新世纪高等学校教材

北京高等教育精品教材

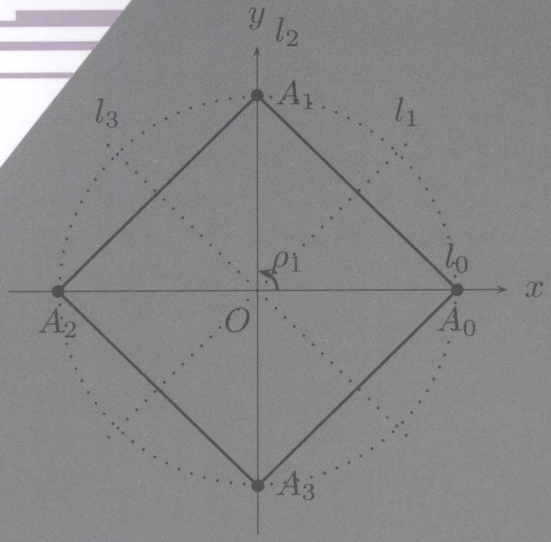
数学与应用数学基础课系列教材

DAISHU XUE JICH

代数学基础（下册）

北京师范大学数学科学学院　主　编

张英伯　王恺顺　编　著



北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

新世纪高等学校教材

北京高等教育精品教材

数学与应用数学基础课系列教材

代数学基础

（下册）

DAISHUXUE JICHU

北京师范大学数学科学学院 主 编
张英伯 王恺顺 编 著

北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

图书在版编目(CIP)数据

代数学基础（下册）／张英伯，王恺顺编著．—北京：北京师范大学出版社，2013.8
（新世纪高等学校教材．数学与应用数学基础课系列教材）
ISBN 978-7-303-16714-2

Ⅰ．①代… Ⅱ．①张…②王… Ⅲ．高等代数－高等学校－教材 Ⅳ．①O15

中国版本图书馆 CIP 数据核字（2013）第 165930 号

营销中心电话　010-58802181 58805532
北师大出版社高等教育分社网　http://gaojiao.bnup.com
电子信箱　gaojiao@bnupg.com

出版发行：北京师范大学出版社 www.bnup.com
北京新街口外大街 19 号
邮政编码：100875
印　刷：北京京师印务有限公司
经　销：全国新华书店
开　本：170 mm × 230 mm
印　张：11.5
字　数：225 千字
版　次：2013 年 8 月第 1 版
印　次：2013 年 8 月第 1 次印刷
定　价：20.00 元

策划编辑：岳昌庆　责任编辑：岳昌庆　胡　维
美术编辑：王齐云　装帧设计：王齐云
责任校对：李　菡　责任印制：孙文凯

序言

北京师范大学张禾瑞先生所编“近世代数基础”是 20 世纪 50 年代以来在同类教材中不可多得的精品，成为当时全国高等院校数学系培养代数人才的入门导引. 随着社会进入了信息化时代，数学科学日趋重要，目前国外一些大学的数学系已大大加强了代数课程的教学. 笔者曾翻译过莫斯科大学的代数学引论第一卷，受到这本书和欧美一些大学代数教材的启发，我们试图将这门课程与国际接轨，将数学学科现代发展所需的基础知识融会贯通.

教材的编排是这样的，第一、二、四章，内容是传统的群、环、域，但做了适当的深化. 比如群在集合上的作用、西罗定理、合成群列、可解群、交换环的素理想等. 第三章是主理想环上有限生成模的结构；第五章伽罗瓦理论. 代数学基础一书介绍了直到 19 世纪初叶代数学的主要框架，试图为学生进入现代代数学理论的学习奠定基础.

书中部分内容用星号标注，使得任课老师可以根据学生的情况进行取舍. 教学安排可以有两种方式. 对于喜欢代数的学生，在大二的上、下两个学期将全书讲完，并选择适当的课外专题，组织讨论班. 否则可以只讲第一、二、四章中的必修内容，第三、五章可作为选修.

