MATH 大学数学选修课丛书

矩阵与编码

郑宝东 张春蕊 编

科学出版社
www.sciencep.com

大学数学选修课丛书

矩阵与编码

郑宝东　张春蕊　编

科学出版社

北京

内 容 简 介

本书主要介绍纠错码、现代密码和认证码的基本理论及其实现方法. 作为预备知识,本书回顾性地介绍近世代数中的基本概念、基本理论,随后介绍在纠错码、现代密码和认证码的理论中起重要作用的交换环上的矩阵理论. 本书侧重于数学在纠错码、现代密码和认证码的理论中的应用,内容全面,文字简练,概念清楚,深入浅出,便于理解.

本书适合作为高等院校数学本科各专业特别是信息与计算科学专业高年级有关选修课程的简明教材,也可供对纠错码、现代密码和认证码有兴趣的技术人员及高等院校有关专业的教师参考.

图书在版编目(CIP)数据

矩阵与编码/郑宝东,张春蕊编. —北京:科学出版社,2009
(大学数学选修课丛书)
ISBN 978-7-03-024701-8

Ⅰ.矩… Ⅱ.①郑…②张… Ⅲ.①矩阵-高等学校-教材②编码-高等学校-教材 Ⅳ.O151.21 O157.4

中国版本图书馆 CIP 数据核字(2009)第 090787 号

责任编辑:姚利丽 房阜午 / 责任校对:陈玉凤
责任印制:张克忠 / 封面设计:陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码:100717
http://www.sciencep.com

骏走印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2009 年 6 月第 一 版 开本:B5(720×1000)
2009 年 6 月第一次印刷 印张:7 1/4
印数:1—3 000 字数:132 000

定价:20.00 元

(如有印装质量问题,我社负责调换〈环伟〉)

序

长期以来，在认识和改造世界的过程中，人们对数学所起作用的认识是逐渐形成的，而且这种认识随着时代的进步在不断深化. 特别是近年来，随着数字信息技术的飞速发展，人们对数学在科学技术中所起作用的认识也越来越深刻. 在我们所处的数字信息时代，数学科学的迅猛发展，更加确立了它在整个科学技术中的基础地位. 数学已突破传统的应用范围，向几乎所有人类知识的领域渗透，并为人类的物质和精神文明作出了贡献. 甚至诸如人文、社会科学这样的领域，为了准确和定量地考虑问题，数学也已经成为了重要的工具.

近年来，随着高等教育事业的不断发展，以及数学在科学技术各领域不断凸显的重要作用，全国许多高等院校纷纷筹办数学和与数学有关的各专业，而且这些新专业的成立已经为我们国家培养了大量的数学和与数学有关的社会急需人才. 但是，毋庸讳言，与规模快速增长不相协调的是，目前招生培养的很多数学类专业毕业生的数学修养、能力等方面的综合素质，却出现了不同程度的下降. 针对这种局面，我们必须从实际出发，加快数学类专业的全方位改革步伐，提高数学类专业的办学质量，努力培养适合数字信息化时代需要的高素质的数学人才.

当前，我国正处于高等教育从精英教育到大众化教育的转型时期，高等教育的培养目标、培养模式、培养方案正处在调整之中. 针对当前压缩必修课教学课时、增开更多选修课的现实情况，如何确保培养学生的质量，已是我们必须面对和迫切需要解决的问题. 显然在夯实基础的前提下，选择适当的教材、精选教学内容、合理选取和配置讲授近现代理论体系是解决质量问题的关键之一.

在课程体系中，选修课在开拓学生视野、激发学生兴趣、提高学生修养、引导学生专业精神、巩固数学基础、沟通分支联系、培养探索和创新能力等方面，都起着不可或缺的作用. 但是，目前国内可供数学类专业本科生作为选修课教材的用书却不多见. 国内多数高校常常是选用研究生教材或专著作为本科生的选修课教材.

