抽象代数

Abstract Algebra

陈　银/编著

科学出版社

抽 象 代 数

陈 银 编著

科 学 出 版 社

北 京

内 容 简 介

本书主要介绍普通高等学校数学专业本科生必修课“近世代数”或“抽象代数”的基础内容. 全书共三章, 分别介绍群论、环论及域论的内容. 第 1 章主要包括群的概念及例子、子群及商群、群同态基本定理、Lagrange 定理、指数定理、自同构群、Cayley 定理、群在集合上的作用、Sylow 的三大定理、幂零群和可解群、有限生成 Abel 群及群的表出等; 第 2 章主要包括环的基本性质、环同态基本定理、中国剩余定理、素理想、分式化、唯一因子分解整环、多项式环及代数不变量理论的简单介绍; 第 3 章主要包括是域扩张、任意域上的向量空间、代数扩张、有限域、域的自同构、Galois 群、Galois 扩张、Galois 基本定理及应用的介绍. 本书引入代数学计算工具 Magma 作为主要的辅助计算工具, 大大节约了师生手工计算的时间.

本书可作为综合性大学、师范类大学和理工科院校数学专业本科生的近世代数或抽象代数课程的教材, 也可作为其他数学工作者或科技工作者的参考书.

图书在版编目(CIP)数据

抽象代数/陈银编著. —北京: 科学出版社, 2019.6

ISBN 978-7-03-059416-7

Ⅰ. ①抽… Ⅱ. ①陈… Ⅲ. ①抽象代数 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字 (2018) 第 253805 号

责任编辑: 李静科 孙翠勤 / 责任校对: 邹慧卿

责任印制: 吴兆东 / 封面设计: 无极书装

科学出版社出版

北京东黄城根北街 16 号

邮政编码: 100717

http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2019 年 6 月第 一 版 开本: 720 × 1000 1/16

2019 年 6 月第一次印刷 印张: 8

字数: 161 000

定价: 48.00 元

(如有印装质量问题, 我社负责调换)

序　　言

该书是作者自 2009 年以来至今讲授近世代数课程的教学经验和心得的结晶, 有很多独到的科学见解. 由于按照数学的思维方式讲课, 因此作者把深奥难懂的抽象代数讲得通俗易懂. 本书内容包括: 群论 (主线为群同态, 讲了群在集合上的作用, Sylow 定理, 有限生成 Abel 群的同构分类等), 环论 (主线为理想, 讲了素理想, 极大理想, 欧几里得整环, 主理想整环, 唯一因子分解整环, 对称多项式及不变量理论等) 和域论 (主线为域扩张, 讲了域扩张的途径, 域扩张的性质, 域扩张的自同构群, 伽罗瓦扩张, 伽罗瓦理论的基本定理等). 本书在每节末附有习题, 非常适合作为本科生学习的教材.

该书的亮点之一是引入了功能强大的代数学计算软件 Magma 作为辅助的计算工具. 每两节后面都附有 Magma 的计算实例, 这些计算实例可以通过 Magma 的免费网上计算器进行验证. 据我所知, 大多数传统的 "近世代数" 中文教材并没有相关的介绍. 但自进入二十一世纪以来, 计算机强大的计算能力对现代代数学里许多分支的教学和科研的影响越来越大; 不仅加快了一些新兴交叉学科的快速发展 (如计算代数几何), 而且对一些经典领域注入了新的活力 (如代数不变量理论). 因此, 掌握某种计算软件, 对现代代数学的学习和研究都是非常有帮助的.

该书同时也注重重要问题和经典研究领域的介绍. 例如, 在本书第 1 章群论里作者谈到了有限群的极小忠实置换表示的维数问题. 这个问题可以推广到有限群或者李代数的线性表示的表示维数, 后者是现代代数学研究里比较活跃的研究主题. 在第 2 章环论里作者介绍了代数不变量理论 (Hilbert 第 14 问题就是关于该理论的), 它是对称多项式理论的自然扩充. 在第 3 章域论里作者介绍了经典的 Galois 理论及其在有理性问题 (Noether 问题) 中的应用.

