高等学校教学参考书

近世代数

范云椽　盛德成

高等教育出版社

高等学校教学参考书

近世代数

范云棣 盛德成

高等教育出版社

内 容 提 要

本书共分五章. 第一章基本概念，第二章群，第三章环与域，第四章格与布尔代数，第五章模及环的进一步讨论.

书中列入较多的富有启发性的例题，各节末附有相当数量的难易程度不同的习题.

本书可作为高等院校数学专业教学参考书.

高等学校教学参考书

近 世 代 数

范云棣　盛德成

*

高等教育出版社出版
新华书店北京发行所发行
河北省香河县印刷厂印装

开本850×1168　1/32　印张7.875　字数196 000
1988年9月第1版　1988年9月第1次印刷
印数 00 001— 2,320
ISBN 7-04-000007-5/O·6

定价 2.95 元

前　言

本书的目的在于为学习“近世代数”的读者提供一本教材或参考书. 本书共分五章. 第一章介绍若干基本概念，它为本书的其余各章提供了一个共同的基础. 对基础较好的读者可以侧重于§1-3至§1-5三节而略去其余各节. 第二章介绍群，第三章介绍环与域，第四章介绍格与布尔代数，这三章是基本内容. 第四章对于对计算机科学有兴趣的读者更是需要的. 第五章介绍“模”及“环论”的一些初步知识，起步比较高一些，我们希望它能为愿意在这方面作进一步钻研的读者开一个头. 几乎每一节的后面都附有相当数量的难易程度不同的习题. 认真做好这些习题可以加深对基本内容的理解，也可以检验读者对基本内容的掌握程度. 有的习题对基本内容作了进一步的补充. 本书最后附有中英对照的名词索引.

本书在写法上力求简明. 初学者往往苦于概念的抽象，因此本书列入了较多的富有启发性的例题和习题，以引起和培养读者的学习兴趣. 本书在介绍基本内容的同时也考虑到为读者提供进一步钻研的余地.

本书由盛德成主笔第一、二、四、五章，由范云棣主笔第三章，并为第五章提供了部分素材. 本书的初稿曾在西北大学多次使用，在此基础上结合教学实践进行几次修改. 西北大学现重起校长对我们合编此书曾给予大力支持和鼓励，我们在此表示衷心的感谢. 同时还感谢对本书初稿的修改曾提过宝贵意见的同行.

由于我们水平所限，因此本书一定还有不少缺点，我们恳切地希望读者批评指正.

作者

目　　录

第一章 基本概念

近世代数是研究各种代数结构的. 例如,群、环、域、格、模等. 但代数结构的基本成分是集和集上的映射. 因此, 在本书中常常要用到集论中的一些概念和结论. 为此, 在着手研究各种代数结构之前,先对集论中的一些基本概念作一个简要的讨论.

§ 1-1 集 · 子集 · 集的运算

集这个概念是数学中的基本概念. 我们对它作如下的说明: 集是由**元素**组成的. 这样,给定了一个集M,即是给出了M是由哪些元素组成的. 例如

数学系全体学生的集.

线性方程组 $Ax=B$ 的解向量的集.

多项式 $f(x)$的零点的集.

平面上过点$M(1,2)$,斜率为 3 的直线上所有点的集.

全部正偶数的集.

所有自然数的集.

数域P上所有m行n列矩阵的集.

多项式 $f(x)$,$g(x)$的所有公因式的集.

一般以大写英文字母A,B,$\cdots$,S,T,$\cdots$表示集,而以小写字母a,b,c,$\cdots$表示集的元素. 两个集M,N**相等**是指它们是由同样的元素组成的, 并记为$M=N$.

若元素a是集A的元素,称a**属于**A,记为 $a\in A$, 否则记为$a\overline{\in} A$.

