中国科学院研究生院教材
Textbooks of Graduate University of Chinese Academy of Sciences

代数学基础与有限域

林东岱 编著

Introduction to Algebra and Finite Fields

高等教育出版社
Higher Education Press

中国科学院研究生院教材
Textbooks of Graduate University of Chinese Academy of Sciences

代数学基础与有限域

林东岱 编著

Introduction to Algebra and Finite Fields

高等教育出版社
Higher Education Press

内容摘要

本书系统介绍了有限域的基本内容和基本知识。全书共分为七章，第一章介绍代数学的基础知识，第二章介绍有限域的结构，第三章介绍有限域上的多项式，第四章介绍有限域上的离散对数问题，第五章介绍有限域上的椭圆曲线，第六章介绍伪随机序列，第七章介绍有限域在编码学和密码学等方面的应用。每章的后面均附有习题，有些习题是对正文内容的补充，以供学生复习巩固书中所学内容。

本书可作为数学、信息科学或其他相关专业的研究生教材，也可作为相关领域中的教学、科研人员以及工程技术人员的参考书。

图书在版编目 (CIP) 数据

代数学基础与有限域 / 林东岱编著. —北京:高等教育出版社, 2006.7

ISBN 7-04-019230-6

Ⅰ.代… Ⅱ.林… Ⅲ.①代数－研究生－教材 ②有限域－研究生－教材 Ⅳ.O15

中国版本图书馆 CIP 数据核字 (2006) 第 060132 号

策划编辑	郭 伟	**责任编辑**	郭 伟	**封面设计**	王凌波
版式设计	范晓红	**责任校对**	刘 莉	**责任印制**	朱学忠

出版发行	高等教育出版社	**购书热线**	010－58581118
社　　址	北京市西城区德外大街 4 号	**免费咨询**	800－810－0598
邮政编码	100011	**网　　址**	http://www.hep.edu.cn
总　　机	010－58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	北京新丰印刷厂	**畅想教育**	http://www.widedu.com
开　　本	787×1092　1/16	**版　　次**	2006 年 7 月第 1 版
印　　张	12.5	**印　　次**	2006 年 7 月第 1 次印刷
字　　数	240 000	**定　　价**	26.70 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　19230-00

郑重声明

总 序

在中国科学院研究生院和高等教育出版社的共同努力下，凝聚着中国科学院新老科学家、研究生导师们多年心血和汗水的中国科学院研究生院教材面世了。这套教材的出版，将对丰富我院研究生教育资源、提高研究生教育质量、培养更多高素质的科技人才起到积极的推动作用。

作为科技国家队，中国科学院肩负着面向国家战略需求，面向世界科学前沿，为国家作出基础性、战略性和前瞻性的重大科技创新贡献和培养高级科技人才的使命。中国科学院研究生教育是我国高等教育的重要组成部分，在新的历史时期，中国科学院研究生教育不仅要为我院知识创新工程提供人力资源保障，还担负着落实科教兴国战略和人才强国战略，为创新型国家建设培养一大批高素质人才的重要使命。

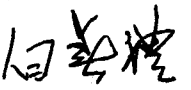
集成中国科学院的教学资源、科技资源和智力资源，中国科学院研究生院坚持教育与科研紧密结合的“两段式”培养模式，在突出科学教育和创新能力培养的同时，重视全面素质教育，倡导文理交融、理工结合，培养的研究生具有宽厚扎实的基础知识、敏锐的科学探索意识、活跃的思维和唯实、求真、协力、创新的良好素质。

研究生教材建设是研究生教育中重要的基础性工作。由一批活跃在科学前沿，同时又具有丰富教学经验的科学家编写的中国科

学院研究生院教材，适合在校研究生学习使用，也可作为高校教师和专业研究人员的参考书。这套研究生教材内容力求科学性、系统性、基础性和前沿性的统一，使学习者不仅能获得比较系统的科学基础知识，也能体会蕴于其中的科学精神、科学思想、科学方法，为进入科学研究的学术殿堂奠定良好的基础；优秀教材不但是体现教学内容和教学方法的知识载体、开展教学的基本条件和手段，也是深化教学改革、提高教育质量、促进科学教育与人文教育结合的重要保证。

“十年树木，百年树人”。我相信，经过若干年的努力，中国科学院研究生院一定能建设起多学科、多类型、多品种、多层次配套的研究生教材体系，为我国研究生教育百花园增添一枝新的奇葩，为我国高级科技人才的培养作出新的贡献。

中国科学院 常务副院长
中国科学院研究生院 院长
中国科学院 院士



二〇〇六年二月二十八日

前言

有理数域、实数域和复数域都是我们比较熟悉的数域，这些域有个共同的特点，就是它们的元素个数都是无限的。我们这本书要向大家介绍的有限域，则只含有限多个元素。有限域是现代代数学的重要分支之一。有限域的理论最早可追溯到费尔马（FERMAT 1601—1665）、欧拉（EULER 1707—1783）和高斯（GAUSS 1777—1855），他们实质研究了一种称之为有限素域的有限域。有限域的一般理论则主要是从伽罗华（GALOIS 1811—1832）的工作开始。1830 年，他在 p 元有限域的基础上，采用域扩张方法构造出全部可能的有限域，证明了每个有限域的元素个数一定是某个素数的幂，而且对每个素数幂，本质上也只有一个相应的有限域。正因为如此，我们有时也把有限域称做伽罗华域。

有限域作为域，当然具有通常域的一般性质，但又因为它只含有有限多个元素，使得它与我们所熟悉的数域又有很大的不同。有限域具有许多优美的特性，在组合设计、编码理论、密码学、计算机代数和通信系统等许多实际领域有着广泛的应用。特别是最近几十年，随着计算机技术的蓬勃发展，有限域的地位愈加重要，例如有限域的计算和算法分析对计算机代数和符号计算的影响，许多从事应用研究的数学家，开始重视有限域理论的研究和应用，有限域已经成为许多工程技术人员不可缺少的数学工具。另一方面，有限域理论本身也吸引了人们的广泛兴趣，成为许多优秀数学家施展自己才华的场所。数学本身和实际应用领域也不断提出关于有限域的大量数学问题，这些问题的解决或者有益于应用，或者推动数学的发展。

本教材是为中国科学院研究生院硕士研究生讲授第二学期课程 —— 代数学基础与有限域而编写的讲义。鉴于近年来对有限域知识的需求，本人从 2003 年起，连续四年在中国科学院研究生院开设该课程。作为数学、计算机和信息科学相关专业硕士研究生的专业基础课，其基本目的是使学生掌握有限域的基本知识和基本定理。由于在教学过程中没有找到合适的中文教材，特参考一些有限域方面的英文著作、文章以及国内相关方面的著作和教材编写了这本讲义。在编写过程中，我们力求做到叙述简洁易懂，推理尽可能详尽，内容尽可能封闭，对所引用的理论，凡需要介绍的都有交代，除了对一些补充或用以提高的内容指定了参考文献外，尽量避免要求读者查看其他参考

书籍，以减少读者阅读困难。

本书共分为七章：第一章主要介绍代数学的基础知识。代数学的内容非常丰富，在这里不可能做到面面俱到。这一章可以看作是本书的预备知识，为后面介绍有限域及相关内容引入必要的概念和代数学知识，因此内容力求简洁，只对后面要用到的内容加以介绍。第二章和第三章可以说是本教材的主体，分别介绍了有限域的结构、特征性质以及有限域上的多项式等内容。考虑到有些读者可能是数学和信息科学领域从事符号计算和算法设计方面研究工作的学生，在这章我们还增加了一些有关有限域上因式分解问题的内容。第四章主要介绍了有限域上的离散对数问题。这部分内容主要面向从事信息安全和算法设计工作的读者。有限域上的离散对数问题是少有的几个密码可信问题之一，在密码算法和安全协议的设计等方面有着广泛的应用。这章内容在简要概述了离散对数问题及其在密码学中的应用之后，介绍了几种常见的求解离散对数问题的算法。第五章简单介绍了有限域上的椭圆曲线。目前人们普遍认为有限域上椭圆曲线中的离散对数问题比有限域上的离散对数问题更难，加之椭圆曲线密码系统的密钥更短、实现更为简单，人们对椭圆曲线密码学的关注愈来愈大。本章的目的是让读者了解什么是椭圆曲线以及有限域上椭圆曲线的一些基本概念、群结构，简单介绍椭圆曲线上的离散对数问题及其在密码学中的应用，希望通过这章的内容，使学生能够对有限域上的椭圆曲线有个初步了解，为进一步学习、从事相关问题研究打下一定的基础。第六章介绍了伪随机序列。有限域上的伪随机序列是一类具有广泛用途的序列，在信息加密、扰动、编码、雷达定位和测距等方面有着重要的应用。这一章，我们在介绍了线性移位寄存器序列和 Berlekamp-Massey 序列综合算法之后，还进一步介绍了二维的线性递归 m- 阵列；第七章介绍了有限域在编码学和密码学中的一些应用，希望能够通过这些应用，让读者对有限域中各种优美性质的使用有个初步的体验。

本教材的编写参考了许多相关方面的专著、文章和教材，在此向这些参考文献的作者表示衷心的感谢，可以说本人只是站在这些作者的肩膀上，做了一点归纳整理工作。另外在本书的编写过程中，中国科学院数学与系统科学研究院刘木兰研究员、清华大学应用数学系冯克勤教授、中国科学院软件研究所冯登国研究员为本书的组织和写作提出了许多宝贵建议，还有中国科学院软件研究所博士生孙海波、周素静、邓焱等也为书稿的校对做了许多工作，作者在此一并致以诚挚的谢意。同时本人还要感谢中国科学院研究生院给了这本讲义出版的机会，感谢高等教育出版社的编辑郭思旭、张小萍、郭伟等同志为本书的出版付出了辛勤劳动。由于本人水平有限，对一些问题的理解和叙述或有肤浅之处。对于讲义中的错误和不足之处，诚挚欢迎大家提出宝贵意见。

编　者

2006 年 4 月

目 录

第一章　代数学基础

代数学的主要研究对象是各种各样的代数结构, 即具有一些代数运算的集合. 本章我们主要介绍代数学中的一些基本概念和基本知识. 第一节和第二节主要介绍群、环与理想的基本概念和基本定理, 第三节主要介绍域上多项式环的一些基本性质, 第四节介绍域和扩域. 这章的内容可以看成是本书的预备知识, 主要是为了帮助读者阅读和理解后面将要介绍的有限域及其相关内容.

1.1 群

群是代数学中的基本概念, 它是一种只含有单个运算的代数结构, 它的运算法则与数的运算法则类似, 在自然科学的许多领域都有着广泛的应用. 在这一节, 我们主要介绍群的一些基本概念和基本性质.

设 S 是一非空集合, 我们把 $S \times S \to S$ 的一个映射 $\circ$ 称为 S 上的 (二元) 运算. 对于 S 上的一个二元运算 $\circ$, 为了方便起见, 我们也把 $a, b \in S$ 的像 $\circ(a, b)$ 记做 $a \circ b$, 或省略 $\circ$, 只简单地写作 ab.

定义 1.1.1 我们说一个非空集合 G 对于 G 上的一个二元运算 $\circ$ 来说作成一个群, 如果:

1) $\circ$ 是结合的, 即对任何 $a, b, c \in G, a \circ (b \circ c) = (a \circ b) \circ c$.
2) G 中存在一个元素 e 满足:$\forall a \in G, a \circ e = e \circ a = a$. 这个元素称为 G 中的单位元. 有时我们也把单位元 e 写成 1_G 或 1.
3) $\forall a \in G$, 存在一个元素 $a^{-1} \in G$ 满足 $a \circ a^{-1} = a^{-1} \circ a = e$, 这个元素称为 a 的逆元.

   如果 G 中的元素还满足

4) $\forall a, b \in G$, $a \circ b = b \circ a$, 则 G 称为交换群或 Abel 群. 这时也把 $\circ$ 表示成 $+$, 同时把单位元 e 写成 0. 因此交换群也称为加法群.

容易证明在一个群中, 单位元和元素的逆元是唯一的, 而且对 $\forall a, b \in G, (a \circ b)^{-1} = b^{-1} \circ a^{-1}$. 我们约定:

$a^0 = e$,

$a^n = \underbrace{a \circ a \circ \cdots \circ a}_{(n\text{个})}$ 或 $na = \underbrace{a + a + \cdots + a}_{(n\text{个})}$,

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

显然有:

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

$(a^n)^m = a^{mn}$.

例 1.1.1 所有整数的集合 $\mathbf{Z}$ 在加法运算下构成一个交换群.

例 1.1.2 只含有一个元素 e 的集合在运算 $e \circ e = e$ 下构成一个群.

例 1.1.3 令 $G = \{0, 1, 2, \cdots, 5\}$, 则 G 在运算"$a \circ b = a + b$ 除 6 后的余数"下 G 构成一个群.

例 1.1.4 元素在数域 K 中的全体 n 阶可逆矩阵对于矩阵的乘法构成一个群, 这个群记为 $GL_n(K)$, 称为 n 级一般线性群; $GL_n(K)$ 中全体行列式为 1 的矩阵对于矩阵乘法也构成一个群, 这个群记为 $SL_n(K)$, 称为特殊线性群. 显然, 一般线性群和特殊线性群都不是交换群.

例 1.1.5 集合 $\{1, 2, \cdots, n\}$ 上的所有置换在置换的复合运算下构成一个非交换群, 这个群称为对称群.

定义 1.1.2 一个群 G 称作有限群 (无限群), 如果 G 中含有有限多个元素 (无限多个元素). 有限群中元素的个数称为 G 的阶, 用 $|G|$ 表示.

定义 1.1.3 设 G 是群, a 是 G 中的一个元素. 如果存在正整数 m, 使得 $a^m = 1$, 我们则称 a 是**有限阶的元素**, 而把最小的满足 $a^m = 1$ 的正整数 m 叫做元素 a 的**阶**, 用 $o(a)$ 或 $|a|$ 表示. 否则称 a 是无限阶的元素.

定理 1.1.1 设 a 是群 G 中的一个有限阶元素, $o(a) = m$. 则对任意的正整数 n, $a^n = 1$ 当且仅当 $m|n$.

证明 充分性: 假设 $m|n$, 则存在 t 使 $n = mt$, 所以 $a^n = a^{mt} = (a^m)^t = 1^t = 1$.

必要性: 假设 $a^n = 1$, $n = qm + r$, 其中 q 和 r 都是非负整数, $0 \leqslant r < m$. 那么

$$1 = a^n = a^{qm+r} = a^{qm} a^r = (a^m)^q a^r = 1 \cdot a^r = a^r.$$

但由于 $0\leqslant r<m$, 根据元素阶的定义, m 是使 $a^m=1$ 成立的最小的正整数, 因此 $r=0$, 所以 $n=qm$, 即 $m|n$. □

定理 1.1.2 *设 a 是群 G 中的一个有限阶元素, $o(a)=m$. 则对任意的正整数 k, a^k 的阶为 $\frac{m}{(k,m)}$, 其中 (k,m) 表示 k 和 m 的最大公因子.*

证明 假设 $d=(k,m)$, $o(a^k)=n$, 则 $(\frac{m}{d},\frac{k}{d})=1$, $a^{kn}=(a^k)^n=1$. 根据定理 1.1.1, $m\mid kn$, 所以 $\frac{m}{d}\mid(\frac{k}{d}\cdot n)$, 从而 $\frac{m}{d}\mid n$. 但显然 $(a^k)^{\frac{m}{d}}=1$, 再次根据定理 1.1.1 知 $n\mid\frac{m}{d}$. 因此 $n=\frac{m}{d}$. □

定理 1.1.3 *设 a,b 是群 G 中的两个元素, $ab=ba$. 如果 $(o(a),o(b))=1$, 那么*

$$o(ab)=o(a)o(b).$$

证明 因为

$$(ab)^{o(a)o(b)}=(a^{o(a)})^{o(b)}(b^{o(b)})^{o(a)}=1^{o(b)}\cdot 1^{o(a)})=1,$$

所以

$$o(ab)|o(a)o(b).$$

反过来, 因为 $(ab)^{o(ab)}=1$, 两边同取 $o(a)$ 次方, 我们有

$$1=(ab)^{o(ab)o(a)}=a^{o(ab)o(a)}b^{o(ab)o(a)}=b^{o(ab)o(a)},$$

所以 $o(b)|o(ab)o(a)$, 但 $(o(a),o(b))=1$, 因此 $o(b)|o(ab)$.

同理, $o(a)|o(ab)$. 再次利用 $(o(a),o(b))=1$, 我们得到

$$o(a)o(b)|o(ab).$$

综上所述, $o(ab)=o(a)o(b)$. 定理得证. □

定理 1.1.4 *设 G 是一有限交换群, n 是 G 中元素的最大阶. 则 G 中任意元素的阶一定能够整除 n.*

证明 设 $g\in G$ 是 G 中阶最大的元素, 其阶为 n. 假设 $f\in G$ 的阶为 m, 不整除 n, 则一定存在一个素数 p, 使得 p 在 m 中的幂次大于 p 在 n 中的幂次, 即存在正整数 s,t,m',n' 满足:$n=p^sn',m=p^tm',p\nmid n',p\nmid m'$, 且 $t>s$. 构造元素 $g'=g^{p^s}$, $f'=f^{m'}$, 则 g' 和 f' 的阶分别为 n' 和 p^t, 且 $(n',p^t)=1$, 从而 $g'f'$ 的阶为 $n'p^t>n$. 这与 n 是 G 中元素的最大阶相矛盾. 所以 G 中任何元素的阶一定能够整除 n. □

定义 1.1.4 (等价关系) *$R\subset S\times S$ 称为等价关系, 如果*

1) $(s,s)\in R$ (自反性);
2) $(s,t)\in R\Rightarrow(t,s)\in R$ (对称性);
3) $(s,t),(t,u)\in R\Rightarrow(s,u)\in R$ (传递性).

$(s,t) \in R$ 有时也写成 sRt.

定义 1.1.5 假设 n 是一个正整数. 对任何整数 a, b, 如果 $n \mid (a-b)$, 我们则称 a 和 b**模**n(或 $\bmod n$) **同余**, 记做 $a \equiv b \bmod n$. n 称为这个同余式的**模**.

显然模 n 的同余关系是整数集合 $\mathbf{Z}$ 上的一个等价关系, 并将 $\mathbf{Z}$ 分成了 n 个互不相交的等价类 $[0],[1],[2],\cdots,[n-1]$, 每个等价类都称为模 n 的剩余类.

例 1.1.6 $\{[0],[1],[2],\cdots,[n-1]\}$ 在运算 $[a]+[b]=[a+b]$ 下构成一个加法群, 称为模 n 的剩余类群, 记作 $\mathbf{Z}_n$.

定义 1.1.6 群 G 的一个子集 H 称为一个**子群**, 如果在 G 的运算下, H 构成一个群.

定理 1.1.5 设 G 是群, 对任何的 $a \in G$, 定义 $\langle a \rangle = \{a^i | i \in \mathbf{Z}\}$. 则 $\langle a \rangle$ 是子群. 且如果 $\langle a \rangle$ 是有限群, 则 $\langle a \rangle$ 的阶恰好等于 a 的阶.

定理 1.1.6 如果 H 是群 G 的一个子群, 则 G 上的关系 $R_H : (a,b) \in R_H \Leftrightarrow a = bh$(对某个 $h \in H$) 是一个等价关系.

证明 要证 R_H 是个等价关系, 我们只要验证它满足定义 1.1.4 中的三条性质即可.

1) $(a,a) \in R_H$, 因为单位元 $1 \in H$.
2) $(a,b) \in R_H \Rightarrow a = bh, h \in H \Rightarrow b = ah^{-1} \Rightarrow (b,a) \in R_H$.
3) $(a,b) \in R_H, (b,c) \in R_H \Rightarrow a = bh_1, b = ch_2 \Rightarrow a = ch_2h_1 = c(h_2h_1) \Rightarrow (a,c) \in R_H$.

□

上述关系称为模 H 的左同余, 同样有模 H 的右同余关系, 等价类 aH 或 Hb 称为左陪集 (left coset) 或右陪集 (right coset).

