普通高等教育“十一五”国家级规划教材

抽象代数

樊 恽 刘宏伟 编

科学出版社
www.sciencep.com

普通高等教育“十一五”国家级规划教材

抽象代数

樊 恽 刘宏伟 编

科学出版社

北京

内 容 简 介

抽象代数，又称近世代数，是综合院校、师范院校数学专业的基础课程，也是电子类等专业的选修课程. 本书以操作性较强的方式组织编排了供一学期抽象代数课程使用的内容. 同时把因限于课时而不能在课堂内容展开的，但却是基本的、有强烈背景的若干问题编排为选读选讲材料，使得本书除可操作性外还具有一定的可塑性.

本书可作为师范院校、综合院校数学系的教材，也可供其他相关专业选作教学用书.

图书在版编目(CIP)数据

抽象代数/樊恽，刘宏伟编. —北京：科学出版社，2008

普通高等教育“十一五”国家级规划教材

ISBN 978-7-03-021548-2

Ⅰ. 抽… Ⅱ. ①樊… ②刘… Ⅲ. 抽象代数-高等学校-教材 Ⅳ. O153

中国版本图书馆 CIP 数据核字(2008) 第 044467 号

责任编辑：李鹏奇 王 静 杨 然／责任校对：陈玉凤

责任印制：张克忠／封面设计：陈 敬

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

北京市文林印务有限公司印刷

科学出版社发行 各地新华书店经销

*

2008 年 6 月第 一 版 开本：B5(720×1000)

2008 年 6 月第一次印刷 印张：12 1/2

印数：1—3 500 字数：234 000

定价：20.00 元

(如有印装质量问题，我社负责调换〈文林〉)

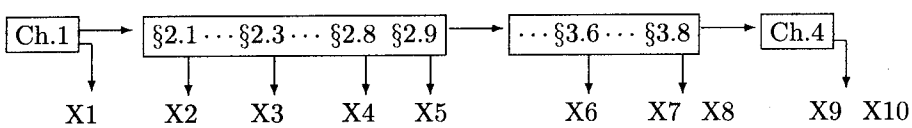
前　言

抽象代数, 也称近世代数, 是高等院校数学专业的基础课程之一. 它对师范院校数学专业也极具亲和力, 因为它包含了初等数学关心但无法一般性地予以解决的许多课题和问题. 通信、信息、计算机等专业把它作为选修课, 因为它是这些科学技术的基本数学工具.

本书是在作者多年从事高等院校数学系抽象代数教学的讲稿基础上编撰而成的, 主要目的是为一般师范院校提供一本一学期的抽象代数课程教材. 从教学实践来看, 一学期课时有限, 使得一些基本内容、一些初等数学关心的内容不能充分展开. 为此, 本书提供了一部分选读选讲材料, 这不但多少弥补了这个缺陷, 也使得本书具有更加广泛的适应性.

关于内容安排和编写体例. 前 4 章可作为一般院校一学期 72 学时课程的内容, 其中有少部分仿宋体排印内容是我们觉得学生应了解也可以自己阅读的内容. 当然教师可根据情况安排, 如某些例子、例题、说明, 甚至某些证明留给学生阅读. 每节后面有内容小结关键词, 帮助读者阅读该节后自己小结一下. 不把内容小结关键词放在每节的前面, 是因为考虑到读者在学习该节之前可能对其内容尚无印象.

选读选讲材料共 16 节, 分别标号 X1, X2, ···, X16. 选读选讲材料的前 10 节是前 4 章的补充材料, 它们与前 4 章各节的逻辑次序图示如下 (X9、X10 是与数系发展相关的两节, X9 也可在 §3.4 后阅读):



选读选讲材料的后 6 节是模论基础, 其中除了基本概念外, 主要是与线性代数密切相关的内容.

习题的编排顺序一般是按照正文内容, 而不是按照难易程度. 标记 $^+$ 的习题, 如习题标号为 1^+, 是在正文中提到了的习题. 有两种情形: 一种是正文中的某些证明过程省略留作习题; 另一种是该习题的结论在正文中被引用到.

书中附有符号说明和名词索引, 方便阅读查找.

不论是内容安排还是陈述方式, 无疑有待修订优化, 欢迎读者斧正.

编者

2008 年 4 月

符 号 说 明

对全书使用符号的惯例和在较多地方出现的符号做一简短说明.

$A := B$　表示用 A 记 B
$B =: A$　表示 B 记作 A
$\forall$　表示“对所有”
$\exists$　表示“存在”
$\square$　表示证明完毕, 或证明省略

$f : A \to B$　从集合 A 到集合 B 的映射
$a \mapsto b$　表示元素 a 映射为元素 b
id　表示恒等映射 (恒等变换)
$\mathrm{Im}(f)$　映射 $f : A \to B$ 的象
$\mathrm{Ker}(\sigma)$　群的同态映射 $\sigma : G \to H$ 的核 (见命题 2.6.1)

板书黑体 $\mathbb{F}$, 表示一个数域;　$\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$, 分别表示有理数域、实数域、复数域
$\mathbb{Q}^\times$、$\mathbb{R}^\times$、$\mathbb{C}^\times$, 分别表示非零有理数集合、非零实数集合、非零复数集合
i　表示虚数单位, 即 $\mathrm{i} = \sqrt{-1}$　(i, j 等常用来表示跑动标号)
$\mathbb{Z}$　表示所有整数的集合;　$\mathbb{Z}^+$ 为所有非负整数的集合;　$\mathbb{Z}_m$ 为所有模 m 剩余类的集合
$\dbinom{n}{k} = \dfrac{n!}{k!(n-k)!}$　表示从 n 个东西选取 k 个的组合数
$m|n$　表示整数 m 整除整数 n;　$f(x)|g(x)$ 表示多项式 $f(x)$ 整除多项式 $g(x)$
$\gcd(m, n)$　表示整数 m, n 的最大公因数
$\mathrm{lcm}(m, n)$　表示整数 m, n 的最小公倍数
$\exp(x)$　表示自然指数函数 (即 $\exp(x) = \mathrm{e}^x$);　$\ln(x)$ 表示自然对数函数
$\min\{a, b, \cdots\}$　表示 a, b, $\cdots$ 中最小的数
$\max\{a, b, \cdots\}$　表示 a, b, $\cdots$ 中最大的数

