研　究　生　数　学　丛　书

Mathematics Series for Graduate Students

数论、群论、有限域

Theory of Numbers, Groups and Finite Fields

周炜　著

清华大学出版社

研 究 生 数 学 丛 书

Mathematics Series for Graduate Students

数论、群论、有限域

Theory of Numbers, Groups and Finite Fields

周炜 著

清华大学出版社

北 京

内 容 简 介

本书系统地研究了基础数论、群论和有限域理论。全书分为11章：集合与函数，整除性理论，数论函数，不定方程，同余式，二次剩余，原根和离散对数，群论，环、域与多项式，有限域，有限域上的线性递归序列。

本书包含了作者多年来的教学经验和研究成果，许多结果是首次公开发表。全书内容丰富，体系完整，论证严谨，行文流畅，深入浅出，特色鲜明。本书可以作为密码学、数学、信息对抗、计算机科学与技术及相关专业研究生和本科生的教材，也可作为其他各专业、各层次的师生和工程技术人员的参考书或自学用书。

图书在版编目(CIP)数据

数论、群论、有限域/周炜著. --北京：清华大学出版社，2013
(研究生数学丛书)
ISBN 978-7-302-34455-1

Ⅰ. ①数…　Ⅱ. ①周…　Ⅲ. ①数论 ②群论 ③有限域　Ⅳ. ①O15

中国版本图书馆CIP数据核字(2013)第270038号

责任编辑：陈　明
封面设计：常雪影
责任校对：王淑云
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：18.75　　**字　　数**：411千字
版　　次：2013年11月第1版　　**印　　次**：2013年11月第1次印刷
印　　数：1～2500
定　　价：45.00元

产品编号：052528-01

前言

FOREWORD

数论是数学的一个重要分支，而群论和有限域理论是数学重要分支——近世代数学的重要组成部分。群论的研究往往要用到基础数论的结果，而有限域理论的研究更是离不开群论的一些重要结果。

数论、群论和有限域理论在组合学、密码学、编码学、理论物理、开关电路设计、信息安全和信息对抗等领域有着广泛的应用。随着数字化、网络化、信息化时代的到来和信息技术的进步，这些理论在信息安全和信息对抗领域的应用变得越发重要。因此，涉及数论、群论和有限域理论的知识学习和课题研究必然受到人们更多的重视。而在国内这方面现存的教科书较少，且内容往往过于专业和深奥，因而不能完全满足非专门从事这方面研究的各专业、各层次研究人员和工程技术人员的需要。这就要求有一批新颖的、特色鲜明的、深入浅出的、便于学习、掌握和应用的有关数论、群论和有限域理论的教科书面世。本书正是作者在这方面的努力。

本书内容分为 11 章：集合与函数，整除性理论，数论函数，不定方程，同余式，二次剩余，原根和离散对数，群论，环、域与多项式，有限域，有限域上的线性递归序列。每章又分为若干节和小节。这些章节有些内容比较浅显，有些内容难度适中，但也有些内容阅读起来有一定的困难，初学者可以暂时绕过，比如二元二次不定方程、Sylow 定理、Pólya 基本定理、有限域上多项式的因式分解、有限域上周期序列的线性复杂度等。每章后面配有一定数量难度不一的习题，可供选做。

本书可以作为密码学、数学、信息对抗、计算机科学与技术及相关专业研究生和本科生的教材，也可作为其他各专业、各层次师生和工程技术人员的参考书或自学用书，打 * 号的内容供选学。若作为教材，学时安排建议：研究生 48 学时，本科生 64 学时，同时根据实际情况和内容联系进行取舍。

本书部分内容已在空军工程大学防空反导学院计算机科学与技术专业博士生、硕士生和本科生中讲授多年。但由于作者水平有限，书中一定还有尚未发现的错误、缺点和纰漏，恳请广大读者批评指正，作者不胜感激！

作　者

2013 年 10 月

目录

CONTENTS

第1章 集合与函数

集合是现代数学的最基本概念之一，人们很难给出它的精确定义，平常只对它进行描述。集合论的创始人是 Cantor。函数和映射也是数学的最基本概念，本书将对函数和映射的概念不加区别。

本章详细介绍集合的基本概念和运算、函数和映射的一般性质、对合映射的不动点定理、置换的循环分解、集合上的偏序关系和等价关系等特殊二元关系，最后介绍容斥原理、鸽巢原理和多项式定理。

1.1 集合论基础

1. 集合的基本概念

简单地说，集合是具有某种共同性质的一类事物(对象)的全体。集合 A 中的每一个对象 a 称为该集合的一个元素，记作 $a\in A$(读作“a 属于 A”或“a 在 A 中”或“A 含有 a”)。如果一个对象 x 不是集合 A 的元素，则记作 $x\notin A$(读作“x 不属于 A”或“x 不在 A 中”或“A 不含有 x”)。

集合中的元素无重复、无顺序且像人的姓名那样可以无限制地反复使用而集合本身不发生任何变化。

一个集合不能是它自己的元素。以集合为元素的集合称为类或族。可以将“集合”和“族”当作量词使用，“一集合……”将意味着“由……组成的一个集合”，“一族……”意味着“由……组成的一个族”。

