_2 之间有边，二部图 $B = (V, E)$ 也可记为 $B = (V_1 \cup V_2, E)$. 进一步，如果 E 包括了全部的 V_1 与 V_2 之间的边，则称 B 为完全二部图 (complete bipartite graph).

3.5.7 引理　设置换 $\alpha = (i_1 i_2 \cdots i_m)(j_1 j_2 \cdots j_l)$ 是两个无公共文字的循环之积，$V_i = \{i_1, i_2, \cdots, i_m\}$ 和 $V_j = \{j_1, j_2, \cdots, j_l\}$. $B = (V_i \cup V_j, E)$ 是完全二部图. 则群 $\langle\alpha\rangle$ 作用在边集 E 上且 E 的每个 $\langle\alpha\rangle$- 轨道长度都是 $|\alpha| = ml/\gcd(m, l)$，这里 $\gcd(m, l)$ 表示最大公约数.

证明　记 $\gamma_i = (i_1 i_2 \cdots i_m)$，$\gamma_j = (j_1 j_2 \cdots j_l)$. 由习题 2.1.2，$|\alpha| = ml/\gcd(m, l)$. 显然 α 作用在 $V = V_i \cup V_j$ 上的轨道正好就是 V_i 和 V_j 两个，所以对于任意 $e = (i_s, j_t) \in E$，$i_s \in V_i$ 而 $j_t \in V_j$，$\alpha(e) = \alpha(i_s, j_t) = (\alpha(i_s), \alpha(j_t)) \in E$. 故群 $\langle\alpha\rangle$ 作用在集合 E 上. 而且对于任意 $(i_s, j_t) \in E$ 有

$$\begin{aligned}
\alpha^k(i_s, j_t) = (i_s, j_t) &\Longleftrightarrow (\alpha^k(i_s), \alpha^k(j_t)) = (i_s, j_t) \\
&\Longleftrightarrow \gamma_i^k(i_s) = i_s \text{ 且 } \gamma_j^k(j_t) = j_t \\
&\Longleftrightarrow i_s + k \equiv i_s (\mathrm{mod}\ m) \text{ 且 } j_t + k \equiv j_t \\
&\qquad (\mathrm{mod}\ l) \qquad\qquad (\text{见本节习题 3}) \\
&\Longleftrightarrow k \equiv 0\ (\mathrm{mod}\ m) \text{ 且 } k \equiv 0\ (\mathrm{mod}\ l) \\
&\Longleftrightarrow k \equiv 0\ (\mathrm{mod}\ ml/\gcd(m, l)).
\end{aligned}$$

亦即任意 $e \in E$ 在 $\langle\alpha\rangle$ 中的稳定子群是单位元子群 1；按命题 2.2.11，任意轨道长度等于 $ml/\gcd(m, l)$. □

现在回到考虑 $\tau(n)$. 以下是关键性引理.

3.5.8 引理 设 n 次置换 α 的型为 $\lambda=(\lambda_1,\lambda_2,\cdots,\lambda_n)$，见定义 2.1.4. 则 α 作为 $\mathcal{T}(n)$ 的置换有

(1) 如果 $|\alpha|$ 为偶数，则 $\mathrm{Fix}(\alpha)=\varnothing$.

(2) 如果 $|\alpha|$ 为奇数，则 $|\mathrm{Fix}(\alpha)|=2^{d(\lambda)}$，其中(这里 $\gcd(m,l)$ 表示最大公约数)

$$d(\lambda)=\frac{1}{2}\Big(\sum_{m,l=1}^{n}\gcd(m,l)\lambda_m\lambda_l-\sum_{m=1}^{n}\lambda_m\Big).$$

证明 证明之前先说明一下，由习题 2.1.2，$|\alpha|$ 为偶数等价于 α 的循环分解有长为偶数的循环；而 $|\alpha|$ 为奇数等价于 α 的循环分解没有长为偶数的循环.

(1) 可设 $(1,\cdots,k,k+1,\cdots,2k)$ 是出现在 α 的循环分解中的一个长为偶数 $2k$ 的循环. 对于任意 $D=(V,E)\in\mathcal{T}(n)$，因为它是有向完全图，$(1\to k+1)$ 与 $(k+1\to 1)$ 二者之一且仅一在 E 中；但由引理 3.5.6 或者直接计算即知，α^k 恰好把这二者互换，所以恒有 $\alpha^k(E)\neq E$，即恒有 $\alpha^k(D)\neq D$；从而恒有 $\alpha(D)\neq D$，$\forall D\in\mathcal{T}(n)$. 此即结论(1).

(2) 设 $\alpha=\gamma_1\gamma_2\cdots\gamma_r$ 为循环分解，每个 $\gamma_i=(i_1i_2\cdots i_m)$ 是长为奇数 m 的循环. 那么集合 $V=\{1,2,\cdots,n\}$ 被划分成了 r 个子集 $V_i=\{i_1,i_2,\cdots,i_m\}$，$i=1,2,\cdots,r$ 的不交并. 所有这样的循环赛图 $D\in\mathrm{Fix}(\alpha)$，可按下述两个步骤构造出来.

步骤 1 对于每个 $\gamma_i=(i_1i_2\cdots i_m)$，先把集合 $V_i=\{i_1,i_2,\cdots,i_m\}$ 的任意二点连接起来构造成完全图 $K_m=(V_i,E_i)$. 当然对于 K_m 的边集 E_i 的边任意赋予定向，使之成为定向边集 E_i'，就可以使 K_m 成为定向完全图 $D_i=(V_i,E_i')$，但它不一定在 α 变换之下不变. 注意 α 在 E_i 上的作用就是 γ_i 在 E_i 上的作用，要使得 $\alpha(D_i)=D_i$ 只要使得 $\gamma_i(D_i)=D_i$ 即可，亦即使得 $\gamma_i(E_i')=E_i'$ 即可. 由引理 3.5.6，未定向边集 E_i 被划分为 $\langle\gamma_i\rangle$- 轨道 Ω_y，每个轨道长都是 $|\Omega_y|=m$；那么可设

$$\Omega_{ij} = \{e_{j1}, e_{j2}, \cdots, e_{jm}\}, \text{ 其中 } e_{jk} = \gamma_i^{k-1}(e_{j1}).$$

一旦把未定向边 e_{j1} 定了向，比如 $e_{j1} = (s, t)$ 定向为 $(s \to t)$，要使得整个定向是 γ_i- 不变的，其他未定向边

$$e_{jk} = \gamma_i^{k-1}(e_{j1}) = (\gamma_i^{k-1}(s), \gamma_i^{k-1}(s))$$

就必须也只需定向为定向边

$$(\gamma_i^{k-1}(s) \to \gamma_i^{k-1}(s)).$$

换句话说，对于 E_i 的任意一个 $\langle\gamma_i\rangle$- 轨道 Ω_{ij}，有且只有两个使得 γ_i 作用不变的定向选择：把 $e_{j1} = (s, t)$ 或者定向为 $(s \to t)$，或者定向为 $(t \to s)$. 由于 $(E_i) = m(m-1)/2$ 而每个轨道长 m，$\langle\gamma_i\rangle$- 轨道共有 $(m-1)/2$ 个. 这样，从未定向的完全图 $K_m = (V_i, E_i)$ 可以构造出的 α- 不变的定向完全图 $D_i = (V_i, E_i')$ 个数为 $2^{(m-1)/2}$，这里 m 是 α 的循环分解 $\gamma_1\gamma_2\cdots\gamma_r$ 中循环 $\gamma_i = (i_1 i_2 \cdots i_m)$ 的长度，而 $V_i = \{i_1, i_2, \cdots, i_m\}$.

作为本步骤小结，上面讨论中的 γ_i 要跑遍 α 的所有循环，长度 m 的循环共 λ_m 个，而 $m = 1, 2, \cdots, n$，所以对所有循环 γ_i，$i = 1, 2, \cdots, r$，共得到构造方式个数为

$$\prod_{m=1}^{n} (2^{(m-1)/2})^{\lambda_m} = 2^{\frac{1}{2}\sum_{m=1}^{n}\lambda_m(m-1)}.$$

步骤 2　对于任意两个不同的循环 $\gamma_i = (i_1 i_2 \cdots i_m)$ 和 $\gamma_j = (j_1 j_2 \cdots j_l)$，$i \neq j$，有不交子集 $V_i = \{i_1, i_2, \cdots, i_m\}$ 和 $V_j = \{j_1, j_2, \cdots, j_l\}$. 因为要作完全图，把 V_i 的每个点与 V_j 的每个点连接起来，得到完全二部图 $B = (V_i \cup V_j, E)$. 由引理 3.5.7，$\langle\alpha\rangle$ 作用在边集 E 上. 现在我们遇到与上述讨论类似的情况：对 E 的每个 $\langle\alpha\rangle$- 轨道有且只有两个使得 α 作用不变的定向选择；而由引理 3.5.7，每个 $\langle\alpha\rangle$- 轨道长度为 $ml/\gcd(m, l)$；另一方面，$|E| = ml$；即轨道个数是 $ml \Big/ \dfrac{ml}{\gcd(m, l)} = \gcd(m, l)$. 这样，对于任意两个不同的循环 $\gamma_i = (i_1 i_2 \cdots i_m)$ 和 $\gamma_j = (j_1 j_2 \cdots j_l)$，得到定向方式

个数是 $2^{\gcd(m,l)}$.

作为本步骤小结,需要知道上面讨论中的两个不同的循环 γ_i 和 γ_j 有多少对. 当 $m \neq l$ 时,长 m 与长 l 的循环分别有 λ_m 个和 λ_l 个,所以共有 ml 对;由此得到的定向方式个数是

$$\prod_{1\leqslant m<l\leqslant n} 2^{\gcd(m,l)\lambda_m\lambda_l} = 2^{\sum\limits_{1\leqslant m\leqslant l\leqslant n}\gcd(m,l)\lambda_m\lambda_l}.$$

但当 $m = l$ 时,只能在长 m 的 λ_m 个循环中配对,故有 $m(m-1)/2$ 对. 由此得到的定向方式个数是

$$\prod_{m=1}^{n} 2^{\gcd(m,m)\lambda_m(\lambda_m-1)/2} = 2^{\sum\limits_{m=1}^{n} m\lambda_m(\lambda_m-1)/2}.$$

那么在步骤 2 中得到的定向方式总个数是

$$\begin{aligned} &2^{\gcd(m,l)\lambda_m\lambda_l} \cdot 2^{\gcd(m,m)\lambda_m(\lambda_m-1)/2} \\ &= 2^{\sum\limits_{1\leqslant m<l\leqslant n}\gcd(m,l)\lambda_m\lambda_l + \sum\limits_{m=1}^{n} m\lambda_m(\lambda_m-1)/2} \end{aligned}$$

通过上述两个步骤,就构造出了全部的在 α 变换之下不变的 n 阶循环赛图,总个数是 $2^{d(\lambda)}$,其中

$$\begin{aligned} d(\lambda) &= \frac{1}{2}\sum_{m=1}^{n}\lambda_m(m-1) + \sum_{1\leqslant m<l\leqslant n}\gcd(m,l)\lambda_m\lambda_l \\ &\quad + \frac{1}{2}\sum_{m=1}^{n} m\lambda_m(\lambda_m-1) \\ &= \frac{1}{2}\Big(\sum_{m,l=1}^{n}\gcd(m,l)\lambda_m\lambda_l - \sum_{m=1}^{n}\lambda_m\Big). \end{aligned}$$

这就是所求证的等式. □

3.5.9 定理 设不超过 n 的最大奇数是 q. 彼此不同构的 n 阶循环赛图的个数是

$$\sum_{\lambda=(\lambda_1,\lambda_3,\cdots,\lambda_q)} \frac{2^{d(\lambda)}}{1!2!\cdots n!\cdot 1^{\lambda_1}3^{\lambda_3}\cdots q^{\lambda_q}},$$

其中 $\lambda = (\lambda_1,\lambda_3,\cdots,\lambda_q)$ 跑遍方程 $x_1 + 3x_3 + \cdots + qx_q = n$ 的非负整数解,而

$$d(\lambda) = \frac{1}{2}\Big(\sum_{m,l=1}^{n}\gcd(m,l)\lambda_m\lambda_l - \sum_{m=1}^{n}\lambda_m\Big).$$

证明　由式(3.5.5)以及引理 3.5.8(1)，只需计算 $|\mathrm{Fix}(\alpha)|$，其中 $\lambda(\alpha)=(\lambda_1(\alpha),\lambda_2(\alpha),\cdots,\lambda_n(\alpha))$ 使得对于任意奇数 k 有 $\lambda_k(\alpha)=0$. 因此只要考虑置换的这种型 $\lambda=(\lambda_1,\lambda_3,\cdots,\lambda_q)$. S_n 中这种型 λ 的置换个数是(见 Cauchy 公式 2.1.6)

$$\frac{n!}{1!2!\cdots n!\cdot 1^{\lambda_1}3^{\lambda_3}\cdots q^{\lambda_q}}.$$

而对每个这种型 λ 的置换 α 由引理 3.5.8 知

$$|\mathrm{Fix}(\alpha)|=2^{d(\lambda)}.$$

把这些知识运用到等式(3.5.5)就得到本定理的结论. □

习题 3.5

1. 证明引理 3.5.3.

2. (1) 设 G 是一个 n 次置换群，对于任意 $\alpha\in G$ 令 $\tilde{\alpha}\in\mathrm{Tran}(\tau(n))$ 与之对应，这里 $\tilde{\alpha}(D)=(V,\alpha(E)),\forall D=(V,E)\in\tau(n)$;见定义 3.5.2. 则 $\alpha\mapsto\tilde{\alpha}$ 给出了群 G 在集合 $\tau(n)$ 上的一个忠实作用.

(2) 记号同上，取 $G=S_n$. 证明:两个循环赛图在同一个 S_n-轨道当且仅当它们同构.

3. 设 $\alpha=(12\cdots m)$ 是一个 m- 循环置换. 则对于任一指标 $1\leqslant i\leqslant m$ 有 $\alpha^k(i)\equiv i+k(\mathrm{mod}\ m)$.

4. 设 n 个运动队 $v_1,v_2,\cdots,v_n$ 进行淘汰赛，两个队进行一场比赛，输者被淘汰，最后决出冠军，则可得到一个 n 阶有向图 $T=(V,E)$: $V=\{1,2,\cdots,n\}$, $(v_i\to v_j)\in E$ 如果 v_i 淘汰了 v_j，这种图称为淘汰赛图. 证明:

(1) n 个队的淘汰赛不论怎样安排比赛场次总是 $n-1$ 场，从而淘汰赛图 T 是一棵有向树.

(2) 一棵有向树 T 可以是某个淘汰赛的淘汰赛图，当且仅当图 T 的每个顶点的入次数至多为 1(v_i 的入次数是指以 v_i 为终点的边的条数).

第 4 章　线 性 码

§4.1　检错码与纠错码

编码理论与信息论几乎发源于同时(20 世纪 40 年代)同地(Bell 实验室).它们研究用适当的字母去恰当地表示与传送信息.

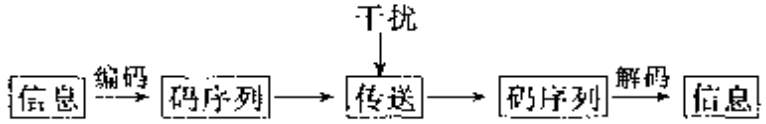


图 4-1

信息论研究信息及其载体(码)转化与传送的性质.这一理论在本质上是统计的.而编码则是研究如何用字母表(如二元系统)按特定要求(检错,纠错,保密等)去表达,去还原信息,它在本质上是代数的与组合的.虽然这两个理论无疑是密切相关的,然而多年来在很大程度上却又是独立发展的.在开始阶段(20 世纪 40 ～ 50 年代)信息论急骤升温,而编码理论的数学基础还没有信息论那样好,未引起众多学者的重视.后来各种数学工具,如群论,有限域理论,甚至线性规划,群表示理论,代数曲线理论等用于编码,编码技术才逐步发展,编码理论也成为数学研究中一个活跃的分支.

现代计算机中所使用的 ASCⅡ 码是为众多人熟知的一个编码的例子,它的字母表是{0,1}由两个字符组成,每个码字长为 8(计算机中称为 8 bits,一个码字就称为一个 byte,称为一个字

节),共可表示 256 个符号.例如信息“OK” 的处理过程如下:

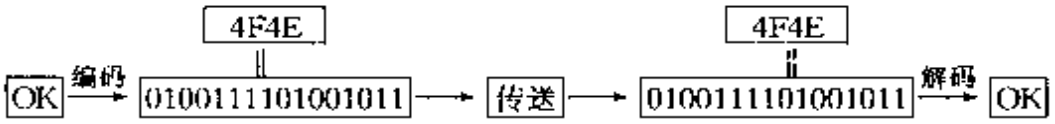


图 4-2

注解 1　早期的 ASCⅡ 码只表示 128 个符号,每个码字仍为 8 位,128 个符号实际上只占用 7 位,第 8 位用于检验位,这就是下面将要讲的检验码.由于计算机技术的发展,计算机稳定性提高,检验位后来被取消,成为现在的 256 个符号的 ASCⅡ 码.

注解 2　由于传输过程中不可避免的干扰,码序列在传送中可能出错,在接受后可纠正错误的码称为纠错码(error-correcting codes),现在说的“编码” 理论与技术,狭义地讲,是指纠错码的理论与技术.

注解 3　为保密而构作的码,称为密码.它的基本目的与纠错码不同,是为了使得除了接收者以外的他人无法认识码序列,因此在发送前人为地变换码序列,称为加密;变换方式应该是所谓“单向的”,即逆变换很难被他人找出.接收人知道逆变换,就可以解密读出信息.在密码理论与技术中,由信息编成的码序列称为明文,加密后的码序列称为密文.

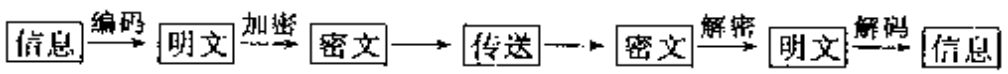


图 4-3

值得注意的是,这里的编码过程主要是指把信息编为字母表的字母序列(即语言表达),与纠错码技术中的编码过程意义有所不同.常用的加密方式是对字母表作变换.如,例 1.4.9 的 RSA 系统就是以模 m 剩余系$\mathbb{Z}_m$为字母表,这里 $m = pq$ 是两个大素数的

乘积，用 τ_e 作加密变换，其中 $ed \equiv 1 \pmod{\varphi(m)}$.

现在给出码的纯数学定义.

4.1.1 定义 设 A 为一个有限集合，称为字母表. 由 A 中元素构成的有限序列(简称串 string) 称为字(word)，序列长度称为字长. 字的全体记作 A^*. 任意两个字 x, y 连起来 xy 显然还是一个字，这就在 A^* 中定义了一个运算，称为乘法. 在此运算之下 A^* 成为一个幺半群. 设 C 是 A^* 的一个子集. 如果下述条件满足(可识别条件)：

对于任意 $c_1, c_2, \cdots, c_m, c_1', c_2', \cdots, c_n' \in C$，只要 $c_1 c_2 \cdots c_m = c_1' c_2' \cdots c_n'$ 就必有 $m = n$ 而且 $c_i = c_i'$ 对于所有 $i = 1, 2, \cdots, n$；

则称 C 为字母表 A 上的一个码(code). 码 C 中的字称为码字. 若 C 中的所有码字 c 的长度为定值，则称 C 为定长码；否则称为变长码. 若 $|A| = n$，则称 C 为 n- 元码.

能检查出错误的码称为检错码. 不仅能检查出错误而且能纠正错误的码称为纠错码.

定义 4.1.1 虽然比较数学化，但可识别条件的实际意义比较清楚：就是在以这种语言写成的文章中，应能分辨出各个单词.

介绍两种常见的检错码.

早期的 ASC 码以 $\{0,1\}$ 为字母表，每个码字长 8 位. 即长度 8 的 2 元码，其中 1 ~ 7 位是信息位(所以只有 128 个码字)，第 8 位是检验位，它使得 8 位数之和模 2 为 0. 例如“OK” 的“O” 编码为码字 11001111，其中 1001111 是“O” 本身的编码，而最高位放置 1 则使得 8 位数之和模 2 为 0. 这样在收到该码字后，把 8 位相加，若模 2 为 0，则可认为无错，去掉最高位得 1001111 即可译码得“O”，否则可断定出错，所以“OK” 编码为“11001111 01001011”.

以上检验错误的方法称为奇偶性检验(parity check)，也称为一致性检验. 显然，当一个码字的出错位不超过 1 个时，可检验出错码字.

需要指出的是，现在的计算机已具有极高的稳定性，出错率极

小,所以已取消检验位.这样就扩大了信息量,具有256个码字.因此现在"OK"的ASC码为"01001111 01001011".

显然,上述一致性检验错误的方法可以推广到对任意长度的码字来检验其错误.

4.1.2结论 令A为模m剩余系的m个字符$0,1,\cdots,m-1$.令$C\subseteq A^*$为一个定长n的码.在每个码字的头部加一位使得各位字符之和模m为0,就成为一个可检查一个错的长$n+1$的m-元检错码.

进一步的方法是所谓的加权,以国际标准书号(称为ISBN)为例来说明之.

按国际惯例,每本书有一个十进制的十位书号,如0-387-11284-7(连字符"-"不是实质性的,其位置在各书上也不尽相同):0表示英文,387是出版社号,11284是出版社给的书号,末位7是检验位.然而各位数之和模10不是0,显然它采用的不是通常的一致性检验法.这里的原因如下.书号原来都是人工处理的,人在处理数字时,除抄错数字外,易犯的错误之一是颠倒相邻数字,例如,把上述书号抄写成了0-387-11248-7.即是说,此码在传送过程中发生了2个错误:$8\to 4, 4\to 8$;但各位数之和却不变;简单的一致性检验失效.一个十分技巧的解决办法是加权求和,使得各位数字的状况在加权和中能反映出来.为此,把右起第一位数字乘以1,第二位数字乘以2,等等,再加起来,称为加权和.这样,上述错码就可检查出来了.然而还有一个问题.一致性检验是模n处理的;对书号问题而言似乎就应该是模10了.但经实践发现,哪怕只出一个错(某数字抄错),加权和也可能查不出来.例如:0-0000-1128-9加权和模10为0,错抄成0-0000-1123-9后加权和模10仍为0.其关键原因是:10不是素数,在模10剩余系中有两个非零元之积为0;如2与5非零但其乘积为0.因此我们取11作为模数.加权位这样确定:使得各位数加权和模11等于0.这带来一个小问题:模11剩余类10得用一个符号表示,在ISBN系统中用X表示它.例如有一本书的书号

是 ISBN 7-80091-125-X,其加权和是 231,模 11 等于 0,正确无误.

从数学的角度可得如下结论.

4.1.3 结论 设 p 是素数,以 $A=\{a_0,a_1,\cdots,a_{p-1}\}$ 为字母表,其中 a_i 为表示数字 i 的符号;设 $C\subseteq A^*$ 为一个定长 $n<p-1$ 的码.对于任一码字在其尾部加一检验位使其各位加权和模 p 为 0,得到长 $n+1$ 的码 $\tilde{C}$ 称为模 p 加权码.那么,如果一个码字出 1 个错或者出现一对邻位易位的错,都可检查出来.

以上介绍的码只能查出 1 个错,却不能判别错在何处,当然就不能纠正错误.

考虑 2 元码,字母表 $\{0,1\}$.如果有进一步办法找出错误的位置就能纠正它了,因为只要把错位变一下(0 变 1,1 变 0)即可.纠正 1 个错的码不难设计出来.比如,对定长 6 位的码,把每个码字的 6 位 * 排成 2×3 矩形:

$$\begin{array}{cccc} * & * & * & x \\ * & * & * & x \\ x & x & x & \end{array}$$

对每行加一个一致检验位 x,对每列加一个一致检验位 x,共加 5 个检验位,从而每个码字加长成 11 位:6 个信息位,5 个检验位.当一个码字至多出一个错时,则不仅可检错而且可纠错.这种码称为矩形码.

4.1.4 结论 $m\times n$ 矩形码有 mn 个信息位,$m+n$ 个检验位.按设计好的位置做 $m+n$ 次奇偶性(一致性)检验;如果 $m+n$ 次检验均是 0,无错;有一个 1,对应的检验位错而信息位均无错;有 2 个 1,则必是 1 个信息位出错,它的行列标号必分别对应于奇偶检验得出 1 的那两个检验位.

这种码虽然可以纠 1 个错,但在每个码字的 $mn+m+n$ 位中只有 mn 个信息位,如上述例子的 11 位中只有 6 个信息位,效率不高.

用类似的思想可设计出三角形码.如 6 个信息位的 2 元码,把信

息位 * 排成三角形：

```
*  *  *  x
*  *  x
*  x
x
```

其中4个x为奇偶(一致)检验位，使得每个x所在的行与列上的数字和为0.这样得到的码可以纠1个错，它的原理与矩形码的原理4.1.4几乎完全一样，比矩形码的巧妙之处只是在于它的每个检验位既是一个行号也是一个列号.这个例子中每个码字的10位中有6个信息位，比矩形码好，但仍然不理想.

把问题置于丰富的数学框架之中，就使得编码理论与技术的面貌焕然一新.

习题 4.1

1. 检查下列ISBN书号是否出错：

   ISBN 0-471-81078-X;

   ISBN 7-5062-0097-X;

   ISBN 7-5622-1412-3.

2. 证明结论4.1.2，结论4.1.3

3. 证明矩形码和三角码的原理4.1.4.

4. 设A是字母表.证明A^*是幺半群.(空串也是字即长度0的字称为空字，记作1.)

5. 如果C为字母表A上的一个码，则$\mathbf{1} \notin C$.

6. 设A是字母表，设$C \subset A^*$.如果C中任意字c的长度都是$l > 0$，则C为字母表A上的一个码(即定长码).

7. 设A是字母表，$a_0 \in A$.$C \subset A^*$.如果C中任意字c都以字母a_0结尾但a_0不出现在c的任何其他位置，则C为字母表A上的一个码(这就是拼音文字语言中的单词识别规则，a_0相当于空格.实

际语言中作为结尾的字母可以有很多,如还有各种标点符号).

8. 设 A 是字母表,$X \subset A^*$.如果 X 不是码,则存在字 $p, u \in X$ 使得 p 是 u 的真前缀(即有字母 $a_1, a_2, \cdots, a_k \in A, k > 0$,使得 $u = pa_1 \cdots a_k$),也存在字 $s \neq v \in X$ 使得 s 是 v 的真后缀(定义类似于真前缀)(注意:此结论的逆命题不成立,见下题).

9. 设字母表 $A = \{a, b\}$.证明:

(1) $X = \{a, ab, ba\}$ 不是码.

(2) $C = \{aa, ba, baa\}$ 是码.

10. 设字母表 $A = \{a\}, X \subset A^*$.证明:X 是码当且仅当 X 只含一个非空字.

§4.2 Hamming 距离

考虑2元码,字母表是 $A = \{0,1\}$.把 A 作为模2剩余系,那么在 A 上有两个运算:加法和乘法,而且构成一个域,即加、减、乘、除(除数不为0)都能做;而定长8的码的每个码字就是 A 上的一个8维向量.从这个简单的观察出发,引入如下定义.有关有限域的最简单常识包含在本节习题1中,基本知识将在 §5.3 中陈述.

4.2.1 定义 设 $\boldsymbol{F}$ 是含 q 个元的有限域,$\boldsymbol{F}^n = \{(x_1, x_2, \cdots, x_n) \mid x_i \in \boldsymbol{F}\}$ 是 $\boldsymbol{F}$ 上的 n- 数组构成的向量空间.$\boldsymbol{F}^n$ 的任一个非空子集 C 称为 $\boldsymbol{F}$ 上的一个 (n, M) 码,其中 $M = |C|$ 为 C 的基数,或称长 n 的 q 元码.进一步,若 C 是 $\boldsymbol{F}^n$ 的一个 k- 维子空间(从而 $M = q^k$),则称 C 是 $\boldsymbol{F}$ 上的一个 $[n, k]$ 线性码,其中 n 称为 C 的长度,而 k 称为 C 的维数.

$\boldsymbol{F}^n$ 的两个码 C 与 C' 称为等价,记作 $C \cong C'$,如果有一个 n 级置换矩阵 P 使得对于任意 $\boldsymbol{c} = (c_1, c_2, \cdots, c_n) \in C, \boldsymbol{c}P \in C'$ 且 $\boldsymbol{c} \mapsto \boldsymbol{c}P$ 给出 C 到 C' 的双射.

以下记 $\boldsymbol{0} = (0,0,\cdots,0), \boldsymbol{1} = (1,1,\cdots,1)$;零子空间称为零码.

注解:回想,向量空间 $\boldsymbol{F}^n$ 是一个加群连同一个"系数乘法".然而当 $\boldsymbol{F}=\boldsymbol{F}_2$ 时,$\boldsymbol{F}^n$ 的系数乘法被包括在加群结构之中,子空间就是子群,等等.换言之,$\boldsymbol{F}^n$ 仅仅就是一个群.所以有的文献把线性码称为群码.

一个简单的几何观念可帮我们的大忙.

4.2.2 定义 规定 $\boldsymbol{F}^n$ 上的二元非负整值函数 d 为:$d(\boldsymbol{x},\boldsymbol{y})=\left|\{i\mid 1\leqslant i\leqslant n, x_i\neq y_i\}\right|$,$\forall \boldsymbol{x}=(x_1,x_2,\cdots,x_n),\boldsymbol{y}=(y_1,y_2,\cdots,y_n)\in\boldsymbol{F}^n$;称 $d(\boldsymbol{x},\boldsymbol{y})$ 为 $\boldsymbol{x}$ 与 $\boldsymbol{y}$ 间的 Hamming 距离,简称距离.

规定 $\boldsymbol{F}^n$ 上的一元非负整值函数 w 为:$w(\boldsymbol{x})=d(\boldsymbol{x},\boldsymbol{0})$,$\forall \boldsymbol{x}\in\boldsymbol{F}^n$;称 $w(\boldsymbol{x})$ 为 $\boldsymbol{x}$ 的 Hamming 重量,简称重量,或称权.令 $\mathrm{Supp}(\boldsymbol{x})=\{i\mid 1\leqslant i\leqslant n, x_i\neq 0\}$,称 $\mathrm{Supp}(\boldsymbol{x})$ 为 $\boldsymbol{x}$ 的支撑指标集,则 $w(\boldsymbol{x})=|\mathrm{Supp}(\boldsymbol{x})|$.

显然 $d(\boldsymbol{x},\boldsymbol{y})=w(\boldsymbol{x}-\boldsymbol{y})$.

距离和重量的直观意义很清楚,如

$$d((0011),(1010))=2;\quad w(0111)=3.$$

从数学的角度来说,他们确实分别满足距离和重量的基本要求.

4.2.3 命题 (1) 对函数 d 下述两条成立:$\forall \boldsymbol{x},\boldsymbol{y},\boldsymbol{z}\in\boldsymbol{F}^n$,

$$d(\boldsymbol{x},\boldsymbol{y})\geqslant 0 \text{ 且仅在 } \boldsymbol{x}=\boldsymbol{y} \text{ 时有 } d(\boldsymbol{x},\boldsymbol{y})=0;$$

$$d(\boldsymbol{x},\boldsymbol{y})\leqslant d(\boldsymbol{x},\boldsymbol{z})+d(\boldsymbol{y},\boldsymbol{z}).$$

(2) 对函数 w 下述两条成立:$\forall \boldsymbol{x},\boldsymbol{y}\in\boldsymbol{F}^n$,

$$w(\boldsymbol{x})\geqslant 0 \text{ 且仅在 } \boldsymbol{x}=\boldsymbol{0} \text{ 时有 } w(\boldsymbol{x})=0;$$

$$w(\boldsymbol{x}+\boldsymbol{y})\leqslant w(\boldsymbol{x})+w(\boldsymbol{y}).$$

证明见本节习题 2. □

4.2.4 定义 设 $C\subseteq\boldsymbol{F}^n$ 是一个码.称 $d=d(C)=\min\{d(\boldsymbol{x},\boldsymbol{y})\mid \boldsymbol{x}\neq\boldsymbol{y}\in C\}$ 为 C 的极小距离;称 $\min\{w(\boldsymbol{x})\mid \boldsymbol{0}\neq\boldsymbol{x}\in C\}$ 为 C 的极小重量.此时,称 C 是 (n,M,d) 码,其中 $M=|C|$.进一步,若 C 是 k 维线性码,则说 C 是 $[n,k,d]$ 线性码.

4.2.5 命题 线性码的极小距离等于极小重量.

证明 由于 $d(x,y)=w(x-y)$,故

$$\min\{d(x,y)\mid x\neq y\in C\}=\min\{w(x-y)\mid x\neq y\in C\}$$
$$=\min\{w(x)\mid \mathbf{0}\neq x\in C\}\quad \square$$

4.2.6 定义 (1)(极大相似译码法(maximal likelihood decoding))设 C 为 $\boldsymbol{F}$ 上的码.把收到的字 r 译为与其距离最小的码字 $c\in C$;若有几个码字与 r 的距离都达到最小,则取其一,这称为极大相似译码法.数学描写如下.令 $L(r)=\{c\in C\mid d(r,c)\leqslant d(r,c')\,\forall\, c'\in C\}$;则显然 $L(r)\neq\varnothing$;把 r 译为 $c\in L(r)$.当 $|L(r)|=1$ 时,这个 c 是惟一的

(2) 发送码字 $c\in C$,收到字 $r\in \boldsymbol{F}^n$,如果在传送中发生错误不超过 k 位,即 $d(r,c)\leqslant k$ 时,极大相似译码法恒能把 r 惟一地译为 c,则称 C 是纠 k 错码.

类似地可定义检 k 错码.

4.2.7 命题 设 C 为 $\boldsymbol{F}$ 上的一个 (n,M,d) 码,设 $e=\left[\frac{d-1}{2}\right]$,这里 $[x]$ 表示实数 x 的整数部分.则 C 是纠 e- 错的码,是检 $(d-1)$- 错的码.

证明 设 $r\in \boldsymbol{F}^n$,$c\in C$ 使得 $d(r,c)\leqslant e$.对于任意 $c'\in C$,$c'\neq c$ 我们有

$$d(r,c')\geqslant d(c,c')-d(r,c)\geqslant d-e\geqslant d-\frac{d-1}{2}$$
$$=\frac{d+1}{2}>\left[\frac{d-1}{2}\right]=e.$$

所以 $L(r)=\{c\}$ 含惟一一个元 c,从而极大相似译码法把 r 惟一地译为 c.

另外易见,如果发生了错误但发生错误数小于 d,即 $0<d(r,c)<d$,则 $r\notin C$.接收者立即知道肯定出错. $\square$

4.2.8 注解 显然,纠 k- 错码也是纠 $(k-1)$- 错码,因此一个码有其最大纠错能力.有的文献说纠 k- 错码是指它的最大纠错能

力为纠 k 个错. 以上命题中的码的最大纠错能力就是纠 $e=\left[\frac{d-1}{2}\right]$ 个错. 因为：由极小距离的定义存在 $\boldsymbol{c}\neq\boldsymbol{c}'\in C$ 使得 $d(\boldsymbol{c},\boldsymbol{c}')=d$，即 $\boldsymbol{c}$ 与 $\boldsymbol{c}'$ 恰有 d 个坐标互不相同，不妨设

$$\boldsymbol{c}=(c_1,\cdots,c_d,c_{d+1},\cdots,c_n),\quad \boldsymbol{c}'=(c_1',\cdots,c_d',c_{d+1},\cdots,c_n),$$

其中 $c_i\neq c_i'$，$i=1,2,\cdots,d$；

令

$$\boldsymbol{r}=(c_1',\cdots,c_e',c_{e+1}',c_{e+2},\cdots,c_d,c_{d+1},\cdots,c_n);$$

则 $d(\boldsymbol{r},\boldsymbol{c})=e+1$；另一方面，由 $e+1>\frac{d-1}{2}$ 可得

$$d(\boldsymbol{r},\boldsymbol{c}')=d-(e+1)<d-\frac{d-1}{2}=\frac{d+1}{2}\leqslant e+1;$$

因此当码字 $\boldsymbol{c}$ 经传送被错为字 $\boldsymbol{r}$ 时，极大相似译码法不会把 $\boldsymbol{r}$ 译为 $\boldsymbol{c}$.

上述论证中的关键思想可用几何语言描述如下. 设 $\boldsymbol{c}\in\boldsymbol{F}^n$，$k$ 为非负整数，则点的集合 $S(\boldsymbol{c},k)=\{\boldsymbol{x}\in\boldsymbol{F}^n\mid d(\boldsymbol{c},\boldsymbol{x})\leqslant k\}$ 称为以 $\boldsymbol{c}$ 为球心以 k 为半径的球. 命题4.2.7的证明的关键点是对两个不同的码字 $\boldsymbol{c},\boldsymbol{c}'\in C$，球 $S(\boldsymbol{c},e)\cap S(\boldsymbol{c}',e)=\varnothing$，因为 $d(\boldsymbol{c},\boldsymbol{c}')\geqslant d>2e$：

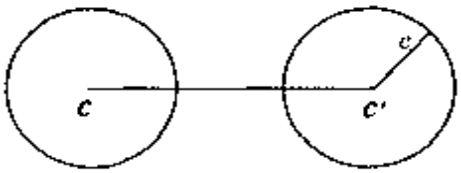


图 4-4

另一方面，当 $d(\boldsymbol{c},\boldsymbol{c}')=d$ 时，球 $S(\boldsymbol{c},e+1)\cap S(\boldsymbol{c}',e+1)\neq\varnothing$，因为 $(e+1)+(e+1)>d$.

实际上，容易确定球 $S(\boldsymbol{c},k)$. 设 $\boldsymbol{c}=(c_1,c_2,\cdots,c_n)\in\boldsymbol{F}^n$；对 $0\leqslant i\leqslant k$，任选定 i 个下标 $1\leqslant\alpha_1<\cdots<\alpha_i\leqslant n$；在字 $\boldsymbol{c}$ 中把 c_{α_1} 换为与 c_{α_1} 不同的任一元，把 c_{α_2} 换为与 c_{α_2} 不同的任一元，等

等,至 c_a 为止;其他坐标(位)不变;这样得到的字与 $\boldsymbol{c}$ 的距离恰好是 i.反之,任一个与 $\boldsymbol{c}$ 的距离为 i 的字都可如此得到.这样,让 i 从 0 跑到 k,就可得到球 $S(\boldsymbol{c},k)$ 的全部点.特别地,我们得到:$\boldsymbol{F}^n$ 中的半径 k 的球所含点的个数 $V_q(n,k)$ 是与球心无关而只与 n,k 有关的函数:

$$(4.2.9)\qquad \begin{aligned} V_q(n,k) &= |S(\boldsymbol{c},k)| \\ &= |\{\boldsymbol{x}\in \boldsymbol{F}^n \mid d(\boldsymbol{c},\boldsymbol{x})\leqslant k\}| \\ &= \sum_{i=0}^{k}\binom{n}{i}(q-1)^i. \end{aligned}$$

结合上述分析我们马上得到下述结果.

4.2.10 命题 设 $|\boldsymbol{F}|=q$,C 是 $\boldsymbol{F}$ 上的 (n,M,d) 码,其中 $M=|C|$ 令 $e=\left[\dfrac{d-1}{2}\right]$,则

$$M\cdot V_q(n,e)=|C|\cdot\sum_{i=0}^{e}\binom{n}{i}(q-1)^i\leqslant q^n. \qquad \square$$

此命题告诉我们 $M\leqslant q^n/V_q(n,e)$.由此引入下述概念.

4.2.11 定义 以 $M_q(n,d)$ 记极小距离 d 的长 n 的 q 元码能达到的最大的基数.则

$$M_q(n,d)\leqslant q^n/V_q(n,e),\quad \text{其中 } e=[(d-1)/2].$$

这称为码的 Hamming 界或球填充界.如果 $\boldsymbol{F}^n$ 上的 (n,M,d) 码 C 使得命题 4.2.10 中的等号成立,则称 C 为完全码.

因为对 $\boldsymbol{c}\neq\boldsymbol{c}'\in C$,球 $S(\boldsymbol{c},e)\cap S(\boldsymbol{c}',e)=\varnothing$,所以 $\bigcup\limits_{\boldsymbol{c}\in C}S(\boldsymbol{c},e)\subseteq\boldsymbol{F}^n$ 是用 M 个半径为 e 的球填充空间 $\boldsymbol{F}^n$.当命题 4.2.10 中的等号成立时,这是完全填充.显然,如果 C 是完全码,则 $d=2e+1$;这个条件并不是充分的(见本节习题 3).

与此相对的有球覆盖问题.无疑地,只要 ρ 足够大,以码字为球心以 ρ 为半径的所有球能覆盖空间 $\boldsymbol{F}^n$,即 $\bigcup\limits_{\boldsymbol{c}\in C}S(\boldsymbol{c},\rho)=\boldsymbol{F}^n$.下述概念与极小距离是对偶的.

4.2.12 定义 使 $\bigcup_{c\in C} S(c,\rho)=\boldsymbol{F}^n$ 成立的最小的 ρ 称为码 C 的覆盖半径(covering radius),记作 $\rho(C)$.

很容易给出 $M_q(n,d)$ 的另一个上界.

4.2.13 命题 $M_q(n,d)\leqslant q^{n-d+1}$. 这个界称为单字界(singleton bound). 如果 (n,M,d) 码 C 使得 $M=q^{n-d+1}$,则称 C 是极大距离可分码(maximal distance separate code),简称MDS码.

证明 对 d 归纳. 当 $d=1$ 时它显然成立. 设 $d>1$,那么存在下标 j 使得有两个码字它们的 j 位不相等;对每个 $c\in C$ 把 c 的 j 位删去得到一个长 $n-1$ 的字 $\tilde{c}\in \boldsymbol{F}^{n-1}$,因为 $d>1$,只要 $c\neq c'\in C$ 就有 $\tilde{c}\neq\widetilde{c'}\in \boldsymbol{F}^{n-1}$. 这样我们就得到一个 $(n-1,M,d-1)$ 码 $\widetilde{C}=\{\tilde{c}\mid c\in C\}$. 按归纳法,$M\leqslant q^{n-1-(d-1)+1}=q^{n-d+1}$. □

4.2.14 注解 这里的技巧是从长 n 的码 C 通过截去若干位构造新码,这样得到的码 $\widetilde{C}$ 称为截断码(punctured code)(与此相反的是扩张码(extended code),参看本节习题8).

