Galois环上特殊矩阵的分类及其应用

吴炎 著

科学出版社
www.sciencep.com

Galois 环上特殊矩阵的分类及其应用

吴 炎 著

科 学 出 版 社

北 京

内 容 简 介

本书主要讨论了 Galois 环上有限典型群理论中几类特殊矩阵的分类及其应用，论述了在特殊 Galois 环上典型群的作用之下，几类特殊矩阵的标准形、特殊矩阵集合的轨道和轨道的长度，以及典型群的阶的计算，并阐述了这些分类结果在实验设计、编码和矩阵广义逆计数理论等方面的应用. 全书主要采用环上矩阵群方法和组合计数方法为主要叙述和论证工具，它丰富了环上典型群及其应用研究、组合计数理论及矩阵论等方面的内容.

本书适合于高等学校数学系高年级学生、研究生及数学工作者使用，也可以作为高等学校数学系高年级学生的选修课教材，数学及信息类专业研究生的教材或教学参考书.

图书在版编目(CIP)数据

Galois 环上特殊矩阵的分类及其应用/吴炎 著. —北京：科学出版社，2006

ISBN 7-03-017211-6

I. G… II. 吴… III. 环上矩阵-分类及应用 IV.O153.3

中国版本图书馆 CIP 数据核字(2006)第 045718 号

责任编辑：张 扬/责任校对：陈丽珠

责任印制：安春生/封面设计：王 浩

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

新蕾印刷厂印刷

科学出版社编务公司排版制作

科学出版社发行 各地新华书店经销

*

2006 年 7 月第 一 版 开本：B5 (720×1000)

2006 年 7 月第一次印刷 印张：12

印数：1—2 000 字数：225 000

定价：36.00 元

(如有印装质量问题，我社负责调换〈环伟〉)

前　言

我国开展典型群理论的研究，是著名数学家华罗庚先生于 20 世纪 50 年代回国后开始的. 在 20 世纪中叶，以华罗庚先生为首的中国学者们，在典型群研究的诸多领域，取得了丰硕的研究成果(见 1963 年华罗庚和万哲先著的《典型群》)，并得到了国外学者的高度评价，他们把华罗庚先生为代表的中国典型群研究群体称为典型群研究的“中国学派”.

随着典型群理论研究的不断深入和研究领域的逐步扩大，我国典型群理论研究的学者们在典型群及其应用研究方面也继续做出了重要的贡献。其中有限域上典型群的几何学——典型群研究的主要领域之一，于 20 世纪 60 年代由万哲先首先在国内开始了这一领域的研究，它主要研究在各种有限典型群作用下向量空间的子空间所分成的轨道数以及一条轨道中子空间的个数，并研究各轨道生成的格，以及结合方案、实验设计、认证码的构作等。万哲先院士同他的学生群体在有限域上典型群的几何学理论和应用研究方面做出了卓越的贡献，主要研究成果汇集在《Geometry of Classical Groups over Finite Fields》、《有限几何与不完全区组设计的一些研究》以及《有限典型群子空间轨道生成的格》等著作中.

作为有限典型群的几何学的推广和发展的另一方面，是研究有限局部环上的相关问题，如研究有限交换环上典型群的阶、有限局部环上由某一类矩阵构成的矩阵集的等价、或合同或共轭分类，以及用有限局部环上矩阵构作认证码、结合方案等. 本书作者于 2001 年开始，有幸在东北师范大学与南基洙教授合作，在有限交换环上典型群几何学方面作了一些研究工作，如研究某些由同阶特殊矩阵构成的集合(或矩阵模)的分类及其在构作结合方案或卡氏认证码、矩阵广义逆计数理论及几何格等方面的应用. 经过几年的努力，本书作者将取得的点滴研究成果汇成本书.

本书主要在有限局部环上利用线性群对某些由同阶特殊矩阵构成的集合进行作用，研究这些集合的合同或共轭分类，以及这些集合被分成的轨道数，并计算每一个轨道中的矩阵个数；另外还研究了这些分类结果在构作结合方案或卡氏认证码等应用问题，以及某些非正常形式的典型群的阶和矩阵广义逆的计数问题. 具体来说，在第 2 章研究并确定了有限局部环 $R=Z/p^kZ$ 上特殊矩阵如交错矩阵、对称和斜对称矩阵及 s 次幂等矩阵等的标准形式；在第 3 章，介绍了有限局部环 $\boldsymbol{R}$ 上矩阵分类所依赖的典型群的阶的计算，并讨论了非正常形式的伪辛群和正交群的阶；在第 4 章中讨论了几类特殊的矩阵集合的分类计数定理，以及某些典型

