普通高等教育“十一五”国家级规划教材

北京大学数学教学系列丛书

本科生
数学基础课教材

# 抽象代数 I

赵春来 徐明曜 编著



北京大学出版社
PEKING UNIVERSITY PRESS

北京大学数学教学系列丛书

ISBN 978-7-301-14168-7

责任编辑：刘　勇
封面设计：林胜利

定价：18

北京大学数学教学系列丛书

# 抽象代数 I

赵春来　徐明曜　编著

北京大学出版社
PEKING UNIVERSITY PRESS

**图书在版编目 (CIP) 数据**

抽象代数 I / 赵春来, 徐明曜编著. — 北京: 北京大学出版社, 2008.10

(北京大学数学教学系列丛书)

ISBN 978-7-301-14168-7

I. 抽 … II. ①赵 … ②徐 … III. 抽象代数 – 高等学校 – 教材 IV. O153

中国版本图书馆 CIP 数据核字 (2008) 第 124478 号

书　　名: **抽象代数 I**

著作责任者: 赵春来　徐明曜　编著

责任编辑: 刘　勇

标准书号: ISBN 978-7-301-14168-7/O · 0759

出 版 者: 北京大学出版社

地　　址: 北京市海淀区成府路 205 号　100871

网　　址: http://www.pup.cn

电　　话: 邮购部 62752015　发行部 62750672　编辑部 62752021

出版部 62754962

电子信箱: zpup@pup.pku.edu.cn

印 刷 者: 北京汇林印务有限公司

发 行 者: 北京大学出版社

经 销 者: 新华书店

890mm×1240mm　A5　7 印张　180 千字

2008 年 10 月第 1 版　2008 年 10 月第 1 次印刷

印　　数: 0001—4000 册

定　　价: 18.00 元

# 作者简介

**赵春来** 1945 年 2 月生，1967 年毕业于北京大学数学力学系数学专业，1984 年在北京大学数学系研究生毕业，获博士学位，1987 年晋升为副教授，1992 年晋升为教授，博士生导师.

赵春来长期从事本科生及研究生代数课程的教学以及代数数论的研究工作，讲授过多门本科生和研究生课程，与他人合著了《代数学》、《线性代数引论》、《模曲线导引》、《代数群引论》等著作. 他的研究工作主要集中于椭圆曲线的算术理论以及信息安全方面，在国内外重要学术刊物上发表论文十余篇. 曾获教育部科技进步二等奖 (2004), 北京市优秀教学成果一等奖 (2005), 国家级优秀教学成果二等奖 (2005).

**徐明曜** 1941 年 9 月生，1965 年毕业于北京大学数学力学系数学专业，1980 年在北京大学数学系研究生毕业，获硕士学位，并留校任教. 1985 年晋升为副教授，1988 年破格晋升为教授，博士生导师.

徐明曜长期从事本科生及研究生代数课程的教学以及有限群论的研究工作，讲授过多门本科生和研究生课程，著有《有限群导引》 (下册与他人合作); 科研方面自 20 世纪 60 年代起进行有限 $p$ 群的研究工作，80 年代中期又开创了我国 "群与图" 的研究领域，至今已发表论文 80 多篇，多数发表在国外的重要杂志上，曾获得国家教委优秀科技成果奖 (1985), 国家教委科技进步二等奖 (1995), 周培源基金会数理基金成果奖 (1995).

# 序　言

自 1995 年以来，在姜伯驹院士的主持下，北京大学数学科学学院根据国际数学发展的要求和北京大学数学教育的实际，创造性地贯彻教育部“加强基础，淡化专业，因材施教，分流培养”的办学方针，全面发挥我院学科门类齐全和师资力量雄厚的综合优势，在培养模式的转变、教学计划的修订、教学内容与方法的革新，以及教材建设等方面进行了全方位、大力度的改革，取得了显著的成效．2001 年，北京大学数学科学学院的这项改革成果荣获全国教学成果特等奖，在国内外产生很大反响．

在本科教育改革方面，我们按照加强基础、淡化专业的要求，对教学各主要环节进行了调整，使数学科学学院的全体学生在数学分析、高等代数、几何学、计算机等主干基础课程上，接受学时充分、强度足够的严格训练；在对学生分流培养阶段，我们在课程内容上坚决贯彻“少而精”的原则，大力压缩后续课程中多年逐步形成的过窄、过深和过繁的教学内容，为新的培养方向、实践性教学环节，以及为培养学生的创新能力所进行的基础科研训练争取到了必要的学时和空间．这样既使学生打下宽广、坚实的基础，又充分照顾到每个人的不同特长、爱好和发展取向．与上述改革相适应，积极而慎重地进行教学计划的修订，适当压缩常微、复变、偏微、实变、微分几何、抽象代数、泛函分析等后续课程的周学时．并增加了数学模型和计算机的相关课程，使学生有更大的选课余地．

在研究生教育中，在注重专题课程的同时，我们制定了 30 多门研究生普选基础课程 (其中数学系 18 门)，重点拓宽学生的专业基础和加强学生对数学整体发展及最新进展的了解．

教材建设是教学成果的一个重要体现．与修订的教学计划相配合，我们进行了有组织的教材建设．计划自 1999 年起用 8 年的

时间修订、编写和出版 40 余种教材. 这就是将陆续呈现在大家面前的《北京大学数学教学系列丛书》. 这套丛书凝聚了我们近十年在人才培养方面的思考, 记录了我们教学实践的足迹, 体现了我们教学改革的成果, 反映了我们对新世纪人才培养的理念, 代表了我们新时期的数学教学水平.

经过 20 世纪的空前发展, 数学的基本理论更加深入和完善, 而计算机技术的发展使得数学的应用更加直接和广泛, 而且活跃于生产第一线, 促进着技术和经济的发展, 所有这些都正在改变着人们对数学的传统认识. 同时也促使数学研究的方式发生巨大变化. 作为整个科学技术基础的数学, 正突破传统的范围而向人类一切知识领域渗透. 作为一种文化, 数学科学已成为推动人类文明进化、知识创新的重要因素, 将更深刻地改变着客观现实的面貌和人们对世界的认识. 数学素质已成为今天培养高层次创新人才的重要基础. 数学的理论和应用的巨大发展必然引起数学教育的深刻变革. 我们现在的改革还是初步的. 教学改革无禁区, 但要十分稳重和积极; 人才培养无止境, 既要遵循基本规律, 更要不断创新. 我们现在推出这套丛书, 目的是向大家学习. 让我们大家携起手来, 为提高中国数学教育水平和建设世界一流数学强国而共同努力.

张 继 平

2002 年 5 月 18 日

于北京大学蓝旗营

# 前　言

代数学是数学专业最基本和最重要的基础课程之一，它对学好数学本身以及数学在现代科学技术的很多方面的应用来说都有重要的意义. 因此我们在数学学习的各个阶段都开设了代数课程. 本课程是为学习过高等代数或线性代数的本科生而编写的. 本书可以作为我们为研究生编写的《抽象代数 II》的预备教材.

现代代数学有很多分支，而每个分支又都有众多的抽象的概念，因此初学者大多会觉得抽象代数似乎就是若干概念的堆积，看不出有什么深刻的结果和用途. 在本书中，我们一方面要讲解必要的基础知识，同时也力图使读者能够对于代数学的主要思想和方法有所体会. 例如，在讲解了群的知识之后，我们用群论的方法考查了正多面体，以诠释群论本质上是研究对称的学科；在讲解了环和域之后，我们介绍了它们在几何与数论方面的应用.

本书总的安排大体上依循了我们多年教学中使用的聂灵沼和丁石孙教授编写的《代数学引论》. 该引论是为一学年的代数学教学而编著的. 为了能够将授课时间限制在一个学期之内 (约 45 学时)，本书不得不在内容上作较大的压缩 (也作了一些补充). 第一章 ( 群、环、体、域的基本概念 ) 中把这些代数结构具有共性的部分 (例如子结构、商结构、同态、同构、直和与直积等) 一并作了介绍；第二、三、四章分别讲授群、环、域比较专门的内容；第五章简述了模与格的最基础的一些知识.

前面提到，我们已经出版了《抽象代数 II》作为研究生教材. 由于研究生的生源复杂，其本科和研究生阶段不一定在同一学校学习. 因此，《抽象代数 I》和《抽象代数 II》内容上有一些重叠，其目的是使两部书都尽量做到独立自封，各成一完整的教材.

本书的习题较多，都是经过我们精心挑选的. 其中包含了大量精典的例子，并且给出了比较详细的提示或解答，这有利于读者理解正文的教学内容. 不过我们仍然建议大家尽量独立地给出

解答，而不是直接去看习题提示.

我们要感谢我学院代数组各位同仁，他们参与了本书教学大纲的讨论，并提出了很多有价值的建议.

作 者

2008 年 3 月于北京大学

数学科学学院

# 目　录

# 第 1 章　群、环、体、域的基本概念

本章介绍代数学中最基本、最常见的一些概念和结果.

首先我们回顾一下集合论中的一些简单知识. 设 $A$, $B$ 为两个集合. $\varphi$ 称为由 $S$ 到 $T$ 的一个**映射**, 如果对于任一 $a \in A$, 都唯一存在 $B$ 中的元素 $\varphi(a)$ 与之对应. 此时 $\varphi(a)$ 称为 $a$(在 $\varphi$ 下)的**像**, $a$ 称为 $\varphi(a)$(在 $\varphi$ 下)的**原像** 或**反像**. 一般地, 设 $S$ 为 $A$ 的任一子集, 则 $\{\varphi(a) \mid a \in S\}$ 称为 $S$(在 $\varphi$ 下)的**像**, 常记为 $\varphi(S)$; 设 $T$ 为 $B$ 的任一子集, 则 $\{a \in S \mid \varphi(a) \in T\}$ 称为 $T$ (在 $\varphi$ 下)的**反像**, 常记为 $\varphi^{-1}(T)$. 如果 $A$ 中任意两个不同元素在 $\varphi$ 下的像都不同, 则称 $\varphi$ 为**单射**. 如果 $B$ 中任一元素在 $A$ 中都有原像, 则称 $\varphi$ 为**满射**. 既单又满的映射称为**双射**, 或**一一对应**.

## §1.0　预备知识

作为特殊情形, 集合到自身的映射称为**变换**.