针对目前国内高等教育中数学类各专业选修课的实际情况，我们总结多年来的教学实践与改革的经验，吸收国内外优秀教材的长处，将传统的教学内容、体系

与近现代理论发展的成果有机结合，组织编写了《大学数学选修课丛书》. 在编写的过程中，我们遵循了以下原则：选修课要与基础课教学内容相衔接，反映近现代数学学科专业研究和发展的概貌，基本覆盖数学本科专业的基本内容，对本科学生进行毕业设计和毕业论文的创作有实际的参考作用.

本丛书力图体现数学类各个专业选修课的概貌，注重基础知识、基本方法的训练，加强应用. 选修课门类的选择，力求适合不同层次高等院校选修课教学的实际情况.

王仁宏

2009 年元月

前　言

作为工具，数学在科学与技术的进步中所起的作用是不言而喻的，数学在信息科学中的作用更是无所不在. 今天，数学技术已成为高技术的突出标志和不可或缺的组成部分. 同时，科学技术的不断进步，也对数学提出了许多富有挑战性的问题，推动着数学的发展. 纠错码、现代密码和认证码的理论为数学提供了很好的应用背景，同时也给数学工作者提出了许多具有实际应用价值的研究课题. 希望通过本书向读者介绍有关纠错码、现代密码和认证码的基本理论和基本方法. 在编写过程中，我们努力遵循如下几个原则：

(1) 精练素材，以利于读者在短时间内了解、掌握纠错码、现代密码和认证码的最基本的理论和方法.

(2) 侧重于数学在纠错码、现代密码和认证码中的应用，尽量用数学的观点提出问题、分析问题、解决问题.

(3) 适当安排例题、习题，便于读者理解有关概念、理论和方法.

本书作者在编写过程中，始终站在读者的角度，力求通俗易懂，充分考虑到数学系本科高年级学生的特点和实际需要.

在本书的编写过程中，作者参考了大量有关文献，在此对有关作者表示感谢.

由于作者水平有限，书中难免有疏漏之处，恳请读者批评指正.

作　者

2009 年 2 月 6 日于哈尔滨工业大学

目　录

第1章

近世代数基础

1.1 群的基本概念

1.1.1 半群

整数的加法、乘法运算，数域上矩阵的加法运算，线性空间上线性算子的加法运算等都有一个共同的特点，就是对给定集合中任意取定的两个元素，该集合中都有唯一一个元素与之对应. 我们将具有这种性质的运算抽象为所谓的“二元运算”.

定义 1.1.1 设 A 是一个非空集合，称由笛卡儿积 $A\times A$ 到 A 的一个映射为集合 A 上的一个**二元运算**.

设 φ 是集合 A 上的一个二元运算，记 $\varphi(a,b)$ 为 (a,b) 在 φ 下的像. 为方便，有时把 $\varphi(a,b)$ 记为 $a\circ b$ 或 $a\cdot b$ 等.

定义 1.1.2 设 S 是一个非空集合，在 S 中定义了一种叫做乘法的二元运算“$\circ$”，若 S 满足结合律

$$(a\circ b)\circ c=a\circ(b\circ c),\quad \forall a,b,c\in S,$$

则称 S 关于这个运算“$\circ$”构成一个**半群**，记为 $(S,\circ)$. 简称 S 是一个半群.

为方便，我们通常把乘积 $a\circ b$ 简记为 ab.

正整数集合 $\mathbf{Z}^+=\{1,2,3,\cdots\}$ 关于通常数的乘法构成半群.

若在半群 S 中存在元素 e，满足

$$ae=ea=a,\quad \forall a\in S,$$

则称 e 是半群 S 的**单位元**(**恒等元**). 称有单位元的半群为**幺半群**，也称幺半群中的单位元为**幺元**.

容易证明，半群 S 中若有单位元，则单位元是唯一的.

设 a 是幺半群 S 中的元素，若存在元素 $b\in S$，使得

$$ab=ba=e,$$

其中 e 是半群 S 的单位元，则称 a 是**可逆元**，称 b 是 a 的**逆元素**.

若幺半群 S 中的元素 a 有逆元素，则 a 的逆元素是唯一的. 事实上，设 b,c 都是 a 的逆元素，则

$$b=be=b(ac)=(ba)c=ec=c.$$

记 a 的逆元素为 a^{-1}.