这思想启发我们逐位考虑一个码的各个码字. 为此把 $\boldsymbol{F}$ 上的 (n,M,d) 码 C 的 M 个码字排成 M 行得到一个 $M\times n$ 矩阵

$$M(C)=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n}\\ c_{21} & c_{22} & \cdots & c_{2n}\\ \vdots & \vdots & & \vdots\\ c_{M1} & c_{M2} & \cdots & c_{Mn}\end{pmatrix}$$

称为码 C 的码矩阵. 按如下方式计算所有的互异码字对(共有 $M(M-1)/2$ 对)的距离的总和. 考虑各个码字的第 j 位,即考虑矩阵 $M(C)$ 的第 j 列. 对 $\lambda\in\boldsymbol{F}$,设 λ 在第 j 列出现 m_λ 次;那么 $\sum_{\lambda\in\boldsymbol{F}} m_\lambda=M$. 另一方面,若 $\lambda_1\neq\lambda_2\in\boldsymbol{F}$,而码字 c_1 的第 j 位是 λ_1,码字 c_2 的第 j 位是 λ_2,则在计算距离 $d(c_1,c_2)$ 时,第 j 位上的差别贡献了1. 这样,在计算所有的互异码字对的距离的总和时,第 j 位上的差异所作的贡献共有

$$\sum_{\lambda\neq\lambda\in F} m_\lambda m_\lambda = \frac{1}{2}\left(\left(\sum_{\lambda\in F} m_\lambda\right)^2 - \sum_{\lambda\in F} m_\lambda^2\right) = \frac{1}{2}\left(M^2 - \sum_{\lambda\in F} m_\lambda^2\right)$$

但是 $\sum_{\lambda\in F} m_\lambda^2 \geqslant \left(\sum_{\lambda\in F} m_\lambda\right)^2 \Big/ q = M^2/q$，所以距离总和为

$$\sum_{c\neq c\in C} d(c,c') = n\cdot \sum_{\lambda\neq\lambda\in F} m_\lambda m_\lambda = \frac{n}{2}\left(M^2 - \sum_{\lambda\in F} m_\lambda^2\right)$$

$$\leqslant \frac{n}{2}\left(M^2 - \frac{M^2}{q}\right) = \frac{n(q-1)M^2}{2q}$$

因此对平均距离我们有

$$\frac{2}{M(M-1)}\sum_{c\neq c\in C} d(c,c') \leqslant \frac{2}{M(M-1)}\cdot\frac{n(q-1)M^2}{2q}$$

$$= \frac{n(q-1)M}{q(M-1)}$$

极小距离 d 显然不超过平均距离.

4.2.15 命题 设 C 是 (n,M,d) 的 q 元码. 则

$$d \leqslant \frac{n(q-1)M}{q(M-1)}$$

这称为 Plotkin 界.

显然，要使上面的等号成立，至少极小距离 d 要等于平均距离；这种码具有以下特征.

4.2.16 定义 如果码 C 的任意两对码字的距离相等(从而任意一对码字的距离等于极小距离 d)，则 C 称为等距码(equidistant code).

习题 4.2

1. 设 F 是一个含 q 个元的有限域.

(1) 存在正整数 p 使得 $p\cdot 1_F = 0$；而且 p 是一个素数，它称为域 F 的特征，记作 $\mathrm{char}F$.

(2) F 的加群的每个非零元的阶都等于 $p = \mathrm{char}F$，即 F 的加群是初等交换群，特别是 $q = p^t$；

(3) $(\lambda+\mu)^{p^n}=\lambda^{p^n}+\mu^{p^n}$，　$\forall \lambda,\mu\in \boldsymbol{F}$.

(4) 子集$\{0,1_{\boldsymbol{F}},\cdots,(p-1)1_{\boldsymbol{F}}\}$是一个子域，它同构于$\mathbb{Z}_p$(模 p 剩余系)，称为 $\boldsymbol{F}$ 的素子域；它包含在 $\boldsymbol{F}$ 的任何子域之中.

(5) $\boldsymbol{F}$ 可以作为它的素子域上的向量空间；由此给出(2)的后一结论的另一证明.

2. (1) 证明命题 4.2.3.

(2) 证明：从命题 4.2.3(1) 的两个条件可推出 $d(\boldsymbol{x},\boldsymbol{y})=d(\boldsymbol{y},\boldsymbol{x})$ 对任意 $\boldsymbol{x},\boldsymbol{y}\in \boldsymbol{F}^n$.

3. 如果极小距离 d 的码 C 是完全码，则 $d=2e+1$. 反之不然.

4. 码 C 是完全码当且仅当$\rho(C)=\left[\dfrac{d(C)-1}{2}\right]$.

5. 设 C 是长 n 极小距离 7 的完全二元码. 证明 $n=7$ 或者 $n=23$.

6. 对 $\boldsymbol{x}\in \boldsymbol{F}_2^6$ 求 $|S(\boldsymbol{x},1)|$. 是否存在参数(6,9,3)(长 6 极小距离 3 含 9 个码字)的二元码?

7. 如果 $V_q(n,d-1)<q^{n-k+1}$，证明存在$[n,k,d]$-线性码.

8. 设 $C\subset \boldsymbol{F}^n$ 是一个(n,M,d)-码. 则码

$$\hat{C}=\left\{(c_1,c_2,\cdots,c_n,c_{n+1})\mid (c_1,c_2,\cdots,c_n)\in C,c_{n+1}\in \boldsymbol{F},\sum_{i=1}^{n+1}c_i=0\right\}$$

称为 C 的扩张码(准确地说是一种扩张码，可以有其他扩张方式)，求码 $\hat{C}$ 的参数.

9. 证明：存在参数$(n,M,2t+1)$的2元码当且仅当存在参数$(n+1,M,2t+2)$的 2 元码.

10. (Plotkin 界). 令 $\theta=1-q^{-1}$. 如果 $d>\theta n$，则 $M_q(n,d)\leqslant \dfrac{d}{d-\theta n}$.

11. 码 C 称为等重码(equiweight code)如果任意两个非零码

字的重量相等.证明:线性码 C 是等距码当且仅当 C 是等重码.

§4.3 线性码

恒设 F 是一个 q 元的有限域.回想定义 4.2.1,线性码是向量空间 F^n 的子空间.通常有两种决定子空间的方式.一是给出它的一个基底,二是把它作为一个线性方程组的解子空间.实际上这两种方式可以容易地互相转化.

回顾线性代数中的一个概念.在向量空间 F^n 上有典型对称双线性型$\langle -, - \rangle$:

(4.3.1) $$\langle x, y\rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n,$$

$$\forall\, x = (x_1, x_2, \cdots, x_n),\quad y = (y_1, y_2, \cdots, y_n) \in F^n;$$

它是非退化的,因为它在 F^n 的典型基底下的矩阵是单位矩阵.

4.3.2 定义 设 $C \subseteq F^n$ 是一个码,其正交子空间 $C^{\perp} = \{x \in F^n \mid \langle x, c\rangle = 0 \quad \forall\, c \in C\}$ 称为 C 的对偶码.

当 C 是线性码时即 C 是 F^n 的子空间时,对偶码 $C^{\perp}$ 也是线性码而且(见本节习题 1):

(4 3.3) $$\dim C + \dim C^{\perp} = n;\quad (C^{\perp})^{\perp} = C.$$

4.3.4 命题与定义 设 C 是 F^n 上的 $[n, k]$ 线性码.$C^{\perp}$ 是其对偶码.令 $k' = \dim C^{\perp} = n - k$.令 $x \in F^n$.

(1) 设 $g_1 = (g_{11}, g_{12}, \cdots, g_{1n}), \cdots, g_k = (g_{k1}, g_{k2}, \cdots, g_{kn})$ 是码 C 的一个基底,令矩阵 $G = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix}$.则 $x \in C$ 当且仅当 $x = aG$ 对某 $a = (a_1, a_2, \cdots, a_k) \in F^k$.称 G 为码 C 的生成矩阵(generating matrix).

(2) 设 $h_1 = (h_{11}, h_{12}, \cdots, h_{1n}), \cdots, h_{k'} = (h_{k'1}, h_{k'2}, \cdots, h_{k'n})$

是对偶码 $C^{\perp}$ 的一个基底，令矩阵 $H=\begin{pmatrix} h_{11} & \cdots & h_{1n} \\ \vdots & & \vdots \\ h_{k1} & \cdots & h_{kn} \end{pmatrix}$. 则 $\boldsymbol{x}\in C$ 当且仅当 $\boldsymbol{x}H^{\mathrm{T}}=0$，这里 H^{T} 表示 H 的转置矩阵. 称 H 为码 C 的检验矩阵(parity check matrix).

证明 结论(1)显然，因为 $\boldsymbol{x}\in C$ 当且仅当 $\boldsymbol{x}$ 是 $\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_k$ 的线性组合.

(2) 令 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$，则 $\boldsymbol{x}H^{\mathrm{T}}=0$ 是以 H 为系数矩阵的线性方程组. 由于 H 的行向量是 $C^{\perp}$ 的基底，此线性方程组的解子空间是 $(C^{\perp})^{\perp}=C$. □

注解：反之，由此命题的证明，任给一个域 $\boldsymbol{F}$ 上秩为 k 的 $k\times n$ 矩阵 C(或秩为 $n-k$ 的 $(n-k)\times n$ 矩阵 H)，有惟一线性码 C 以 G 为生成矩阵(以 H 为检验矩阵).

4.3.5 定理 设 H 是线性码 C 的检验矩阵，设 $H_1,H_2,\cdots,H_n$ 是 H 的全部列向量，则 C 的极小距离 $d(C)$ 等于 H 的列向量的极小线性相关组的基数的极小值，即

$d(C)=\min\{|I|\,|\,I\subseteq\{1,2,\cdots,n\}$，向量组 $H_i,i\in I$，线性相关$\}$.

证明 对于 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\boldsymbol{F}^n$，检验等式 $\boldsymbol{x}H^{\mathrm{T}}=0$ 即是

$$x_1H_1+x_2H_2+\cdots+x_nH_n=0.$$

令 $\mathrm{Supp}(\boldsymbol{x})=\{i\,|\,x_i\neq 0\}$. 若 $\boldsymbol{x}H^{\mathrm{T}}=0$，则向量组 $H_i,i\in\mathrm{Supp}(\boldsymbol{x})$ 线性相关. 反之，若向量组 $H_i,i\in I\subseteq\{1,2,\cdots,n\}$，是极小线性相关组，则存在 $x_i\in\boldsymbol{F},i\in I$，它们全不为零，使得 $\sum_{i\in I}x_iH_i=0$；令 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$，其中 $x_j=0$ 对 $j\notin I$，则 $\mathrm{Supp}(\boldsymbol{x})=I$，且 $\boldsymbol{x}H^{\mathrm{T}}=0$. □

4.3.6 注解 由此可知，线性码 C 可纠1个错当且仅当 $d(C)$

$\geqslant 3$，当且仅当 C 的检验矩阵 H 的任意 2 列线性无关.

而且有一种很简单的办法纠正错误，描述如下. 设 C 就是一个这样的线性码，它的检验矩阵 H 的任意 2 列线性无关. 把检验矩阵 H 按列分块 $H=(H_1,H_2,\cdots,H_n)$，即

$$H_j=\begin{pmatrix} h_{1j} \\ \vdots \\ h_{n-k,j} \end{pmatrix},\quad j=1,2,\cdots,n,$$

是 H 的各列向量. 设 $c\in C$ 传送时发生错误 $e\in F^n$（称为差错向量），即接收到的字为 $x=c+e$；并且设只在第 j 位发生一个错误，所以 $e=(0,\cdots,0,\lambda_j,0,\cdots,0)$. 因为 $cH^{\mathrm{T}}=0$，所以

$$xH^{\mathrm{T}}=(c+e)H^{\mathrm{T}}=eH^{\mathrm{T}}=\lambda_jH_j.$$

这个字被称为接收到的字 x 的和声（syndrome，有的文献称它为伴随式）. 上式表明和声一定是 H 的惟一一个列向量的倍数，j 就是这个列向量的列标号，而这个倍数系数就是 λ_j. 换言之，把接收到的字的和声计算出来就得到了差错向量 e，也就知道了发送码字 $c=x-e$.

从群论的同态基本定理或向量空间的同态基本定理，可以对此过程做一个更理论化的分析，为我们提供了一个极大相似译码法在线性码中的实施办法.

设 $C\subseteq F^n$ 为一个 $[n,k,d]$ 线性码，设 $H=(H_1,H_2,\cdots,H_n)$ 是它的检验矩阵. 则有线性映射 $\varphi:F^n\to F^{n-k}$，$x\mapsto xH^{\mathrm{T}}$；由命题 4.3.4(2)，φ 的核正好是 C，所以 φ 诱导从码 C 的全体陪集 $C+e$，$e\in F^n$，即商空间 F^n/C 到 F^{n-k} 的同构映射

$$\bar{\varphi}:F^n/C\xrightarrow{\cong}F^{n-k},\quad C+e\mapsto eH^{\mathrm{T}}.$$

因此我们有如下定义.

4.3.7 定义 称 $xH^{\mathrm{T}}\in F^{n-k}$ 为 $x\in F^n$ 的和声. 换言之，商空间 $\{C+x\mid x\in F^n\}$，其元素是陪集 $C+x$ 与和声的集合

$\{xH^{\mathrm{T}} \mid x \in F^n\}$ 之间一一对应；x_1 与 x_2 属于 C 的同一陪集当且仅当它们的和声相等 $x_1H^{\mathrm{T}} = x_2H^{\mathrm{T}}$. 发送码字 $c \in C$ 收到字 $r = c + e$，其中 e 就是差错向量，而 $e = r - c \in C + r$，它与收到字 r 属于 C 的同一陪集，也就具有同样的和声. 用极大相似译码法译码时考虑使得距离 $d(r, c_r)$ 最小的 c_r，也就是寻找使得重量 $w(e_r) = w(r - c_r) = d(r, c_r)$ 最小的 $w(e_r)$，这种 $e_r = r - c_r$ 在陪集 $C + r$ 之中，也就是在和声 rH^{T} 对应的陪集之中. 这样就把搜索 C 中使得 $d(r, c_r)$ 最小的字转换为搜索陪集 $C + r$ 中使得 $d(r, c_r)$ 最小的字. 总结上述我们得以下命题：

4.3.8 命题 符号如上. 假设收到字 r. 设 e_r 是和声 rH^{T} 对应的陪集

$$\{v \in F^n \mid vH^{\mathrm{T}} = rH^{\mathrm{T}}\} = C + r$$

中的重量最小的元，则极大相似译码法把 r 译为 $r - e_r$. 又若 $w(e_r) \leqslant e = \left[\frac{d-1}{2}\right]$，则 $C + r$ 中的重量最小的元是惟一的.

□

4.3.9 具体操作办法：

(1) 找出 C 的所有陪集，在每个陪集中找一个重量最小的字 e_i，称为该陪集的头字(leader).

(2) 编制译码表，即列出所有头字以及头字对应的和声.

(3) 收到字 r 后，计算和声 rH^{T}，在译码表的和声栏中找到此和声以及它对应的头字 e，把收到的字 r 译为 $r - e$.

看一个具体例子：

例 F_2(即模2剩余系)上的[5,2,3]线性码

$$C = \{(00000), (11100), (01111), (10011)\},$$

它的检验矩阵是 $H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$. 那么可得译码表如后. 按

照注解 4.3.6 中的分析，如果收到的字 r 至多出一个错，则和声 rH^{T} 只能是前 6 个之一：第 1 个表示无错；其他五个对应的头字恰含一个 1，所在位置恰好是和声在检验矩阵 H 中的列向量的列标号，即错误发生位置.

陪　　集	头字	和声
{(00000),(11100),(01111),(10011)}	(00000)	(000)
{(10000),(01100),(11111),(00011)}	(10000)	(100)
{(01000),(10100),(00111),(11011)}	(01000)	(110)
{(00100),(11000),(01011),(10111)}	(00100)	(010)
{(00010),(11110),(01101),(10001)}	(00010)	(101)
{(00001),(11101),(01110),(10010)}	(00001)	(001)
{(00110),(11010),(10001),(10101)}	(00110)	(111)
{(01010),(10110),(00101),(11001)}	(01010)	(011)

如何构造出满足注解 4.3.6 的“极大”的码？也就是：给定行数 s，如何构造出“极大”的矩阵 H？向量空间中两向量线性无关当且仅当它们不共线. 由此引入下述概念.

4.3.10 定义　设 V 是域 $\boldsymbol{F}$ 上的向量空间. 令 $\mathrm{PG}(V)=\{L \mid L$ 是 V 的 1 维子空间$\}$，称为对应 V 的投射空间(射影空间).

对 $0 \neq x \in V$，以 $\langle x\rangle$ 记向量 x 所在的 1 维子空间，即 $\langle x\rangle \in \mathrm{PG}(V)$. 此时我们说 x 代表 $\mathrm{PG}(V)$ 中的元素 $\langle x\rangle$. 但 $\mathrm{PG}(V)$ 中的一个元素可有不同的代表. 对于 $x \neq 0 \neq x'$，显然，$\langle x\rangle=\langle x'\rangle$ 当且仅当 x 与 x' 线性相关，即有 $a \in \boldsymbol{F}$ 使 $x'=ax$. 特别地，$|\langle x\rangle|=|\boldsymbol{F}|$.

4.3.11 命题　设 $|\boldsymbol{F}|=q$，设 s 是正整数.

(1) $|\mathrm{PG}(\boldsymbol{F}^s)|=(q^s-1)/(q-1)$.

(2) 行数为 s 的任意两列线性无关的矩阵最大列数 $n=\dfrac{q^s-1}{q-1}$，达到这个最大列数 n 的矩阵 H 的各列，恰好代表投射空间 $\mathrm{PG}(\boldsymbol{F}^s)$ 的所有元素.

证明见本节习题 8. □

4.3.12 定义　设 H 是命题 4.3.11(2) 中的矩阵. 以 H 为检验矩阵的码称为 Hamming 码.

4.3.13 命题　符号如上.

(1) Hamming 码的参数是 $\left[\frac{q^s-1}{q-1}, \frac{q^s-1}{q-1}-s, 3\right]$.

(2) Hamming 码是完全码.

证明见本节习题 9. □

4.3.14 例　以 $H=\begin{pmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{pmatrix}$ 为检验矩阵的二元线性码 C 是 Hamming 码, 它的参数是 $[7,4,3]$, 它的纠错能力为 1, 检错能力为 2.

4.3.15 注解　回到注解 4.3.6 的出发点, 考虑任意两列线性无关的 $k\times n$ 矩阵 G 而且秩为 k, 但考虑对偶的情况: 以 G 为生成矩阵得到的码称为投射码(projective code, 或译射影码). 按命题 4 3.11, 取定 k 时这种矩阵 G 的极大列数 $n=(q^k-1)/(q-1)$ 得到的码称为极大投射码(maximal projective code); 按定义知道它就是 Hamming 码的对偶码. 这种码具有很显著的特殊性质. 为了彻底理解它们, 在下一节我们先做一些准备. 这些准备在编码理论中是十分重要的.

习题 4.3

1. 设 F 是域, V 是 F 上的 n- 维向量空间; 设 $\langle x,y\rangle$ 是定义在 V 上的非退化的对称双线性型("非退化"是说若 $0\neq v\in V$ 则存在 $v'\in V$ 使 $\langle v,v'\rangle\neq 0$). 设 U 是 V 的子空间; 记 $U^{\perp}=\{v\in V\mid \langle u,v\rangle=0, \forall u\in U\}$. 称为 U 在 V 中的正交子空间. 证明:

(1) $\dim(U)+\dim(U^{\perp})=n$;

(2) $(U^{\perp})^{\perp}=U$.

2. 设二元域 F_2 上的一个线性码的生成矩阵是 $\begin{pmatrix}1101\\0111\end{pmatrix}$. 利用极大相似译码规则译 $r = 0110$,这个码是否可纠一个错?

3. 一个[6,3] 线性码是否可以纠 2 个错?为什么?

4. 求 4.3.9 后面例子中码的生成矩阵.

5. 设线性码 C 的参数是$[n,k]$,检验矩阵是 H. 证明 C 是极大距离可分码(见命题 4.2.13) 当且仅当 H 的任意 $n-k$ 列线性无关.

6. 设$|F| = q$,C 是 F 上的$[n,k]$ 码,其生成矩阵是 G. 则 $\sum_{c\in C} w(c) \leqslant n(q-1)q^{k-1}$;等号成立当且仅当 G 的任何列都不是零向量.

7. 完成命题 4.3.8 的全部证明.

8. 证明命题 4.3.11.

9. 证明命题 4.3.13.

10. 设 C 是 q 元有限域 F 上的$[n,k,3]$ 线性码. 则以下条件等价:

(1) C 是 Hamming 码;

(2) $n = (q^{n-k}-1)/(q-1)$;

(3) C 是完全码.

11. 编制例 4.3.14 的 Hamming 码的和声译码法的译码表.

12. 设 C 是 F_2 上的$[n,k]$ 码. 如果 C 有一个码字的重量是奇数,则 C 中所有重量为偶数的码字构成一个$[n,k-1]$ 码.

13. 证明极大投射 q 元码的参数是$\left[\frac{q^k-1}{q-1}, k, q^{k-1}\right]$.

§4.4 有限交换群的 Fourier 变换

本节始终设 X 是阶为 n 的有限交换群,但运算写作乘法"$\cdot$";而$\mathbb{C}^*$是复数域的乘群. 设 χ 和 ψ 都是从 X 到$\mathbb{C}^*$的函数,则可定义函

数乘法如下

$$(\chi\psi)(a) = \chi(a)\psi(a), \quad \forall a \in X,$$

这当然还是从 X 到$\mathbb{C}^*$的函数;这个运算显然满足交换律.进一步,如果 χ 和 ψ 都是群同态,则易验证 $\chi\psi$ 也是群同态

$$\begin{aligned}(\chi\psi)(aa') &= \chi(aa')\psi(aa') = \chi(a)\chi(a')\psi(a)\psi(a') \\ &= \chi(a)\psi(a)\chi(a')\psi(a') = (\chi\psi)(a)(\chi\psi)(a')\end{aligned}$$

而且常值函数 $1: X \to \mathbb{C}^*, a \mapsto 1$,显然满足 $1\chi = \chi$.又对函数 χ: $X \to \mathbb{C}^*$,令 $\chi^{-1}: X \to \mathbb{C}^*$为函数 $\chi^{-1}(a) = (\chi(a))^{-1}$.则当 χ 是群同态时,χ^{-1} 也是群同态

$$\begin{aligned}\chi^{-1}(aa') &= (\chi(aa'))^{-1} = (\chi(a)\chi(a'))^{-1} \\ &= (\chi(a))^{-1}(\chi(a'))^{-1} = \chi^{-1}(a)\chi^{-1}(a').\end{aligned}$$

常值函数 $1: X \to \mathbb{C}^*$显然是群同态,也就是一个线性特征标,称为单位特征标(unity character),或称为主特征标(principal character).这样我们可给出以下定义.

4.4.1 定义　从有限交换群 X 到复数域乘群$\mathbb{C}^*$的任一群同态称为 X 的一个线性复特征标(character),简称线性特征标.X 的所有线性特征标的集合,记作 X^*,在函数乘法之下是一个交换群,称为 X 的对偶群(dual group).

4.4.2 注解　显然对于任意域 $\boldsymbol{F}$ 所有的定义都一样给出:任一群同态 $\chi: X \to \boldsymbol{F}^*$ 称为 X 的一个 $\boldsymbol{F}$- 线性特征标,所有 $\boldsymbol{F}$- 线性特征标的集合在函数乘法之下构成一个群,等等.但下面要做的事不是对于任意的域都成立,只是在一定条件下成立;见本节习题 9 和习题 10

实际上,$X^* \cong X$;但是我们将给出比这多得多的信息.以下将遵循习题1.3.13 和习题1.5.12 的思路给出 X 的全部线性特征标.

4.4.3 引理　设 $C = \langle a \rangle$ 是 m 阶循环群,设 ω 是 m 次本原单位根.

(1) 对于任意线性特征标 $\psi: C \to \mathbb{C}^*$,存在整数 k 使得 $\psi(a)$

$=\omega^k$ 而 $\psi(a^t)=\omega^{kt}$，而且整数 k 在 mod m 时是惟一的.

(2) $\mathbb{C}^*=\{\chi^{(k)}\mid k=0,1,\cdots,m-1\}$ 其中 $\chi^{(k)}(a)=\omega^k$，而且 $\mathbb{Z}_m\to\mathbb{C}^*$，$k\mapsto\chi^{(k)}$ 是群同构；从而 $C\to\mathbb{C}^*$，$a^k\mapsto\chi^{(k)}$ 是群同构；特别是 $\mathbb{C}^*=\langle\chi\rangle$，其中 $\chi=\chi^{(1)}$ 而 $\chi^{(k)}=\chi^k$.

证明 因为 $\psi(a)^m=\psi(a^m)=\psi(1)=1$，所以 $\psi(a)$ 是一个 m 次单位根. 因此引理所说的 k 存在而且 mod m 惟一. 令 k 对应特征标 $\chi^{(k)}$ 使得 $\chi^{(k)}(a)=\omega^k$. 这样确定的线性特征标恰与 $\mathbb{Z}_m$ 的元素一一对应. 而且

$$(\chi^{(k)}\chi^{(k')})(a)=\chi^{(k)}(a)\chi^{(k')}(a)=\omega^k\omega^{k'}=\omega^{k+k'}=\chi^{(k+k')}(a)$$

即 $k\mapsto\chi^{(k)}$ 是从 $\mathbb{Z}_m$ 到 $\mathbb{C}^*$ 的同构. 最后，$\mathbb{Z}_m\to C$，$k\mapsto a^k$ 是群同构，所以 $C\to\mathbb{C}^*$，$a^k\mapsto\chi^{(k)}$ 是群同构. □

再利用定理 1.5.9 把任意有限交换群 X 写成循环群的直积，引用上述引理就可以把 X 的对偶群 X^* 弄清楚了.

由此我们得到以下定理：

4.4.4 定理 设 n 阶有限交换群 $X=C_1\times C_2\times\cdots\times C_r$，其中 $C_i=\langle a_i\rangle$ 是 n_i 阶循环群，$|a_i|=n_i$（从而 $n_1n_2\cdots n_r=n$）. 对于每个 $1\leqslant i\leqslant r$ 设 $\omega_i\in\mathbb{C}^*$ 是一个本原的 n_i 次单位根，令 $\chi_i\in\mathbb{C}_i^*$，使得 $\chi_i(a_i)=\omega_i$，则

$$\begin{aligned}X^*&=\mathbb{C}_1^*\times\mathbb{C}_2^*\times\cdots\times\mathbb{C}_r^*\\&=\{\chi_1^{k_1}\times\chi_2^{k_2}\times\cdots\times\chi_r^{k_r}\mid\text{每}\,0\leqslant k_i<n_i\}\cong X,\end{aligned}$$

其中 $(\chi_1^{k_1}\times\chi_2^{k_2}\times\cdots\times\chi_r^{k_r})(a_1^{t_1}a_2^{t_2}\cdots a_r^{t_r})=\omega_1^{k_1t_1}\omega_2^{k_2t_2}\cdots\omega_r^{k_rt_r}$.

证明 对于任意线性特征标 $\chi\in X^*$，限制 χ 到 C_i 就应是 C_i 的一个线性特征标，按引理4.4.3 存在 $0\leqslant k_i<n_i$ 使得 $\chi|_{C_i}=\chi_i^{k_i}$，其中 $\chi_i^{k_i}(a_i)=\omega_i^{k_i}$. 对于任意 $a\in X$，有惟一分解 $a=a_1^{t_1}a_2^{t_2}\cdots a_r^{t_r}$；因为 χ 是同态，所以

$$\begin{aligned}\chi(a) &= \chi(a_1^{t_1}a_2^{t_2}\cdots a_r^{t_r}) = \chi(a_1^{t_1})\chi(a_2^{t_2})\cdots\chi(a_r^{t_r})\\ &= \chi_1^{k_1}(a_1^{t_1})\chi_2^{k_2}(a_2^{t_2})\cdots\chi_r^{k_r}(a_r^{t_r})\\ &= \omega_1^{k_1t_1}\omega_2^{k_2t_2}\cdots\omega_r^{k_rt_r}.\end{aligned} \tag{4.4.4.1}$$

这样就给出了映射

$$\begin{aligned}&X^* \to \mathbb{C}_1^*\times\mathbb{C}_2^*\times\cdots\times\mathbb{C}_r^*\\ &\chi \mapsto (\chi|_{C_1},\chi|_{C_2},\cdots,\chi|_{C_r}) = (\chi_1^{k_1},\chi_2^{k_2},\cdots,\chi_r^{k_r})\end{aligned} \tag{4.4.4.2}$$

这显然是同态映射.反之,对于任意$(\chi_1^{k_1},\chi_2^{k_2},\cdots,\chi_r^{k_r})\in\mathbb{C}_1^*\times\mathbb{C}_2^*\times\cdots\times\mathbb{C}_r^*$,由式(4.4.4.1)可以定义一个$\chi:X\to\mathbb{C}^*$,容易证明它是一个线性特征标.所以(4.4.4.2)是同构.

最后,由引理4.4.3,$C_i^*\cong C_i$;故$\mathbb{C}_1^*\times\mathbb{C}_2^*\times\cdots\times\mathbb{C}_r^*\cong C_1\times C_2\times\cdots\times C_r\cong X$. □

4.4.5 定理(特征标正交关系) 对于任意$\chi,\psi\in X^*$有

$$\sum_{a\in X}\chi(a)\psi(a^{-1}) = \begin{cases}|X|, & \text{若 } \chi=\psi;\\ 0, & \text{若 } \chi\neq\psi.\end{cases}$$

证明 由定理4.4.4可以设

$$\chi = \chi_1^{k_1}\times\chi_2^{k_2}\times\cdots\times\chi_r^{k_r},$$
$$\psi = \chi_1^{k_1'}\times\chi_2^{k_2'}\times\cdots\times\chi_r^{k_r'};$$

注意,$\chi=\psi$当且仅当$k_i=k_i'$对所有$i=1,2,\cdots,r$.再设$a=a_1^{t_1}\cdot a_2^{t_2}\cdots a_r^{t_r}$,在$t_i$分别跑遍$0,1,\cdots,n_i-1$时,$a$就跑遍$X$.所以

$$\begin{aligned}&\sum_{a\in X}\chi(a)\psi(a^{-1})\\ &= \sum_{0\leqslant t_1<n_1}\cdots\sum_{0\leqslant t_r<n_r}(\chi_1^{k_1}(a_1^{t_1})\chi_2^{k_2}(a_2^{t_2})\cdots\chi_r^{k_r}(a_r^{t_r}))\\ &\qquad(\chi_1^{k_1'}(a_1^{-t_1})\chi_2^{k_2'}(a_2^{-t_2})\cdots\chi_r^{k_r'}(a_r^{-t_r}))\\ &= \sum_{0\leqslant t_1<n_1}\cdots\sum_{0\leqslant t_r<n_r}(\omega_1^{k_1t_1}\omega_2^{k_2t_2}\cdots\omega_r^{k_rt_r})(\omega_1^{-k_1't_1}\omega_2^{-k_2't_2}\cdots\omega_r^{-k_r't_r})\\ &= \sum_{0\leqslant t_1<n_1}\cdots\sum_{0\leqslant t_r<n_r}\omega_1^{(k_1-k_1')t_1}\omega_2^{(k_2-k_2')t_2}\cdots\omega_r^{(k_r-k_r')t_r}\end{aligned}$$

$$= \prod_{i=1}^{r} (1 + \omega_i^{k_i - k_i'} + \cdots + (\omega_i^{k_i - k_i'})^{n_i - 1}).$$

对于任一 ω_i，如果 $k_i - k_i' \neq 0$，则 $\omega_i^{k_i - k_i'} \neq 1$ 是一个 n_i 次单位根，那么

$$1 + \omega_i^{k_i - k_i'} + \cdots + (\omega_i^{k_i - k_i'})^{n_i - 1} = \frac{1 - (\omega_i^{k_i - k_i'})^{n_i}}{1 - \omega_i^{k_i - k_i'}} = 0.$$

所以只要 $\chi \neq \psi$ 就有 $1 \leqslant i \leqslant r$ 使得 $k_i \neq k_i'$，就有 $\sum_{a \in X} \chi(a)\psi(a^{-1}) = 0$. 不然对于所有 $i = 1, 2, \cdots, r$ 都有 $k_i = k_i'$，故

$$1 + \omega_i^{k_i - k_i} + \cdots + (\omega_i^{k_i - k_i})^{n_i - 1} = n_i$$

从而

$$\sum_{a \in X} \chi(a)\psi(a^{-1}) = \prod_{i=1}^{r} n_i = n = |X|. \qquad \square$$

换一个角度来考虑对偶问题. 类似于线性代数中的双线性函数(或称双线性型)，我们引入下述概念.

4.4.6 定义 定义在有限交换群 X 上的复值二元函数

$$X \times X \to \mathbb{C}^*, (a, b) \mapsto (a|b); \quad (\text{把}(a, b)\text{ 的像记作}(a|b).)$$

称为 X 的双同态复函数(bihomomorphic complex function) 如果

$$(aa'|b) = (a|b)(a'|b), \quad \forall a, a', b \in X,$$
$$(a|bb') = (a|b)(a|b'), \quad \forall a, b, b' \in X.$$

进一步，X 的一个双同态复函数 $(a|b)$ 称为对称的(symmetric) 如果 $(a|b) = (b|a)$ 对于任意 $a, b \in X$；双同态复函数 $(a|b)$ 称为非退化的(non-degenerate) 如果对于任意 $1 \neq a \in X$ 存在 $b \in X$ 使得 $(a|b) \neq 1$.

4.4.7 注解 双同态复函数 $(-|-)$ 的意义在于，任意 $a \in X$ 给出了 X 到 $\mathbb{C}^*$ 的一个群同态

(4.4.7.1) $$a^* = (a|-): X \to \mathbb{C}^*, x \mapsto a^*(x) = (a|x),$$

也就是给出了一个线性特征标 $a^* \in X^*$，而且

(4.4.7.2) $$X \to X^*, \ a \mapsto a^*$$

是群同态;进一步,如果双同态复函数$(-\mid -)$是非退化的,则这是群同构.所以,只要X有了一个非退化的双同态复函数,就可以把X自己等同于其对偶群X^*.

4.4.8 引理 任何有限交换群X上的非退化的对称的双同态复函数存在.

证明 仍用定理4.4.4中的记号,对于任意

$$a = a_1^{t_1} a_2^{t_2} \cdots a_r^{t_r} \in X,$$

$$b = a_1^{s_1} a_2^{s_2} \cdots a_r^{s_r} \in X,$$

令

$$(a \mid b) = \omega_1^{t_1 s_1} \omega_2^{t_2 s_2} \cdots \omega_r^{t_r s_r}$$

则易验证这是一个非退化的对称的双同态复函数. □

以下始终假设X是有限交换群,以$\mathbb{C}^X$记所有从X到$\mathbb{C}$的函数的集合.设$(-\mid -)$是X上的一个非退化的双同态复函数.

4.4.9 定理 对于任意$a, b \in X$有

$$\sum_{x \in X} (a \mid x)(b \mid x^{-1}) = \begin{cases} \mid X \mid, & \text{若 } a = b; \\ 0, & \text{若 } a \neq b. \end{cases}$$

证明 由注解4.4.7知作为复函数$(a \mid -) \in X^*$和$(b \mid -) \in X^*$,而且因为双同态复函数$(-\mid -)$是非退化的,这两个特征标只在$a = b$时是相等的,所以这就是特征标的正交关系4.4.5. □

4.4.10 注解 由本节习题1知道$(b \mid x^{-1}) = (b \mid x)^{-1} = (b^{-1} \mid x)$,从而$(a \mid x)(b \mid x^{-1}) = (ab^{-1} \mid x)$;所以定理4.4.9也可叙述为

$$(4.4.10.1) \quad \sum_{x \in X} (ab^{-1} \mid x) = \begin{cases} \mid X \mid, & \text{若 } a = b; \\ 0, & \text{若 } a \neq b. \end{cases}$$

这就是本节习题2.又,因为$(- \mid x)$也可看做X的线性特征标而且

$$X \to X^*, \ x \mapsto (\cdot \mid x)$$

也是同构,见本节习题8,那么定理4.4.9还可叙述为

$$(4.4.10.2)\qquad \sum_{x\in X}(a|x)(b^{-1}|x)=\begin{cases}|X|, & \text{若 } a=b;\\ 0, & \text{若 } a\neq b.\end{cases}$$

这就是本节习题 3 的第二正交关系.

4.4.11 定义 对于任意 $f\in\mathbb{C}^X$(即 f 是 X 上的复值函数)构作 X 上的两个复值函数 Φf 和 Ψf 如下:对于任意 $a\in X$,令

$$\Phi f(a)=\sum_{x\in X}f(x)(x|a),$$

$$\Psi f(a)=\frac{1}{|X|}\sum_{x\in X}f(x)(a|x^{-1}).$$

那么得到$\mathbb{C}^X$的两个变换

$$\Phi:\mathbb{C}^X\to\mathbb{C}^X,\ f\mapsto\Phi f;$$

$$\Psi:\mathbb{C}^X\to\mathbb{C}^X,\ f\mapsto\Psi f;$$

分别称为交换群 X 上复值函数的 Fourier 变换和 Fourier 逆变换.

4.4.12 命题 对于任意 $f\in\mathbb{C}^X$有 $\Psi\Phi f=f$ 和 $\Phi\Psi f=f$.

证明 对于任意 $a\in X$

$$\begin{aligned}\Psi\Phi f(a)&=\frac{1}{|X|}\sum_{x\in X}\Phi f(x)(a|x^{-1})\\&=\frac{1}{|X|}\sum_{x\in X}\sum_{y\in X}f(y)(y|x)(a|x^{-1})\\&=\frac{1}{|X|}\sum_{y\in X}f(y)\sum_{x\in X}(y|x)(a|x^{-1})\end{aligned}$$

但是由定理 4.4.9

$$\sum_{x\in X}(y|x)(a|x^{-1})=\begin{cases}|X|, & \text{若 } y=a;\\ 0, & \text{若 } y\neq a.\end{cases}$$

所以 $\Psi\Phi f(a)=f(a)$,故得 $\Psi\Phi f=f$.

类似可证 $\Phi\Psi f=f$. □

下一节我们将把这些知识用到编码上.

习题 4.4

1. 设 χ 是有限交换群 X 的非单位线性特征标,$a\in X$.证明:

$\overline{\chi(a)} = \chi(a)^{-1} = \chi(a^{-1})$，其中$\overline{\chi(a)}$为复数$\chi(a)$的复共轭.

2. 设χ是有限交换群X的线性特征标.证明

$$\sum_{a\in X}\chi(a) = \begin{cases} |X|, & \text{若 } \chi = 1; \\ 0, & \text{若 } \chi \neq 1. \end{cases}$$

3. (第二正交关系) 设X是有限交换群，X^*是对偶群.a，$b \in X$.则

$$\sum_{a^*\in X^*} a^*(a)a^*(b^{-1}) = \begin{cases} |X|, & \text{若 } a = b; \\ 0, & \text{若 } a \neq b. \end{cases}$$

4. 设X, Y是有限交换群.设$W \leqslant X$，令

$W_* = \{a^* \in X^* \mid a^*(w) = 1, \forall w \in W\}$，则：

(1) $(X \times Y)^* \cong X^* \times Y^*$.

(2) $(X/W)^* \cong W_*$.

(3) $W^* \cong X^*/W_*$.

5. 设$(-|-)$是有限交换群X上的双同态复函数.则对于任意$b \in X$有$(1|b) = 1$.

6. 证明注解4.4.7的两个结论.

7. 完成引理4.4.8的证明细节.

8. 设$(-|-)$是有限交换群X上的双同态复函数.如果对于任意$1 \neq a \in X$，存在$b \in X$使得$(a|b) \neq 1$，那么对于任意$1 \neq b \in X$，存在$a \in X$使得$(a|b) \neq 1$(即：如果双同态复函数$(-|-)$是左非退化的则也是右非退化的).

9. 设X是一个n阶有限交换群，设域F含有一个n次本原单位根ω.证明本节的所有结论对F-线性特征标都成立.

10. 设C是一个循环p-群，这里p是一个素数；设F是一个特征为p的有限域.证明：只有一个群同态$C \to F^*$.由此说明C与它的所有F-线性特征标构成的乘群不同构.

11. 设m是正整数，假设复函数$\chi: \mathbb{Z} \to \mathbb{C}$满足以下三条：

(1) $\chi(a) = \chi(b)$对于任意$a \equiv b \pmod{m}$；

(2) $\chi(ab) = \chi(a)\chi(b)$;

(3) $\chi(a) = 0$ 对于任意 $(a, m) \neq 1$.

证明: $\sum_{a=0}^{m-1} \chi(a) = 0$. (这种$\mathbb{Z}$上的复函数 χ 称为一个模 m 的 Dirichlet 特征标.)

§4.5 一般对偶码 MacWilliams 恒等式

如同 §4.3 恒设 $\boldsymbol{F}$ 是一个 q 元的有限域. 但这次我们先考虑一般的码, 即 $\boldsymbol{F}^n$ 的任意子集 C. 令 $X = \boldsymbol{F}^n$, 把它看做一个加群就可以应用上一节的思想, 只是注意这里 X 的运算是加法"+". 首先我们来确定一个 X 上的非退化的对称的双同态复函数 $(-\,|\,-)$.

在 §4.3 中已提到, 在向量空间 $\boldsymbol{F}^n$ 上有典型对称双线性型 $\langle -, - \rangle$

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n,$$

$$\forall\, \boldsymbol{x} = (x_1, x_2, \cdots, x_n),\ \boldsymbol{y} = (y_1, y_2, \cdots, y_n) \in \boldsymbol{F}^n;$$

它是非退化的, 因为它在 $\boldsymbol{F}^n$ 的典型基底下的矩阵是单位矩阵. 再把 $\boldsymbol{F}$ 作为加群取一个非单位的线性特征标 $\theta: \boldsymbol{F} \to \mathbb{C}^*$. 这样就得到一个二元函数

$$(4.5.1) \quad X \times X: \to \mathbb{C}^*,\ (\boldsymbol{x}, \boldsymbol{y}) \mapsto \theta\langle \boldsymbol{x}, \boldsymbol{y} \rangle \quad \left(= \prod_{i=1}^{n} \theta(x_i y_i) \right)$$

4.5.2 引理 $X = \boldsymbol{F}^n$ 上的二元复值函数 $\theta\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ 是非退化的对称的双同态复函数.

