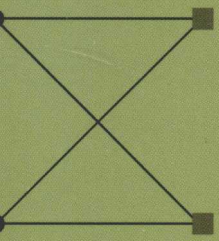
高等院校数学专业教材

DAISHU BIANMA DAOYIN

代数编码导引

胡万宝　孙广人　宛金龙　吴超云　编著



代数编码隶属于通信
用数学中的
析、设计通信
的信道编码，用于可靠
传输。

中国科学技术大学出版社

高等院校数学专业教材

代数编码导引

胡万宝　孙广人　宛金龙　吴超云　编著

中国科学技术大学出版社

内 容 简 介

本书给出了代数编码理论必要的代数导引，并用较大的篇幅介绍了编码理论和算法. 全书分为 3 篇：第 1 篇叙述了必要的近世代数知识. 第 2 篇首先介绍了编码理论的基本概念和线性码的结构，特别对线性码的信息集译码算法作了较为详尽的描述；还给出了循环码的导引，同时简述了循环码译码的纲要；并简要介绍了一些重要的分组码以及较为活跃的 LDPC 码. 第 3 篇重点介绍了 BCH 码与 RS 码的理论及算法.

本书可作为大学数学系信息专业高年级学生编码理论的教材.

图书在版编目(CIP)数据

代数编码导引/胡万宝等编著. —合肥：中国科学技术大学出版社，2013.3
(高等院校数学专业教材)
ISBN 978-7-312-03130-4

Ⅰ. 代… Ⅱ. 胡… Ⅲ. 代数编码 Ⅳ. O157.4

中国版本图书馆 CIP 数据核字（2012）第 314999 号

出版 中国科学技术大学出版社
安徽省合肥市金寨路 96 号，230026
http://press.ustc.edu.cn
印刷 合肥市宏基印刷有限公司
发行 中国科学技术大学出版社
经销 全国新华书店
开本 710 mm×960 mm 1/16
印张 13.75
字数 258 千
版次 2013 年 3 月第 1 版
印次 2013 年 3 月第 1 次印刷
定价 25.00 元

高等院校数学专业教材

编　委　会

前　言

目前国内关于编码理论的教材和专著可谓汗牛充栋，但是专门给数学系信息专业学生编写的编码教程尚属空缺.本书作者希望在这方面作一点努力.

本书希望达到的目的是，在编码理论教学中能够给学生以必要的代数导引，又能使学生得到相应的算法上的训练.因而我们用了较大的篇幅介绍关于编码算法的内容，又对必要的代数知识作了相应扩展，但是我们采取的办法不是直接把必要的数学知识全部堆积在第1章，而是在介绍算法的过程中不断地补充代数知识.

全书的内容是这样安排的：

第1篇：第1章用非正式的数学语言叙述了必要的代数知识，使学生能够对编码所需的代数知识有一个初步的了解.第2章详述了本书编码理论中频繁使用的有限域的基本知识，主要包括有限域的存在唯一性、Frobenius映射、迹与范函数等概念.第3章介绍了有限域的基本算法，包括复杂度的概念、多项式可约性的判别、多项式的分解、分裂多项式等基本内容.

第2篇：第4章简述了编码理论的基本概念.第5章介绍了线性码的结构，特别对线性码的信息集译码算法做出了较为详尽的描述，这是本书与其他教材的一个不同之处.第6章是关于循环码的导引，同时，在该章最后我们简述了循环码译码的纲要.第7章补充了其他一些经典分组码，包括Hadamard码、Reed-Muller码、二次剩余码以及Golay码.现在LDPC码是编码理论中较为活跃的方向，在第8章我们简要地介绍了其基本内容.

第3篇：重点介绍BCH码与RS码的理论及算法.第9章，与其他教材稍有不同的是我们给出了两种推广BCH码的方式，并简要介绍了Goppa码.随后第10章给出了BCH码与RS码译码的一般方法，主要给出了确定错误定位多项式的方法.我们知道关于RS码译码的研究始终相当活跃，所以在第11章，我们又进一步给出了有关RS译码的其他方法，可作为选讲的内容.