给出一个集M通常有两种方式.一种是列出集的全部元素,如

$$M=\{1,2,4,7\},N=\{1,2,\cdots,n,\cdots\}.$$
另一种方式是给出集M的定义性质.这时,集M用如下记号表示:
$$M=\{a \mid P(a)\}.$$
它表示M是由所有使命题 $P(a)$为真命题的元素 a 组成的. 例如
$$M=\{d(x) \mid d(x)是 f(x)的因式,d(x)是g(x)的因式\}.$$
给出一个集的这种方式特别重要，尤其当难于列出一个集的全部元素时更是如此.

空集$\varnothing$是指一个元素也没有的集. **例如**
$$M=\{x \mid x 是实数,x^2+1=0\}$$
就是一个空集,即$M=\varnothing$. 空集的引入可以使我们在谈到一个集时不必事先论证它至少有一个元素.

在本书中经常用到的几个集,常用下述记号表示:

N是所有自然数的集.

Z是所有整数的集.

Q是所有有理数的集.

R是所有实数的集.

C是所有复数的集.

设A,B是两个集,若$b\in B\Rightarrow b\in A$(即由$b\in B$能推出$b\in A$),则称B是A的**子集**,记作$B\subseteq A$或$A\supseteq B$. 这样,容易看到
$$A=B\Longleftrightarrow A\subseteq B,B\subseteq A.$$
由此,当我们要证明$A=B$时,我们常常去证明
$$x\in A\Rightarrow x\in B,x\in B\Rightarrow x\in A.$$
例 1-1-1 全体偶数的集E是Z的子集.

对任何集A,$\varnothing\subseteq A$,$A\subseteq A$.

设A是一个给定的集,令
$$P(A)=\{B \mid B\subseteq A\},$$
它是由A的所有子集组成的集,叫做A的**幂集**.

例 1-1-2 若$A=\{1,2\}$,则$P(A)=\{\varnothing,\{1\},\{2\},A\}$.

这儿应该注意 a 与$\{a\}$的区别，当 $a\in A$ 时$\{a\}\in P(A)$。

设A，B是两个集，令

$$A\cap B=\{c\,|\,c\in A, c\in B\},$$

叫做 A 与 B 的**交**.

例 1-1-3 设$A=\{(x,y)\,|\,2x-y=2\}$是方程$2x-y-2=0$的解向量的集，$B=\{(x,y)\,|\,x-2y=2\}$是方程$x-2y-2=0$的解向量的集，则$A\cap B$是方程组

$$\begin{cases}2x-y-2=0\\x-2y-2=0\end{cases}$$

的解向量的集.

设有集簇$\{A_i\,|\,i\in I\}$，令

$$\cap\{A_i\,|\,i\in I\}=\{c\,|\,\text{对每一}i\in I\text{ 有 }c\in A_i\},$$

称为集簇$\{A_i\,|\,i\in I\}$的**交**.

若 $A\cap B=\varnothing$，即 A,B 没有公共元素，则说 A,B **不相交**.

设有集 A,B，令

$$A\cup B=\{c\,|\,c\in A\text{ 或 }c\in B\},$$

称为A与B的**并**.

例 1-1-4 设$A=\{1,2,3\}$，$B=\{2,4,5\}$，则

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

类似地，设有集簇$\{A_i\,|\,i\in I\}$，令

$$\cup\{A_i\,|\,i\in I\}=\{c\,|\,\text{存在一个 }i\in I\text{，使 }c\in A_i\},$$

称为集簇$\{A_i\,|\,i\in I\}$的**并**.

练　　习 1-1

一、下述诸集中哪些是相等的？

$A=\{x\,|\,x<10, x\text{ 是正偶数}\}$；

$B=\{x\,|\,x\in N, x^2<90\}$；

$C=\{2,4,6,8\}$；

$D=\{1,2,3,4,5,6,7,8,9\}$.

二、下述命题哪些是对的？哪些是错的？

1) $\varnothing\in\{\varnothing\}$；

2) $\varnothing\in\varnothing$；

3) $\varnothing\in\{0\}$；

4) $0\in\varnothing$；

5) $\varnothing\in\{\{\varnothing\}\}$；

6) $\{1,2\}\in\{\{1\},\{2\},\{1,2\},\{\{1,2\}\}\}$；

7) $2\in\{\{1\},\{2\},\{1,2\},\{\{1,2\}\}\}$.