该书集作者在代数不变量方面近十年科研和教学的心得所成, 此书写得既简单又明瞭. 近世代数因涉及的数学基础广泛, 因而写书时常常会因要明瞭而篇幅庞大, 要简单而又不忽略重要的内容实属不易. 本书不仅能做到这一点, 而且以丰富的例子使得传统意义上的抽象代数不再抽象. 我相信此书对我国大学生的代数基础的培养是非常有帮助的, 希望将来能成为国家优秀教材.

杜　荣

华东师范大学数学科学学院

2019 年 2 月

前　言

自 2009 年秋季学期起, 作者开始在东北师范大学数学与统计学院讲授“近世代数”课程. 刚开始的时候, 由于缺乏教学经验, 每学期作者都会重新撰写或修订授课讲义, 以便及时发现自身的教学不足并更好地完成教学任务. 本书是由这些讲义整理而成的, 其主要目的是为了数学系二年级本科生通过一个学期的学习就能大致了解“抽象代数”的基本概念和思想方法. 根据教学大纲的安排, 东北师范大学的秋季学期教学时间为二十周左右; 除去考试周及国家法定节假日, 实际的课堂授课时间为十七八周. 因此, 本书总共 34 节, 差不多每周两节的教学内容; 习题的编排上也基本上是按照两节内容附带一次习题.

本书的亮点之一是引入了功能强大的代数学计算软件 Magma 作为辅助计算工具. 每两节后面都附有 Magma 的计算实例, 这些计算实例可以通过 Magma 的免费网上计算器进行验证. 据作者所知, 大多数传统的“近世代数”中文教材并没有相关的介绍. 但进入二十一世纪以来, 计算机强大的计算能力对现代代数学里许多分支的教学和科研的影响越来越大, 不仅加快了一些新兴交叉学科的快速发展 (如计算代数几何), 而且对一些经典领域注入了新的活力 (如代数不变量理论). 其他的代数学计算软件还有: CoCoA、Macaulay2 及 GAP 等. 熟练掌握这些计算软件中的至少一种, 对现代代数学的学习和研究都是非常有帮助的.

本书也注重重要问题和经典研究领域的介绍, 经典的研究问题和结果总是能吸引广大数学工作者的注意. 例如, 第 1 章群论里谈到了有限群的极小忠实置换表示的维数问题, 这个问题可以推广到有限群或者李代数的线性表示的表示维数, 后者是现代代数学研究里比较活跃的研究主题. 第 2 章环论里介绍了代数不变量理论 (Hilbert 第 14 问题就是关于该理论的), 它是对称多项式理论的自然的扩充. 第 3 章域论介绍了经典的 Galois 理论及在有理性问题 (Noether 问题) 中的应用.

根据作者的教学经验, 一名普通的本科生想要学好“抽象代数”并不是一件容易的事情. 除了要重视现代计算机技术外, 经典代数学教材的刻苦钻研和广泛的阅读更是一个必经的过程. 国内外有许多经典的本科生及研究生代数学教材可供参考和后续学习, 如 [Art91], [DF04], [Fra67], [Jac75a, Jac75b, Jac75c], [Hun80], [Lan02] 及 [Rot02]. 另外, 做练习题和阅读维基百科上相关内容也是学习过程的一个重要的环节, 本书配备了适量的习题; 众多国内专家撰写的中文教材里包含了大量习题, 同时也有专门的中文版习题集供初学者学习.

本书的出版得到了国家自然科学基金 (No: 201114181) 及东北师范大学数学

与统计学院的支持. 特别感谢东北师范大学陶剑教授 (已故) 对我工作的帮助. 感谢加拿大皇家军事学院 David L. Wehlau 教授、南开大学白承铭教授、华东师范大学杜荣教授的长期支持. 感谢我的学生陈天恩、刘俊琰、任珊等指出初稿中的打印错误.