如果把本书只作为一学期68学时左右课程的教材，作者建议舍去其中第8

章的部分内容，并跳过第3篇中一些较为技术性的章节.

本书是编码理论教材中的一个尝试，由于时间仓促，不足与错误在所难免，希望各位读者多多给出批评和建议！

作　者

2012年3月

目　次

前言 …… (ⅰ)

第 1 篇　近世代数基础

第 1 章　基本代数 …… (3)
1.1　代数运算、等价关系与集合的分类 …… (3)
1.2　群 …… (6)
1.3　环 …… (11)
1.4　域的构造方法、扩域及分裂域 …… (17)

第 2 章　有限域基础 …… (23)
2.1　基本知识 …… (23)
2.2　有限域的存在性 …… (24)
2.3　有限域的子域结构与唯一性 …… (28)
2.4　共轭、范与迹 …… (29)

第 3 章　有限域上的算法 …… (34)
3.1　算法与复杂度的含义 …… (34)
3.2　整数的四则运算及模运算 …… (35)
3.3　多项式的四则运算 …… (36)
3.4　多项式的 Euclid 算法 …… (38)
3.5　判别与构造不可约多项式 …… (39)
3.6　计算极小多项式 …… (40)
3.7　分解多项式：无平方因子分解 …… (41)
3.8　分解多项式：Cantor-Zassenhaus 算法 …… (43)
3.9　分解多项式：Berlekamp 算法 …… (47)
3.10　分裂多项式与分裂值 …… (51)
3.11　多项式的重构 …… (54)

3.12 素性测试 …… (57)

第 2 篇 编码理论基础

第 4 章 编码理论基础 …… (67)
4.1 什么是编码理论 …… (67)
4.2 编码理论的基本概念 …… (69)
4.3 Hamming 距离与最大似然译码 …… (70)
4.4 最小距离与码的检错、纠错能力 …… (71)
4.5 编码的基本问题与码的等价变换 …… (73)
4.6 $A_q(n,d)$的上、下界 …… (74)

第 5 章 线性码 …… (77)
5.1 线性码与 Hamming 重量 …… (77)
5.2 线性码的生成矩阵与编码 …… (77)
5.3 内积与对偶码 …… (79)
5.4 线性码的校验矩阵 …… (81)
5.5 标准阵译码与伴随式译码 …… (83)
5.6 信息集译码 …… (85)
5.7 信息集译码的简化 …… (87)

第 6 章 循环码 …… (94)
6.1 循环码的定义 …… (94)
6.2 循环码的生成矩阵与校验矩阵 …… (96)
6.3 循环码的伴随译码 …… (99)
6.4 循环码的译码算法 …… (100)

第 7 章 一些重要分组码 …… (102)
7.1 Hadamard 矩阵 …… (102)
7.2 Hadamard 矩阵的 Paley 构造 …… (104)
7.3 Hadamard 码 …… (108)
7.4 Reed-Muller 码 …… (108)
7.5 二次剩余码 …… (116)
7.6 Golay 码 …… (118)

第 8 章 LDPC 码 …… (122)
8.1 图论基础 …… (122)

8.2　LDPC 码的定义与图表示 …… (124)
8.3　Tanner 图中的环路 …… (125)
8.4　LDPC 码的构造 …… (127)
8.5　LDPC 码的译码 …… (129)

第 3 篇　BCH 码与 RS 码

第 9 章　BCH 码与 RS 码基础 …… (135)
9.1　BCH 码的定义 …… (135)
9.2　BCH 码的参数 …… (137)
9.3　RS 码的参数 …… (138)
9.4　GRS 码 …… (139)
9.5　Goppa 码 …… (141)

第 10 章　BCH 码与 RS 码的译码 …… (144)
10.1　伴随的计算 …… (144)
10.2　错误定位多项式 …… (145)
10.3　找到错误定位多项式 …… (146)
10.4　Berlekamp-Massey 算法 …… (149)
10.5　Berlekamp-Massey 算法中 LFSR 的长度 …… (150)
10.6　非 2 元 BCH 码与 RS 码的译码 …… (154)
10.7　错误定位多项式的 Euclid 算法 …… (157)

第 11 章　RS 码译码的其他方法 …… (158)
11.1　Welch-Berlekamp 的关键方程 …… (158)
11.2　导出关键方程的另一种方法 …… (163)
11.3　找出错误值 …… (165)
11.4　WB 关键方程的解法背景:模的概念 …… (167)
11.5　Welch-Berlekamp 算法 …… (168)
11.6　WB 关键方程的模论解法 …… (175)
11.7　GRS 码的 Sudan 译码算法 …… (183)

附录　本书涉及的部分程序的参考设计 …… (190)

参考文献 …… (207)

第1篇

近世代数基础

第1章 基本代数

本章主要介绍一下抽象代数中的相关概念、命题和定理(证明略去,请参考抽象代数教材中的相关内容).这些是学习编码理论的必备知识.

1.1 代数运算、等价关系与集合的分类

定义 1.1.1 设 A,B 是两个集合.作一个新的集合:

$$\{(a,b) \mid a \in A, b \in B\}$$

称这个集合为 A 与 B 的 **Descartes(笛卡儿)积**,记作 $A \times B$.

注意,(a,b)是一个有序元素对.我们有

$$B \times A = \{(b,a) \mid b \in B, a \in A\}$$

一般来说,$A \times B$ 并不等于 $B \times A$.例如,$A=\{1,2,3\}$,$B=\{4,5\}$,则

$$A \times B = \{(1,4),(1,5),(2,4),(2,5),(3,4),(3,5)\}$$

$$B \times A = \{(4,1),(5,1),(4,2),(5,2),(4,3),(5,3)\}$$

然而,当 A,B 都是有限集时,$A \times B$ 与 $B \times A$ 包含元素的个数是相同的,都等于 $|A||B|$($|A|,|B|$分别表示集合 A,B 中所含元素的个数).

Descartes 积的概念可以推广到任意多个集合.例如,集合 $A_1,A_2,\cdots,A_n$ 的 Descartes 积定义为

$$\{(a_1,a_2,\cdots,a_n) \mid a_i \in A_i, i=1,2,\cdots,n\}$$

并记作 $A_1 \times A_2 \times \cdots \times A_n$ 或者 $\prod_{i=1}^{n} A_i$.

定义 1.1.2 设 A,B,C 是三个非空集合.从 $A \times B$ 到 C 的映射称为 A,B 到 C 的**代数运算**.特别地,当 $A=B=C$ 时,$A \times A$ 到 A 的代数运算简称为 A 上的代数运算.

一个代数运算可以用"$\circ$"来表示,并将(a,b)在"$\circ$"下的像记作 $a \circ b$.

例 1.1.1 一个 $\mathbb{Z} \times \mathbb{Z}^*$ 到 $\mathbb{Q}$ 的映射

$$\circ:(a,b)\mapsto\frac{a}{b}$$

是$\mathbb{Z}\times\mathbb{Z}^*$到$\mathbb{Q}$的代数运算.这就是普通数的除法.

例 1.1.2 一个$\mathbb{Z}\times\mathbb{Z}$到$\mathbb{Z}$的映射

$$\circ:(a,b)\mapsto a(b+1)$$

是$\mathbb{Z}$上的代数运算.

下面介绍代数运算的运算规律.

定义 1.1.3 设$\circ$是集合A上的一个代数运算,那么:

(1) 若对$\forall a_1,a_2,a_3\in A$,都有$(a_1\circ a_2)\circ a_3=a_1\circ(a_2\circ a_3)$,则称$\circ$适合**结合律**;

(2) 若对$\forall a_1,a_2\in A$,都有$a_1\circ a_2=a_2\circ a_1$,则称$\circ$适合**交换律**;

(3) 若对$\forall a,b,c\in A$,有$a\circ b=a\circ c\Rightarrow b=c$,则称$\circ$适合**左消去律**,若对$\forall a,b,c\in A$,有$b\circ a=a\circ c\Rightarrow b=c$,则称$\circ$适合**右消去律**.

例 1.1.3 判定下列有理数集$\mathbb{Q}$上的代数运算$\circ$是否适合结合律、交换律和左、右消去律:

(1) $a\circ b=a+b+ab$:适合结合律、交换律,但不适合左、右消去律;

(2) $a\circ b=(a+b)^2$:适合交换律,但不适合结合律和左、右消去律;

(3) $a\circ b=a$:适合结合律和右消去律,但不适合交换律和左消去律;

(4) $a\circ b=b^3$:适合左消去律,但不适合结合律、交换律和右消去律.

定义 1.1.4 设$\otimes$是$B\times A$到A的代数运算,$\odot$是$A\times B$到A的代数运算,$\oplus$是A上的代数运算,$\forall a_1,a_2\in A,b\in B$.

(1) 若$b\otimes(a_1\oplus a_2)=b\otimes a_1\oplus b\otimes a_2$,则称$\otimes$对于$\oplus$适合左分配律;

(2) 若$(a_1\oplus a_2)\odot b=a_1\odot b\oplus a_2\odot b$,则称$\odot$对于$\oplus$适合右分配律.

注意,左、右分配律还可以推广.

将集合按一定的规则进行分类是研究集合的一种有效方法,而等价关系对于集合的分类起着重要的作用.

定义 1.1.5 设A,B是两个集合,则$A\times B$的一个子集R称为A,B间的一个二元关系.当$(a,b)\in R$时,称a与b具有关系R,记作aRb;当$(a,b)\notin R$时,称a与b不具有关系R,记作$aR'b$.

设R是$A\times B$的一个子集,则R在$A\times B$中的余集$R^c=(A\times B)\backslash R$也是$A\times B$的一个子集,所以$R^c$也是$A,B$间的一个二元关系,称为$R$的**余关系**.

由任意的$(a,b)\in A\times B$,或者在R中,或者在R^c中,所以aRb或$aR'b$二者有且仅有一个成立.

下面主要讨论A,B间的二元关系,简称为A上的关系.

例 1.1.4 设$A=\mathbb{R}$,则

$R_1 = \{(a,b) \mid (a,b) \in \mathbb{R} \times \mathbb{R}, a = b\}$ （实数间的“相等”关系）

$R_2 = \{(a,b) \mid (a,b) \in \mathbb{R} \times \mathbb{R}, a \leqslant b\}$ （实数间的“小于或等于”关系）

$R_3 = \{(a,b) \mid (a,b) \in \mathbb{R} \times \mathbb{R}, a = 2b\}$

$R_4 = \{(a,b) \mid (a,b) \in \mathbb{R} \times \mathbb{R}, a^2 + b^2 = 1\}$

都是实数集$\mathbb{R}$上的关系.

例 1.1.5 设 $A = \mathbb{R}$,则

$$R_5 = \{(a,b) \mid a,b \in \mathbb{Z}, a,b \text{ 的奇偶性相同}\}$$

是整数集$\mathbb{Z}$上的一个关系.

定义 1.1.6 设 R 是集合 A 上的一个二元关系.若它满足下列性质:

(1) 自反性:$\forall\, a \in A, aRa$;

(2) 对称性:$\forall\, a,b \in A, aRb \Rightarrow bRa$;

(3) 传递性:$\forall\, a,b,c \in A, aRb, bRc \Rightarrow aRc$,

则称 R 是 A 上的一个**等价关系**.当 aRb 时,称 a 与 b **等价**.

例 1.1.4 中的 R_1 是实数集$\mathbb{R}$上的一个等价关系,例 1.1.5 中的 R_5 是实数集$\mathbb{R}$上的一个等价关系,但例 1.1.4 中的 R_2, R_3, R_4 都不是等价关系,因为 R_2, R_3 不满足对称性,R_4 不满足传递性.

定义 1.1.7 设一个集合 A 分成若干个非空子集,使得 A 中每一个元素属于且只属于一个子集,则这些子集的全体称为 A 的一个**分类**.每个子集称为一个类.类中的任何一个元素称为这个类的一个代表.

由定义 1.1.7 可知,A 的非空子集族 $S = \{A_i \mid i \in I\}$ 是 A 的一个分类,当且仅当其满足下列性质:

(1) $\bigcup\limits_{i \in I} A_i = A$;

(2) 当 $i \neq j$ 时,$A_i \cap A_j = \varnothing$,即不同的类互不相交.

例 1.1.6 设 $A = \{1,2,3,4,5,6\}$,则

$$S_1 = \{\{1,2\},\{3\},\{4,5,6\}\}$$

是集合 A 的一个分类.但是 $S_2 = \{\{1\},\{3,4\},\{5,6\}\}$ 不是 A 的一个分类,因为 2 不属于任何一个子集;$S_3 = \{\{1,2\},\{2,3,4\},\{5,6\}\}$ 也不是 A 的一个分类,因为 2 属于两个子集:$\{1,2\}$ 与 $\{2,3,4\}$.

集合 A 上的等价关系与集合 A 的分类之间有着本质的联系.集合 A 的一个分类可以决定 A 上的一个等价关系;反之,集合 A 上的一个等价关系可以决定 A 的一个分类.下面的两个定理刻画了这种联系.

定理 1.1.1 设 $S = \{A_i \mid i \in I\}$ 是 A 的一个分类,规定 R 为

$$aRb \quad \Leftrightarrow \quad a \text{ 与 } b \text{ 属于同一类}$$

则 R 是 A 上的一个等价关系.

定理 1.1.2 设 R 是 A 上的一个等价关系. 对于 $a\in A$, 令

$$\bar{a}=\{x\mid x\in A, xRa\}$$

则 A 的子集族 $S=\{\bar{a}\mid a\in A\}$ 是 A 的一个分类.

定义 1.1.8 设 R 是 A 上的一个等价关系. 由 A 的全体不同等价类所组成的集合族称为 A 关于 R 的商集, 记作 A/R.

例 1.1.7 设 $A=\mathbb{Z}, n\in\mathbb{N}^*$. 令

$$R_n=\{(a,b)\mid a,b\in\mathbb{Z}, n\mid a-b\}$$

证明: R_n 是整数集 $\mathbb{Z}$ 上的一个等价关系, 并给出由这个等价关系所确定的 $\mathbb{Z}$ 的一个分类.

证明 显然, R_n 是 $\mathbb{Z}\times\mathbb{Z}$ 的一个子集, 因而 R_n 是 $\mathbb{Z}$ 上的一个关系. 又:

(a) 对 $\forall a\in\mathbb{Z}, n\mid a-a$, 故 aR_na;

(b) 对 $\forall a,b\in\mathbb{Z}$, 如果 aR_nb, 那么 $n\mid a-b$, 即 $n\mid b-a$, 故 bR_na;

(c) 对 $\forall a,b,c\in\mathbb{Z}$, 如果 aR_nb 且 bR_nc, 那么 $n\mid a-b$ 且 $n\mid b-c$, 即 $n\mid(a-b)+(b-c)$, 故 $n\mid a-c$, 即 aR_nc.

因此, R_n 是 $\mathbb{Z}$ 上的一个等价关系. 由这个等价关系 R_n 确定的等价类为

$$\bar{0}=\{pn\mid p=0,\pm1,\pm2,\cdots\}$$

$$\bar{1}=\{pn+1\mid p=0,\pm1,\pm2,\cdots\}$$

$$\cdots$$

$$\overline{n-1}=\{pn+n-1\mid p=0,\pm1,\pm2,\cdots\}$$

R_n 称为模 n 的**同余关系**, 由 R_n 确定的等价类称为模 n 的剩余类. $\mathbb{Z}$ 关于 R_n 的商集为

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

它由 n 个不同的剩余类组成. 今后将 $\mathbb{Z}/R_n$ 记作 $\mathbb{Z}_n$.

1.2 群

抽象代数的主要研究对象是各种各样的代数系, 即具有一些代数运算的集合. 群是具有一种代数运算的代数系, 它是抽象代数中一个比较古老且内容丰富的重要分支, 在数学、物理、化学、计算机等自然科学的许多领域中都有广泛的应用. 半群是比群更加广泛的一个概念. 在本节中, 我们从介绍半群开始.

定义 1.2.1 设 S 是一个非空集合. 若:

(1) 在 S 中存在一个代数运算。;

(2) $\circ$ 适合结合律：

$$(a\circ b)\circ c = a\circ(b\circ c),\quad \forall a,b,c\in S$$

则称 S 关于 $\circ$ 是一个**半群**，记作 $(S,\circ)$.

若半群 S 的运算 $\circ$ 还适合交换：

$$a\circ b = b\circ a,\quad \forall a,b\in S,$$

则称 S 是**交换半群**(又叫 **Abel(阿贝尔)半群**).

半群的代数运算 $\circ$ 通常称为乘法，并且 $\circ$ 常被省略，即 $a\circ b$，记作 ab，称为 a 与 b 的积. 一个交换半群 S 的代数运算常记作 $+$，并称为加法. 此时，对 $\forall a,b,c\in S$，结合律、交换律分别为

$$(a+b)+c = a+(b+c),\quad a+b = b+a$$

例 1.2.1 对于自然数集 $\mathbb{N}$，由于数的加法和乘法都是 $\mathbb{N}$ 上适合结合律与交换律的代数运算，所以 $(\mathbb{N},+)$ 和 $(\mathbb{N},\times)$ 都是交换半群.

类似地，偶数集 $2\mathbb{Z}$、整数集 $\mathbb{Z}$、正有理数集 $\mathbb{Q}^+$、正实数集 $\mathbb{R}^+$、实数集 $\mathbb{R}$、复数集 $\mathbb{C}$ 关于数的加法和乘法分别构成交换半群. 负整数集 $\mathbb{Z}^-$ 关于数的加法也构成交换半群，但 $\mathbb{Z}^-$ 关于数的乘法不是半群，因为 $(-2)(-3)=6\notin\mathbb{Z}^-$. 又非零整数集 $\mathbb{Z}^*$ 关于数的乘法构成交换半群，但 $\mathbb{Z}^*$ 关于数的加法不是半群，因为 $(-1)+1=0\notin\mathbb{Z}^*$.

例 1.2.2 设 n 是一个正整数. 在 $\mathbb{Z}$ 关于等价关系 R_n 的商集 $\mathbb{Z}_n=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$ 中，规定：

$$\bar{a}+\bar{b} = \overline{a+b},\quad \bar{a}\cdot\bar{b} = \overline{ab}$$

其中 $\bar{a},\bar{b}\in\mathbb{Z}_n$，则 $(\mathbb{Z}_n,+)$，$(\mathbb{Z}_n,\cdot)$ 都是交换半群.

定义 1.2.2 设 S 是半群，$n\in\mathbb{N}$，$a\in S$，n 个 a 的连续乘积称为 a 的 n 次幂，记作 a^n. 例如：

$$a^n = \underbrace{aa\cdots a}_{n\text{个}}$$

注意，当 S 是交换半群，而且其代数运算是加法时，a 的 n 次应为 a 的 n 倍，表示 n 个 a 的和，记作 na，即

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

定义 1.2.3 设 S 是半群. 若存在 $e\in S$，使得对 $\forall x\in S$，

$$ex = xe = x$$

则称 e 是 S 的**单位元**. 若 S 是有单位元 e 的半群，则称之为**含幺半群**.