$\mathrm{M}_{m\times n}(R)$　表示环 R 上的所有 $m \times n$ 矩阵的集合 (在矩阵加法下它是一个加群)
$\mathrm{M}_n(R)$　表示环 R 上的所有 n 阶方阵的集合 (在矩阵加法和矩阵乘法下它是一个环)
$\mathrm{GL}_n(R)$　表示环 R 上的所有 n 阶可逆方阵的集合 (在矩阵乘法下它是一个群)
$\mathrm{SL}_n(R)$　表示环 R 上的所有 n 阶的行列式等于 1 的方阵的集合 (它是 $\mathrm{GL}_n(R)$ 的子群)
$\mathrm{diag}(d_1, \cdots, d_n)$　表示对角线元为 $d_1, \cdots, d_n$ 的对角矩阵
$\mathrm{tr}\,\boldsymbol{A}$　表示矩阵 $\boldsymbol{A}$ 的迹
$\det \boldsymbol{A}$　表示矩阵 $\boldsymbol{A}$ 的行列式
$\deg f(x)$　表示多项式 $f(x)$ 的次数
$Z(R)$　表示环 R 的中心
$R^\times$　表示幺环 R 的所有可逆元构成的乘法群

目　录

第1章 集 合

§1.1 集 合

集合, 简称 "集", 是数学中不予定义的原始对象. 数学的定义总是用一些已知的概念, 已知的条件给出一个新的概念. 因此总有一些概念是最原始的, 不予定义的. "集合" 就是这样一个原始概念.

对于原始概念 "集合" 虽然不予定义, 但是可以描述. 一个集合 A 是一些数学对象的群体使得人们可以明确识别一个对象是在 A 里面还是不在 A 里面.

对象 a 在 A 里面就记作 $a \in A$, 读作 "a 属于 A", 称 a 是 A 的元素, 或称 a 是 A 的成员. 否则 a 不在 A 里面, 记作 $a \notin A$, 读作 "a 不属于 A".

通常有两种方式表达一个集合.

列举式记法 在花括号中列举出集合的所有元素. 例如, 所有非负整数的集合用符号 $\mathbb{Z}^+$ 表示, 可列举式记为 $\mathbb{Z}^+ = \{0, 1, 2, \cdots\}$.

描述性记法 在花括号中描述集合的元素. 例如, $\mathbb{R} = \{$ 实数 $\}$ 是所有实数的集合, 即实数轴上全体点的集合. 又如, 实数轴上 0 到 1 闭区间实数的集合 $[0,1] = \{r \in \mathbb{R} \mid 0 \leqslant r \leqslant 1\} = \{r$ 是实数且 $0 \leqslant r \leqslant 1\}$.

这里还采用以下记号: $\mathbb{Z} = \{$ 整数 $\}$, $\mathbb{Q} = \{$ 有理数 $\}$, $\mathbb{C} = \{$ 复数 $\}$.

没有元素的集合称为空集, 记作 $\varnothing$.

人们常说的 "组" 与 "集" 有不同之处: "组" 里的东西是可以重复的, 但 "集" 里的东西是不可重复的, 因为它们是被明确识别的. 例如, 我们说数组 $2, 2, 1, 3, 3, 5$, 就是 6 个数构成的组, 但如果说 $2, 2, 1, 3, 3, 5$ 构成的集合则是 $\{2, 1, 3, 5\}$.

设 A, B 是两个集合. 如果对任 $a \in A$ 有 $a \in B$, 就说 A 是 B 的**子集**, 记作 $A \subseteq B$, 或 $B \supseteq A$. 也说成 A 包含于 B, 或说 B 包含 A. 空集是任何集合的子集.

如果 $A \subseteq B$ 且 $B \subseteq A$, 那么它们就是同一个集合, 记作 $A = B$. 如果 $A \subseteq B$ 但 $A \neq B$, 就说 A 是 B 的真子集, 记作 $A \subsetneq B$.

设 A, B 是两个集合. 定义:

- $A \cup B := \{ c \mid c \in A$ 或 $c \in B \}$, 称为 A 与 B 的**并集**;
- $A \cap B := \{ c \mid c \in A$ 且 $c \in B \}$, 称为 A 与 B 的**交集**;
- $A - B := \{ c \mid c \in A$ 但 $c \notin B \}$, 称为 A 与 B 的**差集**.

并集和交集可以对任意多个集合定义: 设 A_i, $i \in I$, 是用指标集 I 标号的一组集合, 那么:

- 并集定义为 $\bigcup\limits_{i\in I} A_i := \{\, a \mid$ 存在 $i \in I$ 使得 $a \in A_i \,\}$;
- 交集定义为 $\bigcap\limits_{i\in I} A_i := \{\, a \mid$ 对任 $i \in I$ 有 $a \in A_i \,\}$.

按定义马上有:

$$A\cap B\subseteq A\,,\qquad A\cup B\supseteq A\,,\qquad A-B\subseteq A\,,\qquad (A-B)\cap B=\varnothing\,.$$

而且易证明下列结论.

命题 1.1.1　设 A, B, C 是集合. 则以下成立:

$$A\cap B=B\cap A,\quad A\cup B=B\cup A; \tag{交换律}$$

$$\begin{aligned}(A\cap B)\cap C&=A\cap(B\cap C),\\ (A\cup B)\cup C&=A\cup(B\cup C);\end{aligned} \tag{结合律}$$

$$A\cap A=A,\quad A\cup A=A; \tag{幂等律}$$

$$A\cap(A\cup B)=A,\quad A\cup(A\cap B)=A; \tag{吸收律}$$

$$\begin{aligned}A\cap(B\cup C)&=(A\cap B)\cup(A\cap C),\\ A\cup(B\cap C)&=(A\cup B)\cap(A\cup C);\end{aligned} \tag{分配律}$$

$$\begin{aligned}A-(B\cap C)&=(A-B)\cup(A-C),\\ A-(B\cup C)&=(A-B)\cap(A-C).\end{aligned} \tag{德摩根律}$$

证　仅证明最后一式, 其他各式的证明作为练习.

