现代数学基础

55 代数编码与密码

许以超　马松雅　编著

高等教育出版社

55 代数编码与密码

阜阳师范学院图书馆 ★ 藏书

许以超　马松雅　编著

DAISHU BIANMA YU MIMA

高等教育出版社·北京

图书在版编目（CIP）数据

代数编码与密码 / 许以超，马松雅编著．-- 北京：高等教育出版社，2015.3

ISBN 978-7-04-041873-6

Ⅰ.①代… Ⅱ.①许… ②马… Ⅲ.①代数编码－高等学校－教材②密码－理论－高等学校－教材 Ⅳ.①O157.4 ②TN918.1

中国版本图书馆 CIP 数据核字（2015）第 016923 号

策划编辑	王丽萍	责任编辑	李 鹏	封面设计	赵 阳	版式设计	杜微言
责任校对	李大鹏	责任印制	田 甜				

出版发行	高等教育出版社	咨询电话	400-810-0598
社 址	北京市西城区德外大街4号	网 址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印 刷	北京宏伟双华印刷有限公司	网上订购	http://www.landraco.com
开 本	787mm×1092mm 1/16		http://www.landraco.com.cn
印 张	13.25	版 次	2015年3月第1版
字 数	240 千字	印 次	2015年3月第1次印刷
购书热线	010-58581118	定 价	39.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换

版权所有 侵权必究

物 料 号 41873-00

序

很多大学的数学学院 (或数学系) 都开设了信息与计算科学专业. 这个专业有两门重要的专业课, 它们是信息论以及代数编码和密码. 本书作为一种尝试, 试图将代数编码和密码理论方面最基本的内容介绍给学生. 本书定位在普通大学数学学院的信息与计算科学专业.

编码学和密码学作为数学的一个分支, 是在第二次世界大战后期开始形成的. 由信息论中的 Shannon 理论, 我们知道存在好的纠错码方案. 但是迄今为止, 各种编码方案和加密方案都还不能说是很理想的方案. 这和计算机的发展密切相关, 一些过去认为好的方案, 在计算机容量加大、速度加快的情形下, 又变成不是十分满意的方案. 所以需要根据新的要求不断地探讨新的编码方案和加密方案.

所谓代数编码学和代数密码学, 就是用抽象代数的方法来研究编码学和密码学. 发展代数编码学和密码学, 目的在于数字通信的可靠性和安全性. 确切地说, 如何保证在各种电波干扰下 (包括电子战), 能获得我方发出的正确信息, 是研究纠错码的任务; 如何在敌方截获我方发出的信息后无法破译, 以保证我方行动安全, 或者如何在计算机网络中设置防火墙, 以防止黑客和病毒的侵入, 如何在各种信用卡上设置密码, 以防止被他人盗用等在信息学中设置安全措施, 以及金融方面的种种安全要求, 则是研究密码学的任务. 这些当前迫切需要解决的问题推动了代数编码学和密码学的迅速发展.

代数编码学和密码学, 涉及下面三大问题: 如何编制方案, 如何译码以及如何评估密码的好坏. 这里要求的是收发报机制造简单, 编码及译码、加密及解密的运算速度比较快. 所以考虑的问题比较实际.

代数编码和密码理论的入门基础包括概率论、统计学、信息论、计算复杂性

理论、数论、抽象代数、代数数论、代数几何, 组合数学等. 当然, 本书只涉及最基本的概念和性质.

作为数学学院所设专业的教学用书, 本书写作时偏重于数学理论. 其目的在于使数学学院的信息与计算科学专业的毕业生今后在这方面做研究工作或者应用于实际需要时有一个扎实的数学理论基础. 本书的入门基础只涉及最基本的数论、抽象代数 (这包含群、环、域、有限域、域上多项式理论、域上行列式及矩阵, 域上线性空间等).

本书共分三部分, 设有九章. 第一部分是抽象代数基础, 由第一章构成. 第二部分是代数编码理论, 即纠错码理论, 由第二、三、四、五章构成. 第三部分是代数密码理论, 由第六、七、八、九章构成.

