Abstract Algebra

抽象代数

张贤科◎著

清華大學出版社
北京

内 容 简 介

本书是“抽象代数”(也称“近世代数”)课程的教材.前部分最基本,力求浅易具体.后部分内容渐丰.包含群、环、域的标准内容和一些深入内容:群作用于集合,西罗定理,唯一析因整环和主理想整环,伽罗瓦理论和应用,有限域及其上多项式等.还介绍了模与正合序列、半直积,戴德金环和诺特环等可选读参考.有较多例题,习题,有解答和提示,还加上 3 个附录.

本书可作为本科生和研究生的教材,适用于数学、自动化与人工智能、信息通信、编码和密码学、计算机网络电子等专业学生、学者、科技人员学习或参考.本科生初学可略去带 * 号等后部分内容.

图书在版编目(CIP)数据

抽象代数/张贤科著.—北京:清华大学出版社,2022.6
ISBN 978-7-302-60882-0

Ⅰ.①抽… Ⅱ.①张… Ⅲ.①抽象代数—高等学校—教材 Ⅳ.①O153

中国版本图书馆 CIP 数据核字(2022)第 083197 号

责任编辑:刘 颖
封面设计:傅瑞学
责任校对:王淑云
责任印制:宋 林

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:010-83470000 **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:三河市龙大印装有限公司
经 销:全国新华书店
开 本:185mm×230mm **印 张**:17.5 **字 数**:359 千字
版 次:2022 年 6 月第 1 版 **印 次**:2022 年 6 月第1 次印刷
定 价:49.80 元

产品编号:090485-01

前　言

本书是“抽象代数”(也称“近世代数”)课程的教材,前半部分力求浅易具体、清楚易懂,详细讲解最基本的标准内容,引导读者进入抽象殿堂.后半部分内容渐进丰厚、涵盖较广、视角较新.

内容包含群、环、域的完整讲解,同态、同构、商群、商环、理想、多项式、域的扩张和嵌入等,也包含群作用于集合、西罗定理、唯一析因整环、主理想整环、伽罗瓦理论和应用(方程根式解和尺规作图等)、有限域及其上多项式等较深入的内容.后部分还介绍了模与正合序列、代数整数环、坐标环和诺特环、群的半直积等,可作选读参考.配有较多例题、习题,附有解答和提示,还加上 3 个附录.本科生或初学者可略去带 * 号等后部分内容.

作者长期在清华大学、中国科学技术大学、南方科技大学作代数方面的教学和研究工作.在清华尖子生“学堂班(基础科学班)”“钱学森班”和数学系长期主讲“抽象代数”课程.

此教材是基于长期科研和教学实践,反复完善授课讲稿,参阅文献,多年积累写成,融入了不少心得感悟.讲解力求清楚明白,具有透视性,科学准确并采用较新视角,避免不必要的过分形式化和臃肿、烦琐.旨在引导读者较快掌握本课的实质.

本书可作为本科生和研究生的教材,适用于数学、理工科、自动化与人工智能、信息通信、编码和密码学、计算机网络等领域的学生、学者、科技人员学习或参考.第 1、2、4 章为基本内容,其余内容可根据教学需求和学时情况取舍调整.

抽象代数是最重要的数学分支之一.按照布尔巴基(N. Bourbaki)学派的结构主义,全部数学是基于代数、顺序、拓扑这三种母结构,三者分化组合生发出来的.代数学衍生融合出众多现代数学分支,许多是菲尔兹等大奖的最重要获奖领域,例如代数数论、代数几何、交换代数、表示论、同调代数、代数拓扑、模形式、李群、李代数、范畴论,等等,都蓬勃兴旺.随着数字化时代的到来,信息处理、信息安全加密、代数编码、人工智能发展迅猛,代数学在其中起到理论核心作用,是创新的灵魂,应用日益深入广泛.

抽象代数的突出特点是“抽象”,它讨论的是“代数结构”(algebraical structures),而不是数字或具体器物.“今天的数学主要关心的是结构以及结构之间的关系,而不是数之间的关系.这种情况最初发生在 1800 年左右,首次的突破是抽象群概念的引入.目前它在数学领域中已经无所不在.”(塞尔伯格(A. Selberg)语).在抽象代数的产生和发展中,问

题和实例起到重要作用. 寻求五次以上一元多项式方程的求解公式的惊心历程,导致发现“群”以描述方程根的对称性(伽罗瓦的思想困惑了数学界1830年左右). 对二次型、高次互反律、费马大定理的研究,产生了“环”和“理想”的概念(库默尔的理想数震惊了巴黎,1847). 近世代数思潮的兴起,一扫两千年迷雾,古希腊的历史难题一时纷纷瓦解冰消.

发展到19—20世纪之交,抽象思潮引起数学巨变. 数学家不再满足于研究具体对象的性质,而是要建立一般理论. 各种数学结构和分类问题成为潮流. 这种潮流在整个数学领域出现,代数学是引领者. 通过基本运算和公理,形式地定义出许多代数结构,抽象的群论、环论、域论横空出世(施泰尼茨的域论,希尔伯特,阿廷,诺特的环论,斐波那契,舒尔的群表示论等). 1900年前后这半个世纪的辉煌建树,在1930—1931年被范德瓦尔登出版的《近世代数》两卷系统地总结,“代数”一词的含意从此永远改变,数学的含意也从此改变了. 此后,代数学及其融合的诸多学科都飞速发展. 当初的高次互反律期望落实为类域论的优美理论,300多年对费马大定理的不懈追求终成正果. 同时,又生发出郎兰兹猜想等新的梦想,也带给人类诸如椭圆曲线算法等强大的高科技能力.

历史缘由和现实经验告诉我们,代数的“理论抽象性”是必须学习的——这正是代数的“威力”和“精华”所在,正是代数的“独特性”“优越性”. 代数为有志青年提供了大好用武之地,发展之基. 既使是不打算做理论工作的同学,趁年轻多学习一些抽象理论也是最好的. 事实上,代数没有传说的那样难学,它只是初学不习惯而已,“回头看”多了就亲切了. 理论和实例交错,理解和记忆融合,反复多次,就能建立起直观认知,抽象就变得具体而且自然了. 进一步,最好选择一个代数相关专业踏实学下去,更能深入真切. 因为抽象代数现在是多个学科方向的共同基础课,内容难免庞杂,侧面较多,“绝知此事要躬行”.

总之,教书和读书都要用心. 用心久了,岁月和实践会有回报. 在这一点上,教学和科研有些像农林业,种下桃树精心培养定会果实累累;而不太像工业制造业,人工合成桃子很难而且无味. 校园里看到“香蕉开花一条心”很有感触,“志者心之所之也”. 有《香蕉开花赞》一首赠给有心志的青年:

四月芭蕉捧赤心,
紫霞丹玉献青君.
流光结下黄金果,
蜡卷贝叶隐诗痕.

张贤科

2021年2月12日于清华园

目　　录

第1章

群论基础

抽象代数(abstract algebra),也称近世代数(modern algebra),主要探讨群、环、域、模等.兴起于1800年左右,其思想一举扫清两千年古希腊难题和方程根式解等历史困惑,引起了数学近现代的巨变,衍生出众多数学分支和应用.

本章讨论"群".先介绍数与映射、同余式等作为讨论基础.

1.1 数与映射

人类初始,先认识**自然数**,即1,2,3,….自然数全体记为$\mathbb{N}$(源自natural).

渐渐地,人类也承认1−1=0,2−3=0−1等为"数",即零和负自然数.正负自然数以及零合称为**整数**(integers),整数集合记为$\mathbb{Z}$(源自德文zahlen).整数集合$\mathbb{Z}$对加、减、乘三种运算**封闭**(即任意两个整数相加、减、乘,结果仍为整数).

后来,2÷3=2/3,1÷3=1/3等也被承认为"数",即分数.整数与分数合称为**有理数**(rational numbers,或rationals,原意为比例数),有理数集合记为$\mathbb{Q}$(源自quotient).有理数集合$\mathbb{Q}$对加、减、乘、除这四则运算都**封闭**(即任意两个有理数相加、减、乘、除之后的结果仍为有理数.约定0不做除数).注意,文献中常有不同记法书写分数(除法或分式),意义是一样的:

$$\frac{1}{a}=1/a=a^{-1},\quad \frac{b}{a}=b/a=ba^{-1}.$$

再后来(在古希腊时代),人们发现,有的线段的长度不能用有理数表达,例如边长为1的正方形的对角线长为$\sqrt{2}$,它不是有理数.这引导人们承认无限不循环小数也是数,称为**无理数**.例如$\sqrt{2}=1.4142135623\cdots$,圆周率$\pi=3.1415926535\cdots$等都是无理数.有理数与无理数合称为**实数**(real numbers,或reals),实数集合记为$\mathbb{R}$(源自real).实数集合$\mathbb{R}$对加、减、乘、除运算封闭(0不做除数).实数和实数轴上的点一一对应;这也意味着:(数轴上)任意线段的长度总可用实数表示.

到16世纪中叶,意大利人在解三次一元多项式方程时,用到负数开平方,例如$\sqrt{-1}$,

$\sqrt{-5}$等. 这些后来也被承认为数，于是人类就逐渐发展出复数. 每个**复数**(complex numbers)可写为 $a+b\mathrm{i}$，其中 a,b 为实数，i 称为虚单位，满足 $\mathrm{i}^2=-1$；有时也将 i 写为 $\sqrt{-1}$. a,b 分别称为此复数的实部、虚部. 当虚部非零，即 $b\neq 0$ 时，$a+b\mathrm{i}$ 称为**虚数**. 所以复数是实数与虚数的合称. 复数全体记为$\mathbb{C}$(源于 complex). 复数可以像实数一样做加、减、乘、除运算，只要注意 $\mathrm{i}^2=-1$ 即可. 复数运算规则如下(对 $a,b,c,d\in\mathbb{R}$)：

$$(a+b\mathrm{i})+(c+d\mathrm{i})=(a+c)+(b+d)\mathrm{i},$$
$$(a+b\mathrm{i})-(c+d\mathrm{i})=(a-c)+(b-d)\mathrm{i},$$
$$(a+b\mathrm{i})(c+d\mathrm{i})=(ac-bd)+(ad+bc)\mathrm{i},$$
$$\frac{a+b\mathrm{i}}{c+d\mathrm{i}}=\frac{(a+b\mathrm{i})(c-d\mathrm{i})}{(c+d\mathrm{i})(c-d\mathrm{i})}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}\mathrm{i}.$$

故复数集合$\mathbb{C}$对加、减、乘、除运算封闭(约定 0 不做除数).

复数集合最重要的性质是“代数封闭性”，即如下重要定理.

古典代数学基本定理　任意 n 次方程 $x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$ 一定有复数解(这里 $a_1,\cdots,a_n$ 为任意复数，整数 $n\geqslant 1$).

由此定理可推导出：任意 n 次方程一定有 n 个复数解. 后面会证明.

从自然数，到整数、有理数、实数，再到复数，“数”的体系随着人类的发展在“进化”(如图 1.1 所示). 新的“数”不断被“承认”. 后来“数的体系”也还有其他发展.