集合 $A$ 与 $B$ 的**笛卡儿积** (亦称为**直积**) 是指 $A$ 的元素与 $B$ 的元素构成的有序对的集合, 即 $\{(a,b) \mid a \in A,\ b \in B\}$, 通常记为 $A \times B$ (类似地可以定义多个乃至无穷多个集合的笛卡儿积). 集合 $A$ 上的一个**二元运算** 即是由 $A \times A$ 到 $A$ 的一个映射. $A$ 上的一个**二元关系**$R$ 定义为 $A \times A$ 的一个子集. 如果 $(a_1, a_2) \in R$, 就称 $a_1$ 与 $a_2$ 有关系 $R$, 记为 $a_1 R a_2$. 设 $R$ 是 $A$ 上的一个二元关系, 如果满足:

(1) 反身性, 即 $aRa$ $(\forall a \in A)$;

(2) 对称性, 即 $a_1 R a_2$ 蕴含 $a_2 R a_1$ $(\forall a_1, a_2 \in A)$;

(3) 传递性, 即 $a_1 R a_2$ 且 $a_2 R a_3$ 蕴含 $a_1 R a_3$ $(\forall a_1, a_2, a_3 \in A)$,

则称 $R$ 为 $A$ 上的一个**等价关系**. 此时 $A$ 中互相等价的元素组成的子集称为一个**等价类**. 任意两个不同等价类的交为空集，整个集合 $A$ 等于所有等价类的无交并. 等价关系通常用“ $\sim$ ”表示，$A$ 中所有等价类组成的集合记为 $A/\sim$.

如果将等价关系的定义性质 (2) 替换为

(2') 反对称性，即 $a_1Ra_2$ 且 $a_2Ra_1$ 蕴含 $a_1=a_2$,

则称 $R$ 为 $A$ 上的一个**偏序关系**, 或**序关系**. 具有偏序关系的集合称为**偏序集**. 如果一个偏序集中的任意两个元素之间都有偏序关系，则称此偏序集为一个**全序集**. 偏序关系通常用“ $\leq$ ”表示.

## 习　题

1. 设 $X$ 和 $Y$ 是两个集合，$f: X\to Y$ 和 $g: Y\to X$ 是两个映射. 如果 $g\circ f=\mathrm{id}_X$, 则称 $g$ 为 $f$ 的一个**左逆**; 如果 $f\circ g=\mathrm{id}_Y$, 则称 $g$ 为 $f$ 的一个**右逆**. 如果 $g$ 既是 $f$ 的左逆又是 $f$ 的右逆，则称 $g$ 为 $f$ 的一个**逆**. 证明

(1) $f$ 有左逆当且仅当 $f$ 是单射;

(2) $f$ 有右逆当且仅当 $f$ 是满射;

(3) $f$ 有逆当且仅当 $f$ 是双射;

(4) 如果 $f$ 有左逆 $g$, 同时又有右逆 $h$, 则 $g=h$;

(5) 如果 $f$ 有逆，则 $f$ 的逆唯一，$f$ 的逆记为 $f^{-1}$;

(6) 如果 $f$ 有逆，则 $(f^{-1})^{-1}=f$.

2. 举例说明等价关系的定义中的三个条件是相互独立的 (即任意两条不蕴含剩下的一条).

## §1.1　群的基本概念

在这一节中我们将介绍群的一些基本概念. 这些概念的大多数 (例如子结构、商结构、同态、同构、直和等) 在其他的代数结构 (如环、模) 中都有类似的构造.

### 1.1.1 群的定义和简单性质

**定义 1.1** 如果一个非空集合 $G$ 上定义了一个二元运算 $\circ$, 满足:

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

(2) 存在**幺元**: 存在 $e\in G$, 使得

$$e\circ a=a\circ e=a \quad (\forall\, a\in G)$$

($e$ 称为 $G$ 的幺元);

(3) 存在**逆元**: 对任意的 $a\in G$, 存在 $b\in G$, 使得

$$a\circ b=b\circ a=e$$

($b$ 称为 $a$ 的逆元),

则称 $G$ 关于运算 $\circ$ 构成一个**群**, 记为 $(G,\circ)$, 或简记为 $G$.

群 $G$ 中若还成立以下的

(4) **交换律**: $a\circ b=b\circ a$ $(\forall\, a,b\in G)$,

则称 $G$ 为**交换群** 或**Abel 群**.

在不致引起混淆的情况下, 运算符号 "$\circ$" 经常略去不写.

由结合律 (1) 可以推出下面的广义结合律:

(1′) **广义结合律**: 对于任意有限多个元素 $a_1, a_2, \cdots, a_n\in G$, 乘积 $a_1a_2\cdots a_n$ 的任何一种 "有意义的加括号方式" (即给定的乘积的顺序) 都得出相同的值, 因而上述乘积是有意义的.

顺便介绍一下半群和幺半群的概念. 如果一个非空集合 $S$ 上有二元运算, 此运算满足结合律, 则称此集合关于这个二元运算构成一个**半群**. 具有幺元的半群称为**幺半群**.

下面我们介绍群中的一些最基本概念和事实.

**命题 1.2** (1) *群的幺元唯一;*

(2) *群中任一元素的逆元唯一;*

(3) *群中有消去律, 即 $ax=ay$ 蕴含 $x=y$ (左消去律), $xa=ya$ 蕴含 $x=y$ (右消去律).*

**证明**　(1) 设 $e$ 和 $e'$ 都是群 $G$ 的幺元，则有 $e = ee' = e'$.

(2) 设 $b$ 和 $b'$ 都是群 $a$ 的逆元，则有

$$b = be = b(ab') = (ba)b' = eb' = b'.$$

(3) 设 $ax = ay$. 两端左乘 $a$ 的逆元 $b$, 得 $bax = bay$. 而 $ba = e$, 故有 $x = y$. 同样可证右消去律. □

以后我们将 $a$ 的唯一的逆元记为 $a^{-1}$. 由广义结合律 (1′), 任意有限多个元素的乘积 $a_1a_2\cdots a_n$ 是有意义的. 特别地，我们可以规定群 $G$ 中元素 $a$ 的整数次方幂如下：设 $n$ 为正整数，则像通常一样，令

$$a^n = \underbrace{aa\cdots a}_{n\text{个}}, \quad a^0 = e, \quad a^{-n} = (a^{-1})^n.$$

在这种记号下，对于所有整数 $m, n$, 显然有

$$a^m a^n = a^{m+n}.$$

如果 $G$ 是交换群，则易见 $(ab)^n = a^n b^n$.

群所含的元素个数称为群的**阶**. 群 $G$ 的阶记为 $|G|$. 如果 $|G| < \infty$, 则称 $G$ 为**有限群**, 否则称为**无限群**.

现在我们列举一些常见的群的例子.

**例 1.3**　整数集合 $\mathbb{Z}$、有理数集合 $\mathbb{Q}$、实数集合 $\mathbb{R}$、复数集合 $\mathbb{C}$ 关于加法都构成群. 非零有理数集合 $\mathbb{Q}^\times$、非零实数集合 $\mathbb{R}^\times$、非零复数集合 $\mathbb{C}^\times$、正实数集合 $\mathbb{R}^+$ 关于乘法都构成群.

**例 1.4**　设 $n$ 是一个正整数，则 $n$ 次单位根的全体关于乘法构成群，称为 $n$ **次单位根群**, 记为 $\mu_n$, 它包含 $n$ 个元素.

**例 1.5**　设 $n$ 是一个正整数. 整数集合 $\mathbb{Z}$ 模 $n$ 的剩余类关于加法构成群，它包含 $n$ 个元素. 与 $n$ 互素的剩余类关于乘法构成群，它包含 $\varphi(n)$ 个元素， $\varphi$ 为 Euler $\varphi$ 函数.

**例 1.6** 数域 $K$ 上的 $m \times n$ 阶矩阵的全体 $\mathrm{M}_{m\times n}(K)$ 关于加法构成群. $K$ 上的 $n$ 阶可逆矩阵的全体关于乘法构成群，称为 $K$ 上的**一般线性群**，记为 $\mathrm{GL}_n(K)$. $\mathrm{GL}_n(K)$ 中行列式等于 1 的矩阵的全体关于乘法也构成群，称为 $K$ 上的**特殊线性群**，记为 $\mathrm{SL}_n(K)$. $n$ 阶实正交矩阵的全体关于乘法构成群，称为**正交群**，记为 $\mathrm{O}_n(\mathbb{R})$. $n$ 阶酉矩阵的全体关于乘法构成群，称为**酉群**，记为 $\mathrm{U}_n(\mathbb{C})$.

**例 1.7** 设 $T$ 是 $n$ 维欧氏空间的一个子集 (即图形)，则将 $T$ 映成自身的正交变换的全体关于变换的乘法，即变换复合构成一个群，叫做**图形 $T$ 的对称群**，记为 $\mathrm{Sym}(T)$.

**例 1.8** 特别地，考虑实平面上保持正 $n$ 边形 ($n \geqslant 3$) 的全体正交变换的集合 $D_{2n}$. 它包含 $n$ 个旋转和 $n$ 个反射 (沿 $n$ 条不同的对称轴). 从几何上很容易看出，$D_{2n}$ 对于变换的乘法，即变换复合构成一个群，叫做**二面体群**，它包含 $2n$ 个元素.

若以 $a$ 表示绕这个正 $n$ 边形的中心沿逆时针方向旋转 $\dfrac{2\pi}{n}$ 的变换，则 $D_{2n}$ 中所有旋转都可表为 $a^i$ 的形式，$i = 0, 1, \cdots, n-1$. 再以 $b$ 表示沿某一预先指定的对称轴 $l$ 所作的反射变换，则有关系式

$$a^n = e, \quad b^2 = e, \quad b^{-1}ab = a^{-1}.$$

最后一式表示对正 $n$ 边形先作反射 $b$，接着沿逆时针旋转 $\dfrac{2\pi}{n}$，然后再作反射 $b$，其总的效果就相当于将正 $n$ 边形沿顺时针方向旋转 $\dfrac{2\pi}{n}$. 这三个关系式叫做 $D_{2n}$ 的定义关系. 关于定义关系的精确含义需要学过自由群才能理解，可见 §2.4. 但在现在，这些关系能够帮助我们理解群中元素的结构. 比如有了第三个关系，群的每个元素都可以表成 $b^j a^i$ 的形状，即

$$D_{2n} = \{b^j a^i \mid j = 0, 1;\ i = 0, 1, \cdots, n-1\}.$$

由这些关系还可以推出， $D_{2n}$ 中乘法应依照规律：

$$b^j a^i \cdot b^s a^t = b^{j+s} a^{(-1)^s i+t}.$$

**例 1.9**　设 $M$ 是一个非空集合． $M$ 到自身的双射的全体对于映射的乘法 (即复合) 构成一个群，叫做 $M$ 的**全变换群**, 记为 $S(M)$.

上述的例 1.3, 1.4, 1.5 是交换群，其余的一般都不是交换群.