由于作者才疏识浅, 书中若有遗漏之处, 还望广大读者批评指正.

最后, 谨以此书祝贺我的母亲叶华英女士六十岁生日及我的长女 Emmy 六岁生日.

陈　银

2019 年 2 月于重庆

目　　录

第 1 章　群

1.1　集合与映射

1.1.1　集合

本书约定以下集合的符号:

$$\mathbb{N} := \{0, 1, 2, 3, \cdots\};$$

$$\mathbb{N}^+ := \{1, 2, 3, \cdots\};$$

$$\mathbb{Z} := \text{全体整数之集};$$

$$\mathbb{Q} := \text{全体有理数之集};$$

$$\mathbb{R} := \text{全体实数之集};$$

$$\mathbb{C} := \text{全体复数之集};$$

$$\widetilde{n} := \{1, 2, \cdots, n\};$$

$$A^\times := A \setminus \{0\}, \text{即 } A \text{ 中全体非零元素之集}.$$

定义 1.1.1　给定两个集合 A 及 B, 集合 $A \cap B = \{x \mid x \in A \text{ 且 } x \in B\}$ 称为 A 与 B 的**交集**; 集合 $A \cup B = \{x \mid x \in A \text{ 或 } x \in B\}$ 称为 A 与 B 的**并集**; 集合

$$A \times B := \{(x, y) \mid x \in A, y \in B\}$$

称为 A 与 B 的**笛卡儿积**. 定义 $A \setminus B := \{x \in A \mid x \notin B\}$, 称为 B 在 A 中的**差**.

定义 1.1.2　我们用 $|A|$ 表示集合 A 的**基数**或**阶数**. 若 $|A| \in \mathbb{N}$, 称 A 是一个**有限集**; 否则称 A 是一个**无限集**. 特别地, 当 $|A| = 0$, 我们称 A 为**空集**, 以 $A = \varnothing$ 表示之.

注记 1.1.3　一个集合的基数是一个复杂的概念. 若集合 A 是一个有限集, 那么基数 $|A|$ 可以理解为 A 中元素的个数; 若 A 是一个无限集, 基数 $|A|$ 就不能简单地理解为元素的个数, 它需要更加精准的定义. 例如, 虽然 $\mathbb{Q}$ 及 $\mathbb{R}$ 都是无限集, 但是 $|\mathbb{Q}| < |\mathbb{R}|$ (严格小于). 集合论里的**连续统假设**断言: 并不存在集合 A 满足 $|\mathbb{Q}| < |A| < |\mathbb{R}|$; 见 [Hun80], 引言第 8 节.

1.1.2　映射

定义 1.1.4　令 $f : A \longrightarrow B$ 是非空集合 A, B 间的映射. 集合

$$\mathrm{im}(f) = \{f(a) \mid a \in A\} =: f(A)$$

称为 f 的**像**, 它是 B 的一个非空子集. 对于任意子集 $C \subseteq B$, 集合

$$f^{-1}(C) := \{a \in A \mid f(a) \in C\}$$

称为 C 的**原像**, 它是 A 的子集. 特别地, 如果 $C = \{b\}$ 只包含一个元素 b, 则通常用 $f^{-1}(b)$ 代替 $f^{-1}(\{b\})$.

定义 1.1.5　如果映射 $f : A \longrightarrow B$ 满足 $B = \mathrm{im}(f)$, 则称 f 为**满射**; 等价地, f 是满射 $\iff$ 对于任意元素 $b \in B$, 有 $f^{-1}(b) \neq \varnothing$.

如果映射 $f : A \longrightarrow B$ 满足: $a_1 \neq a_2 \in A \Longrightarrow f(a_1) \neq f(a_2)$, 则称之为**单射**; 等价地, f 是单射 $\iff$ 对于任意的元素 $a_1, a_2 \in A$, 若 $f(a_1) = f(a_2)$, 则 $a_1 = a_2$.