集合常用大写的英文字母表示，集合的元素常用小写的英文字母表示。如果一个集合中只有少数有限个元素，可将表示这些元素的符号全部罗列在一对花括号中，元素之间用逗号隔开，如 $A=\{1,2,3\}$，$B=\{1\}$。如果一个集合中有很多元素或无限多元素但通过少数元

素可以毫无歧义地推知其他元素，则将这些少数元素罗列在一对花括号中，而多数元素用英文的省略号表示，如 $B=\{1,3,5,\cdots,2009\}$ 表示不超过 2009 的所有正奇数，而所有奇平方数可用集合 $C=\{1^2,3^2,\cdots,(2n-1)^2,\cdots\}$ 表示，等等。如果一个集合中元素的共同特性是可以精确描述的，则该集合在花括号中的表示分两部分，两部分之间用一条竖线“|”隔开，竖线前面是对该集合元素的一般形式的描述，竖线后面是对该集合所有元素共同特性的精确描述，如 $D=\{x\mid x\in\mathbb{R}\wedge\neg(0\leqslant x<1\vee\sin x=0)\}$。这里$\neg$，$\wedge$，$\vee$ 三个符号分别表示逻辑词“非”(否定)、“与”(并且、但是)、“或”(或者)，今后我们可能还会用到四个符号：$\rightarrow$(逻辑词“蕴涵”)，$\forall$(逻辑词“对于所有的”、“对于任意的”、“对于每一个”)，$\exists$(逻辑词“存在”、“至少有一个”)，$\Rightarrow$(逻辑词“永真蕴涵”、“经过正确的逻辑推理推得”)。

如果集合 A 的所有元素都在集合 B 中，则称集合 A 是集合 B 的一个子集合(子集)，记作 $A\subseteq B$(读作“A 含于 B”)或 $B\supseteq A$(读作“B 包含 A”)。反之，集合 A 不是集合 B 的子集当且仅当集合 A 中至少有一个元素不在集合 B 中。显然，任何一个集合 A 都是它自己的子集，即 $A\subseteq A$。

如果 $A\subseteq B$，而集合 B 至少有一个元素 b 不在集合 A 中，则称集合 A 是集合 B 的一个真子集，记作 $A\subset B$(读作“A 真含于 B”)或 $B\supset A$(读作“B 真包含 A”)。

如果 $A\subseteq B$ 和 $B\subseteq A$ 同时成立，则称这两个集合相等，记作 $A=B$。

我们引入一个称为“空集”的概念，记作$\varnothing$。$\varnothing$没有任何元素，但与所有集合同等对待。对于任何集合或集合族 A，必须有$\varnothing\subseteq A$。否则按照$\subseteq$的定义将至少有一个 $x\in\varnothing$不在 A 中，与空集的定义矛盾。注意$\{\varnothing\}$是由单个空集$\varnothing$组成的集合族，而不是空集$\varnothing$本身，因为它有一个元素$\varnothing$。还应当注意不要将空集$\varnothing$写为希腊字母 ϕ 或 Φ。

若集合 $A\neq\varnothing$，即集合 A 中至少有一个元素，则称集合 A 非空。

我们将把全体实数的集合记作$\mathbb{R}$，全体有理数(能够表示为两个整数之商的实数称为有理数，即全体整数和分数)的集合记作$\mathbb{Q}$，全体整数的集合记作$\mathbb{Z}$，全体非负整数的集合记作$\mathbb{N}$(注意$0\in\mathbb{N}$)。鉴于有的教科书将 0 视为自然数，而又有的教科书不将 0 视为自然数，本书不采用“自然数”这个概念以避免歧义。当我们给字母$\mathbb{R}$，$\mathbb{Q}$，$\mathbb{Z}$加上“+”号或“$*$”号作为上标时，分别表示全体“正”的或者全体“非零”的实数、有理数、整数的集合。对于任意的 $m\in\mathbb{Z}^+$，我们还将使用记号 $Z_m=\{0,1,\cdots,m-1\}$和 $Z_m^*=\{1,2,\cdots,m-1\}(m\geqslant 2)$。

2. 集合的代数运算及性质

设 I 是一个指标集，一族集合$\{A_\alpha\}_{\alpha\in I}$的并、交运算分别定义如下：

$$\bigcup_{\alpha\in I}A_\alpha=\{x\mid\exists\alpha(\alpha\in I\wedge x\in A_\alpha)\},\ \bigcap_{\alpha\in I}A_\alpha=\{x\mid\forall\alpha(\alpha\in I\rightarrow x\in A_\alpha)\}。$$

设$\{A_\alpha\}_{\alpha\in I}$是一族集合。如果对于任意的 $\alpha,\beta\in I$，当 $\alpha\neq\beta$ 时，都有 $A_\alpha\cap A_\beta=\varnothing$，则称这族集合是互不相交的或两两不相交的。