的矩阵方程解数的确定问题和分类结果在矩阵广义逆的计数方面的应用; 最后在第 5 章, 利用了矩阵分类结果和矩阵标准形研究结合方案和卡氏验证码等的构作问题, 也讨论了相关的矩阵 Kronecker 积的广义逆性质及矩阵半群同态等. 为了便于阅读, 作者在第 1 章介绍了本书所用的一些基础知识. 全书主要以矩阵群方法和组合计数方法为工具, 叙述和论证我们研究所得的结果.

本书主要汇聚作者与主要合作者南基洙教授近几年的一些研究成果, 有些成果是作者和南基洙教授合作取得的未曾发表的新成果(如书中 2.4 节、3.3 节等). 另外本书也介绍了必须运用到的一些相关研究成果(如万哲先院士、游宏教授和孙琦教授等的有关结果), 对基础知识以及相关研究进展的分析和介绍方面也引用了许多相关的参考文献, 作者对书中所涉及引用的中外文作者表示衷心的感谢, 特别是向仔细审阅本书初稿多遍并提出了宝贵修改意见的南基洙教授、郑宝东教授表示衷心的感谢!

本书系 2006 年 3 月申报的海南省教育厅科研项目,也得到海南省自然科学基金项目和琼州大学的部分基金资助, 作者在此对海南省教育厅和海南省科技厅以及我校有关领导表示衷心的感谢! 也对课题组成员霍元极教授、王鸿绪教授、王恩周副教授、汪文彬老师、符晓芳老师、李足老师和符昌昭老师、黄敏老师等的支持和帮助表示感谢!

由于作者水平所限及成书时间仓促, 书中难免有不妥之处, 恳请读者批评指正.

吴　炎

2006 年 4 月

目　录

第 1 章　代数学基础

为了便于读者阅读，本章首先介绍代数学的一些基础知识，所介绍的基本定理和基本结论多数都未加证明，它们都能在常见的代数学文献中找到，读者可以参见文献[1]~[13]. 本书中我们用 R 表示有单位元 1 的交换环(或某一个特定的 Galois 环)，用 F 表示域.

1.1　群与环的定义

定义 1.1.1　设非空集合 G 带有一个二元代数运算“ · ”(叫做乘法)，如果它满足

(1) 结合律: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $a,b,c \in G$;

那么称$(G, \cdot)$是一个半群，简称 G 是一个半群，半群的乘法有时被省略，如 $a \cdot b$ 记为 ab.

如果半群 G 还满足

(2) G 中存在单位元 e 满足: $ea = ae = a$, $\forall a \in G$;

(3) G 中任意元 a 存在逆元 a^{-1} 满足: $a^{-1}a = aa^{-1} = e$;

那么称$(G, \cdot)$是一个群，简称 G 是一个群.

如果群 G 还满足

(4) 交换律: $ab = ba$, $a,b \in G$;

那么称 G 是一个交换群或 Abel 群. 有时交换群的运算也用加法“+”来表示，这时其单位元记为 0，元素 a 的逆元记为$-a$，群 G 称为加法群.

定义1.1.2　如果一个群 G 的元素的个数是有限的，就称这个群是有限群，否则，这个群就叫做无限群. 有限群 G 的元素个数记为$|G|$，叫做群 G 的阶.

定理 1.1.1　设非空集合 G 带有一个二元代数运算“ · ”(叫做乘法)，如果 G 中元素对于运算“ · ”，满足结合律和消去律，那么 G 是一个群.

例 1.1.1　设 $G = \{1, -1\}$，在数的乘法“ · ”下成为一个群，它的单位元是 1. -1 的逆元是它本身.

例 1.1.2　设 V 是实数域上 n 维向量空间，V 中的全体向量在加法下也构成一个群，这个群的单位元是零向量.

例 1.1.3　设 $R = Z$ 是全体整数组成的集合，易见$(R, +)$是一个加法群. 而 R 对于通常数的乘法作成一个半群，但它对数的乘法不能构成群，因为有的整数对

于乘法没有逆元，如 0 就没有逆元，但这个乘法半群有单位元$e=1$，且R中元素对于乘法和加法满足下面条件:

(1) 对于任意$a,b,c\in R$，有$(a+b)\cdot c=a\cdot c+b\cdot c$;

(2) 对于任意$a,b,c\in R$，有$c\cdot(a+b)=c\cdot a+c\cdot b$;

像这样的带有两种运算“+”和“·”的非空集合R，我们称为一个环，记为$(R,+,\cdot)$.

