国家科学技术学术著作出版基金
NEAPST

现代数学基础丛书 152

有限群初步

徐明曜 著

科学出版社

国家科学技术学术著作出版基金资助出版

现代数学基础丛书 152

有限群初步

徐明曜 著

科学出版社

北京

内 容 简 介

本书是在十多年前出版的《有限群导引》的基础上进行修改、补充、材料更新以及删减过时内容而形成的新的有限群教材. 全书共分 8 章. 第 1 章叙述群论最基本的概念, 其中有些内容在群论课程的先修课“抽象代数”中已经学过, 但相当部分内容是新的. 整个这一章是学习本书的基础, 因此必须认真阅读, 并且应该做其中大部分的习题. 从第 2 章起则是沿着两条主线进行: 一条主线是群的作用; 另一条主线是关于群的构造问题. 本书作者多年从事有限群的教学和研究工作, 这本教材是他多年教学工作的总结.

本书可作为有限群研究方向的研究生的入门教材及参考书, 也可作为数学专业硕士研究生的公共选修课教材. 认真研读过本书的读者即可在导师指导下开始阅读文献和学位论文写作的准备工作.

图书在版编目(CIP)数据

有限群初步/徐明曜著. —北京: 科学出版社, 2014.1
(现代数学基础丛书; 152)
ISBN 978-7-03-039411-8
Ⅰ. 有… Ⅱ. ①徐… Ⅲ. ①有限群 Ⅳ. ①O152.1

中国版本图书馆 CIP 数据核字(2013) 第 309844 号

责任编辑: 赵彦超 李静科 / 责任校对: 钟 洋
责任印制: 赵德静 / 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

文林印务有限公司 印刷
科学出版社发行 各地新华书店经销
*
2014 年 1 月第 一 版 开本: 720 × 1000 1/16
2014 年 1 月第一次印刷 印张: 24 1/2
字数: 470 000
定价: 118.00 元
(如有印装质量问题, 我社负责调换)

《现代数学基础丛书》编委会

《现代数学基础丛书》序

对于数学研究与培养青年数学人才而言，书籍与期刊起着特殊重要的作用．许多成就卓越的数学家在青年时代都曾钻研或参考过一些优秀书籍，从中汲取营养，获得教益．

20 世纪 70 年代后期，我国的数学研究与数学书刊的出版由于“文化大革命”的浩劫已经破坏与中断了 10 余年，而在这期间国际上数学研究却在迅猛地发展着．1978 年以后，我国青年学子重新获得了学习、钻研与深造的机会．当时他们的参考书籍大多还是 50 年代甚至更早期的著述．据此，科学出版社陆续推出了多套数学丛书，其中《纯粹数学与应用数学专著》丛书与《现代数学基础丛书》更为突出，前者出版约 40 卷，后者则逾 80 卷．它们质量甚高，影响颇大，对我国数学研究、交流与人才培养发挥了显著效用．

《现代数学基础丛书》的宗旨是面向大学数学专业的高年级学生、研究生以及青年学者，针对一些重要的数学领域与研究方向，作较系统的介绍．既注意该领域的基础知识，又反映其新发展，力求深入浅出，简明扼要，注重创新．

近年来，数学在各门科学、高新技术、经济、管理等方面取得了更加广泛与深入的应用，还形成了一些交叉学科．我们希望这套丛书的内容由基础数学拓展到应用数学、计算数学以及数学交叉学科的各个领域．

这套丛书得到了许多数学家长期的大力支持，编辑人员也为其付出了艰辛的劳动．它获得了广大读者的喜爱．我们诚挚地希望大家更加关心与支持它的发展，使它越办越好，为我国数学研究与教育水平的进一步提高做出贡献．

杨　乐

2003 年 8 月

前　言

拙作《有限群导引》上册出版至今已有 26 年, 下册问世也已过去 14 年. 承蒙读者的厚爱, 本书在国内有限群教学和科研上起了一点正面的作用, 这使笔者由衷地欣慰. 在这 26 年中, 我收到了很多读者来信, 有因该书售缺而索要图书的, 有就具体内容与作者商榷的, 有谈自己的学习感受的, 但更多的来信是指出书中的不足之处并提出了很好的修改意见. 另外, 自该书初版出版 26 年来, 有限群论又取得了长足的进步, 致使书中不少材料已经过时, 而新的进展又没能包括进来. 最近, 科学出版社的同仁建议在原书基础上作一次彻底的修改, 出一本适合今天的新书, 这也正是笔者的愿望. 于是我抓紧时间, 对全书的内容做了新的安排, 也充分考虑到使用本书的不同群体的需要, 经过近一年的努力, 最终完成了这本书的写作任务.