证明 对于任意 $\boldsymbol{x}, \boldsymbol{x}', \boldsymbol{y} \in X$, 由典型内积 $\langle -, - \rangle$ 的双线性可得

$$\theta\langle \boldsymbol{x} + \boldsymbol{x}', \boldsymbol{y} \rangle = \theta(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{x}', \boldsymbol{y} \rangle) = \theta\langle \boldsymbol{x}, \boldsymbol{y} \rangle \cdot \theta\langle \boldsymbol{x}', \boldsymbol{y} \rangle.$$

同样可计算

$$\theta\langle \boldsymbol{x}, \boldsymbol{y} + \boldsymbol{y}' \rangle = \theta(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{x}, \boldsymbol{y}' \rangle) = \theta\langle \boldsymbol{x}, \boldsymbol{y} \rangle \cdot \theta\langle \boldsymbol{x}, \boldsymbol{y}' \rangle.$$

又因典型内积 $\langle -, - \rangle$ 是对称的, 易知 $\theta\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ 也是对称的. 最后设

$0 \neq x \in X$,由典型内积$\langle -, - \rangle$的非退化性,x 诱导非零的线性函数 $X = \boldsymbol{F}^n \to \boldsymbol{F}, y \mapsto \langle x, y \rangle$;特别地,这是满射.另一方面,$\theta: \boldsymbol{F} \to \mathbb{C}^*$ 是非单位特征标,故有 $\lambda \in \boldsymbol{F}$ 使得 $\theta(\lambda) \neq 1$. 令 $y \in X$ 满足 $\langle x, y \rangle = \lambda$; 则 $\theta\langle x, y \rangle = \theta(\lambda) \neq 1$. □

以下对 $X = \boldsymbol{F}^n$ 我们总是用(4.5.1)这个非退化的对称的双同态复函数 $\theta\langle x, y \rangle$.因为典型双线性型$\langle -, - \rangle$限制到任何子空间也是双线性型,我们有以下引理:

4.5.3 引理(正交关系)　如果 Y 是 X 的子空间,则

$$\sum_{y \in Y} \theta\langle x, y \rangle \theta\langle x', y \rangle = \begin{cases} |Y|, & \text{若 } x + x' \in Y^{\perp}; \\ 0, & \text{否则.} \end{cases}$$

特别是,该公式对 $Y = X(= \boldsymbol{F}^n)$ 成立.

证明之前作两个注解:

注解:(1) 因为 $\theta\langle -, - \rangle$ 是双同态函数,所以 $\theta\langle x, y \rangle \theta\langle x', y \rangle = \theta\langle x + x', y \rangle$;等价地,上述公式还可写成

$$(4.5.3') \qquad \sum_{y \in Y} \theta\langle x + x', y \rangle = \begin{cases} |Y|, & \text{若 } x + x' \in Y^{\perp}; \\ 0, & \text{否则.} \end{cases}$$

注解:(2) 该公式对 $Y = X(= \boldsymbol{F}^n)$ 当然也成立;写出来就是一个前面已提到的形式

$$\sum_{y \in X} \theta\langle x, y \rangle = \begin{cases} |X|, & \text{若 } x = 0; \\ 0, & \text{否则.} \end{cases}$$

证明　因为对 $x, x' \in \boldsymbol{F}^n$,如果 $x + x' \notin Y^{\perp}$,那么 $\theta\langle x + x', - \rangle$ 就诱导 Y 的一个非单位的线性特征标 $Y \to \mathbb{C}^*$.所以本引理就是有限交换群 Y 上的特征标的正交关系. □

特别是,我们有了 Fourier 变换

$$\Phi: \mathbb{C}^X \to \mathbb{C}^X, \quad f \mapsto \Phi f;$$

$$\Phi f(x) = \sum_{t \in X} f(t) \theta\langle t, x \rangle, \quad \forall f \in \mathbb{C}^X \text{和 } \forall x \in X(= \boldsymbol{F}^n).$$

而且对于任意 $a \in X$ 由正交关系 4.5.3 有

$$\Phi^2 f(a) = \sum_{x\in X}\Big(\sum_{y\in X} f(y)\theta\langle y,x\rangle\Big)\theta\langle x,a\rangle$$
$$= \sum_{y\in X} f(y)\sum_{x\in X}\theta\langle y,x\rangle\theta\langle x,a\rangle = |X|\cdot f(-a)$$

即是

(4.5.4) $$\Phi^2 f(a) = |X|\cdot f(-a),\quad \forall a\in X.$$

又,对于任意 $f\in \mathbb{C}^X$ 令 $|f| = \sum_{x\in X} f(x)$. 因为对于任意 $x\in X$ 有 $\theta\langle x,0\rangle = \theta(0) = 1$,故有 $\sum_{x\in X} f(x) = \sum_{x\in X} f(x)\cdot\theta\langle x,0\rangle$,即

(4.5.5) $$|f| = \sum_{x\in X} f(x) = \Phi f(0).$$

注意到 X 的任何码 C,也就是任何子集 $C\subset X$,可以用所谓特征函数(characteristic function)来刻画

(4.5.6) $$\chi_C(x) = \begin{cases}1, & \text{若 } x\in C;\\ 0, & \text{否则}\end{cases}\quad \text{和}\ |C| = |\chi_C|.$$

4.5.7命题 符号如上. 如果 C 是线性码,则 $\chi_{C^\perp} = \frac{1}{|C|}\Phi\chi_C$ 是 $C^\perp$ 的特征函数.

证明 对于任意 $x\in X = F^n$ 我们有

$$\frac{1}{|C|}\Phi\chi_C(x) = \frac{1}{|C|}\sum_{y\in F^n}\chi_C(y)\theta\langle y,x\rangle$$
$$= \frac{1}{|C|}\sum_{y\in C}\chi_C(y)\theta\langle y,x\rangle$$
$$= \begin{cases}1, & \text{若 } x\in C^\perp;\\ 0, & \text{否则}.\end{cases}$$

因为我们可以把 X 的子集看做一个 X 上的函数,一般地,我们就把任意一个函数 $f\in\mathbb{C}^X$ 看做 X 的一个"形式子集",它以 f 为特征函数.因此引入以下定义:

4.5.8定义 对于任意码 $C\subset F^n$,我们把以 $\frac{1}{|C|}\Phi\chi_C$ 为特征函数的形式子集 C^* 称为码 C 的形式对偶码(formal dual code),即

$\chi_{C^\cdot} = \frac{1}{|C|}\Phi\chi_C$；并且我们记$|C^\cdot| = |\chi_{C^\cdot}|$.

由于技术上的原因，以下我们总假设：

4.5.9 假设　$\mathbf{0} \in C$(容易验证 $\chi_{C^\cdot}(\mathbf{0}) = 1$).

这个假设无碍大局，因为如果 $\mathbf{0} \notin C$，我们可以取 $\boldsymbol{c}_0 \in C$，再把 C 换为$\{\boldsymbol{c} - \boldsymbol{c}_0 \mid \boldsymbol{c} \in C\}$，这后一个子集的距离结构与 C 完全是一样的.

4.5.10 命题　设 $C \subset X = \boldsymbol{F}^n$ 是一个码.

(1) $C^\cdot = C^\perp$ 如果 C 是线性码.

(2) $|C| \cdot |C^\cdot| = |X| = q^n$.

(3) $C^{\cdot\cdot} = -C$；特别是，$C^{\cdot\cdot} = C$ 若C是线性码或$p = 2$(这里 p 表示域$\boldsymbol{F}$ 的特征).

证明　结论(1) 已在命题 4.5.7 中证明过了. 因为

$$\chi_{C^\cdot} = \frac{1}{|C|}\Phi\chi_C,$$

根据式(4.5.4)、式(4.5.5) 和假设 4.5.9 我们有

$$|C^\cdot| = |\chi_{C^\cdot}| = \Phi\chi_{C^\cdot}(\mathbf{0}) = \frac{1}{|C|}\Phi\Phi\chi_C(\mathbf{0})$$

$$= \frac{1}{|C|}|X| \cdot \chi_C(\mathbf{0}) = \frac{|X|}{|C|};$$

这就是(2). 最后，由定义 $C^{\cdot\cdot}$ 的特征函数是$\frac{1}{|C^\cdot|}\Phi\chi_{C^\cdot}$，那么

$$\frac{1}{|C^\cdot|}\Phi\chi_{C^\cdot}(\boldsymbol{x}) = \frac{1}{|C^\cdot|}\Phi\left(\frac{1}{|C|}\Phi\chi_C\right)(\boldsymbol{x}) = \frac{1}{|C^\cdot||C|}\Phi\Phi\chi_C(\boldsymbol{x})$$

$$= \frac{1}{|C^\cdot||C|}|X|\chi_C(-\boldsymbol{x}) = \chi_C(-\boldsymbol{x});$$

这就是(3). □

继续我们上面的记号：$X = \boldsymbol{F}^n$，$C \subset \boldsymbol{F}^n$ 是一个码，$\mathbf{0} \in C$. 进一步设

$$X_i = \{\boldsymbol{x} \in X \mid w(\boldsymbol{x}) = i\}.$$

4.5.11 定义 设 $A_i = |C \cap X_i|$，它是重量为 i 的码字的个数；称 $(A_0, A_1, \cdots, A_n)$ 是码 C 的重量分布(weight distribution)，而下面关于不定元 z 的多项式

$$A_C(z) = \sum_{i=0}^{n} A_i z^i \tag{4.5.11.1}$$

称为码 C 的重量计数子(weight enumerator). 显然 $|C \cap X_i| = \sum_{x \in X_i} \chi_C(x)$. 因此，对于任意 $f \in \mathbb{C}^X$，为方便起见，我们记 $|f(X_i)| = \sum_{x \in X_i} f(x)$. 那么 $A_i = |\chi_C(X_i)|$. 因此，对于形式对偶码 C^*，我们定义它的形式重量分布(formal weight distribution)为 $(B_0, B_1, \cdots, B_n)$ 其中

$$B_i = |\chi_{C^*}(X_i)| = \sum_{x \in X_i} \chi_{C^*}(x), \tag{4.5.11.2}$$

并定义它的对偶重量计数子(dual weight enumerator)为

$$B_C(z) = \sum_{i=0}^{n} B_i z^i. \tag{4.5.11.3}$$

因为 $\chi_{C^*} = |C|^{-1} \Phi \chi_C$，所以

$$B_i = \frac{|\Phi \chi_C(X_i)|}{|\chi_C|} = \frac{1}{|C|} \sum_{t \in X_i} \sum_{x \in X} \chi_C(x) \theta\langle x, t \rangle. \tag{4.5.12}$$

4.5.13 定理(MacWilliams 恒等式)

$$B_C(z) = |C|^{-1} (1 + (q-1)z)^n A_C\left(\frac{1-z}{1+(q-1)z}\right).$$

证明 由式(4.5.12)我们有

$$\begin{aligned} |C| \cdot B_C(z) &= \sum_{i=0}^{n} z^i \sum_{t \in X_i} \sum_{x \in X} \chi_C(x) \theta\langle x, t \rangle \\ &= \sum_{t=0}^{n} \sum_{t \in X_i} z^i \sum_{x \in X} \chi_C(x) \theta\langle x, t \rangle. \end{aligned}$$

因 $X = \bigcup_{i=0}^{n} X_i$ 是不交并，故在 t 跑遍 X_i 并且 i 跑遍 $0, 1, \cdots, n$ 时，

t 就跑遍 X；而且对于 $t \in X$，有 $z^t = z^{w(t)}$. 所以

$$(4.5.13.1)\quad |C| \cdot B_C(z) = \sum_{t\in X} z^{w(t)} \sum_{x\in X} \chi_C(x)\theta\langle x,t\rangle$$
$$= \sum_{c\in C}\sum_{t\in X} z^{w(t)}\theta\langle c,t\rangle.$$

令 $\boldsymbol{c} = (c_1, c_2, \cdots, c_n)$ 和 $\boldsymbol{t} = (t_1, t_2, \cdots, t_n)$，则

$$w(\boldsymbol{t}) = w(t_1) + w(t_2) + \cdots + w(t_n),$$
$$\theta\langle \boldsymbol{c},\boldsymbol{t}\rangle = \theta(c_1t_1 + \cdots + c_nt_n) = \theta(c_1t_1)\cdots\theta(c_nt_n),$$

我们有

$$\sum_{t\in X} z^{w(t)}\theta\langle \boldsymbol{c},\boldsymbol{t}\rangle = \sum_{(t_1,\cdots,t_n)\in X} z^{w(t_1)}\cdots z^{w(t_n)}\theta(c_1t_1)\cdots\theta(c_nt_n)$$
$$= \sum_{(t_1,\cdots,t_n)\in F^n} z^{w(t_1)}\theta(c_1t_1)\cdots z^{w(t_n)}\theta(c_nt_n)$$
$$= \prod_{i=1}^{n}\sum_{\tau\in F} z^{w(\tau)}\theta(c_i\tau).$$

在 $c_i = 0$ 时，$\theta(c_i\tau) = 1, z^{w(\tau)} = \begin{cases}1, & \text{若 } \tau = 0;\\ z, & \text{若 } \tau \in F^*.\end{cases}$ 所以 $\sum_{\tau\in F} z^{w(\tau)}\theta(c_i\tau) = 1 + (q-1)z$. 在 $c_i \neq 0$ 时，则有 $\sum_{\tau\in F} z^{w(\tau)}\theta(c_i\tau)$ $= 1 + z\cdot\sum_{\tau\in F^*}\theta(\tau)$；因为 θ 是 F 的加群的非单位线性复特征标，由特征标正交关系（见习题 4.4.2）得 $\sum_{\tau\in F}\theta(\tau) = 0$；从而 $\sum_{\tau\in F^*}\theta(\tau)$ $= -\theta(0) = -1$. 也就是

$$\sum_{\tau\in F} z^{w(\tau)}\theta(c_i\tau) = \begin{cases}1 + (q-1)z, & \text{若 } c_i = 0;\\ 1 - z, & \text{若 } c_i \neq 0.\end{cases}$$

因此我们得到

$$\sum_{t\in X} z^{w(t)}\theta\langle \boldsymbol{c},\boldsymbol{t}\rangle = (1-z)^{w(c)}(1 + (q-1)z)^{n-w(c)};$$

代入式(4.5.13.1)得

$$|C| \cdot B_C(z) = \sum_{c\in C}(1-z)^{w(c)}(1 + (q-1)z)^{n-w(c)}.$$

再利用不交并 $C=\bigcup_{i=0}^{n} C\cap X_i$，并注意对于 $c\in C\cap X_i$ 有 $z^{w(c)}=z^i$，就把上式改写为

$$\begin{aligned}|C|\cdot B_C(z)&=\sum_{i=0}^{n}\sum_{c\in C\cap X_i}(1-z)^i(1+(q-1)z)^{n-i}\\&=(1+(q-1)z)^n\sum_{i=0}^{n}\sum_{c\in C\cap X_i}\left(\frac{1-z}{1+(q-1)z}\right)^i\\&=(1+(q-1)z)^n\sum_{i=0}^{n}A_i\left(\frac{1-z}{1+(q-1)z}\right)^i\\&=(1+(q-1)z)^nA_C\left(\frac{1-z}{1+(q-1)z}\right).\end{aligned}$$

这就完成了定理的证明. □

习题 4.5

1. 设 $C\subset \boldsymbol{F}^n$ 是一个码，$v\in \boldsymbol{F}^n$，令 $C'=C+v=\{c+v\mid c\in C\}$. 证明：$C$ 与 C' 的距离分布完全相同.

§4.6 极大投射码

本节将把 §4.2 末尾和 §4.3 末尾提到的两种码联系起来. 先来看一个例子，它就是例4.3.14 的对偶.

4.6.1 例 取 $\boldsymbol{F}$ 为 2 元域，$k=3$，$n=|\mathrm{PG}(\boldsymbol{F}^3)|=\dfrac{2^3-1}{2-1}=7$. 以

$$G=\begin{pmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{pmatrix}$$

为生成矩阵的线性码 C 是极大投射码，容易算出它的全部码字共 8 个，为

$$\begin{array}{ccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1
\end{array}$$

它的参数是[7,3,4],它的纠错能力为1,检错能力为3.它的突出特点是每个非零码字的重量都是4;换言之,它是等距码,见定义4.2.16.我们将指出,这不是偶然的;从本质上说,所有等距线性码都是由极大投射码按简单重复的方式构造出来的.

在§4.3中已指出极大投射码是Hamming码的对偶码.我们也将采用多少对偶的方法研究它.在§4.3中较多地使用了检验矩阵,这里则较多地使用生成矩阵.

设$C \leqslant \boldsymbol{F}^n$是一个$[n,k,d]$线性码;并设$C$有基底

$$\boldsymbol{g}_1 = (g_{11}, g_{12}, \cdots, g_{1n}), \cdots, \boldsymbol{g}_k = (g_{k1}, g_{k2}, \cdots, g_{kn});$$

以它们为行向量的$k \times n$矩阵

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}$$

是线性码C的一个生成矩阵.那么矩阵G的秩为k,对于任意码字$\boldsymbol{c} \in C$恰存在一个k-维向量$\boldsymbol{y} = (y_1, y_2, \cdots, y_k) \in \boldsymbol{F}^k$使得$\boldsymbol{c} = \boldsymbol{y}G$,并且容易验证以下命题.

4.6.2 命题 以下映射是线性同构的.

$$\boldsymbol{F}^k \xrightarrow{\cong} C, \quad \boldsymbol{y} \mapsto \boldsymbol{y}G;$$

特别是,C的所有线性子码也以这种方式与$\boldsymbol{F}^k$的线性子空间一一对应.

另一方面,C的对偶码$C^\perp$以G为检验矩阵

(4.6.3) $$C^{\perp} = \{x \in \boldsymbol{F}^n \mid Gx^{\mathrm{T}} = 0\},$$

这里 x^{T} 为行矩阵 $x = (x_1, x_2, \cdots, x_n)$ 的转置矩阵.

如同上一节,令

码	参数	重量分布	重量计数子
C	$[n,k,d]$	$(A_0,A_1,\cdots,A_n)$	$A_C(z) = \sum_{i=0}^{n} A_i z^i$
$C^{\perp}$	$[n,k',d']$	$(B_0,B_1,\cdots,B_n)$	$B_C(z) = \sum_{i=0}^{n} B_i z^i$

把矩阵 G 按列分块写成

$$G = (G_1, G_2, \cdots, G_n),$$

即 G_j 是 G 的第 j 列;特别是,$G_j \in \boldsymbol{F}^k$.那么 C 的任何码字 $c \in C$ 对应于 $y \in \boldsymbol{F}^k$ 使得

(4.6.4) $$c = yG = (yG_1, yG_2, \cdots, yG_n).$$

从 §4.3 中我们已经知道了如何从 G 确定 $C^{\perp}$ 的极小距离 $d' = d(C^{\perp})$;特别地,容易得到以下命题.

4.6.5 命题 以下四条件等价:

(1) $d(C^{\perp}) \geqslant 2$;

(2) 对偶重量分布中 $B_1 = 0$;

(3) G 没有零列;

(4) 对于任意 $1 \leqslant i \leqslant n$ 存在码字 $c = (c_1, c_2, \cdots, c_n) \in C$ 使得 $c_i \neq 0$.

证明 (1) ⇔ (2):重量分布的定义.

(1) ⇔ (3):因为一个零向量线性相关,所以由定理 4.3.5 得出本断言.

(3) ⇔ (4):从式(4.6.4) 直接得出. □

由定义 4.3.10,向量空间 $\boldsymbol{F}^k$ 的投射空间 $\mathrm{PG}(\boldsymbol{F}^k)$ 是 $\boldsymbol{F}^k$ 的所有 1 维子空间的集合,而

$$|\mathrm{PG}(\boldsymbol{F}^k)| = (q^k - 1)/(q - 1).$$

那么生成矩阵 G 的每个非零列向量 G_i 生成的子空间 $\langle G_i\rangle \in \mathrm{PG}(\boldsymbol{F}^k)$. 由此,矩阵 G(实际上任何 k 行的矩阵都可以)决定一个非负整值函数(其中 $\mathbb{Z}^+$ 记所有非负整数的集合).

$$m_G: \mathrm{PG}(\boldsymbol{F}^k) \to \mathbb{Z}^+,\ L \mapsto m_G(L),$$
$$m_G(L) = \big|\{i \mid G_i \neq 0 \text{ 且 } \langle G_i\rangle = L\}\big|. \tag{4.6.6}$$

这里 $m_G(L)$ 称为 $L \in \mathrm{PG}(\boldsymbol{F}^k)$ 在 G 中出现的重数(multiplicity). 这个术语没有反映零列的情况,我们就用 g_0 表示 G 中零列的个数.

使用这个术语,就可以如下描写投射码. 注意 $g_0 > 0$ 时 C 肯定不是投射码.

4.6.7 命题 设 G 是线性码 C 的生成矩阵,$g_0 = 0$. 则:

(1) C 为投射码当且仅当 $m_G(L) \leqslant 1$ 对于任意 $L \in \mathrm{PG}(\boldsymbol{F}^k)$.

(2) C 为极大投射码当且仅当 $m_G = 1$(常值函数 1).

考虑 $\boldsymbol{F}^k$ 的任一子空间 U. 显然 U 的 1 维子空间也是 $\boldsymbol{F}^k$ 的 1 维子空间,换言之,$\mathrm{PG}(U) \subset \mathrm{PG}(\boldsymbol{F}^k)$.

4.6.8 引理 令 $m_G(U) = \sum\limits_{L \in \mathrm{PG}(U)} m_G(L)$. 则 $m_G(U) + g_0$ 是 G 的列向量中属于 U 的向量个数.

证明 设生成矩阵 G 的列向量 $G_i \in U$. 如果 $G_i = 0$,则它被计数在 g_0 中,而且零列的计数没有重复. 如果 $G_i \neq 0$,则 $\langle G_i\rangle = L \in \mathrm{PG}(U)$,它被计数在 $m_G(L)$ 中. 反之,对于任意 $L \in \mathrm{PG}(U)$,按 $m_G(L)$ 的定义(4.6.6),在 $m_G(L)$ 的计数中作贡献的 G_i 必属于 U. 所以得到引理结论. □

我们利用这个工具来研究码字的重量. 设 $\boldsymbol{c} \in C$,由命题 4.6.2,存在惟一的 $\boldsymbol{y} \in \boldsymbol{F}^k$ 使得 $\boldsymbol{c} = \boldsymbol{y}G$. 另一方面,在向量空间 $\boldsymbol{F}^k$ 中把 $\langle \boldsymbol{y}\rangle$ 的正交子空间 $\langle \boldsymbol{y}\rangle^\perp$ 简记为 $\boldsymbol{y}^\perp$,它是 $\boldsymbol{F}^k$ 的一个 $k-1$ 维子空间,这种最大维数的真子空间称为超平面.

4.6.9 命题 $w(\boldsymbol{c}) = w(\boldsymbol{y}G) = n - m_G(\boldsymbol{y}^\perp) - g_0$.

证明 码字 $\boldsymbol{y}G$ 的第 i 个分量为零当且仅当 $\boldsymbol{y}G_i = 0$，当且仅当 $G_i \in \boldsymbol{y}^{\perp}$. 所以 $\boldsymbol{y}G$ 的零分量个数是生成矩阵 G 的列向量中属于 $\boldsymbol{y}^{\perp}$ 的向量个数. 本命题立即由引理 4.6.8 导出. □

因为当 $\boldsymbol{y}$ 跑遍 $\boldsymbol{F}^k$ 时，一方面 $\boldsymbol{y}G$ 跑遍码 C 中的码字，另一方面 $\boldsymbol{y}^{\perp}$ 跑遍 $\boldsymbol{F}^k$ 的超平面. 因而立即得到下述结论，它与定理 4.3.5 多少是对偶的.

4.6.10 定理 设 G 是线性码 C 的生成矩阵，设 m_G 如 (4.6.6) 所定义. 则 C 的极小距离

$$d(C) = n - \max\{m_G(W) \mid W \text{ 跑遍 } \boldsymbol{F}^k \text{ 的超平面}\} - g_0.$$

□

作为命题 4.6.9 的另一个推论，很容易知道极大投射码是等距码，即任意两码字的距离为常数的码，见命题 4.2.15. 下面将叙述的是一个比这更广的结论. 先介绍一个简单结论.

4.6.11 引理 线性码是等距的当且仅当它是等重的.

证明 $d(\boldsymbol{c},\boldsymbol{c}') = d$ 对于任意 $\boldsymbol{c} \neq \boldsymbol{c}' \in C$ 当且仅当 $w(\boldsymbol{c} - \boldsymbol{c}') = d$，对于任意 $\boldsymbol{c} \neq \boldsymbol{c}' \in C$ 当且仅当 $w(\boldsymbol{c}) = d$ 对于任意 $0 \neq \boldsymbol{c} \in C$. □

4.6.12 推论 如果由 q- 元 $[n,k,d]$ 线性码 C 的生成矩阵 G 确定的函数 $m_G = g$ 是常值函数，则 C 是参数为 $\left[g\dfrac{q^{k-1}-1}{q-1} + g_0, k, gq^{k-1}\right]$ 的等距码. 特别是，极大投射码是参数为 $\left[\dfrac{q^k-1}{q-1}, k, q^{k-1}\right]$ 的等距码.

证明 设对于任意 $L \in \mathrm{PG}(\boldsymbol{F}^k)$ 有 $m_G(L) = g$ 是常数，则生成矩阵 G 的非零列共有 $\overline{g \cdot |\mathrm{PG}(\boldsymbol{F}^k)|} = g\dfrac{q^k-1}{q-1}$. 故 $n = g\dfrac{q^k-1}{q-1} + g_0$.

对于 F^k 的任意超平面 W 也有 $m_C(W) = g|\mathrm{PG}(W)| = g\dfrac{q^{k-1}-1}{q-1}$，这是常数. 那么由命题 4.6.9，任意码字的重量

$$w(c) = n - g\frac{q^{k-1}-1}{q-1} - g_0 = gq^{k-1}$$

也是常数. 如果 C 是极大投射码，则 $g_0 = 0, g = 1, n = \dfrac{q^k-1}{q-1}$，从而 $d = q^{k-1}$. □

我们的主要目的是要证明推论 4.6.12 的逆命题也是对的. 为此先做一点准备工作. 在下一结论中 C 不必是线性码.

4.6.13 引理 设 C 是 F 上的含零向量的等重码，即任意两个非零码字的重量相等；并设 $|C| = q^k$. 如果形式对偶码的形式重量分布中的 $B_1 = 0$，则存在正整数 m 使得

$$n = m(q^k-1)/(q-1) \quad 和 \quad d = mq^{k-1}.$$

证明 按假设，$A_0 = 1, A_d = q^k - 1$，而其他的 $A_i = 0$，那么

$$A_C(z) = 1 + (q^k-1)z^d.$$

由 MacWilliams 恒等式(定理 4.5.13)，我们有

$$q^k \cdot B_C(z) = (1+(q-1)z)^n\left(1+(q^k-1)\left(\frac{1-z}{1+(q-1)z}\right)^d\right)$$

$$= (1+(q-1)z)^n + (q^k-1)(1-z)^d \cdot (1+(q-1)z)^{n-d}$$

特别是

$$q^k \cdot B_1 = q(q^{k-1}(q-1)n - (q^k-1)d).$$

而由假设，$B_1 = 0$，所以 $q^{k-1}(q-1)n - (q^k-1)d = 0$，即是

$$d = \frac{q^{k-1}(q-1)n}{(q^k-1)} = \frac{nq^{k-1}}{q^{k-1}+\cdots+q+1}$$

为整数. 但是 q^{k-1} 与 $q^{k-1}+\cdots+q+1$ 是互素的整数，这是因为整数 q 和 $q-1$ 使得 $qq^{k-1} - (q-1)(q^{k-1}+\cdots+q+1) = 1$. 所以存在正整数 m 使得

$$n = m(q^{k-1}+\cdots+q+1) = m(q^k-1)/(q-1),$$

随之 $d = mq^{k-1}$. □

4.6.14 定理 设 G 是线性码 C 的生成矩阵，m_G 是由(4.6.6)确定的函数. 则 C 是等距码当且仅当 m_G 是常值函数.

证明 充分性已在推论 4.6.12 中获证. □

设 C 是等距码，要证明 m_G 是常值函数. 设码 C 的参数是 $[n,k,d]$，其中 d 是任二码字的距离，那么 $|C| = q^k$. 令 $G = (G_1, G_2, \cdots, G_n)$ 是 C 的生成矩阵，并仍用(4.6.6)中的记号. 如果 $k = 1$，则 $|\mathrm{PG}(\boldsymbol{F}^k)| = 1$，则 m_G 显然是常值函数. 以下设 $k > 1$. 如果 $G_i = 0$ 对于某 $1 \leqslant i \leqslant n$，那么对于任意 $\boldsymbol{c} \in C$ 其 i- 分量 $c_i = 0$；把从 G 中去掉列 G_i 后的矩阵记为 G'；则以矩阵 G' 为生成矩阵的线性码 C' 仍是等距码；按对码长 n 的归纳法，m_G 是常值函数，但去掉的是零列，所以 $m_G = m_C$ 从而 m_G 也是常值函数. 故可进一步设所有 $G_i \neq 0$. 那么由命题 4.6.5，对偶重量分布中的 $B_1 = 0$；再由引理 4.6.13 就有：

(4.6.14.1) 存在正整数 m 使得 $n = m(q^k - 1)/(q-1), d = mq^{k-1}$.

现在我们证明断言：

(4.6 14.2) 对于任意 $L \in \mathrm{PG}(\boldsymbol{F}^k)$ 有 $m_i(L) > 0$.

如果不是这样，则存在 $L \in \mathrm{PG}(\boldsymbol{F}^k)$ 使得 $m_i(L) = 0$，即 $\langle G_i \rangle \neq L$ 对于任意 $1 \leqslant i \leqslant n$. 那么，由命题 4.6.2 知 C 有子码

$$\hat{C} = \{\boldsymbol{y}G = (\boldsymbol{y}G_1, \boldsymbol{y}G_2, \cdots, \boldsymbol{y}G_n) \mid \boldsymbol{y} \in L^{\perp}\}$$

是 $k-1$ 维的线性子码，它也是线性等距码，因为它的每个非零码字的重量也是 d；它的参数 $[\hat{n}, \hat{k}, \hat{d}]$ 就是 $\hat{n} = n, \hat{k} = k-1, \hat{d} = d$. 而且对于任意 $1 \leqslant i \leqslant n$，由于 $\langle G_i \rangle \neq L$，故存在 $0 \neq \boldsymbol{y} \in L^{\perp}$ 使得 $\boldsymbol{y}G_i \neq 0$，即存在 $\hat{C}$ 的码字其 i- 分量非零. 所以 $\hat{C}$ 的生成矩阵的所有列非零. 仍由命题 4.6.5，参看(4.6.14.1)，我们有正整数 $\hat{m}$ 使得

$$n = \hat{n} = \hat{m}(q^{k-1} - 1)/(q-1), d = \hat{d} = \hat{m}q^{k-2};$$

把它们与(4.6.14.1)比较，得到

$\hat{m}(q^{k-1}-1)/(q-1)=m(q^k-1)/(q-1)$, $\hat{m}q^{k-2}=mq^{k-1}$. 从后一式得 $\hat{m}=mq$,代入前一式得

$$q(q^k-1)/(q-1)=(q^k-1)/(q-1)=q^{k-1}+\cdots+q+1;$$

特别地,q 整除 $q^{k-1}+\cdots+q+1$ 显然是不可能的. 所以断言(4.6.14.2)成立.

根据断言(4.6.14.2),适当地选取置换矩阵 P 就可使得

$$GP=(G',K)=(G',K_1,K_2,\cdots,K_s),$$

其中 $s=(q^k-1)/(q-1)$ 而 $\langle K_i\rangle, i=1,2,\cdots,s$,恰好跑遍 $PG(\boldsymbol{F}^k)$ 的全部元,K 是 k- 维极大投射码 D 的生成矩阵,而 G' 是一个 $k\times r$- 矩阵,$r=n-(q^k-1)/(q-1)$. 设以 GP 为生成矩阵的线性码是 $\tilde{C}$,那么 $C\cong\tilde{C}$. 从而 $\tilde{C}$ 是等距码而 $m_{GP}=m_G$. 所以我们可设

$$G=(G',K)=(G',K_1,K_2,\cdots,K_s),$$

如果 $G'=0$,则 C 是极大投射码,则 $m_G=1$ 是常值函数.

再设 $G'\neq 0$. 把码 C 的每个码字 $\boldsymbol{y}G$ 的后 s 位截去,得到长 $n-s$ 的字 $\boldsymbol{y}G'$. 对于任意非零的 $\boldsymbol{y},\boldsymbol{y}'\in\boldsymbol{F}^k$,因为 $w(\boldsymbol{y}G')+w(\boldsymbol{y}K)=w(\boldsymbol{y}'G')+w(\boldsymbol{y}'K)$ 而且 $w(\boldsymbol{y}K)=w(\boldsymbol{y}'K)$,所以:

(4.6.14.3) $w(\boldsymbol{y}G')=w(\boldsymbol{y}'G')$, 对于任意非零的 $\boldsymbol{y},\boldsymbol{y}'\in\boldsymbol{F}^k$.

如果 G' 的秩小于 k,那么 G' 的所有列向量生成的子空间 U 是 $\boldsymbol{F}^k$ 的真子空间,从而 $U^{\perp}$ 是非零子空间,即有 $0\neq\boldsymbol{y}_0\in U^{\perp}$,那么 $\boldsymbol{y}_0G'=\boldsymbol{0}$;但另一方面,因 $G'\neq 0$,故有 $\boldsymbol{y}'\in\boldsymbol{F}^k$ 使得 $\boldsymbol{y}'G'\neq\boldsymbol{0}$,这与(4.6.14.3)相矛盾. 所以 G' 的秩只能是 k.

因此,从码 C 的每个码字截去后 s 位得到了一个参数为 $[n-s,k,d-q^{k-1}]$ 的等距线性码,其生成矩阵是 G'. 按对长度的归纳法 m_G 是常值函数. 于是得到 $m_G=m_G+m_K$ 也是常值函数. □

4.6.15 推论 C 是线性等距码当且仅当它的生成矩阵 G 在适当的列置换后可写成

$$G = (K^{(1)}, K^{(2)}, \cdots, K^{(m)}, 0).$$

其中每个 $K^{(j)}$ 是一个极大投射码的生成矩阵. 特别是,线性等距码的参数必形如

$$\left[\frac{m(q^k - 1)}{q - 1} + s, k, mq^{k-1}\right]. \qquad \square$$

4.6.16 推论 存在线性码 C 达到 Plotkin 界,而且只有以下述矩阵为生成矩阵的线性等距码达到 Plotkin 界

$$G = (K^{(1)}, K^{(2)}, \cdots, K^{(m)})$$

其中每个 $K^{(j)}$ 是一个极大投射码的生成矩阵. $\square$

第 5 章　循 环 码

§5.1　群 代 数

我们将从群代数的理想的角度来研究码，这样的码有更多的数学结构.

在 §2.5 中我们已经引进了实数域上的代数，见定义 2.5.2，而且看到了这个工具的重要作用.这里我们要用任意的域 $\mathbf{F}$ 上的代数.这里做得更一般一点，定义有单位元的交换环上的代数.以下说的环与代数都是有单位元的.

5.1.1 定义　设 R 是有单位元的交换环.设 A 是一个非空集合，带有两个运算，分别称为加法和乘法，还有一个纯量运算：$R \times A \to A, (\lambda, a) \mapsto \lambda a$.称 A 为交换环 R 上的一个代数，简称 R- 代数，如果以下三条成立：

(1) A 在加法和纯量乘法下是一个 R- 模(即满足以下四个条件)：

(ⅰ) $(A, +)$ 是一个加群(运算写作加法的交换群)；

(ⅱ) $(\lambda_1\lambda_2)a = \lambda_1(\lambda_2 a), \forall \lambda_1, \lambda_2 \in R$ 和 $a \in A$；

(ⅲ) $(\lambda_1 + \lambda_2)a = \lambda_1 a + \lambda_2 a, \forall \lambda_1, \lambda_2 \in R$ 和 $a \in A$；

$\lambda(a_1 + a_2) = \lambda a_1 + \lambda a_2, \forall \lambda \in R$ 和 $a_1, a_2 \in A$；

(ⅳ) $1_R a = a, \forall a \in A$.

(2) A 在加法和乘法下是一个有单位元的环.

(3) 对于任意 $\lambda \in R, a_1, a_2 \in A$ 有 $\lambda(a_1 a_2) = (\lambda a_1)a_2 = a_1(\lambda a_2)$.

后面将利用群构造代数. 这里先看几个典型例子. 以下 R 总是有单位元的交换环. 环同态都是幺同态, 即把单位元映射为单位元.

例 任何环都可以看做$\mathbb{Z}$- 代数(见本节习题 1). 特别是, 对一般代数成立的结论对环也成立.

例 用 X 表示不定元, 以 $R[X]$ 记所有系数在 R 中的多项式的集合, 两多项式相等规定为它们的次数相等而且所有对应系数相等. 在通常意义的多项式加法、多项式乘法和系数乘多项式运算之下, $R[X]$ 是一个 R- 代数.

例 以 $M_n(R)$ 记所有的元素在 R 中的 $n \times n$ 矩阵的集合, 两矩阵相等规定为它们的所有对应元素相等. 在通常意义的矩阵加法、矩阵乘法和系数乘矩阵运算之下, $M_n(R)$ 是一个 R- 代数.

5.1.2 命题 (1) 设 A 是一个 R- 代数. 则有环同态

$$R \to Z(A), \lambda \mapsto \lambda 1_A.$$

(对于任意环 T, $Z(T) = \{z \in T \mid zt = tz \ \forall\, t \in T\}$ 称为 T 的中心, 显然 $1_T \in Z(T)$.)

(2) 设 A 是一个环. 若有环同态

$$\zeta: R \to Z(A), \lambda \mapsto \zeta(\lambda).$$

则 A 是一个 R- 代数.

证明 (1) 由定义 $(\lambda 1_A)a = \lambda(1_A a) = \lambda(a 1_A) = a(\lambda 1_A)$, $\forall\, a \in A$; 故 $\lambda 1_A \in Z(A)$. 又

$(\lambda_1 \lambda_2)1_A = \lambda_1(\lambda_2(1_A 1_A)) = \lambda_1(1_A \cdot \lambda_2 1_A) = (\lambda_1 1_A)(\lambda_2 1_A)$;

同理可证 $(\lambda_1 + \lambda_2)1_A = (\lambda_1 1_A) + (\lambda_2 1_A)$. 所以 $\lambda \mapsto \lambda 1_A$ 是环同态.

(2) 定义纯量乘法为 $\lambda a = \zeta(\lambda)a$ 即可验证 A 是一个 R- 代数. □

注解：如果 $R = \boldsymbol{F}$ 是一个域，那么命题中的同态 $\boldsymbol{F} \to Z(A)$ 只能是单同态，因为域 $\boldsymbol{F}$ 只有平凡理想. 因此，我们可认为 $\boldsymbol{F}$ 嵌入到 $Z(A)$ 之中，把其像等同于 $\boldsymbol{F}$，即对于 $\lambda \in \boldsymbol{F}$，记 $\lambda = \lambda 1_A$. 那么代数 A 的纯量乘法也可看做环的乘法 $\lambda a = (\lambda 1_A)a$.

5.1.3 定义　设 A 是 R- 代数，$\varnothing \neq B \subseteq A$.

(1) B 称为代数 A 的一个子代数，如果在 A 的运算之下 B 也是一个代数，且 B 的单位元与 A 的单位元一致.

(2) 称 B 为代数 A 的一个理想，如果以下两条件成立：

(Ⅰ) 对于任意 $b, b' \in B$ 有 $b - b' \in B$；

(Ⅱ) 对于任意 $b \in B$ 和 $a \in A$ 有 $ab \in B$ 和 $ba \in B$.

(3) 设 A' 也是一个 R- 代数. 映射 $f: A \to A'$ 称为 R- 代数同态，如果 f 既是环同态也是 R- 模同态，而且 $f(1_A) = 1_{A'}$. 这里 R- 模同态是指下述两条件成立：

(Ⅰ) $f(a + a') = f(a) + f(a')$, $\forall a, a' \in A$（这条件与环同态条件之一重复）；

(Ⅱ) $f(\lambda a) = \lambda f(a)$, $\forall \lambda \in R$ 和 $a \in A$.

5.1.4 定理　对于代数同态 $f: A \to A'$，以下经典结论都成立.

(1) A 的子代数 B 的像 $f(B)$ 是 A' 的子代数.

(2) A' 的子代数 B' 的全原像 $f^{-1}(B')$ 是 A 的子代数；A' 的理想 I' 的全原像 $f^{-1}(I')$ 是 A 的理想；特别地，

$$\mathrm{Ker}(f) = f^{-1}(0) = \{a \in A \mid f(a) = 0\}$$

是 A 的理想，称为同态 f 的核.

(3) 设 I 是 A 的理想. 则 I 在 A 的加群中的陪集类 $\{a + I \mid a \in A\}$ 在运算

$$(a + I) + (a' + I) = (a + a') + I;$$
$$(a + I) \cdot (a' + I) = (a \cdot a') + I;$$
$$\lambda(a + I) = (\lambda a) + I.$$

之下是一个 R- 代数，称为 A（关于理想 I）的商代数，记作 $\overline{A} = A/I$；而 $\tau: A \to \overline{A}$, $a \mapsto \overline{a} = a + I$ 为 R- 代数同态，称为自然同态.

(4)(同态基本定理) 存在惟一代数同态$\bar{f}: A/\mathrm{Ker}(f) \to A'$,使得$f = \bar{f}\ \tau$,这里$\tau$是自然同态,这个$\bar{f}$必为单同态;而且$\bar{f}$为满同态当且仅当$f$是满同态

(5)(理想对应,子代数对应定理) 如果f是满同态,则以下两个映射都是保持包含关系的双射:

$\{I' | I'$是A'的理想$\} \to \{I | I$是A的理想且$I \supseteq \mathrm{Ker}(f)\}$,$I' \mapsto f^{-1}(I')$;

$\{B' | B'$是A'的子代数$\} \to \{B | B$是A的子代数且$B \supseteq \mathrm{Ker}(f)\}$,$B' \mapsto f^{-1}(B')$.

证明 证明都是标准的,这里仅以同态基本定理为例.其他作为习题.代数同态首先是一个加群同态,故由群的同态基本定理1.2.15,使得$f = \bar{f}\ \tau$的加群同态$\bar{f}$存在而且惟一,它定义为$\bar{f}(I + a) = f(a)$;而且(4)的其他结论在定理1.2.15中已被证明成立,剩下只要验证这个加群同态$\bar{f}$也是代数同态,这一点容易直接通过运算验证. □

回头看典型例子.

5.1.5 例 任意环作为$\boldsymbol{Z}$-代数,上述定义和结论都成立.例如子环就是$\boldsymbol{Z}$-子代数,商环就是$\boldsymbol{Z}$-商代数,等等.

以下总设$\boldsymbol{F}$是一个域.

例 所有$\boldsymbol{F}$上的$n \times n$矩阵的集合$M_n(\boldsymbol{F})$在矩阵加法、矩阵乘法和数乘矩阵运算之下是一个$\boldsymbol{F}$-代数.纯量矩阵的集合是$\boldsymbol{F}$的嵌入像.所有对角矩阵的集合构成一个子代数.