本书的写作经历了十余年. 本人从 2000 年起受聘于河南大学数学系,[①] 作为讲座教授担任一些教学任务和研究工作. 2001 年和 2002 年, 在河南大学数学系开设了代数编码与密码讨论班. 2003 年, 在河南大学数学与信息科学学院信息科学专业四年级上学期开设了代数编码与密码课程. 从 2005 年开始, 代数编码与密码作为河南大学数学与信息科学学院信息科学专业的必修课, 由作者每年进行讲授. 经过多年的教学实践, 本书不断修改完善. 参加的老师、研究生和本科生对本书提出了大量宝贵的意见, 在此表示衷心的感谢.

本书被列入“河南大学规划教材资助立项项目”. 在写作过程中得到河南大学冯淑霞、王波的支持. 高等教育出版社王丽萍和李鹏对本书的出版做了大量的工作. 在此一并表示感谢.

最后, 必须指出, 作为普通大学的教材, 如何取材是一个很难的问题. 所以本书只是抛砖引玉, 希望今后有适合普通大学数学学院信息与计算科学专业的教科书的出现. 另一方面, 书中难免出现各种错误, 还望老师和同学们提出宝贵的意见, 以便今后改进.

许以超

中国科学院数学与系统科学研究院

河南大学数学与统计学院

2014 年 10 月 1 日

[①] 本页中涉及的几个机构名称为该教学机构不同历史阶段的名称.

此为试读,需要完整PDF请访问: www.ertongbook.com

前　言

大学数学学院的信息与计算科学专业有两门必修专业课, 它们是信息论 (基础是概率论) 以及代数编码和密码学 (基础是抽象代数). 它们是构建信息安全的理论基础. 当前市面上有大量的代数编码 (即纠错码) 理论和代数密码理论的教科书. 但是它们或者是适合于排名靠前的顶尖大学数学学院的信息与计算科学专业学生用的教材, 或者是适合于研究生用的教材. 这和抽象代数课的教材处于相同的境地. 因此有些大学数学学院干脆就不开抽象代数这门课, 有些大学数学学院在离散数学课中讲点抽象代数了事. 原因在于下面的关键问题没有答案, 即一本教材, 对不同层次的大学, 应该选取什么样的内容? 应达到什么样的目的?

作者的看法是, 作为应用数学的一个重要且实用的分支, 代数编码和密码的入门切入点是让学生掌握一些具体的、较好的纠错码体制和密码体制, 以便在工作中能够使用. 当然也不是讲这些就够了, 本书把对它们的系统阐述建立在严格的数学基础上, 仅仅是忽略了码的好坏的判定标准的理论; 再者在密码学方面, 也不讲过去那些著名的密码体制, 在计算机日新月异的发展过程中是怎样被攻击, 甚至被破译的理论. 例如 DES 密码体制的不安全性的讨论, Hash 函数 SHA-1 的碰撞搜索攻击, 等等. 完整地学习纠错码理论和密码理论是为了从事创造新的编码体制和密码体制, 比较它们和已有体制的优缺点, 以及如何攻击, 甚至破译已有的著名的密码体制, 等等, 这些都是专攻编码学和密码学的研究工作者和研究生的事.

具体而言, 作为一本最初等的入门教科书, 我们挑选若干和当前计算机的技术水平相适应的纠错码体制和密码体制, 以便学生能掌握和运用这些体制. 在大学毕业后, 如果从事信息方面的工作, 这是一个重要的技能. 这比现在所有大学

数学学院的学生都要学线性规划这门课来得对口. 在编码学方面我们只讲 BCH 码; 在密码学方面, 我们只讲 RSA 密码体制, ElGamal 密码体制, AES 高级加密标准和 IDEA 密码体制.

本书共分三部分.

第一部分是抽象代数基础, 由第一章构成. 它是全书的数学基础知识, 包括群、环、域和有限域理论. 由于有些学校讲授过抽象代数课, 所以前三节打上了两个星号, 可以略去. 第四节和第五节讲解有限域和有限域上的多项式环, 这才是代数编码学和密码学的基础.

第二部分由第二、三、四、五章构成, 介绍纠错码理论, 即有限维线性码. 第二章讲为什么要纠错, 介绍纠错码的基本概念和基本问题. 第三章引进线性码. 第四章讲循环码, 这是一类特殊的线性码. 第五章讲著名的 BCH 码和 RS 码. 这是一类在国际上公认的好的纠错码, 它们是循环码. 为了避免指标复杂, 我们重点讲本原 BCH 码. 关于代数编码学, 由于或者是理论上超出现有学生的课程安排或者是没有建立严格的数学理论, 我们没有收入 Goppa 码和卷积码. 虽然从纠错能力而言, Goppa 和卷积码是公认为效果好于一般的有限维线性纠错码. 另一方面, 纠错码理论和信息论中的 Shannon 理论密切相关. Shannon 证明了存在一个线性二元码的序列, 使得线性二元码的纠错能力愈来愈接近最好的纠错码. 但是在本书中略去了从概率统计学来判断纠错码好坏的讨论.