一般地，我们给出如下定义:

定义 1.1.3　非空集合R称为一个环，如果在R上定义了两种运算“+”和“·”，且适合下列条件:

(1) $(R,+)$是一个加法群，其零元素记为 0;

(2) 对于任意$a,b,c\in R$，有$(a\cdot b)\cdot c=a\cdot(b\cdot c)$;

(3) 对于任意$a,b,c\in R$，有

$$(a+b)\cdot c=a\cdot c+b\cdot c,$$

$$c\cdot(a+b)=c\cdot a+c\cdot b.$$

对于环的乘法“·”通常省去，如$a\cdot b$记为ab.

若在环R中存在元素e(对乘法来说)，使得对任意的$a\in R$，有$e\cdot a=a\cdot e=a$，则称这个环是有单位元(或恒等元)的环. 如果R是有单位元的环，并且还满足下面条件:

(4) 对于任意$a,b\in R$，有$ab=ba$;

那么称R是一个有单位元的交换环.

显然，例 1.1.3 给出的环$(R,+,\cdot)$是有单位元的环，其单位元素为$e=1$(对乘法来说)，且它也是交换环，因此R是一个有单位元的交换环.

为了以下讨论方便，我们再给出如下特殊的矩阵乘法半群和矩阵群的例子.

例 1.1.4　设R是一个有单位元的交换环，用$M_n(R)$和$GL_n(R)$分别表示R上n阶矩阵所构成的集合和n阶可逆矩阵所构成的集合，I_n或$I^{(n)}$表示$M_n(R)$(或$GL_n(R)$)中n阶单位矩阵，而0_n或$0^{(n)}$表示其中的n阶零矩阵. 则$M_n(R)$关于矩阵的乘法作成一个半群，而$GL_n(R)$关于矩阵的乘法作成一个群，叫做n级线性群.

显然，$M_n(R)$对于矩阵的加法和乘法可做成一个环，叫做R上的n阶矩阵环，其中I_n是它的单位元，而零矩阵0_n就是它的零元.

1.2　子群与陪集

定义 1.2.1　设G是一个群，W是群G的一个非空子集，如果对于群G的运

算，W 作成一个群，那么称 W 是群 G 的一个子群，记作 $W \leqslant G$.

对于任何群 G 都有两个子群 G 和 $\{e\}$，它们叫做 G 的平凡子群. 群 G 的中心 $C=\{c \in G | cg=gc, \forall g \in G\}$ 必是 G 的子群.

显然子群的概念具有“传递性”，即若 G 是一个群，且 $W \leqslant G$，$H \leqslant W$，则 $H \leqslant G$.

例 1.2.1 设 R 是一个有单位元的交换环，用 $GL_n(R)$ 表示 R 上所有 n 阶可逆矩阵关于矩阵的乘法所做成的线性群. 若令

$$SL_n(R)=\{P \in GL_n(R) | \det P=1\},$$

则由子群的定义容易知道，$SL_n(R)$ 对于矩阵的乘法也做成 $GL_n(R)$ 的一个子群，叫做 n 级特殊线性群.

为了更好地判别群的非空子集在什么条件下做成子群，我们引入下列命题.

定理 1.2.1 设 G 是一个群，W 是群 G 的一个非空子集，如果 W 适合下列两个条件之一，那么 W 是群 G 的子群:

(1) 对任意的元素 $a,b \in W$，有 $ab^{-1} \in W$.

(2) 对任意的元素 $a,b \in W$，有 $ab \in W$，$a^{-1} \in W$.

推论 1.2.2 设 W 是群 G 的有限子集，若对任意的 $a,b \in W$，均有 $ab \in W$，则 W 是 G 的子群.

由定理 1.2.1 和推论 1.2.2，容易看出线性群 $GL_n(R)$ 的如下两个非空子集都做成子群.

例 1.2.2 设 R 是一个交换环，$n=2v(v \in Z^+, v \geqslant 1)$，且

$$H=\begin{pmatrix} 0 & I^{(v)} \\ -I^{(v)} & 0 \end{pmatrix},$$

令

$$Sp_n(R)=\{P \in GL_n(R) | P'HP=H\},$$

则 $Sp_n(R)$ 做成 $GL_n(R)$ 的一个子群，叫做 R 上 n 级辛群.