二集合的差运算定义为 $A-B=\{x\mid x\in A\wedge x\notin B\}$。显然 $A-B=A-(A\cap B)$。

对于非空集合 U，定义它的子集 X 的补运算(余运算)为 $\overline{X}^{(U)}=U-X$。

二集合的异或(对称差)运算定义为 $A\oplus B=(A-B)\cup(B-A)=(A\cup B)-(A\cap B)$。

一个集合的笛卡儿乘积定义为这个集合本身。

$n(n\geqslant 2)$个集合 $A_1,A_2,\cdots,A_n$ 的笛卡儿积定义为

$$A_1\times A_2\times\cdots\times A_n=\{(a_1,a_2,\cdots,a_n)\mid \forall k(k\in\mathbb{Z}\wedge 1\leqslant k\leqslant n\rightarrow a_k\in A_k)\}。$$

集合 U 的所有子集构成的集合族 $2^U=\{A\mid A\subseteq U\}$ 称为 U 的幂集。U 的幂集也记作 $P(U)$。当 U 是有限集合时,其子集个数为 $|2^U|=2^{|U|}$,其中 $|U|$ 表示 U 的元素个数。

设 U 是非空集合,A,B,C 都是 U 的子集,$\{A_\alpha\}_{\alpha\in I}$ 是 U 的一族子集。集合的并、交、补运算具有下列性质:

交换律 $A\cup B=B\cup A,A\cap B=B\cap A$。

分配律 $A\cap\left(\bigcup\limits_{\alpha\in I}B_\alpha\right)=\bigcup\limits_{\alpha\in I}(A\cap B_\alpha),A\cup\left(\bigcap\limits_{\alpha\in I}B_\alpha\right)=\bigcap\limits_{\alpha\in I}(A\cup B_\alpha)$。

同一律 $A\cup\varnothing=A,A\cap U=A$。

补余律 $A\cup\overline{A}^{(U)}=U$(排中律),$A\cap\overline{A}^{(U)}=\varnothing$(矛盾律)。

基元律 $A\cup U=U,A\cap\varnothing=\varnothing$。

幂等律 $A\cup A=A,A\cap A=A$。

吸收律 $A\cup(A\cap B)=A,A\cap(A\cup B)=A$。

交叠律 $A\cup(\overline{A}^{(U)}\cap B)=A\cup B,A\cap(\overline{A}^{(U)}\cup B)=A\cap B$。

结合律 $(A\cup B)\cup C=A\cup(B\cup C),(A\cap B)\cap C=A\cap(B\cap C)$。

对偶律 $\overline{\left(\bigcup\limits_{\alpha\in I}A_\alpha\right)}^{(U)}=\bigcap\limits_{\alpha\in I}\overline{(A_\alpha)}^{(U)},\overline{\left(\bigcap\limits_{\alpha\in I}A_\alpha\right)}^{(U)}=\bigcup\limits_{\alpha\in I}\overline{(A_\alpha)}^{(U)}$。

双重否定律 $\overline{(\overline{A}^{(U)})}^{(U)}=A$。

上述性质中,交换律、分配律、同一律、补余律是最根本的性质,其余的性质都可以由这四条性质推出。对偶律又叫 de Morgan 律。

1.2 函数、置换的循环分解

本节将介绍有关函数和映射的基本概念和一般性质,并讨论置换的循环分解。

1.2.1 函数的基本概念和一般性质

定义 1.1 设 X,Y 是两个非空集合。如果按照从 X 到 Y 的一个确定的对应法则 f,对于集合 X 中的每一个元素 x,在集合 Y 中总有唯一的元素 $f(x)$ 与之对应,则称此对应法则 f(或称三元组(f,X,Y))为从集合 X 到集合 Y 的一个映射或函数,记作 $f:X\rightarrow Y,x\mapsto f(x)$。$X$ 称为此函数的定义域,$f(x)$ 称为元素 x 在函数 f 下的像或函数 f 在元素 x 处的值。对于每一个 $A\subseteq X$,Y 的子集 $f(A)=\{f(a)\mid a\in A\}$ 称为 A 在函数 f 下的像;特别地,$f(X)$ 称为此函数的值域。对于每一个 $B\subseteq Y$,称 X 的子集 $f^{-1}(B)=\{x\mid x\in X\wedge f(x)\in B\}$

(即$f^{-1}(B)=\bigcup_{b\in B}f^{-1}(\{b\})$)为子集 B 在函数 f 下的原像。

今后,常将 $f^{-1}(\{y\})$简写作 $f^{-1}(y)$,并称为元素 $y\in Y$ 在函数 f 下的原像。

例 1.1 定义非空集合 X 到其自身的函数 I_X 为:对于所有的 $x\in X$,$I_X(x)=x$。I_X 称为 X 上的恒等映射、恒同映射或单位映射。今后,我们将多次用到这个函数。

例 1.2 定义$\mathbb{R}$上的符号函数 $\mathrm{sgn}(x)$为:对于任意的 $x\in\mathbb{R}$,当 $x>0$ 时,$\mathrm{sgn}(x)=1$;当 $x=0$ 时,$\mathrm{sgn}(x)=0$;当 $x<0$ 时,$\mathrm{sgn}\ (x)=-1$。