例 设$\boldsymbol{F}[X, Y]$是不定元X, Y上的$\boldsymbol{F}$-多项式的集合.在多项式加法、多项式乘法和数乘多项式运算之下$\boldsymbol{F}[X, Y]$是一个$\boldsymbol{F}$-代数.常数多项式的集合是$\boldsymbol{F}$的嵌入像.所有常数项为零的多项式的集合D是一个理想,而$\boldsymbol{F}[X, Y]/D \cong \boldsymbol{F}$.又$\boldsymbol{F}[X] \subseteq \boldsymbol{F}[X, Y]$是一个子代数.值得指出的是,$\boldsymbol{F}[X]$的理想有下述很有用的结构.

5.1.6 命题 设I是$\boldsymbol{F}[X]$的理想,则存在$g(X) \in \boldsymbol{F}[X]$使得

$$I = \boldsymbol{F}[X] \cdot g(X) = \{f(X)g(X) \mid f(X) \in \boldsymbol{F}[X]\};$$

而且如果 $I = \boldsymbol{F}[X] \cdot h(X)$，则有 $0 \neq \lambda \in \boldsymbol{F}$ 使得 $h(X) = \lambda g(X)$.

证明　如果 $I = \{0\}$ 只含零多项式，可以而且只可以取 $g(X) = 0$，命题显然成立. 设 $I \neq \{0\}$，$g(X)$ 是 I 中次数最小的非零多项式，则由理想的定义，对于任意 $f(X) \in \boldsymbol{F}[X]$ 有 $f(X)g(X) \in I$. 对于任意 $h(X) \in I$ 做欧式除法 $h(X) = q(X)g(X) + r(X)$ 其中 $\deg r(X) < \deg g(X)$，那么 $r(X) = h(X) - q(X)g(X) \in I$；于是只能是 $r(X) = 0$，从而 $h(X) = q(X)g(X)$. 即 $I = \boldsymbol{F}[X] \cdot g(X)$. 如果 $I = \boldsymbol{F}[X] \cdot h(X)$，则有 $f(X)$ 使得 $g(X) = f(X)h(X) \neq 0$；但 $g(X)$ 是 I 中次数最小的非零多项式，所以 $f(X) = \lambda$ 只能是非零常数多项式. □

5.1.7 注解　命题中 $\boldsymbol{F}[X] \cdot g(X)$ 称为由 $g(X)$ 生成的主理想，也记作 $\langle g(X) \rangle$. 因为有这个结构，我们说 $\boldsymbol{F}[X]$ 是主理想整环. 对这些概念略作解释. 对环的理想，也可类似于定义 1.3.1 定义一个子集生成的理想；一个元素生成的理想称为主理想. 交换的、乘法满足消去律的环称为整环. 交换环 R 的由元素 $x_1, x_2, \cdots, x_k$ 生成的理想可以表示如下(证明作为本节习题 6)：

$$\begin{aligned}\langle x_1, x_2, \cdots, x_k \rangle &= Rx_1 + Rx_2 + \cdots + Rx_k \\ &= \left\{ \sum_{i=1}^{k} r_i x_i \,\middle|\, r_i \in R, i = 1, 2, \cdots, k \right\}.\end{aligned}$$

对于任意幺半群可定义一个 $\boldsymbol{F}$- 代数.

5.1.8 定义　设 M 是一个幺半群. 用 $\boldsymbol{F}M$ 记以 M 为基底的 $\boldsymbol{F}$- 向量空间，即 $\boldsymbol{F}M = \left\{ \sum_{x \in M} \lambda_x x \,\middle|\, x \in M, \lambda_x \in \boldsymbol{F}, \text{仅有有限个 } \lambda_x \text{ 非零} \right\}$，且

$$\sum_{x \in M} \lambda_x x + \sum_{x \in M} \mu_x x = \sum_{x \in M} (\lambda_x + \mu_x) x,$$

$$a \cdot \left(\sum_{x \in M} \lambda_x x \right) = \sum_{x \in M} (a\lambda_x) x;$$

再规定

$$\left(\sum_{x\in M}\lambda_x x\right)\cdot\left(\sum_{x\in M}\mu_x x\right)=\sum_{x\in M}\left(\sum_{yz=x}\lambda_y\mu_z\right)x.$$

则易验证 FM 构成一个 F- 代数，称为半群 M 在域 F 上的半群代数. 当 M 为群时，就称 FM 为群代数.

5.1.9 注解 由定义可知，FM 的元素 $\sum_{x\in M}\lambda_x x$ 对应于一个从 M 到 F 的函数 $\lambda: M\to F, x\mapsto\lambda_x$. 反之亦然. 即，$FM$ 的元素与从 M 到 F 的函数一一对应. 在这个观点之下，FM 中的两个元素 $\sum_{x\in M}\lambda_x x$，$\sum_{x\in M}\mu_x x$ 的加法对应于函数加法：$(\lambda+\mu)(x)=\lambda_x+\mu_x$；而数乘向量对应于函数乘法：$(a\cdot\lambda)(x)=a\lambda_x$. 可是元素 $\sum_{x\in M}\lambda_x x$，$\sum_{x\in M}\mu_x x$ 的乘法不对应于通常的函数乘法，而应为

$$(\lambda*\mu)(x)=\sum_{yz=x}\lambda_y\mu_z.$$

半群 M 上的两个函数的这种乘积 $\lambda*\mu$ 称为两函数 λ 与 μ 的卷积 (convolution product).

显然，可认为域 F 嵌入在 FM 之中，$a\in F$ 对应于 FM 的这样的元素 $\sum_{x\in M}\lambda_x x$，其系数 $\lambda_{1_M}=a$，其他系数 $\lambda_x=0$. 为简单计，我们把 FM 中的这个元也记作 a.

另一方面，可认为半群 M 嵌入在 FM 之中，$m\in M$ 对应于 FM 的这样的元素 $\sum_{x\in M}\lambda_x x$，其系数 $\lambda_m=1$，其他系数 $\lambda_x=0$，即是 m 的特征函数. 为简单计，我们把 FM 中的这个元也记作 m.

5.1.10 命题（半群代数的泛性质） 设 M 是半群，A 是 F- 代数. 如 $f: M\to(A,\cdot)$ 是半群同态，这里 $(A,\cdot)$ 表示 A 在乘法“$\cdot$”之下的半群，则存在惟一代数同态 $\bar f: FM\to A$ 使得 $\bar f(m)=f(m)$，$\forall m\in M$（即 $\bar f|_M=f$）. 反之，任何代数同态 $\bar f: FM\to A$ 限制到 M 的限制映射 $f=\bar f|_M: M\to A$ 是一个半群同态.

证明 首先，“反之”部分是显然的，因代数同态把单位元变为单位元，对于任意 $y,z\in M$ 有

$$f(yz)=\bar f(yz)=\bar f(y)\,\bar f(z)=f(y)f(z).$$

即 $f:M\to A$ 为半群同态.

现在设 $f:M\to A$ 为半群同态.定义

$$\bar{f}:\boldsymbol{F}M\to A,\sum_{x\in M}\lambda_x x\mapsto\sum_{x\in M}\lambda_x f(x).$$

易证$\bar{f}$是向量空间同态,且保持乘法,即为代数同态.由定义知对于任意 $x\in M$ 有$\bar{f}(x)=f(x)$.又若$\bar{f}'$也是$\boldsymbol{F}M$到A的代数同态,且$\bar{f}'|_M=f$,则对于任意$\sum_{x\in M}\lambda_x x\in\boldsymbol{F}M$有

$$\bar{f}'\Big(\sum_{x\in M}\lambda_x x\Big)=\sum_{x\in M}\lambda_x\,\bar{f}'(x)=\sum_{x\in M}\lambda_x f(x)=\bar{f}\Big(\sum_{x\in M}\lambda_x x\Big);$$

即$\bar{f}'=\bar{f}$.惟一性获证. □

注解:把半群 M 换成群 G,半群同态换为群同态,一切结论完全一样,即:任何群同态 $f:G\to A^*$ 惟一地扩张成代数同态$\bar{f}:\boldsymbol{F}G\to A$.任何代数同态$\bar{f}:\boldsymbol{F}G\to A$的限制映射$\bar{f}|_G:G\to A$取值在$A^*$中而且是群同态.这称为群代数的泛性质.

5.1.11 例　设 $\boldsymbol{F}[X]$ 是域 $\boldsymbol{F}$ 上的不定元X 的多项式环.注意,集合 $M=\{1,X,X^2,X^3,\cdots\}$ 在单项式乘法之下是一个幺半群,所以 $\boldsymbol{F}[X]$ 实际上是幺半群 M 的半群代数.

再设 $C_3=\{1,x,x^2\}$ 是一个三阶循环群,有群代数 $\boldsymbol{F}C_3=\{\lambda_0+\lambda_1 x+\lambda_2 x^2\mid\lambda_i\in\boldsymbol{F}\}$.

显然$M\to C_3,X\mapsto x$是一个半群同态,由半群代数的泛性质 5.1.10 有代数同态

$$\boldsymbol{F}[X]\to\boldsymbol{F}C_3,\sum\lambda_i X^i\mapsto\sum\lambda_i x^i.$$

因 $x^3=1$,故表达式$\sum\lambda_i x^i$实际合并为只有三项;易见上述同态的核就是 $\boldsymbol{F}[X]$ 的由 X^3-1 生成的理想$\langle X^3-1\rangle$.

本例细节留作习题.

现在设 $\boldsymbol{F}$ 是有限域,设 $G=\{1,x_1,\cdots,x_{n-1}\}$ 是有限群.那么群代数 $\boldsymbol{F}G$ 的元$\sum_{i=0}^{n-1}a_i x_i$就是一个$\boldsymbol{F}$序列$(a_0,a_1,\cdots,a_{n-1})$,即是$\boldsymbol{F}$

上的一个长 n 的字.从这个角度出发有下述定义.

5.1.12 定义 群代数 FG 的一个理想 C 称为一个群代数码.

我们的目的是弄清群代数的理想.我们将以两种方式考虑一个简单情况:循环群的群代数.第一种方式是已经很熟悉的检验矩阵和生成矩阵的方式.

习题 5.1

1. 证明任何环可以作为整数环 $\mathbb{Z}$ 上的代数.

2. 完成命题 5.1.2、定理 5.1.4 的证明.

3. 设 A 是交换环 R 上的代数.A 的非空子集 B 是子代数当且仅当以下两条件成立:

(1) 对于任意 $b,b' \in B$ 有 $b-b' \in B$ 和 $bb' \in B$;

(2) 对于任意 $b \in B$ 和 $\lambda \in R$ 有 $\lambda b \in B$.

4. 设 T 是环,由命题 5.1.2 有同态 $\zeta:\mathbb{Z} \to Z(T)$.证明:

(1) 同态像 $\mathrm{Im}(\zeta)$ 是 T 的最小的子环,即 T 的任何子环包含这个像.

(2) 存在惟一非负整数 m 使得 $\mathrm{Ker}(\zeta)=m\mathbb{Z}$;称 m 是环 T 的特征(characteristic),它满足:$m \cdot t=0, \forall\, t \in T$.

(3) 如果 T 是域,则 T 的特征是零或者是一个素数.

5. 证明复数域 $\mathbb{C}$ 可以作为 R- 代数.再记 $\mathrm{i}=\sqrt{-1}$ 是虚数单位.证明:映射 $a+b\mathrm{i} \mapsto a-b\mathrm{i}, a,b \in \mathbb{R}$,是 R- 代数 $\mathbb{C}$ 的自同构.

6. 设 R 是交换环,证明由元素 $x_1,\cdots,x_k$ 生成的理想 $\langle x_1,x_2,\cdots,x_k\rangle = Rx_1+Rx_2+\cdots+Rx_k = \left\{\sum_{i=1}^{k} r_i x_i \,\middle|\, r_i \in R, i=1,2,\cdots,k\right\}$.

7. 完成例 5.1.11 的证明细节.证明:任何有限循环群 G 的群代数 FG 是一元多项式代数 $\mathbf{F}[X]$ 的同态像,并确定同态的核;从而说明 FG 是主理想环,但不是主理想整环.

8. 设 FG 是域 F 上有限群 G 的群代数.证明:

$$\alpha: FG \to F, \sum_{x\in G}\lambda_x x \mapsto \sum_x \lambda_x,$$

是代数满同态(称为增广同态),同态核是 $I = \sum_{1\neq x\in G} F(1-x)$(称为增广理想),其维数 $\dim I = |G| - 1$.

9. 设 FG 是有限域 F 上有限群 G 的群代数,$C \subseteq FG$ 是一个码(即 FG 的一个理想).如果 C 不是单位理想(即 $C \neq FG$),则 C 的极小距离不小于 2.

10. 设 FG 是有限域 F 上有限群 G 的群代数,$C \subseteq FG$ 是一个码.证明:任意 $x \in G$ 诱导 C 的一个自同构为:$\tau_x: C \to C, c \mapsto xc$.

§5.2　循环码

本节始终设 $G = \{1, x, x^2, \cdots, x^{n-1}\}$ 是一个 n 阶循环群,F 是有限域,其阶为 $q = p^l$,那么 $\mathrm{char}F = p$,并且设 $p \nmid n$.

5.2.1 定义　群代数 FG 的一个理想 C 称为 F 上的一个长 n 的循环码.

5.2.2 例　取 $q = 2$,即 $F = F_2$ 是2元域;取 $n = 3$,即 $G = \{1, x, x^2\}$ 是3阶循环群.易验证 $C = \{0, 1+x, 1+x^2, x+x^2\}$ 是群代数 FG 的一个理想,作为码写出来是

$$C = \{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}.$$

它有一个特点:对于任一码字将其各位作一循环置换(123)得到的仍是一个码字.如:

$$(1,1,0) \xrightarrow{(123)} (0,1,1) \xrightarrow{(123)} (1,0,1).$$

实际上任何循环码都具有这个特征,见本节习题1,这是循环码名称的来历.

如同例 5.1.11,我们有满同态,称为典型同态

$$F[X] \to FG, \sum \lambda_i X^i \mapsto \sum \lambda_i x^i,$$

它的同态核是 $\langle X^n - 1\rangle$,换言之,$F[X]/\langle X^n - 1\rangle \cong FG$.利用这一

点容易确定 FG 的全部理想，即确定所有循环码. $F[X]$ 中的元素自然是 X 的多项式 $a(X)$，把它在 FG 中的像记作 $a(x)$；即 FG 中的元素看似 x 的多项式，但 $a(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ 实际最高次数不大于 $n-1$.

5.2.3 定理 设 C 是 FG 的一个理想，$a(x)\in FG$ 为任意元. 存在 $g(X),h(X)\in F[X]$ 使得 $g(X)h(X)=X^n-1$ 而且

$$a(x)\in C\Longleftrightarrow \exists f(x)\in FG \text{ 使得}$$
$$a(x)=f(x)g(x)\Longleftrightarrow a(x)h(x)=0.$$

分别称 $g(X)$ 与 $h(X)$ 为循环码 C 的生成多项式与检验多项式. 循环码 C 的首 1 的生成多项式与检验多项式都是惟一的.

证明 根据定理 5.1.4(5)，在满同态 $F[X]\to FG$ 之下 C 的原像 $\tilde{C}$ 是 $F[X]$ 的一个包含 X^n-1 的理想. 而 $F[X]$ 是主理想整环(见命题 5.1.6)，即 $\tilde{C}$ 由一个元生成；$\tilde{C}=\langle g(X)\rangle$ 且 $g(X)\mid X^n-1$；从而有 $h(X)\in F[X]$ 使得 $g(X)h(X)=X^n-1$. 这样的首 1 的 $g(X)$ 和 $h(X)$ 是惟一的，见命题 5.1.6.

令 $a(X)\in F[X]$ 是 $a(x)$ 的一个原像. 那么 $a(x)\in C$ 当且仅当 $a(X)\in\tilde{C}$，当且仅当 $\exists f(X)\in F[X]$ 使得 $a(X)=f(X)g(X)$，当且仅当 $\exists f(x)\in FG$ 使得 $a(x)=f(x)g(x)$.

若 $a(x)\in C$，由上一段证明可写 $a(X)=f(X)g(X)$；那么 $a(X)h(X)=f(X)g(X)h(X)=f(X)(X^n-1)$ 在典型同态 $F[X]\to FG$ 的同态核之中，故 $a(x)h(x)=0$.

反之设 $a(x)h(x)=0$，即 $a(X)h(X)\in\langle X^n-1\rangle$，就有 $f(X)\in F[X]$ 使得 $a(X)h(X)=f(X)(X^n-1)=f(X)g(X)h(X)$，所以 $a(X)=f(X)g(X)$. 由以上证明，$a(x)\in C$. □

对此结果和论证有一系列说明.

5.2.4 注解 作为 FG 的理想，C 以 $g(x)$ 为生成元，即 $C=\langle g(x)\rangle=FG\cdot g(x)$. 一个主理想的生成元通常不是惟一的. 如例 5.2.2 中的理想 $C=\{0,1+x,1+x^2,x+x^2\}$，容易验证，除了 0 以外的三个元都是 C 的生成元. 但是，尽管它们都是首 1 的，却只

有 $1+x$ 对应的 $1+X$ 是 C 的生成多项式，$1+X^2$ 和 $X+X^2$ 都不是 C 的生成多项式. 因为按照定理 5.2.3 的陈述，C 的生成多项式 $g(X)$ 需要满足两个条件：

(1) $C=\langle g(x)\rangle$；

(2) $g(X)\mid(X^n-1)$.

FG 的理想的另一类生成元值得一提. 不妨先给出一般定义.

5.2.5 定义　环 R 的元素 e 称为幂等元如果 $e^2=e$.

显然零元 0 和单位元 1 是幂等元. 幂等元的重要性在于它们总是与环的单边直和分解联系在一起，见本节习题 2.

例 5.2.2 中理想 $C=\{0,1+x,1+x^2,x+x^2\}$ 中的 $x+x^2$ 是幂等元是因为由习题 4.2.1(3) 的公式立即得 $(x+x^2)^2=x^2+x^4=x+x^2$，这里 $x^4=x$ 是因为 $x^3=1$. 一般地，我们有下述结论.

5.2.6 命题　对于 FG 的任何理想 C 存在惟一幂等元 $e(x)\in FG$ 使得 $C=FG\cdot e(x)$，称为 C 的生成幂等元.

证明　设 $g(X)$ 和 $h(X)$ 分别是 C 的生成多项式和检验多项式，则 $g(X)h(X)=X^n-1$，两边取导数得 $g'(X)h(X)+g(X)h'(X)=nX^{n-1}\neq 0$. 设 $d(X)$ 是 $g(X)$ 与 $h(X)$ 的最大公因子，则既有 $d(X)\mid X^n-1$，也有 $d(X)\mid X^{n-1}$. 然而 $X\cdot X^{n-1}+(-1)(X^n-1)=1$，即 X^{n-1} 与 X^n-1 互素，所以多项式 $g(X)$ 与多项式 $h(X)$ 互素（也可利用习题 5.3.6 证明 X^n-1 无重根，从而 $g(X)$ 与 $h(X)$ 互素）. 那么就有多项式 $p(X),q(X)\in F[X]$ 使得 $p(X)g(X)+q(X)h(X)=1$. 于是在 FG 中就有

$$p(x)g(x)+q(x)h(x)=1.$$

令 $e(X)=p(X)g(X)$. 于是 $e(x)=p(x)g(x)\in C$，特别地，有 $FG\cdot e(x)\subset C$. 另一方面，对于任意 $c(x)\in C$ 由定理 5.2.3 存在 $f(X)$ 使得 $c(x)=g(x)f(x)$，那么

$$\begin{aligned}e(x)c(x)&=(1-q(x)h(x))c(x)=c(x)-q(x)h(x)c(x)\\&=c(x)-q(x)h(x)g(x)f(x).\end{aligned}$$

因为 $h(x)g(x)=x^n-1=0$，故

$$e(x)c(x) = c(x), \quad \forall\, c(x) \in C.$$

特别地，有 $e(x)^2 = e(x)e(x) = e(x)$ 和 $C \subset \boldsymbol{F}G \cdot e(x)$. 即 $e(x)$ 是 C 中的幂等元而且 $C = \boldsymbol{F}G \cdot e(x)$.

如果 $e'(x)$ 也是 C 中的幂等元使得 $C = \boldsymbol{F}G \cdot e'(x)$，则有 $f(x)$ 使得 $e(x) = f(x)e'(x)$. 于是

$$\begin{aligned} e'(x) &= e(x)e'(x) = f(x)e'(x)e'(x) \\ &= f(x)e'(x) = e(x). \end{aligned}$$

这就证明了这种幂等元的惟一性. □

回到定理 5.2.3，循环码也是线性码，我们把它与线性码的两种确定方式联系起来. 设 $h(X)$ 和 $g(X)$ 分别是循环码 $C \subset \boldsymbol{F}G$ 的检验多项式和生成多项式，注意到 $h(X)g(X) = X^n - 1$，我们可设

$$h(X) = h_0 + h_1 X + \cdots + h_k X^k;$$

$$g(X) = g_0 + g_1 X + \cdots + g_{n-k} X^{n-k}.$$

由此可给出循环码 C 的检验矩阵和生成矩阵如下

$$H = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & & & \\ & h_k & h_{k-1} & \cdots & h_0 & & \\ & & \cdots & \cdots & \cdots & \cdots & \\ & & & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}_{(n-k)\times n}$$

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & & & \\ & g_0 & g_1 & \cdots & g_{n-k} & & \\ & & \cdots & \cdots & \cdots & \cdots & \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}_{k\times n}$$

5.2.7 推论 记号如上. 对于 $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \boldsymbol{F}G$ 以下三条件等价：

(1) $a(x) \in C$;

(2) $H\begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} = 0$;

(3) 存在 $\lambda_0,\lambda_1,\cdots,\lambda_{k-1}\in \boldsymbol{F}$ 使得 $(a_0,a_1,\cdots,a_{n-1})=(\lambda_0,\lambda_1,\cdots,\lambda_{k-1})\cdot G$.

证明　(1) $\Longrightarrow$ (2). 由条件(1)根据定理 5.2.3 有 $a(x)h(x)=0$,即

$$a(X)h(X)\equiv 0 \pmod{X^n-1},$$

故可设 $a(X)h(X)=f(X)(X^n-1)$;比较两边次数可设 $f(X)=\lambda_0+\lambda_1X+\cdots+\lambda_{k-1}X^{k-1}$,即

$$\sum_{i=0}^{n-1}a_iX^i\cdot\sum_{j=0}^{k}h_jX^j=(X^n-1)\cdot\sum_{s=0}^{k-1}\lambda_sX^s.$$

右端 $X^k,X^{k+1},\cdots,X^{n-1}$ 的系数为 0,计算左端相应项的系数得

$$\sum_{i+j=s}a_ih_j=0,\quad s=k,k+1,\cdots,n-1.$$

此即(2).

(2) $\Longrightarrow$ (3). 因 $g(x),xg(x),\cdots,x^{k-1}g(x)\in C$,作为码字它们分别就是矩阵 G 的行向量. 由上一段证明知矩阵 G 的行向量都是关于变元 $\xi_0,\xi_1,\cdots,\xi_{n-1}$ 的线性方程组

$$H\begin{pmatrix}\xi_0\\ \vdots\\ \xi_{n-1}\end{pmatrix}=0$$

的解,而 H 的秩显然是 $n-k$,所以此线性方程组的任意解是矩阵 G 的行向量的线性组合. 由此得(3).

(3) $\Longrightarrow$ (1). 条件(3)即表示 $a(x)=\lambda_0g(x)+\lambda_1xg(x)+\cdots+\lambda_{k-1}x^{k-1}g(x)$,而所有 $g(x),xg(x),\cdots,x^{k-1}g(x)\in C$,故 $a(x)\in C$. □

以一个例子结束本节.

5.2.8 例　取 $q=2,n=5$. 则 2 元域 $\boldsymbol{F}$ 上的长 5 的循环码由 X^5-1 在 $\boldsymbol{F}[X]$ 中的因子全部确定. 然而 $X^5-1=(X-1)(X^4+X^3+X^2+X+1)$,显然 0 与 1 都不是多项式 $X^4+X^3+X^2+X+1$ 的根,所以 $X^4+X^3+X^2+X+1$ 没有 1 次因子. 又,$\boldsymbol{F}[X]$

中的全部 2 次多项式为 $X^2, X^2+X, X^2+1, X^2+X+1$;前两个以 0 为根,故不是 $X^4+X^3+X^2+X+1$ 的因子. X^2+1 以 1 为根,也不是 $X^4+X^3+X^2+X+1$ 的因子,经过简单计算可知最后一个也不是 $X^4+X^3+X^2+X+1$ 的因子.所以 X^5-1 的全部不可约因子是

$$X-1=X+1,\quad X^4+X^3+X^2+X+1.$$

因此全部长度 5 的二元循环码如下(共有 4 个):

C_0:生成多项式 X^5-1,零码(只含零向量,对应零理想);

C_1:生成多项式 1,单位码(即所有字都是码字,对应单位理想);

C_2:生成多项式 $X-1$,一个[5,4,2]码,是方程 $\xi_0+\xi_1+\xi_2+\xi_3+\xi_4=0$ 的解空间;

C_3:生成多项式 $X^4+X^3+X^2+X+1$,一个[5,1,5]码.

从这个例子可以看到,为确定所有的循环码,关键是要对有限域上的多项式做素因子分解.这个例子中的多项式很小,可以逐一检验,但显然不是好办法.为讨论一般情况,需要介绍一般域的理论.

习题 5.2

1. 设 G 是 n 阶循环群,$\boldsymbol{F}$ 是有限域.

(1) 设 $C\subseteq \boldsymbol{F}G$ 是一个理想即一个循环码,证明:对于任意码字 $\boldsymbol{c}=(c_0,c_1,c_2,\cdots,c_{n-1})\in C$ 有 $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$.

(2) 设 C 是 $\boldsymbol{F}$ 上的一个长 n 的码.证明:如果对于任意码字 $\boldsymbol{c}=(c_0,c_1,c_2,\cdots,c_{n-1})\in C$ 有 $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$,则集合 $\left\{\sum_{i=0}^{n-1}c_ix^i \mid (c_0,c_1,c_2,\cdots,c_{n-1})\in C\right\}$ 是群代数 $\boldsymbol{F}G$ 的一个理想.

2. 设 R 是环.R 的非空子集 L 称为 R 的左理想如果满足下列两条:

(1) $a-b\in L,\forall a,b\in L$;

(2) $ab\in L,\forall a\in R$ 和 $b\in L$.

设 $R=L_1\oplus L_2$,其中 L_1,L_2 是左理想,直和是指作为加群的直和.那么存在幂等元 $e_1\in L_1$ 和幂等元 $e_2\in L_2$ 使得 $L_i=Re_i,i=1,2$,而且

$$1=e_1+e_2;\quad e_1e_2=0=e_2e_1.$$

反之如果有幂等元 e_1,e_2 满足以上两条,则 $R=Re_1\oplus Re_2$.

3. 设 G 是 n 阶循环群,$\boldsymbol{F}$ 是有限域,$\mathrm{Char}\boldsymbol{F}\nmid n$.设 $C_1,C_2\subset \boldsymbol{F}G$ 是两个循环码,设 $g_1(X),g_2(X)$ 分别是 C_1,C_2 的生成多项式.证明:

(1) $C_1\subset C_2$ 当且仅当 $g_2(X)\mid g_1(X)$.

(2) $C_1+C_2=\{\boldsymbol{c}_1+\boldsymbol{c}_2\mid \boldsymbol{c}_1\in C_1,\boldsymbol{c}_2\in C_2\}$ 也是循环码,而且它的生成多项式是最大公因式 $\gcd(g_1(X),g_2(X))$.

(3) $C_1\cap C_2$ 是循环码,其生成多项式是最小公倍式 $\mathrm{lcm}(g_1(X),g_2(X))$.

4. 符号同上题.请叙述关于检验多项式的类似结论并加以证明.

5. 设 G 是 n 阶循环群,$\boldsymbol{F}$ 是有限域,$\mathrm{char}\boldsymbol{F}\nmid n$.设 $C_1,C_2\subset \boldsymbol{F}G$ 是两个循环码,设 $e_1(x),e_2(x)$ 分别是 C_1,C_2 的生成幂等元.证明:

(1) $C_1\subset C_2$ 当且仅当 $e_1(x)e_2(x)=e_1(x)$.

(2) C_1+C_2 是循环码,它的生成幂等元是 $e_1(x)+e_2(x)-e_1(x)e_2(x)$.

(3) $C_1\cap C_2$ 是循环码,其生成幂等元是 $e_1(x)e_2(x)$.

6. 设 $h(X)$ 和 $g(X)$ 是长 n 的循环码 C 的检验多项式和生成多项式.则 $\dim C=\deg h(X)$,而 $\deg g(X)=n-\dim C$.

7. 设长度为奇数 n 的二元码 $E_n=\left\{(c_0,c_1,\cdots,c_{n-1})\mid \sum_{i=0}^{n-1}c_i=0\right\}$.

(1) E_n 是生成多项式为 $X+1$ 的循环码.

(2) 设 C 是长度 n 的生成多项式为 $g(X)$ 的二元循环码. 则 $C \subset E_n$ 的充要条件是 $(X+1) \mid g(X)$.

8. 写出例5.2.8中码 C_3 的生成矩阵和检验矩阵,求它的生成幂等元.

9. 求出所有长度 3 的二元循环码,写出它们的生成矩阵,检验矩阵和生成幂等元.

§5.3 域 有限域

本节介绍域和有限域的知识. 先列出比较容易解释的基本知识.

5.3.1 域的基本知识 有单位元的而且每个非零元可逆的交换环称为域. 其中条件"每个非零元可逆"等价于条件"所有非零元在乘法下构成一个群". 域 $\boldsymbol{F}$ 的基数称为 $\boldsymbol{F}$ 的阶,记作 $|\boldsymbol{F}|$. 阶有限的域称为有限域. 阶为 q 的域记作 $\boldsymbol{F}_q$.

(a) $\boldsymbol{F}$ 的加群的每个非零元的阶都相同,如果这个相同的阶是有限的,则它必是一个素数 p,就称域 $\boldsymbol{F}$ 的特征是 p,记作 $\mathrm{char}\boldsymbol{F} = p$,否则就称域 $\boldsymbol{F}$ 的特征是 0,记作 $\mathrm{char}\boldsymbol{F} = 0$. 参看习题 5.1.4. 当 $\mathrm{char}\boldsymbol{F} = p \neq 0$ 时,下述公式成立

$$(\lambda + \mu)^{p^n} = \lambda^{p^n} + \mu^{p^n}, \quad \forall \lambda, \mu \in \boldsymbol{F}.$$

(b) $\boldsymbol{F}$ 的任意一些子域之交仍为子域;因此 $\boldsymbol{F}$ 有惟一极小子域 $\boldsymbol{P}$,称为 $\boldsymbol{F}$ 的素子域.

如果 $\mathrm{char}\boldsymbol{F} = p \neq 0$,则 $\boldsymbol{F}$ 的子集 $\boldsymbol{P} = \{0, 1, \cdots, p-1\}$,其中 $k = k \cdot 1_{\boldsymbol{F}}$,显然在乘法之下也封闭,而且 $\mathbb{Z}_p \to \boldsymbol{P}, k \mapsto k \cdot 1_{\boldsymbol{F}}$ 是同构. 特别是,$\boldsymbol{P}$ 就是 $\boldsymbol{F}$ 的素子域.

如果 $\mathrm{char}\boldsymbol{F} = 0$,则 $\boldsymbol{F}$ 的子集 $P = \{k \cdot 1_{\boldsymbol{F}} \mid k \in \mathbb{Z}\}$ 与 $\mathbb{Z}$ 同构,同构映射是 $\mathbb{Z} \to P, k \mapsto k \cdot 1_{\boldsymbol{F}}$. 同上,记 $k \cdot 1_{\boldsymbol{F}} = k$. 那么在 $\boldsymbol{F}$ 中只要 $k \neq 0$ 它就是可逆元,把其逆元记作 k^{-1},令 $\boldsymbol{P} =$

$\{lk^{-1} \mid l,k\in \boldsymbol{F},k\neq 0\}\subset \boldsymbol{F}$. 则有同构映射 $\mathbb{Q}\to \boldsymbol{P}, l/k \mapsto lk^{-1}$; 即 $\boldsymbol{P}$ 是 $\boldsymbol{F}$ 的素子域.

总结上述,按同构分类,域 $\boldsymbol{F}$ 的素子域 $\boldsymbol{P}$ 由 $\mathrm{char}\boldsymbol{F}$ 惟一确定

$$\boldsymbol{P}\cong \begin{cases} \mathbb{Q}, & \text{若 } \mathrm{char}\boldsymbol{F}=0;\\ \mathbb{Z}_p, & \text{若 } \mathrm{char}\boldsymbol{F}=p. \end{cases}$$

特别是,有限域的特征一定是某素数 p.

(c) 设域 $\boldsymbol{F}$ 是域 $\boldsymbol{K}$ 的子域,那么称域 $\boldsymbol{K}$ 为域 $\boldsymbol{F}$ 的扩域,或扩张,记作 $\boldsymbol{F}\leqslant \boldsymbol{K}$. 此时 $\boldsymbol{K}$ 为 $\boldsymbol{F}$ 上的向量空间,其维数称为 $\boldsymbol{K}$ 对 $\boldsymbol{F}$ 的次数,记作 $|\boldsymbol{K}:\boldsymbol{F}|$. 有维数公式如下(见本节习题 1)

$$|\boldsymbol{E}:\boldsymbol{F}| = |\boldsymbol{E}:\boldsymbol{K}|\,|\boldsymbol{K}:\boldsymbol{F}|, \quad \text{这里 } \boldsymbol{F}\leqslant \boldsymbol{K}\leqslant \boldsymbol{E}.$$

(d) $\boldsymbol{F}$ 的所有非零元构成乘法群,称为域 $\boldsymbol{F}$ 的乘群,记作 $\boldsymbol{F}^*$. 乘群 $\boldsymbol{F}^*$ 的任何有限子群是循环群(命题 1.3.13);特别地,有限域的乘群是循环群.

(e) 设 $\alpha_1,\alpha_2,\cdots,\alpha_n\in \boldsymbol{K}$. 称 $\boldsymbol{K}$ 中包含 $\boldsymbol{F}$ 以及 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的最小子域为 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 在 $\boldsymbol{F}$ 上生成的子域,记作 $\boldsymbol{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)$. 特别地,当 $n=1$ 时,$\boldsymbol{F}(\alpha_1)$ 称为 $\boldsymbol{F}$ 的单扩张. 显然

$$\boldsymbol{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)=\{f(\alpha_1,\alpha_2,\cdots,\alpha_n)/g(\alpha_1,\alpha_2,\cdots,\alpha_n)\mid f,g\in \boldsymbol{F}[X_1,X_2,\cdots,X_n], g(\alpha_1,\alpha_2,\cdots,\alpha_n)\neq 0\}.$$

其中 X_i 表示不定元,$\boldsymbol{F}[X_1,X_2,\cdots,X_n]$ 表示 $\boldsymbol{F}$ 上的多项式环. 特别是,对单扩张 $\boldsymbol{F}(\alpha)$ 有

$$\boldsymbol{F}(\alpha)=\{f(\alpha)/g(\alpha)\mid f,g\in \boldsymbol{F}[X], g(\alpha)\neq 0\}.$$

我们要给出单扩张的结构.

5.3.2 定义　设 $\boldsymbol{F}\leqslant \boldsymbol{K}, \alpha\in \boldsymbol{K}$. 如果存在 $0\neq f(X)\in \boldsymbol{F}[X]$ 使得 $f(\alpha)=0$,则称 $f(X)$ 是 α 在 $\boldsymbol{F}$ 上的零化多项式;此时称 α 为 $\boldsymbol{F}$ 上的代数元,α 在 $\boldsymbol{F}$ 上的次数最低的零化多项式称为 α 在 $\boldsymbol{F}$ 上的极小多项式;极小多项式必为素多项式(见本节习题 3). 如果 α 在 $\boldsymbol{F}$ 上的零化多项式不存在,则称 α 为 $\boldsymbol{F}$ 上的超越元.

5.3.3 定理　设 α 是 $\boldsymbol{F}$ 上的代数元,设 $m(X)$ 是 α 在 $\boldsymbol{F}$ 上的

极小多项式，则 $\boldsymbol{F}(\alpha) \cong \boldsymbol{F}[X]/\langle m(X)\rangle$；特别是，$|\boldsymbol{F}(\alpha):\boldsymbol{F}| = \deg m(X)$，而且

$$\boldsymbol{F}(\alpha) = \{f(\alpha) | f(X) \in \boldsymbol{F}[X], \deg f(X) < \deg m(X)\}.$$

反之，任给素多项式 $m(X)$，则 $\boldsymbol{K} = \boldsymbol{F}[X]/\langle m(X)\rangle$ 是域. 令 $\alpha = \overline{X}$（X 所在的等价类），再通过映射 $\boldsymbol{F} \to \boldsymbol{K}, \lambda \mapsto \overline{\lambda}$（$\lambda$ 作为 $\boldsymbol{F}[X]$ 的元素为常数多项式而 $\overline{\lambda}$ 为 λ 所在等价类），将 $\boldsymbol{F}$ 嵌入 $\boldsymbol{K}$，则 $\boldsymbol{K}$ 是 $\boldsymbol{F}$ 的扩域且 $\boldsymbol{K} = \boldsymbol{F}(\alpha)$ 而 $m(X)$ 是 α 在 $\boldsymbol{F}$ 上的极小多项式.

证明 先设 α 是 $\boldsymbol{F}$ 上的代数元，设 $m(X)$ 是 α 在 $\boldsymbol{F}$ 上的极小多项式，记 $d = \deg m(X)$. 作同态

$$\tau: \quad \boldsymbol{F}[X] \to \boldsymbol{F}(\alpha), f(X) \mapsto f(\alpha).$$

若 $f(\alpha) = 0$，作欧氏除法 $f(X) = m(X)q(X) + r(X), \deg r(X) < d$. 则 $r(\alpha) = f(\alpha) - m(\alpha)q(\alpha) = 0$，由极小多项式的定义 $r(X) = 0$，故 $f(X) = m(X)q(X)$. 反之，如果 $f(X)$ 是 $m(X)$ 的倍式，则显然 $f(\alpha) = 0$. 所以 $\ker(\tau) = \langle m(X)\rangle$. 由环同态基本定理，得到 $\boldsymbol{F}[X]/\langle m(X)\rangle \cong \boldsymbol{F}(\alpha)$.

对剩余类环 $\boldsymbol{F}[X]/\langle m(X)\rangle$，把 $f(X)$ 所在剩余类记作 $\overline{f}(X)$，则 $\boldsymbol{F} \to \boldsymbol{F}[X]/\langle m(X)\rangle, \lambda \mapsto \overline{\lambda}$ 是单同态. 所以可以把 $\boldsymbol{F}$ 嵌入 $\boldsymbol{F}[X]/\langle m(X)\rangle$ 作为子域. 特别是，$\boldsymbol{F}[X]/\langle m(X)\rangle$ 可作为 $\boldsymbol{F}$ 上的向量空间. 在 $\boldsymbol{F}[X]/\langle m(X)\rangle$ 中任一剩余类有惟一一个次数小于 $d = \deg m(X)$ 的代表多项式，因此 $1, \overline{X}, \cdots, \overline{X}^{d-1}$ 是 $\boldsymbol{F}$- 向量空间 $\boldsymbol{F}[X]/\langle m(X)\rangle$ 的基底. 于是得到 $|\boldsymbol{F}(\alpha):\boldsymbol{F}| = d = \deg m(X)$；而且 $\boldsymbol{F}(\alpha)$ 中的任何元 β 可以惟一地写成线性组合 $\beta = \sum_{i=0}^{d-1} \lambda_i \alpha^i$.

反之，设 $m(X)$ 是 $\boldsymbol{F}$ 上的不可约多项式，由上面的论证，只需指出 $\boldsymbol{F}[X]/\langle m(X)\rangle$ 是域就可完成证明. 但 $\boldsymbol{F}[X]/\langle m(X)\rangle$ 中的任何剩余类有惟一次数小于 $d = \deg m(X)$ 的代表多项式 $f(X)$. 因为 $m(X)$ 不可约，如果 $f(X) \neq 0$，则它就与 $m(X)$ 互素. 所以就有

$g(X)$ 和 $h(X)$ 使得 $f(X)g(X)+m(X)h(X)=1$，即是说

$$f(X)g(X)\equiv 1\ (\mathrm{mod}\, m(X)).$$

换言之，在 $\boldsymbol{F}[X]/\langle m(X)\rangle$ 中 $f(X)$ 是可逆元. □

5.3.4 推论　α 是 $\boldsymbol{F}$ 上的代数元当且仅当 $|\boldsymbol{F}(\alpha):\boldsymbol{F}|<\infty$.

证明　如果 α 是 $\boldsymbol{F}$ 上的代数元，由定理 5.3.3 就有 $|\boldsymbol{F}(\alpha):\boldsymbol{F}|<\infty$. 反之，设 $|\boldsymbol{F}(\alpha):\boldsymbol{F}|<\infty$，则存在 d 使得 $1,\alpha,\cdots,\alpha^d$ 在 $\boldsymbol{F}$ 上线性相关，即存在不全为零的 $\lambda_0,\lambda_1,\cdots,\lambda_d\in\boldsymbol{F}$ 使得 $\sum_{i=0}^{d}\lambda_i\alpha^i=0$. 即：非零 $\boldsymbol{F}$- 多项式 $\sum_{i=0}^{d}\lambda_i X^i$ 零化 α.

进一步我们要指出具有相同极小多项式的单扩张彼此同构. 下一推论更能说明这类问题.

5.3.5 推论　设 $\varphi:\boldsymbol{F}\to\boldsymbol{F}'$ 是域同构. 那么 φ 诱导环同构 $\tilde{\varphi}:\boldsymbol{F}[X]\to\boldsymbol{F}'[X]$，记 $f(X)\in\boldsymbol{F}[X]$ 在 $\tilde{\varphi}$ 之下的像为 $\varphi f(X)\in\boldsymbol{F}'[X]$. 再设 $\boldsymbol{K}=\boldsymbol{F}(\alpha),\boldsymbol{K}'=\boldsymbol{F}'(\alpha')$，设 $m(X)$ 是 α 在 $\boldsymbol{F}$ 上的极小多项式，而 $\varphi m(X)$ 是 α' 在 $\boldsymbol{F}'$ 上的极小多项式. 则 φ 可扩张为域同构 $\varphi_\alpha:\boldsymbol{K}\to\boldsymbol{K}'$.