这本教材已经在北京师范大学使用了六年，在首都师范大学的部分班级使用了三年，在这期间，老师和同学们对教材提出了宝贵的意见，因而是一部集体劳动的结晶. 我们特别感谢邓邦明、胡永建教授，李建华、刘玉明、曾紫婷、胡维副教授，他们提出的修改意见无论在数学内容上还是在文字叙述上都是非常关键的. 首都师范大学的学生叶文锐、高剑伟、朱波同学对第四、五章提出了宝贵的改进意见，在此一并致谢.

编者

2013-06-01

前言

1915 年北京高等师范学校成立数理部，1922 年成立数学系．2004 年成立北京师范大学数学科学学院．经过近百年的风风雨雨，数学科学学院在学科建设、人才培养和教学实践中积累了丰富的经验．将这些经验落实并贯彻到教材编著中去是大有益处的．

培养人才和编写教材是学院两项非常重要的工作．教材的编写是学院的基本建设之一．学院要抓好教材建设；教师要研究教学方法．在教材方面，学院要推出一批自己的高水平教材．另外，编写教材要注意的几项基本原则：写教材要慢一点，质量要好一点，教材修订连续化，教材出版系列化．

2005 年 5 月，由学院李仲来教授和北京师范大学出版社理科编辑部岳昌庆、王松浦进行了沟通和协商，由北京师范大学数学科学学院主编 (李仲来教授负责)，准备对学院教师目前使用的，或北京师范大学出版社已经没有存书的部分教材进行修订后再版，另有一些教材需要重新编写．计划用几年时间，出版数学与应用数学系列教材、数学教育主干课程系列教材、大学公共课数学系列教材、数学学科硕士研究生基础课程系列教材，共 4 个系列约 60 余部教材．

2005 年起，由学院组织和动员全院在职和退休教师之力量，主编出版数学一级学科 4 个系列课程教材．教材编写涉及面之广、数量之大、持续时间之长，这在一所高校数学院系内是为数不多的，其数量在中国数学界列全国第一．经过 8 年的编写，至今已经出版了 50 余部教材，原计划的大多数教材已经出版，对于学院来讲，这是一件值得庆贺的大事．现在可以说，数学科学学院和北京师范大学出版社基本上是干成了一件大事．若留下缺憾，则需要后人去补充．

从数量上看，按教材系列，出版数学与应用数学系列教材 28 部、数学教育主干课程系列教材 9 部、大学公共课数学系列教材 7 部、数学学科硕士研究生基础课程系列教材 10 部．按出版教材版次，第 1 版 21 部、第 2 版 21 部、第 3 版 12 部．还出版了 3 部教辅教材．从质量上看，14 部教材被评为普通高等教育“十一五”“十二五”国家级规划教材；7 部教材被评为北京市高等教育精品教材；《师范院校数学学科 4 个系列教材建设》项目获 2012 年北京师范大学教育教学成果一等奖．

本套教材可供高等院校本科生、教育学院数学系、函授和网络学院 (数学专业)，以及在职中学教师等使用和参考．(李仲来执笔)

北京师范大学数学科学学院 2013-06-26

目 录

第一章　群

我们在上册中已经介绍了群的定义，看到了对称群、循环群等一些例子. 在本章中，我们将介绍群论最基本的概念和定理：正规子群与商群，群的同态，群的同构定理，单群，群在集合上的作用与西罗定理，以及合成群列和可解群.

§1.1　群的另一定义

在代数学中，集合的变换群、几何图形的对称群、由满足某些性质的可逆矩阵构成的典型群 (例如一般线性群和特殊线性群)，是群论研究的重要对象. 我们在本节介绍变换群的定义，给出刻画正多边形对称性的群 —— 二面体群，然后叙述群的另一定义.

我们在上册第二章和第三章看到，群的概念的形成是从研究置换开始的. n 元有限集合 X 的全体置换关于置换的合成构成对称群 S_n，它的子群通常称为 X 上的 **置换群** (permutation group). 如果去掉集合 X 有限的限制，我们得到更一般的情况.

例 1　设 X 是一个非空集合，$S(X)$ 是 X 的所有一一变换构成的集合，那么 $S(X)$ 关于变换的合成构成一个群，叫作 X 上的 **全变换群** (full transformation group)，它的子群通常称为 X 上的 **变换群** (transformation group).

例 2　设 G 是一个群，$\mathrm{Aut}(G)$ 是群 G 的所有自同构的集合. 则 $\mathrm{Aut}(G)$ 关于变换的合成构成一个群，称为 G 的 **自同构群** (automorphism group).