偶数集合 $S=\{\cdots,-4,-2,0,2,4,\cdots\}$ 关于通常数的乘法构成半群，但不构成幺半群.

偶数集合 $S=\{\cdots,-4,-2,0,2,4,\cdots\}$ 关于通常数的加法构成幺半群，0 是单位元，其中的非零元素都是可逆元.

若半群 S 满足

$$ab=ba,\quad \forall a,b\in S,$$

则称半群 S 为**交换半群**.

偶数集合 $S=\{\cdots,-4,-2,0,2,4,\cdots\}$ 关于乘法构成交换半群.

定义 1.1.3 设 H 是半群 S 的一个非空子集，若 H 关于半群 S 的运算也构成半群，则称 H 是 S 的一个**子半群**.

半群 S 的非空子集 H 是 S 的一个子半群的充要条件是 H 关于 S 的运算封闭，即

$$ab\in H,\quad \forall a,b\in H.$$

1.1.2 群的定义

定义 1.1.4 设 G 关于二元运算“$\circ$”是一个半群，如果 G 还满足：

(1) G 有单位元 e；

(2) G 中每一元素都有逆元素，

则称 G 关于“$\circ$”是一个**群**，记为 $(G,\circ)$，简记为 G.

当群 $(G,\circ)$ 中乘法“$\circ$”满足交换律时，称 $(G,\circ)$ 为**交换群**或 **Abel 群**.

有时用“+”表示 Abel 群中的运算，并称其为加法，称 $a+b$ 为 a 与 b 的和，此时也称 Abel 群为**加法群**.

通常记加法群中的单位元为 0，称加法群中元素 a 的逆元为 a 的**负元**，记为 $-a$.

整数集合 $\mathbf{Z}=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$ 关于通常数的加法构成交换群.

如果群 G 所含元素的个数有限，则称 G 是**有限群**；如果群 G 含无限多个元素，则称 G 是**无限群**.

称有限群 G 所含元素的个数为 G 的**阶**，记为 $|G|$.

设 n 是一个取定的正整数，$a,b\in\mathbf{Z}$，如果 a 和 b 被 n 除的余数相同，则称 a 与 b 模 n **同余**，记为 $a\equiv b(\mathrm{mod}n)$. 称

$$\bar{a}=\{x\in\mathbf{Z}\mid x\equiv a(\mathrm{mod}n)\}$$

为 a 所在的**模 n 剩余类**，简称**剩余类**. 称 a 为 $\bar{a}$ 的代表元.

显然，$\bar{a}$ 由所有形如 $nq+a(q=0,\pm1,\pm2,\cdots)$ 的整数构成.

显然 $\bar{a}=\bar{b}$ 当且仅当 $n|a-b$，即 a 和 b 属于同一个模 n 剩余类当且仅当 $n|a-b$.

称 $\bar{a}$ 中的最小非负整数为 a 模 n 的**最小非负剩余**，记为 $\langle a\rangle_n$. 例如，$\langle 11\rangle_7=4$. 称 $0,1,\cdots,n-1$ 这 n 个数为模 n 的**最小非负完全剩余系**.

记 $\mathbf{Z}_n=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{n-1}\}$ 是以 n 为模的剩余类集.

例 1.1.1 在 $\mathbf{Z}_n$ 中规定

$$\bar{a}+\bar{b}=\overline{a+b},\quad \forall a,b\in\mathbf{Z},$$

则 $(\mathbf{Z}_n;+)$ 是交换群. 称 $(\mathbf{Z}_n;+)$ 为**模 n 剩余类加群**.

1.1.3 子群

定义 1.1.5 设 H 是群 G 的一个非空子集，若 H 关于群 G 的运算也构成群，则称 H 是群 G 的一个**子群**，记为 $H\leqslant G$.

定理 1.1.1 群 G 的非空子集 H 是 G 的子群的充要条件是：

(1) $ab\in H,\forall a,b\in H$；

(2) $a^{-1}\in H,\forall a\in H$.