第三部分由第六、七、八、九章构成, 介绍代数密码学. 第六章先说明密码学的重要性并讲授编制密码方案的原则. 接下去讲公钥密码, 主要介绍了 RSA 密码体制和 ElGamal 密码体制. 第七章讲分组密码, 主要介绍了高级加密标准 AES 和 IDEA 密码体制. 第八章讲密钥管理, 主要讨论如何管理和分配密钥. 第九章讲数字签名和认证系统, 这是密码学的另一个重要方面. 数字签名和认证系统的目的在于确认身份和确认接收到的信息不是伪造的, 这一章主要介绍了 Hash 函数、数字签名和识别协议.

各章习题都放在每章的最后. 另外有些章节打上了记号 $*$, 凡是打上了记号 $*$ 的地方, 都可以不讲授, 而让学生自己研读. 本书的篇幅, 大体上是一个学期的课, 每周四学时.

目　　录

第一章　抽象代数基础

抽象代数是数 (整数、有理数、实数和复数) 和它们的代数运算 (加、减、乘、除四则运算) 的各种形式的抽象化推广. 最简单及在数字通信领域中最常用的是由两个元素 0 和 1 构成的集合 Π_2, 其中加法的定义为 $0+0=0, 0+1=1+0=1, 1+1=0$. 乘法的定义为 $0\times 0=0, 0\times 1=1\times 0=0, 1\times 1=1$. (这里注意, 对集合 Π_2 的四则运算中, 和数的运算的本质差别是 $1+1=0$.) 而且我们可以直接验证它们关于加法和乘法都适合结合律和交换律, 关于加乘还有分配律, 所以它和数的代数运算有完全相同的四则运算规则.

抽象代数研究的是代数结构的普遍性质. 本章介绍代数编码理论和代数密码理论入门所需要的抽象代数的部分基础知识, 包括群、环、域、域上线性空间、域上多项式环. 其中详细介绍了有限域理论, 包括有限域的一些重要性质, 有限域的结构以及有限域上的多项式环的一些重要性质.

有限域是计算机科学和数字通信领域最基本的数学工具之一, 在编码理论和密码理论中起着关键作用.

§1.1** 群

群是最基本的代数结构, 掌握群的研究方法, 就可以利用类似的方法来研究其他的代数结构.

设 G_1 和 G_2 为两个非空集合, 则集合 $G_1\times G_2$ 定义为

$$G_1\times G_2=\{(x_1,x_2)\mid \forall\, x_1\in G_1,\ x_2\in G_2\}. \tag{1.1.1}$$

此为试读,需要完整PDF请访问: www.ertongbook.com

定义 1.1.1　设 G 为非空集合. 定义 $G\times G$ 到 G 内的单值映射

$$\sigma:\quad (a,b)\to ab=a\times b=a\cdot b, \tag{1.1.2}$$

称在集合 G 中引进了乘法, 或称集合 G 在乘法下封闭, 也称在集合 G 中引进了一种代数运算 —— 乘法 $\cdot$.

定义 1.1.2　设 G 为非空集合. 在 G 中引进一种代数运算, 简称为乘法. 如果这种运算适合结合律

$$(ab)c=a(bc),\quad \forall\, a,b,c\in G, \tag{1.1.3}$$

则 G 称为**半群**.

定义 1.1.3　设 G 为乘法半群. G 称为**群**, 如果它适合条件

(1) 在 G 中存在**幺元** e, 使得

$$ae=ea=a,\quad \forall\, a\in G; \tag{1.1.4}$$

(2) 任取 $a\in G$, 则存在元素 $b\in G$, 使得

$$ab=ba=e. \tag{1.1.5}$$

元素 b 称为元素 a 的**逆元**, 记作 $b=a^{-1}$.

下面先给出群的一些基本性质, 再举若干例子.