证明　易见 $\mathrm{Aut}(G)$ 是 $S(G)$ 的一个非空子集，因而只需证明 $\mathrm{Aut}(G)$ 是 G 的一个子群. 任取 $\sigma, \tau \in \mathrm{Aut}(G)$，都有

$$(\sigma\tau)(xy) = \sigma(\tau(xy)) = \sigma(\tau(x)\tau(y)) = (\sigma\tau)(x)(\sigma\tau)(y), \quad \forall\, x, y \in G,$$

所以 $\sigma\tau \in \mathrm{Aut}(G)$. 另一方面，

$$\sigma(\sigma^{-1}(xy)) = xy = \sigma(\sigma^{-1}(x))\sigma(\sigma^{-1}(y)) = \sigma(\sigma^{-1}(x)\sigma^{-1}(y)), \quad \forall\, x, y \in G.$$

因为 σ 是单射，所以 $\sigma^{-1}(xy) = \sigma^{-1}(x)\sigma^{-1}(y)$，$\sigma^{-1} \in \mathrm{Aut}(G)$. 于是 $\mathrm{Aut}(G) \leqslant S(G)$. □

几何图形对称性的研究是 19 世纪和 20 世纪初的一个庞大课题，在此我们仅举一个例子.

在上册 §3.3 例 6 中，我们讨论过平面绕某个点 O 的旋转，使得中心在 O 点的正 n 边形 P_n 变到自身. 这些旋转的集合关于变换的合成构成一个 n 阶循环群 $C_n = \{\rho_0, \rho_1, \cdots, \rho_{n-1}\}$，其中 ρ_i 是将平面沿逆时针方向旋转 $\frac{2i}{n}\pi$ 的平面变换. 但是使得 P_n 变到自身的平面变换不止旋转，见下述例 3.

例 3 建立平面直角坐标系 O-xy，给定一个以 O 点为中心的正 n 边形 P_n，其顶点按照逆时针方向依次记为 $A_0, A_1, \cdots, A_{n-1}$，$A_0$ 落在 x 轴的正方向上，P_n 的对称轴按逆时针方向依次记为 $l_0, l_1, \cdots, l_{n-1}$，其中 l_0 为 x 轴. 考察集合

$$D_n = \{\rho_0, \rho_1, \cdots, \rho_{n-1}, \tau_0, \tau_1, \cdots, \tau_{n-1}\},$$

其中 ρ_i 是绕 O 点沿逆时针方向旋转 $\frac{2i}{n}\pi$ 的平面变换，τ_i 是平面沿直线 l_i 的翻折，叫作一个 **反射** (reflection). 当 $n = 3, 4$ 时，见图 1-1. 我们来证明 D_n 关于变换的合成构成一个群.

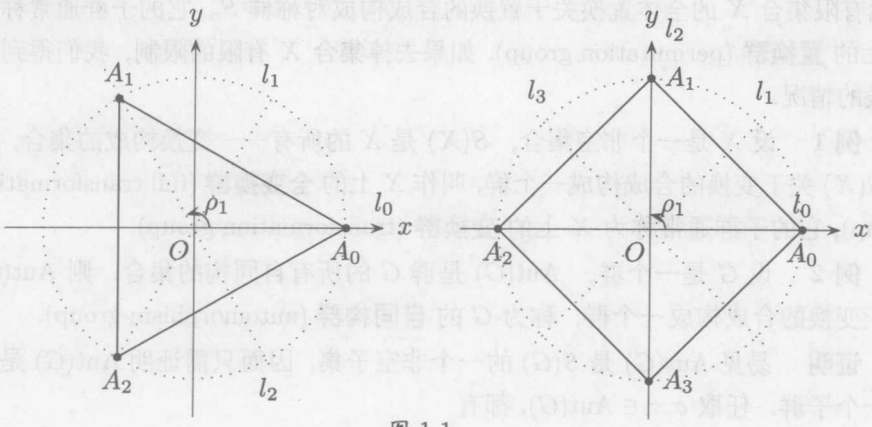


图 1-1

首先指出，D_n 中任意两个变换的合成仍然落在 D_n 中. 事实上，旋转和反射都取决于 A_0 的象. 旋转 ρ_i 把 A_0 变为 A_i，P_n 的顶点依然按照逆时针方向排列；反射 τ_i 仍然把 A_0 变为 A_i，P_n 的顶点改为顺时针方向排列. 我们有下述计算公式：

$$\rho_i = \rho_1^i, \quad \tau_i = \rho_i\tau_0 = \tau_0\rho_{n-i}, \quad 0 \leqslant i \leqslant n-1. \tag{1}$$