证明 必要性. 由子群的定义立即得到.

充分性. 由 G 中结合律成立，故 H 中结合律也成立，再由(1)，H 对 G 的乘法封闭，因而 H 是半群. 由(2)，H 中每个元素 a 的逆元也在 H 中，并且 $e=aa^{-1}\in H$. 因此 H 是 G 的子群. □

定理 1.1.2 群 G 的非空子集 H 是 G 的子群的充要条件是

$$ab^{-1}\in H,\quad \forall a,b\in H.$$

证明 必要性显然，下面证充分性. 设 $a\in H$，从而 $e=aa^{-1}\in H$. 因此，对任意 $b\in H$，有 $b^{-1}=eb^{-1}\in H$. 若 $a,b\in H$ 知 $ab=a(b^{-1})^{-1}\in H$. 由定理 1.1.1 知，H 是 G 的子群. □

定理 1.1.3 群 G 的有限非空子集 H 是 G 的子群的充要条件是

$$ab\in H,\quad \forall a,b\in H.$$

证明 必要性显然，下面证充分性. 由于结合律，消去律在 G 中成立，因此在 H 中也成立，因为 H 对 G 的运算封闭，所以 H 是满足消去律的有限半群，所以 H 是 G 的子群(习题 1 第 5 题). □

设 S 是群 G 的一个非空子集，正整数集合 $\mathbf{Z}^+=\{1,2,3,\cdots\}$，记

$$S^{-1}=\{a^{-1}\mid a\in S\},$$

那么，集合

$$H=\{a_1a_2\cdots a_n\mid a_i\in S\cup S^{-1},n\in\mathbf{Z}^+\}$$

是 G 的一个子群. 称其为由子集 S 生成的子群，记为 $\langle S\rangle$.

如果群 G 可由一个元素生成，即 $G=\langle a\rangle$，则称 G 是循环群.

容易证明，循环群的子群还是循环群.

定义 1.1.6 设 H 是群 G 的一个子群，a 是 G 中一个元素，令

$$aH=\{ax \mid x\in H\},\quad Ha=\{xa \mid x\in H\},$$

称 aH 为 H 在 G 中的一个左陪集，Ha 为 H 在 G 中的一个右陪集.

记 $\varnothing$ 为空集.

定理 1.1.4 设 H 是群 G 的子群，$a,b\in G$，则

(1) $eH=H$，并且 a 在陪集 aH 中.

(2) aH 与 H 含有元素个数相同.

(3) $aH=H\Leftrightarrow a\in H$.

(4) $aH=bH\Leftrightarrow a^{-1}b\in H$.

(5) 若 $b\in aH$，则 $bH=aH$.

(6) aH 与 bH 或者相等或者不相交.

(7) $\bigcup\limits_{a\in G}aH=G$.

证明 (1) 是明显的.

(2) 对任意 $x,y\in H$，因为 $x=y\Leftrightarrow ax=ay$，因而令

$$\varphi:ah\to h,\quad \forall h\in H,$$

则 φ 是 aH 到 H 的双射，因此(2)成立.

(3) $\Rightarrow$ 由 $aH=H$ 知，方程 $ax=e$ 在 H 中可解，即存在 $h\in H$，使 $ah=e$，所以 $a=h^{-1}\in H$.

$\Leftarrow$ $a\in H$，那么 $aH\subseteq H$，另外，$\forall h\in H$，方程 $ax=h$ 在 H 中可解，故 $h\in aH$，$H\subseteq aH$，从而 $aH=H$.

(4) 因为 $aH=bH\Leftrightarrow H=a^{-1}bH$，再由(3)得 $H=a^{-1}bH\Leftrightarrow a^{-1}b\in H$，所以(4)成立.

(5) 若 $b\in aH$，则有 $h\in H$，使 $b=ah$，于是

$$bH=ahH=aH.$$

(6) 如果 $aH\cap bH\neq\varnothing$，设 $c\in aH$，同时 $c\in bH$，由(5)知

$$cH=aH,\quad cH=bH,$$

因此 $aH=bH$.