如果映射 $f : A \longrightarrow B$ 既是单射又是满射, 则称之为**双射**. 两个非空集合 A, B 被称为是**同构**的, 表示为 $A \cong B$, 如果它们之间存在一个双射 $f : A \longrightarrow B$.

我们称两个映射 $f, g : A \longrightarrow B$ **相等**, 表示为 $f = g$, 若对于任意的 $a \in A$, 有 $f(a) = g(a)$.

对于任一的集合 A, 映射 $1_A : A \longrightarrow A, (a \mapsto a)$ 称为 A 上的**恒等映射**; 它是一个双射.

注记 1.1.6　集合论的目的之一就是在集合同构的意义下对所有的集合进行分类. 也就是说, 在集合论里, 两个同构的集合被看作是“一样”的. 例如, $A = \{a, b, c, d\}$ 与 $B = \{1, 2, 3, 4\}$, 作为集合被看作没有本质区别.

以下定理说明: 集合的基数是集合同构的唯一的全系不变量; 其严格的证明 (特别是无限集的时候) 超出了本课程的内容; 见 [Hun80], 引言第 8 节, 第 16 页.

定理 1.1.7　两个集合 A, B 同构的充分必要条件是 $|A| = |B|$.

例 1.1.8　证明 $\mathbb{N}^+ \cong \mathbb{N}$. 事实上, 令 $f : \mathbb{N}^+ \longrightarrow \mathbb{N}(x \mapsto x - 1)$. 只需要证明 f 是双射. 对任一 $x \in \mathbb{N}$, 有 $x + 1 \in \mathbb{N}^+$ 及 $f(x + 1) = (x + 1) - 1 = x$, 所以 f 是满射. 若 $x_1 \neq x_2 \in \mathbb{N}^+$, 则 $f(x_1) = x_1 - 1 \neq x_2 - 1 = f(x_2)$, 所以 f 是单射.

我们通常用符号 $\mathrm{Hom}(A, B)$ 表示从集合 A 到集合 B 的全体映射之集.

1.1.3　映射的复合

定义 1.1.9　令 $f \in \mathrm{Hom}(A, B), g \in \mathrm{Hom}(B, C)$ 是两个映射. 映射

$$g \circ f : A \longrightarrow C, \quad a \mapsto g(f(a))$$

称作 g **复合**上 f.

令 $h \in \mathrm{Hom}(C, D)$ 是任一映射, 则有

命题 1.1.10 $h \circ (g \circ f) = (h \circ g) \circ f$.

证明 令 $x \in A$ 是任一元素, 那么 $\Big(h\circ(g\circ f)\Big)(x) = h\Big((g\circ f)(x)\Big) = h\Big(g(f(x))\Big)$ 及 $\Big((h \circ g) \circ f\Big)(x) = (h \circ g)(f(x)) = h\Big(g(f(x))\Big)$. 所以, $h \circ (g \circ f) = (h \circ g) \circ f$. □

命题 1.1.11 令 $f : A \longrightarrow B$ 是一个映射.

1. f 是单射的充分必要条件是它有一个**左逆映射** $g : B \longrightarrow A$ 使得 $g \circ f = 1_A$.

2. f 是满射的充分必要条件是它有一个**右逆映射** $g : B \longrightarrow A$ 使得 $f \circ g = 1_B$.

