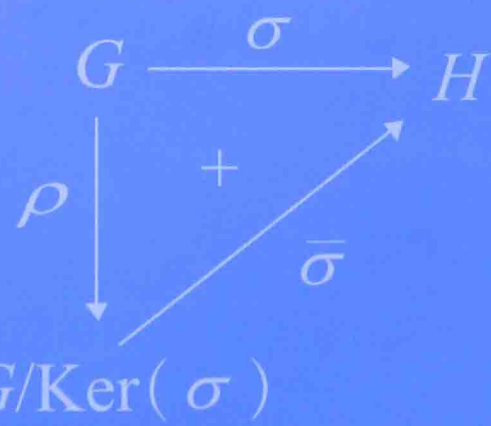
普通高等教育“十二五”规划教材
新世纪新理念高等院校数学教学改革与教材建设精品教材

丛书主编：朱长江 彭双阶
执行主编：何 穗

抽象代数引论

CHOUXIANG DAISHU YINLUN

刘宏伟 左可正 陈生安◎主编



華中師範大學出版社

普通高等教育“十二五”规划教材
新世纪新理念高等院校数学教学改革与教材建设精品教材

抽象代数引论

主　编：刘宏伟　左可正　陈生安
副主编：陈　刚　张四兰　方次军

华中师范大学出版社

内 容 提 要

本书系统地讲述了抽象代数的基本理论和方法，全书分为4章，分别为：集合与映射、群与群同态、环与整环、域的扩张。每一章的每一小节后均配备了数量适当、难易程度不一的习题，以帮助读者更好地掌握抽象代数的相关知识。书末附有名词索引，便于读者阅读查找。

本书可作为综合性大学和师范院校数学各专业的教学用书，也可供其他相关专业的教师和学生参考使用。

新出图证(鄂)字10号

图书在版编目(CIP)数据

抽象代数引论/刘宏伟，左可正，陈生安主编. —武汉：华中师范大学出版社，2014.8

(普通高等教育"十二五"规划教材/新世纪新理念高等院校数学教学改革与教材建设精品教材)

ISBN 978-7-5622-6616-7

Ⅰ.①抽… Ⅱ.①刘… ②左… ③陈… 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(2014)第092120号

抽象代数引论

©刘宏伟 左可正 陈生安主编

责任编辑：田小容 袁正科　　**责任校对**：易 雯　　**封面设计**：胡 灿

编辑室：第二编辑室　　**电话**：027－67867362

出版发行：华中师范大学出版社

社址：湖北省武汉市珞喻路152号　　**邮编**：430079

销售电话：027－67863426/67863280(发行部)　027－67861321(邮购)　027－67863291(传真)

网址：http://www.ccnupress.com　　**电子信箱**：hscbs@public.wh.hb.cn

印刷：湖北新华印务有限公司　　**督印**：章光琼

开本：787 mm×1092 mm　1/16　　**印张**：7.75　　**字数**：180千字

版次：2014年11月第1版　　**印次**：2014年11月第1次印刷

印数：1—2000　　**定价**：15.00元

欢迎上网查询、购书

普通高等教育“十二五”规划教材
新世纪新理念高等院校数学教学改革与教材建设精品教材

丛书编写委员会

丛书总序

未来社会是信息化的社会，以多媒体技术和网络技术为核心的信息技术正在飞速发展，信息技术正以惊人的速度渗透到教育领域中，正推动着教育教学的深刻变革。在积极应对信息化社会的过程中，我们的教育思想、教育理念、教学内容、教学方法与手段以及学习方式等方面已不知不觉地发生了深刻的变革。

现代数学不仅是一种精密的思想方法、一种技术手段，更是一个有着丰富内容和不断向前发展的知识体系。《国家中长期教育改革和发展规划纲要(2010－2020年)》指明了未来十年高等教育的发展目标："全面提高高等教育质量"、"提高人才培养质量"、"提升科学研究水平"、"增强社会服务能力"、"优化结构办出特色"。这些目标的实现，有赖于各高校进一步推进数学教学改革的步伐，借鉴先进的经验，构建自己的特色。而数学作为一个基础性的专业，承担着培养高素质人才的重要作用。因此，新形势下高等院校数学教学改革的方向、具体实施方案以及与此相关的教材建设等问题，不仅是值得关注的，更是一个具有现实意义和实践价值的课题。