我首先对这本书的内容作一介绍.

本书共分 8 章. 第 1 章叙述群论最基本的概念, 其中很多内容 (特别是前五节) 在群论课程的先修课“抽象代数”中已经学过, 因此对这些内容一般不再给出证明. 但本章也补充了相当多的新材料, 它们对以后的学习非常重要. 这一章是学习本书的基础, 必须认真阅读, 并且要做大部分的习题. 第 2 章讲述群在集合上的作用, 介绍了置换表示、转移映射的概念及应用, 也介绍了置换群最基本的概念. 附带提一下, 笔者认为, 群的作用是群论的本质和灵魂, 学习本书者必须很好地体会和把握. 因此, 群作用的思想是贯穿全书的, 而群作用的对象也不一定只是集合, 而应该包括线性空间、组合结构、几何结构, 以至于群本身. 群在线性空间上的作用就是群表示论, 这在第 7 章中详细讲述, 而群在群上的作用则是最后一章, 即第 8 章的内容. 这两章除了介绍这两种作用的基本理论外, 还包括了它们经典的应用, 例如 Burnside p^aq^b 定理、Glauberman ZJ 定理等. 另外, 在以“更多的群例”为名的第 4 章中, 我们主要也是讲群的作用, 其中有群在有限几何和图上作用的两个例子, 也有群在内积空间上的作用 (典型群的介绍). 因此群作用是本书的一条主线. 另一条主线是关于群的构造问题. 大家知道, 代数的基本问题之一就是构造和分类问题. 本书的第 3 章简单介绍了群的构造理论, 包括 Jordan-Hölder 定理、Krull-Schmidt 定理、Schur-Zassenhaus 定理和群扩张理论等. 值得提出的是, 我们对 Schur-Zassenhaus 定理的证明没有使用群扩张理论, 这可以把需要冗长计算的枯燥的群扩张理论一节放在本章的最后. 为了加深对群构造理论的理解, 也为了介绍几族重要的有限单群, 我们在第 4 章中除了前面提到的继续讲群作用外, 还简单介绍了典型单群和最早发现的零散单群 ——Mathieu 群 M_{11} 和 M_{12}. 本书的第 5 章和第 6 章则介绍幂零群

和可解群的基本理论. 由于有限单群分类被认为完成以后, 特别是自本世纪初以来, 有限 p-群异常地活跃, 我们在第 5 章加了几节关于 p-群的介绍. 而第 6 章根据很多同行的建议彻底重写了, 加上了关于群系以及 Carter 子群的内容. 在全书最后, 我们对需要在某个方面了解更多的读者给出了进一步阅读的书目. 而且, 夹杂在各章中, 还安排了六七节所谓“阅读材料”, 讲述了更多的知识. 但不读这些“阅读材料”, 并不影响对全书的理解.

下面, 我再对使用本书的教师提些建议.

本书可作为硕士研究生一个学期的公共选修课的教材. 教师可根据本人的兴趣和学生的代数基础选择第 1, 2, 3 章作为教材, 也可选第 1, 2, 4 章 (为多了解一些单群的例子)、第 1, 2, 7 章 (为讲表示论的基本知识) 作为教材. 如果学生基础较差, 可只选第 1, 2 章为教材. 这样的选修课大约用 48 课时, 每周 3 课时. 还可有一种选择是详讲第 1 章, 再把第 2, 3, 5, 6 章的前面几节做介绍性讲解, 这可使学生对有限群理论的全貌有比较清楚的概念. 至于习题, 可由教师选择半数左右、偏容易的题目.

更多的教师是用本书作为有限群研究方向的研究生的专业课教材, 为此可安排一年时间, 采取教师重点讲授, 学生组织讨论班自行讨论的办法. 建议第 1, 2, 3, 4 章要全学, 第 5, 6, 7, 8 章则根据学生具体的研究方向学习大部分或一部分. 习题要基本全做.