证明 1. ($\Longrightarrow$) 我们需要定义映射 $g : B \longrightarrow A$. 因为 $A \neq \varnothing$, 所以可以选择一个元素 $a \in A$. 将集合 B 写成子集的并: $B = \mathrm{im}(f) \cup (B \setminus \mathrm{im}(f))$. 由于 f 是单射, 所以 $f : A \longrightarrow \mathrm{im}(f)$ 是双射, 即 A 中的元素与 $\mathrm{im}(f)$ 中的元素有一一对应的关系. 现定义映射 g:

$$g(y) := \begin{cases} x, & y = f(x) \in \mathrm{im}(f), \\ a, & y \in B \setminus \mathrm{im}(f). \end{cases}$$

我们发现, 对于任一的 $x \in A$, $(g\circ f)(x) = g(f(x)) = g(y) = x = 1_A(x)$, 即 $g\circ f = 1_A$.

($\Longleftarrow$) 对任意 $x_1, x_2 \in A$, 若 $f(x_1) = f(x_2)$, 那么 $x_1 = 1_A(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = 1_A(x_2) = x_2$. 所以 f 是单射.

2. ($\Longrightarrow$) 对任一元素 $y \in B$, 因为 f 是满射, 所以 $f^{-1}(y) \neq \varnothing$. 选择一个元素 $a_y \in f^{-1}(y)$ 并定义 $g(y) := a_y$. 那么 $(f \circ g)(y) = f(g(y)) = f(a_y) = y = 1_B(y)$, 即 $f \circ g = 1_B$. (注意: 这里 g 的定义并不是唯一的.)

($\Longleftarrow$) 对任一 $y \in B$, 因为 $f \circ g = 1_B$, 所以 $y = 1_B(y) = (f \circ g)(y) = f(g(y)) \in \mathrm{im}(f)$, 即 $B \subseteq \mathrm{im}(f)$. 又因为 $\mathrm{im}(f) \subseteq B$, 所以 $B = \mathrm{im}(f)$, 即 f 是满射. □

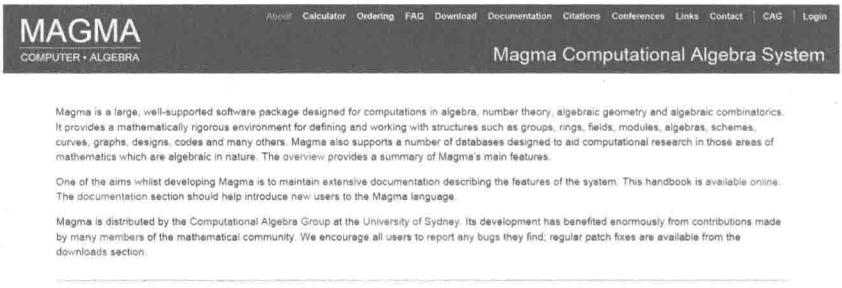
命题 1.1.12 令 $f : A \longrightarrow B$ 是一个双射. 设 g 是 f 的一个左逆映射, g' 是 f 的一个右逆映射. 则 $g = g'$, 称为 f 的一个**逆映射**. 更多地, 若 g_1 及 g_2 都是 f 的逆映射, 同样的方法可证 $g_1 = g_2$; 这意味着双射 f 的逆映射是唯一的, 以 f^{-1} 表示之.

证明 因为 $g \circ f = 1_A$ 及 $f \circ g' = 1_B$, 所以对任一 $y \in B$, $g'(y) = 1_A(g'(y)) = (g \circ f)(g'(y)) = (g \circ f \circ g')(y) = (g \circ 1_B)(y) = g(y)$. 因此 $g = g'$. □