### 1.1.2　对称群和交错群

设 $M$ 是含有 $n$ 个元素的集合． $M$ 的全变换群 $S(M)$ 称为 $n$ 级**对称群**, 记为 $S_n$. 不失一般性，我们可以假定 $M=\{1,2,\cdots,n\}$. $S_n$ 的元素称为**置换**. 任一置换 $\sigma$ 可以用列表的方法表示，即：如果 $\sigma(j)=\sigma_j$ $(j=1,2,\cdots,n)$, 则记

$$\sigma=\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \end{pmatrix}.$$

由于 $\sigma$ 是双射，所以 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 是 $1,2,\cdots,n$ 的一个排列．显然 $1,2,\cdots,n$ 的任一排列 $\tau_1,\tau_2,\cdots,\tau_n$ 都给出一个置换，且不同的排列给出不同的置换．所以 $|S_n|=n!$.

有更方便的办法来表示置换. 首先我们考虑一类特殊的置换：设 $\sigma\in S_n$, $i_1,i_2,\cdots,i_t\in\{1,2,\cdots,n\}$, 如果 $\sigma(i_1)=i_2$, $\sigma(i_2)=i_3$, $\cdots$, $\sigma(i_{t-1})=i_t$, $\sigma(i_t)=i_1$, 且 $i_1,i_2,\cdots,i_t$ 之外的元素在 $\sigma$ 下都保持不变，则称 $\sigma$ 为 $i_1,i_2,\cdots,i_t$ 的**轮换**, 记为 $(i_1\ i_2\ \cdots\ i_t)$. 这里的 $t$ 称为轮换 $\sigma$ 的**长度**. 长度为 2 的轮换称为**对换**. 长度为 1 的轮换 (即恒同变换) 通常记为 (1). 两个轮换 $(i_1\ i_2\ \cdots\ i_t)$ 和 $(j_1\ j_2\ \cdots\ j_s)$ 称为不相交的，如果 $i_k\neq j_l$ $(\forall\ 1\leqslant k\leqslant t,\ 1\leqslant l\leqslant s)$. 显然不相交的轮换的乘积满足交换律，即如果 $\sigma=(i_1\ i_2\ \cdots\ i_t)$ 和 $\tau=(j_1\ j_2\ \cdots\ j_s)$ 为不相交的轮换，则 $\tau\sigma=\sigma\tau$.

**命题 1.10**　对称群 $S_n$ 中任一不等于幺元的元素都可以 (在不计顺序的意义下) 唯一地分解为不相交的轮换的乘积.

**证明** 设 $\sigma \in S_n$, $\sigma \neq (1)$. 取 $i_1 \in \{1,2,\cdots,n\}$ 使得 $\sigma(i_1) \neq i_1$. 考虑 $i_1, \sigma(i_1), \sigma^2(i_1), \cdots \in \{1,2,\cdots,n\}$. 由于 $n$ 有限，故必存在 $t_1 < t_2$ 使得 $\sigma^{t_1}(i_1) = \sigma^{t_2}(i_1)$, 即有 $\sigma^{t_2-t_1}(i_1) = i_1$. 令 $t$ 为满足 $\sigma^t(i_1) = i_1$ 的最小的正整数. 由 $i_1$ 的选取知 $t > 1$. 于是 $\sigma$ 在 $\{i_1, \sigma(i_1), \cdots, \sigma^{t-1}(i_1)\}$ 上的限制构成一个轮换. 如果 $\{1,2,\cdots,n\} \setminus \{i_1, \sigma(i_1), \cdots, \sigma^{t-1}(i_1)\}$ 中的元素在 $\sigma$ 下都不动，则 $\sigma = (i_1\ \sigma(i_1)\ \cdots\ \sigma^{t-1}(i_1))$, 即 $\sigma$ 是 (单个) 轮换的乘积. 否则在 $\{i_1, \sigma(i_1), \cdots, \sigma^{t-1}(i_1)\}$ 之外取一个在 $\sigma$ 下变动的元素 $j_1$ (注意：$\sigma^k(j_1)$ 不会等于 $\sigma^l(i_1)$ $(\forall\ k,l \in \mathbb{Z})$, 否则导致 $j_1 = \sigma^{l-k}(i_1)$, 与 $j_1$ 的选取矛盾), (有限次) 重复上面的讨论，即得到分解的存在性. 唯一性显然. □

**推论 1.11** *任一置换可以分解为对换的乘积.*

**证明** 只要证明任一轮换可以分解为对换的乘积. 事实上，不难验证 $(i_1\ i_2\ \cdots\ i_t) = (i_1\ i_t)(i_1\ i_{t-1})\cdots(i_1\ i_3)(i_1\ i_2)$. □

**命题 1.12** *任一给定的置换分解为对换的乘积时出现的对换个数的奇偶性不变.*

**证明** 设 $\sigma = \sigma_m \cdots \sigma_2\sigma_1$, 其中每个 $\sigma_i$ 都是对换. 由高等代数中的行列式理论我们知道：每一个对换都使得 $\{1,2,\cdots,n\}$ 的任一排列的逆序数改变一个奇数. 如果用 $N(i_1,i_2,\cdots,i_n)$ 表示 $(i_1,i_2,\cdots,i_n)$ 的逆序数，则

$$N(\sigma_1(1),\sigma_1(2),\cdots,\sigma_1(n)) \equiv 1 \pmod 2,$$

$$N(\sigma_2(\sigma_1(1)),\sigma_2(\sigma_1(2)),\cdots,\sigma_2(\sigma_1(n))) \equiv 1+1 = 2 \pmod 2,$$

$$\cdots\cdots$$

以此类推，有 $N(\sigma(1),\sigma(2),\cdots,\sigma(n)) \equiv m \pmod 2$. 这说明 $m$ 的奇偶性被 $\sigma$ 所确定，而与 $\sigma$ 的对换分解式无关. □

如果一个置换等于偶数个对换的乘积，则称之为**偶置换**，否则称为**奇置换**. 对称群 $S_n$ 中所有偶置换在映射的乘法下也构成一个群，叫做 $n$ 级**交错群**, 记为 $A_n$.

### 1.1.3　子群、陪集、 Lagrange 定理

**定义 1.13**　设 $H$ 为群 $G$ 的非空子集. 如果 $H$ 在 $G$ 的运算下构成群, 则称 $H$ 为 $G$ 的**子群**, 记做 $H \leqslant G$.

例如, 上小节中的 $A_n$ 是 $S_n$ 的子群.

1.1.1 最后的例 1.9 所说的集合上的全变换群的子群 (称为该集合上的**变换群**) 涵盖了所有的群. 事实上, 任一群在本质上都可以看做这个群 ( 作为集合 ) 上的一个变换群, 这就是著名的 Cayley 定理. 我们将在 1.1.5 给出这个定理的严格叙述和证明 (见定理 1.28).

为了判断 $G$ 的子集 $H$ 是否是 $G$ 的子群, 并不必验证 $H$ 是否满足群的全部定义性质. 事实上, 我们有

**命题 1.14**　设 $G$ 是群, $H \subseteq G, H \neq \varnothing$, 则下列命题等价:

(1) $H \leqslant G$;

(2) 对任意的 $a, b \in H$, 恒有 $ab \in H$ 和 $a^{-1} \in H$;

(3) 对任意的 $a, b \in H$, 恒有 $ab^{-1} \in H$ (或 $a^{-1}b \in H$).

**证明**　(1)$\Longrightarrow$ (2) 和 (2)$\Longrightarrow$ (3) 都显然. 现在证明 (3)$\Longrightarrow$ (1). 由于 $H \neq \varnothing$, 故存在 $a \in H$. 在条件 (3) 中取 $b = a$, 得到 $e = ab^{-1} \in H$, 即 $H$ 中有幺元. 对于任一 $h \in H$, 在条件 (3) 中取 $a = e, b = h$, 得到 $h^{-1} = eh^{-1} \in H$, 即 $H$ 中含有其中任一元素的逆元. 由于 $H$ 中的运算就是 $G$ 中的运算, 所以满足结合律. 这就证明了 (1). □

设 $G$ 是群, $H, K$ 是 $G$ 的子集, 规定 $H, K$ 的**积**为

$$HK = \{hk \mid h \in H, k \in K\}.$$

如果 $K = \{a\}$, 仅由一个元素 $a$ 组成, 则简记为 $H\{a\} = Ha$. 类似地有 $aH$ 等. 我们还规定

$$H^{-1} = \{h^{-1} \mid h \in H\};$$

对于正整数 $n$, 规定

$$H^n = \{h_1 h_2 \cdots h_n \mid h_i \in H\}.$$

在这样的记号下，命题 1.14 可以改述为

**命题 1.14′** 设 $G$ 是群，$H \subseteq G, H \neq \varnothing$, 则下列命题等价：

(1) $H \leqslant G$;

(2) $H^2 \subseteq H$ 且 $H^{-1} \subseteq H$;

(3) $HH^{-1} \subseteq H$ (或 $H^{-1}H \subseteq H$).

事实上，易验证：如果 $H$ 是 $G$ 的子群，则必有 $H^2 = H$, $H^{-1} = H$. 显然，任何群 $G$ 都有两个子群 $G$ 本身和 $\{e\}$. 子群 $\{e\}$ 叫做 $G$ 的**平凡子群**. 如果子群 $H \neq G$, 则称 $H$ 为 $G$ 的**真子群**, 记做 $H < G$.

容易看出，若干个子群的**交**仍为子群，但一般来说若干个子群的并不是子群. 我们有下述概念：

**定义 1.15** 设 $G$ 是群，$M \subseteq G$ (允许 $M = \varnothing$), 则称 $G$ 的所有包含 $M$ 的子群的交为**由 $M$ 生成的子群**, 记做 $\langle M \rangle$.

容易看出，$\langle M \rangle = \{e, a_1 a_2 \cdots a_n \mid a_i \in M \cup M^{-1}, n = 1, 2, \cdots\}$.

如果 $\langle M \rangle = G$, 我们称 $M$ 为 $G$ 的一个**生成系**, 或称 $G$ 由 $M$ 生成. 仅由一个元素 $a$ 生成的群 $G = \langle a \rangle$ 叫做**循环群**. 可由有限多个元素生成的群叫做**有限生成群**. 有限群当然都是有限生成群.