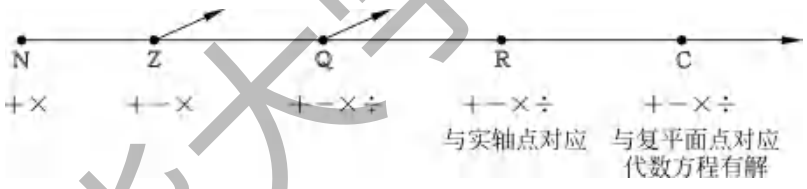

图 1.1　数的进化

复数还可以用几何方法表示. 取定一张平面，则复数可与此平面上的点一一对应：在平面上取定(右手直角)坐标系 Oxy，于是复数 $z=a+b\mathrm{i}$ 与平面上的点 $P=(a,b)$ 是一一对应的. 通常将复数 z 与点 P 等同，或者与向量(即有向线段) $\overrightarrow{OP}$ 等同. 此时 x,y 轴分别称为实数轴和虚数轴，此平面称为复平面(complex plane). 于是，任一复数 z 可以写为

$$z=a+b\mathrm{i}=\rho(\cos\theta+\mathrm{i}\sin\theta)=\rho\mathrm{e}^{\mathrm{i}\theta},$$

其中

$$\mathrm{e}^{\mathrm{i}\theta}=\exp(\mathrm{i}\theta)=\cos\theta+\mathrm{i}\sin\theta$$

是规定的记号(源自 Euler)，$\rho=\sqrt{a^2+b^2}$ 称为 z 的**绝对值**、长度或模 (absolute value, magnitude, modulus，即线段 OP 的长度)，θ 称为 z 的辐角(argument，即 $\overrightarrow{OP}$ 与实轴的夹角，$-180^\circ<\theta\leqslant 180^\circ$)(如图 1.2 所示).

设复数 $z_1=\rho_1 e^{i\theta_1}=\overrightarrow{OP_1}$，$z_2=\rho_2 e^{i\theta_2}=\overrightarrow{OP_2}$. 两复数的和 z_1+z_2 就是以 $\overrightarrow{OP_1}$ 和 $\overrightarrow{OP_2}$ 为邻边的平行四边形的对角线 $\overrightarrow{OQ}$. 两复数的积

$$z_1z_2=\rho_1\rho_2 e^{i(\theta_1+\theta_2)}.$$

故积的长度等于长度之积，积的辐角等于因子的辐角之和. 换一角度说，以 $z_1=\rho_1 e^{i\theta_1}$ 去乘任一复数 $z=\rho e^{i\theta}$，就是将 z 增长 ρ_1 倍并且逆时针旋转 θ_1 角度. 由此可知，z 的 k 次幂为

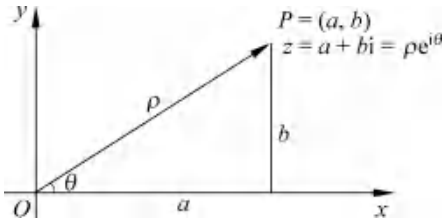

图 1.2 复数的几何表示

$$z^k=(\rho e^{i\theta})^k=\rho^k e^{ik\theta}=\rho^k(\cos k\theta+i\sin k\theta).$$

这些公式显示了欧拉(Euler)记号的优越之处——都易验证.

顺便指出，这些公式利于记忆三角公式. 例如，因

$$(\cos\theta+i\sin\theta)^2=\cos^2\theta-\sin^2\theta+i2\sin\theta\cos\theta,$$

故由上述公式($k=2$)分写实、虚部即得 $\cos2\theta=\cos^2\theta-\sin^2\theta$，$\sin2\theta=2\sin\theta\cos\theta$. 类似地可得到两角和差的公式和三倍角公式等.

设复数 $z=a+bi=\rho e^{i\theta}$，则 $\bar{z}=a-bi=\rho e^{-i\theta}$ 称为 z 的(复)共轭(conjugate). 二者在复平面上相对于实轴对称.

例 1 考虑方程 $x^n-1=0$，或 $x^n=1$ ($n\geqslant2$). 记

$$\zeta=\zeta_n=e^{2\pi i/n}=\cos(2\pi/n)+i\sin(2\pi/n)$$

(即辐角为 $2\pi/n$ 而长为 1 的复数). 则显然 $\zeta^n=1$，且 $\zeta^k\neq1$ (对 $k=1,2,\cdots,n$). 从而知 $x^n=1$ 恰有 n 个复数解：

$$1,\zeta,\zeta^2,\cdots,\zeta^{n-1}$$

(称为 n 次复单位根，共 n 个). 故有因式分解

$$x^n-1=(x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{n-1}).$$

这 n 个 n 次复单位根 $1,\zeta,\zeta^2,\cdots,\zeta^{n-1}$，恰好将复平面上单位圆 n 等分(如图 1.3 所示).

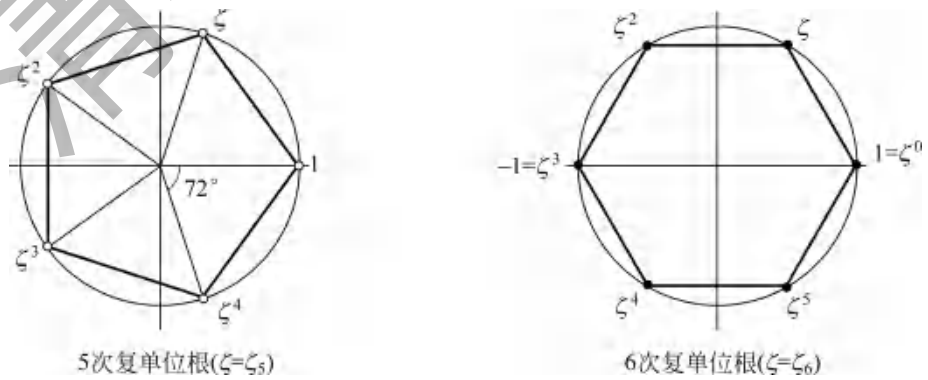

图 1.3 复单位根等分单位圆

评述 1　从自然数到复数，“数”在“进化”. 这一进化过程给了人类重要启示，不但启示发展出更新奇的数，更启示发展出各种新“结构”(即满足一些运算性质的集合). 从而使数学进入现代发展阶段.

现在简介集合与映射的概念和符号(稍详见附录 A)，这在代数中尤其重要.

一个**集合**就是一些互异的确定的对象全体，其中每个对象称为一个成员或元素，简称为元，有时也称为点. 集合也简称为集. 若集合 S 的元素都是集合 T 的元素，则称 S 是 T 的**子集合**(subset)，T 是 S 的**扩集合**(extension)，记为 $S\subset T$ 或 $T\supset S$ (也记为 $S\subseteq T$，$T\supseteq S$). 本书在 $S\neq T$ 时都明确说明. $S\setminus T=S-T=\{a\mid a\in S$ 且 $a\notin T\}$ 称为 T 在 S 中的**补集**，或称**差集**. $S\times T=\{(s,t)\mid s\in S,t\in T\}$ 称为集合 S 与 T 的**笛卡儿**(Descartes)**积**.

从集合 A 到集合 B 的一个映射(也称为函数，mapping，map，function) φ，就是从 A 到 B 的一个对应规则，使得**每个** $a\in A$ 对应于**唯一**的一个 $b\in B$ (记为 $\varphi(a)=b$). 此映射记为 $\varphi:A\to B,a\mapsto b$ (或 $A\xrightarrow{\varphi}B,\varphi(a)=b$). A,B,φ 是**映射的三要素**(即定义域，靶域(上域，值域)，对应规则). 若 $\varphi(a)=b$，则称 b 是 a 的**像**，a 是 b 的一个**原像**. 映射 φ 的**像**为 $\mathrm{Im}(\varphi)=\varphi(A)=\{\varphi(a)\mid a\in A\}$ (也称为 A 的像). B 的子集 C 的**原像**为

$$\varphi^{-1}(C)=\{a\in A\mid \varphi(a)\in C\}.$$

若 $\mathrm{Im}\varphi=B$，则称 φ 为**满射**(此时每个 $b\in B$ 都是某 $a\in A$ 的像). 若“对任意 $a_1\neq a_2$ 必有 $\varphi(a_1)\neq\varphi(a_2)$”，则称 φ 为**单射**. 若 φ 既是单射又是满射，则称 φ 为**双射**，或一一对应.

若有两映射 $\varphi:A\to B,\psi:B\to C$，则定义它们的**复合映射**为 $\psi\circ\varphi:A\to C$，

$$(\psi\circ\varphi)(a)=\psi(\varphi(a))\quad(\text{对任意 } a\in A).$$

也记 $\psi\circ\varphi$ 为 $\psi\varphi$，称为映射 ψ 与 φ 的**乘积**. 特别当 φ,ψ 都是 A 到自身的映射时，可定义 $\psi^{\circ}\varphi$.

设有映射 $\varphi:A\to B$，而 $A_1\subset A$，则可定义新映射 $\varphi_1:A_1\to B,\varphi_1(a)=\varphi(a)$. 称 φ_1 为 φ 到 A_1 的**限制**，记为 $\varphi_1=\varphi|_{A_1}$，而称 φ 为 φ_1 到 A 的**延拓**.

习　题　1.1

1. 自然数集合$\mathbb{N}$对加法、减法运算是否封闭？

2. 整数集合$\mathbb{Z}$对加、减、乘、除法运算是否封闭(0 不做除数)？

3. 分别举出下面例子：(1)对加、减运算封闭的集合；(2)对加、减、乘运算封闭的集合；(3)对加、减、乘、除运算封闭的集合(0 不做除数).

4. (1) 分别列出如下方程的复数解集合，并在复平面上画图表出：

$$x^3-1=0,\quad x^6-1=0,\quad x^4-1=0,\quad x^5-1=0,\quad x^8-1=0.$$

(2) 分别列出方程 $x^n=1$ 的解集合 W_n 的乘法表 ($n=3,6,4,5,8$).

5. $W_n=\{1,\zeta,\zeta^2,\cdots,\zeta^{n-1}\}(\zeta=\zeta_n=\mathrm{e}^{2\pi\mathrm{i}/n})$ 对乘、除运算是否封闭？为什么？

6. 考虑映射 $\varphi:\mathbb{Z}\to\mathbb{Z},k\mapsto k^2$. (1) 求 φ 的像 $\mathrm{Im}(\varphi)$，及 $\varphi^{-1}(1),\varphi^{-1}(0),\varphi^{-1}(-1)$.

(2) 将 φ 限制到正整数集 $\mathbb{Z}_+$ 为 φ_1，则 φ_1 是否为单射，满射？求 $\varphi_1^{-1}(1),\varphi_1^{-1}(0)$.

7. 证明：映射的复合(乘积)运算满足“结合律”，即 $\sigma\circ(\psi\circ\varphi)=(\sigma\circ\psi)\circ\varphi$.

8. 设 $\varphi:A\to B$ 为非空集间映射. 证明：(1)φ 有左逆当且仅当其为单射；(2)φ 有右逆当且仅当其为满射.

1.2 整 数 分 解

整数集合 $\mathbb{Z}$ 是代数的重要基地，其最重要的性质是“**带余除法**”. 即对任意整数 m,n 且 $m\neq0$，必存在唯一的整数 q,r 使得

$$n=mq+r\quad(0\leqslant r<|m|);$$

称 q 为(不完全)商(quotient)，称 r 为余数(remainder).