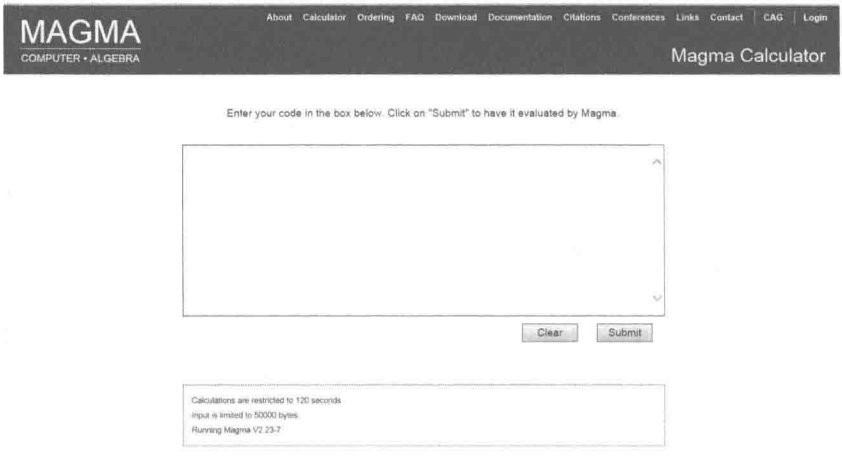
1.1.4 Magma

Magma 计算代数系统是澳大利亚悉尼大学开发的一款功能强大的代数学计算软件, 它可以用来计算代数学及其相关学科中的诸多代数问题, 现已成为现代代数

学工作者重要的辅助研究工具. Magma 的网址为：http://magma.maths.usyd.edu.au/magma/.



本课程将以 Magma 作为主要的辅助计算工具. 上述在线网站提供不超过 120 秒的免费计算器, 基本上足够本课程的教学要求.



1.2　等价关系及群的定义

1.2.1　等价关系

令 A 是一个非空集合, 集合 $A \times A = \{(x, y) \mid x, y \in A\}$ 表示 A 与自身的笛卡儿积.

定义 1.2.1　令 $\mathcal{R} \subseteq A \times A$ 是一个非空子集. 如果对任意的 $x, y, z \in A$, $\mathcal{R}$ 满足以下三个条件:

1. (**自反性**) $(x, x) \in \mathcal{R}$;
2. (**对称性**) 若 $(x, y) \in \mathcal{R}$, 则 $(y, x) \in \mathcal{R}$;

3. (**传递性**) 若 $(x,y)\in\mathcal{R}$ 且 $(y,z)\in\mathcal{R}$, 则 $(x,z)\in\mathcal{R}$.

则称 $\mathcal{R}$ 是 A 上的一个**等价关系**.

假设 $\mathcal{R}$ 是 A 上的一个等价关系, $x,y\in A$ 是两个元素. 若 $(x,y)\in\mathcal{R}$, 则称 x 和 y 是**等价**的, 表示成 $x\sim y$. 上述"等价关系"的定义中的三个条件可以重写为:

1. (自反性) $x\sim x$;

2. (对称性) $x\sim y\Longrightarrow y\sim x$;

3. (传递性) $x\sim y$ 及 $y\sim z\Longrightarrow x\sim z$.

例 1.2.2 子集 $\mathcal{R}:=\{(x,y)\in\mathbb{C}\times\mathbb{C}\mid |x|=|y|\}$ 是复数域 $\mathbb{C}$ 上的一个等价关系, 即对于 $x,y\in\mathbb{C}$, $x\sim y\iff$ 它们的模相等.

例 1.2.3 考虑整数环 $\mathbb{Z}$ 及一个固定的 $m\in\mathbb{N}^+$. 子集

$$\mathcal{R}:=\{(x,y)\in\mathbb{Z}\times\mathbb{Z}\mid x\equiv y \mod m\}$$

是 $\mathbb{Z}$ 上的一个等价关系; 即对于 $x,y\in\mathbb{Z}$, $x\sim y\iff x-y$ 可以被 m 整除.

定义 1.2.4 令 $\mathcal{R}$ (或 $\sim$) 是集合 A 上的一个等价关系. 对于任一元素 $x\in A$, 子集

$$\overline{x}:=\{y\in A\mid (x,y)\in\mathcal{R}\}=\{y\in A\mid x\sim y\}$$

称为 x 所在的**等价类**. 全体等价类之集

$$A/\mathcal{R}=\overline{A}:=\{\overline{x}\mid x\in A\}$$

被称作 A 关于等价关系 $\mathcal{R}$ 的**商集**.