定义 1.2 设 $f:X\to Y$ 是一个函数。如果 $f(X)=Y$,则称 f 为一个满射,或称 f 为满射的。如果对于所有的 $x_1,x_2\in X$,当 $x_1\neq x_2$ 时必有 $f(x_1)\neq f(x_2)$,换句话说,当 $f(x_1)=f(x_2)$时必有 $x_1=x_2$,则称 f 为一个单射,或称 f 为单射的。如果函数 f 既为满射又为单射,则称 f 为一个双射或一一对应,或称 f 为双射的。

定义 1.3 设 f 和 g 都是从 X 到 Y 的函数。如果对于所有的 $x\in X$,都有 $f(x)=g(x)$,则称函数 f 与函数 g 相等,记作 $f=g$。

定义 1.4 设 $f:X\to Y$ 是一个函数,$g:Y\to Z$ 也是一个函数。定义函数 $gf:X\to Z$ 为:对于每一个 $x\in X$,$gf(x)=g(f(x))$。函数 gf 称为函数 g 和函数 f 的复合或积。

定理 1.1(函数的一般性质) 任一函数 $f:X\to Y$ 具有如下的性质:

(1) $X=\bigcup_{y\in Y}f^{-1}(y)$。并且当 $y_1\neq y_2$ 时,$f^{-1}(y_1)\cap f^{-1}(y_2)=\varnothing$。

(2) 若 $A_\alpha\subseteq X$,则 $f\left(\bigcup_{\alpha\in I}A_\alpha\right)=\bigcup_{\alpha\in I}f(A_\alpha)$;

(3) 若 $A_\alpha\subseteq X$,则 $f\left(\bigcap_{\alpha\in I}A_\alpha\right)\subseteq\bigcap_{\alpha\in I}f(A_\alpha)$;

(4) 若 $B_\alpha\subseteq Y$,则 $f^{-1}\left(\bigcup_{\alpha\in I}B_\alpha\right)=\bigcup_{\alpha\in I}f^{-1}\left(B_\alpha\right)$;

(5) 若 $B_\alpha\subseteq Y$,则 $f^{-1}\left(\bigcap_{\alpha\in I}B_\alpha\right)=\bigcap_{\alpha\in I}f^{-1}(B_\alpha)$;

(6) 若 $A\subseteq X$,则 $f^{-1}(f(A))\supseteq A$,当且仅当 f 是单射时等号恒成立;

(7) 若 $B\subseteq Y$,则 $f(f^{-1}(B))\subseteq B$,当且仅当 f 是满射时等号恒成立;

(8) $f^{-1}(A-B)=f^{-1}(A)-f^{-1}(B)$,$A\subseteq Y$,$B\subseteq Y$。

请读者自己给出定理 1.1 的证明。

定义 1.5 设 $f:X\to Y$ 是一个函数。如果存在函数 $g:Y\to X$ 使得 $gf=I_X$ 且 $fg=I_Y$,则称函数 f 为可逆的,并称函数 g 为函数 f 的反函数或逆函数。

容易证明可逆函数 $f:X\to Y$ 的反函数是唯一的,因此记作 f^{-1}。对于每一个 $B\subseteq Y$,$f^{-1}(B)$一般表示子集 B 在函数 f 下的原像。而如果 f 可逆,则 $f^{-1}(B)$还表示子集 B 在函数 f^{-1}下的像,这时二者实际上是一致的。

定理 1.2 函数 $f:X\to Y$ 可逆当且仅当它是双射的。

证明:必要性。设函数 $f:X\to Y$ 可逆且其逆函数为 $g:Y\to X$,则由定义 1.5 有 $gf=I_X$ 和 $fg=I_Y$。对于任意的 $y\in Y$,存在 $x=g(y)\in X$ 使 $f(x)=f(g(y))=fg(y)=I_Y(y)=y$。

所以 $f(X)=Y$，即 f 是满射的。设 $x_1,x_2\in X$ 使 $f(x_1)=f(x_2)$，则 $x_1=I_X(x_1)=gf(x_1)=g(f(x_1))=g(f(x_2))=gf(x_2)=I_X(x_2)=x_2$。所以 f 是单射的。

充分性。设函数 $f:X\to Y$ 是双射的。对于任意的 $y\in Y$，因为 f 是满射的，所以 $f^{-1}(y)\neq\varnothing$。我们断言 $f^{-1}(y)$ 由唯一的一个元素组成。否则将有 $x_1,x_2\in f^{-1}(y)$，$x_1\neq x_2$，但 $f(x_1)=y=f(x_2)$，这与 f 的单射性矛盾。设 $f^{-1}(y)$ 中那个唯一元素为 $g(y)$，则 $g:Y\to X$ 是函数且 $gf=I_X$，$fg=I_Y$。所以 f 可逆。 ■