如果余数 $r=0$，即

$$n=mq,$$

则称 m **整除**(divides)n，记为 $m\mid n$，称 m 是 n 的**因子**(factor, divisor)，n 是 m 的**倍**(multiple). 显然 n 总有因子 $\pm1,\pm n$，这些称为 n 的平凡因子. 非平凡因子称为真因子. 如果整数 $p(\neq0,\pm1)$ 没有真因子，则称 p 为**素数**(prime number). 也就是说，p 为素数意味着：若 $p=mq$ 则必有 $m=\pm1$ 或 $q=\pm1$. 例如，$\pm2,\pm3$ 都是 6 的真因子，7 和 -7 都是素数.

如果 d 是整数 a,b 的公因子(即 $d\mid a,d\mid b$)，而且是 a,b 的任一公因子的倍，则称 d 是 a,b 的**最大公因子**. a,b 的最大公因子 d 是唯一的(不计正负号)，因为若 d' 也是 a,b 的最大公因子，则按定义知 $d\mid d'$ 且 $d'\mid d$，即 $d'=dq,d=d'q'$，故 $d'=dq=(d'q')q$，故 $q'q=\pm1,d'=\pm d$.

以 (a,b) 或 $\gcd(a,b)$ 记 a,b 的正的最大公因子. 例如 $(-6,-4)=2$. 如果 $(a,b)=1$，则称 a 与 b **互素**(relatively prime, coprime).

引理 1 若 $a=bq+r$，其中 a,b,r 为整数(不全为 0)，则

$$(a,b)=(r,b).$$

证明 只需证明左、右互相整除. 首先，(a,b) 整除 a 和 b，从而也整除 $r=a-bq$，故 (a,b) 是 b 和 r 的公因子，所以 (a,b) 整除 (r,b). 同样方法可证明 (r,b) 整除 (a,b). ■

引理 1 的公式 $(a,b)=(r,b)$ 说明：余数 r 可作为原数 a 的“替身”去参与求最大公因子. 进而，我们又可用 b 的替身 r_1 代替 b，等等. 如此继续，就引出著名的“**辗转相除法**”(Euclidean algorithm)：

$$\begin{aligned}
a &= bq_0 + r_1, & 0 < r_1 < |b|,\\
b &= r_1 q_1 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2,\\
&\vdots & \vdots\\
r_{s-2} &= r_{s-1} q_{s-1} + r_s, & 0 < r_s < r_{s-1},\\
r_{s-1} &= r_s q_s & (r_{s+1} = 0).
\end{aligned}$$

因为非负余数 $r_0, r_1, r_2, \cdots$ 逐步减小，终会为零，故可设 $r_{s+1} = 0$，即 $r_s | r_{s-1}$. 从前向后看，不断用余数代替原数去求最大公因子，最终即得最大公因子：

$$d = (a, b) = (r_1, b) = (r_1, r_2) = (r_3, r_2) = \cdots = (r_{s-1}, r_s) = r_s.$$

定理 1　任意两个整数 $a, b (b \neq 0)$ 的正最大公因子 $d = (a, b)$ 是唯一存在的，即 $d = r_s$（就是 a 与 b 辗转相除的最后非零余数），而且存在整数 u, v 使

$$ua + vb = d \quad (\textbf{贝祖等式}, \text{Bézout's identity}).$$

证明　只需再证明贝祖等式，即 d 是 a, b 的整数倍之和. 辗转相除的最后两式为

$$r_{s-1} = r_{s-3} - r_{s-2} q_{s-2}, \quad r_s = r_{s-2} - r_{s-1} q_{s-1}.$$

以前式的 r_{s-1} 代入后式，可得 r_s 是“r_{s-2} 和 r_{s-3} 的整数倍之和”. 再前推一式，以 r_{s-2} 代入，可得 r_s 是“r_{s-3} 和 r_{s-4} 的整数倍之和”. 由此不断上推，最终可得 r_s 是“a 与 b 的整数倍之和”，即得贝祖等式. ■

系 1　两个整数 a, b 互素当且仅当存在整数 u, v 使

$$ua + vb = 1 \quad (\text{贝祖等式}).$$

证明　若 a, b 互素，即 $(a, b) = 1$，则由定理 1 知有 $ua + vb = 1$. 反之，设 $ua + vb = 1$ 成立，则因 (a, b) 整除 a 与 b，故 (a, b) 整除 $ua + vb = 1$，故知 $(a, b) = 1$. ■

对多个整数 $a_1, a_2, \cdots, a_s$，其最大公因子 d 定义为：

(1) $d | a_i (i = 1, 2, \cdots, s)$；(2) 若 $\delta | a_i (i = 1, 2, \cdots, s)$，则 $\delta | d$.

正的 d 记为 $(a_1, a_2, \cdots, a_s)$ 或 $\gcd(a_1, a_2, \cdots, a_s)$；若其为 1，则称 $a_1, a_2, \cdots, a_s$ 互素.

系 2　任意 s 个非零整数 $a_1, a_2, \cdots, a_s$ 的正最大公因子 $d = (a_1, a_2, \cdots, a_s)$ 存在且唯一，且

$$(a_1, a_2, \cdots, a_{s-1}, a_s) = ((a_1, a_2, \cdots, a_{s-1}), a_s).$$

而且存在整数 $u_1, u_2, \cdots, u_s$ 使得

$$u_1 a_1 + u_2 a_2 + \cdots + u_s a_s = d \quad (\text{贝祖等式}).$$

证明　$(a_1, a_2, \cdots, a_s)$ 整除 $a_i (i = 1, 2, \cdots, s)$，从而整除 $(a_1, a_2, \cdots, a_{s-1})$ 与 a_s，从而整除 $((a_1, a_2, \cdots, a_{s-1}), a_s)$. 同理可知 $((a_1, a_2, \cdots, a_{s-1}), a_s)$ 整除 $(a_1, a_2, \cdots, a_s)$. 二者均正，故相等. 由此可归纳地得出：任意 s 个整数 $a_1, a_2, \cdots, a_s$ 的最大公因子 d 是存

在的.假设 $u_1a_1+u_2a_2+\cdots+u_{s-1}a_{s-1}=(a_1,a_2,\cdots a_{s-1})$,则应存在整数 u,v 使得

$$d=(a_1,\cdots,a_{s-1},a_s)=((a_1,\cdots,a_{s-1}),a_s)=u(a_1,\cdots,a_{s-1})+va_s$$
$$=u(u_1a_1+\cdots+u_{s-1}a_{s-1})+va_s=uu_1a_1+\cdots+uu_{s-1}a_{s-1}+va_s.$$ ■

系 3 符号如系 2,则

$$\{k_1a_1+k_2a_2+\cdots+k_sa_s \mid k_1,k_2,\cdots,k_s\in\mathbb{Z}\}=\{kd \mid k\in\mathbb{Z}\}.$$

证明 左边元素都是 d 的倍,故左⊂右.再由贝祖等式知,$kd=ku_1a_1+ku_2a_2+\cdots+ku_sa_s\in$左,故右⊂左. ■

说明 系 3 中等式的左边,称为 $a_1,a_2,\cdots,a_s$ 的"整组合集",记为$\mathbb{Z}a_1+\mathbb{Z}a_2+\cdots+\mathbb{Z}a_s$.右边记为$\mathbb{Z}d$ 或$d\mathbb{Z}$.故系 3 可简述为:若干整数的"整组合集"等于它们最大公因子的"整倍集".例如 $4\mathbb{Z}+6\mathbb{Z}=2\mathbb{Z}$.

定理 2(算术基本定理(fundamental theorem of arithmetic),整数唯一析因定理)任一整数 $n(\neq0,\pm1)$可写为有限个素数之积,且写法是唯一的(不计素数次序和正负号).也就是说,n 可写为

$$n=p_1p_2\cdots p_t, \tag{1.2.1}$$

其中 $p_1,p_2,\cdots,p_t$ 为素数(这称为 n 的唯一因子分解,或唯一析因).

定理 2 中的分解式有不同的写法.将相同的素数因子乘在一起,正负号提到前面,则得

$$n=(-1)^{\varepsilon}p_1^{v_1}p_2^{v_2}\cdots p_r^{v_r}. \tag{1.2.2}$$

这里的 $p_1,p_2,\cdots,p_r$ 为互异正素数,v_i 是正整数,$\varepsilon=0$ 或 1.也可写为

$$n=(-1)^{\varepsilon}\prod_p p^{v_p}, \tag{1.2.3}$$

其中 p 遍历正素数,v_p 是非负整数且只对有限多个 p 取值非零(约定 $p^0=1$).v_p 也写为 $v_p(n)$,是使得 $p^r\mid n$ 的最大整数 r,称为 n 在 p 的**指数**(exponent).此时记为

$$p^{v_p}\parallel n.$$

符号 $\parallel$ 读为**"恰整除"**.

用这种符号可知:$n\mid m$ 当且仅当 $v_p(n)\leqslant v_p(m)$(对任意正素数 p).

引理 2 设 p 为素数,a,b 为整数.(1) 若 $p\nmid a$,则 $(p,a)=1$.

(2) 若 $p\mid ab$,则 $p\mid a$ 或 $p\mid b$.

证明 (1) 因$(p,a)\mid p$,故$(p,a)=p$ 或 1.前者意味着 $p\mid a$,不合条件,故$(p,a)=1$.

(2) 若 $p\nmid a$,则$(p,a)=1$,有整数 u,v 使 $up+va=1$,$upb+vab=b$,而 $p\mid(upb+vab)$,故 $p\mid b$.

定理 2 的证明 (1) 先证因子分解的存在性.只需对自然数 n 证明.用数学归纳法.首先,$n=2$ 时定理显然成立.对任意固定的自然数 $n(>2)$,假设定理对小于 n 的自然数均成立(此句话称为归纳法假设);现需要证明定理对 n 成立.(1)若 n 是素数,则已是一

个素数之积，定理对 n 成立.(2)若 n 不是素数，则可写为 $n=n_1n_2$，其中 n_1,n_2 为小于 n 的自然数，由上述归纳法假设可知，n_1,n_2 均为有限个素数之积，可写为 $n_1=p_1\cdots p_s$，$n_2=p_{s+1}\cdots p_t$，故 $n=n_1n_2=p_1\cdots p_sp_{s+1}\cdots p_t$，为有限个素数之积，故定理对 n 成立.

(2) 现证因子分解的唯一性.若有两种分解 $p_1p_2\cdots p_t=n=q_1q_2\cdots q_s$，则

$$p_t\mid q_1q_2\cdots q_s=(q_1q_2\cdots q_{s-1})q_s,$$

由引理1(2)知，$p_t\mid q_s$ 或 $p_t\mid q_1q_2\cdots q_{s-1}$.若为后一情况，则 $p_t\mid q_{s-1}$ 或 $p_t\mid q_1\cdots q_{s-2}$.如此继续讨论可知，必对某 i 成立 $p_t\mid q_i$，不妨设为 $p_t\mid q_s$(可重排 $q_1,\cdots,q_s$ 的下标顺序).而因 q_s 为素数，只有平凡因子，故知 $p_t=\pm q_s$.从上述两种分解的等式中消去 $p_t=\pm q_s$，得

$$p_1p_2\cdots p_{t-1}=\pm q_1q_2\cdots q_{s-1}.$$

然后再如上继续讨论，不断消去素数因子，最后必会有一方化为 ±1，此时另一方也只能是 ±1，故 $t=s$，$p_i=q_i$($i=1,2,\cdots,t$.不计正负号和素数排列顺序).定理得证. ■

设 $a_1,a_2,\cdots,a_s$ 为非零整数，若整数 M 是所有 a_i 的倍数($i=1,2,\cdots,s$)，则称 M 是 $a_1,a_2,\cdots,a_s$ 的公倍数.$a_1,a_2,\cdots,a_s$ 最小的正公倍数 M_0 称为最小公倍数，记为 $[a_1,a_2,\cdots,a_s]$.

