近世代数

姚炳学　编著

科学出版社

近世代数

姚炳学　编著

科学出版社

北京

内 容 简 介

本书介绍了几类最基本的代数系统. 全书共五章: 第 1 章介绍基本概念, 它是后面各章的基础; 第 2 章介绍群的基本理论, 主要包括群的概念与性质、几类简单的群、子群、商群, 以及群的同态与同构; 第 3 章介绍环的基本理论, 主要包括环的概念与性质、理想与商环, 以及环的同态与同构; 第 4 章介绍整环里的因子分解理论; 第 5 章介绍域的扩张及其在几何作图中的应用.

本书可作为应用型普通高校数学与应用数学专业学生的选用教材, 也可作为其他从事代数学、信息科学、计算机科学研究的专业人员的参考用书.

图书在版编目（CIP）数据

近世代数 / 姚炳学编著. —北京：科学出版社，2018.1
ISBN 978-7-03-055483-3

Ⅰ. 近… Ⅱ. 姚… Ⅲ. 抽象代数 Ⅳ. O153

中国版本图书馆 CIP 数据核字（2017）第 282054 号

责任编辑：王胡权 / 责任校对：张凤琴
责任印制：吴兆东 / 封面设计：迷底书装

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

北京教图印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2018 年 1 月第 一 版 开本：720×1000 B5
2018 年 1 月第一次印刷 印张：11 1/8
字数：225 000

定价：39.00 元

（如有印装质量问题，我社负责调换）

前　言

近世代数既是现代数学的基础，也是现代科学的基础，因为近世代数的概念和方法已经渗透到现代科学的各个分支. 近世代数是每位数学工作者所必须具备的数学知识，也是研究物理学、计算机科学、信息科学等不可缺少的工具. 近世代数的主要研究对象是代数系统的代数结构，而代数结构是重要的数学结构之一，是数学研究对象的一个重要方面.

近世代数是公认的比较难学的课程之一，尤其对于普通高等院校的学生. 其原因在于近世代数概念抽象，推理严密，而且例子较少. 应用型人才培养特色名校建设工程的开展，迫切要求出版一本适用普通高等院校、具备“少而精”特点的近世代数教材，既不能面面俱到，又必须包含最基本的内容. 本书就是为应用型普通高等院校数学专业学生编写的. 本书主要包括群论与环论两部分内容，虽然内容不多，但却体现了丰富的数学思想和方法. 掌握这些数学思想与方法远比记忆概念本身与定理结论重要得多. 希望学生通过一个学期的学习，理解和掌握近世代数的基本内容、基本方法和基本理论，初步具备应用近世代数的思想和理论处理和解决实际问题的能力，为进一步学习现代数学或从事数学教学打下坚实的基础.

本书内容一般 60 学时可讲完，带 * 号的内容可选学. 在每一节后都附有适量的习题，这部分习题大都是基本的，学生在理解了教材的有关内容后就可独立完成. 个别稍难的习题，需要对有关知识深刻理解，并掌握一定的解题技巧.

本书的编写得到“聊城大学应用型人才培养特色名校工程系列教材”出版基金的资助，也得到聊城大学数学科学学院领导的支持和同事的帮助，在此一并对他们表示衷心感谢.

限于编者水平，书中疏漏与不妥之处在所难免，恳请各位专家和读者批评指正.

编　者

2017 年 5 月

目　录

第1章 基本概念

近世代数在数学的各个分支都有重要的应用. 近世代数的主要内容就是研究带有运算的集合, 即代数系统, 其中群与环是最重要的代数系统. 本书主要介绍这两种代数系统的基本内容.

本章主要介绍常用到的一些基本概念, 这些概念在后面的各章中都要用到.

1.1 集 合

集合(set)是近代数学上最基本的概念之一, 它是指由一些事物所组成的一个整体, 集合也简称为集. 组成集合的各个事物称为这个集合的元素或元.

当我们所讨论的问题限定在某一集合内时, 这个集合称为论域或全集, 记为 U.

集合通常用大写拉丁字母 $A,B,C,\cdots$ 表示. 特别地, $\mathbb{C}$ 表示**复数集**(the set of complex numbers), $\mathbb{R}$ 表示**实数集**(the set of real numbers), $\mathbb{Q}$ 表示**有理数集**(the set of rational numbers), $\mathbb{Z}$ 表示**整数集**(the set of integers), $\mathbb{N}$ 表示**自然数集**(the set of natural numbers), 即非负整数集. 另外, $\mathbb{C}^*$ 表示**非零复数集**, $\mathbb{R}^+$ 表示**正实数集**, $2\mathbb{Z}$ 表示**偶数集**, 其余类同.