例 1.2.3 设 R 是一个交换环，$n=2v(v \in Z^+, v \geqslant 1)$，且

$$H=\begin{pmatrix} 0 & I^{(v)} \\ I^{(v)} & 0 \end{pmatrix},$$

令

$$O_n(R)=\{P\in GL_n(R)\big|P'HP=H\},$$

则$O_n(R)$做成$GL_n(R)$的一个子群，叫做R上n级正交群.

由定理1.2.1和推论1.2.2，容易得到:

例1.2.4　设G是一个群，$\{H_\alpha\}_{\alpha\in I}$是群$G$的一个子群族，则$\bigcap\limits_{\alpha\in I}H_\alpha$仍是群$G$的一个子群.

定义 1.2.2　设S是群G的一个子集，把群G中包含集合S的所有子群的交，称为由S生成的子群，记为$<S>$.

由定义容易看出，$<S>\neq\phi$，并且若S是群G的一个子群，则$S=<S>$.

定理 1.2.3　设S是群G的一个子集，N是正整数集，令

$$\overline{S}=\{a_1^{v_1}\cdot a_2^{v_2}\cdots a_n^{v_n}\big|n\in N,a_i\in S,v_i=\pm1;i=1,2,\cdots,n\},$$

则有$<S>=\overline{S}$.

证明　对于$\overline{S}$中任意两个元素$a=a_1^{v_1}\cdot a_2^{v_2}\cdots a_n^{v_n}$，$b=b_1^{u_1}\cdot b_2^{u_2}\cdots b_n^{u_n}$($v_i,u_i=\pm1$)，容易看出$ab^{-1}\in\overline{S}$，因此$\overline{S}$是群$G$的一个子群. 设$H$是群$G$的任一个包含$S$的子群，则有$a_i\in S\subseteq H$，故有$a_1^{v_1}\cdot a_2^{v_2}\cdots a_n^{v_n}\in H$，$\overline{S}\subseteq H$　($v_i=\pm1$;　$i=1,2,\cdots,n$)，由定义1.2.2有$<S>=\overline{S}$.　□

设H是群G的子群，如果$H=<S>$，那么S中元素称为H的生成元. 若H是一个有限集，则称它为有限生成的子群. 特别地，若群G可由一个有限集生成，则称群G为有限生成的群. 如果群G可由一个元素生成，那么称群G为一个循环群.

定义 1.2.3　设a是群G的元素，若存在最小正整数n使得$a^n=e$，则称n为a的周期. 若不存在正整数n使得$a^n=e$成立，则说a的周期为零. 元素a的周期用$o(a)$(或$|a|$)表示.

容易证明如下定理

定理 1.2.4　设a是群G的元素，$o(a)=n$，则由a生成的G的循环子群$<a>$的阶恰好等于n.

由此定理可以给出周期的另一个等价定义: 元素a的周期等于子群$<a>$的阶.

为了阐明群的子群所确定的左(或右)陪集的作用，我们在此首先引入等价关系和等价类的有关知识.

定义 1.2.4　设A,B是两个给定的集合，若R是A,B的笛卡儿积$A\times B$的一个子集，即$R\subset A\times B$，则称R是从A到B的一个关系. 特别地，$A\times A$的一个子集称为A上的一个关系.

如果$(a,b)\in R\subset A\times B$，那么称$a$与$b$为$R$相关的，记做$aRb$.

定义 1.2.5 设R是A上的一个关系，若R适合下列条件:

(1) 自反性: 若$a\in A$，则$(a,a)\in R$;

(2) 对称性: 若$(a,b)\in R$，则$(b,a)\in R$;

(3) 传递性: 若$(a,b)\in R$，$(b,c)\in R$，则$(a,c)\in R$;

则称关系R是A上的一个等价关系.

等价关系R常用~表示，即$a\sim b$表示$(a,b)\in R$.

定义 1.2.6 设~是集合A中的一个等价关系，$a\in A$，与a等价的元素全体组成集合A的一个子集，称为a的一个等价类.

用符号$[a]$表示a的等价类.

设~是集合A中的一个等价关系，$a\in A$，$[a]$是a的等价类. 令

$$A/\sim=\{\text{集合 } A \text{ 上的等价类}\},$$

那么，对于任意$[a]$，$[b]\in A/\sim$，若$[a]\neq[b]$，则有$[a]\bigcap[b]=\phi$；也即若$[a]\bigcap[b]\neq\Phi$，则有$[a]=[b]$.