设 $a\in(A-B)\cap(A-C)$, 即 $a\in A-B$ 且 $a\in A-C$. 那么 a 在 A 中但不在 B 中, 且 a 在 A 中但不在 C 中. 也就是 a 在 A 中, 但 a 既不在 B 中也不在 C 中, 也就是不在 $B\cup C$ 中, 得 $a\in A-(B\cup C)$. 因此 $(A-B)\cap(A-C)\subseteq A-(B\cup C)$.

再设 $a\in A-(B\cup C)$, 即 a 在 A 中但 a 既不在 B 中也不在 C 中. 那么 a 在 A 中但不在 B 中, 即 $a\in A-B$. 且 a 在 A 中但不在 C 中, 即 $a\in A-C$. 得 $a\in(A-B)\cap(A-C)$. 故 $A-(B\cup C)\subseteq(A-B)\cap(A-C)$.

综上两段, 就得 $A-(B\cup C)=(A-B)\cap(A-C)$(图 1.1.1). □

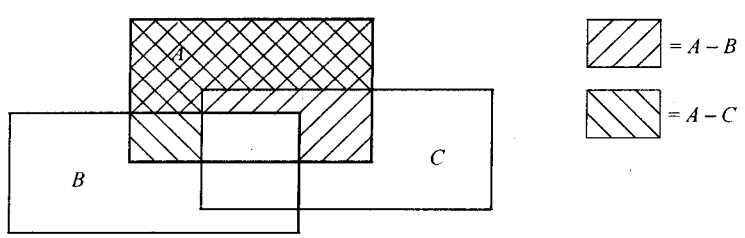


图 1.1.1　$A-(B\cup C)=(A-B)\cap(A-C)$

设 S 是一个集合. 以 S 的所有子集为成员的集合称为 S 的**幂集**, 记作 $\mathcal{P}(S)$:

$$\mathcal{P}(S)=\{A\mid A \text{ 是 } S \text{ 的子集}\}\,.$$

对 $A\in\mathcal{P}(S)$, 记 $\overline{A}=S-A$, 称为 A 在 S 中的**补集**, 则 $\overline{A}\in\mathcal{P}(S)$. 那么对任 $A,\ B\in\mathcal{P}(S)$, 这些集合 $\bar{A}$, $A\cap B$, $A\cup B$, $A-B$ 都还是 $\mathcal{P}(S)$ 的元素. 通常把 "$\bar{}$"、"$\cap$"、"$\cup$"、"$-$" 称为集合 $\mathcal{P}(S)$ 上的运算. 命题 1.1.1 也描述了集合 $\mathcal{P}(S)$ 上的运算所满足的运算律.

特别地, 在命题 1.1.1 的德摩根律中, 取 A 为这里的 S, 则 $A-B=S-B=\overline{B}$, $A-C=S-C=\overline{C}$, $A-(B\cap C)=S-(B\cap C)=\overline{B\cap C}$, 所以命题 1.1.1 的德摩根律的第一式成为 $\overline{B\cap C}=\overline{B}\cup\overline{C}$. 类似地, 命题 1.1.1 的德摩根律的第二式成为 $\overline{B\cup C}=\overline{B}\cap\overline{C}$. 所以在给定集合 S 的幂集 $\mathcal{P}(S)$ 中的德摩根律表述为这个形式:

$$\overline{B\cap C}=\overline{B}\cup\overline{C}\,,\qquad \overline{B\cup C}=\overline{B}\cap\overline{C}\,.$$

设 A 和 B 是两个集合. 定义集合

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

称为 A 与 B 的**卡氏积**, 也称为**集合积**, 简称**积**. 其中, (a,b) 表示有顺序的元素序列. 典型例子: 取 $A=B=\mathbb{R}$, 实数集 $\mathbb{R}$ 与自己的卡氏积 $\mathbb{R}\times\mathbb{R}=\{\ (a,b)\mid a,b\in\mathbb{R}\ \}$, 简记为 $\mathbb{R}^2$, 解析几何中它与欧氏平面的点一一对应. 从这例子可见为什么说 (a,b) 是有顺序的元素序列: 当 $a\neq b$ 时, $(a,b)\neq(b,a)$.

对三个或多个集合同样可以定义**卡氏积**. 如

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

其中, (a,b,c) 表示有顺序的元素序列. 典型例子: 取 $A=B=C=\mathbb{R}$, 实数集 $\mathbb{R}$ 的三重卡氏积 $\mathbb{R}^3:=\mathbb{R}\times\mathbb{R}\times\mathbb{R}=\{\ (a,b,c)\mid a,b,c\in\mathbb{R}\ \}$, 立体解析几何中它与欧氏空间的点一一对应.

集合 A 中元素的个数称为集合 A 的**基数**, 记作 $|A|$. 如果 $|A|$ 是无限的, 记作 $|A|=\infty$, 称 A 是无限集. 如果 $|A|$ 是有限的, 则记作 $|A|<\infty$, 称 A 是有限集.

例如, $|\varnothing|=0<\infty$, $|\{2,1,3,5\}|=4<\infty$, 都是有限集.

例如, $|\mathbb{Z}^+|=\infty$, $\big|[0,1]\big|=\infty$, 都是无限集.

虽然 $\mathbb{Z}^+$ 与 $[0,1]$ 都是无限集, 但它们的基数大小却有本质区别.