对于群 $G$ 中任意元素 $a$, 我们称 $\langle a \rangle$ 的阶为**元素 $a$ 的阶**, 记做 $\mathrm{o}(a)$, 即 $\mathrm{o}(a) = |\langle a \rangle|$. 由此定义知，$\mathrm{o}(a)$ 是满足 $a^n = e$ 的最小的正整数 $n$. 如果这样的正整数 $n$ 不存在，则称 $a$ 的阶为无穷，记为 $\mathrm{o}(a) = \infty$. 又，群中所有元素的阶的最小公倍数叫做群的**方次数**, 记做 $\exp(G)$. 如果最小公倍数不存在，则称其方次数为 $\infty$.

下面我们引入“陪集”的概念.

设 $H \leqslant G$, 用 $H$ 可以给出 $G$ 上的一个等价关系 $\overset{l}{\sim}$ 如下：对于任意的 $a, b \in G$,

$$a \overset{l}{\sim} b \text{ 定义为：存在 } h \in H, \text{ 使得 } a = bh.$$

我们来验证 $\overset{l}{\sim}$ 确实是一个等价关系. (1) 反身性. 对于任一 $a \in G$, 存在 $e \in H$ 使得 $a = ae$, 故 $a \overset{l}{\sim} a$. (2) 对称性. 设 $a \overset{l}{\sim} b$, 则存在

$h \in H$ 使得 $a = bh$. 两端右乘 $h^{-1}$, 得 $ah^{-1} = b$. 而 $h^{-1} \in H$, 故 $b \overset{l}{\sim} a$. (3) 传递性. 设 $a \overset{l}{\sim} b$, $b \overset{l}{\sim} c$, 则存在 $h, k \in H$ 使得 $a = bh$, $b = ck$. 于是 $a = (ck)h = c(kh)$. 由于 $H$ 是子群, 故 $kh \in H$, 所以 $a \overset{l}{\sim} c$. 这就证明了 $\overset{l}{\sim}$ 是等价关系.

不难看出, 在这个等价关系下 $G$ 的元素 $a$ 所在的等价类就是 $aH$. 事实上, $b \overset{l}{\sim} a \iff$ 存在 $h \in H$ 使得 $b = ah \iff b \in aH$.

类似地我们可以定义 $G$ 上的等价关系 $\overset{r}{\sim}$:

$$a \overset{r}{\sim} b \text{ 定义为: 存在 } h \in H, \text{ 使得 } a = hb.$$

在 $\overset{r}{\sim}$ 下 $a$ 所在的等价类就是 $Ha$. 这些等价类有专门的名称:

**定义 1.16**　设 $H \leqslant G$, $a \in G$, 称形如 $aH$ (相应地, $Ha$) 的子集为 $H$ 的一个**左** (相应地, **右**)**陪集**.

由于左陪集是等价类, 所以整个群 $G$ 就分解为左陪集的无交并. 确切地, 有

$$G = \dot{\bigcup_{aH}} aH.$$

$H$ 的左陪集的个数 (不一定有限) 称为 $H$ 在 $G$ 中的**指数**, 记为 $|G : H|$.

不难看出 $H$ 与它的任一左陪集之间存在双射. 确切地说, 映射

$$\begin{aligned} \varphi : H &\to aH, \\ h &\mapsto ah \end{aligned}$$

是双射. 事实上, 由于 $aH$ 的定义即知 $\varphi$ 是满射. 又若 $ah_1 = ah_2$, 两端左乘 $a^{-1}$, 立得 $h_1 = h_2$. 故 $\varphi$ 也是单射. 这就证明了 $\varphi$ 是双射.

同样的结论对于右陪集也成立, 并且 $H$ 在 $G$ 中的左、右陪集个数相等, 都是 $|G : H|$.

现在我们考虑 $G$ 是有限群的情形. 由上面的讨论容易证明下面的重要定理:

**定理 1.17 (Lagrange 定理)** 设 $G$ 是有限群, $H \leqslant G$, 则

$$|G| = |G : H||H|.$$

**证明** 由于 $H$ 与它的任一左陪集 $aH$ 之间有双射, 所以 $|H| = |aH|$. 于是有

$$|G| = \sum_{aH} |aH| = |G : H||H|. \qquad \square$$

在此定理中取 $H = \langle a \rangle$, 其中 $a$ 为 $G$ 的任一元素, 立即得到

**推论 1.18** 有限群 $G$ 的任一元素 $a$ 的阶 $\mathrm{o}(a)$ 整除 $G$ 的阶; 于是 $a^{|G|} = e$.

### 1.1.4 正规子群与商群

在线性空间理论中我们常常要考虑关于一个子空间的商空间, 从而使得问题变得容易解决. 在群论中类似的考虑也非常重要. 我们简单回顾一下商空间的概念. 设 $V$ 是域 $K$ 上的线性空间, $W$ 是 $V$ 的一个子空间, 则商空间 $V/W$ 中的元素是形如 $\bar{\alpha} = \alpha + W$ ($\alpha \in V$) 的 ($V$ 的) 子集. 用上一小节的术语来说, $\bar{\alpha}$ 就是加法群 $V$ 的子群 $W$ 的 ($\alpha$ 所在的) 陪集 (注意, 由于 $V$ 是 Abel 群, 故不必区分 $\alpha$ 所在的陪集是左陪集还是右陪集, 二者是一样的). $V/W$ 中的运算由代表元素的运算所定义, 即对于 $\bar{\alpha}, \bar{\beta} \in V/W$, $\bar{\alpha} + \bar{\beta}$ 定义为 $\overline{\alpha + \beta}$ (又对于 $k \in K$, 定义数乘 $k\bar{\alpha}$ 为 $\overline{k\alpha}$). 这个定义与群中子集的运算定义相吻合, 即 $\alpha + W$ 与 $\beta + W$ 作为加法群 $V$ 的子集的和就等于 $(\alpha + \beta) + W$. 特别地, $\bar{0} = W$ 是商空间 $V/W$ 中的零元素, 即 $W + (\alpha + W) = \alpha + W$. 现在对于一般的群 $G$ 和它的任一子群 $H$, 能否在左 (或右) 陪集的集合 $S$ 上类似地定义运算, 使得 $S$ 成为一个群呢? 答案是不确定的. 例如 $S_2 = \{(1), (1\ 2)\}$ 是 $S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 3\ 2), (1\ 2\ 3)\}$ 的子群 ($S_3$ 相当于上述的 $V$, $S_2$ 相当于 $W$), $(1\ 3)S_2 = \{(1\ 3), (1\ 2\ 3)\}$ 是 $(1\ 3)$ 所在的左陪

集 (相当于 $\alpha+W$). 平行于线性空间中的 $W+(\alpha+W)=\alpha+W$, 似乎应当有 $S_2\cdot((1\ 3)S_2)=(1\ 3)S_2$. 但

$$\begin{aligned}S_2\cdot((1\ 3)S_2)&=\{(1),(1\ 2)\}\{(1\ 3),(1\ 2\ 3)\}\\&=\{(1\ 3),(1\ 2\ 3),(1\ 3\ 2),(2\ 3)\},\end{aligned}$$

甚至不是左陪集, 更不会有 $S_2\cdot((1\ 3)S_2)=(1\ 3)S_2$. 其原因是 $S_2(1\ 3)\neq(1\ 3)S_2$, 即 $(1\ 3)$ 所在的左、右陪集不相等. 一般而言, 我们有下面的命题:

**命题 1.19**　*设 $G$ 是群, $H\leqslant G$, 则 $H$ 的任意两个左陪集的乘积仍是左陪集的充分必要条件是: $aH=Ha\ (\forall\ a\in G)$.*

**证明**　*必要性*　对于任一 $a\in G$, 由于 $a^2\in(aH)^2$, 且 $(aH)^2$ 是左陪集, 故 $(aH)^2=a^2H$. 两端左乘 $a^{-1}$, 得到 $HaH=aH$. 因为 $e\in H$, 所以 $Ha=Hae\subseteq aH$. 同理可证 $aH\subseteq Ha$.

*充分性*　$(aH)(bH)=a(Hb)H=a(bH)H=ab(HH)=abH$.

□

根据上面的讨论, 我们给出下面的重要概念:

**定义 1.20**　设 $G$ 是群, $H\leqslant G$. 如果 $aH=Ha\ (\forall\ a\in G)$, 则称 $H$ 为 $G$ 的**正规子群**, 记为 $H\trianglelefteq G$.

任何群 $G$ 本身和平凡子群 $\{e\}$ 都是正规子群. 如果除此之外群 $G$ 没有其他的正规子群, 则被称为**单群**.

正规子群有若干等价的表述, 例如, 我们有

**命题 1.21**　*设 $G$ 是群, $H\leqslant G$, 则以下三条等价:*

(1) $H\trianglelefteq G$;

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

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

**证明**　(1)$\Longrightarrow$ (2). 由条件 (1), 有 $Ha=aH\ (\forall\ a\in G)$. 两端同时左乘 $a^{-1}$, 即得 (2).

(2) $\Longrightarrow$ (3). 显然.

(3) $\Longrightarrow$ (1). 由条件 (3) 知 $ha\in aH\ (\forall\ h\in H,a\in G)$, 于是

$Ha \subseteq aH$ ($\forall\, a \in G$). 另一方面，在条件 (3) 中以 $a^{-1}$ 代替 $a$, 得到 $aha^{-1} \in H$. 于是 $ah \in Ha$ ($\forall\, h \in H, a \in G$), 故 $aH \subseteq Ha$ ($\forall\, a \in G$). 这就证明了 $aH = Ha$ ($\forall\, a \in G$), 即有 (1). □

**命题 1.22** *设 $G$ 是群，$H \trianglelefteq G$, 则 $H$ 的陪集在乘法下构成群，称为 $G$ 关于 $H$ 的* **商群**, *记为 $G/H$.* .

**证明** 首先，$H \in G/H$, 故 $G/H$ 非空. 其次，由命题 1.19 知 $G/H$ 对于乘法封闭，即陪集乘法确实是 $G/H$ 上的二元运算. 确切地说，有 $(aH)(bH) = a(Hb)H = a(bH)H = (ab)HH = abH$. 此乘法显然满足结合律. 又 $H(aH) = (aH)H = aH$ ($\forall\, aH \in G/H$), 所以 $H$ 是 $G/H$ 的幺元. 最后易见 $a^{-1}H$ 是 $aH$ 的逆元. 这就证明了 $G/H$ 在陪集乘法下构成群. □

作为特殊情形，所有 Abel 群的子群都是正规子群，所以对于 Abel 群的任一子群都可以构造相应的商群. 例如，整数加法群是 Abel 群，对于任一正整数 $n$, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, 此时相应的商群为

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\},$$

其中 $\bar{i} = i + n\mathbb{Z}$. 这个群是 $n$ 阶循环群，生成元是 $\bar{1}$ (参见例 1.5).