第 1 个公式显然. 因为 $\rho_i\tau_0(A_0) = A_i = \tau_0\rho_{n-i}(A_0)$，并且 $\rho_i\tau_0$ 和 $\tau_0\rho_{n-i}$ 均使 $A_0, A_1, \cdots, A_{n-1}$ 按顺时针排列，所以第 2 个公式成立.

对于任意的整数 k, $0 \leqslant i \leqslant n-1$, 约定 $\rho_{kn+i} = \rho_i$, $\tau_{kn+i} = \tau_i$. 应用公式 (1) 得到:

$$\rho_i\rho_j = \rho_1^i\rho_1^j = \rho_1^{i+j} = \rho_{i+j}; \qquad \rho_i\tau_j = \rho_i\rho_j\tau_0 = \rho_{i+j}\tau_0 = \tau_{i+j};$$
$$\tau_i\rho_j = \tau_0\rho_{n-i}\rho_j = \tau_0\rho_{j-i} = \tau_{i-j}; \quad \tau_i\tau_j = \rho_i\tau_0\tau_0\rho_{n-j} = \rho_{i-j}.$$

这就证明了 D_n 关于变换的合成是封闭的. 因为平面变换满足结合律, **G1** 成立. ρ_0 是平面的恒等变换, **G2** 成立. 最后, 因为 $\rho_i^{-1} = \rho_{n-i}$, $\tau_i^{-1} = \tau_i$, **G3** 成立, 所以 $(D_n, \cdot)$ 是一个群, 叫作 **二面体群** (dihedral group).

我们已经看到, 二面体群 D_n 中的平面变换保持正 n 边形 P_n 不变. 反过来, 保持 P_n 不变的变换是否只有这些呢? 答案是肯定的, 在这里就不做进一步的讨论了.

上册群的定义 3.3.1 中的条件 **G1**, **G2**, **G3** 不是独立的, 可以用更简单的条件替代. 下面我们给出群的一种公理化定义.

定义 1.1.1 设 G 是一个非空集合, 在 G 上定义一个二元运算

$$\cdot : G \times G \longrightarrow G, (x, y) \longmapsto x \cdot y,$$

通常把 $x \cdot y$ 简记作 xy. 如果运算满足下述条件:

G1. 结合律;

G2′. G 有一个左单位元 e, 即 $ex = x$, $\forall\, x \in G$;

G3′. G 的任意元素有左逆元, 即任取 $x \in G$, 存在 $y \in G$ 使得 $yx = e$,

那么 $(G, \cdot)$ 叫作一个群.

证明 上册定义 3.3.1 显然包含了定义 1.1.1 的所有条件, 现在来证明由定义 1.1.1 的三个条件可以推导出定义 3.3.1 的三个条件. 结合律是共有的, 我们来证明 **G1**, **G2′**, **G3′** 意味着 **G2**, **G3**.

(i) 一个左逆元也是一个右逆元, 即由 $yx = e$ 可以得到 $xy = e$. 事实上, 根据 **G3′**, 对于元素 y, 存在 $z \in G$, 使得 $zy = e$. 所以

$$xy = e(xy) = (zy)(xy) = z((yx)y) = z(ey) = zy = e.$$

(ii) 一个左单位元也是一个右单位元, 即对于任意 $x \in G$, 都有 $xe = x$. 事实上, 根据 (i), 存在 $y \in G$, 使得 $xy = e = yx$, 所以

$$xe = x(yx) = (xy)x = ex = x. \qquad \square$$

类似地，我们可以把 **G2′** 和 **G3′** 分别换成关于右单位元和右逆元的存在性，得到群的另外一个等价定义，见本节习题第 2 题. 同时，还有其他的等价定义，见本节习题第 3, 4 题.