对于学习本书的研究生, 我想提几点忠告:

1. 知识面不要太窄, 对于有限群这样在整个数学中也是少有的内容十分丰富的研究领域, 本书选择的内容已经非常有限, 如不全学, 恐怕在进入研究论文阶段时会感到知识不足. 有些学生希望尽快进入论文阶段, 对于他们, 我建议在进入研究题目后, 仍应抽出一定时间研读本书未读过的部分.

2. 学习数学, 不是逻辑上弄懂就可以了, 从逻辑上弄懂到真正掌握还有很大的距离. 常言道“知其然要知其所以然”, 我更要说“知其所以然还要知其不得不然”. 把一个定理、一种方法变成自己的东西, 即所谓“学到手”, 其标准是看你会不会用. 这时, 习题是一个方便的检验办法. 因此习题要尽量多做, 而且不要看提示和答案, 憋上它几天, 实在不行再去看提示.

3. 为了学懂一点东西, 做到华罗庚先生所说的“书先要越读越厚, 然后要越读越薄”, 把书本上的东西变成自己的东西, 必须要反复, 而且要反复多遍. 要做到能把隐藏在逻辑推理背后的数学思想找出来 (这常常是作者没有说到的东西), 必须经过反复的思索和揣摩. 一旦把这些东西理解了, 再和有关的知识贯穿起来思考, 才能找到其数学思想的精髓, 而最后豁然开朗, 感到不过就是那么一点东西. 这就达到了华先生所谓的书越读越薄的境界.

4. 学数学要记忆! 有人讲, 学数学主要是理解, 理解了自然就记住了. 我的体

会与此不同. 我觉得固然学数学主要是理解, 但理解了不一定就记住了, 必须经过记忆的功夫才能记住 (至少对常人来说是如此). 如果学了而记不住, 用时就想不到, 还等于没有变成自己的东西.

5. 注重初等技巧的训练. 在群论中, 大定理固然重要, 但容易记, 容易用, 而初等技巧则要靠长时间的磨练才能掌握. 因此, 对于初等方法和技巧的训练, 在本书写作中就特别注意. 比如, 本书相当多的内容就是为了介绍方法而写入的. 另外, 由于作者认为, 本书的读者都受过较充分的抽象代数的训练, 因而书中定理的证明常有意写得比较简短, 以给读者较多的思考余地, 这也是方法训练的一部分.

下面再对书中定义、定理、习题等的编号作一说明. 在课文中定理、定义、命题、引理等一起按顺序编号, 例如我们说命题 5.1.7, 指的是第 5 章第 1 节的第 7 个陈述, 它是一个命题. 它后面的第 8 个陈述是定理, 就叫定理 5.1.8. 但习题单独编号. 习题 1.1.1 是指第 1 章第 1 节的第 1 个习题, 等等.

最后, 我要感谢《有限群导引》(下册) 的作者李慧陵、李世荣、黄建华教授, 在本书的写作中, 笔者使用了他们在该书中写的一些材料或想法. 同时我还要感谢我的同事陈贵云、郭文彬、郭秀云、海进科、李慧陵、李天则、黎先华、李样明、刘伟俊、刘燕俊、钱国华、曲海鹏、申振才、施武杰、王燕鸣、徐竞、曾吉文、张勤海、张志让等人的帮助, 他们仔细阅读了全书的初稿, 并提出大量修改意见.

本书在正式出版前, 曾在北京交通大学试讲, 感谢该校选修此课的研究生提出的大量修改意见.

徐明曜

2013 年 8 月于北京大学

目　录

第 1 章　群论的基本概念

阅读提示： 本章是群论最基本的知识，学习本书者应该仔细研读，并做大部分习题.

本章是对抽象代数课程中已经学过的群论的基本概念进行复习和补充. 因此，很多结果不再给出证明.