引理 1.1.4　*设 G 为群, 则*

(1) *G 中有且只有一个幺元 e, 且对每个元素 a, G 中有且只有一个逆元 a^{-1}.*

(2) *乘法的左、右消去律成立, 即 $\forall\, a,b,c\in G$, 则*

$$ab=ac\quad 蕴含\quad b=c, \tag{1.1.6}$$

$$ba=ca\quad 蕴含\quad b=c. \tag{1.1.7}$$

证　(1) 若群 G 有两个幺元 e_1 和 e_2, 由幺元的定义, 有

$$e_1=e_1e_2=e_2.$$

若群 G 中存在元素 a, 使得群 G 中的元素 b 和 c 都是 a 的逆元, 由逆元的定义, 有

$$ab=ba=e,\quad ac=ca=e.$$

于是 $c=ce=c(ab)=(ca)b=eb=b$.

(2) 设 $ab = ac$. 由于 a 有逆元 a^{-1}, 于是

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

由结合律推出 $(a^{-1}a)b = (a^{-1}a)c$, 因此 $eb = ec$, 这证明了 $b = c$. 即左消去律成立. 同理可证右消去律成立. 证完.

注意 一般来说, 在群 G 中交换律未必成立, 即设 $a, b \in G$, ab 和 ba 不一定相等.

显然有

引理 1.1.5 设 G 为群, 则乘法运算有性质

(1) G 中元素 c 满足 $c^2 = c$ 当且仅当 $c = e$;

(2) G 中任意有限个元素 $a_1, a_2, \cdots, a_s$ 之连乘积只计先后次序, 不计括号. 特别任取 $a \in G$. 记 a^i 为 i 个 a 连乘, 其中 i 为正整数. 规定 $a^0 = e$. 当 i 为负整数时, 定义 $a^i = (a^{-1})^{-i}$. 这时有

$$a^i \cdot a^j = a^{i+j}, \quad \forall i, j \in \mathbb{Z}; \tag{1.1.8}$$

(3) 在群 G 中任取 $a_1, a_2, \cdots, a_n$, 则有

$$(a_1 a_2 \cdots a_{n-1} a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}. \tag{1.1.9}$$

例 1.1.6 设 G 为群. 在 G 中取定一元素 a, 则有 $a^{-1} \in G$. 于是有无穷序列

$$\cdots, a^{-k}, \cdots, a^{-2}, a^{-1}, e = a^0, a, a^2, \cdots, a^k, \cdots. \tag{1.1.10}$$

它们构成 G 的子集合, 记作 (a). 则 (a) 在 G 的乘法下构成群, 称为以 a 为**生成元**的循环群, 简称为**循环群**.

证 显然群 G 的任意非空子集关于群 G 的乘法满足结合律. 由 (1.1.8), 集合 (a) 关于群 G 的乘法封闭. 由幺元的定义可知, 群 G 的幺元 e 为集合 (a) 的幺元. 又在 (a) 中任取一元 a^k, 其中 $k \in \mathbb{Z}$. 则存在元素 $a^{-k} \in (a)$, 使得

$$a^k a^{-k} = a^{-k} a^k = a^{k-k} = a^0 = e.$$

所以 (a) 为群. 证完.

例 1.1.7 设 $\mathfrak{S}$ 为非空集合. $\mathfrak{S}$ 到 $\mathfrak{S}$ 上的一一映射全体构成的集合记为 $\mathrm{Aut}(\mathfrak{S})$, 在集合 $\mathrm{Aut}(\mathfrak{S})$ 中引进乘法运算:

$$\sigma \cdot \tau = \sigma \circ \tau, \quad \forall \sigma, \tau \in \mathrm{Aut}(\mathfrak{S}),$$

其中 $\sigma\circ\tau$ 为映射 σ 和 τ 的连续作用. 即 $\forall s\in\mathfrak{S}$, $(\sigma\circ\tau)(s)=\sigma(\tau(s))$. 由于一一映射的复合映射 $\sigma\circ\tau$ 仍是一一映射, 且满足结合律, 所以得到半群 $G=\mathrm{Aut}\,(\mathfrak{S})$.

显然恒等映射 $\mathrm{id}\colon\ s\to s$, $\forall s\in\mathfrak{S}$ 为幺元. 再任取 $\sigma\in\mathrm{Aut}\,(\mathfrak{S})$, $\forall s\in\mathfrak{S}$, 则唯一存在元素 $\sigma(s)\in\mathfrak{S}$. 由于 σ 为一一映射, 因此 $\sigma(s)\to s$, $\forall s\in\mathfrak{S}$ 定义了一个新的一一映射, 记作 σ^{-1}. 显然 $\sigma\circ\sigma^{-1}=\sigma^{-1}\circ\sigma=\mathrm{id}$, 即映射 σ^{-1} 就是映射 σ 的逆元. 所以 $\mathrm{Aut}\,(\mathfrak{S})$ 是群.