(7) 因为每个元素 a 都属于一个左陪集 aH，故(7)成立. □

由定理 1.1.4 的(6)、(7)知群 G 的每个子群 H 都给群 G 带来一个分类，每一类就是一个左陪集. 于是，当 G 为有限群时，G 可以分解成一些互不相交的左陪集的并，即

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH,$$

其中 $a_1 = e$，并且，当 $i \neq j$ 时，有 $a_iH \cap a_jH = \varnothing$，这个式子称为 G 对 H 的左陪集分解式，称 $a_1, a_2, \cdots, a_r$ 为 H 在 G 中的一个左陪集代表系. 对应地，也有 G 对 H 的右陪集分解式：

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_r.$$

称 r 为 H 在 G 中的指数，记为 $[G:H]$.

因为子群 H 与其每个左陪集 $a_iH(i=1,2,\cdots,r)$ 所含元素个数相同，所以由群对子群的陪集分解式可以得到如下定理.

定理 1.1.5(Lagrange 定理) 设 G 是有限群，H 是群 G 的一个子群，则

$$|G| = |H|[G:H].$$

由 Lagrange 定理可知，有限群 G 中每个元素的阶都是 $|G|$ 的约数. 从而若 $|G| = p$ 是个素数，则 G 必为循环群.

1.1.4 正规子群

定义 1.1.7 设 N 是群 G 的一个子群，若对任意 $a \in G$ 都有 $aN = Na$，则称 N 是群 G 的一个**正规子群**，记为 $N \lhd G$.

显然，$\{e\}$ 和 G 都是群 G 的正规子群.

设 N 是群 G 的一个正规子群，记 $G/N = \{aN \mid a \in G\}$ 为 N 在 G 中所有陪集的集合. 在 G/N 中规定乘法运算“$\cdot$”如下：

$$aN \cdot bN = abN, \quad \forall a,b \in G.$$

可以证明，两个陪集的乘积与代表元的选取无关.

定理 1.1.6 设 N 是群 G 的一个正规子群，则 G/N 关于上述运算“$\cdot$”构成群，称其为 G 对 N 的**商群**.

定义 1.1.8 设 G 和 G' 是两个群，σ 是 G 到 G' 的映射，如果

$$\sigma(ab) = \sigma(a)\sigma(b), \quad \forall a,b \in G,$$

则称 σ 是群 G 到群 G' 的**群同态映射**，简称**同态**. 若同态 σ 是满射，则称 σ 是**满同态**，这时称 G 与 G' 同态，记为 $G \overset{\sigma}{\sim} G'$. 若同态 σ 是单射，则称 σ 是**单同态**；若同态 σ 是双射，则称 σ 是**同构映射**，简称**同构**，此时称 G 与 G' **同构**，记为 $G \cong G'$.

定理 1.1.7(第一同态定理) 设 σ 是群 G 到群 G' 的群同态映射，则同态核 $N = \ker\sigma$ 是群 G 的正规子群，且

$$\sigma(x) = \sigma(y) \iff xN = yN, \quad \forall x,y \in G.$$

证明 由定理 1.1.1 知 $\ker\sigma$ 是 G 的子群. $\forall g \in G$，$\forall a \in \ker\sigma$，

$$\sigma(g^{-1}ag) = \sigma(g^{-1})\sigma(a)\sigma(g) = \sigma(g)^{-1}e'\sigma(g) = e',$$

其中 e' 是 G' 的单位元，故 $g^{-1}ag\in\ker\sigma$，$\ker\sigma$ 是 G 的正规子群.

若 $x,y\in G$，则

$$\begin{aligned}\sigma(x)=\sigma(y) &\Leftrightarrow \sigma(x)^{-1}\sigma(y)=\sigma(x^{-1})\sigma(y)=\sigma(x^{-1}y)=e'\\ &\Leftrightarrow x^{-1}y\in\ker\sigma=N \Leftrightarrow x^{-1}yN=N \Leftrightarrow yN=xN.\end{aligned}$$ □

定理 1.1.8(第二同态定理) 设 N 是群 G 的一个正规子群，定义映射

$$\begin{aligned}&\sigma: G\to G/N,\\ &g\mapsto gN,\quad \forall g\in G,\end{aligned}$$

则 σ 是 G 到 G/N 的满同态，且 $\ker\sigma=N$.