定义 1.6 设 $f:X\to Y$ 是一个函数，$\varnothing\neq A\subset X$。定义从 A 到 Y 的函数 $f|A$ 为：对于任意的 $x\in A$，$(f|A)(x)=f(x)$。函数 $f|A$ 称为函数 f 在集合 A 上的限制。反过来，函数 f 称为函数 $f|A$ 向集合 X 的一个延拓或扩张。

函数 f 在集合 A 上的限制具有如下性质：

$$(f|A)^{-1}(B)=A\cap f^{-1}(B),B\subseteq Y。$$

今后，在不产生混淆的情况下，我们有时说到从 A 到 Y 的函数 f，实际上是指函数 f 在集合 A 上的限制。下面定义中用到的有限集概念具体可参考定义 1.12。

定义 1.7 非空集合 X 到其自身的任一函数 f 称为该集合上的一个变换或一元运算。非空集合 X 到其自身的任一二元函数 $f:X\times X\to X$ 称为该集合上的一个二元运算。非空有限集合 X 上的任一可逆变换 f 称为该集合(上)的一个置换。

当 f 的确是集合 X 上的一元或二元运算时，也称该运算是良定的。良定性有两个方面的含义：(1) 运算的唯一性，即运算结果存在且唯一；(2) 运算的封闭性，即运算结果在 X 中。

在具体论及二元运算时，常使用中缀表示法，就是将二元函数 $f:X\times X\to X$ 的函数名 f 看成运算符，将函数值 $f(a,b)$ 写成 afb。例如 $a+b$，$a\times b$，$a\oplus b$，$a\otimes b$，$a\odot b$，$a\cdot b$，$a\circ b$，$a*b$ 等。

定理 1.3 设 X,Y 是非空有限集合，$|X|=|Y|$。若 f 是从 X 到 Y 的一个函数，则 f 可逆当且仅当它是单射的，当且仅当它是满射的。特别地，非空有限集合上的变换是置换当且仅当它是单射的，当且仅当它是满射的。

请读者自己完成此定理的证明。

定义 1.8 如果非空集合 X 上可逆变换 f 的逆变换就是 f 本身，则称 f 是对合的，或称 f 为该集合上的一个对合或对合映射。

定义 1.9 设 f 是集合 X 上的一个变换，$x\in X$。如果 $f(x)=x$，则称 x 为 f 的一个不动点；否则称 x 为 f 的一个非不动点。

X 中每一元素都是 $f:X\to X$ 的不动点当且仅当 $f=I_X$。

1.2.2 置换的循环分解

定义 1.10 设 f 是非空有限集合 X 上的一个置换，F 是 f 的所有不动点的集合，$E=X-F$ 是 f 的所有非不动点的集合。如果 $E=\{x_1,x_2,\cdots,x_{|E|}\}\neq\varnothing$，且当 $1\leqslant i<|E|$ 时 $f(x_i)=x_{i+1}$，而 $f(x_{|E|})=x_1$，则称 f 是 X 上的一个 E-循环或 E-轮换，记作 $f=(x_1x_2\cdots x_{|E|})$，并将 $|E|$ 称为这个 E-循环的阶，$\mathrm{sgn}(f)=(-1)^{|E|-1}$ 称为这个 E-循环的符号。当 $\mathrm{sgn}(f)=1$(即 $|E|$ 为奇数)时称 f 为偶循环；当 $\mathrm{sgn}(f)=-1$(即 $|E|$ 为偶数)时称 f 为奇循

环。阶为 2 的 E-循环称为 E-对换。若 f_1 是 X 上的一个 E_1-循环，f_2 是 X 上的一个 E_2-循环，且 $E_1 \cap E_2 = \varnothing$，则称 f_1 和 f_2 是不相交的循环。

引理 1.1 设 f 是非空有限集合 X 上的一个置换，E 是 f 的所有非不动点的集合。如果 $f \neq I_X$，则 $|E| \geqslant 2$，并且对于每一个 $x \in E$，都有 $f(x) \in E$ 和 $f^{-1}(x) \in E$。从而 E 中必有一个长度 m 不小于 2 且各项两两不同的有限序列 $x_1, x_2, \cdots, x_m$，使得

$$x_{k+1} = f(x_k)(1 \leqslant k < m), x_1 = f(x_m)。$$

证明：反证法。如果对于某一个 $x \in E$，有 $f(x) \notin E$，则 $y = f(x)$ 是 f 的不动点，从而 $f(y) = y = f(x)$，而 $y \neq x$，这与 f 的单射性矛盾。所以对于每一个 $x \in E$，都有 $f(x) \in E$。因为 f^{-1} 与 f 具有相同的不动点和非不动点，所以对于每一个 $x \in E$，也都有 $f^{-1}(x) \in E$。如果 $|E| < 2$，则因 $f \neq I_X$ 有 $|E| = 1$，不妨设 $E = \{x\}$。已经证明 $f(x) \in E$，即 $f(x) = x$，与 E 的定义矛盾。所以必有 $|E| \geqslant 2$。