作为具体例子, 记 $\mathfrak{S}$ 是由 n 个元素 $a_1, a_2, \cdots, a_n$ 构成的集合. 为简单起见, 我们改记 $\mathfrak{S}=\mathfrak{S}_n=\{1, 2, \cdots, n\}$.

我们知道, n 个数字 $1, 2, \cdots, n$ 的排列 $i_1i_2\cdots i_n$ 共有 $n!$ 个. 集合 $\mathfrak{S}$ 上的一一映射为

$$\sigma:\quad j\to i_j,\quad 1\leqslant j\leqslant n, \tag{1.1.11}$$

其中 $i_1i_2\cdots i_n$ 为 $1, 2, \cdots, n$ 的一个排列. 这个映射又可以用**置换**来表示, 记作

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}=\begin{pmatrix}j_1 & j_2 & \cdots & j_n\\ i_{j_1} & i_{j_2} & \cdots & i_{j_n}\end{pmatrix}, \tag{1.1.12}$$

其中 $j_1j_2\cdots j_n$ 为 $1, 2, \cdots, n$ 的任一排列, 所以 $i_{j_1}i_{j_2}\cdots i_{j_n}$ 仍为 $1, 2, \cdots, n$ 的一个排列. 由此可见, 同一个置换 σ 可以写成 $n!$ 种不同的表达形式.

在集合 $\mathrm{Aut}\,(\mathfrak{S}_n)$ 中定义乘法

$$\begin{aligned}&\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix}\\ =&\begin{pmatrix}j_1 & j_2 & \cdots & j_n\\ i_{j_1} & i_{j_2} & \cdots & i_{j_n}\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix}=\begin{pmatrix}1 & 2 & \cdots & n\\ i_{j_1} & i_{j_2} & \cdots & i_{j_n}\end{pmatrix},\end{aligned} \tag{1.1.13}$$

则 $\mathrm{Aut}\,(\mathfrak{S}_n)$ 构成群, 称为**置换群**. 它的幺元为恒等置换

$$\mathrm{id}=\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}. \tag{1.1.14}$$

每个元素 σ 的逆元为

$$\sigma^{-1}=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}^{-1}=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ 1 & 2 & \cdots & n\end{pmatrix}. \tag{1.1.15}$$

下面对群加若干条件.

定义 1.1.8　设 G 为群. G 称为**交换群**或 **Abel 群**, 如果它的乘法适合交换律

$$ab=ba,\quad \forall\ a, b\in G. \tag{1.1.16}$$

在交换群的情形, 有时我们不用乘法符号 $\cdot$, 而改用加法符号 $+$. 这时幺元改记为 0, 称为零元; 元素 a 的逆元改记为 $-a$, 称为元素 a 的负元.

定义 1.1.9 设 G 为群. G 的元素个数称为群 G 的**阶**, 记作 $|G|$. 如果 $|G|<\infty$, 则 G 称为**有限群**. 否则称为**无限群**.

例 1.1.10 所有**整数**构成的集合记为 $\mathbb{Z}$, 所有**有理数**构成的集合记为 $\mathbb{Q}$, 所有**实数**构成的集合记为 $\mathbb{R}$, 所有**复数**构成的集合记为 $\mathbb{C}$. 于是

$$\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}.$$

它们都关于加法构成无限交换群, 其中群的幺元为数 0, 每个元素 a 的**逆元**为 a 的**负数** $-a$. 在本书中包含符号 $\subset$ 泛指真包含或者相等, 即等同于 $\subseteq$.

例 1.1.11 记 $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ 分别为 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 除去零后构成的子集合, 则 $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ 都关于乘法构成无限交换群, 其中群的幺元为数 1, 每个元素 a 的**逆元** a^{-1} 为 a 的倒数 $\dfrac{1}{a}$.

例 1.1.12 所有一元整系数**多项式**构成的集合记为 $\mathbb{Z}[x]$, 它在多项式的加法下构成无限交换群. 这时群的幺元为零多项式 0, 每个多项式 $f(x)$ 的**逆元**为 $f(x)$ 的**负多项式** $-f(x)$.