现代代数学中最经典、内容最丰富的领域，就建立在这组简单的公理之上，令人叹为观止.

群这一术语是由群论的创始人伽罗瓦 (E. Galois, 1811—1832) 引入的. 正如最基本的数学思想产生之前常常发生的那样，群论的思想在伽罗瓦之前已有流传. 拉格朗日就曾经证明过置换群的一些定理，尽管定理的形式是原始而朴素的. 伽罗瓦天才的工作在 1832 年他去世之后，并没有被数学家们理解和接受，直到 1870 年若尔当出版介绍伽罗瓦理论的著作《置换与代数方程》，才重新引起了人们的兴趣. 克莱因 (F. Klein, 德国数学家， 1849—1925) 在《19 世纪数学发展史讲义》中谈到，直到 19 世纪，群论才 “完全脱离了梦幻，代之以精细整理过的逻辑结构 ”. 现代代数学理论以群论为基础得以产生和发展.

习题一

1. 设 G 是一个群， $a \in G$. 集合 $C_G(a) = \{x \in G \mid xa = ax\}$ 称为元素 a 在 G 中的 **中心化子** (centralizer). 证明 $C_G(a)$ 是 G 的一个子群.

2. 证明可以利用 **G1**, 以及下面的条件 **G2″**, **G3″** 来作群的定义：

G2″. G 有一个右单位元 e, 即 $\forall\, x \in G, xe = x$;

G3″. G 的任意元素 x 有右逆元 y, 即 $xy = e$.

3. 设 G 是一个具有结合的二元运算的集合. 如果任取 $a, b \in G$, 方程 $ax = b$ 和 $ya = b$ 在 G 里都有解，证明 G 关于该二元运算构成一个群.

4. 设 G 是一个具有结合的二元运算的有限集合. 如果消去律成立，那么证明 G 关于该二元运算构成一个群.

5. 有限群 G 的一个非空子集 H 是 G 的子群，当且仅当 H 对于 G 的运算封闭.

6*. 计算有理数加群 $(\mathbb{Q}, +)$ 的全自同构群.

§1.2 有限生成子群

我们知道群 G 的非空子集 S 一般不是 G 的子群，本节先讨论如何构造包含 S 的最小子群，然后介绍循环群的子群的结构以及群元素阶的计算.

设 G 是一个群，S 是 G 的一个非空子集. 记

$$\langle S\rangle = \{a_1^{\varepsilon_1}a_2^{\varepsilon_2}\cdots a_s^{\varepsilon_s} \mid a_1, a_2, \cdots, a_s \in S, \varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s = \pm 1, s \in \mathbb{Z}^+\},$$

其中 $a_1, a_2, \cdots, a_s$ 一般会有重复. 显然 $\langle S\rangle$ 是 G 的一个子群，称为 G 的 **由 S 生成的子群** (subgroup generated by S). 特别地，如果 $G = \langle S\rangle$，那么称群 G 是由 S 生成的，S 叫作 G 的一个 **生成元集** (generator set). 如果 $S = \{a_1, a_2, \cdots, a_n\}$ 是一个有限集，那么就称 G 是 **有限生成的** (finitely generated)，记作 $G = \langle a_1, a_2, \cdots, a_n\rangle$.

显然，由一个元素生成的群就是循环群. 二面体群 D_n 是由两个元素 ρ_1 和 τ_0 生成的，即 $D_n = \langle \rho_1, \tau_0\rangle$.

命题 1.2.1 *设 S 是群 G 的一个非空子集，那么 $\langle S\rangle = \bigcap\limits_{S\subseteq H\leqslant G} H$. 因而 $\langle S\rangle$ 是 G 中包含 S 的最小子群.*

证明 如果 $S \subseteq H \leqslant G$，那么 H 关于 G 的乘法封闭保证了 $\langle S\rangle \subseteq H$，所以 $\langle S\rangle \subseteq \bigcap\limits_{S\subseteq H\leqslant G} H$. 因为 $S \subseteq \langle S\rangle \leqslant G$，所以 $\langle S\rangle \supseteq \bigcap\limits_{S\subseteq H\leqslant G} H$. 从而等号成立. □

我们知道循环群是最简单的有限生成群，下面研究循环群的子群.