为推进教学改革的进一步深化，加强各高校教学经验的广泛交流，构建高校数学院系的合作平台，华中师范大学数学与统计学学院和华中师范大学出版社充分发挥各自的优势，由华中师范大学数学与统计学学院发起，诚邀华中和周边地区部分颇具影响力的高等院校，面向全国共同开发这套"新世纪新理念高等院校数学系列精品教材"，并委托华中师范大学出版社组织、协调和出版。我们希望，这套教材能够进一步推动全国教育事业和教学改革的蓬勃兴盛，切实体现出教学改革的需要和新理念的贯彻落实。

总体看来，这套教材充分体现了高等学校数学教学改革提出的新理念、新方法、新形式。如目前各高等学校数学教学中普遍推广的研究型教学，要求教师少

讲、精讲，重点讲思路、讲方法，鼓励学生的探究式自主学习，教师的角色也从原来完全主导课堂的讲授者转变为学生自主学习的推动者、辅导者，学生转变为教学活动的真正主体等。而传统的教材完全依赖教师课堂讲授、将主要任务交给任课教师完成、学生依靠大量的被动练习应对考试等特点已不能满足这种新教学改革的推进。如果再叠加脱离时空限制的网络在线教学等教学方式带来的巨大挑战，传统教材甚至已成为教学改革的严重制约因素。

基于此，我们这套教材在编写的过程中注重突出以下几个方面的特点：

一是以问题为导向、引导研究性学习。教材致力于学生解决实际的数学问题、运用所学的数学知识解决实际生活问题为导向，设置大量的研讨性、探索性、应用性问题，鼓励学生在教师的辅导、指导下于课内课外自主学习、探究、应用，以加深对所学数学知识的理解、反思，提高其实际应用能力。

二是精选内容、逻辑清晰。整套教材在各位专家充分研讨的基础上，对课堂教学内容进一步精炼浓缩，以应对课堂教学时间、教师讲授时间压缩等方面的变革；与此同时，教材还在各教学内容的结构安排方面下了很大的功夫，使教材的内容逻辑更清晰，便于教师讲授和学生自主学习。

三是通俗易懂、便于自学。为了满足当前大学生自主学习的要求，我们在教材编写的过程中，要求各教材的语言生动化、案例更切合生活实际且趣味化，如通过借助数表、图形等将抽象的概念用具体、直观的形式表达，用实例和示例加深对概念、方法的理解，尽可能让枯燥、繁琐的数学概念、数理演绎过程通俗化，降低学生自主学习的难度。

当然，教学改革的快速推进不断对教材提出新的要求，同时也受限于我们的水平，这套教材可能离我们理想的目标还有一段距离，敬请各位教师，特别是当前教学改革后已转变为教学活动“主体”的广大学子们提出宝贵的意见！

朱长江

于武昌桂子山

2013 年 7 月

前　言

抽象代数是我国综合性大学和师范类院校数学及相关专业重要的基础课程之一，随着现代科技水平的迅猛发展，抽象代数的相关理论和知识在计算机、信息通信等领域也得到了广泛的应用，因此，它也是这些领域相关专业本科生的选修课程之一。

国内外已有较多抽象代数方面的相关教材和教学参考书，但由于这门课程具有知识内容高度抽象、逻辑推理非常严密等特点，所以，大多数学生学起来比较吃力，且最后的效果也不是很理想。我们结合自身多年教学实践及体会，共同编写此书，以期能对这种情况的扭转做一些探索和尝试。

本书作者既有在师范院校从事多年抽象代数课程教学与研究的相关学者，也有在其他专门院校（如农学、工学等）从事本课程教学的老师，各自所面对的教学对象具有不同的专业背景。针对这些不同专业学生的实际情况，同时也考虑到在当前教学改革的大环境下，抽象代数课程的内容和学时也需要不断地更新和调整，因此，我们在传统抽象代数教学内容的基础上，对其进行了适当取舍和重新组织，既保证了知识内容的基本完整性和连续性，又突出重点，使得学生在经过一学期的课程学习后能够掌握本门课程的基本内容和基本思想，同时能运用通过学习这门课程培养出来的逻辑思维能力和推理能力来处理相关的应用问题。

本书主要涵盖了抽象代数课程中的群、环、域等基本概念和相关性质，同时也包含了这些知识在中学数学中的一些应用：如三大古典几何作图问题、代数基本定理等。在主要内容的安排上力求做到深入浅出、系统完整，在习题的安排上尽量做到难易适中。每一小节的习题均分为 A、B 两组，A 组为必做题，B 组为选做题。

本书第 1 章和第 2 章的 1～4 节由华中师范大学刘宏伟编写；第 2 章的 5～8 节由湖北师范学院左可正编写；第 3 章 1～3 节由华中农业大学张四兰编写；第 3 章 4～6 节由湖北工业大学方次军编写；第 4 章由华中师范大学陈刚和湖北科技学院陈生安共同编写。全书由刘宏伟统稿、定稿。

尽管在编写过程中我们做出了较大努力，但由于水平有限，书中肯定存在诸多不妥之处，敬请广大读者批评指正。

编者

2014 年 7 月

本书符号说明

$\mathbf{Z}$	整数集(环)
$\mathbf{Q}$	有理数集(域)
$\mathbf{Z}^+$(或 $\mathbf{N}$)	所有非负整数(或自然数)的集合
$\mathbf{Z}_m$	所有模整数 m 剩余类的集合
$R^\times$	幺环 R 的所有可逆元构成的乘法群
$\sim$	同态
$\cong$	同构
$\forall$	对所有
$\square$	表示证明完毕
$A:=B$	用 A 记 B
id_A	集合 A 上的恒等映射(恒等变换)
$m\mid n$	整数 m 整除整数 n
$f(x)\mid g(x)$	多项式 $f(x)$ 整除多项式 $g(x)$
$\gcd(m,n)$	整数 m,n 的最大公约数
$\mathrm{lcm}(m,n)$	整数 m,n 的最小公倍数
$\exp(x)$	自然指数函数(即 $\exp(x)=\mathrm{e}^x$)
$\det \boldsymbol{A}$	矩阵 $\boldsymbol{A}$ 的行列式
$\deg f(x)$	多项式 $f(x)$ 的次数
$\mathrm{Char}\ R$	环 R 的特征
$\lvert G\rvert$	群 G 的阶
$o(a)$	群中元素 a 的阶
$A\leqslant B$	A 是 B 的子群(子环)
$N\lhd G$	N 是群 G 的正规子群
$\langle a\rangle$	由群中元素 a 生成的子群
(a)	由环中元素 a 生成的主理想
S_n	n 次对称群
A_n	n 次交错群
K_4	Klein 四元群
$\mathrm{Sym}(M)$	集合 M 上的对称群

$\mathrm{End}(G)$	加群 G 的自同态环
$Z(G)$	群 G 的中心
$C_G(H)$	群 G 中子群 H 的中心化子
$N_G(H)$	群 G 中子群 H 的正规化子
$\mathrm{Ker}(\varphi)$	同态映射 φ 的核
$\mathrm{Im}(\varphi)$	同态映射 φ 的象
$\mathrm{Aut}(G)$	群 G 的自同构群
$\mathrm{Inn}(G)$	群 G 的内自同构群
$\lvert G:H\rvert$	群 G 中子群 H 的指数
$\lvert K:F\rvert$	扩域 K 在子域 F 上的扩张次数
$F[S]$	子集 S 在域 F 上生成的环
$F(S)$	子集 S 在域 F 上生成的域
$GL_n(F)$	域 F 上一般线性群
$SL_n(F)$	域 F 上特殊线性群
$M_n(R)$	环 R 上的所有 n 阶方阵的集合
$M_{m\times n}(R)$	环 R 上的所有 $m\times n$ 矩阵的集合

目 录

第 1 章

集合与映射

本章介绍集合、等价关系和映射，这三个概念在现代数学中具有基础性的地位。

1.1 集合及其运算

集合是数学中不予定义的原始对象，是现代数学中的最基本也是最重要的概念之一，在数学的几乎所有分支中都要用到这个概念。

集合可以描述。一般来说，一个集合是一些数学对象的群体，它使得我们可以明确识别一个对象是在这个群体里面还是不在这个群体里面。

通常用大写英文字母 A,B,C 等表示集合；用小写英文字母 a,b,c 等表示组成集合的对象。如果对象 a 在 A 里面，称 a 是 A 的元素，或称 a 是 A 的成员，此时记作 $a\in A$，读作“a 属于 A”。

如果对象 a 不在 A 里面，称 a 不是 A 的元素，或称 a 不是 A 的成员，此时记作 $a\notin A$，读作“a 不属于 A”。

通常有以下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。如：$A=\{a,b,c,d\}$，$B=\{$301 班，302 班，305 班$\}$。

描述性记法：在花括号中描述集合的元素。如：$S=\{P\mid P$ 是中国的省或直辖市$\}$。又如：实数轴上 0 到 1 闭区间实数的集合 $[0,1]=\{r\mid r$ 是实数，$0\leqslant r\leqslant 1\}$。

本书中，我们还采用以下记号表示一些常用的集合：$\mathbf{Z}=\{$整数$\}$，$\mathbf{Q}=\{$有理数$\}$，$\mathbf{R}=\{$实数$\}$，$\mathbf{C}=\{$复数$\}$，$\mathbf{N}=\mathbf{Z}^{+}=\{$所有非负整数$\}=\{0,1,2,\cdots\}$。

没有元素的集合称为**空集**，记作 $\varnothing$。如果集合 A 中的成员都在集合 B 中，则称集合 A 是集合 B 的子集。更严格地，我们有如下定义：

定义 1.1.1 设 A,B 是两个集合。如果对任意 $a\in A$ 有 $a\in B$，则称 A 是 B 的**子集**，记作 $A\subseteq B$，或 $B\supseteq A$。也说 A 包含于 B，或说 B 包含 A。

特别地，如果 $A\subseteq B$ 且 $B\subseteq A$，则称集合 A 与 B **相等**，记作 $A=B$。如果 $A\subseteq B$ 但 $A\neq B$，就说 A 是 B 的**真子集**，记作 $A\subsetneq B$。

空集是任何集合的子集。

容易证明：集合的包含具有传递性。即：如果 $A\subseteq B,B\subseteq C$，则 $A\subseteq C$。

定义 1.1.2 设 A,B 是两个集合，称

$$A\cup B:=\{x\mid x\in A\text{ 或 }x\in B\}$$

为 A 与 B 的**并集**。称

$$A\cap B:=\{x\mid x\in A \text{ 且 } x\in B\}$$

为 A 与 B 的**交集**。称

$$A-B:=\{x\mid x\in A \text{ 但 } x\notin B\}$$

为 A 与 B 的**差集**。

按定义有：

$$A\cap B\subseteq A,\quad A\cup B\supseteq A,\quad A-B\subseteq A,\quad (A-B)\cap B=\varnothing。$$

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

(1) 并集定义为 $\bigcup\limits_{i\in I}A_i:=\{a\mid \text{存在 } i\in I \text{ 使得 } a\in A_i\}$；

(2) 交集定义为 $\bigcap\limits_{i\in I}A_i:=\{a\mid \text{对任意 } i\in I \text{ 有 } a\in A_i\}$。

例 1.1.1 设集合 $I=[0,1]$ 表示从 0 到 1 的全体实数组成的闭区间，$i\in I$，$A_i=\{r\mid 0\leqslant r\leqslant i\}$，则容易得到

$$\bigcup_{i\in I}A_i=[0,1],\quad \bigcap_{i\in I}A_i=\{0\}。$$

关于集合的运算，我们有以下运算规律：

命题 1.1.1 设 A，B，C 是集合，则以下运算律成立：

(1) 交换律：$A\cap B=B\cap A$，$A\cup B=B\cup A$；

(2) 结合律：$(A\cap B)\cap C=A\cap(B\cap C)$，$(A\cup B)\cup C=A\cup(B\cup C)$；

(3) 分配律：$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$，$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$；

(4) 幂等律：$A\cap A=A$，$A\cup A=A$；

(5) 吸收律：$A\cap(A\cup B)=A$，$A\cup(A\cap B)=A$；

(6) 德摩根律：$A-(B\cap C)=(A-B)\cup(A-C)$，$A-(B\cup C)=(A-B)\cap(A-C)$。

证明 只证明德摩根律中的第二个等式，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 $A-(B\cup C)\subseteq(A-B)\cap(A-C)$。

综上可得 $A-(B\cup C)=(A-B)\cap(A-C)$。 □

定义 1.1.3 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 $\mathscr{P}(S)$，即 $\mathscr{P}(S)=\{A\mid A \text{ 是 } S \text{ 的子集}\}$。

命题 1.1.2 设 S，T 是两个集合，则 $S\subseteq T$ 当且仅当 $\mathscr{P}(S)\subseteq\mathscr{P}(T)$。

证明 必要性。任取 $C\in\mathscr{P}(S)$，由定义 1.1.3 知，$C\subseteq S$，从而 $C\subseteq T$，得 $C\in\mathscr{P}(T)$，即得 $\mathscr{P}(S)\subseteq\mathscr{P}(T)$。

充分性。因为 $S\in\mathscr{P}(S)$，$\mathscr{P}(S)\subseteq\mathscr{P}(T)$，故 $S\in\mathscr{P}(T)$，从而 $S\subseteq T$。　□

由命题 1.1.2，容易得到下述推论：

推论 1.1.1　设 S，T 是两个集合，则 $S=T$ 当且仅当 $\mathscr{P}(S)=\mathscr{P}(T)$。

注 1.1.1　对 $A\in\mathscr{P}(S)$，记 $\overline{A}=S-A$，称为 A 在 S 中的**补集**。对任意 $A\in\mathscr{P}(S)$，有 $\overline{A}\in\mathscr{P}(S)$。因此对任意 $A,B\in\mathscr{P}(S)$，集合 $\overline{A}$，$A\cap B$，$A\cup B$，$A-B$ 还是 $\mathscr{P}(S)$的元素。我们把“$\cup$”，“$\cap$”，“$-$”，“ $\overline{\ }$ ”称为集合 $\mathscr{P}(S)$上的运算。命题 1.1.1 也描述了集合 $\mathscr{P}(S)$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 $\mathscr{P}(S)$中的德摩根律表述为以下形式：

$$\overline{B\cap C}=\overline{B}\cup\overline{C},\quad \overline{B\cup C}=\overline{B}\cap\overline{C}。$$

对集合 S 的任何子集 A 容易证明：$A\cap\overline{A}=\varnothing$。

利用已知集合，可以构造出新的集合。

定义 1.1.4　设 A 和 B 是两个集合，称集合

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

为 A 与 B 的**卡氏积**，也称为**集合积**，简称**积**。这里(a,b)表示有顺序的元素序列，且$(a,b)=(a',b')$当且仅当 $a=a'$，$b=b'$。

例 1.1.2　取 $A=B=\mathbf{R}$，实数集 $\mathbf{R}$ 与自身的卡氏积为 $\mathbf{R}\times\mathbf{R}=\{(a,b)\mid a,b\in\mathbf{R}\}$，简记为 $\mathbf{R}^2$，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我们说(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：

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

这里(a,b,c)表示有顺序的元素序列。

例 1.1.3　取 $A=B=C=\mathbf{R}$，实数集 $\mathbf{R}$ 的三重卡氏积 $\mathbf{R}^3=\mathbf{R}\times\mathbf{R}\times\mathbf{R}=\{(a,b,c)\mid a,b,c\in\mathbf{R}\}$，立体解析几何中它与欧氏空间的点一一对应。

定义 1.1.5　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，$|\mathbf{Z}^+|=\infty$，$|[0,1]|=\infty$，都是无限集。

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

$\mathbf{Z}^+$ 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，称$[0,1]$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。

容易得到任意有限集合 A 与 B 的卡氏积 $A\times B:=\{(a,b)\mid a\in A,b\in B\}$的基数为

$|A\times B|=|A|\cdot|B|$。即使 A，B 中有空集，这个公式也是正确的，参看习题 1.1(B 类)第 1 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，如果对任意两个互异的标号 $i\neq j\in I$ 都有 $A_i\cap A_j=\varnothing$，我们就称并集 $A:=\bigcup\limits_{i\in I}A_i$ 是**不交并集**。对于这样的不交并集 A 中的任意一个元素 x，只存在唯一的指标 $i\in I$，使得 $x\in A_i$，因此只要把每个 A_i 的元素个数都计数一遍，就正好把 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 $\left|\bigcup\limits_{i\in I}A_i\right|=\sum\limits_{i\in I}|A_i|$。

但关于一般集合的并集的基数计算就要复杂得多，其中任意两个有限集合的并集是最简单的情形。

命题 1.1.3 (容斥原理)设 A，B 是有限集合，证明：

$$|A\cup B|=|A|+|B|-|A\cap B|。$$

证明 容易得到

$$A\cup B=(A-B)\cup(B-A)\cup(A\cap B),$$

其中等式右边的都是不交并，参见习题 1.1(A 类)第 7 题的(3)。因此有

$$\begin{aligned}|A\cup B|&=|(A-B)\cup(B-A)\cup(A\cap B)|=|A-B|+|B-A|+|A\cap B|\\&=|A|-|A\cap B|+|B|-|B\cap A|+|A\cap B|=|A|+|B|-|A\cap B|。\end{aligned}$$ □

习题 1.1

(A 类)

1. 求 $\varnothing\cap A$，$\varnothing\cup A$。
2. 设 $A=\{\{\varnothing,\{\varnothing\}\},\{\{\varnothing\},\varnothing\}\}$。
   (1) $\mathscr{P}(A)$ 中的元素有多少个？
   (2) 判断下列哪些结论是正确的：

   $$\varnothing\in A,\ \{\varnothing,\{\varnothing\}\}\in A,\ \{\varnothing,\{\varnothing\}\}\subseteq A,\ \{\{\{\varnothing\},\varnothing\}\}\subseteq A,\ \{\varnothing,\{\{\varnothing\}\}\}\in A。$$

3. 判断下列结论是否正确，如果正确，请证明；如果错误，请给出反例。
   (1) $(A\times A)\cup(B\times C)=(A\cup B)\times(A\cup C)$；
   (2) $(A\times B)-(A\times C)=A\times(B-C)$；
   (3) $A-B$ 一定不是 B 的子集。
4. 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) $\left(\bigcap\limits_{i\in I}A_i\right)\cup B=\bigcap\limits_{i\in I}(A_i\cup B)$；
   (2) $\left(\bigcup\limits_{i\in I}A_i\right)\cap B=\bigcup\limits_{i\in I}(A_i\cap B)$。
5. 设 A，B 分别为如下集合，分别计算这两个集合的差。
   (1) $A=\{2,5,6\}$，$B=\{1,2,4,7,9\}$，求 $A-B$，$B-A$；
   (2) A 是素数的集合，B 是奇数的集合，求 $A-B$。
6. 设 $A=\{\alpha,\beta\}$，$B=\{1,2,3\}$。求 $A\times B$，$B\times A$，$A\times A$，$B\times B$，$(A\times B)\cap(B\times A)$。

7. 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) $A\cup B=(A-B)\cup(A\cap B)\cup(B-A)$。

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

(B 类)

1. 设 A,B 是集合。证明：

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

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

2. 设 A,B,C 是集合，且 $C\neq\varnothing$。证明以下三个条件等价：

(1) $A\subseteq B$；

(2) $(A\times C)\subseteq(B\times C)$；

(3) $(C\times A)\subseteq(C\times B)$。

3. 设 X,Y,Z 是集合，且 $X\neq\varnothing$。证明：若 $X\times Y=X\times Z$，则 $Y=Z$。

4. 设 A,A',B,B' 分别是集合，且满足 $|A|=|A'|$，$|B|=|B'|$。证明：

$$|A\times B|=|A'\times B'|。$$

进一步，如果还有 $A\cap B=\varnothing=A'\cap B'$，那么 $|A\cup B|=|A'\cup B'|$。

5. 设 A,B,C 是有限集合。证明：

$$|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|。$$

6. 设集合 A 有 101 个元素。试问：

(1) 集合 A 有多少个子集？

(2) 其中有多少个子集的元素个数为奇数？

(3) 是否会有 102 个元素的子集？

1.2 关　　系

在日常生活以及数学中，经常会考虑集合上的各种关系，如一个学校的学生集合中的同班关系，实数集合 $\mathbf{R}$ 上的小于关系，等等。

用集合语言来描述就是：集合 A 上的关系 $\sim$，是说对任意 $a,b\in A$ 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：

定义 1.2.1　非空集合 A 上的**关系** $\sim$ 是卡氏积 $A\times A$ 的一个子集，即 $\sim\subseteq A\times A$。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 $\sim$。

定义 1.2.2　非空集合 A 上的关系 $\preceq$ 称为一个**偏序关系**，如果以下三条满足：

自反律：对任意 $a\in A$，有 $a\preceq a$；

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

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

例 1.2.1 $\mathbf{R}$ 上的关系“$\leqslant$”是偏序关系。集合 S 的幂集 $\mathscr{P}(S)$ 上的包含关系“$\subseteq$”是偏序关系。

本节主要讨论集合上的一种特殊的关系——“等价关系”，它与集合的划分有密切联系。

定义 1.2.3 非空集合 A 上的关系 $\sim$ 称为一个**等价关系**，如果以下三条满足：

自反律：对任意 $a\in A$，有 $a\sim a$；

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

对称律：对任意 $a,b\in A$，如果 $a\sim b$，则 $b\sim a$。

注 1.2.1 (1) 任何非空集合 A 上的等价关系一定存在。如：$R=\{(a,a)\mid a\in A\}$，$R_A=A\times A$ 均是等价关系。这两个等价关系有时称为集合 A 上的“最小等价关系”和“最大等价关系”。

(2) 设 $\sim$ 是集合 A 上的等价关系，$a\in A$。将 A 中所有与 a 具有关系“$\sim$”的元素放在一起构成的集合 $[a]=\{b\in A\mid b\sim a\}$ 称为 a 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。

(3) 因为 $a\sim a$，故按等价类的定义有 $a\in[a]$，因此也常说 $[a]$ 是 a 所在的等价类。特别地，$[a]\neq\varnothing$。

例 1.2.2 设 $A=\{1,2,3,4,5\}$，定义：$a\sim b\Leftrightarrow 2\mid(a+b)$，$\forall a,b\in A$。证明：$\sim$ 是集合 A 上的一个等价关系，并求其所有等价类。

证明 对任意 $a\in A$，有 $2\mid(a+a)$，所以 $a\sim a$ 成立。设 $a,b\in A$，若有 $a\sim b$，则 $2\mid(a+b)$，从而 $2\mid(b+a)$，所以 $b\sim a$ 成立。再设 $a,b,c\in A$，若有 $a\sim b,b\sim c$，则 $2\mid(a+b),2\mid(b+c)$，从而 $2\mid[(a+b)+(b+c)]$，于是 $2\mid(a+c)$，所以 $a\sim c$ 成立。因此 $\sim$ 是 A 上的一个等价关系。

由等价类的定义，有

$$[1]=\{x\in A\mid x\sim 1\}=\{x\in A\mid 2\mid(x+1)\}=\{1,3,5\}=[3]=[5],$$

$$[2]=\{x\in A\mid x\sim 2\}=\{x\in A\mid 2\mid(x+2)\}=\{2,4\}=[4]。\qquad\square$$

例 1.2.3 设 m 是非零整数。在整数集 $\mathbf{Z}$ 上定义“模 m 同余关系”：对 $a,b\in\mathbf{Z}$，如果 $m\mid(a-b)$，则记 $a\equiv b(\mathrm{mod}\ m)$，称 a 模 m 同余于 b。证明：

(1) $\equiv(\mathrm{mod}\ m)$ 是 $\mathbf{Z}$ 上的等价关系；

(2) 等价类 $[a]_m=a+m\mathbf{Z}$，其中 $m\mathbf{Z}:=\{mk\mid k\in\mathbf{Z}\}$ 是所有 m 的倍数的集合，而 $a+m\mathbf{Z}:=\{a+d\mid d\in m\mathbf{Z}\}$。这里用 $[a]_m$ 记 $a\in\mathbf{Z}$ 所在的模 m 同余的等价类，通常称为模 m **剩余类**。

证明 (1) 仿照例 1.2.2 可以证明 $\equiv(\mathrm{mod}\ m)$ 是 $\mathbf{Z}$ 上的等价关系。

(2) 对 $a\in\mathbf{Z}$，a 所在的等价类是

$$\begin{aligned}[a]_m&=\{x\in\mathbf{Z}\mid x\sim a\}=\{x\in\mathbf{Z}\mid m\mid(x-a)\}=\{x\in\mathbf{Z}\mid x=a+mk,k\in\mathbf{Z}\}\\&=\{a+mk\mid k\in\mathbf{Z}\}=a+m\mathbf{Z}。\qquad\square\end{aligned}$$

特别地，当 $m=2$ 时，在全体整数集合 $\mathbf{Z}$ 上，模 2 同余关系是等价关系，等价类