例 1.1.13 所有 n 阶实方阵构成的集合记为 $\mathrm{gl}\,(n,\mathbb{R})=\mathbb{R}^{n\times n}$, 它在矩阵的加法下构成无限交换群, 其中群的幺元为零方阵 0, 每个方阵 A 的逆元为它的负方阵 $-A$.

所有 n 阶非异实方阵构成的集合记为 $\mathrm{GL}\,(n,\mathbb{R})$, 它在矩阵的乘法下构成无限非交换群, 称为**一般线性群**, 其中群的幺元为 n 阶单位方阵 E_n, 每个 n 阶非异方阵 A 的逆元为它的逆方阵 A^{-1}.

下面给出一类有限交换群, 它在本书中起了重要作用.

例 1.1.14 考虑所有整数构成的集合 $\mathbb{Z}$. 给定一个正整数 n, 在 $\mathbb{Z}$ 中引进关系: 任取 $a,b\in\mathbb{Z}$, 如果 $n|(a-b)$, 则称 a 和 b **模** n **同余**, 即它们用 n 除后, 余数相同. 记作

$$a\equiv b\ (\mathrm{mod}\,n). \tag{1.1.17}$$

容易证明这是一个等价关系. 它将 $\mathbb{Z}$ 分成等价类, 每个等价类中的元素, 被 n 除后余数相同, 因此每个等价类称为**同余类**. 任取 $m\in\mathbb{Z}$, 用 n 除 m 得 $m=qn+r$, 其中余数 $r\in\{0,1,\cdots,n-1\}$. 记

$$C_r=\{m\in\mathbb{Z}\mid m\equiv r\ (\mathrm{mod}\,n)\},\quad \forall r\in\{0,1,\cdots,n-1\}. \tag{1.1.18}$$

因此共有 n 个同余类, 它们是 C_0, C_1, $\cdots$, C_{n-1}. 记子集合 C_j, $j = 0, 1, \cdots, n-1$ 构成的集合为商集合

$$\mathbb{Z}_n = \{C_0, C_1, \cdots, C_{n-1}\}. \tag{1.1.19}$$

它有子集

$$\mathbb{Z}_n^* = \mathbb{Z}_n - \{C_0\} = \{C_1, C_2, \cdots, C_{n-1}\}. \tag{1.1.20}$$

为了在商集合 $\mathbb{Z}_n$ 中能定义加法和乘法, 我们约定下面的符号:

$$C_{r+kn} = \{m \in \mathbb{Z} | m \equiv r + kn \ (\mathrm{mod}\, n)\}, \quad \forall k \in \mathbb{Z}.$$

由定义可知 $C_{r+kn} = C_r, \forall k \in \mathbb{Z}$. 在 $\mathbb{Z}_n$ 中定义加法和乘法如下:

$$C_i + C_j = C_{i+j}, \quad C_i C_j = C_{ij}, \quad 0 \leqslant i, j \leqslant n-1, \tag{1.1.21}$$

这里 $i+j$, ij 虽然不一定在集合 $\{0, 1, \cdots, n-1\}$ 中, 但是可以证明, 上面的加法和乘法的定义是合理的, 即与同余类中的代表元 i 和 j 的选取无关. 于是商集合 $\mathbb{Z}_n$ 在加法下构成 n 阶交换群. 而 $\mathbb{Z}_n^*$ 在乘法下构成群当且仅当 n 为素数. 事实上, 如果 n 是合数, 即 $n = n_1 n_2$, 其中 $n > n_1$, $n_2 > 1$, 于是 $C_{n_1}, C_{n_2} \neq C_0$, 而 $C_{n_1} C_{n_2} = C_n = C_0$. 这说明集合 $\mathbb{Z}_n^*$ 在乘法下不封闭, 即 $\mathbb{Z}_n^*$ 不是群. 若 n 为素数, 改记 n 为 p. 于是

$$\mathbb{Z}_p = \{C_0, C_1, C_2, \cdots, C_{p-1}\}, \quad \mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{C_0\}. \tag{1.1.22}$$