证明　$\tilde{\varphi}$ 诱导剩余环的同构

$$\boldsymbol{F}[X]/\langle m(X)\rangle\xrightarrow{\cong}\boldsymbol{F}'[X]/\langle\varphi m(X)\rangle,\ \overline{f(X)}\mapsto\overline{\varphi f(X)}$$

而由定理 5.3.3 有 $\boldsymbol{K}=\boldsymbol{F}[\alpha]\cong\boldsymbol{F}[X]/\langle m(X)\rangle$ 和 $\boldsymbol{K}'=\boldsymbol{F}'[\alpha']\cong\boldsymbol{F}'[X]/\langle\varphi m(X)\rangle$；所以，$\varphi_\alpha:\boldsymbol{F}(\alpha)\to\boldsymbol{F}'(\alpha'),\varphi_\alpha(f(\alpha))=\varphi f(\alpha')$ 是同构. □

以下概念属重要的基本知识.

5.3.6 定义　设 $\boldsymbol{F}$ 是域，$f(X)\in\boldsymbol{F}[X],\deg f(x)=n\geqslant 1$. 说 $\boldsymbol{K}$ 是 $f(X)$ 在 $\boldsymbol{F}$ 上的分裂域如果扩域 $\boldsymbol{K}$ 满足：

(1) 在 $\boldsymbol{K}[X]$ 中 $f(X)=\lambda_0(X-\alpha_1)\cdots(X-\alpha_n)$，即在 $\boldsymbol{K}$ 中 $f(X)$ 恰有 n 个根；

(2) $\boldsymbol{K}=\boldsymbol{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

5.3.7 定理　（分裂域的存在与惟一性）　记号如上. $f(X)$

在 $\boldsymbol{F}$ 上的分裂域$\boldsymbol{K}$ 存在.又若 $\boldsymbol{K}'$ 也是$f(X)$ 在 $\boldsymbol{F}$ 上的分裂域,则有域同构 $\varphi:\boldsymbol{K}\to\boldsymbol{K}'$ 使得$\varphi(\lambda)=\lambda,\forall\lambda\in\boldsymbol{F}$.

由于技术上的原因,对于惟一性我们证明下述更广的形式.

命题 设 $\tau:\boldsymbol{F}\to\boldsymbol{F}'$ 是域同构,$f(X)\in\boldsymbol{F}[X]$ 而 $\tau f(X)\in\boldsymbol{F}'[X]$ (符号见 定义5.3.6).如果 $\boldsymbol{K}$ 是$f(X)$ 在 $\boldsymbol{F}$ 上的分裂域,而 $\boldsymbol{K}'$ 是 $\tau f(X)$ 在 $\boldsymbol{F}'$ 上的分裂域,则 τ 可扩张为域同构 $\varphi:\boldsymbol{K}\to\boldsymbol{K}'$.

证明 对 $n=\deg f(X)$ 进行归纳.$n=1$ 显然成立;此时只能是 $\boldsymbol{K}=\boldsymbol{K}'=\boldsymbol{F}$.

下设 $n>1$.令 $p(X)\in\boldsymbol{F}[X]$ 是 $f(X)$ 的一个素因式,$f(X)=p(X)q(X)$.由定理5.3.3,$\boldsymbol{E}=\boldsymbol{F}[X]/\langle p(X)\rangle=\boldsymbol{F}(\alpha_1)$ 是 $\boldsymbol{F}$ 的扩域,其中 $\alpha_1=\overline{X}\in\boldsymbol{E}$ 是$f(X)$ 的一个根;故在 $\boldsymbol{E}[X]$ 中有

$$f(X)=(X-\alpha_1)\cdot f_1(X),\quad \deg f_1(X)=n-1.$$

由归纳法,$f_1(X)$ 在 $\boldsymbol{E}$ 上的分裂域$\boldsymbol{K}$ 存在;它使得

$f(X)=\lambda_0(X-\alpha_1)\cdots(X-\alpha_n)$, 在 $\boldsymbol{K}[X]$ 中;

$\boldsymbol{K}=\boldsymbol{E}(\alpha_2,\alpha_3,\cdots,\alpha_n)=\boldsymbol{F}(\alpha_1)(\alpha_2,\alpha_3,\cdots,\alpha_n)=\boldsymbol{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)$;

即 $\boldsymbol{K}$ 是$f(X)$ 在 $\boldsymbol{F}$ 上的分裂域.

再证明命题成立.由 $\boldsymbol{K}'$ 是$\tau f(X)$ 在 $\boldsymbol{F}'$ 上的分裂域,有

$$\tau f(X)=\lambda_0'(X-\alpha_1')\cdots(X-\alpha_n'),\quad \text{在 } \boldsymbol{K}'[X] \text{ 中},$$

$$\boldsymbol{K}'=\boldsymbol{F}'(\alpha_1',\alpha_2',\cdots,\alpha_n').$$

而 $\tau f(X)=\tau p(X)\cdot\tau q(X)$,故 $\alpha_1',\alpha_2',\cdots,\alpha_n'$ 中有 $\tau p(X)$ 的根,不妨设 α_1' 是$\tau p(X)$ 的根.那么 $p(X)$ 是 α_1 在 $\boldsymbol{F}$ 上的极小多项式,而 $\tau p(X)$ 是 α_1' 在$\boldsymbol{F}'$ 上的极小多项式.由推论 5.3.5 知 τ 可扩张成域同构 $\tau_{\alpha 1}:\boldsymbol{F}(\alpha_1)\to\boldsymbol{F}'(\alpha_1')$.那么,由于 $\boldsymbol{K}$ 是$f_1(X)$ 在 $\boldsymbol{F}(\alpha_1)$ 上的分裂域,而且类似地,$\boldsymbol{K}'$ 是$\tau f_1(X)$ 在 $\boldsymbol{F}'(\alpha_1')$ 上的分裂域,按归纳法,τ_{α_1} 可扩张为域同构 $\varphi:\boldsymbol{K}\to\boldsymbol{K}'$. □

某些对于复数域有用的知识对于任意的域也对.如多项式重根判断法则(见本节习题 5).

以下专门讨论有限域,即总设 $\boldsymbol{F}$ 是有限域,$\boldsymbol{F}^*$ 是它的乘群.

5.3.8 引理　设$|F|=q$，K是F的有限扩域，则$|K|=q^m$.

证明　由5.3.1(c)，K是F上的m维向量空间，故$|K|=q^m$. □

5.3.9 推论　设$\mathrm{char}F=p$，则$q=|F|=p^l$.

证明　由5.3.1(b)，F是$\mathbb{Z}_p$的有限扩域，故$|F|=p^l$. □

5.3.10 推论　设$q=|F|=p^l$，则F^*是阶为$q-1=p^l-1$的循环群.

证明见5.3.1(d). □

下面是本节的主要定理.

5.3.11 定理　设$|F|=q=p^l$.则对于任意正整数m，域F的m次扩域存在并且在同构意义下惟一，它就是多项式$X^{q^m}-X$在F上的分裂域，而它的q^m个元恰为此多项式的全部根.

证明　若K是F的m次扩域，则$|K|=q^m$，于是K^*是q^m-1阶的循环群，由Lagrange定理，K^*的所有元满足方程$X^{q^m-1}-1=0$；因而K的所有q^m个元恰为多项式$X^{q^m}-X$的全部根.由分裂域的定义，K是$X^{q^m}-X$在F上的分裂域.惟一性获证.

对于存在性，由定理5.3.7，$X^{q^m}-X$在F上的分裂域K存在.因为$X^{q^m}-X$与其导出的多项式互素，所以此多项式无重根.由分裂域的定义，K包含此多项式的全部根，它们构成K的q^m元子集R.显然，$0,1\in R$；对$\alpha,\alpha'\in R$有

$$(\alpha+\alpha')^{q^m}=\alpha^{q^m}+\alpha'^{q^m}=\alpha+\alpha',\ \text{即}\ \alpha+\alpha'\in R;$$

$$(\alpha\cdot\alpha')^{q^m}=\alpha^{q^m}\cdot\alpha'^{q^m}=\alpha\cdot\alpha',\ \text{即}\ \alpha\cdot\alpha'\in R;$$

又若$\alpha\neq 0$则$(\alpha^{-1})^{q^m}=(\alpha^{q^m})^{-1}=\alpha^{-1}$，即$\alpha^{-1}\in R$.所以$R$是$K$的子域.再由以上推理，$F$的所有元恰为$X^q-X$的全部根，而$X^q-X\,|\,X^{q^m}-X$；故$F\subseteq R$.那么按分裂域的定义，$R$是$X^{q^m}-X$在$F$上的分裂域.由分裂域的惟一性得$R=K$；于是$|K|=q^m$，

即 K 是 F 的 m 次扩域. □

5.3.12 推论 设 p 为素数，l 为正整数. 则 p^l 阶的有限域存在并且在同构意义下惟一，它是多项式 $X^{p^l}-X$ 在 p 阶域 $\mathbb{Z}_p$ 上的分裂域，它的 p^l 个元恰为此多项式的全部根. □

5.3.13 注解 因此，以下我们恒以 F_q 记阶为 $q=p^l$ 的有限域. 特别地，$F_p=\mathbb{Z}_p$. 那么 F_p 的元素可表示为 $0,1,\cdots,p-1$. 一般的有限域 F_{p^l} 的元素可有两种表示方法.

写法一：F^* 是 p^l-1 阶的循环群，有生成元 β，它是 p^l-1 次本原单位根. 那么 $F_{p^l}=\{0,1=\beta^0,\beta,\beta^2,\cdots,\beta^{p^l-2}\}$.

写法二：令 β 如上. β 在 F_p 上的极小多项式必为 l 次多项式：$\lambda_0+\lambda_1X+\cdots+\lambda_{l-1}X^{l-1}+X^l$；那么 $1,\beta,\cdots,\beta^{l-1}$ 构成 F_{p^l} 作为 F_p 上的向量空间的基底. 于是，F_{p^l} 的元 α 惟一地写成 $1,\beta,\cdots,\beta^{l-1}$ 的以 F_p 为系数的线性组合；其组合系数（即 α 的坐标）为长 l 的 F_p- 序列，这便于计算机处理.

5.3.14 命题 $F_{q^m}\subseteq F_{q^n}\Longleftrightarrow m\mid n\Longleftrightarrow q^m-1\mid q^n-1$.

证明见本节习题 8. □

5.3.15 引理 设 $p(X)\in F_q[X]$ 是素多项式，$\deg p(X)=m$. 则

(1) F_{q^m} 是 $p(X)$ 在 F_q 上的分裂域；

(2) $p(X)\mid X^{q^k}-X\Longleftrightarrow m\mid k$.

证明 (1) 由定义 5.3.2 知有扩域 $F_q(\alpha)$ 使得 α 为 $p(X)$ 的根，并且 $|F_q(\alpha):F_q|=m$；故 $F_q(\alpha)=F_{q^m}$. 由定理 5.3.11，α 是 $p(X)$ 和 $X^{q^m}-X$ 的公共根，所以 $p(X)$ 和 $X^{q^m}-X$ 不互素；但 $p(X)$ 是 F_q 上的素多项式，故 $p(X)\mid X^{q^m}-X$. 由定理 5.3.11，$p(X)$ 的根全在 F_{q^m} 中. 按定义即知，$F_q(\alpha)=F_{q^m}$ 是 $p(X)$ 在 F_q 上的分裂域.

(2) $p(X)\mid X^{q^k}-X$ 当且仅当 $\boldsymbol{F}_{q^k}$ 包含 $p(X)$ 的全部根，当且仅当 $\boldsymbol{F}_{q^m}\subseteq\boldsymbol{F}_{q^k}$，由命题 5.3.14，当且仅当 $m\mid k$. □

5.3.16 定理　设 $q=p^l$，$\gcd(n,p)=1$. 设在模 n 剩余系的乘群 $\mathbb{Z}_n^*$ 中剩余类 $\bar{q}$ 的阶为 m. 则 $\boldsymbol{F}_{q^k}$ 含 n 次本原单位根 ω 当且仅当 $m\mid k$. 此时，ω 在 $\boldsymbol{F}_q$ 上的极小多项式次数为 m.

证明　$\boldsymbol{F}_{q^k}$ 含 n 次本原单位根 ω 当且仅当乘群 $\boldsymbol{F}_{q^k}^*$ 含 n 阶元，当且仅当 $n\mid q^k-1$，当且仅当 $q^k\equiv 1(\bmod n)$，当且仅当 $m\mid k$. 另一方面，$\boldsymbol{F}_{q^k}$ 含 n 次本原单位根 ω 当且仅当 $\boldsymbol{F}_{q^k}\supseteq\boldsymbol{F}_q(\omega)$ 由此可知，$\boldsymbol{F}_{q^m}$ 是含 ω 的 $\boldsymbol{F}_q$ 的最小扩域，即 $\boldsymbol{F}_{q^m}=\boldsymbol{F}(\omega)$. □

如同在上一节末尾提到的，最后作为应用实例，我们分析稍长一点的循环码.

5.3.17 例　取 $q=2,n=7$，则 $\boldsymbol{F}_2$ 上的长 7 的循环码由 X^7-1 在 $\boldsymbol{F}_2[X]$ 中的因子全部确定. 据定理 5.3.11 知 X^7-1 的全部根正好是 $\boldsymbol{F}_8^*$ 的全部元，故除 1 以外 X^7-1 的每个根 ω 都是 F_8^* 的生成元，即 $\boldsymbol{F}_2(\omega)=\boldsymbol{F}_8$；而 $|\boldsymbol{F}_8:\boldsymbol{F}_2|=3$；由此知道 X^7-1 的素因式除 $X-1$ 以外都是 3 次的. 所以 X^7-1 的素因式分解如下.

$$X^7-1=(X-1)(X^3+X^2+1)(X^3+X+1).$$

因此全部长度 7 的二元循环码如下(共有 8 个)：

C_0：生成多项式 X^7-1，零码(只含零向量，对应于零理想)；

C_1：生成多项式 1，单位码(即所有字都是码字，对应单位理想)；

C_2：生成多项式 $X-1$，一个[7,6,2]码，是方程 $x_0+x_1+\cdots+x_6=0$ 的解空间；

C_3：生成多项式 X^3+X^2+1，一个[7,4,3]Hamming 码；

C_3'：生成多项式 X^3+X+1，实际上与上面的 C_3 同构；

C_4：生成多项式 $X^6+X^5+X^4+X^3+X^2+X+1$，一个[7,1,7]码，即全 1 码；

C_5:生成多项式 X^4+X^2+X+1,一个[7,3,4]码;

C_6:生成多项式 $X^4+X^3+X^2+X+1$,一个[7,3,4]码,实际上与上面的 C_5 同构.

习题 5.3

1. 设 K 是 F 的扩域,则 K 是 F- 代数.

2. 证明维数公式 5.3.1(c).

3. 证明 5.3.1(e) 中的等式.

4. 证明一个域上的代数元的极小多项式一定是素多项式.

5. 设 F 是域,$f(X)\in F[X]$.设在其分裂域 K' 中 $f(X)=\lambda_0(X-\alpha_1)\cdots(X-\alpha_n)$,如果有 $\alpha_i=\alpha_j$,$i\neq j$,则称 $f(X)$ 有重根.证明 $f(X)$ 无重根,当且仅当 $f(X)$ 与它的导数多项式 $f'(X)$ 互素.

6. 设 F 是特征 p 的域,n 是正整数.证明:若 $\gcd(n,p)=1$,则 F- 多项式 X^n-1 无重根.否则它有重根.

7. 按注解 5.3.13 的两种方式写出 F_4 的所有元.

8. 证明命题 5.3.14.

9. 设 $q=p^l$,其中 p 是素数,$n=\dfrac{q^m-1}{q-1}$.证明本原 n 次单位根 ω 在 F_q 上的极小多项式的次数是 m,从而 $|F_q(\omega):F_q|=m$,$|F_q(\omega)|=q^m=p^{lm}$.

§5.4 有限域上的特征标

在 §4.4 中已经介绍了有限交换群的复特征标,并看到了它们的重要作用.这里我们用特征标来分析循环码,但不是复特征标而是有限域上的特征标,参看注解 4.4.2.对此,只需讨论 n 阶循环群的特征标.

5.4.1 假设 本节始终设 $G=\langle x\rangle$ 为 n 阶循环群.$F=F_q$

为 $q = p^l$ 的有限域，p 为素数，设 $\gcd(n, p) = 1$，则有正整数 m，使 $n \mid q^m - 1$. 令 $\boldsymbol{F}_{q^m}$ 是 $\boldsymbol{F}$ 的 m 次扩域，令 ω 是 $\boldsymbol{F}_{q^m}$ 中的本原 n 次单位根，从而 $1, \omega, \omega^2, \cdots, \omega^{n-1}$ 是全部的 n 次单位根.

注解　这里 m 的选取不惟一，但不会影响以下所有的推导.

5.4.2 定义　群 $G = \langle x \rangle$ 到 $\boldsymbol{F}_{q^m}^*$ 的一个群同态 $\psi: G \to \boldsymbol{F}_{q^m}^*$ 称为 G 的一个 $\boldsymbol{F}_{q^m}$- 线性特征标.

但注意，这里的特征标与第 4 章中的特征标表示不相同，那里是复特征标. 尽管如此，由于有本原 n 次单位根，很多基本结论却相同. 而且注意，有本原 n 次单位根这个条件蕴含着条件 $p \nmid n$ 即 $\gcd(n, p) = 1$，见本节习题 1. 为方便计，以下还是简称 $\boldsymbol{F}_{q^m}$- 特征标为特征标.

5.4.3 引理　群 $G = \langle x \rangle$ 恰有 n 个互不相同的特征标 ψ_i，$i = 1, 2, \cdots, n$ 它们使 $\psi_i(x) = \omega^i$，$i = 1, 2, \cdots, n$.

证明类似于引理 4.4.3 的证明. □

5.4.4 定义　令 $\langle \psi_i, \psi_j \rangle = \dfrac{1}{n} \sum\limits_{y \in G} \psi_i(y) \psi_j(y^{-1})$，称为 ψ_i 与 ψ_j 的内积.

5.4.5 定理　（正交关系）

$$\langle \psi_i, \psi_j \rangle = \begin{cases} 1, & \text{当 } i = j; \\ 0, & \text{否则.} \end{cases}$$

证明类似于定理 4.4.5 的证明. □

5.4.6 引理　对群 $G = \langle x \rangle$ 到 $\boldsymbol{F}_{q^m}^*$ 的一个群同态 $\psi: G \to \boldsymbol{F}_{q^m}^*$，存在惟一一个代数同态 $\bar{\psi}: \boldsymbol{F}G \to \boldsymbol{F}_{q^m}$ 使得 $\bar{\psi}|_G = \psi$；反之，一个代数同态 $\bar{\psi}: \boldsymbol{F}G \to \boldsymbol{F}_{q^m}$ 给出一个特征标 $\bar{\psi}|_G = \psi$，即令 $\psi(y) = \bar{\psi}(y)$，$\forall\, y \in G$，则 ψ 为 G 的一个特征标.

证明见命题 5.1.4 及其注解. □

5.4.7 引理　设 ψ_i 是群 $G = \langle x \rangle$ 的一个特征标，令 $\bar{\psi}_i$ 是如上面引理给出的代数同态，设 ω^i 在 $\boldsymbol{F}$ 上的极小多项式是 $p(X)$，则

$$\begin{aligned}\mathrm{Ker}(\bar{\psi}_t) &= \{f(x)p(x) \mid f(x) \in \boldsymbol{F}G\} \\ &= \{a(x) \in \boldsymbol{F}G \mid a(\omega^t) = 0\}.\end{aligned}$$

证明 将 $\boldsymbol{F}G$ 中的元素写成 x 的多项式 $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$，由于

$$\begin{aligned}\bar{\psi}_t(a(x)) &= \bar{\psi}_t\Big(\sum_{k=0}^{n-1} a_k x^k\Big) = \sum_{k=0}^{n-1} a_k \psi_t(x^k) \\ &= \sum_{k=0}^{n-1} a_k \omega^{tk} = a(\omega^t)\end{aligned}$$

故

$$\begin{aligned}a(x) \in \mathrm{Ker}(\bar{\psi}_t) &\Longleftrightarrow a(\omega^t) = 0 \\ &\Longleftrightarrow \omega^t \text{ 是 } a(X) \text{ 的根} \\ &\Longleftrightarrow a(X) \text{ 是 } \omega^t \text{ 的零化多项式} \\ &\Longleftrightarrow p(X) \mid a(X) \\ &\Longleftrightarrow \text{存在 } f(X) \in \boldsymbol{F}[X] \text{ 使得 } a(X) = f(X)p(X) \\ &\Longleftrightarrow \text{存在 } f(x) \in \boldsymbol{F}G \text{ 使得 } a(x) = f(x)p(x)\end{aligned}$$

□

注解 在引理 5.4.7 中，ω^t 的极小多项式 $p(X)$ 是 $\boldsymbol{F}[X]$ 中的不可约多项式，且 $p(X) \mid X^n - 1$. 故 $p(X)$ 的根都是 n 次单位根，因此可能有几个特征标都对应于同一个不可约多项式 $p(X)$.

当然，还可以用检验多项式来描述 $\mathrm{Ker}(\bar{\psi}_t)$，注意到 $X^n - 1 = p(X)q(X)$.

5.4.8 定理 任给 $G = \langle x \rangle$ 的 l 个特征标 $\psi_{t_1}, \psi_{t_2}, \cdots, \psi_{t_l}$，作矩阵

$$H = \begin{pmatrix} \psi_{t_1}(1) & \psi_{t_1}(x) & \cdots & \psi_{t_1}(x^{n-1}) \\ \psi_{t_2}(1) & \psi_{t_2}(x) & \cdots & \psi_{t_2}(x^{n-1}) \\ \vdots & \vdots & & \vdots \\ \psi_{t_l}(1) & \psi_{t_l}(x) & \cdots & \psi_{t_l}(x^{n-1}) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \omega^{t_1} & \cdots & \omega^{(n-1)t_1} \\ 1 & \omega^{t_2} & \cdots & \omega^{(n-1)t_2} \\ \vdots & \vdots & & \vdots \\ 1 & \omega^{t_l} & \cdots & \omega^{(n-1)t_l} \end{pmatrix}$$

考虑线性方程组(其中 $\xi_0, \xi_1, \cdots, \xi_{n-1}$ 表示未知元)$(\xi_0, \xi_1, \cdots, \xi_{n-1})H^{\mathrm{T}} = 0$ 在 $\boldsymbol{F}^n$ 中的解，则解子空间是群代数 $\boldsymbol{F}G$ 的理想 $\bigcap_{k=1}^{l} \mathrm{Ker}(\bar{\psi}_{t_k})$ 给出的循环码；进一步，其生成多项式是 $\omega^{t_1}, \omega^{t_2}, \cdots, \omega^{t_l}$ 在 $\boldsymbol{F}$ 上的极小多项式的最小公倍式.

反之，任给 $\boldsymbol{F}G$ 的一个理想 I，其生成多项式 $g(X) = p_1(X)p_2(X)\cdots p_l(X)$，每个 $p_k(X)$ 是 $\boldsymbol{F}[X]$ 中的不可约多项式，对每个 $p_k(X)$ 取一个根 ω^{t_k}，则可作矩阵 H 如上，则 $a(x) \in I$ 当且仅当 $(a_0, a_1, \cdots, a_{n-1})H^{\mathrm{T}} = 0$.

证明　由引理 5.4.7，对于任意 $a(X) \in \boldsymbol{F}[X]$

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathrm{Ker}(\bar{\psi}_{t_k})$$

$$\Longleftrightarrow (a_0, a_1, \cdots, a_{n-1}) \begin{pmatrix} \psi_{t_k}(x^0) \\ \psi_{t_k}(x^1) \\ \vdots \\ \psi_{t_k}(x^{n-1}) \end{pmatrix} = 0$$

所以

$$a(x) \in \bigcap_{k=1}^{l} \mathrm{Ker}(\bar{\psi}_{t_k}) \Longleftrightarrow (a_0, a_1, \cdots, a_{n-1})H^{\mathrm{T}} = 0$$

反之，$\forall\, a(x) = \sum_{i=0}^{n-1} a_i x^i \in \boldsymbol{F}G$

$$a(x) \in I \Longleftrightarrow g(X) \mid a(X)$$
$$\Longleftrightarrow p_k(X) \mid a(X), \forall\, k = 1, 2, \cdots, l$$
$$\Longleftrightarrow a(\omega^{t_k}) = 0, \forall\, k = 1, 2, \cdots, l$$

$$\Longleftrightarrow \sum_{j=0}^{n-1} a_j \omega^{ij} = 0, \forall\, k = 1,2,\cdots,l$$

$$\Longleftrightarrow (a_0, a_1, \cdots, a_{n-1}) H^{\mathrm{T}} = 0. \qquad \square$$

5.4.9 注解 (1) 定理 5.4.8 表明,循环码由循环群 $G = \langle x \rangle$ 的特征标完全决定,尽管定理中由特征标决定的矩阵 H 的元素不一定在 $\boldsymbol{F}$ 中(在其扩域中),为方便计,我们仍称 H 是检验矩阵,但应注意只有 $(\xi_0, \xi_1, \cdots, \xi_{n-1}) H^{\mathrm{T}} = 0$ 在 $\boldsymbol{F}^n$ 中的解才是循环码的码字.

(2) 定理 5.4.8 中对每个 $p_k(X)$ 中取一个根即可,若多取几个根构成矩阵 H,虽多了一些行,但相应的线性方程组在 $\boldsymbol{F}^n$ 中的解空间并未变化.

(3) 后面注解 5.4.11 与例 5.4.12 将给出一个办法,把矩阵 H 转化为 $\boldsymbol{F}$- 矩阵.

作为应用我们指出,在很多场合下,Hamming 码实际上是一种循环码.

5.4.10 定理 如果 $n = \dfrac{q^k - 1}{q - 1}$,而且 $\gcd(k, q-1) = 1$,令 ψ_1 是使得 $\psi_1(x) = \omega$ 的 G 的特征标,则以 $H = (\psi_1(x^0), \psi_1(x), \cdots, \psi_1(x^{n-1})) = (1, \omega, \cdots, \omega^{n-1})$ 为检验矩阵的 $\boldsymbol{F}G$ 的循环码是 Hamming 码. 特别是,二元 Hamming 码是循环码.

证明 首先注意 $\gcd(n, q-1) = \gcd(k, q-1)$,这是因为

$$\begin{aligned} n &= \frac{q^k - 1}{q - 1} = q^{k-1} + \cdots + q + 1 \\ &= (q-1)(q^{k-2} + 2q^{k-3} + \cdots + (k-1)) + k. \end{aligned}$$

所以 $\gcd(k, q-1) = 1$ 等价于 $\gcd(n, q-1) = 1$. 那么 $\omega^i \in \boldsymbol{F}$ 当且仅当 $\omega^{i(q-1)} = 1$,当且仅当 $n \mid i(q-1)$,当且仅当 $n \mid i$. 这表明对所有 $i = 1,2,\cdots,n-1$ 都有 $\omega^i \notin \boldsymbol{F}$. 利用这一点可证明 H 的任二列在 $\boldsymbol{F}$ 上线性无关. 事实上,如果 $\lambda\omega^i + \mu\omega^j = 0$,其中 $0 \leqslant i < j \leqslant n-1$,而 $\lambda, \mu \in \boldsymbol{F}$;则 $\omega^i(\lambda + \mu\omega^{j-i}) = 0$,即 $\lambda + \mu\omega^{j-i} = 0$;而 $0 < j - i < n - 1$,所以 $\omega^{j-i} \notin \boldsymbol{F}$,于是,$\lambda = \mu = 0$.

再由习题5.3.9，$|F(\omega):F| = k$，即 $F(\omega)$ 可作为 F 上的 k 维向量空间，它的一维子空间个数为 $\frac{q^k-1}{q-1} = n$ 个，见命题 4.3.11. 因而 H 的 n 列恰好分别是这 n 个一维子空间中的非零向量，由 Hamming 码的定义知，以 H 为检验矩阵的 FG 中的码是 Hamming 码. □

5.4.11 注解　在 $F(\omega)$ 中取一组 F- 基，就可把 $F(\omega)$ 中的每一个元写成 F 上的 k- 序列，把 ω^i 对应的 F 上长度为 k 的序列作为列向量，就给出了一个 F 上的 $k \times n$ 矩阵，它就是 §4.3 中的 Hamming 码在 F 上的检验矩阵.

5.4.12 例　取 $q=2, k=3$，则 $n = \frac{2^3-1}{2-1} = 7$，而 ω 是 $F_{2^3} = F_8$ 中的 7 次本原单位根，从而 $F_8 = F_2(\omega)$，按域的单扩张理论知，ω 的 F_2- 极小多项式 $m_\omega(X)$ 是一个 3 次多项式，$m_\omega(X) | X^7-1$，其中 $X^7-1 = (X-1)(X^6+X^5+\cdots+1) = (X+1)(X^3+X+1)(X^3+X^2+1)$，由于除 1 以外的其他 6 个 7 次单位根都是本原的，故上述分解为不可约分解，不妨假设 $m_\omega(X) = X^3+X+1$，即 $\omega^3+\omega+1=0$，故 $1, \omega, \omega^2$ 构成了 F_8 作为 F_2 上向量空间的基，下面对照写出 $\omega^0=1, \omega^1, \cdots, \omega^6$ 在这组基下的坐标.

$$\begin{matrix} \omega^0 = 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \end{matrix}$$

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

这就是例 4.3.14 中的二元的[7,4,3]Hamming 码的检验矩阵.

习题 5.4

1. 设 F 是特征 $p \neq 0$ 的域. 如果特征 $p \neq 0$ 的域 F 中含有本原 n 次单位根，则 $p \nmid n$. 反之，如果 $p \nmid n$，则 F 有有限扩域含有本

原 n 次单位根.

2. 求出所有的长度 4 的 3 元循环码.

3. 证明参数[4,2,3] 的 3 元 Hamming 码不是循环码.

4. 设 G 是 n 阶循环群,$|\boldsymbol{F}| = p^l, p \nmid n$. 设 ω 是本原 n 次单位根,其极小多项式是 $m(X)$,C 是以 $H = (1, \omega, \cdots, \omega^{n-1})$ 为检验矩阵的循环码. 证明:

(1) $\dim C = |\{0 \leqslant i < n \mid m(\omega^i) \neq 0\}|$.

(2) $\dim C^{\perp} = |\{0 \leqslant i < n \mid m(\omega^i) = 0\}|$.

§5.5 BCH 码

BCH 码是一种特殊的能纠多个错误的循环码.

5.5.1 记号 设 $G = \langle x \rangle$ 为 n 阶循环群,$\boldsymbol{F} = \boldsymbol{F}_q$ 为 q 阶有限域,$q = p^a$,p 为素数,且 $(n, p) = 1$,ω 为 $\boldsymbol{F}$ 的某个扩域中的 n 次本原单位根,$\psi_0, \psi_1, \cdots, \psi_{n-1}$ 是 G 的全部线性特征标,$\psi_i(x) = \omega^i$,$i = 0, 1, \cdots, n-1$.

5.5.2 定义 设 $l \geqslant 0, d \geqslant 2$ 为正整数,$l + d - 2 < n$,则由 G 的特征标 $\psi_l, \psi_{l+1}, \cdots, \psi_{l+d-2}$ 决定的 q- 元长 n 的 $\boldsymbol{F}G$ 的循环码称为设计距离为 d 的 BCH 码(也称为由 $\omega^l, \omega^{l+1}, \cdots, \omega^{l+d-2}$ 决定的 BCH 码),它的检验矩阵是

$$H = \begin{pmatrix} 1 & \omega^l & \omega^{2l} & \cdots & \omega^{(n-1)l} \\ 1 & \omega^{l+1} & \omega^{2(l+1)} & \cdots & \omega^{(n-1)(l+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{l+d-2} & \omega^{2(l+d-2)} & \cdots & \omega^{(n-1)(l+d-2)} \end{pmatrix}$$

特别地,若 $l = 1$,则称为狭义的 BCH 码.

若 $n = q^m - 1$,即 ω 是 $\boldsymbol{F}_{q^m}^*$ 的生成元,则称为本原 BCH 码.

BCH 码因发现者 R.C.Bose,D.K.Ray-Chaudhuri(1960) 和 A.Hocquenghem(1956) 而得名,设计距离则因下述结果而得名.

5.5.3 定理　设计距离为 d 的BCH码如果不是零码，则极小距离不小于 d.

证明　任取 H 的 $d-1$ 列：不妨设为第 $j_1, j_2, \cdots, j_{d-1}$ 列，并设 $0 \leqslant j_1 < j_2 < \cdots < j_{d-1} \leqslant n-1$，这 $d-1$ 列构成 $d-1$ 阶方阵，其行列式为

$$\det\begin{pmatrix} \omega^{j_1 l} & \omega^{j_2 l} & \cdots & \omega^{j_{d-1} l} \\ \omega^{j_1 (l+1)} & \omega^{j_2 (l+1)} & \cdots & \omega^{j_{d-1} (l+1)} \\ \vdots & \vdots & & \vdots \\ \omega^{j_1 (l+d-2)} & \omega^{j_2 (l+d-2)} & \cdots & \omega^{j_{d-1} (l+d-2)} \end{pmatrix}$$

$$= \omega^{j_1 l}\omega^{j_2 l}\cdots\omega^{j_{d-1} l} \cdot \det\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \omega^{j_1} & \omega^{j_2} & \cdots & \omega^{j_{d-1}} \\ \vdots & \vdots & & \vdots \\ \omega^{j_1 (d-2)} & \omega^{j_2 (d-2)} & \cdots & \omega^{j_{d-1} (d-2)} \end{pmatrix}$$

$$= \omega^{j_1 l}\omega^{j_2 l}\cdots\omega^{j_{d-1} l} \prod_{1 \leqslant \alpha < \beta \leqslant d-1} (\omega^{j_\beta} - \omega^{j_\alpha})$$

因 $0 \leqslant j_\alpha < j_\beta \leqslant n-1$，故上述行列式不等于零，因此，$H$ 的任意 $d-1$ 列线性无关，从而码的极小距离不小于 d. □

5.5.4 注解　(1) 若 $l \geqslant 1$，则 BCH 码不是零码，因为此时特征标 $\psi_l, \psi_{l+1}, \cdots, \psi_{l+d-2}$ 对应的单位根为 $\omega^l, \omega^{l+1}, \cdots, \omega^{l+d-2}$，其中任意一个不等于 1，相应的极小多项式 $p_l(X), \cdots, p_{l+d-2}(X)$ 都是 $X^{n-1} + X^{n-2} + \cdots + X + 1$ 的因式，故这些多项式的最小公倍式(即 BCH 码的生成多项式) 是 $X^{n-1} + X^{n-2} + \cdots + X + 1$ 的因式，特别地，这个生成多项式的次数小于 n，故维数大于等于 1.

(2) 在设计距离为 d 的 BCH 码的检验矩阵 H 中，如果将其每个元素都用 F_q^m 中的元素表示(即将 ω^i 看成是 F 上的 m 维列向量)，则得到一个 $m(d-1)$ 行的矩阵，但这些行不一定全都线性无关，故秩$(H) \leqslant m(d-1)$，从而生成矩阵 G 的秩为 $n -$ 秩$(H) \geqslant n - m(d-1)$，故得到 BCH 码的维数 $k \geqslant n - m(d-1)$.

(3) 由定义可知,若 $c(x)=\sum_{i=0}^{n-1}c_ix^i\in C$,则 $H^{\mathrm{T}}\cdot c=0$,或者说 $\sum_{i=0}^{n-1}c_i(\omega^j)^i=0, l\leqslant j\leqslant l+d-2$,亦即 $c(\omega^j)=0$,设 ω^l, $\omega^{l+1},\cdots,\omega^{l+d-2}$ 的极小多项式为 $p_l(X),\cdots,p_{l+d-2}(X)$,则上式表明 $p_l(X)\mid c(X),\cdots,p_{l+d-2}(X)\mid c(X)$,由于 $p_i(X)$ 不可约,因而 $p_l(X),\cdots,p_{l+d-2}(X)$ 的最小公倍式整除 $c(X)$,记它们的最小公倍式为 $\mathrm{lcm}(p_l(X),\cdots,P_{l+d-2}(X))$,即

$$\mathrm{lcm}(p_l(X),\cdots,p_{l+d-2}(X))\mid c(X).$$

由于 $c(X)=g(X)f(X)$,这里 $g(X)$ 是码 C 的生成多项式,特别地,$g(x)\in C$,故

$$\mathrm{lcm}(p_l(X),\cdots,p_{l+d-2}(X))\mid g(X).$$

换言之,$g(X)$ 以 ω 的 $d-1$ 个连续的方幂 $\omega^l,\omega^{l+1},\cdots,\omega^{l+d-2}$ 作为零点.

(4) BCH 码的极小距离可以真大于 d,如上节末的[7.4.3]Hamming 码,它实际上是 $l=1,d=2$ 的 BCH 码,其极小距离为 3,一般来说,确定一个 BCH 码的极小距离是一个困难的问题.

(5) 关于 BCH 码的覆盖半径也没有一般地确定.

5.5.5 例 构造长为 26,设计距离为 5 的三元 BCH 码.

解 由于 X^3+2X+1 在 $\boldsymbol{F}_3$ 不可约,故其生成 $\boldsymbol{F}_{27}$,如果 β 是一个本原元,它以 X^3+2X+1 作为其极小多项式,利用域的相关知识就能得到 β^2 的极小多项式 $(X-\beta^2)(X-\beta^6)(X-\beta^{18})=X^3+X^2+2$,类似地,$\beta^4$ 的极小多项式为 X^3+2X+2,这些多项式的积是一个包含 $\beta,\beta^2,\beta^3,\beta^4$ 为零点的多项式,因此它生成所求的码,即该码的生成多项式是 $g(X)=1+X+X^2+X^3+2X^4+X^6+2X^7+X^9$,码是 17 维,为[26,17,$\geqslant 5$]码.

以下我们介绍 BCH 码的译码.

Berlekamp 的译码算法原理:

为方便计，我们只考虑狭义BCH码，即 $l=1$ 的情形. 以下假设 $l=1$，设计距离 $d=2t+1$，即码 C 由单位根 $\omega,\omega^2,\cdots,\omega^{2t}$ 决定.

设 $c(x)\in C$，发送出去，接收到的是 $r(x)=r_0+r_1x+\cdots+r_{n-1}x^{n-1}$，那么错码是 $e(x)=r(x)-c(x)$. 设 $e(x)=e_0+e_1x+\cdots+e_{n-1}x^{n-1}$.

注意到接收者只知道 $r(x)$，我们的目的是由 $r(x)$ 求出 $c(x)$（实际上只需求出 $e(x)$）. 其给定的条件是：$e(\omega^i)=r(\omega^i)$，这是由于 $c(\omega^i)=0$.

为了准确地叙述算法，我们先给出几个概念.

令 $M=\{0\leqslant i\leqslant n-1\mid e_i\neq 0\}$ 称为错误发生的位置，$f=|M|$ 称为错误的个数，并恒设 $f\leqslant t$.

(5.5.6)
$$\sigma(z)=\prod_{i\in M}(1-\omega^i z),\text{称为错误探测多项式.}$$
$$\tau(z)=\sum_{i\in M}e_i\omega^i z\prod_{j\in M-\{i\}}(1-\omega^j z)$$

显然

(5.5.7)
$$\deg(\sigma(z))=f$$
$$\deg(\tau(z))\leqslant f.$$

$$k\in M\Longleftrightarrow\sigma(\omega^{-k})=0.$$

(5.5.8)
$$k\in M\Longrightarrow e_k=\frac{-\tau(\omega^{-k})\omega^k}{\sigma'(\omega^{-k})}$$

其中 $\sigma'(z)$ 是 $\sigma(z)$ 的导出多项式，且

$$\sigma'(z)=\sum_{i\in M}-\omega^i\prod_{j\in M-\{i\}}(1-\omega^j z)$$

因此译码归结为：

(5.5.9)　由 $r(x)$ 求出 $\sigma(z)$ 与 $\tau(z)$

现在计算 $\tau(z)$

$$\tau(z)=\sigma(z)\sum_{i\in M}e_i\frac{\omega^i z}{1-\omega^i z}=\sigma(z)\sum_{i\in M}e_i\omega^i z\sum_{t=0}^{\infty}(\omega^i z)^t$$

$$= \sigma(z)\sum_{i\in M}e_i\sum_{l=1}^{\infty}(\omega^i z)^l = \sigma(z)\sum_{l=1}^{\infty}\Big(\sum_{i\in M}e_i\omega^{il}\Big)z^l$$

注意到 $i \notin M$ 时，$e_i = 0$

$$\sum_{i\in M}e_i\omega^{il} = \sum_{i=0}^{n-1}e_i(\omega^l)^i = e(\omega^l) = r(\omega^l)$$

故

$$\tau(z) = \sigma(z)\cdot\sum_{l=1}^{\infty}r(\omega^l)z^l.$$

于是译码可进一步简化为：

(5.5.10) 由 $r(x)$ 求出 $\sigma(z)$

设 $\sigma(z) = \sigma_0 + \sigma_1 z + \cdots + \sigma_t z^t(\sigma_0 = 1)$，则

$$\tau(z) = \sigma(z)\sum_{l=1}^{\infty}r(\omega^l)z^l = \sum_{j=0}^{t}\sigma_j z^j\sum_{l=1}^{\infty}r(\omega^l)z^l$$

$$= \sum_{k=1}^{\infty}\Big(\sum_{j+l=k}\sigma_j r(\omega^l)\Big)z^k.$$

比较等式两边 z^k 的系数，由于 $\deg(\tau(z)) \leqslant f \leqslant t$，故 $k = t+1, t+2, \cdots, 2t$ 时，右边 z^k 的系数为零，由此我们得出 t 个等式

$$\sum_{j+l=k}\sigma_j r(\omega^l) = 0, 0 \leqslant j \leqslant t, k = t+1, t+2, \cdots, 2t.$$

即

(5.5.11) $$\sum_{j=0}^{t}\sigma_j r(\omega^{k-j}) = 0, k = t+1, t+2, \cdots, 2t$$

换言之，$(\sigma_0, \sigma_1, \cdots, \sigma_t)$ 是下述齐次线性方程组

(5.5.12) $$\sum_{i=0}^{t}r(\omega^{k-i})\xi_i = 0, k = t+1, t+2, \cdots, 2t$$

的解.