### 1.1.5 同态与同构，同态基本定理，正则表示

线性映射（包括线性变换）在线性代数中起着十分重要的作用. 对于一般的代数系统，类似的考虑也同样非常重要. 这种考虑使得我们可以在不同的对象之间建立联系，可以把问题简化，归结为一些基本的情形. 这就是我们要引入的同态的概念.

**定义 1.23** *设 $G$ 和 $G_1$ 是群. 映射 $\varphi : G \to G_1$ 称为由 $G$ 到 $G_1$ 的一个* **群同态**, *如果 $\varphi$ 保持群运算，即对于所有的 $a, b \in G$, 都有 $\varphi(ab) = \varphi(a)\varphi(b)$. 如果 $\varphi$ 又是单（满）射，则称 $\varphi$ 为* **单（满）同态**. *既单又满的同态称为* **同构**. *如果存在由 $G$ 到 $G_1$ 的一个同构，则称 $G$ 同构于 $G_1$, 也说 $G$ 和 $G_1$ 是* **同构的**, *记为 $G \cong G_1$.*

群 $G$ 到自身的同态及同构具有重要的意义，我们称之为群 $G$ 的 **自同态** 和 **自同构**. 我们以 $\mathrm{End}(G)$ 表示 $G$ 的全体自同态组成

的集合，而以 $\mathrm{Aut}(G)$ 表示 $G$ 的全体自同构组成的集合. 对于映射的乘法，$\mathrm{End}(G)$ 组成一个有幺元的半群，而 $\mathrm{Aut}(G)$ 组成一个群，叫做 $G$ 的**自同构群**.

同构满足等价关系的三个条件 (读者自己证明). 从抽象的角度来看，两个同构的群没有区别.

容易看出，群同态 $\varphi: G \to G_1$ 把 $G$ 的幺元映为 $G_1$ 的幺元，把 $G$ 的任一元素 $a$ 的逆元映为 $a$ 的像的逆元. 事实上，设 $e$ 和 $e_1$ 分别是 $G$ 和 $G_1$ 的幺元，则有 $\varphi(e)^2 = \varphi(e^2) = \varphi(e) = \varphi(e)e_1$，所以 $\varphi(e) = e_1$. 又有 $e_1 = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$，所以 $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

像通常的映射一样，$\varphi(G)$ 称为 $\varphi$ 的**像**，记为 $\mathrm{im}\varphi$. 又将 $e_1$ 的原像称为 $\varphi$ 的**核**，记为 $\ker\varphi$，即

$$\ker\varphi = \{a \in G \mid \varphi(a) = e_1\}.$$

对于群同态，为检验其是否是单射，没有必要去验证像集合中的任一元素的原像都只有一个元素. 事实上，我们有

**命题 1.24**　设 $\varphi: G \to G_1$ 是群同态，则 $\varphi$ 单 $\iff \ker\varphi = \{e\}$.

**证明**　设 $e$ 和 $e_1$ 分别是 $G$ 和 $G_1$ 的幺元，则

$$\begin{aligned}
\varphi \text{ 不单} &\iff \text{存在 } a, b \in G, a \neq b, \text{ 使得 } \varphi(a) = \varphi(b) \\
&\iff \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_1 \\
&\iff \ker\varphi \supseteq \{ab^{-1}, e\} \\
&\iff \ker\varphi \neq \{e\}.
\end{aligned}$$

□

关于同态的像与核有下面的简单事实：

**命题 1.25**　设 $\varphi: G \to G_1$ 是群同态，则 $\mathrm{im}\varphi \leqslant G_1$，$\ker\varphi \trianglelefteq G$.

**证明**　设 $e$ 和 $e_1$ 分别是 $G$ 和 $G_1$ 的幺元，则 $e_1 = \varphi(e) \in \mathrm{im}\varphi$，故 $\mathrm{im}\varphi \neq \varnothing$. 对于任意的 $a_1, b_1 \in \mathrm{im}\varphi$，存在 $a, b \in G$ 使得 $\varphi(a) = a_1$，$\varphi(b) = b_1$，于是

$$a_1 b_1^{-1} = \varphi(a)(\varphi(b))^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \mathrm{im}\varphi,$$

故 $\mathrm{im}\varphi \leqslant G_1$.

由于 $e \in \ker\varphi$, 故 $\ker\varphi \neq \varnothing$. 对于任意的 $a, b \in \ker\varphi$, 有 $\varphi(ab^{-1}) = \varphi(a)(\varphi(b))^{-1} = e_1 \cdot e_1 = e_1$, 故 $ab^{-1} \in \ker\varphi$, 所以 $\ker\varphi \leqslant G$. 又对于任意的 $a \in \ker\varphi$, $g \in G$, 有

$$\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\varphi(g) = \varphi(g)^{-1}e_1\varphi(g) = e_1,$$

于是 $g^{-1}ag \in \ker\varphi$. 这就证明了 $\ker\varphi \trianglelefteq G$. □

下面的定理在群论中有基本的重要性.

**定理 1.26 (同态基本定理)** 设 $\varphi: G \to G_1$ 是群同态, 则

$$G/\ker\varphi \cong \mathrm{im}\varphi.$$

**证明** 为简单起见, 记 $\ker\varphi = H$. 定义映射

$$\begin{aligned} \psi:\ G/H &\to \mathrm{im}\varphi, \\ aH &\mapsto \varphi(a). \end{aligned}$$

我们来验证 $\psi$ 是良定义的, 即 $\psi(aH)$ 与陪集代表 $a$ 的选取无关. 事实上, 如果 $aH = bH$, 即 $b \in aH$, 则存在 $h \in H$ 使得 $b = ah$. 故

$$\psi(bH) = \varphi(b) = \varphi(ah) = \varphi(a)\varphi(h) = \varphi(a) = \psi(aH),$$

即 $\psi$ 良定义.

下面证明 $\psi$ 是群同构. 首先, 对于任意的 $aH, bH \in G/H$, 有

$$\psi((aH)(bH)) = \psi(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aH)\psi(bH),$$

所以 $\psi$ 是群同态. 又设有 $\psi(aH) = e_1$ ($G_1$ 的幺元), 即 $\varphi(a) = e_1$, 故 $a \in H$, 即 $aH = H$ ($G/H$ 的幺元), 所以 $\psi$ 是单射. 最后, 设 $g \in \mathrm{im}\varphi$, 则存在 $a \in G$ 使得 $\varphi(a) = g$. 于是 $\psi(aH) = \varphi(a) = g$. 这说明 $\psi$ 是满射. 这就证明了 $\psi$ 是同构. □

**推论 1.27** 设 $\varphi: G \to G_1$ 是群的满同态, 则 $G/\ker\varphi \cong G_1$.

现在我们给出 Cayley 定理. 先介绍一个术语. 设 $G$ 是群. 对于任一 $a \in G$, 定义 $G$ 上的变换

$$\begin{aligned} L(a): \ G &\to G, \\ g &\mapsto ag. \end{aligned}$$

$L(a)$ 称为由 $a$ 引起的 ($G$ 的)**左平移**. 对于任一 $g \in G$, 有

$$L(a)L(a^{-1})(g) = L(a)(a^{-1}g) = a(a^{-1}g) = g,$$

所以 $L(a)L(a^{-1}) = \mathrm{id}_G$. 同样 $L(a^{-1})L(a) = \mathrm{id}_G$. 故 $L(a)$ 是 $G$ 上的双射, 即 $L(a) \in S(G)$.

**定理 1.28 (Cayley 定理)** *任一群都同构于某一集合上的变换群.*

**证明** 以 $L(G)$ 记 $G$ 的左平移的全体所构成的 $G$ 的全变换群 $S(G)$ 的子集. 定义映射

$$\begin{aligned} L: \ G &\to S(G), \\ a &\mapsto L(a). \end{aligned}$$

对于任意的 $a, b \in G$, 有

$$\begin{aligned} L(ab)(g) &= (ab)g = a(bg) = L(a)L(b)(g) \\ &= (L(a)L(b))(g), \quad \forall\, g \in G, \end{aligned}$$

所以 $L(ab) = L(a)L(b)$, 即 $L$ 是群同态. 显然 $\mathrm{im}L = L(G)$, 又显然 $\ker L = \{e\}$, 由同态基本定理即知 $G \cong L(G)$. 而 $L(G)$ 是集合 $G$ 上的变换群, 故定理为真. □

**定义 1.29** 上述的 $L(G)$ 称做群 $G$ 的**左正则表示**.

类似地可以定义由群 $G$ 的元素 $a$ 引起的**右平移** $R(a)$, 即 $R(a)(g) = ga^{-1}$ ($\forall\, g \in G$). 以 $R(G)$ 记 $G$ 的所有右平移组成的 $S(G)$ 的子集, 则同样可以证明 $G \cong R(G)$ (读者自行验证). $R(G)$ 称为 $G$ 的**右正则表示**.

作为特殊情形，如果 $G$ 是有限群，$|G| = n$, 则 Cayley 定理告诉我们：$G$ 同构于对称群 $S_n$ 的一个子群.

### 1.1.6 群的同构定理

设 $G$ 是群，$H \trianglelefteq G$. 由商群中运算的定义立见

$$\begin{aligned} \pi: G &\to G/H, \\ a &\mapsto aH \end{aligned}$$

是群同态. 这种同态称为由 $G$ 到 $G/H$ 的**典范同态**.

**定理 1.30 (第一同构定理)** 设 $G$ 是群，$H \trianglelefteq G$, 则在典范同态

$$\begin{aligned} \pi: G &\to G/H, \\ a &\mapsto aH \end{aligned}$$

下，

(1) $G$ 的包含 $H$ 的子群与 $G/H$ 的子群一一对应；

(2) 在此对应下，正规子群对应于正规子群；

(3) 若有 $K \trianglelefteq G$ 且 $K \supseteq H$, 则

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

**证明** 为简单起见，对于 $G$ 的任意子集 $M$, 以 $\overline{M}$ 记 $M$ 在典范同态 $\pi$ 下的像 (对于 $G$ 的元素也类似).

(1) 首先，对于 $G$ 包含 $H$ 的子群 $M$, 由于 $\pi$ 是群同态，所以 $\pi$ 在 $M$ 上的限制 $\pi|_M: M \to \overline{G}$ 也是群同态，故 $\overline{M}(= \mathrm{im}(\pi|_M))$ 是 $\overline{G}$ 的子群. 其次，设 $M_1$ 和 $M_2$ 都是 $G$ 包含 $H$ 的子群，且 $M_1 \neq M_2$, 则不妨设 $M_1 \not\subseteq M_2$, 即存在 $a \in M_1 \setminus M_2$. 此时必有 $\overline{a} \notin \overline{M_2}$ (否则存在 $b \in M_2$ 使得 $\overline{a} = \overline{b}$, 即 $a \in bH \subseteq M_2$, 矛盾 ). 这就是说 $G$ 包含 $H$ 的不同的子群在典范映射下的像必不

同. 最后我们对于 $\overline{G}$ 的任一子群 $N$, 容易验证 $\pi^{-1}(N)$ 是 $G$ 包含 $H$ 的子群 ($H=\pi^{-1}(\overline{e})\subseteq\pi^{-1}(N)$; 且对于任意的 $a,b\in\pi^{-1}(N)$, 有 $\overline{a},\overline{b}\in N\Rightarrow\overline{a}\overline{b}^{-1}\in N\Rightarrow\overline{ab^{-1}}\in N\Rightarrow ab^{-1}\in\pi^{-1}(N)$), 且 $\pi(\pi^{-1}(N))=N$, 即 $\overline{G}$ 的任一子群都是 $G$ 某个包含 $H$ 的子群在 $\pi$ 下的像. 这就证明了结论 (1).