任取 $x_1 \in E$，必有 $x_2 = f(x_1) \in E - \{x_1\}$，$x_3 = f(x_2) \in E - \{x_2\}$，……如此进行下去，就得到 E 中的一个无限序列 $x_1, x_2, \cdots$，满足 $x_{k+1} = f(x_k) \in E - \{x_k\}$。由于 E 有限，一定存在一个最小的 i_0 和最小的长度 $m \geqslant 2$，使 $x_{i_0} = x_{i_0+m}$，而 $x_i \neq x_j (i_0 \leqslant i < j < i_0 + m)$。我们断言 $i_0 = 1$。否则将由 $f(x_{i_0-1}) = x_{i_0} = x_{i_0+m} = f(x_{i_0+m-1})$ 及 f 的单射性得到 $x_{i_0-1} = x_{i_0+m-1}$，与 i_0 的最小性矛盾。所以 $i_0 = 1$。这样就有 E 中长度为 $m \geqslant 2$ 且各项两两不同的有限序列 $x_1, x_2, \cdots, x_m$，使 $x_{k+1} = f(x_k)(1 \leqslant k < m)$，而 $x_1 = f(x_m)$。 ■

引理 1.2 设 $f \neq I_X$ 是非空有限集合 X 上的一个置换，F 是 f 的所有不动点的集合，$E = X - F$ 是 f 的所有非不动点的集合，则存在 X 的非空子集 $D(|D| \geqslant 2)$ 和 X 上的一个 D-循环 g，满足：对于任意的 $x \in X$，若 $x \in D$，则 $g(x) = f(x)$；否则 $g(x) = x$。

证明：因 $f \neq I_X$，故由引理 1.1，$|E| \geqslant 2$，且 E 中必有一个长度不小于 2 且各项两两不同的有限序列 $x_1, x_2, \cdots, x_m$，使 $x_{i+1} = f(x_i)(1 \leqslant i < m)$，而 $x_1 = f(x_m)$。记 $D = \{x_1, x_2, \cdots, x_m\}$，并定义函数 $g: X \to X$ 为：对任意的 $x \in X$，若 $x \in D$，则 $g(x) = f(x)$，否则 $g(x) = x$。显然 g 是 X 上的一个 D-循环。 ■

引理 1.3 非空有限集合 X 上任意两个不相交循环 f_1 和 f_2 都是可交换的。

证明：设 f_1 是 X 上的 E_1-循环，f_2 是 X 上的 E_2-循环，且 $E_1 \cap E_2 = \varnothing$。对于任意的 $x \in X$，若 $x \in E_1$，则由引理 1.1 知 $f_1(x) \in E_1$，从而 x 和 $f_1(x)$ 都是 f_2 的不动点，所以 $f_1 f_2(x) = f_1(x) = f_2 f_1(x)$；若 $x \in E_2$，则由引理 1.1 知 $f_2(x) \in E_2$，从而 x 和 $f_2(x)$ 都是 f_1 的不动点，所以 $f_1 f_2(x) = f_2(x) = f_2 f_1(x)$；若 $x \notin E_1 \cup E_2$，则 x 同时是 f_1 和 f_2 的不动点，故 $f_1 f_2(x) = x = f_2 f_1(x)$。所以 $f_1 f_2 = f_2 f_1$。 ■

定理 1.4 非空有限集合 X 上任意一个置换 f 都可以唯一地分解为有限个不相交循环的积。

证明：若 $f = I_x$，则 f 可以看成是 0 个不相交循环的积。以下设 $f \neq I_X$。

设 F 是 f 的所有不动点的集合，$E = X - F$ 是 f 的所有非不动点的集合。由引理 1.2，存在 E 的非空子集 $E_1(|E_1| \geqslant 2)$ 和 X 上的 E_1-循环 f_1，使得对于任意的 $x \in X$，若 $x \in E_1$，

则 $f_1(x)=f(x)$；若 $x\notin E_1$，则 $f_1(x)=x$。当 $E_1=E$ 时，$f=f_1$，证明结束。若 $E_1\neq E$，令 $E'=E-E_1$，这时必有 $|E'|\geqslant 2$。否则如果 $|E'|<2$，即 $|E'|=1$，可设 $E'=\{x\}$。因 $x\in E$，由引理1.1知 $f(x)\in E$，故 $f(x)\neq x$，$f(x)\notin E'$，从而 $f(x)\in E_1$。因 f_1 是 E_1-循环，故有某个 $x'\in E_1$ 使 $f(x')=f_1(x')=f(x)$，而 $x'\neq x$，与 f 的单射性矛盾。所以 $|E'|\geqslant 2$。定义 $f':X\to X$ 为：对于任意的 $x\in X$，若 $x\in E'$，则 $f'(x)=f(x)$，否则 $f'(x)=x$。这时，$F'=F\cup E_1$ 是 f' 的所有不动点的集合，E' 是 f' 的所有非不动点的集合。f' 显然是 X 上的置换。由引理1.2，存在 E' 的非空子集 E_2 和 X 上的 E_2-循环 f_2，使得对于任意的 $x\in X$，若 $x\in E_2$，则 $f_2(x)=f'(x)$；否则 $f_2(x)=x$。当 $E_2=E'$ 时，$f=f_1f_2$，证明结束。否则按照上面的方法继续进行。因 E 有限，这个过程必然在有限步之内结束。