1.1　群 的 定 义

定义 1.1.1　称非空集合 G 为一个群，如果在 G 中定义了一个二元运算，叫做乘法，它满足

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

(2) 存在单位元素：存在 $1 \in G$，使得对任意的 $a \in G$，恒有

$$1a = a1 = a;$$

(3) 存在逆元素：对任意的 $a \in G$，存在 $a^{-1} \in G$，使得

$$aa^{-1} = a^{-1}a = 1.$$

定义一个群有多种不同的方式. 例如，上述条件 (2)，(3) 可以分别减弱为

(2′) 存在左 (右) 单位元素：存在 $1 \in G$，使得对任意的 $a \in G$，有 $1a = a$ $(a1 = a)$；

(3′) 存在左 (右) 逆元素：对任意的 $a \in G$，存在 $a^{-1} \in G$，使得 $a^{-1}a = 1$ $(aa^{-1} = 1)$.

则条件 (1)，(2′) 和 (3′) 亦可定义一个群. 又，我们有

定义 1.1.2　称非空集合 G 为一个群，如果在 G 中定义了一个二元运算，叫做乘法. 它满足

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

(4) 对任意的 $a, b \in G$，存在 $x, y \in G$，满足 $ax = b$ 和 $ya = b$.

更多的定义群的方法可以参看 [45].

定义 1.1.3　如果群 G 满足

(5) 交换律：$ab = ba$，$a, b \in G$，则称 G 为交换群或 Abel 群.

在我们熟悉的基本数系, 即正整数系 $\mathbb{N}$、整数系 $\mathbb{Z}$、有理数系 $\mathbb{Q}$、实数系 $\mathbb{R}$ 和复数系 $\mathbb{C}$ 中就可以找到很多群的例子, 而且它们都是交换群.

例 1.1.4　$\mathbb{Z}$ 对加法成群 $(\mathbb{Z},+)$.

例 1.1.5　任一数域 $\mathbf{F}$ 对加法成群 $(\mathbf{F},+)$. 特别地, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ 是群.

例 1.1.6　任一数域 $\mathbf{F}$ 的非零元素集合 $\mathbf{F}^{\#}$ 对乘法成群 $(\mathbf{F}^{\#},\cdot)$. 特别地, $(\mathbb{Q}^{\#},\cdot),(\mathbb{R}^{\#},\cdot),(\mathbb{C}^{\#},\cdot)$ 是群.

例 1.1.7　正有理数集 $\mathbb{Q}^{+}$ 和正实数集 $\mathbb{R}^{+}$ 对乘法成群 $(\mathbb{Q}^{+},\cdot)$, $(\mathbb{R}^{+},\cdot)$.

例 1.1.8　模为 1 的全体复数对乘法成群 $\mathbb{C}_1$.

例 1.1.9　设 n 为正整数, n 次单位根的全体对乘法组成群 U_n, 并且 $\bigcup\limits_{n=1}^{\infty} U_n = U$ 对乘法也成群. 容易证明, 由数组成的所有有限乘法群都是 U 的子群.

例 1.1.10　整数环 $\mathbb{Z}$ 关于理想 (n) 的同余类环 $\mathbb{Z}_n = \mathbb{Z}/(n)$ 对加法成群 $(\mathbb{Z}_n,+)$.

在抽象代数中我们还学过四元数体 $\mathbf{Q} = \mathbb{R} + i\mathbb{R} + j\mathbb{R} + k\mathbb{R}$.

例 1.1.11　四元数体的 8 个单位元素 $\{\pm 1, \pm i, \pm j, \pm k\}$ 在四元数的乘法下封闭, 它们组成 8 阶**四元数群** Q_8. 这个群是非交换的.

例 1.1.12　设 $\mathbf{F}$ 是一个域, 则 $\mathbf{F}$ 上二阶满秩上三角矩阵集合

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a,b,c \in \mathbf{F}, ac \neq 0 \right\}$$

对矩阵乘法组成一个群.

例 1.1.13　上例中行列式为 1 的二阶上三角矩阵集合 H 以及主对角线元素为 1 的二阶上三角矩阵集合 K 对矩阵乘法都组成群:

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \middle| a,b \in \mathbf{F}, a \neq 0 \right\}, \quad K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbf{F} \right\}.$$

请读者自行判断上面二例中的群 G, H, K 哪个是交换群, 哪个是非交换群.

在本书中, 我们还将接触到很多其他的群, 这将在后面陆续介绍.

现在回过来看群的定义. 由第 1 条公理即结合律可推出下面的**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"[①] 都得出相同的值, 因而上述乘积是有意义的.