定理 1.2.2 *循环群的子群仍然是循环群.*

证明 设 $G = \langle a\rangle$，H 是 G 的非平凡子群. 那么存在整数 $k \neq 0$，使得 $a^k \in H$. 如果 $k < 0$，那么 $a^{-k} \in H$，并且 $-k > 0$. 从而我们可以定义 $\mathbb{Z}^+$ 的非空子集

$$S = \{k \in \mathbb{Z}^+ \mid a^k \in H\}.$$

根据最小数原理，S 有最小数 m. 我们断言，$H = \langle a^m\rangle$. 事实上，任取 $a^l \in H$，根据整数的带余除法，我们有

$$l = mq + r, \quad 0 \leqslant r < m.$$

于是 $a^r = a^{l-mq} = a^l(a^m)^{-q} \in H$. 根据 m 的取法，$r = 0$，即 $a^l = a^{mq}$，所以 $H = \langle a^m\rangle$. □

根据定理 1.2.2，循环群 $\langle a\rangle$ 的任意子群形如 $\langle a^m\rangle$，其中 m 是正整数. 当 a 的阶 $o(a) = \infty$ 时，$\langle a^m\rangle$，$m \in \mathbb{Z}^+$，是 $\langle a\rangle$ 的所有不同的非平凡子群. 事实上，

如果 $\langle a^r\rangle = \langle a^m\rangle$, $r \in \mathbb{Z}^+$, 那么 $a^m \in \langle a^r\rangle$. 于是存在 $s \in \mathbb{Z}$, 使得 $a^m = a^{rs}$. 因为 $o(a) = \infty$, 所以 $m = rs$, 从而 $r \mid m$. 同理, $m \mid r$. 于是 $m = r$. 下面考虑 $o(a)$ 是有限的情况.

引理 1.2.3 设 G 是一个群, 元素 a 的阶为 n, $m \in \mathbb{Z}^+$. 记 $(n,m) = d$. 则

(i) $o(a^m) = \dfrac{n}{d}$;

(ii) $\langle a^m\rangle = \langle a^d\rangle$.

证明 记 $n = n_1 d, m = m_1 d$, 则 $(n_1, m_1) = 1$.

(i) 设 $o(a^m) = s$. 那么 $(a^m)^s = e$, 根据上册命题 3.4.6 (ii), $n \mid ms$, 从而 $n_1 \mid m_1 s$, $n_1 \mid s$. 另一方面, $(a^m)^{n_1} = (a^n)^{m_1} = e$, 所以 $s \mid n_1$. 于是 $s = n_1$.

(ii) 因为 $a^m = (a^d)^{m_1} \in \langle a^d\rangle$, 所以 $\langle a^m\rangle \subseteq \langle a^d\rangle$. 另一方面, 存在 $u, v \in \mathbb{Z}$, 使得 $nu + mv = d$, 所以

$$a^d = a^{nu+mv} = (a^n)^u (a^m)^v = (a^m)^v \in \langle a^m\rangle,$$

于是 $\langle a^d\rangle \subseteq \langle a^m\rangle$. 从而 $\langle a^d\rangle = \langle a^m\rangle$. □

这就表明, 当 $G = \langle a\rangle$ 是一个 n 阶循环群时, $\langle a^d\rangle$, 其中 $d \mid n, d \in \mathbb{Z}^+$, 是 G 的所有不同的子群.

例 求 $\mathbb{Z}_{12}$ 的全部子群.

解 因为 $\mathbb{Z}_{12}$ 是 12 阶循环群, 12 的正因子为 $1, 2, 3, 4, 6, 12$, 所以 $\mathbb{Z}_{12}$ 的所有子群为:

$$\langle [1]\rangle = \mathbb{Z}_{12},\ \langle [2]\rangle = \{[0],[2],[4],[6],[8],[10]\},\ \langle [3]\rangle = \{[0],[3],[6],[9]\},$$

$$\langle [4]\rangle = \{[0],[4],[8]\},\ \langle [6]\rangle = \{[0],[6]\},\ \langle [0]\rangle = \{[0]\}.$$ □

在本节的最后, 我们介绍两个经常用到的关于元素阶的性质.