$\mathbb{Z}^+$ 的元素可以列举出来, 就是可以像数数那样把它的元素一个一个数下去: 从 0 数起; 数了 n 以后数 $n+1$; 按 "数学归纳法" 的意思就把它的元素数完了. 但 $[0,1]$ 的元素却数不完, 具体情形可参看选读选讲材料 X1.

因此 $\mathbb{Z}^+$ 称为**可数无限集**, 而 $[0,1]$ 称为**不可数无限集**. 这是数学家康托 (Cantor) 发现的事实, 由此出发康托创立了现代集合论, 参见选读选讲材料 X1.

集合 A 与 B 的卡氏积 $A\times B=\{(a,b)\mid a\in A,\ b\in B\}$ 中, 对每 $a\in A$, b 在 B 中跑动时, 得到的元素序列 (a,b) 共有 $|B|$ 个; 再让 a 在 A 中跑动, 共得到元素序列 (a,b) 有 $|A|\cdot|B|$ 个, 所以 $|A\times B|=|A|\cdot|B|$. 即使 A、B 中有空集, 这个公式也是正确的, 参看习题 1.1 中的第 4 题.

上述公式可推广到多个集合的卡氏积, 如 $|A\times B\times C|=|A|\cdot|B|\cdot|C|$.

设 $A_i, i\in I$, 是用指标集 I 标号的一组集合. 如果对任两个互异的标号 $i\neq j\in I$ 都有 $A_i\cap A_j=\varnothing$, 就称并集 $A:=\bigcup\limits_{i\in I}A_i$ 是不交并集. 此时, 只要把每个 A_i 的元素个数都计数一遍以后, 就正好是把 A 的所有元素都无重复地计数了. 所以, 对不交并集有简单的基数计算公式 $|\bigcup\limits_{i\in I}A_i|=\sum\limits_{i\in I}|A_i|$.

但对一般的并集的基数计算就要复杂得多, 习题 1.1 中的第 6 题是其中最简单的情况.

内容小结关键词: 集合, 集合运算和运算律, 基数.

习　题　1.1

1. 求 $\varnothing\cap A$, $\varnothing\cup A$.

2. 设 $A_i, i\in I$, 是指标集 I 标号的一组集合, B 是集合. 证明:

(1) $\Big(\bigcap\limits_{i\in I}A_i\Big)\bigcup B=\bigcap\limits_{i\in I}(A_i\bigcup B)$;

(2) $\Big(\bigcup\limits_{i\in I}A_i\Big)\bigcap B=\bigcup\limits_{i\in I}(A_i\bigcap B)$.

3. 如果 $A\cap B=\varnothing$, 则说 A 与 B 不相交, 称并集 $A\cup B$ 为不交并集. 证明以下等式并证明它们的右边都是不交并:

(1) $A=(A-B)\cup(A\cap B)$;

(2) $(A\cup B)-(A\cap B)=(A-B)\cup(B-A)$;

(3) $A\cup B=(A-B)\cup(A\cap B)\cup(B-A)$.

4.$^+$ 设 A, B 是集合. 证明:

(1) 如果 $A=\varnothing$, 则 $A\times B=\varnothing$;

(2) 如果 $A\times B=B\times A$, 则 $A=B$ 或者 A, B 之一是空集.

5. 设 A 是有限集, $|A|=n$. 求: $|A\cap A|$, $|A\cup A|$, $|A\times A|$, $|\mathcal{P}(A)|$.

6.$^+$ (容斥原理) 设 A, B 是有限集合. 证明 $|A\cup B|=|A|+|B|-|A\cap B|$.

§1.2　关　　系

不论是在平常生活中还是在数学中都会考虑各种关系, 如一个学校的学生集合

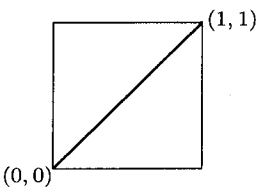
中的同班关系、实数集合 $\mathbb{R}$ 上的小于关系等.

一种关系的实质是：对任何两个被考虑的对象可以明确识别一个与另一个要么具有这种关系要么不具有这种关系.

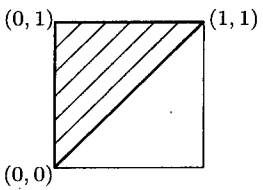
使用集合语言来描述就是：集合 A 上的关系 $\sim$, 是说对任 $a,b\in A$ 可以明确识别 a 与 b 有关系即 $a\sim b$, 或没有关系即 $a\not\sim b$. 更准确的数学化的定义如下.

集合 A 上的关系 $\sim$ 是卡氏积 $A\times A$ 的一个子集 $\sim\subseteq A\times A$. 对 $a,b\in A$, 如果 $(a,b)\in\sim$ 就记作 $a\sim b$ 并称 a 与 b 具有关系 $\sim$. 否则记作 $a\not\sim b$ 并说 a 与 b 不具有关系 $\sim$.

例如, $[0,1]$ 上的 "等于" 关系 "$=$", 就是卡氏积 $[0,1]\times[0,1]$ 中连接点 $(0,0)$ 与点 $(1,1)$ 的对角线上的所有点构成的子集.



$[0,1]$ 上的关系 "$=$"



$[0,1]$ 上的关系 "$\leqslant$"

又例如, $[0,1]$ 上的 "小于等于" 关系 "$\leqslant$", 就是卡氏积 $[0,1]\times[0,1]$ 中以 $(0,0)$、$(0,1)$、$(1,1)$ 为三个顶点的三角形 (包括边界) 的所有点.

定义 1.2.1　如果以下三条满足, 集合 A 上的关系 $\preceq$ 称为一个**偏序关系**.

自反律　对任 $a\in A$, 有 $a\preceq a$;

传递律　对任 $a,b,c\in A$, 如果 $a\preceq b$ 且 $b\preceq c$, 则 $a\preceq c$;

反对称律　对任 $a,b\in A$, 如果 $a\preceq b$ 且 $b\preceq a$, 则 $a=b$.

例如, $\mathbb{R}$ 的关系 "$\leqslant$" 是偏序关系.