多项式

多项式与整数非常类似，现在做类比讨论可事半功倍.

形如 X^3+2X^2+3X+4 的式子，称为一元多项式，这在中学时已知.

下面我们取定复数的一个子集合 F(称为域)，通常取定 $F=\mathbb{Q}$ 为有理数集合(也可取 $F=\mathbb{R}$ 或 $\mathbb{C}$(实数或复数集合)，或其他，只需 F 对加、减、乘、除运算封闭(0不做除数)).

如下形式的表达式，称为域 F 上的一元多项式(简称多项式)：

$$a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0\quad(\text{其中 } a_i\in F,\ \ i=0,1,\cdots,n).$$

这里 X(也可写为 x)是一个符号，不是 F 中的元素，称为不定元.n 为非负整数.称各个 $a_i\in F$ 为**系数**，$a_n\neq0$ 为首项系数，非负整数 n 为**次数**(degree).并规定 $0\in F$ 也为多项式，次数为 $-\infty$，没有首项.例如 $\frac{2}{3}X^5+X$ 是 $\mathbb{Q}$ 上的多项式，而 $2X^{\frac{5}{6}}+X$ 不是.

对两个多项式 $f(X)=a_nX^n+\cdots+a_1X+a_0$ 和 $g(X)=b_mX^m+\cdots+b_1X+b_0$，规定 $f(X)=g(X)$ 当且仅当它们的次数相等，且 $a_i=b_i$(对 $i=0,1,\cdots,n$).特别可知，$f(X)=0$ 当且仅当 $f(X)$ 的所有系数都是0.

注记 1 因为这个 $f(X)=g(X)$ 的规定，故这里的多项式也称为多项式形式.

设 $f(X),g(X)$ 如上，不妨设次数 $n\geqslant m$.对 $m<j\leqslant n$ 记 $b_j=0$，则定义多项式的和

与积为

$$f(X)+g(X)=\sum_{i=0}^{n}(a_i+b_i)X^i,$$

$$f(X)g(X)=\sum_{k=0}^{n+m}\Big(\sum_{i+j=k}a_ib_j\Big)X^k.$$

多项式 $f(X)$也简记为 f,其次数记为 $\deg f$.

域 F 上的多项式集合记为 $F[X]$,它与整数集合$\mathbb{Z}$有类似性质.特别是,多项式也可进行**带余除法**,即对任意 $f(X),g(X)\in F[X]$ 且 $g(X)\neq 0$,必存在 $q(X),r(X)\in F[X]$ 使得

$$f(X)=g(X)q(X)+r(X)\quad (r(X)=0 \text{ 或 } \deg r(X)<\deg g(X)).$$

这由中学学过的多项式除法即可得到.例如,对 $f(X)=2X^3+X^2+X+1$,$g(X)=3X^2-1$,有带余除法:

$$f(X)=g(X)\Big(\frac{2}{3}X+\frac{1}{3}\Big)+\Big(\frac{5}{3}X+\frac{4}{3}\Big).$$

如果 $f(X)=g(X)q(X)$ $(g(X)\neq 0)$,则称 $g(X)$**整除** $f(X)$,记为 $g(X)\mid f(X)$,称 $g(X)$是 $f(X)$的**因子**,$f(X)$是 $g(X)$的倍.

若多项式 $f(X)$可以写为 $f(X)=g(X)q(X)$,而且 $q(X),g(X)\in F[X]$均不属于 F(不是常数),则称 $f(X)$是**可约的**,否则称 $f(X)$是**不可约的**(在 $F[X]$中或在 F 上).也就是说,$f(X)$不可约意味着:若 $f(X)=g(X)q(X)$,则必有 $q(X)$或 $g(X)$为常数(即属于 F).例如,X^2-2 在$\mathbb{Q}[X]$中(或$\mathbb{Q}$ 上)是不可约的.但是 X^2-2 在$\mathbb{R}[X]$中(或$\mathbb{R}$ 上)是可约的,因为 $X^2-2=(X-\sqrt{2})(X+\sqrt{2})$.

多项式 $d(X)$称为 $f(X),g(X)$的**最大公因子**是指:(1) $d(X)$是 $f(X)$和 $g(X)$的公因子;(2) $d(X)$是 $f(X),g(X)$的任一公因子的倍.易知,若 $d(X)$是 $f(X),g(X)$的最大公因子,则 $cd(X)$也是(这里 $c\in F$ 非零,称为非零常数).常用 $(f(X),g(X))$ 记 $f(X),g(X)$的首项系数是 1 的最大公因子.

由于多项式可作带余除法,故多项式 $f(X),g(X)$可作**辗转相除**.于是,完全与整数情形类似,我们有如下定理.

定理 3 域 F 上的任意两个多项式 $f(X),g(X)(g(X)\neq 0)$ 的最大公因子 $d(X)$是唯一存在的,即 $d(X)=r_s(X)$(就是 $f(X)$与 $g(X)$辗转相除的最后非零余式.这里的唯一性不计非零常数倍),而且存在 F 上的多项式 $u(X),v(X)$使

$$u(X)f(X)+v(X)g(X)=d(X)\quad (\text{贝祖等式}).$$

回忆讨论整数时候的逻辑链:

带余除法 → 辗转相除 → 贝祖等式 → 唯一析因定理.

现在同样的逻辑链适用于多项式,则由多项式的“带余除法”易推知“多项式的唯一析因

定理”.

定理 4　域 F 上任一多项式 $f(X)$（不是 F 中常数）均可唯一写为不可约多项式之积.（唯一性不计非零常数倍和乘积次序）

评述　整数（和多项式）的唯一析因定理，使数学的认知深入了一层. 从此我们视每个整数为若干素数之积. 例如，视 12 为 $2\times2\times3$，或者 $2^2\times3$（而通常不再视为 $11+1$）. 如此，处理整除因子倍数等问题，都了如指掌. 进一步想，每个正整数 n，由其在素数$\{2,3,5,\cdots,p_i,\cdots\}$的指数序列$(v_2,v_3,v_5,\cdots,v_{p_i},\cdots)$所唯一决定. 这将进一步大放异彩.

习　题　1.2

1. 设非零整数 m,n 的唯一素因子分解分别为

$$m=(-1)^e\prod_p p^{u_p},\quad n=(-1)^\varepsilon\prod_p p^{v_p},$$

其中 p 取遍正素数，u_p,v_p 为非负整数且均只对有限个 p 取值非零. 证明：

$$d=(m,n)=\prod_p p^{d_p},\quad M=[m,n]=\prod_p p^{M_p},\quad dM=mn,$$

其中 $d_p=\min\{u_p,v_p\}$，$M_p=\max\{u_p,v_p\}$. 特别知，m,n 的公倍数恰为$[m,n]$的倍数.

2. 证明：(1) 任意公倍数 M 必是最小公倍数 M_0 的倍数.

(2) $[a_1,\cdots,a_{s-1},a_s]=[[a_1,\cdots,a_{s-1}],a_s]$.

3. 设 a,b 为整数，$(a,b)=d$，证明

$$\{am+bn\mid m,n\in\mathbb{Z}\}=\{dk\mid k\in\mathbb{Z}\}.$$

4.（秦九韶：大衍求一术）求解方程 $65x+83y=1$.

5. 求证：$(ak,bk)=(a,b)k$；$(a/\delta,b/\delta)=(a,b)/\delta$；记 $d=(a,b)$，则$(a/d,b/d)=1$.（这里 k 为任一正整数，δ 是 a 和 b 的任一正公因子，a,b 是不全零的整数）.

6. 证明：(1) 若 $a\mid bc$，$(a,b)=1$，则 $a\mid c$. (2) 若 $a\mid c$，$b\mid c$，$(a,b)=1$，则 $ab\mid c$.

7. 证明：$[a_1,a_2,\cdots,a_s]=a_1a_2\cdots a_s$ 当且仅当 $a_1,a_2,\cdots,a_s$ 两两互素.

8. 对任意整数 $a_1,a_2,\cdots,a_s$，证明

$$a_1\mathbb{Z}\cap a_2\mathbb{Z}\cdots\cap a_s\mathbb{Z}=[a_1,a_2,\cdots,a_s]\mathbb{Z},$$

其中 $a\mathbb{Z}=\{ak\mid k\in\mathbb{Z}\}$.

9. 证明：当且仅当整数 $d\mid n$ 时，$(X^d-1)\mid(X^n-1)$.

10. 将定理 1 前的辗转相除式改写如下（也将 q_i 改记为 a_i）：

$$\frac{a}{b}=a_0+\frac{r_1}{b},\quad \frac{b}{r_1}=a_1+\frac{r_2}{r_1},\quad \cdots,\quad \frac{r_{s-1}}{r_s}=a_s.$$

即取 $r=a/b$ 的整数部分 a_0，再取其分数部分的倒数的整数部分 a_1，然后用同样方法得到 a_2，等等. 记为 $r=[a_0,a_1,a_2,\cdots,a_s]$，称为 $r=a/b$ 的连分数（展开）.

(1) 试求 $r=17/10$ 的连分数. (2)试求 $r=\sqrt{7}$ 的连分数到第 6 步（提示：按上述“取整数部分，再取分数部分倒数的整数部分”方法，可得实数的连分数展开，可能无限步）. (3)求 $\pi_0=3.14159$ 的连分数到第 3 步. (4)记连分数的前 n 部分为 $r_n=[a_0,a_1,\cdots,a_n]=p_n/q_n$，称为部分分数. 求 $r=\sqrt{7}$ 的部分分数

($n=3,4,5$). 求 $\pi_0=3.14159$ 的部分分数($n=0,1,2,3$).

1.3 同余与同余类

同余,我国古代早有研究. 高斯(Gauss)在其 21 岁所写的名著《算术研究》(1800 年)的开篇,就详细论述过.

定义 1 固定一个正整数 m 称为模(modulus). 若整数 a 与 b 除以 m 的余数相同,则称 a 与 b 对模 m **同余**(congruent modulo m),记为

$$a \equiv b \pmod{m}.$$

由定义可知,a 与 b 对模 m 同余恰相当于 $m \mid (a-b)$,或 $a=b+mk$(对某 $k\in\mathbb{Z}$),或者说"不计 m 的倍数时 a 与 b 相等".

例如:$8\equiv 1 \pmod 7$, $14\equiv 0 \pmod 7$, $1+1\equiv 0 \pmod 2$

符号"$\equiv$"称为同余号,读作"同余于",上述表达式称为同余式(congruence). 同余式的运算称为"模算术"(modular arithmetic),是近代数学入门之必须. "modulo m"相当于"measured (metered) with m",即以(m 为标准尺度作测量)(只计零头).

"同余"与"相等"有不少性质类似.

引理 1 同余式有如下性质(对任意 $a,b,c,d\in\mathbb{Z}$):

(1)(传递性,transitive) 若 $a\equiv b \pmod m$,$b\equiv c \pmod m$,则 $a\equiv c \pmod m$.

(2)(对称性,symmetric) 若 $a\equiv b \pmod m$,则 $b\equiv a \pmod m$.

(3)(自反性,reflexive) 总有 $a\equiv a \pmod m$.