证明 显然 σ 是 G 到 G/N 上的满映射，并且对任意 $x,y\in G$，有

$$\sigma(xy)=xyN=xN\cdot yN=\sigma(x)\sigma(y),$$

即 σ 是 G 到 G/N 上的同态，因此 $G\overset{\sigma}{\sim}G/N$.

另外，对任一元素 $a\in G$，有

$$a\in\ker\sigma \Leftrightarrow \sigma(a)=aN=N \Leftrightarrow a\in N,$$

故 $\ker\sigma=N$. □

定理 1.1.9(第三同态定理) 设 σ 是群 G 到群 G' 的同态满射，即 $G\overset{\sigma}{\sim}G'$，$\ker\sigma=N$，则 $G/N\cong G'$.

证明 记 $G/N=\{gN\mid g\in G\}$. 于是对任一 $gN\in G/N$，由 $G\overset{\sigma}{\sim}G'$，$g\in G$，故有 $\sigma(g)\in G'$，令

$$\tau: gN\to\sigma(g),$$

由第一同态定理知，τ 的像与陪集的代表元的选取无关，即若 $g_1N=g_2N$，则有 $\sigma(g_1)=\sigma(g_2)$，因此 τ 是 G/N 到 G' 的映射.

对任意 $g'\in G'$，由 $G\overset{\sigma}{\sim}G'$ 知，存在 $g\in G$，使 $\sigma(g)=g'$，因此有

$$\tau(gN)=\sigma(g)=g',$$

即 τ 是满射.

对任二元素 $g_1N,g_2N\in G/N$，有

$$\begin{aligned}g_1N\neq g_2N &\Leftrightarrow g_1^{-1}g_2N\neq N \Leftrightarrow g_1^{-1}g_2\notin N\\ &\Leftrightarrow \sigma(g_1^{-1}g_2)\neq e' \Leftrightarrow \sigma(g_1)^{-1}\sigma(g_2)\neq e'_1\\ &\Leftrightarrow \sigma(g_1)\neq\sigma(g_2),\end{aligned}$$

故 τ 是单射. 因此 τ 是双射. 再由

$$\begin{aligned}\tau(g_1N\cdot g_2N)&=\tau(g_1g_2N)=\sigma(g_1g_2)=\sigma(g_1)\sigma(g_2)\\ &=\tau(g_1N)\tau(g_2N),\end{aligned}$$

因此 τ 是 G/N 到 G' 的同构映射，$G/N\cong G'$. □

上述三个定理统称为同态基本定理，它们一起揭示了群与其商群之间的内在联系. 群 G 的正规子群与商群是相互决定的，G 的每一个同态像都同构于它的一个商群. 因此，如果能找出 G 的所有不同的正规子群，那么也就掌握了 G 的所有的同态像.

定理 1.1.10(第一同构定理) 设 σ 是群 G 到群 G' 的同态满射，即 $G\overset{\sigma}{\sim}G'$，如果 H' 是 G' 的正规子群，H 是 H' 的完全原像，那么，H 是 G 的正规子群，并且

$$G/H\cong G'/H'.$$

证明 设 τ 是 G' 到 G'/H' 上的自然同态，即

$$\tau: g'\to g'H',\quad \forall g'\in G',$$

其同态核为 H'，由

$$G\overset{\sigma}{\sim}G'\overset{\tau}{\sim}G'/H'$$

知 σ 与 τ 的合成映射 $\tau\sigma$ 是 G 到 G'/H' 上的满射.

对任意 $g_1, g_2\in G$，由

$$\begin{aligned}\tau\sigma(g_1g_2)&=\tau[\sigma(g_1g_2)]=\tau[\sigma(g_1)\cdot\sigma(g_2)]\\&=(\tau\sigma)(g_1)(\tau\sigma)(g_2)\end{aligned}$$

知 $\tau\sigma$ 是 G 到 G'/H' 上的同态映射. 因此

$$G\overset{\tau\sigma}{\sim}G'/H'.$$

下面证明 $\ker(\tau\sigma)=H$. 事实上

$$x\in\ker(\tau\sigma)\iff\tau\sigma(x)=\sigma(x)H'=H'\iff\sigma(x)\in H'\iff x\in H.$$

于是 $H=\ker(\tau\sigma)$，由定理 1.1.7 知，H 是 G 的正规子群，再由定理 1.1.9 知 $G/H\cong G'/H'$. □

定理 1.1.11(第二同构定理) 设 N 是群 G 的正规子群，如果 H 是 G 的子群，则 $N\lhd HN$，$(H\cap N)\lhd H$，且

$$H/H\cap N\cong HN/N.$$

证明 容易证明 $N\lhd HN$，$(H\cap N)\lhd H$，HN/N 中的每个元素都是 N 的陪集. 我们在 H 与 HN/N 之间建立映射

$$\sigma: h\to hN,\quad \forall h\in H.$$

容易知道 σ 是一个满射，并且对任意 $h_1, h_2\in H$，

$$\sigma(h_1h_2)=h_1h_2N=h_1Nh_2N=\sigma(h_1)\sigma(h_2).$$

因此 σ 是 H 到 HN/N 上的同态映射，$H\overset{\sigma}{\sim}HN/N$.

如果 $x\in H$,那么

$$x\in \ker\sigma \Leftrightarrow xN=N \Leftrightarrow x\in N \Leftrightarrow x\in H\cap N.$$

因此,$\ker\sigma=H\cap N$,由定理 1.1.9 得

$$H/H\cap N\cong HN/N.$$ □

1.2 环的基本概念

1.2.1 环的定义

定义 1.2.1 设 R 是一个非空集合,如果 R 有两种代数运算,一种称作加法,一种称作乘法,这两种运算满足如下条件:

(1) 对加法"+",R 是交换群;

(2) 对乘法"·",R 是半群;

(3) 乘法对加法满足分配律,即

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca,\quad \forall a,b,c\in R,$$

则称 R 关于这个加法和乘法构成一个**环**. 记为$(R;+,\cdot)$,简记为 R.

通常将环 R 对加法的零元记为 0.

如果环 R 的乘法半群有单位元,将这个单位元记为 1. 此时,称 R 为有 1 的环.

如果环 R 对乘法构成交换半群,则称 R 为**交换环**.

设 R 是一个环,记 $R^+=R\backslash\{0\}$是 R 中所有非零元素构成的集合. 如果$(R^+,\cdot)$是群,则称 R 是一个**除环**(或**体**). 称交换除环为**域**.

显然,除环至少有两个元素 0 和 1.

设 P 是一个非空数集(元素均为复数的集合),如果 P 关于数的加法和乘法构成一个环,则称 P 是一个**数环**;如果 P 关于数的加法和乘法构成一个域,则称 P 是一个**数域**.

偶数集、整数集关于通常数的加法和乘法运算都构成数环. 有理数集、实数集和复数集关于通常数的加法和乘法运算均构成数域.

用 $\mathbf{Z}$ 表示整数环,用 $\mathbf{Q},\mathbf{R},\mathbf{C}$ 分别表示有理数域、实数域和复数域.

例 1.2.1 设$(\mathbf{Z}_n;+)$是模 n 剩余类加群. 规定

$$\bar{a}\cdot\bar{b}=\overline{a\cdot b},\quad \forall a,b\in\mathbf{Z}_n,$$

则$(\mathbf{Z}_n;+,\cdot)$是有 1 的交换环. 称$(\mathbf{Z}_n;+,\cdot)$为**模 n 剩余类环**,简记为 $\mathbf{Z}_n$.

例 1.2.2 数域 F 上 $n(\geqslant 2)$阶矩阵全体 $F^{n\times n}$关于通常矩阵的加法和乘法运算构成环,但不构成交换环.