反之，任取方程组(5.5.12)的一解：$(\tilde{\sigma}_0, \tilde{\sigma}_1, \cdots, \tilde{\sigma}_t)$，其使得 $\tilde{\sigma}_0 = 1$，令 $\tilde{\sigma}(z) = \sum_{i=0}^{t}\tilde{\sigma}_i z^i$，则对 $k = t+1, t+2, \cdots, 2t$ 注意到

$1 \leqslant k - i \leqslant 2t$ 和 $r(\omega^{k-i}) = e(\omega^{k-i})$，则

$$0 = \sum_{i=0}^{t} r(\omega^{k-i})\tilde{\sigma}_i = \sum_{i=0}^{t} e(\omega^{k-i})\tilde{\sigma}_i$$

$$= \sum_{i=0}^{t}\left(\sum_{j=0}^{n-1} e_j\omega^{(k-i)j}\right)\tilde{\sigma}_i = \sum_{i=0}^{t}\left(\sum_{j\in M} e_j\omega^{(k-i)j}\right)\tilde{\sigma}_i$$

$$= \sum_{j\in M}\left(\sum_{i=0}^{t}\tilde{\sigma}_i(\omega^{-j})^i\right)e_j\omega^{kj} = \sum_{j\in M}\tilde{\sigma}(\omega^{-j})e_j\omega^{kj}$$

将 M 适当地加上指标使 M 扩充成 $M' = \{j_1, j_2, \cdots, j_t\}$，而 $e_{j_\alpha} = 0$，$\alpha = f+1, f+2, \cdots, t$，从而上面等式

$$0 = \sum_{j\in M}\tilde{\sigma}(\omega^{-j})e_j\omega^{kj}, k = t+1, t+2, \cdots, 2t$$

设 $0 \leqslant j_1 < j_2 < \cdots < j_t \leqslant n-1$，则 $\tilde{\sigma}(\omega^{-j_1})e_{j_1}, \cdots, \tilde{\sigma}(\omega^{-j_t})e_{j_t}$ 就是

$$\sum_{\alpha=1}^{t}\omega^{kj_\alpha}\xi_{j_\alpha} = 0$$

的解，这里 $k = t+1, t+2, \cdots, 2t$. 其系数行列式为

$$\det\begin{pmatrix} \omega^{(t+1)j_1} & \omega^{(t+1)j_2} & \cdots & \omega^{(t+1)j_t} \\ \omega^{(t+2)j_1} & \omega^{(t+2)j_2} & \cdots & \omega^{(t+2)j_t} \\ \vdots & \vdots & & \vdots \\ \omega^{2tj_1} & \omega^{2tj_2} & \cdots & \omega^{2tj_t} \end{pmatrix}$$

$$= \omega^{(t+1)(j_1+j_2+\cdots+j_t)} \cdot \det\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \omega^{j_1} & \omega^{j_2} & \cdots & \omega^{j_t} \\ \vdots & \vdots & & \vdots \\ \omega^{(t-1)j_1} & \omega^{(t-1)j_2} & \cdots & \omega^{(t-1)j_t} \end{pmatrix}$$

$$= \omega^{(t+1)(j_1+j_2+\cdots+j_t)} \prod_{1\leqslant\alpha<\beta\leqslant t}(\omega^{j_\beta} - \omega^{j_\alpha}) \neq 0$$

故上述方程组只有零解，则

$$\tilde{\sigma}(\omega^{-j_1})e_{j_1} = 0, \cdots, \tilde{\sigma}(\omega^{-j_t})e_{j_t} = 0$$

所以 $\tilde{\sigma}(\omega^{-j}) = 0, j \in M$，而 $\{\omega^{-j} \mid j \in M\}$ 是 $\sigma(z)$ 的全部根，故

$$\sigma(z) \mid \tilde{\sigma}(z).$$

据方程组(5.5.12),我们可得下述译码原理:

5.5.13 译码原理 取方程组(5.5.12)的解$(\tilde{\sigma}_0, \tilde{\sigma}_1, \cdots, \tilde{\sigma}_t)$,$t$已知,使$\tilde{\sigma}_0 = 1$,其中使$\tilde{\sigma}(z) = \tilde{\sigma}_0 + \tilde{\sigma}_1 z + \cdots + \tilde{\sigma}_t z^t$次数最低,此时的多项式即为$\sigma(z)$.

下面我们通过一个具体的例子来结束本节.

5.5.14 例 设ω是由$\omega^4 + \omega + 1 = 0$定义的$F_{2^4}$中的本原域元素,$\omega^{15} = 1, \omega^i \neq 1, 1 \leqslant i \leqslant 14$,设此时我们采用的是码长为15,设计距离为$d = 5$的狭义BCH码,且接收向量为

$$r(x) = 1 + x^2 + x^4 + x^7 + x^9 + x^{11} + x^{12} + x^{13} + x^{14}$$

下面我们采用Berlekamp译码法来译出这个向量.

解 此时$t = 2$,考虑方程组$\sum_{i=0}^{2} r(\omega^{k-i})\xi_i = 0, k = 3,4$的解,由于

$$r(\omega) = \omega, r(\omega^2) = \omega^2, r(\omega^3) = 0, r(\omega^4) = \omega^4$$

故此方程组为

$$\begin{cases} r(\omega^3)\xi_0 + r(\omega^2)\xi_1 + r(\omega)\xi_2 = 0 \\ r(\omega^4)\xi_0 + r(\omega^3)\xi_1 + r(\omega^2)\xi_2 = 0 \end{cases}$$

亦即

$$\begin{cases} \omega^2\xi_1 + \omega\xi_2 = 0 \\ \omega^4\xi_0 + \omega^2\xi_2 = 0 \end{cases} \Longleftrightarrow \begin{cases} \omega^2\xi_1 + \omega\xi_2 = 0 \\ \omega^4 + \omega^2\xi_2 = 0 \end{cases}$$

由此即得

$$\xi_2 = \omega^2, \xi_1 = \omega, \xi_0 = 1$$

将其写成

$$\sigma(z) = \prod_{j \in M}(1 - \omega^j z) = (1 - \omega^6 z)(1 - \omega^{11} z).$$

因此$r(x)$在第6个和第11个位置出错,由于其是二元码,只需将出错位置对应的0变为1,1变为0即可.故将$r(x)$译为

$$c(x) = 1 + x^2 + x^4 + x^6 + x^7 + x^9 + x^{12} + x^{13} + x^{14}.$$

习题 5.5

1. 设 $n = ab$，证明码长为 n、设计距离是 a 的二元狭义 BCH 码 C 的极小距离是 a.

2. 证明设计距离为 d、码长为 n 的 q 元 BCH 码是循环码，它的生成多项式是最小公倍式 $\mathrm{lcm}(m_1(X), m_2(X), \cdots, m_{d-1}(X))$，其中 $m_j(X)$ 是 $\alpha^j (1 \leqslant j \leqslant d-1)$ 的极小多项式.

3. 设 α 是 $\boldsymbol{F}_{2^5}$ 的一个本原元，满足 $\alpha^5 = \alpha^2 + 1$. 利用一个长为 31、设计距离为 5 的狭义 BCH 码进行编码. 设我们收到字

(1001　0110　1111　0000　1101　0101　0111　111)

试用 Berlekamp 译码法来译出这个字.

4. 求出所有码长为 7 的二元狭义本原 BCH 码.

§5.6　Reed-Solomon 码

由 §5.5 中的注解 5.5.4(3) 知道，BCH 码是由本原单位根 ω 的 $d-1$ 个接连的方幂 $\omega^l, \omega^{l+1}, \cdots, \omega^{l+d-2}$ 的极小多项式的最小公倍式为生成多项式的线性码.

BCH 码的一个最简单的实例，即 $n = q - 1$ 的情形，有许多重要的应用，我们在前面讨论的码都是纠正独立差错的纠错码，但有时信息在信道中传送或存储时，它的错误往往成区间出现，即连续几个位上的码元都发生差错，或连续几个位的码元除其中少数几个以外都发生差错，这在实际中是经常碰到的，如在将信息存储在磁带、磁盘的过程中就会碰到，因此讨论纠正成区间的差错的码是有意义的. 为了处理这样的一类错误，常常使用下面将要讨论的一类码来对信息进行编码.

5.6.1 定义　设 $n = q - 1$，ω 是一个 n 次本原单位根，记 $g(X)$ 为 $\omega^l, \omega^{l+1}, \cdots, \omega^{l+d-2}$ 的极小多项式的最小公倍式，则以 $g(X)$ 为生成多项式的循环码称为 $\boldsymbol{F}$ 上的一个设计距离为 d 的

Reed-Solomon 码(有时简称为 RS 码).

5.6.2 注解 (1) 在 RS 码的定义中,一般(但并不总是)取 $l = 1$.

(2) 由定义知,ω 是 $\boldsymbol{F}$ 的一个本原元,故 ω^i 的极小多项式是 $p_i(X) = X - \omega^i$,因而设计距离为 d 的 RS 码的生成多项式为 $g(X) = \prod_{i=l}^{d-1}(X - \omega^i)$,由定理 5.5.3,RS 码的极小距离不小于 d,其维数 $k = n - \deg(g(X)) = n - (d-1) = n - d + 1$;另一方面,由 Singleton 界,RS 码的极小距离不大于 $n - k + 1 = n - (n - d + 1) + 1 = d$,从而其极小距离就是 d,故其是一个 $[n, n-d+1, d]$ 码,因而 RS 码是一个最大距离可分码. 而且这进一步表明,当 $q > 2$ 时,非平凡的 MDS 码是存在的.

关于 RS 码与其对偶码,我们有下面的定理:

5.6.3 定理 RS 码的对偶码等价于 RS 码.

证明 设 ω 是 $\boldsymbol{F}$ 上的一个本原元,C 是由 $g(X) = (X - \omega^l)\cdots(X - \omega^{l+d-2})$ 生成的 RS 码,现考虑由 $g'(X) = (X - \omega^{l+d-1})(X - \omega^{l+d})\cdots(X - \omega^{q+l-1}) = (X - \omega^{l+d-1})\cdots(X-1)(X-\omega)\cdots(X - \omega^{l-1})$ 生成的 RS 码 C',因为 $g(X)g'(X) = X^n - 1$,这里 $n = q - 1$,由循环码的性质知道,由 $g'(X)$ 生成的码是 C 的对偶码(在码等价的意义下). □

以下我们简要地介绍 RS 码的编码.

设 C 是一个 $[n, k, d]$ RS 码,这里 $n = q - 1, d = n - k + 1$,设 $\boldsymbol{m} = (m_0, m_1, \cdots, m_{k-1}) \in \boldsymbol{F}^k$ 是一个信息向量,像通常一样,将它等同于 $m_0 + m_1 X + \cdots + m_{k-1}X^{k-1} = m(X)$,则可以将 $m(X)$ 编成如下的一个字 $\boldsymbol{c}$

$$\boldsymbol{c} = (c_0, c_1, \cdots, c_{n-1}) = (m(1), m(\omega), \cdots, m(\omega^{n-1}))$$

或者说 $c_i = \sum_{j=0}^{k-1} m_j(\omega^i)^j$,当然我们必须验证经过这样编码得到的一个字在 C 中,从而表明经过这样编码得到的一个码就是 RS 码,

由此我们只需证明多项式 $c(X)=\sum_{i=0}^{n-1}c_iX^i$ 有因子$(X-\omega^l)$,对于任意 $l\in\{1,2,\cdots,n-k\}$,换言之,只需验证 $c(\omega^l)=0$.由于

$$c(\omega^l)=\sum_{i=0}^{n-1}c_i(\omega^l)^i=\sum_{i=0}^{n-1}\sum_{j=0}^{k-1}m_j(\omega^i)^j(\omega^l)^i$$
$$=\sum_{j=0}^{k-1}m_j\sum_{i=0}^{n-1}(\omega^{j+l})^i=\sum_{j=0}^{k-1}m_j\sum_{i=0}^{q-2}(\omega^{j+l})^i.$$

注意到对于任意 j,l,只要 $j+l\neq q-1$,就有 $\omega^{j+l}\neq 1$.进一步,对于满足这样条件的 ω^{j+l}

$$\sum_{i=0}^{q-2}(\omega^{j+l})^i=\frac{1-(\omega^{j+l})^{q-1}}{1-\omega^{j+l}}=0.$$

因为 $0\leqslant j\leqslant k-1$,故当 $1\leqslant l\leqslant q-1-k=n-k$ 时,$1\leqslant l+j\leqslant q-2$,从而,$\omega^{l+j}\neq 1$,故对于任意 $l\in\{1,2,\cdots,n-k\}$,我们得到 $c(\omega^l)=0$.

对于 RS 码的译码,由于其是一类特殊的 BCH 码,故可采用 Berlamp 译码算法对其进行译码,也由于其是 BCH 码的特殊情况,其也有特殊的译码方法.下面我们简要介绍一下它的译码.

设 c 是形如上述编码得到的 RS 码的一个码字,经过信道传送后,接收到的向量为 $r=(r_0,r_1,\cdots,r_{n-1})$,设差错向量为 $e=(e_0,e_1,\cdots,e_{n-1})$,即 $r=c+e$,将其写成分量的形式,这样接收者知道下列方程

$$\begin{aligned}
r_0&=e_0+m_0+m_1+\cdots+m_{k-1}\\
r_1&=e_1+m_0+\omega m_1+\cdots+\omega^{k-1}m_{k-1}\\
&\vdots\\
r_{n-1}&=e_{n-1}+m_0+\omega^{n-1}m_1+\cdots+\omega^{(k-1)(n-1)}m_{k-1}
\end{aligned}$$

如果码字在传输中无差错,亦即接收向量无差错,此时将 $e=0$ 代入上面 n 个方程组成的方程组,由于系数矩阵是范德蒙矩阵,其任意 k 个方程联立都有解,该解向量 $m=(m_0,m_1,\cdots,m_{k-1})$ 即为

信息向量，按这种求解思路，共有$\binom{n}{k}$种选择方程组的方法得到正确的$\boldsymbol{m}$.

如果在传输的过程中有 t 个差错，亦即 $\boldsymbol{e} \neq 0$，此时若以 $e_0 = \cdots = e_{n-1} = 0$ 代入上述方程组，则得到 t 个方程是不对的（含有差错），而有 $n - t$ 个方程是正确的.

如果我们选择上述方程组中的 k 个方程来求解，则有$\binom{n-t}{k}$个子方程组可得到正确的$\boldsymbol{m}$. 进一步，一个给定的不正确的解不能够满足任何由 k 个正确的方程组成的子方程组，因此它至多是 $t + k - 1$ 个方程的解，由此，一个不正确的解至多从$\binom{t+k-1}{k}$个方程组中得到，因而如果选择这样的方程组联立求解后，将不能得到正确的信息 $\boldsymbol{m}$.

可以证明：如果 $t \leqslant \frac{d}{2}$，这里 $d = n - k + 1$ 为码的极小距离，则通过上述方程组，我们可以找出正确的信息，亦即上述译码方案可以纠正 $t \leqslant \frac{d}{2}$ 个错误.

习题 5.6

1 设 C 是一个$[n, k]$线性码，G 为 C 的一个生成矩阵，H 为 C 的一个奇偶检验矩阵，则以下三条件彼此等价.

(1) C 为 MDS 码；

(2) G 中任意 k 列都线性无关；

(3) H 中任意 $n - k$ 列都线性无关.

2. 设 ω 是 F_4 的一个生成元，并且满足 $\omega^2 + \omega + 1 = 0$. 给出码长为 $n = 3$，设计距离为 2 的 RS 码的一个生成多项式及生成矩阵，并写出它的全部码字.

§5.7　Goppa 码

回忆 §5.5 中关于 BCH 码的定义，我们知道，设计距离为 d、长为 n 的 BCH 码，其奇偶检验矩阵 H 是由循环群 $G=\langle x\rangle$ 的特征标 $\psi_l,\psi_{l+1},\cdots,\psi_{l+d-2}$ 决定的，这里 $\psi_i(x)=\omega^i$，而 ω 是 F_{q^m} 的一个 n 次本原单位根，并且 H 的每个元素可看做 F 上长为 m 的列向量. 本节将先对 BCH 码做进一步的分析，然后给出 BCH 码的一种推广形式，即所谓的 Goppa 码.

现在设 $(c_0,c_1,\cdots,c_{n-1})$ 是长为 n、设计距离为 d 的 BCH 码的一个码字，则由 BCH 码的定义知，$\sum_{i=0}^{n-1}c_i(\omega^j)^i=0,1\leqslant j<d$，这个形式将在例 5.7.3 以另外的方式表达出来，在此先做一些准备. 我们注意到

$$\frac{X^n-1}{X-\omega^{-i}}=\frac{X^n-(\omega^{-i})^n}{X-\omega^{-i}}=\sum_{k=0}^{n-1}X^k(\omega^{-i})^{n-1-k}$$
$$=\sum_{k=0}^{n-1}\omega^{i(k+1)}X^k$$

故得

$$\sum_{i=0}^{n-1}\frac{c_i}{X-\omega^{-i}}=\sum_{i=0}^{n-1}\frac{c_i}{X^n-1}\sum_{k=0}^{n-1}\omega^{i(k+1)}X^k$$
$$=\sum_{k=d-1}^{n-1}\frac{X^k}{X^n-1}\sum_{i=0}^{n-1}c_i\omega^{i(k+1)}$$
$$=\frac{X^{d-1}p(X)}{X^n-1}$$

这里 $p(X)$ 表示 F 上的某一多项式. 我们将这一思想进行推广，则可以得到另一类码 ——Goppa 码.

令 $g(X)$ 是系数取自 F_{q^m} 上的任一多项式，并定义 S_m 为

$$S_m=F_{q^m}[X]/\langle g(X)\rangle$$

S_m 表示 F_{q^m} 上的模 $g(X)$ 的剩余多项式环，显然，如果 $g(X)$ 是不

可约的,则 S_m 是一个域.

进一步,对于 $\alpha \in \boldsymbol{F}_{q^m}$,如果 $g(\alpha) \neq 0$,那么多项式 $X-\alpha$ 在 S_m 中可逆,为了说明这一点,用 $X-\alpha$ 去除 $g(X)$,得到

$$g(X) = q(X)(X-\alpha) + g(\alpha)$$

从而,$q(X)(X-\alpha) \equiv -g(\alpha)(\mathrm{mod} g(X))$,因此得到

$$[-g(\alpha)^{-1}q(X)](X-\alpha) \equiv 1(\mathrm{mod} g(X))$$

但

$$q(X) = \frac{g(X)-g(\alpha)}{X-\alpha}$$

因此进一步得

(5.7.1) 在 S_m 中,$\dfrac{1}{X-\alpha} = \dfrac{-1}{g(\alpha)}\left(\dfrac{g(X)-g(\alpha)}{X-\alpha}\right)$.

利用这一想法,能定义表达式 $\dfrac{1}{X-\alpha}$ 为 S_m 中如上式给出的多项式.现在能定义 Goppa 码.

5.7.2 定义 设 $g(X)$ 是 $\boldsymbol{F}_{q^m}$ 上的 t 次首项系数为一多项式,令 $L = \{\gamma_0, \gamma_1, \cdots, \gamma_{n-1}\} \subset \boldsymbol{F}_{q^m}$,满足 $|L| = n$,且 $g(\gamma_i) \neq 0$,$0 \leqslant i \leqslant n-1$,$n > \deg(g(X))$. 现在对于任意的字 $c = (c_0, c_1, \cdots, c_{n-1})$,$c_i \in \boldsymbol{F}_q$,设

$$Rc(X) = \sum_{i=0}^{n-1} \frac{c_i}{X-\gamma_i} \in S_m,$$

定义 q 元 Goppa 码 $\Gamma(L,g)$ 为

$$\Gamma(L,g) = \{c \in \boldsymbol{F}_q^n \mid R_c(X) \equiv 0 \bmod g(X)\}.$$

多项式 $g(X)$ 被称为 Goppa 多项式,如果 Goppa 多项式是不可约的,我们称 Goppa 码是不可约的.

显然,如上定义的码是一个线性码.

事实上,若 $(a_0, a_1, \cdots, a_{n-1}), (b_0, b_1, \cdots, b_{n-1}) \in \Gamma(L,g)$,则

$$\sum_{i=0}^{n-1} \frac{a_i}{X-\gamma_i} \equiv 0(\mathrm{mod} g(X)), \sum_{i=0}^{n-1} \frac{b_i}{X-\gamma_i} \equiv 0(\mathrm{mod} g(X)).$$

从而 $\sum_{i=0}^{n-1}\frac{a_i-b_i}{X-\gamma_i}\equiv 0(\mathrm{mod}g(X))$，且 $k\sum_{i=0}^{n-1}\frac{a_i}{X-\gamma_i}\equiv 0(\mathrm{mod}g(X))$，$\forall k\in \boldsymbol{F}$ 且关于线性空间的其他条件也满足，故 $\Gamma(L,g)$ 是线性码.

先看一个简单的例子.

5.7.3 例　若取 Goppa 多项式 $g(X)=X^{d-1}$，$L=\{\omega^{-i}\mid 0\leqslant i\leqslant n-1\}$，其中 ω 是 $\boldsymbol{F}_{q^m}$ 中的 n 次本原单位根，则得到的 Goppa 码 $\Gamma(L,g)$ 是设计距离为 d 的狭义的 BCH 码.

由定义知，Goppa 码是码长 $|L|=n$ 的线性码，以下找出其一个奇偶检验矩阵 H.

设 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})$ 是 $\Gamma(L,g)$ 的一个码字，根据定义

$$\sum_{i=0}^{n-1}\frac{c_i}{X-\gamma_i}\equiv 0(\mathrm{mod}g(X)),$$

利用式(5.7.1)，将其变形后得

$$\sum_{i=0}^{n-1}c_i\frac{g(X)-g(\gamma_i)}{X-\gamma_i}g(\gamma_i)^{-1}\equiv 0(\mathrm{mod}g(X)).$$

但因为

$$\deg\left(\frac{g(X)-g(\gamma_i)}{X-\gamma_i}\right)<\deg(g(X)),$$

这等价于

$$\sum_{i=0}^{n-1}c_i\frac{g(X)-g(\gamma_i)}{X-\gamma_i}g(\gamma_i)^{-1}=0. \tag{5.7.4}$$

为了计算上的方便，设 $g(X)=\sum_{i=0}^{t}g_iX^i$，这里 $g_t\neq 0$. 那么

$$\begin{aligned}\frac{g(X)-g(\gamma_i)}{X-\gamma_i}&=\sum_{j=0}^{t}g_j\frac{X^j-\gamma_i^j}{X-\gamma_i}\\&=\sum_{j=0}^{t}g_j\sum_{u=0}^{j-1}\gamma_i^{j-1-u}X^u.\end{aligned}$$

因此式(5.7.4)的左边等于

$$\sum_{i=0}^{n-1}c_i\left(\sum_{j=0}^{t}g_j\sum_{u=0}^{j-1}\gamma_i^{j-1-u}\right)g(\gamma_i)^{-1}X^u$$

$$= \sum_{i=0}^{n-1} c_i g(\gamma_i)^{-1} \sum_{u=0}^{t-1} \Big(\sum_{j=u+1}^{t} g_j \gamma_i^{j-1-u} \Big) X^u$$

$$= \sum_{u=0}^{t-1} \Big(\sum_{i=0}^{n-1} c_i g(\gamma_i)^{-1} \sum_{j=u+1}^{t} g_j (\gamma_i^{j-1-u}) \Big) X^u .$$

因此 $c \in \Gamma(L,g)$ 当且仅当

$$\sum_{i=0}^{n-1} c_i g(\gamma_i)^{-1} \sum_{j=u+1}^{t} g_j \gamma_i^{j-1-u} = 0 \tag{5.7.5}$$

对于所有的 $0 \leqslant u \leqslant t-1$. 我们将式(5.7.5)的左边看成矩阵的乘积

$$\Big(\sum_{j=u+1}^{t} g_j \gamma_0^{j-1-u}, \cdots, \sum_{j=u+1}^{t} g_j \gamma_{n-1}^{j-1-u} \Big) \cdot \begin{pmatrix} c_0 g(\gamma_0)^{-1} \\ c_1 g(\gamma_1)^{-1} \\ \vdots \\ c_{n-1} g(\gamma_{n-1})^{-1} \end{pmatrix}$$

$$= \Big(\sum_{j=u+1}^{t} g_j \gamma_0^{j-1-u}, \cdots, \sum_{j=u+1}^{t} g_j \gamma_{n-1}^{j-1-u} \Big) \cdot \begin{pmatrix} g(\gamma_0)^{-1} & 0 & \cdots & 0 \\ 0 & g(\gamma_1)^{-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & g(\gamma_{n-1})^{-1} \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

现在将其写成如下形式

$$\Big(\sum_{j=u+1}^{t} g_j \gamma_0^{j-1-u}, \cdots, \sum_{j=u+1}^{t} g_j \gamma_{n-1}^{j-1-u} \Big) \cdot G_1 \cdot c^{\mathrm{T}}$$

而

$$\Big(\sum_{j=u+1}^{t} g_j \gamma_0^{j-1-u}, \cdots, \sum_{j=u+1}^{t} g_j \gamma_{n-1}^{j-1-u} \Big)$$

$$= (g_{u+1} \quad \cdots \quad g_t \quad 0 \quad \cdots \quad 0) \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \gamma_0 & \gamma_1 & \cdots & \gamma_{n-1} \\ \vdots & \vdots & & \vdots \\ \gamma_0^{t-1} & \gamma_1^{t-1} & \cdots & \gamma_{n-1}^{t-1} \end{pmatrix}$$

可以写成

$$(g_{u+1} \quad \cdots \quad g_t \quad 0 \quad \cdots \quad 0) \cdot V$$

因此式(5.7.5)成立当且仅当

$$(g_{u+1} \quad \cdots \quad g_t \quad 0 \quad \cdots \quad 0) \cdot V \cdot G_1 \cdot \boldsymbol{c}^{\mathrm{T}} = 0$$

对于所有的 $0 \leqslant u \leqslant t-1$，当且仅当

$$\begin{pmatrix} g_t & 0 & 0 & \cdots & 0 \\ g_{t-1} & g_t & 0 & \cdots & 0 \\ g_{t-2} & g_{t-1} & g_t & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ g_1 & g_2 & g_3 & \cdots & g_t \end{pmatrix} \cdot V \cdot G_1 \cdot \boldsymbol{c}^{\mathrm{T}} = 0$$

但左边的矩阵是可逆矩阵，因此上式等价于

$$V \cdot G_1 \cdot \boldsymbol{c}^{\mathrm{T}} = 0$$

令

$$\begin{aligned} H &= V \cdot G_1 \\ &= \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \gamma_0 & \gamma_1 & \cdots & \gamma_{n-1} \\ \vdots & \vdots & & \vdots \\ \gamma_0^{t-1} & \gamma_1^{t-1} & \cdots & \gamma_{n-1}^{t-1} \end{pmatrix} \cdot \begin{pmatrix} g(\gamma_0)^{-1} & 0 & \cdots & 0 \\ 0 & g(\gamma_1)^{-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & g(\gamma_{n-1})^{-1} \end{pmatrix} \\ &= \begin{pmatrix} g(\gamma_0)^{-1} & g(\gamma_1)^{-1} & \cdots & g(\gamma_{n-1})^{-1} \\ \gamma_0 g(\gamma_0)^{-1} & \gamma_1 g(\gamma_1)^{-1} & \cdots & \gamma_{n-1} g(\gamma_{n-1})^{-1} \\ \gamma_0^2 g(\gamma_0)^{-1} & \gamma_1^2 g(\gamma_1)^{-1} & \cdots & \gamma_{n-1}^2 g(\gamma_{n-1})^{-1} \\ \vdots & \vdots & & \vdots \\ \gamma_0^{t-1} g(\gamma_0)^{-1} & \gamma_1^{t-1} g(\gamma_1)^{-1} & \cdots & \gamma_{n-1}^{t-1} g(\gamma_{n-1}^{-1}) \end{pmatrix} \end{aligned}$$

由此得到 $H \cdot \boldsymbol{c}^{\mathrm{T}} = 0$. 则其在某种意义上就是Goppa码的奇偶检验矩阵. 注意到 H 中的元素取值于 F_q^m，因此如果将 H 的每一个元素看做是 F 上的长为 m 的列向量，则其就是真正意义上的Goppa码的奇偶检验矩阵，由此即得以下定理.

5.7.6 定理 记号如上，长为 n，Goppa 多项式为 $\deg(g(X)) = t < n$ 的 Goppa 码 $\Gamma(L,g)$ 的维数 k 满足

$$n - mt \leqslant k \leqslant n - t$$

极小距离 $d \geqslant t + 1$.

证明 完全类似于 BCH 码，由奇偶检验矩阵的性质即可得到. □

对于二元 Goppa 码，其极小距离的界可以作进一步改进.

5.7.7 定理 设 $q = 2$，如果 $g(X)$ 在 $\boldsymbol{F}_2$ 的任何扩域中无重根，那么 $\Gamma(L,g) = \Gamma(L,g^2)$. 特别地，Goppa 码 $\Gamma(L,g)$ 的极小距离大于等于 $2t + 1$，其中 $t = \deg(g(X))$. 从而 Goppa 码 $\Gamma(L,g)$ 至少可以纠正 t 个错.

证明 设 $\boldsymbol{c} = (c_0, c_1, \cdots, c_{n-1})$ 是二元 Goppa 码 Γ 的一个重量为 w 的码字，不妨假设 $c_{i_1} = \cdots = c_{i_w} = 1$，定义

$$f(X) = \prod_{i=0}^{n-1}(X - \gamma_i)^{c_i}$$

因此

$$f(X) = \prod_{i=0}^{n-1}(X - \gamma_i)^{c_i} = \prod_{j=1}^{w}(X - \gamma_{i_j})$$

对 $f(X)$ 求其形式导数得

$$f'(X) = \sum_{j=1}^{w}\prod_{i \neq j}(X - \gamma_{i_j})$$

故

$$R_c(X) = \sum_{i=0}^{n-1}\frac{c_i}{X - \gamma_i} = \sum_{j=1}^{w}\frac{1}{X - \gamma_{i_j}} = \frac{f'(X)}{f(X)}$$

注意到 $f'(X)$ 和 $f(X)$ 在 $\boldsymbol{F}_2$ 的任何扩域中没有次数大于 1 的公共因式，即 $\gcd(f(X), f'(X)) = 1$，因此

$$\boldsymbol{c} \in \Gamma(L,g) \Longleftrightarrow g(X) \mid R_c(X) \Longleftrightarrow g(X) \mid f'(X)$$

因 $q = 2$，$f'(X)$ 中只有 X 的偶数次幂出现，即 $f'(X)$ 为一完全平方，换言之，存在某一个多项式 $h(X)$ 使得 $f'(X) = (h(X))^2 =$

$h(X^2)$，而且，由于 $g(X)$ 无重根，$f'(X)$ 为一完全平方式，故 $g^2(X)\mid f'(X)$，由此

$$c\in\Gamma(L,g)\Longleftrightarrow g(X)\mid R_c(X)\Longleftrightarrow g^2(X)\mid f'(X).$$

特别地，如果 $w(c)=w\neq 0$，则 $\deg(f'(X))\geqslant\deg(g^2(X))+1$，故 $\Gamma(L,g)$ 的极小距离大于等于 $2t+1$. □

一个二元 Goppa 码 $\Gamma(L,g)$ 如果其 Goppa 多项式无重根，则称为可分 Goppa 码.

5.7.8 例　设 $g(X)=X^2+1$，$L=(0,\omega,\omega^2,\omega^3,\omega^5,\omega^6)\subset \boldsymbol{F}_8$，这里 ω 是 $\boldsymbol{F}_8$ 的本原单位根，由此可得，$q=2,m=3,t=2$，根据定理5.7.7，$\Gamma(L,g)=\Gamma(L,X^2+1)=\Gamma(L,(X+1)^2)=\Gamma(L,X+1)$，由此即得 $n=6$，维数 $k\geqslant 6-3\times 1=6-3=3$，极小距离 $d\geqslant 3$. 进一步

$$H=\left(\frac{1}{0+1}\quad\frac{1}{\omega+1}\quad\frac{1}{\omega^2+1}\quad\frac{1}{\omega^3+1}\quad\frac{1}{\omega^5+1}\quad\frac{1}{\omega^6+1}\right)$$
$$=(1\quad\omega^4\quad\omega\quad\omega^6\quad\omega^3\quad\omega^5)$$

从而 $\Gamma(L,g)$ 的一个检验矩阵为

$$H=\begin{pmatrix}1&1&0&1&0&1\\0&1&1&0&1&1\\0&0&0&1&1&1\end{pmatrix}$$

故 $\Gamma(L,g)$ 是长为6，维数为3，极小距离为3的码.

关于 Goppa 码的译码.

在 §5.5 中，我们讨论了 BCH 码的 Berlekamp 译码算法，实际上这一方法也可以用于 Goppa 码的译码. 由于篇幅所限，这里就不再作详细的介绍了.

习题 5.7

1. 证明如果 H 是一个参数为 $[n,k]$ 的码 C 的奇偶检验矩阵，而 K 是一个 $k\times k$ 可逆矩阵，那么 KH 也是码 C 的奇偶检验矩阵.

2. 设 $g(X)=X^2+X+1$，$L=\{0,1,\omega,\cdots,\omega^6\}=\boldsymbol{F}_8$，$\omega$ 是

F_8 的本原元素.

(1) 证明 $g(X)$ 在 F_2 上不可约.

(2) 给出 Goppa 码 $\Gamma(L,g)$ 的一个奇偶检验矩阵.

3. 设 C 是一个码长为 15,生成矩阵为 $g(X)=X^2+X+1$ 的二元循环码,设 ω 是一个 15 次的本原单位根.

(1) 证明 ω^5 是 $g(X)$ 的一个根.

(2) 证明 C 是一个 BCH 码.

(3) 证明 C 的极小距离是 2.

(4) 证明 C 不是一个 Goppa 码.

习题答案与提示

第 1 章

习题 1.1

1. (1) $\alpha\beta = (1327546), \beta\alpha = (1653247), \alpha^{-1} = (264)(1753)$.

(2) 由(1) 可得例子.

2. $|\mathrm{Tran}(X)| = n^n$.

3 直接验证.

4. (1) $\mathbb{Q}$ 的单位元是 0,任意的 $a \in \mathbb{Q}$ 的逆元是 $-a$.

$\mathbb{Q}^*$ 的单位元是 1,任意的 $a \in \mathbb{Q}^*$ 的逆元是 $\frac{1}{a}$.

(2) 同理可证.

6. 如果 $(xy)^2 = x^2y^2$,则 $xyxy = xxyy$,等式两边分别左乘以 x^{-1},右乘以 y^{-1},得 $yx = xy$.

7. 对于任意 $x, y \in \bigcup_{i=1}^{\infty} H_i$,存在 H_i, H_j 使得 $x \in H_i, y \in H_j$,不妨设 $i \leqslant j$,则 $H_i \subset H_j$,从而 $xy^{-1} \in H_j \subset \bigcup_{i=1}^{\infty} H_i$.

8. 由 $1 \in Z(G)$ 知 $Z(G)$ 不是空集;对于任意的 $z_1, z_2 \in Z(G)$,有 $(z_1z_2^{-1})x = z_1(xz_2^{-1}) = x(z_1z_2^{-1})$,故 $z_1z_2^{-1} \in Z(G)$,从而 $Z(G) \leqslant G$. 又由 $Z(G)$ 的定义可知它是交换子群.

9. 假设群 $G = H \cup K$,这里 H, K 是群 G 的真子群;则存在 $x \in H - K$, $y \in K - H$,从而 $xy \in G - (H \cup K)$. 矛盾.

10. 直接验证.

11. (1) 可直接验证 $\equiv (\mathrm{mod}\ m)$ 是 $\mathbb{Z}$ 的等价关系. $a \equiv b\ (\mathrm{mod}\ m)$ 当且仅当 $m \mid (a - b)$,当且仅当存在 $k \in \mathbb{Z}$ 使得 $a - b = mk$,当且仅当

$a-b\in m\mathbb{Z}$.

(2) a 所在的等价类是

$[a]=\{b\in\mathbb{Z}\mid b\equiv a(\mathrm{mod}\ m)\}=\{b\in\mathbb{Z}\mid x\in\mathbb{Z}$使得$b-a=mx\}$
$=a+m\mathbb{Z}$.

(3) 显然

(4) 若$[a]=[a'],[b]=[b']$,则 $m\mid(a-a')$ 且 $m\mid(b-b')$,从而 $m\mid(a+b)-(a'+b')$,即$[a+b]=[a'+b']$

(5) 类似于(4)

(6) $[a]\in\mathbb{Z}_m^*$,即$(a,m)=1$,从而存在整数a',b使得$aa'+mb=1$,即$[a][a']=[1]$.

12 由消去律,映射 $X\to X,y\mapsto xy$ 是单射,从而是满射,故对于任意 x, y 有 u 使得$y=xu$,同理也有 z 使得$y=zx$ 特别地,可取 $x_0=x_0u_0$.把任意 x 写成$x=zx_0$,就有 $xu_0=x$.同理可找到 z_0,使得对于任意 x 有$z_0x=x$. 于是 $z_0=z_0u_0=u_0$ 是单位元 类似证逆元存在.

考虑 $X=\mathbb{Z}^*$为非零整数的集合,则 X 在整数乘法之下满足消去律但不成为群

习题 1.2

1 (1)$\Longrightarrow$(2): 设 $c\in aH\cap bH$,即 $c=ah_1=bh_2$ 其中 $h_1,h_2\in H$,对于任意的$ah\in aH$,$ah=bh_2h_1^{-1}h\in bH$,从而 $aH\subset bH$,同理可得 $bH\subset aH$.

(2) $\Longrightarrow$(3): 由 $aH=bH$, 得 $H=a^{-1}bH$,即 $a^{-1}b\in H$.

(3) $\Longrightarrow$(4): 由 $a^{-1}b\in H$,及 $H\leqslant G$ 知$(a^{-1}b)^{-1}=b^{-1}a\in H$

(4) $\Longrightarrow$(5): 由 $b^{-1}a\in H$ 知,存在 $h\in H$ 使得 $b^{-1}a=h$,即 $a=bh\in bH$

(5)$\Longrightarrow$(6): 由 $a\in bH$ 得, 存在 $h\in H$ 使得 $a=bh$, 即 $b=ah^{-1}\in aH$.

(6) $\Longrightarrow$(1): 由 $b\in aH$ 可得$bH=aH$,从而 $aH\cap bH\neq\varnothing$.

2. 设 $G=\bigcup\limits_{i\in I}Ha_i$ 是个右陪集分解,$H=\bigcup\limits_{j\in J}Kb_j$ 也是个右陪集分解,则 $G=\bigcup\limits_{i\in I}Ha_i=\bigcup\limits_{i\in I}(\bigcup\limits_{j\in J}Kb_j)a_i=\bigcup\limits_{(i,j)\in I\times J}Kb_ja_i$.由此只需证 Kb_ja_i 互不相同即可. 若 $Kb_ja_i=Kb_ra_s$,则 $HKb_ja_i=HKb_ra_s$,从而 $Ha_i=Ha_s$,$i=s$,故 $Kb_j=Kb_r$,$j=r$.于是$|G:K|=|I\times J|=|G:H|\cdot|H:K|$.

3. (1) $\Longrightarrow$(2): 若 $Hy=xH$,则 $y\in xH$ 从而$y=xh$,$h\in H$;故 yH

$= xH = Hy$.

(2) $\Longrightarrow$(3) $\Longrightarrow$(4):显然

(4) $\Longrightarrow$(1): $Hy = y(y^{-1}Hy) \subset yH$. 同理证 $yH \subset Hy$.

4 对于任意 $H \leqslant Z(G)$,任意 $x \in G$,有 $x^{-1}Hx = Hx^{-1}x = H$,故 H 是 G 的正规子群.

5 (1) $(ST)W = \{(st)w \mid s \in S, t \in T, w \in W\} = \{s(tw) \mid s \in S, t \in T, w \in W\} = S(TW)$.

(2) $(ST)^{-1} = \{(st)^{-1} \mid s \in S, t \in T\} = \{t^{-1}s^{-1} \mid s \in S, t \in T\} = T^{-1}S^{-1}$

(3) 因 $W \leqslant G$,得 $WS = \{ws \mid w \in W, s \in S\} \subset W$; 因 $1 \in S$, 得 $W = \{w1 \mid w \in W\} \subset WS$

(4) 若 $W^{-1} = W$ 且 $WW = W$, 则由 $w \in W$ 有 $w^{-1} \in W^{-1} = W$. 又若 $w_1, w_2 \in W$,则 $w_1w_2 \in WW = W$.

(5) 设 H 是正规子群,对于任意的两个陪集 xH, yH, 有 $(xH)(yH) = xy(y^{-1}Hy)H = xy(HH) = xyH$.

(6) $HK = \{hk \mid h \in H, k \in K\} = \{k(k^{-1}hk) \mid h \in H, k \in K\} = \{kh' \mid h' \in H, k \in K\} = KH$

6 设 H, K 是群 G 的两个正规子群, 则任意的 $g \in G$, $g^{-1}HKg = (g^{-1}Hg)(g^{-1}Kg) = HK$

7 (1) $f(1_G) = f(1_G^2) = f(1_G)^2$, 两边左乘 $f(1_G)^{-1}$, 得 $1_G = f(1_G)$.

(2) $1_G = f(1_G) = f(xx^{-1}) = f(x)f(x^{-1})$,故 $f(x^{-1}) = f(x)^{-1}$.

(3) 任意的 $x \in H \cdot \mathrm{Ker}(f)$, 则存在 $h \in H, y \in \mathrm{Ker}(f)$ 使得 $x = hy$, 从而 $f(x) = f(hy) = f(h)f(y) = f(h) \cdot 1_G = f(h) \in f(H)$, 即 $H \cdot \mathrm{Ker}(f) \subset f^{-1}(f(H))$

反之,若 $f(x) \in f(H)$,则存在 $h \in H$ 使得 $f(x) = f(h)$, 则 $f(h^{-1}x) = 1_G$, 故 $h^{-1}x \in \mathrm{Ker}(f)$.

(4) 仿照命题 1.2.14(1) 的证明.

(5) 对于任何 $x, y \in G'$, 我们有

$$\begin{aligned} f^{-1}(x) \cdot f^{-1}(y) &= (f^{-1}f(f^{-1}(x) \cdot f^{-1}(y))) \\ &= f^{-1}(f(f^{-1}(x) \cdot f^{-1}(y))) \\ &= f^{-1}(ff^{-1}(x) \cdot ff^{-1}(y)) = f^{-1}(x \cdot y). \end{aligned}$$

8. 作同态映射 ψ: $\mathbb{Z}\to\mathbb{Z}_m$; $m\to[m]$; 它显然是满射,且 $\mathrm{Ker}(\psi)=\{k\in\mathbb{Z}\mid\psi(k)=[0]\}=\{k\in\mathbb{Z}\mid[k]=[0]\}=\{k\in\mathbb{Z}\mid k=mq,q\in\mathbb{Z}\}=m\mathbb{Z}$.