集合中的元素常用小写拉丁字母 $a,b,c,\cdots$ 来表示. 如果 a 是集合 A 中的一个元素, 就说 a 属于集合 A, 记为 $a\in A$; 如果 a 不是集合 A 中的元素, 就说 a 不属于集合 A, 记为 $a\notin A$. 不包含任何元素的集合称为**空集**(empty set), 记为 $\varnothing$.

包含有限个元素的集合称为**有限集**(finite set), 包含无穷多个元素的集合称为**无限集**(infinite set). 有限集 A 所包含的元素个数用 $|A|$ 表示, 特别地, $|\varnothing|=0$.

表示一个集合的方法通常有列举法和描述法.

列举法就是列出它的所有元素, 并用大括号括起来. 例如,

$$A=\{1,3,5,7\},\quad B=\{\text{红, 黄, 蓝}\},\quad C=\left\{1,\frac{1}{2},\frac{1}{3},\cdots\right\}.$$

描述法就是利用元素所具有的特性来刻画集合. 例如,

$$D=\{\text{全体自然数}\},\quad E=\{x\mid x^2-3x+2=0\}.$$

定义 1.1.1 如果集合 A 的每一个元素都属于集合 B, 则称 A 是 B 的一个**子**

集(subset), 也称 A 包含于 B, 记为 $A \subseteq B$.

如果集合 A 是集合 B 的一个子集, 且集合 B 中有元素不在集合 A 中, 则称 A 是 B 的一个**真子集**(proper subset), 记为 $A \subset B$.

空集被认为是任何集合的子集.

由集合 A 的所有子集为元素构成的集合, 称为 A 的**幂集**(power set), 记为 $P(A)$. 例如, 若 $A=\{1,2,3\}$, 则 $P(A)=\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},A\}$.

易知, 当 $|A|=n$ 时, $|P(A)|=2^n$.

当集合 A 与集合 B 有完全相同的元素时, 称 A 与 B **相等**, 记为 $A=B$. 显然, $A=B$ 当且仅当 $A\subseteq B$ 且 $B\subseteq A$.

定义 1.1.2 由集合 A 和集合 B 的所有公共元素构成的集合, 叫做 A 与 B 的**交集**(intersection set), 简称 A 与 B 的**交**, 记为 $A\cap B$.

例如, 若 $A=\{0,1,3,5\}, B=\{1,2,3\}, C=\{4,5,6\}$, 则 A 与 B 的交为 $A\cap B=\{1,3\}$. 而 B 与 C 的交为空集, 即 $B\cap C=\varnothing$.

定义 1.1.3 由集合 A 和集合 B 的所有元素作成的集合, 叫做 A 与 B 的**并集**(union set), 简称 A 与 B 的**并**, 记为 $A\cup B$.

例如, 在上面的例子中, A 与 B 的并为 $A\cup B=\{0,1,2,3,5\}$, 而 B 与 C 的并为 $B\cup C=\{1,2,3,4,5,6\}$.

定义 1.1.4 设论域为 U, A 为 U 的子集. 由 U 中不属于 A 的元素作成的集合, 叫做 A 的**补集**或**余集**(complementary set), 记为 A^c 或 A'.

例如, 若论域 $U=\{1,2,3,4,5,6,7,8,9,10\}$, $A=\{1,3,5,7,9\}$, 则 $A^c=\{2,4,6,8,10\}$.

定义 1.1.5 设论域为 U, A,B 为 U 的子集, 由 U 中既属于 A 又不属于 B 的元素作成的集合, 叫做 A 与 B 的**差集**(difference set), 记为 $A-B$ 或 $A\setminus B$.

例如, 若论域 $U=\{1,2,3,4,5,6,7,8,9,10\}$, $A=\{1,3,5,7,9\}$, $B=\{1,2,3,4,5\}$, 则 $A-B=\{7,9\}$.

不难验证, 集合的运算满足以下性质.

定理 1.1.1 设论域为 U, A,B,C 为 U 的三个子集, 则有

(1) 幂等律: $A\cap A=A, A\cup A=A$;

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

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

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

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

(6) 两极律: $A\cup U=U, A\cap U=A, A\cup\varnothing=A, A\cap\varnothing=\varnothing$;

(7) 补余律: $A\cup A^c=U, A\cap A^c=\varnothing$;

(8) 复原律: $(A^c)^c = A$;

(9) 对偶律: $(A\cup B)^c = A^c \cap B^c, (A\cap B)^c = A^c \cup B^c$.

集合的 "交" 与 "并", 可以推广到任意多个子集的情况.

设论域为 U, I 为一个非空指标集, 对每个 $i\in I$, A_i 为 U 的子集, 定义这些子集的 "**交**" 与 "**并**" 如下:

$$\bigcap_{i\in I} A_i = \{x\in U \mid \forall i\in I, x\in A_i\}, \quad \bigcup_{i\in I} A_i = \{x\in U \mid \exists i\in I, 使 x\in A_i\}.$$

容易验证, 当 B 也是 U 的子集时, 有

$$B\cup\left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I}(B\cup A_i), \quad B\cap\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I}(B\cap A_i);$$

$$\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c, \quad \left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c.$$

习题 1.1

1. 判断下列命题的真假.

(1) $a\in\{a\}$; (2) $a\subseteq\{a\}$; (3) $\{a\}\subseteq\{a\}$; (4) $a\in\{a,\{a\}\}$; (5) $\{a\}\subseteq\{a,\{a\}\}$;

(6) $\{a\}\in\{a,\{a\}\}$; (7) $\varnothing\subseteq\{a\}$; (8) $\varnothing\subseteq\varnothing$; (9) $\varnothing\in\{\varnothing\}$; (10) $\varnothing\subseteq\{\varnothing\}$.

2. 设 A,B,C 是论域 U 的三个子集. 证明:

(1) 若 $A\cap B = A\cup B$, 则 $A = B$;

(2) 若 $A\cap B = A\cap C, A\cup B = A\cup C$, 则 $B = C$.

3. 设 A,B 是两个有限集合. 证明:

$$|A\cup B| = |A| + |B| - |A\cap B|.$$

4. 设 A,B,C 是论域 U 的三个子集. 证明:

(1) $A - B = A\cap B^c$;

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

(3) $A - (B\cap C) = (A - B)\cup(A - C)$;

(4) $A\cap(B - C) = (A\cap B) - (A\cap C)$;

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

1.2 映　　射

映射是在两个集合之间建立的一种联系, 通过映射来研究代数系统, 是近世代数中一种重要的研究方法.

定义 1.2.1　设 X 与 Y 是两个非空集合, 如果有一个对应法则 f, 使得对于

X 中每个元素 x，在 Y 中都有一个唯一确定的元素 y 与它对应，则称 f 为集合 X 到集合 Y 的一个**映射**(mapping)，X 称为这个映射的**定义域**(domain)，记为

$$f: X \to Y,$$
$$x \mapsto f(x),$$

也可简记为 $f: X \to Y$ 或 $f: x \mapsto y, \forall x \in X$. 并且把 $y = f(x)$ 叫做 x 在映射 f 之下的**像**(image)，而 x 叫做 y 在映射 f 之下的**原像**或**逆像**(preimage).

例 1.2.1 设 $X = \{a,b,c\}, Y = \{1,3,5,7\}$，则

$$f: X \to Y,$$
$$a \mapsto 1, \quad b \mapsto 3, \quad c \mapsto 7$$

是 X 到 Y 的一个映射；而

$$g: X \to Y,$$
$$a \mapsto 1, \quad b \mapsto 1, \quad c \mapsto 1$$

也是 X 到 Y 的一个映射；但

$$h: X \to Y,$$
$$a \mapsto 1, \quad b \mapsto 7$$

不是 X 到 Y 的映射，因为 X 中的元素 c 在 h 下没有像.

例 1.2.2 设 $\mathbb{Q}$ 为有理数集，则法则

$$f: \mathbb{Q} \to \mathbb{Q},$$
$$\frac{b}{a} \mapsto a + b$$

不是 $\mathbb{Q}$ 到 $\mathbb{Q}$ 的映射，因为对于 $\frac{1}{2}$ 和 $\frac{2}{4}$，显然它们在 $\mathbb{Q}$ 中表示同一个元素，但是按照对应法则 f，它们的像却不同，从而不符合映射的定义.

从上面的例子可以看出，集合 X 到集合 Y 的一个对应法则 f 必须满足下列三个条件时才是 X 到 Y 的一个映射:

(1) X 中的每个元素在对应法则 f 下都有确定的像;

(2) X 中的每个元素的像都在 Y 中;

(3) X 中的相等的元素的像也相等.

定义 1.2.2 设 f 是集合 X 到集合 Y 的一个映射.

(1) 若 A 是 X 的一个子集，则称 Y 的子集

$$\{f(x) \mid x \in A\}$$

为 A 在 f 下的像，记为 $f(A)$. 特别地，$f(X)$ 称为 f 的**值域**(codomain)，也记为 $\mathrm{Im} f$.

(2) 若 B 是 Y 的一个子集, 则称 X 的子集

$$\{x \in X \mid f(x) \in B\}$$

为 B 在 f 下的**逆像**, 记为 $f^{-1}(B)$. 特别地, 当 $B=\{b\}$ 为单元素集合时, $f^{-1}(\{b\})$ 也简记为 $f^{-1}(b)$.

根据上面所述定义, 若 B 是 Y 的子集, 则 $x \in f^{-1}(B) \Leftrightarrow f(x) \in B$. 并且 $f(\varnothing)=\varnothing$, $f^{-1}(\varnothing)=\varnothing$.

在例 1.2.1 中, 若 $A=\{a,b\}$, $B=\{5,7\}$, 则 $f(A)=\{1,3\}$, $f^{-1}(B)=\{c\}$, $\operatorname{Im} f=\{1,3,7\}$.

定义 1.2.3 设 f 与 g 都是集合 X 到集合 Y 的映射. 如果对 X 中每个元素 x 都有 $f(x)=g(x)$, 则称映射 f 与映射 g **相等**, 记为

$$f=g.$$

例如, 设 $X=\{1,2,3\}$, $Y=\{2,4,6,8,10\}$,

$$f: x \mapsto 2^x, \quad g: x \mapsto x^2-x+2,$$

则 $f=g$. 因为 $f(1)=2=g(1)$, $f(2)=4=g(2)$, $f(3)=8=g(3)$.

定义 1.2.4 设 f 是集合 X 到集合 Y 的一个映射. 若在 f 下 Y 中每个元素在 X 中都有逆像, 即对任意的 $y \in Y$, 存在 $x \in X$, 使 $f(x)=y$, 则称 f 是 X 到 Y 的一个**满射**(surjection).

根据这个定义, 集合 X 到集合 Y 的映射 f 是满射当且仅当 $f(X)=Y$.

定义 1.2.5 设 f 是集合 X 到集合 Y 的一个映射. 若在 f 下 X 中不相等的元素在 Y 中的像也不相等, 即由 $x_1 \neq x_2$ 能推出 $f(x_1) \neq f(x_2)$, 则称 f 是 X 到 Y 的一个**单射**(injection).

显然, 映射 $f: X \to Y$ 是单射, 当且仅当 f 满足 $f(x_1)=f(x_2) \Rightarrow x_1=x_2$, $\forall x_1, x_2 \in X$.

定义 1.2.6 设 f 是集合 X 到集合 Y 的一个映射. 若 f 既是满射, 又是单射, 则称 f 是 X 到 Y 的一个**双射**(bijection).

当 f 是集合 X 到集合 Y 的一个双射时, 对于任意的 $y \in Y$, 由于只有唯一的 $x \in X$, 使 $f(x)=y$, 因此法则

$$Y \to X,$$
$$y \mapsto x, \quad \text{使 } f(x)=y$$

给出了一个集合 Y 到集合 X 的映射, 而且是个双射. 这个映射称为 f 的逆映射, 记为 f^{-1}, 即 $f^{-1}(y)=x$.

应注意, 只有当 f 是一个双射时, f 才有逆映射 f^{-1}, 此时 $f^{-1}(y)$ 是一个元素. 而当 f 为一般映射时, $f^{-1}(y)$ 是一个集合, 即

$$f^{-1}(y)=f^{-1}(\{y\})=\{x\in X\mid f(x)=y\}.$$

定理 1.2.1　设 X 与 Y 是两个有限集合，且 $|X|=|Y|$，则集合 X 到集合 Y 的一个映射 f 是满射当且仅当 f 是单射.

证　设 $|X|=|Y|=n$，且 $X=\{x_1,x_2,\cdots,x_n\}$，$Y=\{y_1,y_2,\cdots,y_n\}$，

$$f: x_i\to y_{k_i}\quad (i=1,\cdots,n;1\leqslant k_i\leqslant n)$$

是 X 到 Y 的一个映射.

若 f 是满射，则由 $x_1\neq x_2$，必有 $y_{k_1}\neq y_{k_2}$. 因若 $y_{k_1}=y_{k_2}$，则

$$f(X)=\{y_{k_1},y_{k_2},\cdots,y_{k_n}\}$$

最多有 $n-1$ 个元素，因此 $f(X)\neq Y$，这与 f 是满射矛盾. 这种讨论对 X 中任意两个元素都成立，因此 f 是单射.

反之，设 f 是单射，则由于 X 中不同元素的像也不同，故 $|f(X)|=n=|Y|$. 但 $f(X)\subseteq Y$，故 $f(X)=Y$，即 f 是满射. □

由上述定理，容易得到下面的结论.

推论 1.2.1　如果 X 与 Y 是两个有限集合，且 $|X|=|Y|$，则 X 到 Y 的映射 f 是双射当且仅当 f 是满(单)射.

根据定义 1.2.2，映射 $f: X\to Y$ 可以诱导下列两个映射:

$$f: P(X)\to P(Y),$$
$$A\mapsto f(A)=\{f(x)\mid x\in A\},\quad \forall A\subseteq X$$

及

$$f^{-1}: P(Y)\to P(X),$$
$$B\mapsto f^{-1}(B)=\{x\in X\mid f(x)\in B\},\quad \forall B\subseteq Y.$$

在这里，我们依然用 f 表示映射 $P(X)\to P(Y)$. 因为如果对 $f(x)$ 与 $f(\{x\})$ 不加区别的话，映射 $f: P(X)\to P(Y)$ 可以看成是映射 $f: X\to Y$ 的扩展.

需要注意的是，符号 f^{-1} 可以表示映射 $f^{-1}: P(Y)\to P(X)$，也可以表示 f 的逆映射，但只有当 f 为双射时，f 才能有逆映射 f^{-1}.

不难验证，映射 $f: P(X)\to P(Y)$ 与 $f^{-1}: P(Y)\to P(X)$ 满足下列性质.

定理 1.2.2　设 $f: X\to Y$ 是一个映射，$A, A_1, A_2\subseteq X$，$B, B_1, B_2\subseteq Y$，则下列性质成立.

(1) $A_1\subseteq A_2\Rightarrow f(A_1)\subseteq f(A_2)$.

(2) $B_1\subseteq B_2\Rightarrow f^{-1}(B_1)\subseteq f^{-1}(B_2)$.

(3) $f(A_1\cup A_2)=f(A_1)\cup f(A_2)$，$f(A_1\cap A_2)\subseteq f(A_1)\cap f(A_2)$.

(4) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

(5) $f^{-1}(B^c) = f^{-1}(B)^c$.

(6) $A \subseteq f^{-1}(f(A))$, 当 f 是单射时 "=" 成立; $f(f^{-1}(B)) \subseteq B$, 当 f 是满射时 "=" 成立.

证明留作习题.

定义 1.2.7　设 f 是集合 X 到集合 Y 的一个映射, 而 g 是集合 Y 到集合 Z 的一个映射. 对于任意的 $x \in X$, 规定

$$h(x) = g(f(x)),$$

则 h 是集合 X 到集合 Z 的一个映射, 称为映射 f 与 g 的**合成**(composition), 记为 $g \circ f$, 即

$$(g \circ f)(x) = g(f(x)), \quad \forall x \in X.$$

映射 f 与 g 的合成 $g \circ f$ 有时也简记为 gf.

映射的合成可用图 1.2.1 表示出来, 这种图称为**交换图**(commuting diagram).

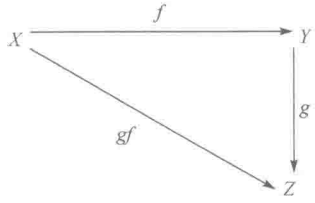

图 1.2.1　交换图

映射的合成满足下列性质.

定理 1.2.3　设 $f: X \to Y$, $g: Y \to Z$, $h: Z \to W$ 是三个映射, 则

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

证　显然 $(h \circ g) \circ f$ 与 $h \circ (g \circ f)$ 有相同的定义域 X. 又对任意的 $x \in X$,

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))),$$

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))),$$

因此, $(h \circ g) \circ f = h \circ (g \circ f)$. □

定义 1.2.8　集合 X 到自身的映射, 叫做集合 X 的一个**变换**(transformation).

同样可以定义满射变换、单射变换、双射变换. 集合 X 的双射变换也称为 X 的一一变换.

定理 1.2.4　含 n 个元素的任意集合共有 $n!$ 个双射变换.

证　设 $X = \{1,2,\cdots,n\}$, 则对 X 的每个双射变换 φ, 都能确定元素 $1,2,\cdots,n$ 的一个全排列

$$\varphi(1)\varphi(2)\cdots\varphi(n).$$

反之, 元素 $1,2,\cdots,n$ 的任意一个全排列都确定 X 的一个双射变换; 而且不同的排列确定不同的双射变换. 因此这 n 个元素有多少个全排列, X 就有多少个双射变换. 由于 n 个元素共有 $n!$ 个全排列, 故 X 共有 $n!$ 个双射变换. □

集合 X 的变换

$$f: x \mapsto x, \quad \forall x \in X$$

称为 X 的**恒等变换**(identity transformation), 通常记为 1_X.

恒等变换必为一一变换, 但一一变换不一定是恒等变换.

例如, $f: n \mapsto n+1, \forall n \in \mathbb{Z}$ 是整数集 $\mathbb{Z}$ 的一个一一变换, 但显然不是 $\mathbb{Z}$ 的恒等变换.

不难验证, 若 $f: X \to Y$ 是映射, 则

$$1_Y \circ f = f, \quad f \circ 1_X = f.$$

习题 1.2

1. 设 $F^{2\times 2}$ 为数域 F 上全体 2 阶方阵作成的集合. 问

$$f: \boldsymbol{A} \mapsto |\boldsymbol{A}|, \quad \forall \boldsymbol{A} \in F^{2\times 2}$$

是否是 $F^{2\times 2}$ 到 F 的一个映射? 是否是满射或单射?

2. 设 $f: X \to Y$, $g: Y \to Z$ 是两个映射. 证明:

(1) 若 f, g 为单射, 则 gf 为单射;

(2) 若 f, g 为满射, 则 gf 为满射;

(3) 若 gf 为单射, 则 f 为单射;

(4) 若 gf 为满射, 则 g 为满射.

3. 证明定理 1.2.2.

4. 设 $f: X \to Y$ 是一个映射. 证明:

(1) f 为单射 $\Leftrightarrow$ 存在映射 $g: Y \to X$, 使 $gf = 1_X$;

(2) f 为满射 $\Leftrightarrow$ 存在映射 $g: Y \to X$, 使 $fg = 1_Y$.

5. 设 $X = \{x_1, x_2, \cdots, x_n\}$, $Y = \{y_1, y_2, \cdots, y_m\}$. 问

(1) 从 X 到 Y 可以规定多少个不同的映射?

(2) 当 $m = n$ 时, 从 X 到 Y 可以规定多少个不同的双射?

1.3　卡氏积与代数运算

集合与映射是近代数学中的最基本的概念, 而代数运算则是一种特殊的映射.

定义 1.3.1　设 X, Y 是两个非空集合, 称集合

$$\{(x, y) \mid x \in X, y \in Y\}$$

为集合 X 与集合 Y 的**笛卡儿积**(Cartesian product), 简称**卡氏积**, 记为 $X \times Y$. 即 $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$, 且规定

$$(x_1,y_1)=(x_2,y_2)\Leftrightarrow x_1=x_2,y_1=y_2.$$

一般地，$X\times Y\neq Y\times X$. 例如，设 $X=\{1,2\}$, $Y=\{a,b,c\}$，则

$$X\times Y=\{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\},$$

$$Y\times X=\{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}.$$

当 X,Y 都有限时，$|X\times Y|=|Y\times X|$.

卡氏积的概念可以推广到 n 个集合的情形. 设 $X_1,X_2,\cdots,X_n$ 为 n 个集合，则称集合

$$\{(x_1,x_2,\cdots,x_n)\mid x_i\in X_i,i=1,2,\cdots,n\}$$

为集合 $X_1,X_2,\cdots,X_n$ 的**卡氏积**，记为 $X_1\times X_2\times\cdots\times X_n$ 或 $\prod_{i=1}^{n}X_i$.

定义 1.3.2　设 X,Y,Z 是三个非空集合. 集合 $X\times Y$ 到集合 Z 的一个映射叫做一个 $X\times Y$ 到 Z 的**代数运算**(algebraic operation). 特别地，$X\times X$ 到 X 的代数运算称为 X 的代数运算，也称为 X 的**二元运算**或**运算**.

一个代数运算通常用 $\circ$ 表示，并将 (x,y) 在 $\circ$ 下的像记为 $a\circ b$，即元素 x 与 y 在运算 $\circ$ 下的结果为 $a\circ b$. 在不会引起混淆的情况下也将 $a\circ b$ 简记为 ab.

例 1.3.1　一个 $\mathbb{Z}\times\mathbb{Z}^*$ 到有理数集 $\mathbb{Q}$ 的映射

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

是 $\mathbb{Z}\times\mathbb{Z}^*$ 到 $\mathbb{Q}$ 的一个代数运算.

例 1.3.2　设 M 是数域 F 上的 n 维向量空间，则映射

$$\circ:(\lambda,\boldsymbol{\alpha})\mapsto\lambda\boldsymbol{\alpha}$$

是 $F\times M$ 到 M 的一个代数运算.

今后我们将主要讨论集合 M 的二元运算.

当 $M=\{x_1,x_2,\cdots,x_n\}$ 是一个有限集合时，M 的代数运算 $\circ$ 可以用下面的矩形表来表示:

$\circ$	x_1	x_2	…	x_n
x_1	d_{11}	d_{12}	…	d_{1n}
x_2	d_{21}	d_{22}	…	d_{2n}
⋮	⋮	⋮		⋮
x_n	d_{n1}	d_{n2}	…	d_{nn}

其中，$d_{ij}=x_i\circ x_j, i=1,2,\cdots,n, j=1,2,\cdots,n.$

这个表称为 M 的**运算表**或**乘法表**(multiplication table).

当非空集合 M 有代数运算 $\circ$ 时，称 $(M,\circ)$ 是一个**代数系统**(algebraic system)，或简称 M 是一个代数系统. 更一般地，一个代数系统可以有多个代数运算.

例如，数的普通加法、减法与乘法都是整数集、有理数集、实数集和复数集的代数运算.

例 1.3.3　设 M 是一个非空集合，则子集的“并”与“交”是 M 的幂集 $P(M)$ 的两个代数运算.

下面我们给出变换的一种代数运算.

设 M 是一个非空集合，$T(M)$ 是由 M 的全体变换作成的集合. 任取 $\sigma,\tau\in T(M)$，定义 $\sigma\tau$ 为

$$\sigma\tau: x\mapsto \sigma(\tau(x)),\quad \forall x\in M,$$

则显然 $\sigma\tau\in T(M)$，从而是 $T(M)$ 的一个代数运算，并称这个代数运算为**变换的乘法**(multiplication of transformation)，即变换的乘法就是变换的合成.

若 $S(M)$ 表示 M 的全体一一变换的集合，则 $S(M)$ 是 $T(M)$ 的一个子集. 下面证明，变换的乘法也是 $S(M)$ 的代数运算，即 M 的任意两个一一变换的“乘积”仍是 M 的一一变换.

事实上，任取 $\sigma,\tau\in S(M)$，$a\in M$，则由于 σ 是 M 的一个满射变换，所以存在 $b\in M$，使 $\sigma(b)=a$. 又因为 τ 也是 M 的一个满射变换，所以存在 $c\in M$，使 $\tau(c)=b$. 于是

$$(\sigma\tau)(c)=\sigma(\tau(c))=\sigma(b)=a,$$

即 $\sigma\tau$ 是 M 的满射变换.

任取 $x,y\in M$，若有 $(\sigma\tau)(x)=(\sigma\tau)(y)$，则 $\sigma(\tau(x))=\sigma(\tau(y))$. 由于 σ 是 M 的单射变换，故 $\tau(x)=\tau(y)$. 而 τ 也是 M 的单射变换，所以 $x=y$. 因此，$\sigma\tau$ 是 M 的单射变换.

这说明 $\sigma\tau$ 是 M 的一一变换，故变换的乘法也是 $S(M)$ 的代数运算.

习题 1.3

1. 设 M 为正整数集，下列各个法则 $\circ$ 是否是 M 的代数运算?

(1) $a\circ b=a+b-1$;

(2) $a\circ b=b$;

(3) $a\circ b=\dfrac{a}{b}$;