又如, 集合 S 的幂集 $\mathcal{P}(S)$ 上的包含关系 "$\subseteq$" 是偏序关系.

定义 1.2.2　(1) 如果以下三条满足, 集合 A 上的关系 $\sim$ 称为一个**等价关系**.

自反律　对任 $a\in A$, 有 $a\sim a$;

传递律　对任 $a,b,c\in A$, 如果 $a\sim b$ 且 $b\sim c$, 则 $a\sim c$;

对称律　对任 $a,b\in A$, 如果 $a\sim b$, 则 $b\sim a$.

(2) 设 $\sim$ 是集合 A 上的等价关系. $a\in A$. 称 A 的子集 $[a]=\{\,b\in A\mid b\sim a\,\}$ 是 A 的关于等价关系 $\sim$ 的一个**等价类**, 在默认等价关系的情况下简称为等价类. 以 A 的所有等价类为成员构成新的集合, 记作 $A/\sim$, 称为集合 A 关于等价关系 "$\sim$" 的**商集**.

例如, 在全体整数集合 $\mathbb{Z}$ 上, 模 2 同余关系 $a\equiv b\pmod 2$ 是等价关系, 参看习题 1.2 中的第 1 题. 等价类

$$[a]=\begin{cases}\text{偶数集合}, & \text{若 } a \text{ 是偶数};\\ \text{奇数集合}, & \text{若 } a \text{ 是奇数}.\end{cases}$$

商集 $\mathbb{Z}/\equiv \pmod 2$ 由两个成员构成：偶数集合, 奇数集合. 对这个商集的习惯记号是 $\mathbb{Z}/2\mathbb{Z}$ 或者 $\mathbb{Z}_2$, 即商集 $\mathbb{Z}/2\mathbb{Z}=\{$偶数集合, 奇数集合$\}$.

一个生活例子. 一个学校的全体学生构成集合, "同班" 关系是等价关系. 学生张三的等价类 [张三], 按定义就是所有与张三同班的学生构成的子集, 也就是张三的班; 商集 "学生集合/同班" 就是该校的所有的班级构成的集合.

注 (等价关系性质)　设 $\sim$ 是集合 A 的等价关系. 对等价关系 $\sim$, 阐述几条性质, 对各条性质, 证明之后有简短说明.

(1) 对任 $a\in A$ 有 $a\in[a]$.

证　因为 $a\sim a$, 按定义就有 $a\in[a]$.　□

因此, 也常说 $[a]$ 是 a 所在的等价类.

(2) 对任 $a'\in[a]$ 有 $[a']=[a]$.

证　按定义有 $a'\sim a$. 对任 $b\in[a']$ 有 $b\sim a'$, 按传递律得 $b\sim a$, 所以 $b\in[a]$, 得 $[a']\subseteq[a]$. 按对称律还有 $a\sim a'$. 同样的推理得出 $[a]\subseteq[a']$, 即得 $[a']=[a]$.　□

直观地解释这条性质就是：一个等价类中的任何元可以 "代表" 这个等价类. 例如, 学生集合上的同班关系, 如果张三在李四的班上, 那么 "张三的班" 也就是 "李四的班". 这条性质还可以进一步发挥为以下性质.

(3) $a\sim a'$ 当且仅当 $[a]=[a']$.

证　如果 $a\sim a'$, 按定义 $a\in[a']$. 从上述性质得 $[a]=[a']$. 反过来设 $[a]=[a']$, 那么 $a\in[a]=[a']$, 则 $a\in[a']$, 即 $a\sim a'$.　□

以学生集合上的同班关系为例来理解这条断言就是, 如果张三与李四同班, 那么日常语言说的 "张三的班"、"李四的班" 是同一个班. 反过来, 如果 "张三的班"、"李四的班" 是同一个班, 那么张三与李四同班.

下一条性质是关于商集的, 先做点说明. 按照定义, 商集 $A/\sim$ 是幂集 $\mathcal{P}(A)$ 的子集, 因为 $A/\sim$ 的成员是等价类 $[a]$, 是 A 的子集. 可以描述商集为 $A/\sim=\{\,[a]\mid a\in A\,\}$. 尽管这个描述中的 "$a\in A$" 是说 a 跑遍 A, 但可能对很多不同的元素 a 得的是同一个等价类, 从对集合概念的解释知道, 这同一个等价类尽管在描述过程中可能出现多次但作为集合 $A/\sim$ 的成员只是一个. 例如, 在前面例子 $\mathbb{Z}/\equiv \pmod 2$ 中, 所有的偶数 a 给出的是同一个等价类 "偶数集合", 所有的奇数 a 给出的是同一个等价类 "奇数集合", 商集 $\mathbb{Z}/\equiv \pmod 2$ 恰含这两个成员.

(4) 作为幂集 $\mathcal{P}(A)$ 的子集, 商集 $A/\sim$ 具有以下特点.

"非空"：对任 $[a]\in A/\sim$, 有 $[a]\neq\varnothing$;

"不交"：如果 $[a],[b]\in A/\sim$ 且 $[a]\neq[b]$, 则 $[a]\bigcap[b]=\varnothing$;

"覆盖": $\bigcup\limits_{[a]\in A/\sim}[a]=A$, 其中, $\bigcup$ 的脚标 $[a]\in A/\sim$ 表示 $[a]$ 取遍商集的成员.

证 性质 (1) 已证 $a\in[a]$, 所以 "非空" 成立.

若 $[a]\bigcap[b]\neq\varnothing$, 则取 $c\in[a]\bigcap[b]$. 那么 $c\in[a]$, 故由性质 (2) 知 $[a]=[c]$. 同样, 从 $c\in[b]$ 得 $[b]=[c]$, 故 $[a]=[b]$, 所以 "不交" 成立.