由引理1.3知，在不考虑不相交循环顺序的情况下，分解式是唯一的。 ■

推论1.1 非空有限集合 X 上任意一个对合 f 都可以唯一地分解为有限个不相交对换的积。

证明：由定理1.4知，非空有限集合 X 上任意一个置换 f 都可以唯一地分解为有限个不相交循环的积。更进一步，如果 f 还是对合的，则分解式中每一个循环都是对换。 ■

定义1.11 非空有限集合 X 上任意一个置换 $f\neq I_X$ 的不相交循环分解式中各个不相交循环的符号之积称为 f 的符号，记作 $\operatorname{sgn}(f)$，并且当 $\operatorname{sgn}(f)=1$ 时称 f 为偶置换，而当 $\operatorname{sgn}(f)=-1$ 时称为 f 奇置换。另外，定义 $\operatorname{sgn}(I_X)=1$。

设有限集合 X 上的置换 $f\neq I_X$ 的不相交循环分解式为 $f=f_1f_2\cdots f_m$，其中 $f_k(1\leqslant k\leqslant m)$ 是 E_k 循环，$E_i\cap E_j=\varnothing$，$1\leqslant i<j\leqslant m$。显然 $\operatorname{sgn}(f)=(-1)^{|E|-m}$，其中 $E=E_1\cup\cdots\cup E_m$ 是 f 的非不动点集合。

引理1.4 若 f 和 g 是非空有限集合 X 上的两个置换，f 的非不动点集合为 E_1，g 的非不动点集合为 E_2，且 $E_1\cap E_2=\varnothing$，则 $\operatorname{sgn}(fg)=\operatorname{sgn}(f)\operatorname{sgn}(g)$。

证明：若 $f=I_X$ 或 $g=I_X$，则结论显然。设 $f\neq I_X$，$g\neq I_X$，且 f 和 g 的不相交循环分解式分别为 $f=f_1f_2\cdots f_m$，$g=g_1g_2\cdots g_n$，则 fg 的非不动点集合为 $E_1\cup E_2$，不相交循环分解式为 $fg=f_1f_2\cdots f_mg_1g_2\cdots g_n$。因此

$$\operatorname{sgn}(fg)=(-1)^{|E_1\cup E_2|-(m+n)}=(-1)^{|E_1|-m}(-1)^{|E_2|-n}=\operatorname{sgn}(f)\operatorname{sgn}(g)。$$ ■

定理1.5 非空有限集合 X 上任何一个对换作用在任何一个置换上将改变该置换的奇偶性。简单地说，对换改变置换的奇偶性。

证明：显然，对换改变恒等置换 I_X 的奇偶性。

设，$E=\{x_1,x_2,\cdots,x_m\}$，$f\neq I_X$ 是 X 上的一个 E-循环。对于 X 上的任意一个对换 $(a\ b)$，考虑 $(a\ b)$ 与 f 的积，即证明 $\operatorname{sgn}((a\ b)f)=-\operatorname{sgn}(f)$，$\operatorname{sgn}(f(a\ b))=-\operatorname{sgn}(f)$。若 $a,b\notin E$，则 $(a\ b)f$ 和 $f(a\ b)$ 有不相交循环分解式 $(a\ b)f=f(a\ b)=(a\ b)(x_1\ x_2\ \cdots\ x_m)$，所以 $\operatorname{sgn}((a\ b)f)=\operatorname{sgn}(f(a\ b))=-\operatorname{sgn}(f)$。若 $a,b\in E$，不失一般性，可设 $a=x_1$，$b=x_i$，即 $f=(a\ x_2\ \cdots\ x_{i-1}\ b\ x_{i+1}\ \cdots\ x_m)$。若 $i=2$，即 $f=(a\ b\ x_3\ \cdots\ x_m)$，则 a 是 $(a\ b)f$ 的不动点，b 是 $f(a\ b)$ 的不动点。这时，$(a\ b)f$ 有不相交循环分解式 $(a\ b)f=(b\ x_3\ \cdots\ x_m)$，$f(a\ b)$ 有