下面证明 $\mathbb{Z}_p^*$ 在乘法下构成 $p-1$ 阶交换群. 显然 $\mathbb{Z}_p^*$ 关于乘法满足交换律和结合律. 事实上, 记 (u, v) 为整数 u 和 v 的最大公因子. 任取 $i, j \in \{1, 2, \cdots, p-1\}$, 则最大公因子 $(i, p) = (j, p) = 1$. 因此 $(ij, p) = 1$. 于是 $C_i C_j = C_{ij} \neq C_0$, 即 $\mathbb{Z}_p^*$ 在乘法下封闭. $\mathbb{Z}_p^*$ 的幺元为 C_1. 每个元素 C_i, $1 \leqslant i \leqslant p-1$ 的逆元的求法如下: 因为 $(i, p) = 1$, 所以存在 u, $v \in \mathbb{Z}$, 使得 $ui + vp = 1$. 于是 $ui \equiv 1 \ (\mathrm{mod}\, p)$. 即 $C_u C_i = C_1$, 所以 C_u 为 C_i 的逆元. 证完.

研究群论的一个重要工具是研究它的“子”代数结构, 下面介绍子群, 左陪集、右陪集, 正规子群, 商群.

定义 1.1.15 设 G 为群. G 的非空子集 H 称为 G 的**子群**, 如果

(1) 群 G 的乘法运算限制在子集 H 上仍封闭, 即 $ab \in H, \forall a, b \in H$;

(2) 群 G 的幺元 $e \in H$;

(3) 任取 $h \in H$, 则 h 在 G 中的逆元 $h^{-1} \in H$.

由于在子群 H 中结合律显然成立, 所以群 G 的子群 H 关于群 G 的乘法仍为群. 当 H 为群 G 的子群时, 记作 $H \leqslant G$.

如果 $H=\{e\}$ 或 $H=G$, 则 H 称为 G 的**平凡子群**, 否则称为 G 的**非平凡子群**. 如果 $H\neq G$, 则 H 称为 G 的**真子群**.

现在开始考虑群和它的子群之间的关系.

设 G 为群, H 为 G 的子群. 在 G 中引进关于子群 H 的一种等价关系: 称 G 中元素 a 和 b 有关系

$$a\approx b,$$

如果 $a^{-1}b\in H$.

引理 1.1.16 *上述关系 $\approx$ 是等价关系.*

证 $\forall a\in G$, 由于 $a^{-1}a=e\in H$, 所以 $a\approx a$, 即自反性成立; 若 $a\approx b$, 即 $a^{-1}b\in H$, 则 $b^{-1}a=(a^{-1}b)^{-1}\in H$, 所以 $b\approx a$, 即对称性成立; 若 $a\approx b$, $b\approx c$, 即 $a^{-1}b\in H$, $b^{-1}c\in H$, 则 $a^{-1}c=(a^{-1}b)(b^{-1}c)\in H$, 所以 $a\approx c$, 即传递性成立. 证完.

引理 1.1.17 *在关系 $\approx$ 下, 以 a 为代表元的等价类为*

$$aH=\{ah\mid\forall h\in H\}. \tag{1.1.23}$$

证 记以 a 为代表元的等价类为 S_a. 任取 $b\in S_a$, 由于 $a\approx b$, 所以 $a^{-1}b=h\in H$, 即 $b=ah\in aH$. 这证明了 $S_a\subset aH$. 反之, 任取 $b=ah\in aH$, 则 $a^{-1}b=a^{-1}(ah)=h\in H$, 即 $a\approx b$. 这证明了 $aH\subset S_a$. 至此证明了 $S_a=aH$, 即以 a 为代表元的等价类为 aH. 证完.

由等价关系的性质可知, 群 G 可分解为等价类 aH 的并集, 且任意两个不同的等价类作为集合的交为空集.

定义 1.1.18 设 H 为群 G 的子群. 任取群 G 中元素 a, 集合 aH 称为以 a 为**代表元素**的**左陪集**.

由左陪集的定义可知, 判断两个左陪集是否相同, 有下面的充要条件: $xH=yH$ 当且仅当 $x^{-1}y\in H$.

前面已经定义了有限群的阶. 下面定义子群的指数, 并给出它们之间的关系.

定义 1.1.19 设 H 为有限群 G 的子群, 则 G 关于子群 H 的所有不同左陪集的个数称为子群 H 的指数, 记作 $[G:H]$.

定理 1.1.20 (Lagrange 定理) *设 H 为有限群 G 的子群, 则*

$$|G|=[G:H]|H|. \tag{1.1.24}$$

此为试读,需要完整PDF请访问: www.ertongbook.com