例 1.1.7 $G = \mathbf{Z}_{12}$, $H = \{[0],[3],[6],[9]\}$. 则 H 的陪集有:

$[0]+H = \{[0],[3],[6],[9]\}$,
$[1]+H = \{[1],[4],[7],[10]\}$,
$[2]+H = \{[2],[5],[8],[11]\}$.

定理 1.1.7 如果 H 是 G 的一个有限子群, 则 H 每一个 (左或右) 陪集都和 H 有同样多的元素.

定义 1.1.7 如果群 G 的子群 H 只构造出有限多个模 H 的陪集, 则这个陪集的个数称为 H 在 G 中的**指数**.

定理 1.1.8 (Lagrange) 一个有限群 G 的阶正好等于任何一个子群 H 的阶乘以 H 在 G 中的指数. 特别的, H 的阶整除群 G 的阶, 任一元素的阶整除 G 的阶.

证明 由于 G 是有限的, 所以 H 的陪集的个数 j 也是有限的. 由于每一个陪集都和 H 含有相同个数的元素, 且两个不同的陪集互不相交, 所以 $|G| = |H|j$. □

例 1.1.8 (欧拉 (Euler) 定理) *设 n 是一正整数, 考察由模 n 的等价类构成的集合 $G = \{[\alpha]|(\alpha, n) = 1\}$. 则 G 在模 n 的乘法运算下构成一有限群, 阶为 $|G| = \phi(n)$. 对任给 $a \in \mathbf{Z}$, $(a, n) = 1$, 则 $[a] \in G$, 所以 $[a]$ 的阶是 $|G|$ 的因子, 因此 $[a]^{\phi(n)} = 1$, 也就是 $a^{\phi(n)} \equiv 1(\mod n)$.*

在上述例子中, 如果取 n 为某个素数 p, 我们则得到**费尔马** (Fermat) **定理**: 设 p 是一素数, 则对任意 $a \neq 0$, $a^{p-1} \equiv 1(\mod p)$.

定义 1.1.8 *群 G 的一个子群 H 称为**正规子群**, 如果对任何 $a \in G, h \in H$, 有 $aha^{-1} \in H$. 如果 H 是 G 的正规子群, 我们记成 $H \lhd G$.*

显然交换群的任一子群都是正规子群.

定理 1.1.9 *设 H 是群 G 的子群, 则下列条件彼此等价:*

1) $H \lhd G$;
2) *对于每个* $g \in G$, $gHg^{-1} = H$;
3) H *的每个左陪集都是右陪集. 事实上, 对于每个* $g \in G$, $gH = Hg$.

证明

1) $\Rightarrow$ 2): 假设 H 是 G 的正规子群, g 是任一给定的 G 中的元素. 根据正规子群的定义, 易知 $gHg^{-1} \subset H$. 另外, $\forall h \in H$, 因为 $g^{-1} \in G$, 所以根据正规子群的定义, 我们也有 $(g^{-1})h(g^{-1})^{-1} \in H$, 所以存在 $h' \in H$ 使 $(g^{-1})h(g^{-1})^{-1} = h'$, 因此 $h = gh'g^{-1}$, $H \subset gHg^{-1}$. 从而 $H \subset gHg^{-1}$.

2) $\Rightarrow$ 3): 当 $gHg^{-1} = H$ 时, $gH = Hg$ 是显然的.

3) $\Rightarrow$ 1): 假设 H 的每个左陪集都是右陪集, 则对任何的 g, 存在 g' 使得 $gH = Hg'$. 由于 $1 \in H$, 因此有 $h' \in H$ 满足 $g = g \cdot 1 = h'g'$, 从而 $Hg = Hg' = gH$, 所以对任何 $h \in H$, 存在 $h'' \in H$ 使得 $gh = h''g$, 所以 $ghg^{-1} = h'' \in H$. 从而 H 是一个正规子群. □

定理 1.1.10 *如果群 G 的子群 H 是正规的, 则模 H 的陪集的集合在运算 $(aH) \cdot (bH) = (ab)H$ 下构成一个群.*

证明 关键是证明上述定义的运算是良定义的. 即如果 $a_1 \in aH, b_1 \in bH$, 则 $a_1b_1H = (ab)H$. 由 H 正规可知 $a_1 = ha, b_1 = bh'$, 所以 $a_1b_1 = h(ab)h' = (ab)h''h'$(因为 H 是正规的), 其中 $h, h', h'' \in H$. 所以 $a_1b_1H = abH$. □

定义 1.1.9 设 H 是 G 的正规子群, 定理 1.1.10 中由 H 的陪集定义的群称为 G 关于 H 的**商群**, 记作 G/H.