不相交循环分解式 $f(a\ b)=(a\ x_3\cdots\ x_m)$，故 $\mathrm{sgn}((a\ b)f)=\mathrm{sgn}(f(a\ b))=-\mathrm{sgn}(f)$。若 $i=m>2$，即 $f=(a\ x_2\cdots\ x_{m-1}b)=(b\ a\ x_2\ \cdots\ x_{m-1})$，则 b 是 $(a\ b)f$ 的不动点，a 是 $f(a\ b)$ 的不动点。这时，$(a\ b)f$ 有不相交循环分解式 $(a\ b)f=(a\ x_2\ \cdots\ x_{m-1})$，$f(a\ b)$ 有不相交循环分解式 $f(a\ b)=(b\ x_2\ \cdots\ x_{m-1})$，故 $\mathrm{sgn}((a\ b)f)=\mathrm{sgn}(f(a\ b))=-\mathrm{sgn}(f)$。若 $2<i<m$，容易验证 $(a\ b)f$ 有不相交循环分解式 $(a\ b)f=(a\ x_2\cdots\ x_{i-1})(b\ x_{i+1}\ \cdots\ x_m)$，$f(a\ b)$ 有不相交循环分解式 $f(a\ b)=(b\ x_2\ \cdots\ x_{i-1})(a\ x_{i+1}\ \cdots\ x_m)$，故 $\mathrm{sgn}((a\ b)f)=\mathrm{sgn}(f(a\ b))=-\mathrm{sgn}(f)$。若 $a\in E$，而 $b\notin E$，不失一般性，可设 $a=x_m$，即 $f=(x_1\ x_2\ \cdots\ x_{m-1}\ a)$。这时，$(a\ b)f$ 有不相交循环分解式 $(a\ b)f=(x_1\ \cdots\ x_{m-1}\ ba)$，$f(a\ b)$ 有不相交循环分解式 $f(a\ b)=(x_1\ \cdots\ x_{m-1}\ ab)$，故 $\mathrm{sgn}((a\ b)f)=\mathrm{sgn}(f(a\ b))=-\mathrm{sgn}(f)$。

在一般情况下，设 $f\neq I_X$ 的不相交循环分解式为 $f=f_1f_2\cdots f_n$，其中 f_i 是 X 上的 E_i-循环。这时候，f 的非不动点集合为 $E=E_1\cup E_2\cup\cdots\cup E_n$。我们来证明 $\mathrm{sgn}((a\ b)f)=-\mathrm{sgn}(f)$，$\mathrm{sgn}(f(a\ b))=-\mathrm{sgn}(f)$ 的证明是类似的。

对于 X 上的任意一个对换 $(a\ b)$，若 $a\in E$，而 $b\notin E$，可设 $a\in E_1$，上面已证 $\mathrm{sgn}((a\ b)f_1)=-\mathrm{sgn}(f_1)$，由引理 1.4 和定义 1.11 知 $\mathrm{sgn}((a\ b)f)=-\mathrm{sgn}(f)$。若 $a,b\notin E$，则 $(a\ b)f$ 有不相交循环分解式 $(a\ b)f=(a\ b)f_1f_2\cdots f_n$，因此 $\mathrm{sgn}((a\ b)f)=-\mathrm{sgn}(f)$。若 $a,b\in E$，分两种情况讨论：(1) a 与 b 同在某个 E_i 中，$(a\ b)f_i$ 的不相交循环分解式中每一个循环都与其他 $f_j(j\neq i)$ 不相交，上面已证明 $\mathrm{sgn}((a\ b)f_i)=-\mathrm{sgn}(f_i)$，由引理 1.3、引理 1.4 和定义 1.11 知 $\mathrm{sgn}((a\ b)f)=-\mathrm{sgn}(f)$；(2) a 与 b 分别在 E_i 和 E_j 中，而 $i\neq j$，不失一般性，设 $f_i=(a\ x_2\cdots\ x_s)$，$f_j=(b\ y_2\cdots\ y_t)$，这时有不相交循环分解式 $(a\ b)f_if_j=(a\ x_2\cdots\ x_s\ b\ y_2\cdots\ y_t)$，因此 $\mathrm{sgn}((a\ b)f_if_j)=(-1)^{s+t-1}=-\mathrm{sgn}(f_if_j)$，由引理 1.3、引理 1.4 和定义 1.11 知 $\mathrm{sgn}((a\ b)f)=-\mathrm{sgn}(f)$。■

从定理 1.5 的证明过程可以看出，在定义 1.11 中，规定 $\mathrm{sgn}(I_X)=1$ 是正确的。

定理 1.6 非空有限集合 X 上任意一个置换 $f\neq I_X$ 都可以分解为有限个对换之积，且分解式中对换个数的奇偶性与 f 的奇偶性相同。

证明：当 f 是一个循环时，由 $f=(x_1\ x_2\cdots\ x_m)$ 有 $f=(x_1\ x_m)\cdots(x_1\ x_3)(x_1\ x_2)$，且这个表示式中对换的个数为 $m-1$，与 f 有相同的奇偶性。设 f 还有另一种表示形式 $f=(x\ y)\cdots(u\ v)(s\ t)$，则 $f^{-1}=(s\ t)(u\ v)\cdots(x\ y)$，因此 $I_X=(s\ t)(u\ v)\cdots(x\ y)f$。由于 $\mathrm{sgn}(I_X)=1$，由定理 1.5 知对换 $(s\ t)$，$(u\ v)$，$\cdots$，$(x\ y)$ 的个数与 f 有相同的奇偶性。有限个不相交循环按照上面方法分别分解成有限个对换之积后，各分解式中没有相同的对换。所以当 f 不是单个循环时，结论也成立。■

1.3 对合映射不动点定理

定义 1.12 如果存在正整数 n，并且存在从集合 S 到集合 Z_n 的一个一一对应，则称集合 S 的基数为 n，记作 $|S|=n$。规定空集 $\varnothing$ 的基数为 0。基数为非负整数的集合称为有限