命题 1.2.5 令 $\sim$ 是集合 A 上的一个等价关系, $x,y\in A$. 则

1. $\overline{x}=\overline{y}\iff x\sim y$;

2. 若 x 和 y 不等价, 则 $\overline{x}\cap\overline{y}=\varnothing$;

3. $A=\cup_{x\in A}\overline{x}=\cup_{\overline{x}\in\overline{A}}\overline{x}$;

4. 映射 $\pi: A\longrightarrow\overline{A}, (x\mapsto\overline{x})$ 是一个满射, 称为**标准的**满射.

证明 1. 由自反性, 有 $y\in\overline{y}$. 若 $\overline{x}=\overline{y}$, 那么 $y\in\overline{x}$, 即 $x\sim y$. 反之, 若 $x\sim y$, 那么对于任一 $x'\in\overline{x}$, 有 $x'\sim x\sim y$. 因此 $x'\in\overline{y}$, 所以 $\overline{x}\subseteq\overline{y}$. 相似地证明, $\overline{y}\subseteq\overline{x}$. 因此 $\overline{x}=\overline{y}$.

2. 假设存在一个元素 $z\in\overline{x}\cap\overline{y}$. 那么 $x\sim z\sim y$, 矛盾.

3. 首先证明 $A=\cup_{x\in A}\overline{x}$. 因为对任一的 $x\in A$, 有 $\overline{x}\subseteq A$, 所以 $\cup_{x\in A}\overline{x}\subseteq A$. 反之, 对任一的 $x\in A$, 因为 $x\in\overline{x}$, 所以 $A\subseteq\cup_{x\in A}\overline{x}$. 相同的证法可得, $A=\cup_{\overline{x}\in\overline{A}}\overline{x}$.

4. 为证 π 是满射, 只需证对于任一的 $\overline{x} \in \overline{A}$, $\pi^{-1}(\overline{x}) \neq \varnothing$. 这是显然的, 因为 $\pi(x) = \overline{x}$, 所以 $x \in \pi^{-1}(\overline{x}) \neq \varnothing$. □

1.2.2　分拆

定义 1.2.6　令 $A \neq \varnothing$ 是一个集合且 $\{A_i \mid i \in I\}$ 是 A 的非空子集族. 若

1. $A = \cup_{i \in I} A_i$;
2. $A_i \cap A_j = \varnothing, \forall i \neq j \in I$.

则称 $\{A_i \mid i \in I\}$ 为 A 的一个**分拆**(partition).

假设 $\sim$ 是集合 A 上的一个等价关系. 在每一个等价类里任意选择一个元素(称为**代表元**) 出来组成一个集合 T; 集合 T 被称为**代表元集**. 例如, 在例 1.2.3 中, 令 $m = 6$. 那么商集为 $\overline{\mathbb{Z}} = \{\overline{0}, \overline{1}, \cdots, \overline{5}\}$, 而 $T_1 = \{0, 1, \cdots, 5\}$ 是一个代表元集; $T_2 = \{6, 1, 8, 3, 10, 5\}$ 也可以作为一个代表元集. 由命题 1.2.5 知道, 对于任一非空集合 A, 给定一个等价关系 $\sim$, 对应的商集 $\overline{A} = \{\overline{x} \mid x \in T\}$ 构成 A 的一个分拆. 反之, 有

命题 1.2.7　令 $\{A_i \mid i \in I\}$ 是非空集合 A 的一个分拆. 则下面的关系

$$\mathcal{R} := \{(x, y) \in A \times A \mid \text{存在某个 } i \in I \text{ 使得 } x, y \in A_i\}$$

是 A 上的一个等价关系.