(4)(同余式相加) 若 $a\equiv b \pmod m$,$c\equiv d \pmod m$,则 $a+c\equiv b+d \pmod m$.

(5)(同余式相乘) 若 $a\equiv b \pmod m$,$c\equiv d \pmod m$,则 $ac\equiv bd \pmod m$.

(6)(同余式约化) ①若 $a\equiv b \pmod m$,且 $d\mid a$,$d\mid b$,d 与 m 互素,则

$$\frac{a}{d}\equiv\frac{b}{d} \pmod m.$$

② 若 $a\equiv b \pmod m$,且 d 为 a,b,m 的公因子,则

$$\frac{a}{d}\equiv\frac{b}{d}\left(\bmod \frac{m}{d}\right).$$

证明都很简单,例如对(6)之①,记 $a=b+mk$,由 $d\mid a$,$d\mid b$ 知 $d\mid km$. 再因 d 与 m 互素,故 $d\mid k$. 所以 $a/d=b/d+m(k/d)$,即得 $a/d\equiv b/d \pmod m$. ■

例 1 求 3^{2049} 除以 13 的余数 r.

解 因 $3^3=27\equiv 1 \pmod{13}$,故 $3^{2049}=3^{3k}\equiv 1^k=1 \pmod{13}$,故 $r=1$.

例 2 对任意整数 a,b,以下成立:

$$a\equiv b \pmod 6 \quad \text{当且仅当} \quad \begin{cases} a\equiv b \pmod 2, \\ a\equiv b \pmod 3. \end{cases}$$

证明　若 $a\equiv b(\mathrm{mod}\ 6)$，则 $6|(a-b)$，故 $2|(a-b)$ 且 $3|(a-b)$，即 $a\equiv b(\mathrm{mod}\ 2)$ 且 $a\equiv b(\mathrm{mod}\ 3)$.

反之，若 $a\equiv b(\mathrm{mod}\ 2)$ 且 $a\equiv b(\mathrm{mod}\ 3)$，则 $2|(a-b)$ 且 $3|(a-b)$，故 $6|(a-b)$（这是因为：记 $a-b=p_1\cdots p_s$ 为其素因子分解，由 $2|(a-b)$ 且 $3|(a-b)$ 知可设 $p_1=2$，$p_2=3$，从而 $a-b=p_1p_2p_3\cdots p_s=2\cdot 3\cdot p_3\cdots p_s$），从而 $a\equiv b(\mathrm{mod}\ 6)$. ■

例 2 可推广，读者不难自证：若 m_1,m_2 互素，则

$$a\equiv b(\mathrm{mod}\ m_1m_2)\quad \text{当且仅当}\quad a\equiv b(\mathrm{mod}\ m_1)\ \text{且}\ a\equiv b(\mathrm{mod}\ m_2).$$

数学（和生活）中，有各种关系、例如相等关系、同余关系、同龄关系、师生关系，等等. 上述已知，同余关系满足传递性、对称性、自反性. 满足这三种性质的关系称为**等价关系**. 例如，同龄关系是等价关系.

我们可以按等价关系将对象分为等价类，例如按“同龄关系”可以将学校的学生分类，有 18 岁类、19 岁类、20 岁类等. 可按“同奇偶关系”将整数分为偶数类、奇数类. 可按“同性别关系”将班上同学分为男生、女生两类.

现在，固定正整数 m，按“模 m 同余的关系”将整数集 $\mathbb{Z}$ 分类：相互同余者分在同一类，称为一个**同余类**（congruence class）. 整数 a 所在的**同余类**记为 $\overline{a}$ 或 $a+m\mathbb{Z}$，即

$$\overline{a}=a+m\mathbb{Z}=\{a+mk\mid k\in\mathbb{Z}\},$$

称 a 为此同余类的**代表**（representative）. 于是 $\mathbb{Z}$ 被分为 m 个同余类：同余于 0 的类，同余于 1 的类，……，同余于 $m-1$ 的类；即整数集 $\mathbb{Z}$ 被划分为 m 个同余类的无交之并：

$$\mathbb{Z}=(m\mathbb{Z})\cup(1+m\mathbb{Z})\cup(2+m\mathbb{Z})\cup\cdots\cup(m-1+m\mathbb{Z}).$$

例如，当 $m=7$ 时，整数集 $\mathbb{Z}$ 被划分为 7 个同余类：

$$\{0,7,14,-7,\cdots\}=7\mathbb{Z}=\overline{0},$$
$$\{1,8,15,-6,\cdots\}=1+7\mathbb{Z}=\overline{1},$$
$$\vdots$$
$$\{6,13,20,-1,\cdots\}=6+7\mathbb{Z}=\overline{6}.$$

（这好像是：将日历上的所有星期日归为一类记为 $\overline{0}$，将所有的星期 1 归为一类记为 $\overline{1}$，等等. 共得到“星期 0，星期 1，…，星期 6”，即“$\overline{0},\overline{1},\overline{2},\cdots,\overline{6}$”，这 7 个类）.

按定义，同余者同类，即

$$a\equiv a'(\mathrm{mod}\ m)\Leftrightarrow\overline{a}=\overline{a'}.$$

故一个同余类可有不同写法，即代表元可以不同. 例如模 $m=7$ 时，$\overline{1}=\overline{8}=\overline{15}=\overline{-6}$，等等. 事实上，此同余类中任一成员均可作为代表元.

在每个同余类中任意取定一个代表元，这些代表元构成的集合称为一个“**代表元集**”，或一个“**剩余系**”. 例如，模 7 的剩余系可取为 0，1，…，6；当然也可取为 0，1，2，3，−3，−2，−1. 前者称为最小正剩余系，后者称为绝对（值）最小剩余系.

现在我们要更进一步，我们将“一个同余类”作为“一个元素”，于是 m 个同余类作为

m 个元素构成一个全新的集合：

$$\mathbb{Z}/m\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{m-1}\},$$

称为整数模 m 的**同余类集**，也记为$\mathbb{Z}/(m)$，它共有 m 个元素，每个元素是一个同余类.

定义 2 在同余类集 $\mathbb{Z}/m\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{m-1}\}$中定义**加法和乘法**运算如下：

$$\overline{a}+\overline{b}=\overline{a+b}\quad(\text{即}(a+m\mathbb{Z})+(b+m\mathbb{Z})=a+b+m\mathbb{Z});$$

$$\overline{a}\cdot\overline{b}=\overline{a\cdot b}\quad(\text{即}(a+m\mathbb{Z})\cdot(b+m\mathbb{Z})=a\cdot b+m\mathbb{Z}).$$

(可叙述为：同余类之和等于代表元之和所代表的同余类；同余类之积等于代表元之积所代表的同余类. 乘号“·”常可省略不写，即记 $\overline{a}\cdot\overline{b}$ 为 $\overline{a}\,\overline{b}$).

容易验证，这样定义的加法和乘法不受代表元选取的影响. 事实上，设 $\overline{a}=\overline{a'}$，$\overline{b}=\overline{b'}$，则 $a\equiv a'(\mathrm{mod}\ m)$，$b\equiv b'(\mathrm{mod}\ m)$，故 $a'=a+mk$，$b'=b+mj$，从而得

$$\overline{a'+b'}=\overline{(a+mk)+(b+mj)}=\overline{a+b+m(k+j)}=\overline{a+b}.$$

对乘法也类似.

$\mathbb{Z}/m\mathbb{Z}$ 内的加法、乘法运算，性质很好，与整数运算类似. 例如(对任意 $a,b,c\in\mathbb{Z}$)：

$$\overline{a}+\overline{b}=\overline{b}+\overline{a},\quad(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c}),\quad\overline{0}+\overline{a}=\overline{a},\quad\overline{a}+(\overline{-a})=\overline{0},$$

$$\overline{a}\cdot\overline{b}=\overline{b}\cdot\overline{a},\quad(\overline{a}\cdot\overline{b})\cdot\overline{c}=\overline{a}\cdot(\overline{b}\cdot\overline{c}),\quad\overline{1}\cdot\overline{a}=\overline{a}.$$

特别地，因 $\overline{0}+\overline{a}=\overline{a}$，故称 $\overline{0}$为 $\mathbb{Z}/m\mathbb{Z}$ 的**加法单位元**(或**零元**). 因 $\overline{1}\cdot\overline{a}=\overline{a}$，故称 $\overline{1}$ 为**乘法单位元**(或**幺元**). 它们与整数运算中的 0 和 1 角色类似.

由 $\overline{a}+(\overline{-a})=\overline{0}$，可称$(\overline{-a})$为负 $\overline{a}$，即 $(\overline{-a})=-\overline{a}$. 从而可定义$\mathbb{Z}/m\mathbb{Z}$ 中的减法：

$$\overline{b}-\overline{a}=\overline{b}+(\overline{-a})=\overline{b}+\overline{(-a)}=\overline{b-a}.$$

同余类集$\mathbb{Z}/m\mathbb{Z}$ 对上述加法、减法、乘法三种运算是封闭的. 常简记 $\overline{a}+\cdots+\overline{a}$($k$ 个)为 $k\overline{a}$ 或 $k\cdot\overline{a}$，记 $\overline{a}\,\overline{a}\cdots\overline{a}$($k$ 个)为 $\overline{a}^k$.

例 3 $\mathbb{Z}/7\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{6}\}$，$\overline{4}+\overline{5}=\overline{4+5}=\overline{2}$，$\overline{4}-\overline{5}=\overline{4-5}=\overline{6}$，$\overline{3}\cdot\overline{5}=\overline{3\cdot5}=\overline{1}$.

例 4 $\mathbb{Z}/2\mathbb{Z}=\{\overline{0},\overline{1}\}$，其中 $\overline{0}=2\mathbb{Z}=\{2k\mid k\in\mathbb{Z}\}$即偶数集，$\overline{1}=1+2\mathbb{Z}=\{1+2k\mid k\in\mathbb{Z}\}$就是奇数集. $\overline{1}+\overline{1}=\overline{0}$ 即“奇数加奇数为偶数”. 最重要的运算性质是 $\overline{1}+\overline{1}=\overline{0}$，除此之外，$\mathbb{Z}/2\mathbb{Z}$ 中的加法和乘法都与整数相同.

例 5 $\mathbb{Z}/3\mathbb{Z}=\{\overline{0},\overline{1},\overline{2}\}$，其中 $\overline{0}=3\mathbb{Z}=\{3k\mid k\in\mathbb{Z}\}$，$\overline{1}=1+3\mathbb{Z}=\{1+3k\mid k\in\mathbb{Z}\}$，$\overline{2}=2+3\mathbb{Z}=\{2+3k\mid k\in\mathbb{Z}\}$. 最重要的性质是 $\overline{1}+\overline{1}+\overline{1}=\overline{2}+\overline{1}=\overline{0}$，除此之外，加法和乘法都与整数相同.

在$\mathbb{Z}/m\mathbb{Z}$ 中能否做除法呢？首先看 $\overline{1}$ 除以 $\overline{a}$ 可行吗？即 $\overline{1}/\overline{a}$ 有意义吗？(若有意义则称 $\overline{a}$ 可逆). 事实上，有时是不可行的. 例如，$\mathbb{Z}/8\mathbb{Z}$ 中，$\overline{2}$ 不可逆 (即 $\overline{1}/\overline{2}$ 无意义). 否则，由 $\overline{2}\cdot\overline{4}=\overline{0}$，两边都乘以 $\overline{1}/\overline{2}$，得 $\overline{4}=\overline{0}$，即 $8|4$，矛盾.