9. 若 $h_iK=h_jK$, 则 $h_j^{-1}h_i\in H\cap K$,从而 $h_j(H\cap K)=h_i(H\cap K)$, 故 $HK=\cup_{i\in I}h_iK$ 是不交并. 由此

$$|HK|=|I|\cdot|K|=(|H|/|H\cap K|)\cdot|K|.$$

由于 $HK\subset G$, 故 $|G|\geqslant|HK|$, 从而有 $|G|\geqslant|HK|=(|H|\cdot|K|)/|H\cap K|$, 即 $|G:K|=|G|/|K|\geqslant|H|/|H\cap K|=|H:H\cap K|$,得证.

10. (1) 利用上题, $|G:H\cap K|=|G:H|\cdot|H:H\cap K|\leqslant|G:H|\cdot|G:K|$.

(2) 注意到 $|G:H|\mid|G:H\cap K|$ 和 $|G:K|\mid|G:H\cap K|$.

11 (1) 若 $1,1'$ 都是 R 的单位元,则 $1=1\cdot1'=1'$.

(2) 若 a',a'' 都是 a 的逆元,则 $a'=a'\cdot1=a'(aa'')=(a'a)a''=1\cdot a''=a''$.

(3) 显然 $1\in R^*$,若 a,b 可逆, 则 ab 也可逆, 且 a^{-1} 也可逆.

12. (1) 考虑 $\mathbb{Z}_m^*$,$[a]\in\mathbb{Z}_m^*$当且仅当$(a,m)=1$,而这样的 a 的个数是 $\varphi(m)$ 个 即 $|\mathbb{Z}_m^*|=\varphi(m)$,从而$[a]^{\varphi(m)}=[1]$,亦即 $a^{\varphi(m)}\equiv1\pmod m$.

(2) 令 $m=p$,此时 $\varphi(p)=p-1$

习题 1.3

1. 注意分正负情况讨论.

2. $(xy)^n=(xy)(xy)\cdots(xy)=x(yx)y\cdots(xy)=x(xy)y\cdots(xy)=x^ny^n$.

例如 S_3 中,$x=(12)$,$y=(13)$,有$(xy)^3=1$,$x^3y^3=(132)$.

3. (1) 设群 G 是 p 阶群, 任取 $1\neq g\in G$ 有 $\langle g\rangle\leqslant G$ 从而 $|\langle g\rangle|\mid|G|$,但$|G|$只有正因子 $1,p$,故$\langle g\rangle=G$.

(2) p 阶群G 的子群只有G和1,故 p 阶群G是交换单群,反之,若 G 是交换单群,任取 $1\neq g\in G$,设 $m=|g|$,令素数 $p\mid m$,则$\langle g^{m/p}\rangle$ 是 G 的 p 阶子群,因此是 p 阶正规子群.由 G 是单群,得$\langle g^{m/p}\rangle=G$.

4. $f(G)=\{f(g)\mid g\in G\}=\{f(a^m)\mid g=a^m\in G;\ m\in\mathbb{Z}\}=$

$\{f(a)^m \mid m \in \mathbb{Z}\}$，即 $f(G) = \langle f(a)\rangle$.

5 注意到$\langle S\rangle = \{s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n} \mid s_i \in S; a_i = \pm 1\}$

6. (1) 考虑自然满同态$\mathbb{Z} \to \mathbb{Z}_m, x \mapsto [x]$，则由习题1.2.7(3)，$\langle [a]\rangle$在$\mathbb{Z}$中的原像是$\langle a\rangle + \langle m\rangle = a\mathbb{Z} + m\mathbb{Z} = \gcd(a,m)\,\mathbb{Z}$. 由子群对应定理，$|\mathbb{Z}_m : \langle [a]\rangle| = |\mathbb{Z} : \gcd(a,m)\,\mathbb{Z}| = \gcd(a,m)$

(2) 由(1)即得

(3) 由(2)可得

7 (1) 设$|ab| = m$，$|a| = s$，$|b| = t$. 则$(ab)^n = a^n \cdot b^n = 1$，故$m \mid st$ 另一方面，$(ab)^{sm} = a^{sm} \cdot b^{sm} = b^{sm} = 1$，从而，$t \mid sm$. 但$(s,t) = 1$，故$t \mid m$ 类似地，$s \mid m$.

(2) 如 S_2 中，$a = (12), b = (12), ab = 1$，但$2 \cdot 2 / \gcd(2,2) = 2 \neq 1$.

8. (1) $a^n = 1$ 当且仅当$(a^{-1})^n = 1$.

(2) $a^n = 1$ 当且仅当$(bab^{-1})^n = 1$

(3) 注意到 $ab = b^{-1}(ba)b$，由(2)即得

9 (1) 分 $n = 0$，$n > 0$，$n < 0$ 三种情况讨论

(2) 设$|x| = m$，则 $x^m = 1, f(x)^m = f(x^m) = f(1) = 1$，则$|f(x)| < \infty$ 设$|f(x)| = k$，由 $f(x^m) = (f(x))^m = 1_H$，得 $k \mid m$.

10 设 $G = \langle g\rangle$、$H = \langle h\rangle$，若存在从 G 到 H 的全同态，不妨设 $f: G \to H$ 为全同态，则 $G/\mathrm{Ker}(f) \cong H$，若$|G| < \infty$，则$|\mathrm{Ker}(f)| < \infty$，从而$|H| = |G| / |\mathrm{Ker}(f)| < \infty$

反之，构造映射 $f: G \to H, g^r \mapsto h^r$，易证其为全同态.

11 设 $H = \left\langle \frac{a_1}{b}, \frac{a_2}{b}, \cdots, \frac{a_n}{b} \right\rangle$ 是$\mathbb{Q}$的一个有限生成子群(若这有限个有理数的分母不同，可以将它们变为相同的分母)，令 $d = \gcd(a_1, a_2, \cdots, a_n)$ 表示 $a_1, a_2, \cdots, a_n$ 的最大公约数，则 $H = \left\langle \frac{d}{b} \right\rangle$，因此 H 是循环群.

若$\mathbb{Q}$是一个循环群，设$\mathbb{Q} = \left\langle \frac{n}{m} \right\rangle$，其中$\frac{n}{m}$是有理数，此时$\mathbb{Q} = \left\langle \frac{n}{m} \right\rangle = \left\{ r\frac{n}{m} \,\middle|\, r \in \mathbb{Z} \right\}$，显然$\frac{1}{2m} \in \mathbb{Q}$，而$\frac{1}{2m} \notin \left\{ r\frac{n}{m} \,\middle|\, r \in \mathbb{Z} \right\}$，矛盾. 故$\mathbb{Q}$不是循环群

12. (1) 设$|x| > 2$，则可推出$|x^{-1}| > 2$，且 $x \neq x^{-1}$，即证.

(2) 用反证法,设$|G|=2k$,如果群G中没有2阶元,则任意的$1\neq g\in G,|g|>2$,由(1)知,$|G|=1+2m$,矛盾

13 $a^m=1$,故$\chi(a)^m=\chi(a^m)=\chi(1)=1$,从而$\chi(a)$是一个$m$次单位根,而所有$m$次是$1=\omega^0,\omega,\cdots,\omega^t,\cdots,\omega^{m-1}$.故存在惟一整数$k$满足$0\leqslant k<m$使得$\chi(a)=\omega^k$.

14. (1) 存在性:有整数k_1,k_2使得$k_1m_1+k_2m_2=1$,于是$a=a^{k_1m_1}a^{k_2m_2}$.令$a_1=a^{k_2m_2}$,$a_2=a^{k_1m_1}$ 惟一性:从$a=a_1'a_2'$可得$a^{k_1m_1}=(a_1')^{k_1m_1}(a_2')^{k_1m_1}=(a_2')^{k_1m_2}=a_2'$

(2) 对r用归纳法

习题 1.4

1 作映射$f:(G_1\times G_2)\times G_3\to G_1\times(G_2\times G_3);((g_1,g_2),g_3)\mapsto(g_1,(g_2,g_3))$,验证其为群同构

2. 易验证f是群同态

(1) $$\begin{aligned}\mathrm{Ker}(f)&=\{g\in G\mid f(g)=(1_{G_1},1_{G_2})\}\\&=\{g\in G\mid(f_1(g),f_2(g))=(1_{G_1},1_{G_2})\}\\&=\{g\in G\mid f_1(g)=1_{G_1},f_2(g)=1_{G_2}\}\\&=\{g\in G\mid g\in\mathrm{Ker}(f_1),g\in\mathrm{Ker}(f_2)\}\\&=\mathrm{Ker}(f_1)\cap\mathrm{Ker}(f_2)\end{aligned}$$

(2) 必要性:对于任意的$x\in G$,令$f_1(x)=a$.由f是满同态,存在一个$y\in G$使得$f(y)=(a,1_{G_2})$,即$f_1(y)=a$. $y\in\mathrm{Ker}(f_2)$ 从而,$f_1(xy^{-1})=1_{G_1}$,于是$xy^{-1}\in\mathrm{Ker}(f_1)$.故$x\in\mathrm{Ker}(f_1)\cdot\mathrm{Ker}(f_2)$.

充分性:对于任意$(a_1,a_2)\in G_1\times G_2$,由$f_i$是满同态,存在$x\in G$使得$f_1(x)=a_1$.但$G=\mathrm{Ker}(f_1)\cdot\mathrm{Ker}(f_2)$,有$y_1\in\mathrm{Ker}(f_1)$和$y_2\in\mathrm{Ker}(f_2)$使得$x=y_1y_2$,故$a_1=f_1(x)=f_1(y_1y_2)=f_1(y_1)f_1(y_2)=f_1(y_2)$.同理,存在$z_1\in\mathrm{Ker}(f_1)$使得$f_2(z_1)=a_2$ 那么$f(y_2z_1)=(f_1(y_2z_1),f_2(y_2z_1))=(a_1,a_2)$

(3) 例如,取$G=G_1=G_2\neq1$,取$f_1=f_2=\mathrm{id}_G$为满同态,但$\delta:G\to G\times G,x\mapsto(x,x)$不是满同态.

3. (1) 由 Lagrange 定理知，$|G_1 \times G_2| = |H_1 \times H_2| \cdot |G_1 \times G_2 : H_1 \times H_2|$ 由此得 $|G_1 \times G_2 : H_1 \times H_2| = |G_1 \times G_2| / |H_1 \times H_2| = |G_1| \cdot |G_2| / |H_1| \cdot |H_2|$，即 $|G_1 \times G_2 : H_1 \times H_2| = (|G_1| / |H_1|) \cdot (|G_2| \cdot |H_2|) = |G_1 : H_1| \cdot |G_2 : H_2|$

(2) 作映射 $f : G_1 \times G_2 \to G_1/H_1 \times G_2/H_2$；$(g_1, g_2) \mapsto (g_1 H_1, g_2 H_2)$，可验证其是群的满同态.且 $\mathrm{Ker}(f) = H_1 \times H_2$.

4 (1) $h_1^{-1} h_2^{-1} h_1 h_2 \in H_1 \cap H_2$，但 $H_1 \cap H_2 = \{1\}$.

(2) 设 $m = |h_1| \cdot |h_2| / \gcd(|h_1|, |h_2|)$，则 $(h_1, h_2)^m = (h_1^m, h_2^m) = 1$；另一方面，若 $(h_1, h_2)^k = 1$，则 $h_1^k = 1$ 且 $h_2^k = 1$，即 $|h_1| \mid k$ 且 $|h_2| \mid k$，故 $m \mid k$

5 用反证法 假设 $G \cong P_1 \times P_2$ 为同构，这里 $P_1 \neq \{1\} \neq P_2$，设 $r = \max\{|P_1|, |P_2|\}$，则 $r < |G|$ 且 $a^r = 1, \forall a \in P_1 \times P_2$ 这与 G 是循环群矛盾

6 对 k 用归纳法

7 设 n 有素因子分解为 $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$，则

$$\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_s^{a_s}) = p_1^{a_1 - 1}(p_1 - 1) \cdots p_s^{a_s - 1}(p_s - 1).$$

若 $p_1, p_2, \cdots, p_s$ 中有 p_i 是奇数，则由 $2 \mid (p_i - 1) \mid \varphi(n)$. 否则 $n = 2^{a_1}$，但 $n > 2$，故 $a_1 > 1$，所以 $2 \mid 2^{a_1 - 1} = \varphi(n)$

8 设 $m_1, m_2, \cdots, m_{\varphi(m)}$ 是全部小于 m 且与 m 互素的正整数，则 $m - m_1, \cdots, m - m_{\varphi(m)}$ 也是全部小于 m 且与 m 互素的正整数，故 $(m - m_1) + \cdots + (m - m_{\varphi(m)}) = m_1 + m_2 + \cdots + m_{\varphi(m)}$，即 $m\varphi(m) = 2(m_1 + m_2 + \cdots + m_{\varphi(m)})$，所以 $m_1 + m_2 + \cdots + m_{\varphi(m)} = m\varphi(m)/2$

9 $d = 7$

习题 1.5

1. (1) 因为任何两个单位根之积还是单位根，单位根的逆元还是单位根 对于任意大的正整数 n，存在 $\varepsilon \in \mathbb{C}^*$ 使得 $\varepsilon^n = 1$ 但 $\varepsilon^k \neq 1 \forall 0 < k < n$，所以 $\exp(U) = \infty$

(2) 设 $H \leqslant \mathbb{C}^*$ 且 $|H| = m < \infty$，对于任意 $h \in H$ 有 $h^m = 1$，即 $h \in U$

2. 设 a 为 A 中阶最大的元，若 $b \in A$ 使得 $|b| \nmid |a|$，则有素数 $p \mid |b|$ 但 $p \nmid |a|$；而 $c = b^{|b|/p}$ 的阶是 p，由习题 1.3.7(1)，有 $|ac| = |a| \cdot p > |a|$，与 a 为 A 中阶最大的元相矛盾. 所以 A 中任意元素的阶都是 $|a|$ 的因子

3 (1) 不妨设 $\max\{\exp(A), \exp(B)\} = \exp(A) = p^l$. 由于 $\exp(A)$，$\exp(B)$ 都是 p 的幂，故 $\exp(B) \mid p^l$，从而对于任意的 $(a,b) \in A \times B$，按习题 1.4.4(2)，有 $|(a,b)| = \max\{|a|, |b|\} \mid p^l$.

(2) $\Omega_t(A \times B) = \{(a,b) \in A \times B \mid (a,b)^{p^t} = 1\} = \{(a,b) \in A \times B \mid a^{p^t} = 1, b^{p^t} = 1\} = \Omega_t(A) \times \Omega_t(B)$

4. 当 $l < t$ 时按定义显然 $\Omega_t(A) = A$ 设 $0 \leqslant t \leqslant l$；因为对于任意 $m \mid |A|$，循环群 A 有惟一 m 阶子群，而 $\langle a^{p^{l-t}} \rangle$ 是 A 的惟一 p^t 阶子群，那么 $\Omega_t(A) = \{x \in A \mid |x| \mid p^t\} \subseteq \langle a^{p^{l-t}} \rangle$；另一方面，显然 $a^{p^{l-t}} \in \Omega_t(A)$.

5. 所有的8阶交换群在同构意义下有3种：Z_8，$Z_2 \times Z_2 \times Z_2$ 和 $Z_2 \times Z_4$.

6 由于 $|A| = |A_1 A_2| = \dfrac{|A_1| \cdot |A_2|}{|A_1 \cap A_2|}$，故 $A = A_1 \times A_2$，当且仅当 $A_1 \cap A_2 = \{1\}$ 当且仅当 $|A| = |A_1| \cdot |A_2|$

7 $\dfrac{(p^n-1)(p^{n-1}-1)\cdots(p^{n-k+1}-1)}{(p^k-1)(p^{k-1}-1)\cdots(p-1)}$. 提示：$A$ 可作为 Z_p 上的向量空间，p^k 阶子群就是 k 维子空间 任一 k 维子空间可如下产生：任取 $a_1 \in A - \{0\}$，再任取 $a_2 \in A - \langle a_1 \rangle$，依此继续，取出线性无关组 $a_1, a_2, \cdots, a_k$，产生一个 k 维子空间，共产生 $(p^n-1)(p^n-p)\cdots(p^n-p^{k-1})$ 个. 同理，一个 k 维子空间中长 k 的线性无关向量序列个数等于 $(p^k-1)(p^k-p)\cdots(p^k-p^{k-1})$，这是一个 k 维子空间在上述过程中重复产生的次数

8. 若素数 $p \mid n$，由定理 1.5.9，A 中有 p 阶子群. 再对 $d \mid n$ 做归纳，设对于任意 $d' \mid d, d' < d$ 结论成立 任取素数 $p \mid d$，设 $P \leqslant A$ 且 $|P| = p$，那么 $d/p \mid |A/B|$，而 $d/p < d$，按归纳假设，A/B 有阶为 d/p 的子群 $\bar{B}$，令其在 A 中的原像是 $B \leqslant A$，即 $B/P = \bar{B}$，则 $|B| = d$.

9. 必要性显然. 充分性可从定理 1.5.9 得到，也可直接证明如下. 对 $|A|$ 做归纳法. 设 A 只有一个 p 阶子群 P，考虑映射 $f: a \mapsto a^p$，$a \in A$，易验

证 f 是 A 的自同态，而 $\mathrm{Ker}(f)=P$. 由同态基本定理有 $A/P\cong \mathrm{Im}(f)$，于是 $|A:\mathrm{Im}(f)|=p$ 若 $\mathrm{Im}(f)=1$，显然 A 是循环群 若 $\mathrm{Im}(f)\neq 1$，则必有 $P\leqslant \mathrm{Im}(f)$. 由归纳假设，$\mathrm{Im}(f)$ 循环 设 $\mathrm{Im}(f)=\langle b\rangle$，再设 a 是在 f 之下 b 的任一原像，即 $f(a)=a^p=b$，于是 $|\langle a\rangle:\mathrm{Im}(f)|=p$. 又已证 $|A:\mathrm{Im}(f)|=p$，故 $A=\langle a\rangle$ 是循环群

10 (1) 可从定理 1.5.9 得到，类似下面的(2) 也可直接证明如下 对 $|A|$ 进行归纳. 由于 A 是有限交换群，取 $a\in A$ 为 A 中元素阶最大的元，则对于任意的 $x\in A$，有 $|x|\,\big|\,|a|$，且存在 $B\leqslant A$ 使得 $A=\langle a\rangle\times B$，令 $A_1=\langle a\rangle$，由于 $|B|<|A|$，所以按归纳法，$B=A_2\times A_3\times\cdots\times A_r$，从而 $A=A_1\times A_2\times A_3\times\cdots\times A_r$，并且 $|A_{i+1}|\,\big|\,|A_i|$.

(2) 设 $p_1,p_2,\cdots,p_k$ 是 $|A|$ 的全部互异的素因数，则可设 $|A_j|=p_1^{a_{1j}}\cdots p_k^{a_{kj}}$，$j=1,2,\cdots,r$，每个 $a_{ij}\geqslant 0$ 由条件，$a_{ij}\geqslant a_{i,j+1}$，因 A_j 都是循环群，所以 $A_j=A_{1j}\times\cdots\times A_{kj}$ 其中 $|A_{ij}|=p_i^{a_{ij}}$. 故

$$A=A_{11}\times\cdots\times A_{1r}\times A_{k1}\times\cdots\times A_{kr}$$

在去掉单位元群因子后就是定理 1.5.9 的循环分解，特别是

$$p_i^{a_{i1}},p_i^{a_{i2}},\cdots,p_i^{a_{ir}},\quad i=1,2,\cdots,k,$$

在去掉 1(即去掉 $a_{ij}=0$) 后是 A 的全部 p_i 初等因子. 同理，可设 $|B_j|=p_1^{b_{1j}}\cdots p_k^{b_{kj}}$，$j=1,2,\cdots,r'$，每个 $b_{ij}\geqslant 0, b_{ij}\geqslant b_{i,j+1}$ 而

$$p_i^{b_{i1}},p_i^{b_{i2}},\cdots,p_i^{b_{ir'}},\quad i=1,2,\cdots,k.$$

在去掉 1(即去掉 $b_{ij}=0$) 后是 A 的全部 p_i 初等因子. 令 $s=\max\{r,r'\}$，适当补充因子 1 后就得：由定理 1.5.9 的初等因子的惟一性

$$|A_j|=p_1^{a_{1j}}\cdots p_k^{a_{kj}}=p_1^{b_{1j}}\cdots p_k^{b_{kj}}=|B_j|,\ j=1,2,\cdots,s$$

最后，r 就是使得 $A_j\neq 1$ 的最小脚标，r' 则是使得 $B_j\neq 1$ 的最小脚标. 所以 $r=r'$

11 (1)、(2) 都直接根据映射和同态的定义进行验证

12. (1) 利用习题 11(1)

(2) 利用习题 11(2)

(3) 由上面的(1) 和(2)，A 到 $\mathbb{C}^*$ 同态由 $A_1\to\mathbb{C}^*$ 的同态完全确定. 由习题 1.3.13，A_1 到 $\mathbb{C}^*$ 的同态恰有 $|A_1|$ 个，故 A 到 $\mathbb{C}^*$ 互不相同的同态共有 $|A_1|\cdots|A_r|$ 个.

第 2 章

习题 2.1

1 S_4 有 5 个共轭类

2. (1) 设$(a_1a_2\cdots a_l)$是 l 循环. 则$(a_1a_2\cdots a_l)^l = 1$,$(a_1a_2\cdots a_1)^k \neq 1$, $k = 1,2,\cdots,l-1$

(2) 由于α和β无公共字符,故它们相乘可交换,然后利用(1)可知$(\alpha\beta)^k = 1$当且仅当 k 是$|\alpha|$和$|\beta|$的公倍数

(3) 同(2)

3 (1) 如果 n 次置换α的型是$(\lambda_1,\lambda_2,\cdots,\lambda_n)$,这表明 α 分解为彼此不相交的长 i 的循环有λ_i,$i = 1,2,\cdots,n$ 个,而 α 本身是 n 个文字的置换,故结论显然成立.

(2) 显然

4. 注意到方程 $x_1 + 2x_2 + \cdots + nx_n = n$ 的每一个非负整数解对应一个置换的型,由 Cauchy 公式,型为$(\lambda_1,\lambda_2,\cdots,\lambda_n)$的 n 次置换个数是

$$\frac{n!}{\lambda_1!\lambda_2!\cdots\lambda_n!\cdot 1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}}$$

因此,当$(\lambda_1,\lambda_2,\cdots,\lambda_n)$跑遍方程 $x_1 + 2x_2 + \cdots + nx_n = n$ 的全部解时,就得到了全部的 n 元置换,而全部的 n 元置换有 $n!$个,由此即得所证的结论.

5. 根据定义直接验证.

6 (1) 设有对换分解 $\alpha = (a_1b_1)\cdots(a_nb_n)$,那么 α^2 有对换分解

$$\alpha^2 = (a_1b_1)\cdots(a_nb_n)(a_1b_1)\cdots(a_nb_n)$$

(2) 由本节习题 2(3),奇阶置换的循环分解的循环长度都是奇数. 只需指出奇数长度的循环置换可写成偶数个对换之积 一般地说,长 l 的循环 $\sigma = (a_1a_2\cdots a_l) = (a_1a_l)\cdots(a_1a_2)$

7 设$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$有一个对换分解是$\alpha = (i_1j_1)(i_2j_2)\cdots(i_mj_m)$,则 $m \equiv T(\alpha)(\mathrm{mod}\ 2)$ 对于 $\alpha\cdot(i_mj_m)$,我们有$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}(i_mj_m) = (i_1j_1)(i_2j_2)\cdots(i_{m-1}j_{m-1})$,而对于该等式左边有 $i_m \mapsto j_m \mapsto a_{j_m}$;$j_m \mapsto i_m \mapsto a_{i_m}$,即

$$\alpha\cdot(i_mj_m)=\begin{pmatrix}1 & \cdots & i_m & \cdots & j_m & \cdots & n\\ a_1 & \cdots & a_{j_m} & \cdots & a_{i_m} & \cdots & a_n\end{pmatrix}$$

与原置换 α 相比正好是 a_{i_m} 与 a_{j_m} 互换，所以其逆序数的奇偶性改变，即 $N(\alpha\cdot(a_mb_m))=N(\alpha)-1 \pmod 2$. 对 m 采取数学归纳法，$N(\alpha\cdot(a_mb_m))\equiv m-1 \pmod 2$ 即是 $N(\alpha)\equiv m\equiv T(\alpha) \pmod 2$.

8. 由于 S_n 中的任何元素都可以写成对换之积，故只需验证任何对换 (ij) 可以用 $(1i),(1j)$ 表示即可，而显然有 $(ij)=(1i)(1j)(1i)$

9. 从 $(12i)=(1i)(12)$ 知 $(123),(124),\cdots,(12n)$ 都是偶置换. 反之，从习题 8，任意偶置换可写成偶数个形如 $(1i)$ 的对换之积，故只要证明 $(1i)(1j)$ 可写成形如 $(12k)$ 之积 而 $(12)(1j)=(12j)^2$；$(1i)(12)=(12i)$，$(1i)(1j)=(1i)(12)(12)(1j)=(12i)(12j)^2$.

10 显然 G 的所有偶置换作成 G 的一个子群 H，而 G 关于 H 的陪集只有 H 和 gH，这里 g 是 G 的奇置换，而 $|H|=|gH|$ 因此 G 中奇置换的个数与偶置换的个数相等

习题 2.2

1 由(1),(2)两条易验证 $\mathrm{Im}\tau\subset\mathrm{Sym}(X)$.

2 由 $G_x=\{y\in G\mid \bar{y}(x)=x\}$，对于 $s\in gG_xg^{-1}$ 存在 $t\in G_x$ 使得 $s=gtg^{-1}$，故 $sg(x)=gtg^{-1}g(x)=gt(x)=g(x)$ 即 $s\in G_{\bar{g}(x)}$，即 $gG_xg^{-1}\subset G_{\bar{g}(x)}$ 把其中 x 换为 $\bar{g}(x)$，g 换为 g^{-1}，得 $g-1G_{\bar{g}(x)}g\subset G_{g^{-1}\bar{g}(x)}=G_x$，即 $G_{\bar{g}(x)}\subset gG_xg^{-1}$

5 一般不再可迁

6 设映射为 $f:G\to G,g\mapsto g^{-1}$，则 $f(g_1g_2)=(g_1g_2)^{-1}=g_2^{-1}g_1^{-1}=f(g_2)f(g_1)$ 故为群反同态，易证其是双射，故为同构

7 作映射 $f:G\times\mathrm{Hom}(X,G)\to\mathrm{Hom}(X,C),(g,\varphi)\mapsto\varphi g$，易证映射 f 以这种方式作用在集合 $\mathrm{Hom}(X,C)$ 上

8. 易证群 G 作用于集合 $X\times Y$ 上. 一般而言，G 在 $X\times Y$ 上的作用是不可迁的 当 $X=Y$ 且 $|X|>1$ 时，不可迁

9 (1) 易证 $G=\{\mathrm{id}_X,\gamma\}$ 是群，作映射 $f:G\times X\to X;(\sigma,x)\mapsto\sigma(x)$，可以验证其是群作用

(2) 由 Burnside 引理计数公式 $t = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$，只需计算 $\mathrm{Fix}(g)$，可得 $t = \frac{1}{2}(|X| + |X_r|)$，其中 X_r 是所有 n 次实单位根的集合，即 $t = \begin{cases}(n+1)/2, & \text{若 } n \text{ 是奇数;}\\ (n+2)/2, & \text{若 } n \text{ 是偶数.}\end{cases}$ 这与几何直观是一致的.

10. (1) 作映射 $f: H\times X = (G) \to X = (G); (h, x)\mapsto hx$，即可验证.

(2) x 所在的 H- 轨道为 $\Omega_x = \{h(x) = hx \mid h \in H\} = Hx$.

(3) 显然.

(4) 考虑群 G 的子群 H 在 G 上的左(右) 平移作用，其轨道就是右(左) 陪集，任何 $x \in G$ 在 H 中的稳定子群 $H_x = 1$ 是单位元群.

习题 2.3

1. (1) 易证 $C_G(X) \trianglelefteq N_G(X)$，设 $g \in N_G(X)$，则 $\gamma_g: x\mapsto g^{-1}xg$ 是 X 的一个双射，显然 $\sigma: g\mapsto \gamma_g$ 是 $N_G(X)$ 到 X 的一个变换群的同态，其核为 $\mathrm{Ker}(\sigma) = \{g \in N_G(H) \mid \gamma_g = \mathrm{id}_X\} = \{g \in N_G(H) \mid g^{-1}xg = x, \forall x \in X\} = C_{N_G(X)}(X) = C_G(X) \cap N_G(X) = C_G(X)$. 再用同态基本定理：$\sigma(N_G(X)) \cong N_G(X)/C_G(X)$

(2) 若 $X \leqslant G$，则每个变换 γ_g 是 X 的自同构.

2. 易证循环群 Z 作用在集合 $\mathscr{A}$ 上，由引理 2.3.1 可得.

3 由 Sylow 定理，G 的任意两个 Sylow-p 子群 P, Q 彼此共轭，即群 G 以共轭方式可迁地作用在 Sylow-p 子群的集合上. 对于任意的 Sylow-p 子群 P，在 G 的稳定子群是 $N_G(P)$，因此 Sylow-p 子群的个数是 $|G: N_G(P)|$. 显然 $P \leqslant N_G(P)$，由 Lagrange 定理，$|P| \,\big|\, |N_G(P)|$，因此 $|G: N_G(P)| \,\big|\, |G: P|$.

4. 由于 $10 = 2\times 5$，由 Sylow 定理和习题 3，其 Sylow-5 子群的个数 $(1+5k) \mid 2$，故 $k = 0$，从而 Sylow-5 子群只有一个，仍然由 Sylow 定理，它是正规子群. 再考虑 Sylow-2 子群，应为 $1+2k$ 个，且 $1+2k \mid 5$，若 $k = 0$ 或 2.

(1) 若 G 只有一个正规的 2 阶群，而它的 5 阶子群也是正规的，这两个子群的交是单位元群 1，所以 G 是 2 阶子群和 5 阶子群的直积，故为循环群.

(2) G 的 5 阶子群 $\langle a\rangle$ 是正规的，2 阶子群 $\langle b\rangle$ 不正规，所以 b 在 $\langle a\rangle$ 上的作用 γ_b (参看本节习题 1(2)) 是 2 阶自同构，5 阶群 $\langle a\rangle$ 的 2 阶自同构只有 $a \mapsto a^{-1}$，故 $bab^{-1} = a^{-1}$.

(3) 正五边形的自同构群由五个旋转和五个反射构成,是 10 阶群,而且任一非恒等的旋转与任一反射相乘不可交换,故为非交换群,所以只能同构于上述(2) 中的群 或者,还可以具体论证如下. 取 a 为顺时针旋转 $2\pi/5$,则 $\langle a\rangle$ 为正规的 Sylow-5 子群 任取一个反射 b,则易验证 bab^{-1} 是反时针旋转 $2\pi/5$,即 $bab^{-1} = a^{-1}$

5. 类似于习题 4,证明 6 阶群 G 的 Sylow-3 子群必定是正规的. Sylow-2 子群如果正规,则 G 是循环群. 否则 2 阶元的共轭作用是 Sylow-3 子群的 2 阶自同构.

6 显然 $P \cap H \leqslant P$ 为 H 的 p- 子群,由习题 1.2.9, $|H:P \cap H| = |HP:P|$ 但 $p \nmid |G:P|$,而 $HP \leqslant G$(因 H 是正规子群,见下题(1)),故 $|HP:P| \mid |G:P|$. 所以 $p \nmid |H:P \cap H|$,所以 $P \cap H$ 是 H 的 Sylow p- 子群 类似地证明后一个结论

7 (1) 注意到 $(h_1k_1)(h_2k_2)^{-1} = h_1(k_1k_2^{-1}h_2^{-1}k_2k_1^{-1})k_1k_2^{-1} \in HK$.

(2) $(hk)^{-1}H(hk) = k^{-1}(h^{-1}Hh)k = k^{-1}Hk = H$ 同样地,$k^{-1}(K \cap H)k = K \cap H$

(3) 作映射 $f:K \to HK/H$, $k \mapsto hkH$, 这是满射同态,同态核是 $H \cap K$.

8. 任取 $g \in G$,由 H 在 X 上的作用是可迁的,存在 $h \in H$ 使 $h(x) = g(x)$,故 $(h^{-1}g)(x) = x$,即 $h^{-1}g \in G_x$,那么 $g = h(h^{-1}g) \in HG_x$.

9 因 $p \nmid |G:H|$,H 的 Sylow-p 子群 P 也是 G 的 Sylow-p 子群,由 Sylow 定理,G 的任何 Sylow-p 子群为 P 的共轭 $gPg^{-1} \subset gHg^{-1} = H$. 由 Sylow 定理,$H$ 在 Sylow-p 子群的集合上可迁作用,由习题 8,可得 $G = HN_G(P)$. 也可直接证明:对于任意 $g \in G$, $gPg^{-1} \subset gHg^{-1} = H$;由 Sylow 定理,存在 $h \in H$ 使得 $hPh^{-1} = gPg^{-1}$, 即 $h^{-1}gP(h^{-1}g)^{-1} = P$ 从而 $h^{-1}g \in N_G(P)$, 故 $g \in HN_G(P)$

10 设 P 是 G 的 Sylow-p 子群,则 $p^e \mid |P|$. 由推论 2.3.2,有 $1 \neq z \in Z(P)$, 那么就有 $z \in Z(P)$ 使得 $|z| = p$. 当 $e = 1$ 时,$\langle z\rangle$ 就是 P 的(也是 G 的)p 阶子群. 不然,对 e 归纳,$P/\langle z\rangle$ 有 p^{e-1} 阶子群,它在 P 中的原像就是 P 的 p^e 阶子群.

习题 2.4

1. 45. 提示:自同构群 $G = \langle (14)(23)\rangle$. 循环指标多项式 $P(G;x_1,$

$x_2,\cdots,x_4)=\frac{1}{2}(x_1^4+x_2^2)$.

2 36. 提示：自同构群 $G=\langle(12345678)\rangle$，循环指标多项式为 $P(G;x_1,x_2,\cdots,x_8)=\frac{1}{8}(x_1^8+x_2^4+2x_4^2+4x_8)$.

3. $\frac{1}{4}(2^{64}+2^{32}+2\times 2^{16})$. 提示：自同构群 G 为 4 个旋转(因为对棋盘只能从一面看不能从两面看)，循环指标多项式 $P(G;x_1,x_2,\cdots,x_4)=\frac{1}{4}(x_1^{64}+x_2^{32}+2x_4^{16})$.

4. 设正 n 边形的顶点依次为 $1,2,\cdots,n$，则正 n 边形的对称群(记为 D_n)共有 $2n$ 个元素，它们分别是正 n 边形 n 个顶点的置换，首先绕正 n 边形中心反时针旋转 $\frac{2k\pi}{n}$ 角度的旋转是 D_n 中的元素，这共有 n 个元素，设 $\sigma=(12\cdots n)$ 是其中一个旋转，它是一个 n 循环，则 σ^t 有 $\gcd(n,t)$ 个圈，每一个的长度是 $\frac{n}{\gcd(n,t)}$，这里 $1\leqslant t\leqslant n$ 其次，还有 n 个反射 我们对 n 为奇偶分别讨论，令 $\varphi(k)$ 表示 Euler 函数，当 n 为偶数时，其循环指标多项式为

$$P(D_n;x_1,x_2,\cdots,x_n)=\frac{1}{2n}\sum_{k\mid n}\varphi(k)(x_k)^{\frac{n}{k}}+\frac{1}{2n}\left(\frac{n}{2}x_1^2x_2^{\frac{n}{2}-1}+\frac{n}{2}x_2^{\frac{n}{2}}\right)$$

当 n 为奇数时，其循环指标多项式为

$$P(D_n;x_1,x_2,\cdots,x_n)=\frac{1}{2n}\sum_{k\mid n}\varphi(k)(x_k)^{\frac{n}{k}}+\frac{1}{2n}(nx_1x_2^{\frac{n-1}{2}})$$

5. 都根据定义验证.

6. 设 $g\in G$ 作为 X 上的置换，其型为 $(\lambda_1(g),\lambda_2(g),\cdots,\lambda_n(g))$，设 $h\in H$ 作为 Y 上的置换，其型为 $(\lambda_1(h),\lambda_2(h),\cdots,\lambda_m(h))$. 由习题 5(1)，$(g,h)\in G\times H$ 作用于 $X\cup Y$ 的循环分解的循环圈由 g 在 X 上的循环圈和 h 在 Y 上的循环圈合并而成 所以 (g,h) 在 $X\cup Y$ 上的型为

$$(\lambda_1(g)+\lambda_1(h),\lambda_2(g)+\lambda_2(h),\cdots,\lambda_{n+m}(g)+\lambda_{n+m}(h))$$

但其中 $\lambda_t(g)=0$ 当 $t>n$ 时，$\lambda_t(h)=0$ 当 $t>m$ 时. 故

$$P(G\times H;x_1,x_2,\cdots,x_{m+n})=\frac{1}{|G\times H|}\sum_{(g,h)\in G\times H}\prod_{t=1}^{m+n}x_t^{\lambda_t(g)+\lambda_t(h)}$$

$$=\frac{1}{|G|\cdot|H|}\sum_{(g,h)\in G\times H}\prod_{t=1}^{m+n}x_t^{\lambda_t(g)}x_t^{\lambda_t(h)}$$

$$= \frac{1}{|G|\cdot|H|}\sum_{(g,h)\in G\times H}\left(\prod_{i=1}^{n}x_i^{\lambda_i(g)}\prod_{i=1}^{m}x_i^{\lambda_i(h)}\right)$$

$$= \left(\frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{n}x_i^{\lambda_i(g)}\right)\cdot\left(\frac{1}{|H|}\sum_{h\in H}\prod_{i=1}^{m}x_i^{\lambda_i(h)}\right)$$

$$= P(G;x_1,x_2,\cdots,x_n)\cdot P(H;x_1,x_2,\cdots,x_m)$$

习题 2.5

1 可穿出 8 种项链;其中 3 个红珠,2 个黄珠有 2 种

2 $P(G;p_1,p_2,p_3,p_4,p_5,p_6)=\frac{1}{12}(p_1^6+2p_6+2p_3^2+4p_2^3+3p_1^2p_2^2)$. 其中 $p_i=r^i+y^i+b^i$ 经简单计算可得:两个红珠、两个黄珠、两个蓝珠的项链有 9 种

3 有 5 种分法 提示:把 5 本书作为结构,把 3 个人作为 3 种颜色 $\{r,y,b\}$;那么结构的自同构群是 $G\cong S_3\times S_2$;计算 $P(G;p_1,p_2,p_3,p_4,p_5)$ 中的 r^2y^2b,r^2yb^2,ry^2b^2 的系数之和,这里 $p_i=r^i+y^i+b^i$.

4. 考虑在一个袋中装入红、黄两种颜色的 n 个球有多少种装法.则自同构群 $G=S_n$ 对于任意 $0\leqslant k\leqslant n$,k 个红球、$n-k$ 个黄球的装法只有一种,因此 $P(S_n;r^1+y^1,r^2+y^2,\cdots,r^n+y^n)$ 中 r^ky^{n-k} 的系数是 1 故 $P(S_n;r^1+y^1,r^2+y^2,\cdots,r^n+y^n)=y^n+ry^{n-1}+r^2y^{n-2}+\cdots+r^n$.令 $r=1$,即得所求证公式

5 由于 $G/\mathrm{Ker}(\tau)\cong\mathrm{Im}(\tau)=H$,故 $|G|=|\mathrm{Ker}(\tau)|\cdot|H|$.陪集 $h\mathrm{Ker}(\tau)$ 与 H 的元素 $\bar{h}$ 一一对应,对于任意 $g\in h\mathrm{Ker}(\tau)$ 作为 X 上的置换与 $\bar{h}$ 是一样的,因此它对应的型 $\lambda_1(g)=n,\lambda_i(g)=0,\forall i>1$,从而有

$$P(G;x_1,x_2,\cdots,x_n)=\frac{1}{|G|}\sum_{g\in G}x_1^{\lambda_1(g)}x_2^{\lambda_2(g)}\cdots x_n^{\lambda_n(g)}$$

$$=\frac{1}{|\mathrm{Ker}(\tau)|\cdot|H|}\sum_{h\in H}\sum_{g\in h\mathrm{Ker}(\tau)}x_1^{\lambda_1(g)}x_2^{\lambda_2(g)}\cdots x_n^{\lambda_n(g)}$$

$$=\frac{1}{|\mathrm{Ker}(\tau)|\cdot|H|}\sum_{h\in H}|\mathrm{Ker}(\tau)|\cdot x_1^{\lambda_1(\bar{h})}x_2^{\lambda_2(\bar{h})}\cdots x_n^{\lambda_n(\bar{h})}$$

$$=P(H;x_1,x_2,\cdots,x_n).$$

7. 任意取 $f,g\in\mathbb{R}[0,1],k\in\mathbb{R}$,定义 $(f+g)(x)=f(x)+g(x)$;$(f\cdot g)(x)=f(x)\cdot g(x)$;$(kf)(x)=kf(x)$.由此可以验证其是一个 $\mathbb{R}$-代数.

第 3 章

习题 3.1

1. 设 $X=(V,E)$ 是一个图，若 $v\in V$，根据定义，则 v 与 v 连通. 若 v_1 与 v_2 连通，则 v_1 到 v_2 有一条道，亦即 v_2 到 v_1 有一条道；如果 v_1 与 v_2 连通，v_2 与 v_3 连通，即 v_1 到 v_2 有一条道，v_2 到 v_3 有一条道，从而 v_1 到 v_3 有一条道，即 v_1 与 v_3 连通. 故图中顶点集的连通关系是等价关系.

2. 设 V_1 和 V_2 分别是奇度点的集合和偶度点的集合，由命题 3.1.6，$\sum\limits_{v\in V_1}d(v)+\sum\limits_{v\in V_2}d(v)=2|E|$ 因为 $\sum\limits_{v\in V_2}d(v)$ 为偶数，所以 $\sum\limits_{v\in V_1}d(v)$ 必为偶数.

3. 必要性. 注意到一条道经过任何中间点时一定包含了以该点为端点的两条边 所以，一条 Euler 道若是闭道，则跨过的每个点都可作为中间点，故每点的次数都是偶数. 若不是闭道，则除起点与终点外其他点次数都是偶数.