因为对任 $a\in A$ 有 $a\in[a]$, 故 $A\subseteq\bigcup\limits_{[a]\in A/\sim}[a]$; 反过来, 显然 $\bigcup\limits_{[a]\in A/\sim}[a]\subseteq A$. 所以第三条 "覆盖" 成立. □

以一个学校全体学生的集合上的同班关系为例, 比较容易理解关于商集的性质 (4) 中的三条: 商集 "学生集合/同班" 是所有班级的集合. 第一, 没有空班; 第二, 两个不同的班交集为空; 第三, 所有班的并集为全体学生的集合.

定义 1.2.3 (1) 如果集合 A 的幂集的子集 $\mathcal{T}\subseteq\mathcal{P}(A)$ 满足以下三条:

"非空": 对任 $T\in\mathcal{T}$ 有 $T\neq\varnothing$;

"不交": 如果 $T,T'\in\mathcal{T}$ 且 $T\neq T'$, 则 $T\bigcap T'=\varnothing$;

"覆盖": $\bigcup\limits_{T\in\mathcal{T}}T=A$,

就称 A 的幂集 $\mathcal{P}(A)$ 的子集 $\mathcal{T}$ 是集合 A 的一个**划分**.

(2) 对集合 A 的划分 $\mathcal{T}$, 定义关系 "$\underset{\mathcal{T}}{\sim}$" 为: 如果存在 $T\in\mathcal{T}$ 使得 A 的元素 a 与 b 都在 T 中, 就说 $a\underset{\mathcal{T}}{\sim}b$.

例如, 某校 2008 级新生入学后构成集合 A, 分班以后得到班级集合 $\mathcal{T}$. 因为每个班有学生, 不同的班不交, 所有班的并集就是集合 A, 所以 $\mathcal{T}$ 是 A 的划分. 这个划分给出了集合 A 上的关系 "$\underset{\mathcal{T}}{\sim}$", 学生 a, b 具有关系 $a\underset{\mathcal{T}}{\sim}b$ 是说有一个班 $T\in\mathcal{T}$ 使得 $a,b\in T$, 也就是学生 a, b 都在班级 T 中, 所以 "$\underset{\mathcal{T}}{\sim}$" 就是学生集合 A 上的同班关系.

前面讨论集合上的等价关系, 这里讨论集合的划分, 都以学生和班级为典型例子予以阐述. 这是否启示等价关系与划分实质上是同一件事情的不同表现形式? 这里将从数学上严格论述确实如此. 先叙述关于划分的一个结论.

引理 1.2.1 对集合 A 的幂集的子集 $\mathcal{T}\subseteq\mathcal{P}(A)$, 定义 1.2.3(1) 中的 "不交" 与 "覆盖" 两条成立当且仅当对任 $a\in A$ 存在唯一一个 $T\in\mathcal{T}$ 使得 $a\in T$.

证 对任 $a\in A$, 从 "覆盖" 推出存在 $T\in\mathcal{T}$ 使得 $a\in T$; 从 "不交" 推出不能有两个不同的 $T,T'\in\mathcal{T}$ 都包含 a, 因为 T 与 T' 没有公共元.

反过来, 设对任 $a\in A$ 存在唯一一个 $T\in\mathcal{T}$ 使得 $a\in T$. 那么对任 $a\in A$ 有 $a\in\bigcup\limits_{T\in\mathcal{T}}T$, 从而 $\bigcup\limits_{T\in\mathcal{T}}T=A$, 即 "覆盖" 成立. 对 $T,T'\in\mathcal{T}$, 如果 $T\bigcap T'\neq\varnothing$ 则可取 $a\in T\bigcap T'$, 即 T 与 T' 都包含 a, 由唯一性得 $T=T'$, 所以 "不交" 成立. □

定理 1.2.1 (等价关系与划分的定理) 设 A 是集合.

(1) 如果 "$\sim$" 是 A 的等价关系, 那么商集 $\mathcal{T} := A/\sim$ 是 A 的一个划分, 而且这个划分给出的关系 $\underset{\mathcal{T}}{\sim}$ 就是原来的关系 $\sim$, 即 $\underset{\mathcal{T}}{\sim} = \sim$.

(2) 如果 $\mathcal{T}$ 是 A 的一个划分, 那么 "$\underset{\mathcal{T}}{\sim}$" 是 A 的等价关系, 而且作为幂集 $\mathcal{P}(A)$ 的子集, 商集 $A/\underset{\mathcal{T}}{\sim}$ 就是原来的划分 $\mathcal{T}$, 即 $A/\underset{\mathcal{T}}{\sim} = \mathcal{T}$.

证　(1) 上面等价关系性质 (4) 已经证明了商集 $A/\sim$ 是 A 的一个划分. 为书写简单, 记 $\mathcal{T} := A/\sim$. 剩下需要证明这个划分产生的关系 $\underset{\mathcal{T}}{\sim}$ 与原来的等价关系 $\sim$ 是同一个关系, 即要证: 对 $a, b \in A$, 如 $a \underset{\mathcal{T}}{\sim} b$ 则 $a \sim b$; 反过来, 如 $a \sim b$ 则 $a \underset{\mathcal{T}}{\sim} b$.

设 $a \underset{\mathcal{T}}{\sim} b$, 即存在 $T \in \mathcal{T}$ 使得 $a, b \in T$. 但 T 是一个等价类, 即 $T = [c] \in A/\sim$ 对某 $c \in A$, $a, b \in [c]$. 按等价类定义, $a \sim c$ 且 $b \sim c$, 从对称律得 $c \sim b$, 再从传递律得 $a \sim b$.

反过来, 设 $a \sim b$, 那么 $a \in [b]$. 由等价关系性质 (2), 得 $[a] = [b]$, 记这个等价类为 $T \in \mathcal{T}$. 而 $a \in [a]$, $b \in [b]$, 即 $a, b \in T$. 按定义, 得 $a \underset{\mathcal{T}}{\sim} b$.