因为，若$[a]\bigcap[b]\neq\Phi$，设$c\in[a]\bigcap[b]$，则有$a\sim c$，$c\sim b$. 于是由传递性有$a\sim b$，因此有$[a]=[b]$.

由此可见，若令I是$A/\sim$中所有等价类的代表元素的集合，则有

$$A=\bigcup_{a\in I}[a].$$

这就是说，若在集合A上定义了一个等价关系~，则这个集合可以被分划成互不相交的等价类之并. 一个集合如果能表示为两两互不相交的子集之并，那么称这些子集族为该集合的一个分划. 上面的分析说明了集合上的一个等价关系，决定该集合的一个分划.

反之，若设$\{A_i\}_{i\in I}$是集合A上的一个分划，即

$$A_i\bigcap A_j=\Phi(i\neq j),\quad A=\bigcup_{i\in I}A_i.$$

我们据此可以定义如下关系

$$R=\{(a,b)\in A\times A\,|\,a,b\in A_i;i\in I\},$$

则容易验证R是集合A上的一个等价关系. 因此，给出集合A上的一个分划，可以得到A上的一个等价关系.

定义 1.2.7 设~是集合A中的一个等价关系，集合A上所有等价类组成的集

合用 $A/\sim$ 表示，称之为集合 A 关于等价关系~的商集.

注意，$A/\sim$ 实际上就是集合 A 的某些子集构成的子集族(或集合)，而 $A/\sim$ 中的元素，就是集合 A 的某个元素 a 所在的等价类 $[a]$，为了方便，这个等价类也常记作 $\bar{a}$.

下面我们来研究群的子群所确定的左(或右)陪集及其作用.

定义 1.2.8　设 H 是群 G 的子群，$a \in G$，则称集合 $Ha = \{ha | h \in H\}$ 为群 G 的一个右陪集，称集合 $aH = \{ah | h \in H\}$ 为群 G 的一个左陪集.

容易证明

定理 1.2.5　设 H 是群 G 的子群，a，$b \in G$；那么

(1) $Ha = Hb$ (或 $aH = bH$)的充要条件是 $ab^{-1} \in H$ (或 $a^{-1}b \in H$)；

(2) $|Ha| = |Hb|$，$|aH| = |bH|$；

(3) 若 $Ha \neq Hb$ (或 $aH \neq bH$)，则 $Ha \cap Hb = \Phi$ (或 $aH \cap bH = \Phi$).

令

$$\bar{G} = \{G \text{ 的子群 } H \text{ 的互不相同的右陪集}\} = \{A_1, A_2, \cdots, A_t\},$$

$$(\text{或 } \bar{G} = \{G \text{ 的子群 } H \text{ 的互不相同的左陪集}\}).$$

则从以上性质可以看出，$\bar{G}$ 构成了群 G 的一个分划，且有 $G = \bigcup\limits_{A_i \in \bar{G}} A_i$，$A_i \cap A_j = \Phi (i, j = 1, \cdots, l)$. 并且 $\bar{G}$ 也决定了群 G 的一个等价关系:

$$a \sim b \Leftrightarrow Ha = Hb \Leftrightarrow ab^{-1} \in H.$$

在这个等价关系下的商集就是 $\bar{G}$，也是 G 的子群 H 的右陪集的全体. 因此定义

定义 1.2.9　一个群 G 的一个子群 H 的右陪集(或左陪集)的个数叫 H 在 G 中的指数，记作 $[G: H]$.

由此容易得到

定理 1.2.6(Lagrange 定理)　设 H 是有限群 G 的子群，则有

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

推论 1.2.7　设 a 是有限群 G 的任一个元素，则 a 的周期是 $|G|$ 的因子.

1.3　正规子群和商群

定义 1.3.1　设 H 是群 G 的子群，若对于 G 中任意元素 a，总有 $Ha = aH$ 成

立，则称 H 是群 G 的正规子群(或群 G 的不变子群)，记作 $H \lhd G$.

任何一个群 G 至少有两个正规子群 G 和 $\{e\}$，其中 e 是 G 的单位元素.

定理 1.3.1 设 H 是群 G 的子群，则以下条件是等价的:

(1) 设 H 是群 G 的正规子群;

(2) $aHa^{-1} = H$, $\forall a \in G$;

(3) $aHa^{-1} \subseteq H$, $\forall a \in G$;

(4) $aha^{-1} \in H$, $\forall a \in G$, $\forall h \in H$.

定理 1.3.2 设 G 是交换群，则群 G 的任一子群都是正规子群.

定理 1.3.3 设 H 是群 G 的子群，$[G:\ H]=2$，则 H 是群 G 的正规子群.

定理 1.3.4 群 G 的中心必是群 G 的正规子群. 群 G 的任意个正规子群的交仍是群 G 的正规子群.

定义 1.3.2 若 S 是群 G 的子集，把所有包含 S 的正规子群的交叫做由 S 生成的正规子群.

定理 1.3.5 设 H 是群 G 的子群，令 $N(H) = \{g \in G | gH = Hg\}$ ，则 $N(H)$ 是 G 的正规子群，而 H 是 $N(H)$ 的正规子群.

$N(H)$ 叫做 H 在 G 中的正规化子，它是 G 中包含 H 作为正规子群的“最大”的一个子群. 但注意，若 G 是群，而 $H \leqslant G, K \leqslant H$ ，则有 $K \leqslant G$ ；但若 $H \lhd G, K \lhd H$ ，则未必有 $K \lhd G$.

例 1.3.1 设 R 是实数域，R^* 是 R 的非零元素构成的乘法群，Z 是整数集. 令

$$G = \left\{ \begin{bmatrix} a & c \\ 0 & 1 \end{bmatrix} \middle| a \in R^*, c \in R \right\},$$

$$H = \left\{ \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix} \middle| v \in R \right\},$$

$$K = \left\{ \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} \middle| u \in Z \right\}.$$

则容易验证 $H \lhd G$, $K \lhd H$. 但我们可以证明 K 不是 G 的正规子群.

事实上，对于 $g = \begin{bmatrix} a & c \\ 0 & 1 \end{bmatrix} \in G$ (其中 a 是无理数)和 K 中元素 $w = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}$ $(u \neq 0)$，有

$$g^{-1}wg=\begin{bmatrix}a^{-1} & -a^{-1}c\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & u\\ 0 & 1\end{bmatrix}\begin{bmatrix}a & c\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & -a^{-1}u\\ 0 & 1\end{bmatrix}\notin K\,.$$

定理1.3.6　设 H 是群 G 的子群，$\bar{G}$ 是 H 的全体右陪集所成的商集，规定 $\bar{G}$ 中乘法为

$$(Ha)\cdot(Hb)=H(ab)\,,\tag{1.3.1}$$

则(1.3.1)式是 $\bar{G}$ 上的代数运算的充要条件是 $H\lhd G$.

证明　设 H 是群 G 的正规子群，若有 $Ha=Ha_1, Hb=Hb_1$，则有 $aa_1^{-1}\in H$，$bb_1^{-1}\in H$. 于是有 $ab(a_1b_1)^{-1}=abb_1^{-1}a_1^{-1}=ah_1a_1^{-1}$ (其中 $h_1\in H$)，又由于 H 是群 G 的正规子群，故有 $ah_1\in aH=Ha$，即有 $h_2\in H$，使得 $ah_1=h_2a$ (其中 $h_2\in H$). 因此有 $ah_1a_1^{-1}=h_2aa_1^{-1}\in H$，即有 $ab(a_1b_1)^{-1}\in H$，故有 $Hab=Ha_1b_1$.

反之，若(1.3.1)式定义了 $\bar{G}$ 上的代数运算，即 $\bar{G}\times\bar{G}\to\bar{G}:(Ha,Hb)\to Hab$ 是映射. 若设 $a\in G, b=a^{-1}$，则有 $(Ha,Ha^{-1})\to Haa^{-1}=H$. 但是对于任意 $h\in H, H=Hh$，故有 $(Ha,Ha^{-1})=(Ha,Hha^{-1})\to Haha^{-1}$. 由于 $(Ha,Hb)\to Hab$ 是映射，故必有 $Haha^{-1}=H$，即 $aha^{-1}\in H$，因此 H 是群 G 的正规子群. □

同理可证

定理1.3.7　设 H 是群 G 的子群，$\tilde{G}$ 是 H 的全体左陪集所成的商集，规定 $\tilde{G}$ 中乘法为

$$(aH)\cdot(bH)=(ab)H\,,\tag{1.3.2}$$

则(1.3.2)式是 $\tilde{G}$ 上的代数运算的充要条件是 $H\lhd G$.

定理1.3.8　设 H 是群 G 的正规子群，$\bar{G}$ 和 $\tilde{G}$ 分别是 H 的全体右陪集和全体左陪集所成的商集. 则 $\bar{G}$ 和 $\tilde{G}$ 分别关于(1.3.1)式和(1.3.2)式所定义的运算都分别做成一个群，且 $\bar{G}=\tilde{G}$.

证明　由于 H 是群 G 的正规子群，由定理 1.3.6 可知在 $\bar{G}$ 上可按(1.3.1)式定义运算. 且有

$$(Ha\cdot Hb)\cdot Hc=H(ab)\cdot Hc=Ha(bc)\,,$$

$$Ha\cdot(Hb\cdot Hc)=Ha\cdot Hbc=Ha(bc)\,,$$

于是有

$$(Ha\cdot Hb)\cdot Hc=Ha\cdot(Hb\cdot Hc)\,.$$

又显然有 $H=He$ 是 $\bar{G}$ 的单位元素(e 是 H 的单位元素), 且 Ha^{-1} 是 Ha 的逆元, 因此 $\bar{G}$ 关于运算(1.3.1)做成一个群. 同理可证 $\tilde{G}$ 关于(1.3.2)式所定义的运算也做成一个群.

又由于 H 是群 G 的正规子群, 故对任意 $a\in G$, 有 $Ha=aH$, 因此对于 $\bar{G}$ 中任意元素 Ha 也有 $Ha=aH\in\tilde{G}$, 即 $\bar{G}\subseteq\tilde{G}$. 同样可证 $\bar{G}\supseteq\tilde{G}$, 故有 $\bar{G}=\tilde{G}$. □

定义1.3.3 设 H 是群 G 的正规子群, $\bar{G}$ 是 H 的全体右陪集(或全体左陪集)所成的商集. 称 $\bar{G}$ 在运算 $(Ha)\cdot(Hb)=H(ab)$ (或在运算 $(aH)\cdot(bH)=(ab)H$)下构成的群为 G 的商群, 记作 $\bar{G}=G/H$.

容易证明: 若 G 是交换群, 则 G/H 也是交换群; 若 G 是有限群, 则 G/H 也是有限群, 且有

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

定理1.3.9 设 G 是群, $a,b\in G$, 记 $[a,b]=aba^{-1}b^{-1}$, 称 $[a,b]$ 是 a 和 b 的换位子. 则 G 中所有的换位子生成 G 的子群, 我们称之为 G 的换位子群, 记作 $[G,G]$.

易知 $[G,G]$ 是 G 的正规子群.

定理1.3.10 设 G 是群, $[G,G]$ 是 G 的换位子群. 则商群 $G/[G,G]$ 是交换群, 并且若 $K\lhd G$ 及 G/K 是交换群, 则 $[G,G]\leqslant K$.

设 A,B 是群 G 的两个非空子集, 把 $\{ab|a\in A,b\in B\}$ 叫做 A,B 的积, 记为 AB.

定理 1.3.11 设 A,B 是群 G 的两个子群, 那么

(1) 若 A 是群 G 的正规子群, 则 AB 是 G 的子群;

(2) AB 是 G 的子群充要条件是 $AB=BA$.

定理 1.3.12 设 A,B 是群 G 的两个有限子群, 那么

$$|AB|=\frac{|A||B|}{|A\cap B|},\ \text{特别地当}\ A\cap B=\{e\}\ \text{时, 有}\ |AB|=|A||B|.$$

1.4 群的同态定理

定义1.4.1 设 G_1 和 G_2 都是群, $f:G_1\to G_2$ 是映射, 且对于任意的 $a,b\in G_1$, 都有

$$f(ab)=f(a)f(b),$$

则称 f 是群 G_1 到群 G_2 的同态. 若 f 是单映射, 则称群同态 f 为单同态, 若 f 是满

映射，则称群同态为满同态或映上同态；若 f 是双射，则称群同态 f 为群 G_1 到 G_2 的同构. 群 G 到自身的同态称为自同态，群 G 到自身上的同构称为自同构.

易见，群 G 到自身的所有自同态构成一个乘法半群，群 G 到自身上的所有自同构做成一个群，它们分别记作 $EndG$ 和 $AutG$.

若映射 $f: G_1 \to G_2$ 是群 G_1 到群 G_2 的同构，则记之为 $G_1 \cong G_2$，称群 G_1 与 G_2 同构. 凡同构的群，从代数结构上来看是一样的.