定义 3 (1) 称 $\overline{a}\in\mathbb{Z}/m\mathbb{Z}$ 是**可逆的**，是指存在 $\overline{x}\in\mathbb{Z}/m\mathbb{Z}$ 使

$$\bar{a}\cdot\bar{x}=\bar{1}\quad(\text{即 } ax\equiv 1(\bmod m)).$$

此时，称 $\bar{x}$ 为 $\bar{a}$ 的（乘法）**逆元**，记为 $\bar{a}^{-1}$（或 $\bar{1}/\bar{a}$）.

（2）$\mathbb{Z}/m\mathbb{Z}$ 中的可逆元集合记为$(\mathbb{Z}/m\mathbb{Z})^*$.$(\mathbb{Z}/m\mathbb{Z})^*$ 中的每个同余类各取一个代表元，这些代表元的集合称为模 m 的一个**既约剩余系**.

例 6　$\mathbb{Z}/8\mathbb{Z}$ 中，$\bar{2},\bar{4},\bar{6}$ 不可逆，$(\mathbb{Z}/8\mathbb{Z})^*=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$，且 $\bar{3}^{-1}=\bar{3},\bar{5}^{-1}=\bar{5},\bar{7}^{-1}=\bar{7}$. 故$\{1,3,5,7\}$是一个既约剩余系.

例 7　$(\mathbb{Z}/4\mathbb{Z})^*=\{\bar{1},\bar{3}\}$. 而 $\bar{3}^{-1}=\bar{3}$. $\{1,3\}$或$\{5,-1\}$都是既约剩余系.

例 8　$\mathbb{Z}/7\mathbb{Z}$ 中的 $\bar{3}$ 是可逆的，因为 $\bar{3}\cdot\bar{5}=\overline{15}=\bar{1}$，故 $\bar{3}^{-1}=\bar{5}$. 又显然 $\bar{2}^{-1}=\bar{4},\bar{6}^{-1}=\bar{6}$. 故$\mathbb{Z}/7\mathbb{Z}$ 中元素除 $\bar{0}$ 之外都是可逆的. 即$(\mathbb{Z}/7\mathbb{Z})^*=\{\bar{1},\bar{2},\cdots,\bar{6}\}$.

定理 1　（1）设 a 为整数，则 $\bar{a}$ 在$\mathbb{Z}/m\mathbb{Z}$ 中是（乘法）可逆的当且仅当 a 与 m 互素. 故 $\mathbb{Z}/m\mathbb{Z}$ 中的可逆元集合恰为

$$(\mathbb{Z}/m\mathbb{Z})^*=\{\bar{a}\mid(a,m)=1,1\leqslant a<m\},$$

即“小于 m 且与 m 互素的正整数”所代表的同余类集.

（2）若 $m=p$ 为素数，则$\mathbb{Z}/p\mathbb{Z}$ 中非 $\bar{0}$ 元素均可逆.

（3）若 m 不是素数，则$\mathbb{Z}/m\mathbb{Z}$ 中存在着非 $\bar{0}$ 不可逆元素.

证明　（1）若$(a,m)=1$，则由辗转相除可得贝祖等式

$$ua+vm=1.$$

模 m 看同余类，得 $\overline{ua+vm}=\bar{1}$，即 $\bar{u}\bar{a}+\bar{v}\bar{m}=\bar{1}$，故 $\bar{u}\bar{a}=\bar{1}$. 故 $\bar{a}$ 可逆，且逆为 $\bar{u}$.

反之，若$(a,m)=d>1$，则 $a(m/d)=(a/d)m\equiv 0(\bmod m)$，即

$$\bar{a}\cdot\overline{(m/d)}=\bar{0}.$$

此时若 $\bar{a}$ 有逆 $\bar{x}$，上式两边都乘以 $\bar{x}$ 得 $\overline{(m/d)}=\bar{0}$，此不可能，因 $0<m/d<m$.

（2）因 $m=p$ 为素数，故 $1,2,\cdots,p-1$ 均与 p 互素，从而 $\bar{1},\bar{2},\cdots,\overline{p-1}$ 均可逆.

（3）若 m 不是素数，必有因子 b 且 $1<b<m$，由(1)知 $\bar{b}$ 不可逆. ■

以 Φ_m 记“小于 m 且与 m 互素的正整数”集合，称为**最小既约剩余系**. 以 $\varphi(m)$ 记 Φ_m 中元素个数，即$\mathbb{Z}/m\mathbb{Z}$ 中可逆元个数. 称 φ 为**欧拉(Euler)函数**.

例如，$\varphi(1)=1$（规定），$\varphi(2)=1,\varphi(3)=2,\varphi(4)=2,\varphi(6)=2$.

定理 2　欧拉函数 $\varphi(m)$的取值由以下等式决定：

（1）$\varphi(p^e)=p^e-p^{e-1}=p^{e-1}(p-1)$　（当 p 为素数）；

（2）$\varphi(mn)=\varphi(m)\varphi(n)$　（当 m,n 为互素正整数）；

（3）设有因子分解 $m=p_1^{e_1}\cdots p_s^{e_s}$（其中 $p_1,\cdots,p_s$ 为互异素数），则

$$\varphi(m)=(p_1^{e_1}-p_1^{e_1-1})\cdots(p_s^{e_s}-p_s^{e_s-1}).$$

证明　(1)“与 p^e 不互素”（即含因子 p）的正整数有 $p,2p,3p,\cdots,p^{e-1}\cdot p$，共计 p^{e-1} 个. 故“与 p^e 互素而小于 p^e”的正整数个数为 p^e-p^{e-1}，即 $\varphi(p^e)$.

(3)是(2)的推论.为证明(2),先证明如下定理.

定理 3 设 m,n 为互素的正整数.记 Φ_m 为模 m 最小既约剩余系.当 x 遍历 Φ_n,y 遍历 Φ_m 时,则 $mx+ny$ 遍历 Φ_{mn}(在模 mn 意义下).特别知

$$\varphi(mn)=\varphi(m)\varphi(n).$$

(此定理形式上可记为 $m\Phi_n+n\Phi_m\equiv\Phi_{mn}$)

证明 (1) $(mx+ny,m)=(ny,m)=1$.同理知 $mx+ny$ 与 n 互素,故与 mn 互素,故属于 Φ_{mn}.

(2) $\{mx+ny\}$ 互不同余(mod mn),因为它们模 m 和模 n 相互都不同余.

(3) 任取 $a\in\Phi_{mn}$,则 a 与 m 互素,故 a 同余于 $n\Phi_m$ 中某元(mod m)(因 $n\Phi_m$ 也是模 m 的一个既约剩余系),故可设 $a\equiv ny\pmod m$,$y\in\Phi_m$.同理得 $a\equiv mx\pmod n$,$x\in\Phi_n$.故 $a\equiv mx+ny$ 对模 m 和模 n 都成立.即知 $a\equiv mx+ny\pmod{mn}$. ■

系 1 $\sum\limits_{d\mid m}\varphi(d)=m$. (求和遍历 m 的正因子 d)

证明 考虑 m 个分数:$1/m,2/m,\cdots,(m-1)/m,m/m$.将它们皆约化为既约分数.约化后分母均为 m 的因子.考虑其中分母为固定 d 的分数 $*/d$ 全体,其分子取遍与 d 互素而不超过 d 的正整数(每个这样的分数 k/d 是由 $k\delta/d\delta$ 约化而来,其中 $d\delta=m$),这样的分数共 $\varphi(d)$ 个.对各个 $d\mid m$ 将 $\varphi(d)$ 求和,则得 m. ■

例如,$m=12$ 时,系 1 的等式为

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)=1+1+2+2+2+4=12.$$

证明中的 m 个分数 $1/m,2/m,\cdots,m/m$ 即是

$$\frac{1}{12},\frac{1}{6},\frac{1}{4},\frac{1}{3},\frac{5}{12},\frac{1}{2},\frac{7}{12},\frac{2}{3},\frac{3}{4},\frac{5}{6},\frac{11}{12},\frac{1}{1}.$$

其中分母为 12 的是 $\varphi(12)=4$ 个,分母为 6 的是 $\varphi(6)=2$ 个,等等.

同余的概念,可推广到多项式集 $F[X]$,例如 $\mathbb{Q}[X]$.固定非零多项式 $m(X)\in F[X]$,对任意 $f(X),g(X)\in F[X]$,如果 $m(X)\mid(f(X)-g(X))$,则称 $f(X)$ 与 $g(X)$ 对于模 $m(X)$ 同余,记为

$$f(X)\equiv g(X)\pmod{m(X)}.$$

这相当于 $f(X)=g(X)+m(X)q(X)$(对某 $q(X)$).例如 $X^3-X^2-1\equiv -X\pmod{(X^2+1)}$.

与 $f(X)$ 同余的多项式都归为一类,记为 $\overline{f(X)}$,称为一个同余类.所有的同余类构成一个新集合(同余类集),记为

$$F[X]/(m(X))=\{\overline{f(X)}\mid f(X)\in F[X]\}.$$

其中元素的加法、乘法定义为:$\overline{f}+\overline{g}=\overline{f+g}$,$\overline{f}\cdot\overline{g}=\overline{f\cdot g}$.

由带余除法,可将同余类集写得更明确简洁:

$$f(X)=m(X)q(X)+r(X),\quad \deg r(X)<\deg m(X)=n$$

$$\overline{f(X)}=\overline{m(X)}\,\overline{q(X)}+\overline{r(X)}=\overline{r(X)}.$$

故同余类集由余式的同余类组成：

$$F[X]/(m(X))=\{\overline{f(X)}\}=\{\overline{r(X)}\}.$$

这类似于 $\mathbb{Z}/(7)=\{\overline{a}\}=\{\overline{r}\}=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{6}\}$.

$\mathbb{Z}/m\mathbb{Z}$ 的许多性质都可平移到 $F[X]/(m(X))$来讨论、推广.

习 题 1.3

1. 详细证明同余式的各项性质.

2. 讨论：(1)$n^2\equiv?\pmod 4$；(2) $n^2\equiv?\pmod 8$；(3) $n^2\equiv?\pmod{16}$.

3. 由整数 n 的十进制表示如何判断：(1)9 整除 n,(2)11 整除 n.

4. 如何判断：(1)13 整除 n,(2)7 整除 n.

5. 在$\mathbb{Z}/7\mathbb{Z}$ 中,求出$\{2^k\},\{3^k\}(k\in\mathbb{Z})$.

6. 在$\mathbb{Z}/8\mathbb{Z}$ 中,求出$\{2^k\},\{6^k\},\{3^k\},\{5^k\},\{7^k\}(k\in\mathbb{Z})$.

7. (1) 在$\mathbb{Z}/12\mathbb{Z}$ 中,哪些元素是可逆的？求它们的逆.

(2) 在$\mathbb{Z}/105\mathbb{Z}$ 中,有多少元素可逆？求 $\overline{23}$ 的逆.

(3) 在$\mathbb{Z}/360\mathbb{Z}$ 中,有多少元素可逆？求 $\overline{77}$ 的逆.

8. 证明：若 $a\equiv b\pmod m$,且 $d\mid a,d\mid b$,则

$$\frac{a}{d}\equiv\frac{b}{d}\left(\bmod\frac{m}{(d,m)}\right).$$

9. 求方程 $167x+23y=1$ 的整数解.