(2) 先证 "$\underset{\mathcal{T}}{\sim}$" 是 A 的等价关系. 对任 $a \in A$, 由引理 1.2.1, 存在唯一 $T \in \mathcal{T}$ 使得 $a \in T$. 那么 $a, a \in T$, 所以 $a \underset{\mathcal{T}}{\sim} a$. 自反律成立.

如 $a \underset{\mathcal{T}}{\sim} b$, 按照关系 $\underset{\mathcal{T}}{\sim}$ 的定义, 存在 $T \in \mathcal{T}$ 使得 $a, b \in T$, 于是 $b, a \in T$, 即 $b \underset{\mathcal{T}}{\sim} a$. 对称律成立.

设 $a \underset{\mathcal{T}}{\sim} b$ 和 $b \underset{\mathcal{T}}{\sim} c$, 就是存在 $T, T' \in \mathcal{T}$ 使得 $a, b \in T$ 和 $b, c \in T'$, 那么 T 与 T' 都包含 b, 由引理 1.2.1, $\mathcal{T}$ 中包含 b 的成员是唯一的, 所以 $T = T'$, 于是 $a, c \in T$, 即 $a \underset{\mathcal{T}}{\sim} c$. 传递律成立.

以上证明了 $\underset{\mathcal{T}}{\sim}$ 是等价关系. 把 a 的等价类记作 $[a]_{\mathcal{T}}$. 下面证明商集 $A/\underset{\mathcal{T}}{\sim} = \mathcal{T}$, 也就是要证明 $A/\underset{\mathcal{T}}{\sim} \subseteq \mathcal{T}$ 且 $\mathcal{T} \subseteq A/\underset{\mathcal{T}}{\sim}$.

设 $[a]_{\mathcal{T}} \in A/\underset{\mathcal{T}}{\sim}$. 由引理 1.2.1, 存在唯一 $T \in \mathcal{T}$ 使得 $a \in T$. 对任 $b \in T$, 按照关系 $\underset{\mathcal{T}}{\sim}$ 的定义, 有 $b \underset{\mathcal{T}}{\sim} a$, 所以 $b \in [a]_{\mathcal{T}}$, 即得 $T \subseteq [a]_{\mathcal{T}}$. 反过来, 对任 $c \in [a]_{\mathcal{T}}$, 按等价类的定义, 有 $c \underset{\mathcal{T}}{\sim} a$. 再按关系 $\underset{\mathcal{T}}{\sim}$ 的定义有 $T' \in \mathcal{T}$ 使得 $c, a \in T'$, 那么 T' 与 T 都包含 a, 而 $\mathcal{T}$ 中包含 a 的成员是唯一的, 所以 $T' = T$, 因此 $c \in T$.

综上所述, 从 $a \in T$ 就得出 $[a]_{\mathcal{T}} = T$. 特别就得到 $[a]_{\mathcal{T}} \in \mathcal{T}$, 所以 $A/\underset{\mathcal{T}}{\sim} \subseteq \mathcal{T}$.

反过来, 对任 $T \in \mathcal{T}$, 因为 $T \neq \varnothing$, 所以可以取 $a \in T$. 按上段推理, 有 $[a]_{\mathcal{T}} = T$, 即 T 是 a 所在的等价类, 故 $T \in A/\underset{\mathcal{T}}{\sim}$. 所以 $\mathcal{T} \subseteq A/\underset{\mathcal{T}}{\sim}$.　□

一个集合 A 可以有不同的等价关系, 可以有不同的划分. 定理说明: A 的等价关系和划分是一一对应的. 所以, 本节的两个主要概念等价关系和划分是完全互相转化的.

定义 1.2.4　设 $\mathcal{T}$ 是集合 A 的一个划分. 从 $\mathcal{T}$ 的每个成员 T(它是 A 的非空子集) 选出一个元素作为 T 的代表元; 代表元构成 A 的子集 R, 称为划分 $\mathcal{T}$ 的一

个**完全代表系**.

以一个学校全体学生的集合 A 为例. 分班后, 所有班的集合 $\mathcal{T}$ 是一个划分. 每班选一个班长, 全体班长开会, 构成的 A 的子集 R 就是一个完全代表系. 这样考虑处理各班的事务就方便一些.

设 $\sim$ 是 A 的等价关系. 前面说过, 把商集描述为 $A/\sim = \{\,[a] \mid a \in A\,\}$, a 跑遍 A 时一个等价类可能重复出现. §1.1 说过作为集合成员, 重复出现的等价类仍只是同一个成员. 尽管如此, 有时处理具体问题时仍以不重复出现为方便. 这时就可以取一个完全代表系.

例如, 整数集 $\mathbb{Z}$ 模 2 同余的商集 $\mathbb{Z}_2 = \{$偶数集合, 奇数集合$\}$. 偶数集合中选取 0 做代表, 奇数集合中选取 1 做代表, 得到 $R = \{\,0, 1\,\}$ 是一个完全代表系, 则 $\mathbb{Z}_2 = \{\,[a] \mid a \in R\,\} = \{\,[0],\ [1]\,\}$. 这样描述集合 $\mathbb{Z}_2$ 时成员没有重复出现.

内容小结关键词: 关系, 等价关系, 商集, 划分.

正文和习题中涉及整数的整除问题. 这里简述有关基本性质.

整除、因数、倍数等概念在中、小学数学中已介绍. 只是注意现在是考虑所有整数的整除问题而不是仅仅考虑正整数. 用 $m \mid n$ 表示 m 整除 n.

设整数 n 非零也不等于 ± 1. 那么 $\pm 1, \pm n$ 总是 n 的因数, 称为 n 的平凡因数. 如果 n 只有平凡因数就称 n 是素数.

设整数 $n_1, \cdots, n_k$ 不全为零. 定义:

(1) 如果整数 $c \mid n_i$, $i = 1, \cdots, k$, 就称 c 是 $n_1, \cdots, n_k$ 的公因数.

(2) 如果整数 d 是 $n_1, \cdots, n_k$ 的公因数, 而且只要 c 是 $n_1, \cdots, n_k$ 的公因数就有 $c \mid d$, 那么就称 d 是 $n_1, \cdots, n_k$ 的最大公因数.