(2) 若 $K$ 为 $G$ 包含 $H$ 的正规子群, 则对于任意的 $\overline{g}\in\overline{G}$, $\overline{g}^{-1}\overline{K}\overline{g}=\overline{g^{-1}Kg}=\overline{K}$, 故 $\overline{K}\trianglelefteq\overline{G}$. 反之, 若 $N\trianglelefteq\overline{G}$, 则对于任意的 $g\in G$ 和 $a\in\pi^{-1}(N)$, 有 $\pi(g^{-1}ag)=\overline{g}^{-1}\overline{a}\overline{g}\in N$, 故 $g^{-1}ag\in\pi^{-1}(N)$, 所以 $\pi^{-1}(N)\trianglelefteq G$.

(3) 考虑映射

$$\begin{aligned}\varphi:\ G/H &\to G/K,\\ aH &\mapsto aK.\end{aligned}$$

此映射是良定义的. 事实上, 若 $aH=bH$, 则 $a^{-1}b\in H\subseteq K$, 故 $aK=bK$.

对于 $aH,bH\in G/H$, 有 $\varphi((aH)(bH))=\varphi(abH)=abK=(aK)(bK)=\varphi(aH)\varphi(bH)$, 故 $\varphi$ 是群同态. 考虑 $\ker\varphi$. 有 $aH\in\ker\varphi\iff\varphi(aH)=K\iff aK=K\iff a\in K\iff aH\in K/H$, 所以 $\ker\varphi=K/H$. 又显然 $\varphi$ 是满的, 由推论 1.27 即得所要证的结论. □

如果用满同态的像代替定理 1.30 中的 $G/H$, 即设 $\psi:\ G\to G_1$ 为满同态, 由推论 1.27, 有同构 $\bar{\psi}:\ G/\ker\varphi\cong G_1$. 与定理 1.30 结合, 得到同态

$$G\xrightarrow{\pi}G/\ker\varphi\overset{\bar{\psi}}{\cong}G_1.$$

于是定理 1.30 可以改写成

**定理 1.30′**　设 $\psi:\ G\to G_1$ 为群的满同态, 则

(1) $G$ 的包含 $\ker\psi$ 的子群与 $G_1$ 的子群一一对应;

(2) 在此对应下, 正规子群对应于正规子群;

(3) 若有 $K \trianglelefteq G$ 且 $K \supseteq \ker\psi$, 则

$$G/K(\cong (G/\ker\psi)/(K/\ker\psi)) \cong G_1/\psi(K).$$

**定理 1.31 (第二同构定理)** 设 $G$ 是群, $H \trianglelefteq G$, $K \leqslant G$, 则

(1) $HK \leqslant G$, $H \cap K \trianglelefteq K$;

(2) $(HK)/H \cong K/(H \cap K)$.

**证明** (1) 显然 $HK \neq \varnothing$. 又设 $h_1k_1, h_2k_2 \in HK$, 其中 $h_i \in H$, $k_i \in K$ $(i = 1, 2)$. 由于 $H \trianglelefteq G$, 故 $(k_1k_2^{-1})h_2^{-1}(k_1k_2^{-1})^{-1} \in H$, 记此元素为 $h_3$. 则有 $(h_1k_1)(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1} = h_1h_3(k_1k_2^{-1}) \in HK$. 这意味着 $HK$ 是 $G$ 的子群.

设 $a \in H \cap K$, $k \in K$. 由 $H \trianglelefteq G$ 知 $k^{-1}ak \in H$. 又由 $a \in K$ 和 $k \in K$ 知 $k^{-1}ak \in K$. 所以 $k^{-1}ak \in H \cap K$. 这就证明了 $H \cap K \trianglelefteq K$.

(2) 考虑映射

$$\begin{aligned} \varphi\colon\ HK &\to K/(H \cap K), \\ hk &\mapsto \overline{k}(= k(H \cap K)). \end{aligned}$$

其中 $h \in H$, $k \in K$. 此映射是良定义的. 事实上, 若 $h_1k_1 = h_2k_2$ $(h_i \in H,\ k_i \in K)$, 则 $k_1k_2^{-1} = h_1^{-1}h_2 \in H \cap K$, 故 $k_1 \in k_2(H \cap K)$, 即 $\overline{k}_1 = \overline{k}_2$.

我们断言 $\varphi$ 是群同态. 事实上, 设 $h_i \in H$, $k_i \in K$ $(i = 1, 2)$, 由于 $H \trianglelefteq G$, 故存在 $h_3 \in H$ 使得 $k_1h_2 = h_3k_1$. 于是

$$\varphi((h_1k_1)(h_2k_2)) = \varphi(h_1h_3k_1k_2) = \overline{k_1k_2} = \overline{k}_1\overline{k}_2 = \varphi(h_1k_1)\varphi(h_2k_2).$$

这就证明了我们的断言.

对于任一 $\overline{k} \in K/(H \cap K)$, 设 $\overline{k} = k(H \cap K)$ $(k \in K)$, 则 $k = ek \in HK$, 且 $\varphi(ek) = \overline{k}$. 所以 $\varphi$ 是满同态. 由推论 1.27, 只要再证明 $\ker\varphi = H$. 事实上, 对于任一 $h \in H$, 有 $\varphi(h) = \varphi(he) = \overline{e}$, 所以 $H \subseteq \ker\varphi$. 反之, 若 $hk \in \ker\varphi$, 则 $\overline{k} = \overline{e}$, 即 $k \in K \cap H$, 更有 $k \in H$. 于是 $hk \in H$. 这意味着 $\ker\varphi \subseteq H$. 这就证明了

$$\ker\varphi = H. \qquad \square$$

### 1.1.7　群的直和与直积

从已知的一些群出发可以构造新的群，其中最简单的途径就是直和与直积的构作.

**定义 1.32**　设 $G_1, G_2$ 是群，在笛卡儿积 $G_1 \times G_2$ 上定义运算为按分量进行，即对于 $(a_1, b_1), (a_2, b_2) \in G_1 \times G_2$，定义

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2),$$

则 $G_1 \times G_2$ 在此运算下构成群 (读者自行验证)，称为 $G_1$ 与 $G_2$ 的 **(外) 直和**，记为 $G_1 \oplus G_2$. $G_1$ 和 $G_2$ 称为 $G_1 \oplus G_2$ 的**直和因子**.

在 $G_1 \oplus G_2$ 中有两个子群

$$\overline{G}_1 = \{(a, e_2) \mid a \in G_1\}, \quad \overline{G}_2 = \{(e_1, b) \mid b \in G_2\},$$

其中 $e_1$ 和 $e_2$ 分别为 $G_1$ 和 $G_2$ 的幺元.

显然，映射 $a \mapsto (a, e_2)$ 是从 $G_1$ 到 $\overline{G}_1$ 的同构. 同样 $b \mapsto (e_1, b)$ 是从 $G_2$ 到 $\overline{G}_2$ 的同构. 如果把 $G_i$ 与 $\overline{G}_i$ $(i = 1, 2)$ 等同起来. 就可以认为 $G_1 \oplus G_2$ 是由子群 $G_1$ 和 $G_2$ 出发构造的的群. 反过来考虑，是否可以将一个群表示成它的两个子群的直和？如果可以，则对于这个群的研究就归结为对于它的这两个子群的研究，从而使得问题简化.

我们考虑这样的两个子群所应满足的条件. 首先，显然有 $G_1 \oplus G_2 = \overline{G}_1 \overline{G}_2$. 其次，不难看出 $\overline{G}_1$ 和 $\overline{G}_2$ 都是 $G_1 \oplus G_2$ 的正规子群. 事实上，对于任意的 $(a', b') \in G_1 \oplus G_2$ 和 $(a, e_2) \in \overline{G}_1$，有

$$(a', b')^{-1}(a, e_2)(a', b') = (a'^{-1} a a'; b'^{-1} b') = (a'^{-1} a a', e_2) \in \overline{G}_1,$$

故 $\overline{G}_1 \trianglelefteq G_1 \oplus G_2$. 同样 $\overline{G}_2 \trianglelefteq G_1 \oplus G_2$.

在上述的两个必要条件之下，一个群能够表示为两个子群的直和有几个等价的说法. 确切地说，我们有

**命题 1.33** 设 $G$ 是群，$H, K \trianglelefteq G$, $G = HK$, 则下述四条等价：

(1) 映射

$$\begin{aligned} \sigma: H \oplus K &\to G, \\ (h,k) &\mapsto hk \end{aligned}$$

是同构；

(2) $G$ 的任一元素表为 $H$ 与 $K$ 的元素的乘积的表示法唯一；

(3) $G$ 的幺元表为 $H$ 与 $K$ 的元素的乘积的表示法唯一；

(4) $H \cap K = \{e\}$.

**证明** (1) $\Longrightarrow$ (2). 设 $g \in G$, $g = hk = h'k'$, 其中 $h, h' \in H$, $k, k' \in K$, 则 $\sigma((h,k)) = hk = h'k' = \sigma((h',k'))$. 由于 $\sigma$ 是同构，故 $\sigma$ 是单射，所以 $(h,k) = (h',k')$. 于是 $h = h'$, $k = k'$. 故断言为真.

(2) $\Longrightarrow$ (3). 显然.

(3) $\Longrightarrow$ (4). 设 $g \in H \cap K$, 则 $e = gg^{-1}$. 而 $e = ee$, 由 (3) 即知 $g = e$.

(4) $\Longrightarrow$ (1). 首先证明 $\sigma$ 为同态.