证明　已知对任一 $x \in A = \cup_{i \in I} A_i$, 存在某个 $i \in I$ 使得 $x \in A_i$, 所以 $(x, x) \in \mathcal{R}$. 另外, 由 $(x, y) \in \mathcal{R}$ 推出 $x, y \in$ 某个 A_i, 所以 $(y, x) \in \mathcal{R}$. 最后, $(x, y) \in \mathcal{R}$ 意味着 $x, y \in$ 某个 A_i; $(y, z) \in \mathcal{R}$ 意味着 $y, z \in$ 某个 A_j. 所以 $y \in A_i \cap A_j$. 如果 $i \neq j$, 有 $A_i \cap A_j = \varnothing$, 所以 $i = j$. 因此, $(x, z) \in \mathcal{R}$. □

Magma 的应用

正整数 $n \in \mathbb{N}^+$ 的一个**分拆**是指一个下降的正整数列 $[n_1, n_2, \cdots, n_k]$ 使得 $n = \sum_{i=1}^{k} n_i$. 例如, 当 $n = 3$ 时, 所有的分拆为: $[3], [2, 1], [1, 1, 1]$; 当 $n = 4$ 时, 所有的分拆为: $[4], [3, 1], [2, 2], [2, 1, 1], [1, 1, 1, 1]$. 用 $p(n)$ 表示 n 的分拆的个数. 通常来讲, n 越大, 要得出 n 的所有分拆或者 $p(n)$ 就越难.

Magma 可以用来计算正整数 $n \in \mathbb{N}^+$ 的分拆的个数 $p(n)$ 及全部分拆. 例如:

```
n:=2018;
p:=NumberOfPartitions(n);
p;
```

输出结果为

```
783128900535895315634465488801349863833971169 2
```

上面的计算意味着:

$$p(2018) = 783128900535895315634465488801349863833971169 2.$$

1.2.3 群的定义

定义 1.2.8 令 $(S,*)$ 是一个带有二元运算 $*: S\times S \longrightarrow S((x,y)\mapsto x*y)$ 的非空集合 (二元运算 $*$ 被称为 S 的**乘法运算**). 若 $(S,*)$ 满足以下结合性:

$$(x*y)*z = x*(y*z), \qquad \text{(结合性)}$$

这里 $x,y,z\in S$ 是任意元素, 则称 $(S,*)$ 是一个**半群**.

例如, $(\mathbb{N}^+,+)$ 及 $(\mathbb{Z},\times)$ 分别关于通常的加法和乘法是半群.

定义 1.2.9 若半群 $(S,*)$ 里存在一个元素 $1_S\in S$ 满足以下性质: 对于任一的 $x\in S$,

$$1_S * x = x * 1_S = x, \qquad \text{(幺元)}$$

则称 $(S,*)$ 为一个**幺半群**, 其中 1_S 称为**幺元**.

例如, $(\mathbb{N},+)$ 是幺半群, 但是 $(\mathbb{N}^+,+)$ 不是幺半群.

注记 1.2.10 幺半群里的幺元是唯一的. 事实上, 若 $a,1_S$ 都是幺半群 S 里的幺元, 则 $a = 1_S * a = 1_S$.

定义 1.2.11 若幺半群 $(G,*)$ 满足以下性质: 对于任一的元素 $x\in G$, 存在一个元素 $x^{-1}\in G$ 使得

$$x^{-1} * x = x * x^{-1} = 1_G, \qquad \text{(逆元)}$$

则称 $(G,*)$ 为一个**群**, 其中 x^{-1} 称为元素 x 的**逆元**.

例如, $(\mathbb{Z},+)$ 是一个群, 但是 $(\mathbb{Z},\times)$ 并不是群.

注记 1.2.12 以后在不导致歧义的前提下, 我们通常省略掉幺半群 $(S,*)$ 里的符号 $*$, 简写成 S; 半群 S 中两个元素 x,y 的二元运算 $x*y$ 也简写成 xy; 通常我们也用 1 代替 1_S 来表示幺半群 S 的幺元.

命题 1.2.13 令 G 是群, $x\in G$ 是任一元素. 则 x 的逆元也是唯一的.