10. 试证明 $x^2+5y^2=3z^2$ 没有非零整数解.

1.4 群 与 例

群,是最基本的,也是最神奇的代数概念.起源于一元多项式方程的研究.天才少年伽罗瓦(Galois)在 19 世纪 30 年代看透实质,引入方程根的对称群,震惊了当时的权威.到现在,群已经“无所不在”.

设 $\mathrm{i}=\sqrt{-1}$,考虑集合

$$G=\{1,\mathrm{i},-1,-\mathrm{i}\}.$$

此集合内的元素之间可进行乘法,而且满足：(1)乘积仍在 G 中(封闭性)；(2)$a(bc)=(ab)c$ 对任意 $a,b,c\in G$ 成立 (结合律)；(3)G 中含有 1,它乘任何元素都不变；(4)G 中的元素都有倒数(称为逆)仍在 G 中.以上 4 条性质将可用一句话概括：$G=\{1,\mathrm{i},-1,-\mathrm{i}\}$对乘法是一个群(group).

再考虑非零实数全体 $\mathbb{R}^*=\mathbb{R}\setminus\{0\}$,其中元素可进行乘法,也满足：(1)封闭性 (即非零实数之积仍为非零实数)；(2)结合律；(3)$\mathbb{R}^*$ 含有 1；(4)$\mathbb{R}^*$ 中元素都有倒数(逆)仍在$\mathbb{R}^*$ 中.故也可用一句话概括为：$\mathbb{R}^*$ 对乘法是一个群.详言之,群的定义如下.

定义 1 一个**群**(**group**)就是一个非空集合 G,且其元素之间有一种运算,此运算将 G 中任意元素 a,b(可以相等)对应于 G 中的一个元素(记为 $a\cdot b$ 或 ab),而且满足如下 4 个条件(称为**群的公理**,group axioms):

(**G1**)(**封闭性**,**closure**) ab 仍然在 G 中(对任意 $a,b\in G$);

(**G2**)(**结合律**,**associativity**) $a(bc)=(ab)c$(对任意 $a,b,c\in G$);

(**G3**)(**存在单位元**,**identity**) 存在元素 $e\in G$ 使 $ea=ae=a$(对任意 $a\in G$);

(**G4**)(**可逆性**,**invertibility**) 对每个元素 $a\in G$,存在 $a'\in G$ 使 $a'a=aa'=e$.

此定义中的群记为$(G,\cdot)$或 G. 因为 a,b 的运算结果写为 $a\cdot b$(或 ab),故此运算也称为乘法运算,也称$(G,\cdot)$为**乘法群**.(此运算是两个元素参与的,故也称为二元运算).

条件(G3)中的 e 称为**单位元**,或**幺元**、恒元,有时也记 e 为 1(注意,虽然有时候记 e 为 1,但它一般不是整数 1,以下有例子说明).

条件(G4)常被概括为"每个元素 $a\in G$ 都可逆",其中的 a' 常记为 a^{-1} 或 $1/a$ 或 $\dfrac{1}{a}$,称为 a 的**逆元**(inverse).

对 $a\in G$,常记 $aa=a^2$,$aaa=a^3$,$a^{-1}a^{-1}=a^{-2}$ 等,记 $a^0=e=1$. 于是 $a^ma^n=a^{m+n}$(对任意整数 m,n).

如果群$(G,\cdot)$在上述 4 个条件之外,还满足第 5 个条件:

(**G5**)(**交换律**,**commutative law**) $ab=ba$(对任意 $a,b\in G$);

则称$(G,\cdot)$为**交换群**,或**阿贝尔群**(Abel 群,abelian group).

群$(G,\cdot)$中的元素个数称为群的**阶**(order),记为$|G|$ 或 $\sharp G$.

例 1 $\{1\}$是 1 阶群(对整数乘法).

例 2 $\{1,-1\}$是 2 阶群(对整数乘法).

例 3 $\{1,\omega,\omega^2\}$ 是 3 阶群(对复数乘法),其中 $\omega=\mathrm{e}^{2\pi\mathrm{i}/3}=-1/2+\mathrm{i}\sqrt{3}/2$,$\mathrm{i}=\sqrt{-1}$. 注意 $\omega^3=1$,$\omega^2=\overline{\omega}=\omega^{-1}$.

例 4 $\{1,\mathrm{i},-1,-\mathrm{i}\}$是 4 阶群,其中 $\mathrm{i}=\sqrt{-1}$. 注意 $\mathrm{i}^2=-1$,$\mathrm{i}^3=-\mathrm{i}$,$\mathrm{i}^4=1$.

例 5 设 $W_n=\{1,\zeta,\zeta^2,\cdots,\zeta^{n-1}\}$为 n 次复单位根集,其中

$$\zeta=\zeta_n=\mathrm{e}^{2\pi\mathrm{i}/n}=\cos(2\pi/n)+\mathrm{i}\sin(2\pi/n).$$

则 W_n 是 n 阶乘法群. 注意 $\zeta^n=1$,且 $\zeta^k\neq1$(对 $1\leqslant k<n$). 例 1~例 4 是此群的特例.

例 6 令 $G=\{(1,1),(1,-1),(-1,1),(-1,-1)\}$,定义$(a,b)(a',b')=(aa',bb')$,则 G 是 4 阶群. 单位元是 $e=(1,1)$(此例说明:单位元可以不是整数 1). 每个元素的平方都等于单位元,所以每个元素的逆也都是自身. G 称为克莱因(Klein)四元群.

例 7 非零实数全体$\mathbb{R}^*=\mathbb{R}\setminus\{0\}$,是乘法群,是无限(阶)群. 同理可知,非零有理数全体$\mathbb{Q}^*=\mathbb{Q}\setminus\{0\}$,非零复数全体$\mathbb{C}^*=\mathbb{C}\setminus\{0\}$,都是无限乘法群.

例 8　令 $G=\{z\in\mathbb{C}:|z|=1\}$，即长度为 1 的复数集合. 此集合在复平面上形成单位圆. 则 G 为乘法群.

例 9　$\mathbb{Z}/m\mathbb{Z}$ 中的可逆元全体 $(\mathbb{Z}/m\mathbb{Z})^*$ 是乘法群，$\varphi(m)$ 阶. 乘法单位元为 $e=\overline{1}$. 例如，$(\mathbb{Z}/4\mathbb{Z})^*=\{\overline{1},\overline{3}\}$ 为二阶群. 而 $(\mathbb{Z}/8\mathbb{Z})^*=\{\overline{1},\overline{3},\overline{5},\overline{7}\}$ 为 4 阶群.

定义 2　设 $(G,\cdot)$ 为(乘法)群，H 是群 G 的子集合，且 $(H,\cdot)$ 是群，则称 H 为 G 的**子群**(subgroup). 记为 $H<G$(也有文献记为 $H\leqslant G$).

注意子群 H 中的运算就是 G 中原来的运算(在 H 上的限制).

要验证 $(H,\cdot)$ 为子群，只需验证 H 对**乘法和求逆封闭**(即只需验证群公理的 G1 和 G4 两条)，因为结合律显然成立，而由求逆封闭知道单位元 $e=aa^{-1}$ 在 H 中. 以后会看到，当 H 为有限集合时，只需验证乘法封闭即可(因为逆可由幂表示).

例如，$\{1,-1\}$ 是 $\{1,\mathrm{i},-1,-\mathrm{i}\}$ 的子群(参见例 2、4). W_3 是 W_6 的子群.

群 G 本身和 $\{1\}$，显然是 G 的子群，称为平凡子群. 常记子群 $\{1\}$ 为 1.

我们可以说，ba^{-1} 是 b 右除以 a，而 $a^{-1}b$ 是 b 左除以 a. 对于阿贝尔群二者一致. 所以可以认为，群是对乘除法封闭的集合.

加法群

对于阿贝尔群(即交换群)G，有时候将运算符号记为加号“+”，从而称 G 为加法群. 这时候，单位元 e 常记为 0，称为零元；a 的逆元记为 $-a$，称为负元. 用这种加法的符号和语言，上述定义 1 可改述为如下(加法群的定义).

定义 1′　一个**加法群**(additive group)就是一个集合 G，且其元素之间有一种运算(称为加法)，此运算将 G 中任意元素 a,b(可以相等)对应于 G 中的一个元素(记为 $a+b$)，且满足如下 5 个条件：

(**A1**)(**封闭性**，**closure**)　$a+b$ 仍然在 G 中(对任意 $a,b\in G$)；

(**A2**)(**结合律**，**associativity**)　$a+(b+c)=(a+b)+c$(对任意 $a,b,c\in G$)；

(**A3**)(**存在单位元**，**identity**)　存在 $e\in G$ 使 $e+a=a+e=a$(对任意 $a\in G$)；

(**A4**)(**可逆性**，**invertibility**)　对任意 $a\in G$ 总存在 $a'\in G$ 使 $a'+a=a+a'=e$.

(**A5**)(**交换律**，**commutative law**)　$a+b=b+a$(对任意 $a,b\in G$ 成立).

此定义中的群记为 $(G,+)$ 或 G. 条件(A3)中的**加法单位元** e 也称为**零元**，常记为 0(注意此 0 不一定是整数 0，不一定属于整数集 $\mathbb{Z}$). 条件 A4 中的 a' 常记为 $-a$，称为 a 的**负元**.

对 $a\in G$，常记 $a+a=2a$，$a+a+a=3a$，$-a-a=2(-a)=-2a$ 等，记 $0a=0$. 于是 $(m+n)a=ma+na$(对任意整数 m,n).

一些加法群的例子如下.

例 10 $\{0\}$ 是 1 阶加法群（对整数加法）.

例 11 整数集$\mathbb{Z}$是加法群（对整数加法）. 偶数集 $2\mathbb{Z}=\{2k\mid k\in\mathbb{Z}\}$是加法群. 对固定的整数 m，集合 $m\mathbb{Z}=\{mk\mid k\in\mathbb{Z}\}$是加法群，是$\mathbb{Z}$ 的子群.

例 12 实数集$\mathbb{R}$ 是加法群. 同理，有理数集$\mathbb{Q}$、复数集$\mathbb{C}$，都是加法群.

例 13 对固定的非零整数 m，模 m 的同余类集合

$$\mathbb{Z}/m\mathbb{Z}=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{m-1}\}$$

是加法群，是 m 阶群. 于是我们有了 2,3,4,…阶加法群：

$$\mathbb{Z}/2\mathbb{Z}=\{\bar{0},\bar{1}\},\quad \mathbb{Z}/3\mathbb{Z}=\{\bar{0},\bar{1},\bar{2}\},\quad \mathbb{Z}/4\mathbb{Z}=\{\bar{0},\bar{1},\bar{2},\bar{4}\},\text{等等.}$$

例 14 已知$\mathbb{Z}/2\mathbb{Z}=\{\bar{0},\bar{1}\}$是加法群. 令 $G=\{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})\}$，定义运算 $(a,b)+(a',b')=(a+a',b+b')$，则 G 是加法群. 零元是$(\bar{0},\bar{0})$.

在加法群 G 中可以定义减法：$a-b=a+(-b)$. 故加法群是对加减法封闭的集合.

设 G 为加法群，H 是其子集合. 若 H 对加法和求负元素封闭，则称 H 为 G 的（加法）子群. G 和$\{0\}$称为平凡子群. 常记子群$\{0\}$为 0.