① 因为群的乘法是二元运算, 根据定义, 只有两个元素的乘积才有意义, 多个元素的乘积必须通过逐步作两个元素的乘积来实现. 所谓 "有意义的加括号方式" 指的就是给定的一种确定的运算次序. 例如对乘积 $abcde$, 我们称 $((ab)c)(de)$, $((a(bc))d)e, \cdots$ 为 "有意义的加括号方式", 但 $((abc)d)e$, $(ab)(cd)e, \cdots$ 则不是.

由广义结合律, 有限多个群元素的乘积 $a_1a_2\cdots a_n$ 是有意义的, 不需要再具体指定乘法是依什么次序实施的. 而在交换群中, 连乘积 $a_1a_2\cdots a_n$ 中诸因子 $a_1,a_2,\cdots,a_n$ 的次序也可以任意调换, 其值是不变的.

又, 由广义结合律 (1′), 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

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

显然有

$$a^ma^n=a^{m+n},\qquad (a^m)^n=a^{mn},\qquad m,n是整数.$$

又, 对于乘积的逆, 有下列法则:

命题 1.1.14 设 G 是群, $a_1,a_2,\cdots,a_n\in G$, 则

$$(a_1a_2\cdots a_n)^{-1}=a_n^{-1}\cdots a_2^{-1}a_1^{-1}.$$

有人称命题 1.1.14 为穿–脱原理 (dressing-undressing principle), 这种叫法是很形象的, 就是先穿的衣服只能后脱下来.

下面对我们使用的符号做些说明: 我们用大写英文字母 $G,H,K,A,B,\cdots$ 表示群或集合, 小写英文字母 $a,b,c,\cdots$ 表示它的元素; 以 1 表示群的单位元素以及仅由单位元素组成的子群, 对二者不加区别, 读者可从上下文来判断 1 究竟代表单位元素还是单位子群. 以 $|G|$ 表示集合 G 的势. 如果 G 是群, 则 $|G|$ 叫群的阶. 又, 称 G 为有限群, 如果 $|G|$ 是有限数, 否则叫做无限群.

除了群中元素的乘积之外, 我们还可以如下定义群中子集的乘积: 设 G 是群, H,K 是 G 的子集, 规定 H,K 的乘积为

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

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

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

很明显, 子集的乘法也满足结合律和广义结合律, 因而也可以定义子集 H 的正整数次幂 H^n:

$$H^n=\{h_1h_2\cdots h_n\mid h_i\in H\},$$

并且对子集的乘法也成立命题 1.1.14.

最后我们定义群中元素的阶.

定义 1.1.15　设 G 是群, $a \in G$. 能使 $a^n = 1$ 成立的最小的正整数 n 叫做元素 a 的阶, 记作 $o(a) = n$. 如果不存在这样的正整数 n, 我们就称 a 是无限阶元素, 记作 $o(a) = \infty$.

例如, 在例 1.1.4 中, 整数 0 在群 $(\mathbb{Z}, +)$ 中的阶是 1, 而其他整数的阶都是 ∞. 在例 1.1.11 中, 元素 $\pm i$, $\pm j$, $\pm k$ 的阶都是 4, 而元素 -1 的阶是 2, 元素 1 的阶是 1.

例 1.1.16　设 G 是群, $g \in G$, $o(g) = n$, 则 $o(g^m) = n/(m, n)$.

解　首先, $(g^m)^{n/(n,m)} = (g^n)^{m/(n,m)} = 1$, 得 $o(g^m) \leqslant n/(m, n)$. 又若 $o(g^m) = k$, 则 $(g^m)^k = 1$, $n|mk$. 令 $m = m_1(m, n)$, $n = n_1(m, n)$, 得 $n_1|m_1k$. 但 $(m_1, n_1) = 1$, 得 $n_1 \mid k$, 即 $n/(m, n) \leqslant o(g^m)$. 于是 $o(g^m) = n/(m, n)$. □

习　　题

1.1.1. 设 G 是群, 则 G 中满足*消去律*

$$ac = bc \Longrightarrow a = b, \qquad \forall a, b \in G$$

和

$$ca = cb \Longrightarrow a = b, \qquad \forall a, b \in G.$$

举例说明只假定结合律和消去律不足以定义一个群. 但对有限非空集合 G 来说, 如果定义了一个满足结合律和消去律的二元运算, 那么 G 是一个群.