命题 1.2.4 设 G 是一个群, $a, b \in G, o(a) = n, o(b) = m$. 如果 $ab = ba$ 并且 $(m,n) = 1$, 那么 $o(ab) = mn$.

证明 设 $o(ab) = r$. 那么 $(ab)^r = e$. 由 $ab = ba$, 得到 $a^r = b^{-r}$, $o(a^r) = o(b^r)$. 根据引理 1.2.3 (i), $\dfrac{n}{(n,r)} = \dfrac{m}{(m,r)}$, 即 $n(m,r) = m(n,r)$. 因为 $(m,n) = 1$, 所以 $n \mid r, m \mid r$, $mn \mid r$. 另一方面, $(ab)^{mn} = e$, $r \mid mn$. 于是 $r = mn$. □

命题 1.2.5 设 G 是一个有限交换群, m 是 G 的元素阶的最大值. 那么 m 可以被 G 的每一个元素的阶整除.

证明 设 $a \in G, o(a) = m$. 如果存在元素 b, $o(b) = n$, 但 $n \nmid m$, 那么存在素数 p 以及非负整数 $i < j$, 使得

$$m = p^i m_1,\ p \nmid m_1; \quad n = p^j n_1,\ p \nmid n_1.$$

根据引理 1.2.3 (i), $o(a^{p^i}) = m_1, o(b^{n_1}) = p^j$. 根据命题 1.2.4, $o(a^{p^i} b^{n_1}) = m_1 p^j > m$, 与 m 的选取矛盾. □

习题二

1. 求 $\mathbb{Z}_{18}$ 的所有子群.

2. 设 p 是素数, n 是正整数, 试确定 p^n 阶循环群 $G = \langle a \rangle$ 的全部子群.

3. 设 G 是一个群, $a, b \in G, o(a) = n, o(b) = m$. 如果 $ab = ba$ 并且 $\langle a \rangle \cap \langle b \rangle = \{e\}$, 那么 $o(ab) = [m, n]$, 其中 $[m, n]$ 是 m, n 的最小公倍数.

4. 任取 $\pi \in S_n$, π 可以分解为互不相交的循环的乘积: $\pi = \pi_1 \pi_2 \cdots \pi_s$. 如果每个 π_i 都是 k_i- 循环, 那么 $o(\pi) = [k_1, k_2, \cdots, k_s]$.

5. 设群 G 的元素 g 的阶 $o(g) = mn$, 其中 $(m, n) = 1$. 证明存在 $a, b \in G$, 使得 $g = ab$, 并且 $o(a) = m, o(b) = n$.

6. 在偶数阶群 G 中, 方程 $x^2 = e$ 有偶数个解.

7. 有理数的加法群 $(\mathbb{Q}, +)$ 是不是有限生成的? 非零有理数的乘法群 $(\mathbb{Q}^*, \cdot)$ 是不是有限生成的? 说明理由.

8. 设 G 是一个群, $\sigma : G \longrightarrow G$, $a \longmapsto a^{-1}$. 证明 σ 是群 G 的自同构, 当且仅当 G 是阿贝尔群.

9. 设 $n \geqslant 3$. 在 S_n 中找一个与 D_n 同构的子群. 特别地, $D_3 \simeq S_3$.

10. 设 $G = \langle a, b \rangle$, 其中 $o(a) = n \geqslant 3, o(b) = 2$, 且 $bab = a^{n-1}$. 证明 $G \simeq D_n$.

§1.3 子群的陪集

我们在本节中研究一个群由其子群确定的划分. 先从一个熟悉的例子谈起.

给定一个正整数 n, 回忆上册 §3.1 例 2, 整数模 n 的同余关系定义为:

$$a \equiv b \pmod{n} \Longleftrightarrow n \mid (a-b),\ \forall\, a, b \in \mathbb{Z}.$$

"$\equiv$" 是整数集合 $\mathbb{Z}$ 上的一个等价关系, 它把 $\mathbb{Z}$ 划分成 n 个子集的不交并:

$$\mathbb{Z} = [0] \dot{\cup} [1] \dot{\cup} \cdots \dot{\cup} [n-1].$$

现在将集合 $\mathbb{Z}$ 换成整数加群 $(\mathbb{Z}, +)$ 来观察这个问题. 令 $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, 则 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个子群, 于是

$$a \equiv b \pmod{n} \Longleftrightarrow a - b \in n\mathbb{Z}.$$

引入一个符号 $i + n\mathbb{Z} = \{i + nk \mid k \in \mathbb{Z}\}$, 显然有 $[i] = i + n\mathbb{Z}$. 于是上述不交并可以写成:

$$\mathbb{Z} = n\mathbb{Z} \dot{\cup} (1 + n\mathbb{Z}) \dot{\cup} \cdots \dot{\cup} (n - 1 + n\mathbb{Z}). \tag{1}$$

在一般的情况下, 设 G 是一个群, H 是 G 的子群. 规定 G 的一个关系 $\sim$:

$$a \sim b \Longleftrightarrow a^{-1}b \in H, \quad \forall\, a, b \in G. \tag{2}$$

易见 $\sim$ 是一个等价关系. 事实上, 任取 $a, b, c \in G$, 因为 $a^{-1}a = e \in H$, 所以 $a \sim a$; 如果 $a \sim b$, 即 $a^{-1}b \in H$, 那么 $b^{-1}a = (a^{-1}b)^{-1} \in H$, 即 $b \sim a$; 如果 $a \sim b$, $b \sim c$, 即 $a^{-1}b \in H$, $b^{-1}c \in H$, 那么 $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$, 即 $a \sim c$.

设 H 是群 G 的一个子群. 称集合

$$aH = \{ah \mid h \in H\}$$

为群 G 关于子群 H 的一个 **左陪集** (left coset), a 叫作 aH 的一个 **代表元**. 我们来证明 G 可以分解为若干个左陪集的不交并.

定理 1.3.1 *设 G 是一个群, H 是 G 的一个子群. 那么任取 $a \in G$, 由 (2) 式定义的等价关系 $\sim$ 确定的包含 a 的等价类是左陪集 aH.*

证明 任取 $b \in aH$, 存在 $h \in H$, 使得 $b = ah$, 于是 $a^{-1}b = h \in H$, 即 $a \sim b$. 反之, 如果 $b \sim a$, 那么 $a^{-1}b = h \in H$, $b = ah \in aH$. □

设 I 是子群 H 在群 G 中的左陪集的代表元集，那么

$$G=\dot{\bigcup_{a\in I}}aH$$

给出了 G 的一个划分.

例 1 设 $G=S_3$, $H=\{(1),\ (12)\}$. 那么

$$(1)H=\{(1),\ (12)\}=(12)H;$$

$$(13)H=\{(13),\ (123)\}=(123)H;$$

$$(23)H=\{(23),\ (132)\}=(132)H;$$

$$S_3=(1)H\,\dot{\cup}\,(13)H\,\dot{\cup}\,(23)H.$$

我们看到，左陪集代表元的选择不是唯一的. 事实上，左陪集中的任意一个元素都可以作为这个左陪集的代表元.

类似地，我们还可以利用子群 H 定义群 G 的另一个等价关系 $\sim'$:

$$a\sim' b\Longleftrightarrow ab^{-1}\in H,$$

见本节习题第 1 题.

称集合 $Ha=\{ha\mid h\in H\}$ 为群 G 关于子群 H 的一个 **右陪集** (right coset), a 叫作 Ha 的一个代表元. 与左陪集的情况类似可证由等价关系 $\sim'$ 确定的含有 a 的等价类是右陪集 Ha.

例 2 设 $G=S_3$, $H=\{(1),\ (12)\}$. 那么 H 的右陪集是

$$H(1)=\{(1),\ (12)\}=H(12);$$

$$H(13)=\{(13),\ (132)\}=H(132);$$

$$H(23)=\{(23),\ (123)\}=H(123);$$

并且

$$S_3=H(1)\,\dot{\cup}\,H(13)\,\dot{\cup}\,H(23).$$

显然，S_3 关于 H 的左、右陪集的分解是不同的. 等价关系 $\sim$ 与 $\sim'$ 也不相同，$a^{-1}b\in H$ 并不意味着 $ba^{-1}\in H$, 因为 G 的运算不一定交换. 整数加群 $\mathbb{Z}$ 关于子群 $n\mathbb{Z}$ 的左、右陪集是一致的，因为整数加群是交换的.