评述 “群”降临世间的标志事件，是少年伽罗瓦在 1830 年用群彻底解决 5 次以上一元多项式方程根式解这一历史难题，创立神奇的伽罗瓦理论，令权威失措. 新风一扫古希腊以来困扰人类千年的难题迷阵. 1882 年，群的抽象形式确立，仅以 4 条公理衍出五彩缤纷的体系. 带动了环、域、模等系统的创立，推动数学不断向前.

习 题 1.4

1. 求乘法群$\{1,\mathrm{i},-1,-\mathrm{i}\}$的所有子群.

2. 求例 6 中群 G 的所有子群.

3. 求加法群$\mathbb{Z}$的所有子群.

4. 加法群$\mathbb{Z}/4\mathbb{Z}$中有哪些子群？$\mathbb{Z}/6\mathbb{Z}$呢？

5. 设 G 是群，$a,b\in G$，求如下元素的逆：$ab,a^{-1},e,a^{-3},aba^{-1}b^{-1}$.

6. 求例 6 中群 G 的所有元素的逆.

7. 设 G 是一个集合，且其元素之间有一种运算，满足群的定义 1 中的前 3 个条件，则称 G 为**半群**（monoid）或含幺半群. 试举出半群而非群的两个例子.

8. 设 G 为群，S 为非空集合，$M(S,G)$为 S 到 G 的映射全体. 对 $f,g\in M(S,G)$，定义 $fg\in M(S,G)$如下：

$$(fg)(x)=f(x)g(x)\quad(\forall x\in S).$$

试证明 $M(S,G)$是一个群，求单位元 e 和 f^{-1}. 且证明：若 G 为阿贝尔群，则 $M(S,G)$也是阿贝尔群. 若 G 为加法群，$M(S,G)$也为加法群.

9. 设$(G,\cdot)$为乘法群，H 是群 G 的子集合，则 H 为 G 的子群当且仅当 H 对除法封闭（即 $ab^{-1}\in H$ 对任意 $a,b\in H$ 成立）.

*__10.__ 求乘法群 W_n 的所有子群.

1.5　非阿贝尔群例

1.5.1　置换群

定义 1(置换群)　集合 $N=\{1,2,\cdots,n\}$ 到自身的一个**双射**

$$\sigma:\{1,2,\cdots,n\}\longrightarrow\{1,2,\cdots,n\}$$

称为一个 n 级**置换** (permutation). 此置换 σ 常记为

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix},$$

意思是 σ 将 1 映射为 $\sigma(1)$,将 2 映射为 $\sigma(2)$,等等. 显然,n 级置换共有 $n!$ 个,其集合记为 S_n(或 S_N). 例如,当 $n=3$ 时,共有 $3!=6$ 个置换如下:

$$\sigma_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix},\quad \sigma_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},\quad \sigma_3=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix},$$

$$\sigma_4=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix},\quad \sigma_5=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},\quad \sigma_6=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}.$$

从这记号易知,排列与置换之间一一对应,即置换 σ 与排列 $\sigma(1)\sigma(2)\cdots\sigma(n)$ 对应. 例如上述 σ_5 对应于排列 231.

置换的另一种记法为**循环记法**,例如,上述 σ_5 可记为 $\sigma_5=(123)$,意思是 σ_5 映 1 为 2,映 2 为 3,映 3 为 1. 同样知 $\sigma_6=(132)$. 而记上述 $\sigma_2=(12)$,意思是 1 与 2 对换,而 3 不变. 用循环记法,可知 3 级置换集合为

$$S_3=\{(1),(123),(321),(12),(13),(23)\}.$$

将两个数字互换(而其余数字)不变的置换,称为**对换**. 例如,(12)是一个对换,(23)也是.

两个 n 级置换 $\sigma,\tau\in S_n$ 的**乘积** $\tau\sigma$ 由下式定义,仍为 S_n 中的置换:

$$(\tau\sigma)(k)=\tau(\sigma(k))\quad(1\leqslant k\leqslant n)$$

(也记 $\tau\sigma=\tau\circ\sigma$,称为映射的复合(composition)).

例如,S_3 中 $\lambda=(12)$ 和 $\rho=(123)$ 的乘积 $\rho\lambda$,作用到 1 上效果是:

$$((123)(12))1=(123)((12)1)=(123)2=3,$$

即 $(\rho\lambda)1=3$. 同样可知 $(\rho\lambda)2=2$,$(\rho\lambda)3=1$. 综上得 $\rho\lambda=(13)$.

引理 1　n 级置换全体 S_n 对上述乘法运算为群. 当 $n\geqslant 3$ 时,S_n 不是阿贝尔群. (称 S_n 为**对称群** (symmetric group) 或**全置换群**. 恒等映射 $(1)=1$ 是乘法单位元).

证明　乘法封闭性和结合律均显然. 因为任意 $\sigma\in S_n$ 是双射,故有逆,即逆映射. 故

S_n 是群. 当 $n\geqslant 3$ 时，S_n 中含 $\rho=(123)$ 和 $\lambda=(12)$，而

$$\rho\lambda=(123)(12)=(13),\quad \lambda\rho=(12)(123)=(23),$$

知 $\rho\lambda\neq\lambda\rho$，故 S_n 不是阿贝尔群. 特别可知，S_3 是 6 阶非阿贝尔群. ■

我们可以列出 S_3 的“乘法表”(如表 1.5.1 所示)，其中“以 σ_i 为首的行”与“以 σ_j 为首的列”的交叉位置填写 $\sigma_i\sigma_j$.

表 1.5.1 S_3 的乘法表

	1	(123)	(321)	(12)	(13)	(23)
1	1	(123)	(321)	(12)	(13)	(23)
(123)	(123)	(321)	1	(13)	(23)	(12)
(321)	(321)	1	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	1	(321)	(123)
(13)	(13)	(12)	(23)	(123)	1	(321)
(23)	(23)	(13)	(12)	(321)	(123)	1

记 $\lambda=(12)$，$\rho=(123)$. 易知 $\lambda^2=1$，$\rho^3=1$. 故 $\lambda^{-1}=\lambda$，$\rho^{-1}=\rho^2=(132)$. 而且由 $(12)(123)(12)=(132)$，可知 $\lambda\rho\lambda=\rho^2$，即

$$\lambda\rho=\rho^2\lambda.$$

此式说明，ρ,λ 不可交换，但 ρ 可“穿过”λ 而变为 ρ^2. 基于此式，ρ,λ 的任何次序的乘积都可表示为 $\rho^i\lambda^j$ ($i=0,1,2$; $j=0,1$). 所以 S_3 中的元素可写为

$$S_3=\{1,\rho,\rho^2,\lambda,\rho\lambda,\rho^2\lambda\}.$$

由此，S_3 的乘法表可列成如表 1.5.2.

表 1.5.2 S_3 的乘法表——符号写法 ($\rho=(123)$，$\lambda=(12)$)

	1	ρ	ρ^2	λ	$\rho\lambda$	$\rho^2\lambda$
1	1	ρ	ρ^2	λ	$\rho\lambda$	$\rho^2\lambda$
ρ	ρ	ρ^2	1	$\rho\lambda$	$\rho^2\lambda$	λ
ρ^2	ρ^2	1	ρ	$\rho^2\lambda$	λ	$\rho\lambda$
λ	λ	$\rho^2\lambda$	$\rho\lambda$	1	ρ^2	ρ
$\rho\lambda$	$\rho\lambda$	λ	$\rho^2\lambda$	ρ	1	ρ^2
$\rho^2\lambda$	$\rho^2\lambda$	$\rho\lambda$	λ	ρ^2	ρ	1

再如，S_4 是 24 阶群，不可交换.

1.5.2 可逆方阵群

如下表达式称为一个 2 阶实方阵(也简称方阵,或矩阵):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(其中 a,b,c,d 为实数,称为此方阵的系数或分量). 2 阶实方阵的集合记为 $M_2(\mathbb{R})$. 两个方阵的乘积定义为

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}=\begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix}.$$

容易验证,这种乘法满足结合律,但是不满足交换律,例如:

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ 不等于 } \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}.$$

方阵 $\boldsymbol{I}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 称为**单位方阵**,有性质:$\boldsymbol{IA}=\boldsymbol{AI}=\boldsymbol{A}$(对任意 $\boldsymbol{A}\in M_2(\mathbb{R})$).

对任意 $\boldsymbol{A}\in M_2(\mathbb{R})$,如果存在 $\boldsymbol{B}\in M_2(\mathbb{R})$ 使得

$$\boldsymbol{AB}=\boldsymbol{BA}=\boldsymbol{I},$$

则称 $\boldsymbol{A}$ 为**可逆**方阵. 称 $\boldsymbol{B}$ 为 $\boldsymbol{A}$ 的逆,记为 $\boldsymbol{B}=\boldsymbol{A}^{-1}$.

对方阵 $\boldsymbol{A}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$,记 $|\boldsymbol{A}|=ad-bc$,称为 $\boldsymbol{A}$ 的**行列式**(也记为 $\det \boldsymbol{A}$). 对两个 2 阶方阵 $\boldsymbol{A},\boldsymbol{B}$,容易验证 $|\boldsymbol{AB}|=|\boldsymbol{A}||\boldsymbol{B}|$.

易知:当且仅当行列式 $|\boldsymbol{A}|$ 非零时 $\boldsymbol{A}$ 可逆. 事实上,若 $|\boldsymbol{A}|$ 非零,则可构作方阵

$$\boldsymbol{A}'=\begin{pmatrix} d/|\boldsymbol{A}| & -b/|\boldsymbol{A}| \\ -c/|\boldsymbol{A}| & a/|\boldsymbol{A}| \end{pmatrix}.$$

直接计算可验证 $\boldsymbol{AA}'=\boldsymbol{A}'\boldsymbol{A}=\boldsymbol{I}$,故 $\boldsymbol{A}$ 可逆,且 $\boldsymbol{A}'$ 就是逆. 反之,若 $\boldsymbol{A}$ 可逆,设 $\boldsymbol{AB}=\boldsymbol{BA}=\boldsymbol{I}$,则 $|\boldsymbol{A}||\boldsymbol{B}|=|\boldsymbol{AB}|=|\boldsymbol{I}|=1$,故 $|\boldsymbol{A}|\neq 0$.

于是知道,可逆方阵之积仍为可逆方阵. 故可逆方阵全体构成一个群.

引理 2 记 $G_2(\mathbb{R})$ 为可逆的 2 阶实方阵集,则 $G_2(\mathbb{R})$ 对矩阵乘法是群,不是阿贝尔群.

现在考虑系数属于 $\mathbb{Z}/2\mathbb{Z}$ 的 2 阶方阵集合 $M_2(\mathbb{Z}/2\mathbb{Z})$(为符号简便,我们记 $\mathbb{Z}/2\mathbb{Z}=\{0,1\}$. 即省去横线而记 $\bar{0},\bar{1}$ 为 0,1. 此时注意,1 不是整数,$1+1=0$). 此时,方阵的每个系数取值为 0 或 1,故共有 $2^4=16$ 个可能的方阵. 行列式 $ad-bc\neq 0$ 相当于 $ad\neq bc$,故有两种情形:(1)$ad=1$ 而 $bc=0$;(2)$ad=0$ 而 $bc=1$. 注意 $ad=1$ 恰当 $a=d=1$,故在此情形下,可逆方阵全体如下,是 6 阶乘法群: