抽象代数学

上海科学技术出版社

抽象代数学

谢邦杰 编著

上海科学技术出版社

内 容 提 要

本书是作者通过多年教学实践而写成的，系统地介绍了近代的代数学的基础知识，可供理工科二年级以上的同学与科技、教育工作者的自学与参考用书。全书共分八章，其内容分别是：基本概念与方法，群论，交换环论，域论，线性代数，有序的与赋值的代数系统，具有链条件的环论，一般的环论。每节末附有较多的思考题以助对基础理论的消化与对基本功的磨练。书末附有一些近代文献。全书的内容是按照由浅入深、循序渐进、配以 * 号的原则而灵活适用于自学、教学以至科研的需要而写的。

抽 象 代 数 学

谢 邦 杰　编著

上海科学技术出版社出版

（上海瑞金二路 450 号）

新华书店上海发行所发行　上海商务印刷厂印刷

开本 850×1156 1/32　印张 18.25　字数 486,000

1982 年 5 月第 1 版　1982 年 5 月第 1 次印刷

印数 1—10,000

统一书号：13119·984　　定价：（科五）2.25 元

序　　言

抽象代数学是近代数学的一个重要分支. 它不仅在知识方面，而且在思想方法上，对于学习和研究近代数学都起着很明显而有力的作用，甚至对研究其它自然科学，如理论物理和理论化学等都是不可缺少的工具.

对于本书的取材、写法以及如何使用等方面，有如下一些考虑和说明：

一、在基础知识面上力求能够宽广一些. 就同性质的一般书来说，本书的下列内容常常未必属于取材之列：拓扑空间与拓扑群；Lie 代数；非交换行列式；无零因子的有限维实交错代数；赋范环与理想理论；近期的环与根论等.

二、在深度方面，本书的某些部分较同性质的书来说要深入一些. 具体说来如：从通常的 Galois 理论讲到 Krull 的 Galois 理论；从一般非结合代数讲到 Albert 定理，Artin 定理及推广的 Frobenius 定理；从通常的交换环论讲到与赋值论密切相关的 Dedekind 环论；从有链条件的环讲到近期的根的抽象理论等.

三、为了使青年初学者能循序渐进得更快一些，特对某些内容加上 * 号. 不带 * 号的部分已自成系统，看完这些内容后，再从广度和深度方面发展而看带 * 号的内容. 这样分两步走，效率可能更高一些.

四、为了贯彻少而精的原则和加强对基本功的训练，每节只有少数最基本的定理，而在每节末却安排了大量的理论性思考题，这些题的多数是对基本定理的发展或推广. 例如只讲一般的群而不讲算子群，仅把后者安排在思考题中并明确指出哪些基本定理可以毫不费力地推广到算子群中去. 希望这样做能收到事半功倍、举一反三的效果. 有些思考题还是新成果的介绍，但指明了出处.

这样有利于培养青年同志的独立工作能力和科研工作的习惯．同时也为了磨练基本功，故不附题目解答．仅对少量较难而基本的题目附有提示或扼要的解答．

以上考虑仅系对研究生讲课的初步尝试，有待于更多的实践．对于本书一切不妥以及错误之处，务请读者多加批评和帮助．

谢邦杰，1979.12.8.

目　录

第一章 基本概念与方法

§1. 集　合

集合论中的概念与方法是全部近代数学的基础.

关于**集合**的定义，有各种不同的提法. 例如集合论的创始人 Cantor 就定义集合的概念为:

一组确定的,人们在直觉或思维上的不同对象,作为一个整体来想象,就称为一个集合.

概率论的权威 Kolmogorov 在其经典著作"概率论基本概念"中却这样定义集合:

一个东西 M 与某些别的东西 a, b, … 等以一种固有的不下定义的方式相互决定着；这种关系我们表为：集合 M 由 a, b, … 等东西所作成.

数学名著之一，Van der Waerden 的代数学中又是这样定义的:

每个单个元素具有或者不具有的性质就定义一个集合；这个集合的元素就是全体具有这个性质的对象.

还有其它一些提法,如

由某性质所确定的对象物的总体称为一个集合；或一组无重复的东西作成的总体称为一个集合,等等.

通常用大写字母 A, B 等表示集合；小写字母 a, b 等表示集合的**元素**. 当 a 是集合 A 的元素时，简称 a 属于 A 或 A 含 a，记为

$$a\in A \quad \text{或} \quad A\ni a.$$

不含元素的集合称为**空集合**，常记为$\emptyset$. 对任意集合 A 恒有 $\emptyset\subset A$. 因当 $x\in\emptyset$ 时,必有 $x\in A$. 例如所有满足

$$x^2<0$$

的实数 x 就作成一个空集合.

有限个元素作成的集合称为**有限集合**;否则称为**无穷集合**.当 $a_1, a_2, \cdots, a_n$ 是有限集合 A 的全部元素时,亦记为

$$A=\{a_1, a_2, \cdots, a_n\},$$

并说 A 为一个 $\boldsymbol{n}$ **元集合**,或 A 的**元数**为 n.

如果凡是集合 A 的元素都是集合 B 的元素,则说 A 是 B 的**子集合**(或简称**子集**),也说 A 含于 B 或 B 包含 A, 记为

$$A\subset B \quad 或 \quad B\supset A.$$

如果 $A\subset B$ 且 $B\subset A$, 则说两集合 A 与 B **相等**,记为

$$A=B.$$

如果 $A\subset B$ 且 $A\neq B$(即 A 与 B **不相等**,或简称 A **不等于** B),则说 A 为 B 的**真子集**,也说 A 小于 B 或 B 大于 A, 记为

$$A<B \quad 或 \quad B>A.$$

设 A, B 为任意两个集合. 所有既属于 A 又属于 B 的元素作成的集合叫做 A, B 的**交集**,记为

$$A\cap B;$$

所有属于 A 或属于 B 的元素作成的集合叫做 A, B 的**并集**, 记为

$$A\cup B.$$

例如 A 与 B 都是自然数作成的集合的子集,而

$$A=\{1, 2, 3\};\ B=\{3, 4, 5, 6\},$$

则 $$A\cap B=\{3\};\ A\cup B=\{1, 2, 3, 4, 5, 6\}.$$

但不能误认为 $A\cup B$ 等于下面这个“数组”:

$$\{1, 2, 3, 3, 4, 5, 6\},$$

因为集合中没有重复的东西.

命题 1 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

证明. 如果 $a\in A\cap(B\cup C)$, 则有

$$a\in A,\ a\in B\cup C,$$

即 $a\in A$, 且 $a\in B$ 或 $a\in C$. 于是有

$$a\in A\cap B \quad 或 \quad a\in A\cap C,$$

此即 $a\in(A\cap B)\cup(A\cap C)$. 这就证明了

$$\{A\cap(B\cup C)\}\subset\{(A\cap B)\cup(A\cap C)\}. \tag{1}$$

如果 $a\in(A\cap B)\cup(A\cap C)$, 则有

$$a\in A\cap B \quad 或 \quad a\in A\cap C,$$

即 $a\in A$ 且 $a\in B$, 或 $a\in A$ 且 $a\in C$. 于是有

$$a\in A, \quad a\in B\cup C,$$

此即 $a\in A\cap(B\cup C)$. 这便又证得

$$\{(A\cap B)\cup(A\cap C)\}\subset\{A\cap(B\cup C)\}. \tag{2}$$

由(1)与(2)即知

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C). \qquad 证毕.$$

同理可证

命题 2 $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$.

借助于通常的分配律, 命题 1 与 2 就可以毫不费力地记住了. 所以有时也把此二命题统称为: 集合的交、并运算之间的相互对偶的分配律.

设 A 为任意集合, S 是 A 的一个子集. A 中所有不属于 S 的元素作成的集合, 自然又是 A 的一个子集, 叫做 S 在 A 中的**余集**, 记为 $A-S$. 特别地, 当 $S=A$ 时, $A-A$ 为空集合 $\emptyset$.

现在设 A 为一个非空集合. 考虑 A 中元素作成的 n 元序列

$$(a_1, a_2, \cdots, a_n), \quad a_i\in A \quad (i=1, 2, \cdots, n).$$

所有这些 n 元序列作成的集合, 叫做 A 的 ***n* 次幂或 *n* 方**, 记为

$$A^n 或 A\times A\times\cdots\times A(共 n 个 A).$$

特别地, 当 $n=2$ 时, $A^2=A\times A$ 又叫 A 的**平方**; 当 $n=3$ 时,

$$A^3=A\times A\times A$$

又叫 A 的**立方**.

例如 $A=\{a, b\}$ 时, A 的立方就恰含下面 8 个元素:

$$(a, a, a), (a, a, b), (a, b, a), (a, b, b),$$

$$(b, a, a), (b, a, b), (b, b, a), (b, b, b);$$

A 的平方就恰含 4 个元素; A 的 n 方就恰含 2^n 个元素.

现在再设 A 为任意一个集合. A 的所有子集作成的集合叫

做 A 的幂集合，记为 UA. 这时 A 就成为 UA 的一个元素了，而且空集合(作为 A 的子集)也是 UA 的一个元素. 特别地，当 A 为空集合时，UA 却不是空集合，它恰含一个元素，即空集合.

思 考 题

1. 两个集合的交集与并集可以分别推广为若干个集合 $A_i(i\in I)$ 的交集(其中 I 表一集合)

$$\bigcap_{i\in I} A_i$$

与并集

$$\bigcup_{i\in I} A_i.$$

2. 命题 1 可推广为 $A\cap(\bigcup_i B_i)=\bigcup_i(A\cap B_i)$.

3. 命题 2 可推广为 $A\cup(\bigcap_i B_i)=\bigcap_i(A\cup B_i)$.

4. 在一个固定的集合中，若干个子集之交集仍为一子集；若干个子集的并集仍为一子集.

5. 一个集合 A 的一些子集 $S_i(i\in I)$的交集与并集有如下对偶关系:

$$A-\bigcup_i S_i=\bigcap_i(A-S_i),\quad A-\bigcap_i S_i=\bigcup_i(A-S_i).$$

即：并集之余集为余集之交集，交集之余集为余集之并集. 这叫做 **Morgan 定律**.

6. 设 R 为所有实数作成的集合. R 可以看成一条直线上所有的点作成的集合；R^2 可以看成一个平面上所有的点作成的集合. R^3 又可如何看?

7. 如果 A 恰含 n 个元素，则 UA 恰含 2^n 个元素；$U(UA)$ 恰含 2^{2^n} 个元素.

§2. 广 义 映 射

设 $A_1, A_2, \cdots, A_n, D$ 为给定的 $n+1$ 个非空集合. 如果有一规则 f 使对任意的

$$a_1\in A_1,\ a_2\in A_2,\ \cdots,\ a_n\in A_n,$$

恒有唯一的 $d\in D$ 与之相应，记为

$$f(a_1, a_2, \cdots, a_n)=d,$$

则 f 就叫做从 $A_1, A_2, \cdots, A_n$ 到 D 内的一个广义映射，而 d 则叫

做 $a_1, a_2, \cdots, a_n$ 在此广义映射 f 下的映象.

广义映射的概念是单值函数的概念的推广. 当上面的诸 A_i 与 D 都是实数集 R 时, 广义映射 f 就是定义在 R^n 上的一个实函数.

一般说来, 在广义映射 f 下, D 的任意一个元素未必能当"映象". 这犹如一个实函数的值不能取遍一切实数时, 任意一个实数就未必能当"函数值"一样.

如果上面的广义映射 f 能使 D 中每个元素都有机会当映象, 则就说这个 f 是到 D 上的一个广义映射. 对于到 D 内的广义映射, 也不排斥它能到 D 上.

从上面的一般定义中, 我们来看四个方面的重要特款:

(一) 当 $A_1, A_2, \cdots, A_n, D$ 都是同一个非空集合 A 时, 广义映射 f 就特称为 **A 的一个 n 元运算**. 特别地, $n=2$ 时, A 的一个 2 元运算又简称 **A 的一个运算**(即从 **A, A 到 A 内的一个广义映射**); $n=1$ 时, A 的一个 1 元运算又叫做 **A 的一个变换** (或从 **A 到 A 内的一个映射**). 一个非空集合的运算与变换都是今后经常要碰到的基本概念, 是非常重要的.

(二) 当 $n=1$ 时, 令 $A_1=A$, 广义映射 f 又叫做**从 A 到 D 内的一个映射**. 从一个非空集合到一个非空集合内的映射, 也是一个基本而重要的概念, 它又是上面的基本概念"变换"的推广(当这两个非空集合相等时, 映射就是变换).

(三) 当 $n=2$ 时, 令 $A_1=A$, $A_2=B$, 广义映射 f 就是从 A, B 到 D 内的一个广义映射, 特称为**从 A, B 到 D 的一个运算**. 这显然是一个非空集合的运算的推广, 同样是一个基本而重要的概念.

(四) 当 $A_1, A_2, \cdots, A_n$ 是同一个非空集合 A, 而

$$D=\{\text{有}, \text{无}\}$$

是由两个字"有"与"无"作成的集合时, 广义映射 f 又叫做 **A 中元素之间的一个 n 元关系**, 并当 A 中元素 $a_1, a_2, \cdots, a_n$ 合于

$$f(a_1, a_2, \cdots, a_n)=\text{有}$$

时, 就说 $a_1, a_2, \cdots, a_n$ 在 A 中有 n 元关系 f. 特别地, $n=2$ 时, A 中元素之间的一个 2 元关系又简称 **A 中元素之间的一个关系**.

这也是一个非常基本而重要的概念.

下面几节就是对广义映射的这几种重要的特款作进一步较详细的阐述. 所以对初学者来说, 如果感到本节的概念太多, 则可以跳过上面这一段, 只要看完广义映射的定义(包括在 D 内和在 D 上), 就直接看下几节也行. 看完后再把上一段作为简单概括的总结来看.

思 考 题

1. 设 f 为 A 中元素之间的一个 2 元关系. 于是 $A^2=A\times A$ 中所有满足

$$f(a, b)=\text{有}$$

的有序对 (a, b) 就作成 A^2 的一个子集 F. 显然 F 是由 f 所唯一确定的. 反过来, A^2 的任意一个子集 F 也唯一确定 A 中元素之间的一个 2 元关系 f, 使得在上面这样的考虑下, f 在 A^2 中所唯一确定的子集恰为此 F. 所以 A 中元素之间的一个关系可以用 A^2 中的一个子集来具体刻划. 同样, 对 n 元关系又当如何具体刻划?

2. $n+1$ 元关系的概念是 n 元运算的概念的推广.

3. 关系的概念是多值函数的概念的推广.

4. $n>2$ 时, n 元关系的概念是多元多值函数的概念的推广.

5. 由题 1 知 A 的一个关系可由 A^2 的一个子集 F 来具体刻划, 故不妨就用符号 F 来表此关系, 且当 a, b 有此关系时就记为 aFb. 于是

aFb 必要而且只要 $(a, b)\in F$.

这样一来, 就可以定义 A 的某个关系 F **包含**于某关系 F' 中, $F\subset F'$, 以及若干个关系的**交**与**并**(关系). 而且关系 F 的**余**关系就可以通过 F 在 A^2 中的余集来定义.

6. A 的两个关系 F, G 的**乘积**定义为下面这样的一个关系(记为 FG):

$aFGb$ 成立必要而且只要有 $C\in A$ 使 aFc 和 cGb 成立.

于是这样定义的关系与关系的乘法就适合结合律但不适合交换律.

7. 如果 F_i(i 取遍足指标集 I 中的元素)与 G 都是 A 的关系, 则有

$$\left(\bigcup_{i\in I} F_i\right)G=\bigcup_{i\in I}(F_iG), \quad G\left(\bigcup_{i\in I} F_i\right)=\bigcup_{i\in I}(GF_i).$$

并由此易证: 当 $F\subset F'$ 时, 就有

$$FG\subset F'G, \quad GF\subset GF'.$$

8. 对 A 的每个关系 F 恒存在一个所谓它的**逆**关系 F^{-1}:

$aF^{-1}b$ 成立必要而且只要 bFa 成立. 于是有

(i) $(F^{-1})^{-1}=F$;

(ii) 当 $F\subset G$ 时，就有 $F^{-1}\subset G^{-1}$;

(iii) $(FG)^{-1}=G^{-1}F^{-1}$;

(iv) $(\bigcup_{i\in I}F_i)^{-1}=\bigcup_{i\in I}F_i^{-1}$;

(v) $(\bigcap_{i\in I}F_i)^{-1}=\bigcap_{i\in I}F_i^{-1}$.

9. 任意非空集合 A 恒有一个所谓单位关系 E:

aEb 成立必要而且只要 $a=b$.

于是有 $E^{-1}=E$; 对 A 的任意关系 F 有 $FE=EF=F$.

10. 由 A^2 的空子集定义的关系叫做 A 的空关系，记为 0. 于是对 A 的任意关系 F 恒有 $0\subset F$, $F0=0F=0$.

§3. 运　算

设 A 为一个非空集合. 从 A, A 到 A 内的一个广义映射又特称为 A 的一个**运算**. 也可称为 A 的一个**代数运算**.

例如: 设 R 为所有实数作成的集合. 通常对数的加法就是 R 的一个运算，并早已称之为加法运算. 同样，减法与乘法也都是 R 的运算. 除法不是 R 的运算，因为对实数 a, 0 就没有实数与之相应，更谈不上唯一性了. 不过习惯上早已把除法叫做除法运算，为了弥补在概念上的不严密性，我们可以把除法叫做 R 的一个**部分运算**. 同理，乘方

$$a,\ b\to a^b\quad (a,\ b\in R,\ a>0)$$

也是 R 的一个部分运算.

从 A 到 A 内的映射，本来是下节要阐述的内容，但为了解释为什么它又叫做 A 的 1 元运算，或者说，为什么要在 A 的 n 元运算中考虑特款 $n=1$(甚至还会发展出 0 元运算的概念)？乃在此顺便说明如下:

在 R 中对正数开 n 方

$$a\to\sqrt[n]{a}\quad (a\in R,\ a>0,\ \sqrt[n]{a}\in R)$$

不仅早已习惯地称为开方运算，而且按照上面的定义，它确实是 R 的一个部分运算:

$$a,\ n \to \sqrt[n]{a} \quad (a,\ n \in R,\ a>0,\ n\text{ 为自然数}).$$

特别是，当 n 为奇数时，对每个 $a\in R$ 都有唯一的 $\sqrt[n]{a}\in R$ 与之相应，故把"开奇次方"叫做 R 的一个 1 元运算，不仅从习惯上易于理解而接受，并且它确实是 R 的 n 元运算的特款 $n=1$ 的情形．于是开偶次方也就可以叫做 R 的一个部分 1 元运算．

设 $A,\ B,\ D$ 为三个非空集合．从 $A,\ B$ 到 D 内的一个广义映射又叫做从 $A,\ B$ 到 D 的一个**运算**(或**代数运算**)．

例如：设 V 是实数域 R 上的一个向量空间．R 与 V 的纯量乘法就是从 $R,\ V$ 到 V 的一个运算．又当 V 为 R 上的一个欧氏空间时，V 的向量的内积(运算)就是从 $V,\ V$ 到 R 的一个运算．

从 $A,\ B$ 到 D 的运算是 A 的运算的推广，后者是前者的特款 $A=B=D$ 的情形．

思 考 题

1．数学分析中的在定义域 D 上的一个二元实函数

$$u=f(x,\ y)$$

何时能够是实数集 R 的一个运算？何时只能够是 R 的一个部分运算？

2．复变函数中的在定义域 D 上的一个单值函数

$$w=f(z)$$

是所有复数作成的集合的什么运算？

§4．映射与变换

设 $A,\ D$ 为两个非空集合．如果对 A 中任意元素都能规定 D 的一个确定的元素与之相应，则这个规则就叫做**从 A 到 D 内的一个映射**．映射显然是 §2 中广义映射在 $n=1$ 时的特款．

通常用希腊字母 $\sigma,\ \tau,\ \cdots$ 等代表映射．如果 σ 是从 A 到 D 内的一个映射，而 $a\in A$，则与 a 相应的 $\sigma(a)\in D$ 就叫做 **a 在 σ 下的映象**，以后就记为 a^{σ}．当 A_0 是 A 的一个非空子集时，A_0 中所有元素在 σ 下的映象作成 D 的一个非空子集，叫做 **A_0 在 σ 下的映象集合**，或简称 **A_0 在 σ 下的映象**，记之为 A_0^{σ}．特别地，A^{σ} 是

D 的非空子集，但在一般情况下，A^σ 未必等于 D．当 $A^\sigma=D$ 时，特称 σ 为把 A 映到 D 上的映射，或说 σ 是从 A 到 D 上的映射．一般说 σ 把 A 映到 D 内并不排斥可能映到 D 上．

设 σ 与 τ 都是从 A 到 D 内的映射．如果

$$a^\sigma=a^\tau,\ 对任意\ a\in A,$$

则说 σ **等于** τ，记为 $\sigma=\tau$．此时 σ 与 τ 为同一个映射，只不过符号不同罢了．

设 σ 是从 A 到 D 内的一个映射．D 的一个元素可能不是 A 的任何元素在 σ 下的映象，也可能是 A 的若干个（不只 1 个）元素的共同映象．如果 D 的任意一个元素恰好是 A 的一个元素的映象，则说 σ 是从 A 到 D 上的**一对一的映射**（这显然是从 A 到 D 上的映射中的特殊映射）．

从 A 到 A 内的一个映射又叫做 **A 的一个变换**（或 **A 的一个 1 元运算**）．

A 的最简单的变换就是把 A 的每个元素映成它自己的变换，叫做 **A 的恒等变换**，记为 I_A（或在不致发生混淆的情况下就简记为 I 也行）：

$$a^{I_A}=a,\ 对任意\ a\in A.$$

现在设 σ 是从 A 到 B 的一个映射，τ 是从 B 到 C 的一个映射．由 σ 与 τ 可以引出从 A 到 C 的一个映射 ρ 如下：

$$a^\rho=(a^\sigma)^\tau,\quad a\in A.$$

这个映射 ρ 叫做 σ 与 τ **之积**，记为

$$\rho=\sigma\tau.$$

也就是有 $$a^{\sigma\tau}=(a^\sigma)^\tau,\ 对任意\ a\in A.$$

上面这样由两个映射 σ 与 τ 引出新映射 $\sigma\tau$ 就叫做映射的**乘法**．或更确切说，用 σ **左乘** τ（或用 τ **右乘** σ）就得到映射的积 $\sigma\tau$，它是一个新的映射．

此时要注意两点：

（一）τ 能右乘 σ，但 σ 未必能右乘 τ．即 $\sigma\tau$ 有意义，但 $\tau\sigma$ 未必有意义．因为当 $B^\tau\not\subseteq A$ 时，$\tau\sigma$ 就没有意义了．所以在积 $\sigma\tau$ 中，

符号 σ 与 τ 的先后次序是不能写错的，$\sigma\tau$ 是先用 σ 去起作用然后再用 τ 去起作用.

(二)任意给定两个映射 σ 与 τ,

$$A \xrightarrow{\sigma} B, \quad C \xrightarrow{\tau} D,$$

以后，欲 $\sigma\tau$ 有意义，必要而且只要 $A^\sigma \subset C$; 欲 $\tau\sigma$ 有意义，必要而且只要 $C^\tau \subset A$. 故一般说来，任意两个映射未必能相乘. 但特别地，当

$$A = B = C = D$$

时，$\sigma\tau$ 与 $\tau\sigma$ 均有意义. 即一个集合 A 的任意两个变换恒可相乘. 不过，此时 $\sigma\tau$ 与 $\tau\sigma$ 未必是 A 的同一个变换，这样的例子我们在几何学上是很熟悉的.

用一句话来概括上面两点，可以简单地陈述为："映射的乘法不适合交换律". 但却有

命题 1 映射的乘法适合结合律. 即只要有

$$A \xrightarrow{\sigma} B, \quad B \xrightarrow{\tau} C, \quad C \xrightarrow{\rho} D,$$

则恒有

$$(\sigma\tau)\rho = \sigma(\tau\rho).$$

证明. 因为对任意 $a \in A$, 有

$$a^{(\sigma\tau)\rho} = (a^{\sigma\tau})^\rho = [(a^\sigma)^\tau]^\rho,$$

$$a^{\sigma(\tau\rho)} = (a^\sigma)^{\tau\rho} = [(a^\sigma)^\tau]^\rho,$$

即有

$$a^{(\sigma\tau)\rho} = a^{\sigma(\tau\rho)}, \text{ 对任意 } a \in A.$$

故由定义即知

$$(\sigma\tau)\rho = \sigma(\tau\rho).$$

证毕.

如果 σ 是从 A 到 B 的一个映射，则显然有

$$I_A\sigma = \sigma, \quad \sigma I_B = \sigma.$$

其中 I_A 与 I_B 分别为 A 与 B 的恒等变换.

如果 σ 是从 A 到 B 上的一个一对一的映射，则 σ 可引出从 B 到 A 上的一个映射 τ 如下：对任意 $b \in B$, 有

$$b^\tau = a, \text{ 当 } a^\sigma = b \text{ 时}.$$

易见 τ 是从 B 到 A 上的一个一对一的映射. 这个 τ 叫做 σ 的逆，它是由 σ 所唯一确定的，记为