定理 1.1.11 如果 G 是有限群, 则 $|G/H| = |G|/|H|$.

证明 由定理 1.1.8 立得. □

定义 1.1.10 一个群 G 称为**循环群**, 如果存在一个元素 $a \in G$ 使得 $G = \langle a \rangle$. 这样的元素 a 称为 G 的**生成元**.

显然任何的循环群都是交换群 (习题 8). 例 1.1.1 是一个循环群, 生成元为 1. $\mathbf{Z}_n$ 也是一个循环群, 且 $\mathbf{Z}_n = \langle [1] \rangle$, 而且对任何一个与 n 互素的整数 t, $[t]$ 都是 $\mathbf{Z}_n$ 的生成元.

定理 1.1.12 任意循环群的子群仍是循环群.

证明 设 $G = \langle a \rangle$ 是一循环群, H 是 G 的一个子群. 不妨设 $H \neq \{1\}$. 因为 $a^n \in H \Rightarrow a^{-n} \in H$, 所以 a 的某一正次幂一定在 H 中. 设 d 是使得 $a^d \in H$ 的最小的正整数, 即 $d = \min\{n \in \mathbf{Z} | n > 0 且 a^n \in H\}$. 下面我们证 $H = \langle a^d \rangle$. 任给 $h \in H$, 存在 $s \in Z$ 使 $h = a^s$, 写 $s = qd + r, 0 \leqslant r < d$, 则有 $a^s = a^{qd} \cdot a^r \in H$, 从而 $a^r \in H$. 根据 d 的选取可知 $r = 0$, 所以 $H = \langle a^d \rangle$. □

定理 1.1.13 设 $G = \langle a \rangle$ 是一有限阶的循环群, 阶为 m. 那么

1) 如果 d 是 m 的一个因子, 则 G 包含且只包含一个指数为 d 的子群. 而且对 m 的任一因子 f, G 正好包含一个阶为 f 的子群.
2) 设 f 是 m 的因子, 则 G 中有 $\phi(f)$ 个阶为 f 的元素. 其中 $\phi(f)$ 是 Euler 函数, 即小于 f 且与 f 互素的正整数的个数.
3) G 正好有 $\phi(m)$ 个生成元, 且每一生成元都具有形式 a^r, 其中 $(r, m) = 1$.

证明

1) 假设 d 已给定, 则根据定理 1.1.2, $\langle a^d \rangle$ 是阶为 $\frac{m}{d}$ 的子群, 因此指数为 d. 假设 $\langle a^k \rangle$ 是另一个指数为 d 的子群, 则根据定理 1.1.8, $|\langle a^k \rangle| = \frac{m}{d}$. 但另一方面, $|\langle a^k \rangle| = \frac{m}{(m,k)}$. 所以 $d = (m, k)$, 因此有 $d \mid k$, $a^k \in \langle a^d \rangle$, $\langle a^k \rangle \subset \langle a^d \rangle$. 但由于 $\langle a^k \rangle$ 和 $\langle a^d \rangle$ 有相同的阶. 所以 $\langle a^k \rangle = \langle a^d \rangle$.

   注意到, 对 m 的任一因子 f, 阶为 f 的子群正好 (一定) 是指数为 $\frac{m}{f}$ 的子群, 容易证明 G 正好包含一个阶为 f 的子群.
2) 设 a^k 是 G 中的一个元素. 则 a^k 的阶是 $\frac{m}{(k,m)}$. 所以 a^k 的阶是 $f \Leftrightarrow m = f \cdot (k, m) \Leftrightarrow (k, m) = \frac{m}{f}$. 令 $k = h \cdot \frac{m}{f}$, 则 $(k, m) = \frac{m}{f} \Leftrightarrow (h, f) = 1$. 而 h 的个数正好是 $\phi(f)$.