1.1.2. 设 G 是群, $a, b \in G$, 则 $o(a) = o(a^{-1})$, $o(ab) = o(ba)$.

1.1.3. 设 G 是群, $g_1, g_2 \in G$. 若 $o(g_1) = n_1$, $o(g_2) = n_2$, $(n_1, n_2) = 1$, 且 $g_1g_2 = g_2g_1$, 则 $o(g_1g_2) = n_1n_2$. 并举例说明如果 $g_1g_2 \neq g_2g_1$, 则无此结论.

1.1.4. 设 G 是群, $g \in G$. 若 $o(g) = n_1n_2$, $(n_1, n_2) = 1$, 则存在 $g_1, g_2 \in G$, 使 $g = g_1g_2 = g_2g_1$, 并且 $o(g_1) = n_1$, $o(g_2) = n_2$. 证明 g_1, g_2 被这些条件所唯一决定.

1.1.5. 设 $|G| = n$, $a_1, a_2, \cdots, a_n$ 是群 G 的 n 个元素, 不一定互不相同, 则存在整数 i, j, $1 \leqslant i \leqslant j \leqslant n$ 使 $a_ia_{i+1} \cdots a_j = 1$.

1.2　子群和陪集

定义 1.2.1　称群 G 的非空子集 H 为 G 的*子群*, 如果 $H^2 \subseteq H$, $H^{-1} \subseteq H$. 这时记作 $H \leqslant G$.

事实上, 易验证如果 H 是 G 的子群, 则必有 $H^2 = H$, $H^{-1} = H$, 并且 $1 \in H$. 显然, 任何群 G 都有二子群 G 和 1, 我们称 1 为 G 的*平凡子群*.

命题 1.2.2　*设 G 是群, $H \subseteq G$, 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 $a^{-1}b\in H$).

命题 1.2.3 设 G 是群, $H\subseteq G$, $|H|$ 是有限数, 则

$$H\leqslant G \iff H^2\subseteq H.$$

若干个子群的交仍为子群, 即我们有

定理 1.2.4 设 G 是群. 若 $H_i\leqslant G$, $i\in I$, I 是某个指标集, 则 $\bigcap\limits_{i\in I}H_i\leqslant G$.

一般来说若干子群的并不是子群, 例如可见习题 1.2.3. 但我们有下述概念:

定义 1.2.5 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, 记作 $\langle M\rangle$.

容易看出, $\langle M\rangle=\{1,a_1a_2\cdots a_n \mid a_i\in M\cup M^{-1},\ n=1,2,\cdots\}$.

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. 能由一个元素 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.

下面的结论是十分重要的.

定理 1.2.6 设 G 是群, $H\leqslant G, K\leqslant G$, 则

$$HK\leqslant G \iff HK=KH.$$

证明 $\Rightarrow$: 由 $HK\leqslant G$ 有 $(HK)^{-1}=HK$, 即 $K^{-1}H^{-1}=HK$. 又由 $H\leqslant G$, $K\leqslant G$, 有 $H^{-1}=H$, $K^{-1}=K$, 于是 $KH=HK$.

$\Leftarrow$: 由 $HK=KH$ 可得 $(HK)^2=HKHK=HHKK=HK$, $(HK)^{-1}=K^{-1}H^{-1}=KH=HK$, 由定义 1.2.1 即得 $HK\leqslant G$. □

下面我们研究子群的陪集.

定义 1.2.7 设 $H\leqslant G$, $a\in G$. 称形如 $aH(Ha)$ 的子集为 H 的一个左 (右) 陪集. 容易验证 $aH=bH \iff a^{-1}b\in H$. 类似地, 有 $Ha=Hb \iff ab^{-1}\in H$.

命题 1.2.8 设 $H\leqslant G, a,b\in G$, 则

(1) $|aH|=|bH|$;

(2) $aH\cap bH\neq\varnothing\Rightarrow aH=bH$.

于是, G 可表成 H 的互不相交的左陪集的并:

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

元素 $\{a_1,a_2,\cdots,a_n\}$ 叫做 H 在 G 中的一个(左) 陪集代表系. H 的不同左陪集的个数 n (不一定有限) 叫做 H 在 G 中的指数, 记作 $|G:H|$.

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 $|G:H|$.

下面的定理对于有限群是基本的.