对于 $h \in H$, $k \in K$, 我们断言 $hk = kh$. 考虑 $hkh^{-1}k^{-1}$. 由于 $K \trianglelefteq G$, 故 $hkh^{-1} \in K$. 所以 $hkh^{-1}k^{-1} \in K$. 类似地 $hkh^{-1}k^{-1} \in H$. 于是 $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, 即有 $hk = kh$. 故断言为真.

现在，对于 $(h,k), (h',k') \in H \oplus K$, 有

$$\begin{aligned} \sigma((h,k)(h',k')) &= \sigma((hh',kk')) = h(h'k)k' \\ &= (hk)(h'k') = \sigma((h,k))\sigma((h',k')). \end{aligned}$$

这就证明了 $\sigma$ 是同态.

再证明 $\sigma$ 是单射. 为此只要证明 $\ker\sigma = \{(e,e)\}$. 设 $(h,k) \in \ker\sigma$, 则 $hk = e$, 所以 $h = k^{-1} \in H \cap K = \{e\}$, 故 $(h,k) = (e,e)$.

由 $G = HK$ 以及 $\sigma$ 的定义立见 $\sigma$ 是满射. 证毕. □

如果群 $G$ 和它的两个子群 $H, K$ 满足命题 1.33, 则称 $G$ 是 $H$ 与 $K$ 的**(内) 直和**, 也记为 $G = H \oplus K$. 此时 $H$ 与 $K$ 也称为 $G$ 的**直和因子**.

直和的概念容易推广的多个群的情形. 设 $G_1, \cdots, G_n$ 是群, 在 $G_1 \times \cdots \times G_n$ 上定义运算为按分量进行, 所得到的群称为 $G_1, \cdots, G_n$ 的**(外) 直和**, 记为 $G_1 \oplus \cdots \oplus G_n$. $G_i$ $(1 \leqslant i \leqslant n)$ 称为 $G_1 \oplus \cdots \oplus G_n$ 的**直和因子**.

关于多个子群的内直和, 有

**命题 1.34**　设 $G$ 是群, $H_1, \cdots, H_n \trianglelefteq G$, $G = H_1 \cdots H_n$, 则下述四条等价:

(1) 映射

$$\begin{aligned} \sigma:\ H_1 \oplus \cdots \oplus H_n &\to G, \\ (h_1, \cdots, h_n) &\mapsto h_1 \cdots h_n \end{aligned}$$

是同构;

(2) $G$ 的任一元素表为 $H_1, \cdots, H_n$ 的元素的乘积的表示法唯一;

(3) $G$ 的幺元表为 $H_1, \cdots, H_n$ 的元素的乘积的表示法唯一;

(4) $H_i \cap (H_1 \cdots \widehat{H}_i \cdots H_n) = \{e\}$ $(\forall\ i = 1, \cdots, n)$, 这里 $\widehat{H}_i$ 表示去掉 $H_i$.

此命题的证明与命题 1.33 的证明类似, 读者可以作为练习.

进一步可以考虑从无穷多个群出发的情形.

一般而言, 设 $G_i$ $(i \in I)$ 是群, 这里 $I$ 为指标集 (可以是有限或无限集). 令 $G$ 为集合 $G_i$ $(i \in I)$ 的笛卡儿积, 在 $G$ 上定义运算为按分量进行, 所得到的群称为 $G_i$ $(i \in I)$ 的**(外) 直积**, 记为 $\prod\limits_{i \in I} G_i$. $G_i$ $(i \in I)$ 称为 $G$ 的**直积因子**. 群 $G$ 的子集

$$\{\ (\cdots, a_i, \cdots) \mid a_i \in G_i,\ \text{除有限多个 } i \text{ 之外都有 } a_i = e_i\ \}$$

($e_i$ 为 $G_i$ 的幺元) 构成 $\prod\limits_{i\in I} G_i$ 的子群，此子群称为 $G_i$ $(i \in I)$ 的**(外) 直和**, 记为 $\bigoplus\limits_{i\in I} G_i$ 或 $\coprod\limits_{i\in I} G_i$. 容易看出，当 $I$ 为有限集时，直积与直和是同一个概念.

对于任一 $i \in I$, 有自然的群同态

$$\begin{aligned} \iota_i : G_i &\to \prod_{i\in I} G_i, \\ a_i &\mapsto (\cdots, e, a_i, e, \cdots) \end{aligned}$$

和

$$\begin{aligned} \pi_i : \prod_{i\in I} G_i, &\to G_i, \\ (\cdots, a_i, \cdots) &\mapsto a_i, \end{aligned}$$

其中的 $a_i$ 为 $G_i$ 的元素. 这两个映射中的 $\prod\limits_{i\in I} G_i$ 都可以换成 $\bigoplus\limits_{i\in I} G_i$.

直和任一元素都可以唯一地表为 $\iota_i$ 的像的和，但当 $I$ 是无限集时直积却不具有这样的性质.

## 习 题

1. 证明群的定义可以简化为：如果一个非空集合 $G$ 上定义了一个二元运算 $\circ$, 满足：

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

(2) 存在**左幺元**：存在 $e \in G$, 使得对任意的 $a \in G$, 恒有

$$e \circ a = a;$$

(3) 存在**左逆元**：对任意的 $a \in G$, 存在 $b \in G$, 使得

$$b \circ a = e,$$

则 $G$ 关于运算 $\circ$ 构成一个群.

2. 举例说明：在上题中将条件 (3) 改为 “存在**右逆元**：对任意的 $a \in G$, 存在 $b \in G$, 使得 $a \circ b = e$ ”，则 $G$ 不一定是群.

3. 设 $G$ 是一个非空集合，其中定义了一个二元运算 $\circ$. 证明：如果此运算满足结合律，并且对于 $G$ 中的任意两个元素 $a, b$, 方程 $a \circ x = b$ 和 $y \circ a = b$ 都在 $G$ 中有解，则 $(G, \circ)$ 是群.

4. 设 $G$ 是一个非空的有限集合，其中定义了一个二元运算 $\circ$. 证明：如果此运算满足结合律，并且对于 $G$ 中的任意三个元素 $a, b, c$, 都有 (左消去律) $ab = ac \Rightarrow b = c$ 以及 (右消去律) $ba = ca \Rightarrow b = c$, 则 $(G, \circ)$ 是群.

5. 设 $G$ 是群，$a, b \in G$, 如果 $aba^{-1} = b^r$, 证明 $a^i ba^{-i} = b^{r^i}$.

6. 证明不存在恰有两个 2 阶元素的群.

7. 设 $G$ 是群. 如果对于任意的 $a, b \in G$, 都有 $(ab)^2 = a^2 b^2$, 证明 $G$ 是交换群. 并由此证明：如果 $\exp(G) = 2$, 则 $G$ 交换.

8. 在 $S_3$ 中找出两个元素 $x, y$, 使得 $(xy)^2 \neq x^2 y^2$.

9. 设 $G$ 是群，$i$ 为任一确定的正整数. 如果对于任意的 $a, b \in G$, 都有 $(ab)^k = a^k b^k$, $k = i, i+1, i+2$, 证明 $G$ 是交换群.

10. 证明：群 $G$ 为交换群当且仅当 $x \mapsto x^{-1}$ $(x \in G)$ 是同构映射.

11. 设 $S$是群 $G$的非空子集, 在 $G$中定义一个二元关系 “$\sim$”：$a \sim b \iff ab^{-1} \in S$. 证明 $\sim$ 是一个等价关系当且仅当 $S$ 是 $G$ 的子群.

12. 设 $H, K$ 为群 $G$ 的子群，证明 $HK \leqslant G$ 当且仅当 $HK = KH$.

13. 设 $n \in \mathbb{Z}$, 则 $n\mathbb{Z}$ 是整数加法群 $\mathbb{Z}$ 的子群. 并证明 $n\mathbb{Z} \cong \mathbb{Z}$.

14. 证明：$S_4$ 的子集 $B = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ 是一个子群，且 $B$ 与四次单位根群 $\mu_4$ 不同构.

15. 令

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}} & 0 \\ 0 & \mathrm{e}^{-\frac{2\pi \mathrm{i}}{n}} \end{pmatrix},$$

证明集合 $\{B, B^2, \cdots, B^n, AB, AB^2, \cdots, AB^n\}$ 在矩阵乘法下构成群，并且此群与二面体群 $D_{2n}$ 同构.

16. 证明偶数阶群中必有元素 $a \neq e$, 满足 $a^2 = e$.

17. 设 $n > 2$, 证明在有限群 $G$ 中阶为 $n$ 的元素个数是偶数.

18. 对于群中的任意二元素 $a, b$, 证明 $ab$ 与 $ba$ 的阶相等.

19. 在群 $\mathrm{SL}_2(\mathbb{Q})$ 中，证明元素

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

的阶为 4, 元素

$$b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

的阶为 3, 而 $ab$ 为无限阶元素.

20. 设 $G$ 是交换群，证明 $G$ 中的全体有限阶元素构成 $G$ 的一个子群.

21. 如果 $G$ 只有有限多个子群，证明 $G$ 是有限群.

22. 设 $H, K$ 为有限群 $G$ 的子群，证明 $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

23. 证明指数为 2 的子群必为正规子群.

24. 证明不存在恰有两个指数为 2 的子群的群.

25. 写出二面体群 $D_{20}$ 的全部正规子群.

26. 设 $S$ 为群 $G$ 的非空子集. 令

$$C_G(S) = \{x \in G \mid xa = ax, \ \forall\, a \in S\},$$
$$N_G(S) = \{x \in G \mid xSx^{-1} = S\}$$

($C_G(S)$ 和 $N_G(S)$ 分别称为 $S$ 在 $G$ 中的**中心化子**和**正规化子**). 证明：

(1) $C_G(S)$ 和 $N_G(S)$ 都是 $G$ 的子群；

(2) $C_G(S) \trianglelefteq N_G(S)$.

27. 设 $H, K$ 为 $G$ 的正规子群，证明：

(1) $HK = KH$;

(2) $HK \trianglelefteq G$;

(3) 如果 $H \cap K = \{e\}$, 则 $G$ 同构于 $G/H \oplus G/K$ 的子群.

28. 设 $m, n \in \mathbb{Z}$. 证明 $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ 当且仅当 $m$ 与 $n$ 互素.

29. 设 $G$ 为有限群, $N \trianglelefteq G$, $|N|$ 与 $|G/N|$ 互素. 如果 $G$ 的元素 $a$ 的阶整除 $|N|$, 证明 $a \in N$.

30. 设 $H, K$ 是群 $G$ 的子群, 证明 $H \cap K$ 的任一左陪集是 $H$ 的一个左陪集与 $K$ 的一个左陪集的交.

31. 设 $H, K$ 都是群 $G$ 的指数有限的子群, 证明 $H \cap K$ 在 $G$ 中的指数也有限.

32. 设 $H$ 是群 $G$ 的指数有限的子群, 证明 $G$ 有指数有限的正规子群.

33. 设 $p$ 为素数. 证明所有的 $p$ 阶群必为循环群, 因此也是交换群.

34. 试定出所有互不同构的 4 阶群.

35. 证明阶小于 6 的群皆交换, 举例说明存在 6 阶非交换群.

36. 设 $G$ 是 $n$ 阶群, 整数 $m$ 与 $n$ 互素. 如果 $g, h \in G$, 且 $g^m = h^m$, 证明 $g = h$. 再证明对于任一 $x \in G$, 存在唯一的 $y \in G$ 使得

$$y^m = x.$$

37. 设 $G$ 是群, $g \in G$. 若 $\mathrm{o}(g) = n$, 则 $\mathrm{o}(g^m) = n/(m, n)$.

38. 设 $H \leqslant G$, $K \leqslant G$, $a, b \in G$. 若 $Ha = Kb$, 则 $H = K$.

39. 设 $A, B, C$ 为 $G$ 的子群, 并且 $A \leqslant C$, 证明

$$AB \cap C = A(B \cap C).$$

40. 设 $A, B, C$ 为群 $G$ 的子群, 并且 $A \leqslant B$. 如果 $A \cap C = B \cap C$, $AC = BC$, 证明 $A = B$.

41. 设 $G$ 是群. 令 $Z(G)=\bigcap\limits_{g\in G}C_G(g)$. 称 $Z(G)$ 为 $G$ 的**中心**. 证明 $Z(G)$ 是 $G$ 的正规子群.

42. 证明 2 阶正规子群必属于群的中心.

43. 证明 $A_4$ 没有 6 阶子群.

44. 证明 $Z(A\oplus B)=Z(A)\oplus Z(B)$.

45. 证明：有限群 $G$ 是二面体群的充分必要条件是 $G$ 可由两个 2 阶元素生成.

## §1.2 环的基本概念

### 1.2.1 定义和简单性质

**定义 2.1** 如果一个非空集合 $R$ 上定义了两个二元运算 $+,\cdot$ (分别称为加法和乘法), 满足：

(1) $(R,+)$ 构成 Abel 群;

(2) **乘法结合律**: $(a\cdot b)\cdot c=a\cdot(b\cdot c),\ \forall\, a,b,c\in G$;

(3) **分配律**: $(a+b)\cdot c=a\cdot c+b\cdot c,\ c\cdot(a+b)=c\cdot a+c\cdot b,\forall\, a,b,c\in R$,

则称 $R$ 关于运算 $+,\cdot$ 构成一个**环**, 记为 $(R;+,\cdot)$, 或简记为 $R$.

环 $R$ 中若成立

(4) **乘法交换律**: $a\cdot b=b\cdot a,\ \ \forall\, a,b\in R$,

则称 $R$ 为**交换环**.

环 $R$ 中若存在乘法幺元, 即存在 $e\in R$, 使得对任意的 $a\in G$, 恒有

$$e\cdot a=a\cdot e=a,$$

则称 $R$ 为**幺环**.

环中的乘法运算符号 "$\cdot$" 经常略去不写. 加法群 $(R,+)$ 的幺元通常记为 0, 元素 $a$ 的加法逆元通常记为 $-a$. 乘法幺元通常记为 1.

我们比较熟悉的环有整数环 $(\mathbb{Z};+,\times)$、域 $K$ 上的一元多项式环 $K[x]$、多元多项式环 $K[x_1,\cdots,x_n]$、偶数环 $(2\mathbb{Z};+,\times)$ (不是幺环)、域 $K$ 上的 $n$ 阶全矩阵环 $\mathrm{M}_n(K)$ ($n>1$ 时不是交换环) 等.

如果一个环只有一个元素 (必为 0), 则称之为**零环**.

0 元素和负元素关于乘法有简单性质:

**命题 2.2** 设 $R$ 是环, 则

(1) $0a=a0=0,\ \forall\ a\in R$;

(2) $(-a)b=a(-b)=-(ab),\ \forall\ a,b\in R$.

**证明** (1) $0a+0a=(0+0)a=0a=0+0a$, 故 $0a=0$. 同样可证 $a0=0$.

(2) $(ab)+((-a)b)=(a+(-a))b=0b=0$, 故 $(-a)b=-(ab)$. 同样可证 $a(-b)=-(ab)$. □

下面我们考虑幺环中的乘法逆元素.

**定义 2.3** 设 $R$ 为幺环, $a\in R$. 如果 $b\in R$ 使得 $ba=1$, 则称 $b$ 为 $a$ 的一个**左逆元**. 类似地, 如果 $c\in R$ 使得 $ac=1$, 则称 $c$ 为 $a$ 的一个**右逆元**.

**命题 2.4** 设 $R$ 是幺环, $a\in R$. 如果 $a$ 有左逆元, 也有右逆元, 则左、右逆元必相等且唯一.

**证明** 如果 $b,c\in R$ 满足 $ba=1$, $ac=1$, 则 $b=b\cdot 1=b(ac)=(ba)c=1\cdot c=c$. 若又有 $d\in R$ 满足 $da=ad=1$, 则

$$b=b(ad)=(ba)d=d.$$ □

**定义 2.5** 设 $R$ 为幺环, $a\in R$. 如果 $b\in R$ 使得 $ba=ba=1$, 则称 $b$ 为 $a$ 的**逆元**, 记为 $a^{-1}$. 同时称 $a$ 为**可逆元** 或**单位元**.

容易验证幺环 $R$ 的可逆元的全体构成乘法群, 记为 $R^{\times}$.

在环中我们使用通常的运算记号, 即对于环 $R$ 的元素 $a$ 和正整数 $n$, 令

$$na=\underbrace{a+\cdots+a}_{n\text{个}},$$

$0a = 0$ (左端的 0 是数，右端的 0 是 $R$ 的零元素),

$(-n)a = n(-a)$,

$a^n = \underbrace{a \cdots a}_{n个}$.

若 $R$ 是幺环，则令

$$a^0 = 1.$$

又若 $a$ 为可逆元，则令

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

在这些记号下，容易验证

$$ma + na = (m+n)a,$$
$$a^m a^n = a^{m+n},$$
$$(ma)(nb) = mn(ab),$$

其中 $m, n$ 为任意整数， $a, b$ 为环 $R$ 的任意元素 (只要记号有意义).

在矩阵环中我们遇到过两个非零的矩阵相乘可以为零. 这导致所谓"零因子"的概念. 设 $a$ 为环 $R$ 的元素，如果存在 $b \in R\setminus\{0\}$ 使得 $ab = 0$, 则称 $a$ 是 $R$ 中的一个**左零因子**；如果存在 $c \in R\setminus\{0\}$ 使得 $ca = 0$, 则称 $a$ 是 $R$ 中的一个**右零因子**. 如果 $a$ 既是左零因子又是右零因子，则称 $a$ 是 $R$ 中的一个**零因子**. 在交换环中显然左、右零因子是同一概念，它们都是零因子.

一类非常重要的环是:

**定义 2.6** 没有非零零因子的、至少含有两个元素的交换幺环称为**整环**.

定义中所说的"至少含有两个元素"等同于"$0 \neq 1$" (请读者自己验证之).

### 1.2.2　子环、理想及商环

**定义 2.7**　设 $(R;+,\cdot)$ 是环，$S\subseteq R$. 如果 $(S;+,\cdot)$ 构成一个环，则称 $S$ 为 $R$ 的**子环**.

如同对于子群的讨论，要验证环 $R$ 的一个子集 $S$ 是子环，没有必要验证 $S$ 满足环的定义中的全部条件，而只需验证

(1) $S$ 非空；

(2) $S$ 关于加法构成群，即对于任意的 $a,b\in S$, 有 $a-b\in S$;

(3) $S$ 在乘法下封闭，即对于任意的 $a,b\in S$, 有 $a\cdot b\in S$.

例如 $2\mathbb{Z}$ 是 $\mathbb{Z}$ 的子环，$\mathbb{Z}$ 是 $\mathbb{Q}$ 的子环，$\mathrm{M}_n(\mathbb{R})$ 是 $\mathrm{M}_n(\mathbb{C})$ 的子环.

子环作为环的加法子群当然有陪集，但是一般而言这种陪集的乘积不一定还是陪集 (这里的乘积的含义类似于群的子集的乘积，即对于环 $R$ 的子集 $S,T$, 定义 $ST=\{\,st\mid s\in S,\ t\in T\,\}$), 甚至不是任一陪集的子集. 例如 $\mathbb{Z}$ 作为 $\mathbb{Q}$ 的加法子群，其陪集中不可能同时含有整数和非整数 (否则与“不同的陪集不相交”矛盾). 但是 $\left(\frac{1}{2}+\mathbb{Z}\right)\mathbb{Z}\supset\left\{1,\frac{1}{2}\right\}$, 所以 $\left(\frac{1}{2}+\mathbb{Z}\right)\mathbb{Z}$ 不含于任一陪集. 为了避免这种情形的发生 (进而在陪集集合上定义环结构)，我们需要对于子环增加一些限制，而引入“理想”的概念，它在环论中的地位类似于正规子群在群论中的地位.

**定义 2.8**　设 $(R;+,\cdot)$ 是环，$I$ 是 $R$ 的加法子群，并且对于任意的 $r\in R$, 有 $rI\subseteq I$ (相应地，$Ir\subseteq I$), 则称 $I$ 为 $R$ 的一个**左** (相应地，**右**)**理想**. 如果一个加法子群 $I$ 同时是左、右理想，则称 $I$ 为 $R$ 的**双边理想**，或简称为**理想**.

显然左（右）理想都是子环.

**命题 2.9**　*设 $I$ 是 $R$ 的理想，则对于任意的 $r,s\in R$, 有*

$$(r+I)(s+I)\subseteq rs+I.$$

**证明**　对于任意的 $a,b\in I$, 由于 $I$ 是双边理想，所以 $rb,as,ab\in I$. 故 $(r+a)(s+b)=rs+rb+as+ab\in rs+I$. □

# 有关此电子图书的说明

本人由于一些便利条件，可以帮您提供各种中文电子图书资料，且质量均为清晰的PDF图片格式，质量要高于网上大量传播的一些超星 PDG 的图书。方便阅读和携带。只要图书不是太新，文学、法律、计算机、人文、经济、医学、工业、学术等方面的图书，我都可以帮您找到电子版本。所以，当你想要看什么图书时，可以联系我。我的 QQ是：85013855，大家可以在 QQ上联系我。