若 S 是有单位元的半群，则 S 的单位元是唯一的. 规定：$a^0=e(\forall a\in S)$.

定义 1.2.4 设 S 是含幺半群，$a\in S$. 若 $\exists b\in S$，使得 $ab=ba=e$，则称 a 是

可逆元，b 是 a 的一个**逆元**.

设 S 是有单位元 e 的半群. 若 $a\in S$ 可逆，则其逆元是唯一的，记作 a^{-1}.

定义 1.2.5 设 $(G,\cdot)$ 是一个有单位元的半群. 若 G 中的每个元都是可逆元，则称 G 是一个**群**.

适合交换律的群称为**交换群**或 **Abel 群**. 交换群 G 的运算常用“+”表示，并称 G 是加群. 若 G 中的元素个数是有限的，则称 G 为有限群，否则称 G 为无限群.

例 1.2.3 数集 $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ 关于数的加法都构成加群. 零元(加群的单位元)是 0，一个数 a 的负元(加群中元素的逆元)是它的相反数 $-a$.

例 1.2.4 数域 P 上全体 n 阶矩阵所组成的集合 $M_n(P)$ 关于矩阵的加法构成一个加群. 零元是零矩阵 $\mathbf{0}$，一个 n 阶矩阵 $\boldsymbol{A}$ 的负元是它的负矩阵 $-\boldsymbol{A}$.

例 1.2.5 $GL(n,P)$ 表示数域 P 上全体 n 阶可逆矩阵组成的集合，关于矩阵的乘法构成一个群，单位元是矩阵 $\boldsymbol{E}_n$，一个 n 阶可逆矩阵 $\boldsymbol{A}$ 的逆元是它的逆矩阵 $\boldsymbol{A}^{-1}$($GL(n,P)$ 称为 P 上 n 次一般线性群，$n\geqslant 2$ 时，是非交换群).

例 1.2.6 $\mathbb{Z}_n=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$，关于加法运算 $\bar{a}+\bar{b}=\overline{a+b}$ 构成一个加群(模 n 的剩余类加群).

命题 1.2.1 群 G 的运算适合左、右消去律.

定义 1.2.6 设 G 是一个群，e 是 G 的单位元，$a\in G$. 使得

$$a^m=e \tag{2.1}$$

成立的最小正整数 m 称为元素 a 的阶，记作 $|a|=m$(或者 $\mathrm{ord}(a)=m$). 若这样的正整数 m 不存在，则称 a 是无限阶的，记作 $|a|=\infty$.

注意，当 G 是加群时，其运算是加法，单位元是零元：0，所以式(2.1)具有形式：$ma=0$.

定义 1.2.7 设 G 是一个群，$a\in G$. 若对 $\forall\, b\in G$，$\exists\, n\in\mathbb{Z}$，使得

$$b=a^n$$

则称 G 是由 a 生成的**循环群**，a 是 G 的**生成元**，记作 $G=(a)$.

例 1.2.7 整数加群 $\mathbb{Z}$ 是由 1 生成的无限循环群. 模 n 的剩余类加群 $\mathbb{Z}_n$ 是由 $\bar{1}$ 生成的 n 阶循环群.

定理 1.2.1 设 $G=(a)$ 是一个循环群，那么：

(1) 若 $|a|=m$，则 G 是含有 m 个元素的有限群，G 有 $\varphi(m)$(Euler(欧拉)函数)个形如 $a^k(k=0,1,\cdots,m-1)$ 的生成元，其中 $(r,m)=1$，且 $G=\{e=a^0,a^1,a^2,\cdots,a^{m-1}\}$；

(2) 若 $|a|=\infty$，则 G 是无限群，G 有两个生成元：a,a^{-1}，且

$$G=\{\cdots,a^{-2},a^{-1},a^0,a^1,a^2,\cdots\}$$

定义 1.2.8 设 G 是一个群，$\varnothing\neq H\subseteq G$. 若 H 关于 G 的乘法构成群，则称 H