显然, 如果 d 是 $n_1, \cdots, n_k$ 的最大公因数, 则 $-d$ 也是 $n_1, \cdots, n_k$ 的最大公因数.. 用 $\gcd(n_1, \cdots, n_k)$ 记正的最大公因数.

(3) 如果 $\gcd(n_1, \cdots, n_k) = 1$, 就说 $n_1, \cdots, n_k$ 互素.

设 p 是素数, n 是整数. 按素数的定义, 有 $\gcd(p, n) = \begin{cases} p, & \text{若 } p \mid n; \\ 1, & \text{若 } p \nmid n. \end{cases}$

带余除法(欧氏除法)　如果 m, n 是整数, $n \neq 0$, 则存在整数 q, r 使得

$$m = nq + r\,, \qquad 0 \leqslant r < n,$$

其中, q 称为商数; r 称为余数.　□

那么一个整数 c 整除 m 和 n 当且仅当 c 整除 n 和 r, 所以 $\gcd(m, n) = \gcd(n, r)$.

所以, 若 $r = 0$ 则 $\gcd(m, n) = n$. 不然, 接着做带余除法

$$n = rq_1 + r_1\,, \qquad 0 \leqslant r_1 < r\,;$$

$$\gcd(m,n)=\gcd(n,r)=\gcd(r,r_1).$$

以此递推, 直至得到余数等于 0 为止. 则最后一个非零余数 d 就是 m,n 的最大公因数. 而且适当处理各辗转相除表达式, 可以得到整数 s,t 使得最大公因数 $d=ms+nt$. 这种方法称为**辗转相除法**.

定理 1.2.2　设整数 $n_1,\cdots,n_k$ 不全为零. 则 $d:=\gcd(n_1,\cdots,n_k)$ 存在, 而且有整数 $t_1,\cdots,t_k$ 使得 $n_1t_1+\cdots+n_kt_k=d$.

证　不妨设 $n_1\neq 0$. $k=2$ 时上述辗转相除法给出了证明. 再设 $k>2$. 按归纳法, $n_1,\cdots,n_{k-1}$ 最大公因数 d' 存在, 且有整数 $t_1',\cdots,t_{k-1}'$ 使得 $n_1t_1'+\cdots+n_{k-1}t_{k-1}'=d'$. 而且 $d'\neq 0$. 那么 d',n_k 的最大公因数 d 存在, 于是易验证 d 就是 $n_1,\cdots,n_{k-1},n_k$ 的最大公因数, 且有整数 s,t_k 使得 $d's+n_kt_k=d$. 再将 $d'=n_1t_1'+\cdots+n_{k-1}t_{k-1}'$ 代入此式, 令 $st_1'=t_1,\cdots,st_{k-1}'=t_{k-1}$, 得 $n_1t_1+\cdots+n_{k-1}t_{k-1}+n_kt_k=d$. □

推论　$\gcd(n_1,\cdots,n_k)=1$ 当且仅当有整数 $t_1,\cdots,t_k$ 使得 $n_1t_1+\cdots+n_kt_k=1$.

证　必要性: 从上面定理立即得出. 充分性: 如果 $n_1t_1+\cdots+n_kt_k=1$, 那么 $n_1,\cdots,n_k$ 的任何公因数 c 整除等式 $n_1t_1+\cdots+n_kt_k=1$ 左端所有项, 因此 c 整除右端的 1; 所以 $n_1,\cdots,n_k$ 的最大公因数只能是 ± 1. □

推论　设 $c\mid\gcd(n_1,\cdots,n_k)$, 则 $\gcd(n_1/c,\cdots,n_k/c)=\gcd(n_1,\cdots,n_k)/c$. 特别地, 若 $d=\gcd(n_1,\cdots,n_k)$, 则 $\gcd(n_1/d,\cdots,n_k/d)=1$.

证　记 $d=\gcd(n_1,\cdots,n_k)$. 从 $d\mid n_i$ 得 $(d/c)\mid(n_i/c)$. 所以, d/c 是 $n_1/c,\cdots,n_k/c$ 的公因数. 又, 有整数 $t_1,\cdots,t_k$ 使得 $n_1t_1+\cdots+n_kt_k=d$, 那么

$$\frac{n_1}{c}\cdot t_1+\cdots+\frac{n_k}{c}\cdot t_k=\frac{d}{c}.$$

故 $n_1/c,\cdots,n_k/c$ 的任何公因数整除 d/c. 按最大公因数的定义, d/c 是 $n_1/c,\cdots,n_k/c$ 的最大公因数. □

推论　设 $n|mm'$ 且 $\gcd(n,m)=1$, 则 $n|m'$.

证　存在整数 s,t 使得 $ms+nt=1$, 两边乘以 m' 得 $m'ms+m'nt=m'$. 整数 n 整除等式左边各项, 所以 n 整除右边. □

推论　设 p 是素数. 如果 $p\mid m_1\cdots m_r$, $r\geqslant 2$, 则存在 i, $1\leqslant i\leqslant r$, 使得 $p\mid m_i$.

证　先设 $r=2$, 即 $p\mid m_1m_2$. 若 $p\nmid m_1$, 则 $\gcd(p,m_1)=1$. 由上述推论, $p\mid m_2$. 所以 $r=2$ 时结论成立.

再设 $r>2$. 那么由上已证的结论, 或者 $p\mid m_1$, 或者 $p\mid m_2\cdots m_r$. 若是前者, 结论已成立. 若是 $p\mid m_2\cdots m_r$, 按归纳法, 存在 i, $2\leqslant i\leqslant r$, 使得 $p\mid m_i$. 总之, 结论对 r 成立. □

定理 1.2.3(算术基本定理)　设整数 $n\neq 0,n\neq\pm 1$. 则:

(1)　n 可以写成素数之积 $n=p_1\cdots p_k$, 其中, 各 p_i 是素数;