定理1.4.1　若映射 $f: G_1 \to G_2$ 是群 G_1 到群 G_2 的同态，e_1 和 e_2 分别是群 G_1 和 G_2 的单位元素，则有

(1) $f(e_1) = e_2$；

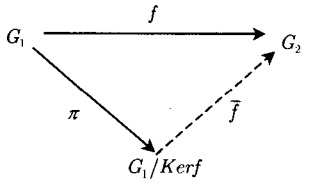
(2) $f(x^{-1}) = f(x)^{-1}$，$x \in G_1$；

(3) $\mathrm{Im} f$ 是 G_2 的子群；

(4) f 的核 $Kerf = \{x \in G_1 \,|\, f(x) = e_2\}$ 是 G_1 的正规子群.

定理1.4.2　设 H 是群 G 的正规子群，则群 G 到商群 G/H 上的自然映射是群同态，称之为自然同态，记为 $\pi: G \to G/H$.

定理1.4.3(同态基本定理)　若映射 $f: G_1 \to G_2$ 是群 G_1 到群 G_2 的满同态，则 f 诱导出 $G_1/Kerf$ 到 G_2 的同构 $\overline{f}: \overline{a} \to \overline{f}(\overline{a})$ ($\overline{a} \in G_1/Kerf$)，其中 $\overline{f}(\overline{a}) = f(a)$，对于 $\forall a \in G_1$ 成立，即有如下交换图(I)



(I)

推论 1.4.4　若 $f: G_1 \to G_2$ 是群 G_1 到群 G_2 的同态，则 $G_1/Kerf \cong \mathrm{Im} f$.

推论 1.4.5　任一群同态 $f: G_1 \to G_2$ 可分解为

$$f = j \circ \overline{f} \circ \eta,$$

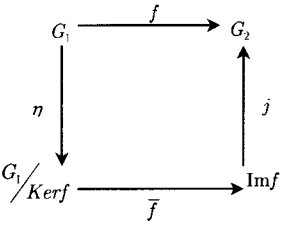
其中 η 是 G_1 到 $G_1/Kerf$ 的自然同态，$\overline{f}$ 是 f 诱导出 $G_1/Kerf$ 到 $\mathrm{Im} f$ 的同构 $\overline{f}: \overline{a} \to \overline{f}(\overline{a})$，$j$ 是 $\mathrm{Im} f$ 到 G_2 的包含映射. 见如下交换图(II)

定理1.4.6(对应定理)　若映射 $f: G_1 \to G_2$ 是群 G_1 到群 G_2 的满同态，e_1 和 e_2 分别是群 G_1 和 G_2 的单位元素，则如下命题叙述成立：

(1) H 是群 G_1 的子群，则 $f(H)$ 是 G_2 的子群；

(2) 若 K 是 G_2 的子群，则 $f^{-1}(K) = \{x \in G_1 \,|\, f(x) \in K\}$ 是 G_1 的子群且

$f^{-1}(K) \supseteq Kerf$;



(II)

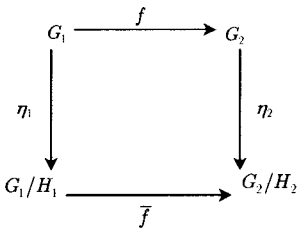
(3) 映射 $H \to f(H)$ 定义了 G_1 的包含 $Kerf$ 的子群集与 G_2 的子群集之间的一一对应，在这个对应下，H 是群 G_1 的正规子群的充要条件是 $f(H)$ 是 G_2 的正规子群；且有

$$G_1/H \cong G_2/f(H).$$

定理 1.4.7 若映射 $f: G_1 \to G_2$ 是群 G_1 到群 G_2 的同态，则

(1) f 是单同态的充要条件是 $Kerf = \{e_1\}$，$e_1 \in G_1$；

(2) 若 H_1 和 H_2 分别是群 G_1 和群 G_2 的正规子群且 $f(H_1) \subseteq H_2$，则存在 $G_1/H_1 \to G_2/H_2$ 的同态 $\overline{f}$，使得 $\eta_2 f = \overline{f}\eta_1$，其中 $\eta_i: G_i \to G_i/H_i\ (i=1,2)$ 是自然同态. 如图(III)



(III)

定理 1.4.8(第一同构定理) 设 H 和 N 都是群 G 的正规子群且 $H \subseteq N$，则有

$$(G/H)/(N/H) \cong G/N.$$

定理 1.4.9(第二同构定理) 设 H 是群 G 的正规子群，K 是群 G 的子群，则 $K \cap H$ 是群 K 的正规子群且有

$$KH/H \cong K/(H \cap N).$$