充分性 对 $X=(V,E)$ 的边数进行归纳，证明，若 X 的奇度点个数为 2，则有 Euler 道以这两个奇度点为起点和终点，若奇度点个数为 0，则有 Euler 闭道 $|E|=1$ 时显然成立 如 X 有奇度点就取一条以奇度点 u 为端点的边 (uv)，否则任取一条边 (uv). 去掉边 (uv) 得图 $X'=(V,E')$ 分两种情况讨论：

情形 1：X' 不连通 则 X' 有两个连通分支 $u\in X_1'$，$v\in X_2'$. 此时 u 一定是 X 的奇度点，否则 X 没有奇度点，于是 u 和 v 分别成为 X_1' 和 X_2' 的奇度点，但 X_1' 和 X_2' 至少有一个不是孤立点图，那么除 u，v 外还有其他奇度点，就与 X 没有奇度点矛盾. 既然 u 在 X 中是奇度点，它在 X_1' 中就是偶度点而且 X_1' 没有奇度点（否则 X 的奇度点个数大于 2，见习题 2）. 类似可知 X_2' 也没有奇度点，按归纳法，X_1' 和 X_2' 都有 Euler 闭道，从 X_1' 的 Euler 闭道的点 u 出发走完该 Euler 道回到 u 后再经 uv 走到 X_2' 的 v 点再走完 X_2' 的 Euler 道至 v 为止，这就是 X 的一条从奇度点到奇度点的 Euler 道.

情形 2：X' 连通. 如果 u 在 X 中是奇度点，则 X' 没有奇度点. 否则 u，v 就是 X' 的仅有的两个奇度点. 可以类似于上面完成证明.

4. 设 (uv) 属于 X 的某一个连通分支，如果 (uv) 刚好属于该连通分支的一个闭道，则 X' 的连通分支个数为 r，否则去掉边 (uv) 后，原来 (uv) 所在的

连通分支变为两个,因此总的连通分支数是 $r+1$

5. 必要性:去掉圈上的一条边,显然其仍然连通.充分性:假设图中不含圈,则去掉该连通图的一条边,其变为两个连通分支

6. 若 X 是树,则 X 显然是林,且 X 的任意两个不同点之间恰好有一条路相连,因此如果在某两点之间添加一条边,则在该两点之间形成了一个圈.反之,X 是林,因而 X 无圈,只需证明 X 连通.事实上,对于任意的 X 的两个顶点 $v_i, v_j \in V$,由条件,在 v_i, v_j 之间添加一条边后就形成了一个圈,故 v_i, v_j 两点在 X 中已经连通,故 X 是树.

7. 由定理 3.1.12 即得

8 设 $X=(V,E)$ 为一个连通图,$T=(V,E')$ 是其一棵生成树,如果 X 只有一棵生成树 T,则显然 X 无圈,事实上,如果 X 有圈,则 X 至少有两棵生成树 反之,如果 X 本身是树,则其显然只有一棵生成树.

9. 对分支个数 t 进行归纳

习题 3.2

2. (1) 如果 α 是一个循环置换,不妨设 $\alpha=(i_1 i_2 \cdots i_k)$,则 $m \geqslant \tau(\alpha)=\sum_{i=1}^{k}(1-\lambda_i(\alpha))=k-1$,即 $k \leqslant m+1$

(2) 如:$V=\{1,2,3\}$,$E=\{(12),(13),(23)\} \subset S_n$,令 $\alpha=(12)(13)(23)=(13)$.

(3) 令 $\alpha=(i_1 i_2 \cdots i_{m+1})$,则 α 在 $\{i_1,i_2,\cdots,i_{m+1}\}$ 上可迁,由引理 3.2.3 知,子图 $Y=(\{i_1,i_2,\cdots,i_{m+1}\},E)$ 连通,因为 $|E|=m$,根据定理 3.1.12,Y 是树.

4 把 K_n 的各顶点标号 $1,2,\cdots,n$,那么 K_n 的一棵生成树就是一棵 n 阶标号树 反之,一棵 n 阶标号树恰好按对应标号嵌入 K_n 成为一棵生成树.

习题 3.3

1. $A(X)^k$ 的 (i,j) 元是 $\sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_k=1}^{n}a_{ii_1}a_{i_1i_2}\cdots a_{i_{k-1}i_k}a_{i_kj}$,其中 a_{ii_1}, $a_{i_1i_2},\cdots a_{i_{k-1}i_k},a_{i_kj}=0$ 或 1,它等于 1 表示从 $v_i \mapsto v_{i_1}, v_{i_1} \mapsto v_{i_2},\cdots,v_{i_k} \mapsto v_j$ 有一条长为 k 的道

2. (1) 适当安排顶点的顺序,二部图的邻接矩阵形如 $A=\begin{pmatrix}0 & A_1\\ A_1^{\mathrm{T}} & 0\end{pmatrix}$,

其中 A_1^{T} 是 A_1 的转置矩阵

(2) 由习题1，$A(X)^k$ 的对角线元素为零表示 X 的任一点自己到自己的长 k 的道不存在，即长 k 的闭道不存在. 当 X 是二部图时，从一点出发回到自己的闭道在二部之间来回穿梭所以长度只能是偶数 反之，如果奇数长的闭道不存在，那么二点之间的任意两条连接道的长度之和是偶数，所以二点之间的连接道的长度的奇偶性是固定的. 所以可以把每个连通分支 X_t 的顶点这样分类：任意取定一点 $v_1 \in X_t$，与 v_1 有偶数长的道相连的点的集合记为 W_1，令 $W_2 = X_t - W_1$，则 $X_t = W_1 \cup W_2$ 为二部图.

习题 3.4

1 此时，拟阵所需的三条性质就是向量组的线性关系的性质：(1) 空组约定为线性无关；(2) 线性无关组的部分组还线性无关；(3) 替换引理，因为，当 $F, F' \in M$ 而 $|F| < |F'|$ 时，若每 $e' \in F' - F$ 都使得 $F \cup \{e'\}$ 线性相关，即每个 $e' \in F'$ 是 F 的线性组合，则由替换引理应有 $|F| \geqslant |F'|$.

2. (1) 用定义 3.4.5 条件(3) 即可

(2) 取两个不同的极大成员 F_1, F_2，取 $e \in F_1 - F_2$，定义加权 w：$S \to \mathbb{R}^+$ 为 $w(e) = 1$，而 $w(s) = 0$ 对所有 $s \neq e$

3. 根据拟阵的定义直接验证

5. 设 $|F| = r$ 为拟阵的秩(见习题2)；对 $r - |E|$ 进行归纳. 若 $|E| = r$ 则结论自然成立 不然，由定义 3.4.5(3)，存在 $e' \in F - E$ 使得 $E' = E \cup \{e'\} \in M$，再对 E' 使用归纳假设即可.

6. (1) 参看定理 3.4.4 的证明. 如果有 $w(e_i) < w(e_i')$，对 $\{e_1, e_2, \cdots, e_{i-1}\}$ 和 $\{e_1', \cdots, e_i', e'\}$ 使用定义条件 3.4.5(3)，存在 $1 \leqslant k \leqslant i$ 使得 $E = \{e_1, e_2, \cdots, e_{i-1}, e_k'\} \in M$ 而 $w(e_k') > w(e_i)$；再由习题 5，存在子集 $E' \subset \{e_i, e_{i+1}, \cdots, e_r\}$ 使得 $E \cup E' \in M$；由构造过程知 $w(E) > w(\{e_1, e_2, \cdots, e_i\})$ 和 $w(E') \geqslant w(\{e_{i+1}, \cdots, e_r\})$，故 $w(E \cup E') > w(\{e_1, e_2, \cdots, e_i, e_{i+1}, \cdots, e_r\})$，与假设矛盾

(2) 由(1) 即得.

(3) 用 Greedy 算法找一个重量最大的极大成员 $\{f_1, f_2, \cdots, f_r\}$，由(2)，$w(e_1) = w(f_1)$ 是 S 的重量最大的元素.

7. 设 $\{e_1, e_2, \cdots, e_r\}$ 是 M 中重量最大的极大成员且可设 $w(e_1) \geqslant \cdots \geqslant w(e_r)$. 由习题 6(3)，执行 Greedy 算法的第一步时可选取 e_1；第二步取 $D =$

$\{e \in S \mid \{e_1, e\} \in M\}$ 时，由习题6(2)，$e_2 \in D$ 且 e_2 是 D 中重量最大的元素之一，故可取 e_2 加入构成 $\{e_1, e_2\} \in M$. 依此类推

习题 3.5

1 n 阶完全图共有 $n(n-1)/2$ 条边，每条边有两种定向，故共有 $2^{n(n-1)/2}$ 个 n 阶定向完全图

2. (1) 如果群 G 忠实作用在集合 V 上，则 G 也忠实作用在 V 的所有 2-子集的集合上

(2) 定义 3.5.2

3 由于 $|\alpha| = m$，故当 $k > m$ 时，不妨设 $k = qm + r, 0 \leqslant r < m$，则 $\alpha^k = \alpha^{qm+r} = \alpha^r$，而 $\alpha(i) = i + 1, i < m, \alpha(m) = 1$，故 $\alpha^k = i + k \pmod m$.

4 (1) 一场比赛恰好淘汰一个队，共淘汰 $n-1$ 个队，所以是 $n-1$ 场比赛 在淘汰赛图中任一队与冠军队相连，所以淘汰赛图是连通图. 由定理 3.1.12 淘汰赛图是树

(2) 必要性：任一队至多输一次

充分性：设有向树 T 的每个顶点的入次数不大于 1，对阶 n 进行归纳. T 至少有一个孤立点 v_n，设 v_n 的惟一边为 $(v_n v_{n-1})$，去掉 v_n 和边 $(v_n v_{n-1})$ 后得 $n-1$ 阶有向树 T' 且仍满足题目条件 按归纳假设存在 $n-1$ 个队的淘汰赛以 T' 为它的淘汰赛图 有两种情形

情形 1：T 中边 $(v_n v_{n-1})$ 方向为 $v_{n-1} \to v_n$ 则由 v_{n-1} 先淘汰 v_n. 再由剩下的 $n-1$ 个队进行上面存在的淘汰赛，得到的淘汰赛的图就是 T

情形 2：T 中边 $(v_n v_{n-1})$ 方向为 $v_n \to v_{n-1}$ 那么 T' 中 v_{n-1} 就没有入边，因此上面存在的淘汰赛中 v_{n-1} 是冠军，再由 v_n 淘汰 v_{n-1}，得到的淘汰赛的图就是 T

第 4 章

习题 4.1

1 错，对，对

2. 每个码字的头部加了一位，得码长是 $n+1$ 的 m- 元码 任意给定一个码字，若其中有一位出错，则所有位的元加起来之后模 m 不是 0

3 假定只出一个错误 注意：只对信息位的行列做了奇偶检验，所以当出错位在检验位时只会得出一个 1 但出错位在信息位时所在行列的奇偶检

验都会得 1.

4. 任意两个字在相连运算下还是一个字,且空字与任何字相连还等于该字,相连显然满足可结合性.

5. 如果 $1 \in C$,则由于对于任意的 $a \in C, a \neq 1, a1 = 1a = a$,由码的可识别条件,得 $a = 1$,矛盾.

6. 由码的可识别条件可得

7. 由 a_0 在每一个字的结尾知,其满足可识别条件.

8. 存在 $x_1, x_2, \cdots, x_m \in X$ 和 $x_1', x_2', \cdots, x_m' \in X$ 使得 $x_1x_2\cdots x_m = x_1'x_2'\cdots x_m'$ 但 $x_1 \neq x_1'$(若它们相等则把它们消去继续往后看),故 x_1 与 x_1' 的长度不相等(否则是相等的字). 若 x_1 的长度小于 x_1' 的长度,则 x_1 是 x_1' 的真前缀,否则 x_1' 是 x_1 的真前缀. 类似地证明后一结论.

9. (1) 因为 $a(ba) = aba = (ab)a$,如果 X 是一个码,则由码的可识别条件得 $a = ab, ba = a$,矛盾.

(2) 如果码字序列以 a 开头,则第一个码字只能是 aa. 如果是 b,那么形如 $b\overbrace{a\cdots a}^{k}b\cdots$,到第二个 b 为止,若 a 的个数 k 是奇数,则第一个码字是 ba,否则是 baa 第一个码字识别出来后,继续往后识别.

10. 由于 $X = \{a^n \mid n \in \mathbb{Z}^+\}$,假如 X 是一个码,且至少含有两个非空字 x, y,则由 $x = a^m, y = a^n$ 知 $xy = a^{m+n} = yx$ 可推出 $x = y$,矛盾.

习题 4.2

1 (1) 由 $(\boldsymbol{F}, +)$ 是一个有限加群 每一个元素的阶都是有限的,而 $1_{\boldsymbol{F}} \in \boldsymbol{F}$,故存在正整数 p 使得 $p \cdot 1_{\boldsymbol{F}} = 0$. 进一步,由于域没有零因子,可得 p 是素数.

(2) 任意的 $0 \neq a \in \boldsymbol{F}, p \cdot a = (p \cdot 1_{\boldsymbol{F}})a = 0a = 0$

(3) $(\lambda + \mu)^p = \lambda^p + \cdots + \binom{p}{k}\lambda^{p-k}\mu^k + \cdots + \mu^p$, 其中 $\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$ 是从 p 个物体中选取 k 个的选取数,当 $0 < k < p$ 时,$p \nmid k!$,所以 $\binom{p}{k}$ 是 p 的倍数,因此 $\binom{p}{k}\lambda^{p-k}\mu^k = 0$. $n > 1$ 时做归纳法.

(4) 据定义可得子集 $P = \{0, 1_{\boldsymbol{F}}, \cdots, (p-1)1_{\boldsymbol{F}}\}$ 是一个子域. 作映射 $f: P \to \mathbb{Z}_p; i \cdot 1_{\boldsymbol{F}} \mapsto [i]$,可得其是一个域同构.

2. (1) 设 $x=(x_1,x_2,\cdots,x_n),y=(y_1,y_2,\cdots,y_n),z=(z_1,z_2,\cdots,z_n)$,分别考虑第 i 位对距离函数 $d(x,y),d(x,z),d(y,z)$ 的贡献. 当 $x_i\neq y_i$ 时,$x_i\neq z_i$ 与 $y_i\neq z_i$ 至少有一个不成立;即得三角不等式 注意到重量函数不等式实际上可表示为 $d(x+y,0)\leqslant d(x+y,x)+d(0,x)$.

(2) 由距离三角不等式,一方面有 $d(x,y)\leqslant d(x,x)+d(y,x)=d(y,x)$;另一方面有:$d(y,x)\leqslant d(y,y)+d(x,y)=d(x,y)$.

3. 注意到 $e=\left[\frac{d-1}{2}\right]$,若 $d\neq 2e+1$,则 $d=2e+2$ 利用注解 4.2.8 的技巧可在两个码字 c' 与 c'' 之间找到一个字 x 使得 $d(c',x)=d(c'',x)=e+1$,用三角不等式易证 x 不在任何球 $S(c,e)$ 之中 反之,取长 4 的 2 元码 $C=\{(0,0,0,0),(1,1,1,0)\}$,极小距离是 3,但不是完全码

4 定义 4.2.11 和定义 4.2.12

5 由 4.2.10 可得 $\sum_{i=0}^{3}\binom{n}{i}=2^l$,其中 l 是整数,即 $(n+1)(n^2-n+6)=3\cdot 2^{l+1}$,也就是 $(n+1)((n+1)^2-3(n+1)+8)=3\cdot 2^{l+1}$. 所以 $n+1=3^a2^b$. 若 $b>3$,则 $(n+1)^2-3(n+1)+8$ 被 8 整除但不被 16 整除,而它整除 $3\cdot 2^{l+1}$ 所以 $(n+1)^2-3(n+1)+8=8$ 或 24,但这都不可能. 故 $a\leqslant 1,b\leqslant 3$ 而 $n\geqslant 7$,得 $n=7,11,23$. 但 $n=11$ 不满足方程. 故 $n=7$ 或 $n=23$

6 $|S(x,1)|=1+6=7$. 参数(6,9,3)的二元码不存在;证明提示:若存在,由容斥原理,有三个码字的后两位完全相同,去掉后两位,得到(4,3,3)的二元码;再由容斥原理,有两个码字的第四位相同:只能是(111a)和(000a),而另一个码字的前三位至少有两位为同一字母,与极小距离为 3 矛盾.

7 如果 $k=0$ 显然. 下设 $k\geqslant 1$ 设 C_{k-1} 是 $[n,k-1,d]$ 码,因为 $|C_{k-1}|V_q(n,d-1)<q^n$,这个码不是完全码,从而有一个字 $x\in F^n$,它与 C_{k-1} 的所有码字的距离不小于 d 设 $C_k=\langle C_{k-1}\cup\{x\}\rangle$,设 $z=ax+y,0\neq a\in F,y\in C_{k-1}$,则 $w(z)=w(a^{-1}z)=w(x+a^{-1}y)=d(x,-a^{-1}y)\geqslant d$.

8. 码 C 是一个 $(n+1,M,d$ 或 $d+1)$- 码.

9. 如果存在参数 $(n,M,2t+1)$ 的 2 元码 C,令 $\hat{C}$ 是如习题 8 构造的扩

张码，则 $\hat{C}$ 的每一个码字都有偶重量，且其任意两个码字的距离是偶数，因而是参数$(n+1,M,2t+2)$的2元码. 反过来，假设C是一个二元$(n+1,M,2t+2)$-码，不妨设$d(\boldsymbol{c},\boldsymbol{d})=2t+2$，我们可以通过截去$C$中$\boldsymbol{c},\boldsymbol{d}$的坐标不同的一个位置，即可得到所求的码.

10. 将4.2.15变形即得.

11. 设C是线性等重码，则对于任意$\boldsymbol{c}\neq\boldsymbol{c}'\in C$有$d(\boldsymbol{c},\boldsymbol{c}')=w(\boldsymbol{c}-\boldsymbol{c}')$为常数. 反之，如果对于任意$\boldsymbol{c}\neq\boldsymbol{c}'\in C$有$d(\boldsymbol{c},\boldsymbol{c}')$为常数，则对$C$的任意非零码字$\boldsymbol{c}$有$w(\boldsymbol{c})=d(\boldsymbol{c},0)$为常数

习题 4.3

1 (1) 设$u_1,u_2,\cdots,u_k$是U的基，设以该组基为行向量作成的矩阵为A，则$\boldsymbol{x}\in U^{\perp}$当且仅当$A\boldsymbol{x}=\boldsymbol{0}$，这线性方程组的解子空间的维数为$n-k$

(2) 根据定义$(U^{\perp})^{\perp}=\left\{\boldsymbol{v}\in V\middle|\langle\boldsymbol{u},\boldsymbol{v}\rangle=0,\forall\,\boldsymbol{u}\in U^{\perp}\right\}=U$

2 极大相似译码规则把$r=0110$译为0111，这个码不能纠一个错，因为其极小距离为2 而要纠一个错，其极小距离至少是3

3 不能 由Singelton界，其极小距离$d\leqslant 6-3+1=4$，从而最多能纠$e=\left[\frac{4-1}{2}\right]=1$个错.

4. 它的一个生成矩阵是$G=\begin{pmatrix}1&1&1&0&0\\0&1&1&1&1\end{pmatrix}$

5. 必要性. 设C是极大距离可分码，则$d=n-k+1$，从而H的任意$d-1=n-k$列线性无关.

充分性：如果H的任意$n-k$列线性无关，则其极小距离$d\geqslant n-k+1$，由于H的行数是$n-k$，故存在$n-k+1$列线性相关，即$d=n-k+1$.

6 设$G=(G_1,G_2,\cdots,G_n)$，其中G_j是G的第j个列向量 为求各码字重量之和，可考虑所有码字中固定的一位对总和的贡献，因此也只需考虑该位为零的码字个数. 任意$\boldsymbol{c}=a\boldsymbol{G}=(aG_1,aG_2,\cdots,aG_n)$，由线性方程组理论，若$G_j\neq 0$，则$aG_j=0$的个数为$q^{k-1}$，从而在第$j$位不为零的元素的个数是$q^k-q^{k-1}$，由此推出$\sum\limits_{\boldsymbol{c}\in C}w(\boldsymbol{c})\leqslant n(q-1)q^{k-1}$. 而要使等式成立，$G$应无零列

8. (1) $\boldsymbol{F}^t$中的所有非零向量有q^t-1个，每一个非零向量生成一个包含$q-1$个非零向量的一维子空间，故$\boldsymbol{F}^t$的一维子空间的个数是$(q^t-1)/(q-1)$.

(2) 注意到行数为 s 的矩阵的任意两列线性无关，当且仅当它的任意两列代表两个不同的一维子空间，列数达到极大当且仅当它的列跑遍 F^s 的一维子空间；那么由(1)得(2)

9 直接验证

10 (1) $\Longrightarrow$ (2)：命题 4.3.13

(2) $\Longrightarrow$ (3)：注意到 $e = \left[\frac{3-1}{2}\right] = 1$，将 C 的参数代入命题 4.2.10.

(3) $\Longrightarrow$ (1)：由 $e = 1$，$|C| = q^k$，命题 4.2.10 中取等号，得 $n = \frac{q^n - 1}{q-1}$ 再由 $d = 3$ 和定理 4.3.5，C 的检验矩阵的任二列线性无关

12 C 中任意两个重量为偶数的码字之和仍然为偶数重量的码字，故所有偶数重量的码字构成一个子空间 C'. 而 C 关于 C' 的陪集个数只有两个：C' 和 $x + C'$，其中 x 的重量是奇数

13 极大投射 q 元码的生成矩阵是 Hamming 码的检验矩阵，从而其参数是 $\left[\frac{q^k-1}{q-1}, k\right]$ 另一方面，考虑该码的非零码字的重量 $w(aG)$，其中 $aG = (aG_1, aG_2, \cdots, aG_n)$，参看本节习题 6 的解答 $aG_i = 0$ 当且仅当 $G_i \in \langle a \rangle^{\perp}$，而 $\dim\langle a\rangle^{\perp} = k-1$，所以含在 $\langle a\rangle^{\perp}$ 中的 G_i 的个数是 $(q^{k-1}-1)/(q-1)$(见命题 4.3.11)，故 $w(aG) = n - (q^{k-1}-1)/(q-1) = q^{k-1}$

习题 4.4

1 因为 $\chi(a)$ 是一个 $|X|$ 次的单位根，故 $\chi(a)\overline{\chi(a)} = 1$. 再用 $\chi(a)\cdot\chi(a^{-1}) = \chi(1) = 1$

2 在定理 4.4.5 中取 $\psi = 1$(单位特征标)即可 另一直接证明如下.

若 $\chi = 1$，则显然 $\sum_{a\in X}\chi(a) = |X|$ 若 $\chi \neq 1$，则存在 $b \in X$ 使得 $\chi(b) \neq 1$ 又有 $\chi(b)\sum_{a\in X}\chi(a) = \sum_{a\in X}\chi(ab)$，注意到当 a 跑遍 X 时，ab 也跑遍 X，从而 $\chi(b)\sum_{a\in X}\chi(a) = \sum_{a\in X}\chi(a)$ 整理并注意到 $\chi(b) \neq 1$，即得所求的结论.

3 见式(4.4.10.2). 或类似于上面的习题 2 直接证明.

4 (1) 注意 $(X\times Y)^* \cong X\times Y$，又有 $X\times Y \cong X^*\times Y^*$.

(2) 对每个 $a^* \in W_*$，因为限制映射 $a^*|W$ 是单位同态，a^* 诱导同态 $X/W \to C^*$，这就给出了映射 $W_* \to (X/W)^*$ 易验证这是同态而且是单射

满射.

(3) 把 x^* 限制到 W 诱导满同态 $X^* \to W^*$,同态核是 $W_\perp$.

5. 注意到 $(1 \mid b) = (1^2 \mid b) = (1 \mid b)^2$,且 $(1 \mid b) \neq 0$.

6. 7. 都直接验证.

8. 由定理 4.4.4 存在 $\chi \in X^*$ 使得 $\chi(b) \neq 1$. 再由(4.4.7.2),存在 $a \in X$ 使得 $a^* = \chi$,即 $(a \mid b) = *(b) = \chi(b) \neq 1$.

9. 参看 §5.4.

10. 对于任意的 $x \in C$, $\chi(x^p) = \chi(x)^p = \chi(1) = 1_F$,而 F 只有一个 p 次单位根.

11. 选取 $b \in \mathbb{Z}$ 使得 $\chi(b) \neq 1$,则 $\chi(b)\sum_{a=0}^{m-1}\chi(a) = \sum_{a=0}^{m-1}\chi(ab)$,整理即得.

第 5 章 循环码

习题 5.1

1 对环 R,定义映射 $f: \mathbb{Z} \times R \to R; (n, r) \mapsto nr$.

2. 3. 都直接验证.

4. (1) $\xi(1) = 1_T$,而 T 的任何子环包含 1_T.

(2) $\mathbb{Z}$ 是主理想整环.

(3) 如 T 是一个域则 T 是一个整环,故无零因子;若 $m = m_1 m_2$,则 $0 = m \cdot 1_T = (m_1 \cdot 1_T)(m_2 \cdot 1_T)$,故或者 $m_1 \cdot 1_T = 0$ 或者 $m_2 \cdot 1_T = 0$.

5. 定义映射 $f: \mathbb{R} \times \mathbb{C} \to \mathbb{C}; (r, x) \mapsto rx$,由此易证 $\mathbb{C}$ 可作为 $\mathbb{R}$ - 代数.

6. 先验证 $\left\{\sum_t r_t x_t \,\middle|\, r_t \in R\right\}$ 是 R 的理想;另一方面,R 的一个理想如包含所有 x_t 就一定包含所有 $\sum_t r_t x_t$.

7 设 $|G| = n$,作映射 $g: F[X] \to FG; f(X) \mapsto f(x)$ 显然该映射是满射,易证其是代数同态. 该同态的核为 $\mathrm{Ker}(g) = \{f(X) \mid f(x) = 0\} = \langle X^n - 1 \rangle$.

8. 易证其是代数满同态,同态核 $I = \left\{\sum_{x \in G}\lambda_x x \,\middle|\, \sum_{x \in G}\lambda_x = 0\right\}$. 而在 $\sum_{x \in G}\lambda_x$

$=0$ 时，$\sum_{x\in G}\lambda_x x = \sum_{1\neq x\in G}\lambda_x(x-1)$.

9 若存在 $c\in C$，使得 $w(c)=1$，则存在 $x\in G$ 和 $0\neq\lambda\in F$ 使得 $c=\lambda x$. 注意到 C 是 FG 的理想，知 $1=\lambda^{-1}x^{-1}\cdot\lambda x\in C$ 于是 $C=FG$，与 C 不是单位理想，矛盾.

10. 对于任意的 $c\in C\subset FG$，则 c 可表示为 $c=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$，易证 τ_x 是一个自同构.

习题 5.2

1. (1) 对于任意的一个码字 $c=(c_0,c_1,c_2,\cdots,c_{n-1})\in C$，则 c 表示为 FG 中的元为 $c(x)=c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}$，由于 C 是 FG 的理想，故 $x\cdot c(x)=c_{n-1}+c_0x+c_1x^2+\cdots+c_{n-2}x^{n-2}\in C$，此即 $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$

(2) 集合 $\left\{\sum_i c_ix^i\right\}$ 是 FG 的一个子空间，而且 $x\sum_i c_ix^i$ 还在这个集合中

2. 由 $R=L_1\oplus L_2$ 可写 $1=e_1+e_2$，其中 $e_i\in L_i, e_2\in L_2$；则 $e_1=e_1\cdot 1=e_1e_1+e_1e_2$，但 $e_1e_1\in L_1$ 和 $e_1e_2\in L_2$，由直和的定义 1.4.2，得 $e_1=e_1^2$ 和 $e_1e_2=0$. 类似地，$e_2=e_2^2$ 和 $e_2e_1=0$ 对于任意 $r_1\in L_1$，有 $r_1=r_1\cdot 1=r_1e_1+r_1e_2$ 同上推理，$r_1e_2=0$，即 $r_1=r_1e_1\in Re_1$ 同理 $L_2=Re_2$

反之，如果 e_1,e_2 满足条件，则对于任意的 $r\in R$，有 $r=r\cdot 1=re_1+re_2$，由此得 $R=Re_1+Re_2$. 设 $r_1e_1+r_2e_2=r_1'e_1+r_2'e_2$，两边右乘 e_1 得 $r_1e_1=r_1'e_1$. 同理，$r_2e_2=r_2'e_2$，因此 $R=Re_1\oplus Re_2$.

3. (1) 由于 $F[X]/\langle X^n-1\rangle\cong FG$，由理想对应定理 5.1.4，$FG$ 的理想与 $F[X]$ 包含 $\langle X^n-1\rangle$ 的理想一一对应 但 $F[X]$ 是主理想整环，故与整除 X^n-1 的多项式一一对应 所以 $C_1\subset C_2$ 当且仅当在 $F[X]$ 中 $\langle g_1(X)\rangle\subset\langle g_2(X)\rangle$，当且仅当 $g_2(QX)\mid g_1(X)$.

(2) 易验证 C_1+C_2 是 FG 的一个理想. 类似于(1)，C_1+C_2 对应于 $F[X]$ 的理想 $\langle g_1(X)\rangle+\langle g_2(X)\rangle=\langle\gcd(g_1(X),g_2(X))\rangle$.

另证：$C=C_1+C_2$ 是包含 C_1 和 C_2 的最小理想. 由(1)，C 的生成多项式 $g(X)$ 是整除 $g_1(X)$ 和 $g_2(X)$ 的最大的多项式.

(3) 类似于(2).

4. 设 G 是 n 阶循环群，F 是有限域，$\mathrm{char}F \nmid n$. 设 $C_1, C_2 \subset FG$ 是两个循环码，设 $h_1(X), h_2(X)$ 分别是 C_1, C_2 的检验多项式 则：

(1) $C_1 \subset C_2$ 当且仅当 $h_1(X) \mid h_2(X)$.

(2) $C_1 + C_2$ 也是循环码其检验多项式是最小公倍式 $\mathrm{lcm}(h_1(X), h_2(X))$.

(3) $C_1 \cap C_2$ 是循环码其检验多项式是最大公因式 $\mathrm{gcd}(h_1(X), h_2(X))$.

证明提示.(1) 利用检验多项式和生成多项式的关系 $g_1(X)h_1(X) = X^n - 1 = g_2(X)h_2(X)$ 和本节习题 3(1).

(2) 仍利用检验多项式和生成多项式的关系和本节习题 3(2)，或者像习题 3(2) 的解答中的另证那样做

(3) 类似(2)

5. 本题实际上是对交换环都成立的一般结论(参看本节习题 2) 设 R 是交换环，$e_1^2 = e_1, e_2^2 = e_2, C_1 = Re_1, C_2 = Re_2$

(1) $C_1 \subset C_2 \Longrightarrow e_1 \in C_2 \Longrightarrow e_1 = re_2 \Longrightarrow e_1e_2 = re_2e_2 = e_1$ 反之是显然结论

(2) 令 $e = e_1 + e_2 - e_1e_2$ 和 $C = Re$ 显然 $e \in C_1 + C_2$ 从而 $C \subset C_1 + C_2$. 简单计算知 e 是幂等元，而 $e_1e = e_1(e_1 + e_2 - e_1e_2) = e_1$，从而 $C_1 = Re_1 \subset C$，同理 $C_2 \subset C$，故 $C = C_1 + C_2$

(3) 类似(2).

6. 由推论 5.2.7 推出.

7. (1) 按 E_n 的定义，$1 + x \in E_n$，而 $1 + X \mid X^n - 1$，故以 $1 + X$ 为生成多项式的循环码 $C \subset E_n$. 但 $\dim E_n = n - 1 = \dim C$.

注：E_n 就是二元域 F_2 上 n 阶循环群 G 的群代数 F_2G 的增广理想. 一般地，循环群 $\langle x \rangle$ 的群代数的增广理想都可由 $1 - x$ 生成.

(2) 利用习题 3(1).

8. 生成矩阵 $(1\ \ 1\ \ 1\ \ 1\ \ 1)$，检验矩阵 $\begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & 1 & 1 & \\ & & & 1 & 1 \end{pmatrix}$，生成幂等元 $x^4 + x^3 + x^2 + x + 1$.

9 不可约分解：$X^3-1=(X+1)(X^2+X+1)$. 结果列表如下，其中 C_0 和 C_1 分别是零理想和单位理想，情况稍特殊.

码	生成多项式	生成矩阵	检验矩阵	生成幂等元
C_0	X^3-1	0	E	0
C_1	1	E	0	1
C_2	$X+1$	$\begin{pmatrix}1&1\\&1&1\end{pmatrix}$	$(1\ 1\ 1)$	x^2+x
C_3	X^2+X+1	$(1\ 1\ 1)$	$\begin{pmatrix}1&1\\&1&1\end{pmatrix}$	x^2+x+1

习题 5.3

1 定义映射 $f:\boldsymbol{F}\times\boldsymbol{K}\to\boldsymbol{K},(r,\alpha)\mapsto r\alpha$，即可验证.

2 设 $\alpha_i,i\in I$ 是 $\boldsymbol{K}$ 作为 $\boldsymbol{F}$- 向量空间的基底，$\beta_j,j\in J$ 是 $\boldsymbol{E}$ 作为 $\boldsymbol{K}$- 向量空间的基底，则 $\boldsymbol{E}$ 的任一元可写成 $\alpha_i\beta_j,i\in I,j\in J$ 的 $\boldsymbol{F}$- 线性组合，而且 $\alpha_i\beta_j,i\in I,j\in J$ 在 $\boldsymbol{F}$ 上线性无关

3 检验集合 $\{f(\alpha_1,\alpha_2,\cdots,\alpha_n)/g(\alpha_1,\alpha_2,\cdots,\alpha_n)\}$ 构成一个域.

4 设 α 是域 $\boldsymbol{F}$ 上的一个代数元，在 $\boldsymbol{F}$ 上的极小多项式是 $p(X)$，若 $p(X)=g(X)h(X)$，其中 $0<\deg g(X)<\deg p(X),0<\deg h(X)<\deg p(X)$. 则由 $0=p(\alpha)=g(\alpha)h(\alpha)$ 知，$g(\alpha)=0$ 或 $h(\alpha)=0$，这与 $p(X)$ 是 α 在 $\boldsymbol{F}$ 上的极小多项式矛盾

5 $f'(X)=\lambda_0\sum_j\Big(m_j(X-\alpha_j)^{m_j-1}\prod_{i\neq j}^{n}(X-\alpha_i)^{m_i}\Big)$ 所以，存在 $m_j>1$ 当且仅当 $(X-\alpha_j)\mid\gcd(f(X),f'(X))$

6 利用习题 5 记 $f(X)=X^n-1$，则

$$\gcd(f(X),f'(X))=\gcd(X^n-1,nX^{n-1})=\begin{cases}1, & \text{当 } p\nmid n;\\ X^n-1, & \text{当 } p\mid n.\end{cases}$$

7. 设 α 是 $\boldsymbol{F}_4$ 的乘法群的生成元，则 $\boldsymbol{F}_4$ 的一种表示方法是 $\boldsymbol{F}_4=\{0,\alpha^0,\alpha^1,\alpha^2\}$

另一方面，α 在 $\boldsymbol{F}_2$ 上的极小多项式的次数是 2，且 α 满足方程 $X^4-X=X(X-1)(X^2+X+1)=0$，由此知 X^2+X+1 是 α 的极小多项式，此时 $\boldsymbol{F}_4$ 可表示为 $\{(0,0),(1,0),(0,1),(1,1)\}$.

8. $\boldsymbol{F}_{q^m}\subset\boldsymbol{F}_{q^n}\Longrightarrow q^n=(q^m)^k\Longrightarrow n=mk\Longrightarrow q^m-1\mid q^n-1\Longrightarrow q^m$

-1 阶循环群是 q^n-1 阶循环群的子群$\Longrightarrow X^{q^m}-X \mid X^{q^n}-X \Longrightarrow \boldsymbol{F}_{q^m} \subset \boldsymbol{F}_{q^n}$.

9 用定理 5.3.16 由条件 $q^m \equiv 1 \pmod{n}$. 又对 $1 \leqslant k < m$, 因 $q^k - 1 < q^k < \dfrac{q^m-1}{q-1} = n$, 故 $n \nmid q^k - 1$, 即 $q^k \not\equiv 1 \pmod{n}$.

习题 5.4

1. 在特征 p 的域中, $X^p - 1 = (X-1)^p$, 所以没有本原 p 次单位根, 因此在 $p \mid n$ 时也就没有本原 n 次单位根. 反之, $p \nmid n$ 时, $X^n - 1$ 无重根(见习题 5.3.6), 在其分裂域中, 它的 n 个根构成分裂域的乘群的 n 阶子群, 所以是 n 阶循环群(见命题 1.3.13), 它的生成元就是本原 n 次单位根.

2. 在 $\boldsymbol{F}_3$ 上, $X^4 - 1 = (X-1)(X+1)(X^2+1)$. 由此得长度 4 的三元循环码共有 8 个, 除了零理想和单位理想外, 生成多项式分别是 $X-1, X+1, X^2+1, X^2-1, (X-1)(X^2+1), (X+1)(X^2+1)$.

3. 由本节习题 2, 在 $\boldsymbol{F}_3$ 上的参数为[4,2]的循环码只有两个, 其生成多项式分别是 X^2+1, X^2-1. 检验矩阵分别是

$$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

按定义, 它们显然都不是参数为[4,2]的三元 Hanuming 码的检验矩阵

4 (1) 由定理 5.4.8, $m(X)$ 是 C 的生成多项式, 再由习题 5.2.6, $\dim C = n - \deg m(X)$ 但 $m(X)$ 的根都是 n 次单位根, 因此 $\deg m(X) = |\{0 \leqslant i < n \mid m(\omega^i) = 0\}|$.

(2) $\dim C^{\perp} = n - \dim C$.

习题 5.5

1. 设 α 是一个 n 次本原单位根, 则 $\alpha^b \neq 1, \forall\, i < a$, 由于

$$X^n - 1 = (X^b)^a - 1 = (X^b - 1)(1 + X^b + X^{2b} + \cdots + X^{(a-1)b})$$

故 $\alpha, \alpha^2, \cdots, \alpha^{a-1}$ 不是 $X^b - 1$ 的零点, 因而它们都是下述多项式的零点

$$1 + X^b + X^{2b} + \cdots + X^{(a-1)b},$$

故 $1 + x^b + x^{2b} + \cdots + x^{(a-1)b} \in C$, 从而 C 的极小重量不大于 a.

2. 定理 5.4.8.

3. 将该字译为(10010 11011 11001 01101 01010 11011 1).

4. 参看例 5.3.17. $X^7 - 1 = (X-1)(X^3+X^2+1)(X^3+X+1)$. 设本

原 7 次单位根 ω 是 X^3+X^2+1 的根，则 X^3+X^2+1 的根是 ω,ω^2,ω^4，而 X^3+X+1 的根是 $\omega^3,\omega^5,\omega^6$ 所以有两个长为 7 的二元狭义本原 BCH 码：

由 ω,ω^2 决定的 BCH 码，即例 5.3.17 中的 C_3；

由 ω,ω^2,ω^3 决定的 BCH 码，即例 5.3.17 中的 C_4.

习题 5.6

1 (1) $\Longleftrightarrow$(3)：C 为 MDS 码当且仅当 $d=n-k+1$，当且仅当其奇偶检验矩阵 H 的任意 $n-k$ 列线性无关

(2) $\Longleftrightarrow$(3)：事实上只需验证 C 为 MDS 码当且仅当 $C^{\perp}$ 为 MDS 码.

2 生成多项式为 $g(X)=X-\omega$，它的一个生成矩阵为

$$G=\begin{pmatrix}\omega & 1 & 0\\ 0 & \omega & 1\end{pmatrix}.$$

习题 5.7

1. 事实上，对于任意的 $c\in C$，有 $H\cdot c^{\mathrm{T}}=0$，由于 K 可逆，故 $KH\cdot c^{\mathrm{T}}=0$ 且 $\mathrm{rank}(H)=\mathrm{rank}(KH)$

2 (1) 验证 0,1 都不是其根即可

(2) 有一个奇偶检验矩阵 H 是

$$H=\begin{pmatrix}1&1&0&0&0&0&0&0\\0&0&0&1&0&1&1&1\\0&0&1&1&1&0&0&1\\0&1&1&1&1&1&1&1\\0&0&1&0&1&1&0&1\\0&0&0&1&1&1&1&0\end{pmatrix}$$

3 在定义 5.5.2 中取 $l=5,d=2$，我们即知 C 是 BCH 码，其极小距离不小于 2 因为 $(x+1)(x^2+x+1)=x^3+1\in C$，所以 $d=2$. 若在定义 5.7.2 中取 $g(X)$ 的次数大于 1，则由定理 5.7.6 知，Goppa 码 $\Gamma(L,g)$ 的极小距离至少为 3. 如果 $g(X)$ 的次数是 1，则由定理 5.7.7 能得到同样的结论. 所以 C 不是 Goppa 码.

参 考 文 献

[1] Y. Fan, Q.Y. Xiong, Y.L. Zheng, A Course in Algebra, World Scientific Publ. Co. Pte Ltd Singapore, 2000

[2] N.Jacobson, Basic Algebra I, W.H. Freemanand Company, San Francisco, 1974

[3] J.H. van Lint, Introduction to Coding Theory, Graduate Texts in Mathematics Vol.86, Springer-Verlag, New York, 1982

[4] S.Roman, Coding Theory and Information Theory, Graduate Texts in Mathematics Vol.134, Springer-Verlag, New York, 1992

[5] F. 哈拉里.图论.李慰萱译 上海:上海科技出版社,1980

[6] I. Tomescu 组合学引论 栾汝书等译,北京:高等教育出版社,1985

[7] 樊恽等.代数学辞典 武汉:华中师范大学出版社,1994

[8] 樊恽,刘宏伟 线性等距码与极大投射码.通讯学报,第22卷第6期(2001年6月) 48～52

常 用 符 号

$\mathbb{Z}$，整数集合，有时表示整数加群、整数环

$\mathbb{Q}$，有理数域

$\mathbb{R}$，实数域

$\mathbb{C}$，复数域.

$\boldsymbol{F}[X]$，域 $\boldsymbol{F}$ 上的不定元 X 的多项式环

$n!$，$=1\cdot 2\cdot\cdots\cdot(n-1)\cdot n$

$a\mid b$，a 整除 b

$\gcd(a,b)$，a,b 的最大公因子

$\mathrm{lcm}(a,b)$，a,b 的最小公倍子

$\max\{a,b,\cdots\}$，$a,b,\cdots$ 中最大的一个.

$\min\{a,b,\cdots\}$，$a,b,\cdots$ 中最小的一个.

$[x]$，不超过实数 x 的最大整数.

$\binom{n}{k}$，从 n 个物体中取 k 个的选取数

$\equiv\ \ (\mathrm{mod}\ m)$，模 m 同余.

$\deg f$，多项式的次数

$\det A$，矩阵 A 的行列式.

$|G|$，集合 G 的基数，群中元素 G 的阶.

$|G:H|$，群 G 对子群 H 的指数，扩域 G 对子域 H 的次数

$\dim C$，向量空间的维数

$\langle x,y\rangle$，向量空间 $\boldsymbol{F}^n$ 的典型内积

$\langle a,b,\cdots\rangle$，在群中表示生成子群；在环中表示生成理想；在向量空间中表示生成子空间

名词索引