三、对任何集 A 完成下述等式：

$$A\cup\varnothing=\qquad;\qquad A\cap A=\qquad;$$
$$A\cap\varnothing=\qquad;\qquad A\cup A=\qquad.$$

四、设 $A=\{1,3,5\}$，$B=\{3,7\}$，$C=\{x\mid x\in N,\ x\geqslant 9\}$，$D=\{x\mid x\in N,\ x<45\}$，$E=\{x\mid x\in N,\ 2<x<50\}$。确定下列各集：

$A\cap D=\qquad$；

$C\cup D=\qquad$；

$C\cup E=\qquad$；

$D\cap E=\qquad$；

$C\cap D\cap E=\qquad$；

$(C\cap D)\cup E=\qquad$；

$\{x\mid x\in N, x^2\in B\}=\qquad$.

五、设 $A=\{a,\square,\triangle,*\}$，写出 $P(A)$ 的全部元素.

六、对于给定的集 A，考虑幂集 $P(A)$，此时常称 A 为**全集**. 对 $B\in P(A)$，称 $B'=\{x\mid x\in A, x\overline{\in}B\}$ 为 B 的**余集**. 试证下述 De Morgan 定理：

$$(B_1\cup B_2)'=B_1'\cap B_2',$$
$$(B_1\cap B_2)'=B_1'\cup B_2',$$

其中 $B_1,B_2\in P(A)$.

§ 1-2 笛卡尔积集·映射

1° 笛卡尔积集

设 S，T 是两个集，令

$$S\times T=\{(s,t)\mid s\in S,t\in T\},$$

其中$(s_1,t_1)=(s_2,t_2)$是指 $s_1=s_2,t_1=t_2$. 称 $S\times T$ **为** S **与** T **的笛卡尔积集**. 这儿并不要求 $S\neq T$. 若 S 有 m 个元素, T 有 n 个元素, 则 $S\times T$ 有 mn 个元素. 例如

设 $S=\{1,2\},T=\{1,2,3\}$, 则 $S\times T=\{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3)\}$.

设 S 为平面上 x 轴上点的集, T 为 y 轴上点的集, 则 $S\times T$ 是整个平面上的点的集.

一般地, 若 $S_1,S_2,\cdots,S_r$ 是任意 r 个集, 则称**所有 r 有序组** $(s_1,s_2,\cdots,s_r)$, $s_i\in S_i$, **的集为 $S_1,S_2,\cdots,S_r$ 的笛卡尔积集**, 并记为 $S_1\times S_2\times\cdots\times S_r$. 从而

$$S_1\times S_2\times\cdots\times S_r=\{(s_1,s_2,\cdots,s_r)\mid s_i\in S_i,1\leqslant i\leqslant r\}.$$

2° 映射

定义 1-2-1 集 S 到集 T 的**一个映射**是指有序三组$\langle S,T,\mu\rangle$, 其中 μ 是一个对应法则, 依此, 对每一 $s\in S$, 有唯一的 $t\in T$ 与之对应. 常记 t 为 $t=s\mu$, 集 S 叫做该映射的**区域**, T 叫**余区域**. 映射$\langle S,T,\mu\rangle$也常常记为 $\mu:S\to T$ 或 $S\xrightarrow{\mu}T$. 当上下文中 S

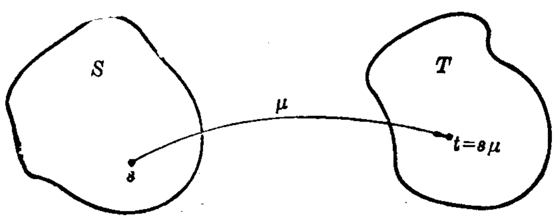

图 1-2-1

及 T 是清楚的时候, 可以简单地说映射 μ. 对于映射 $\mu:S\to T$, 若 $t=s\mu$, 则 t 叫 s 的**象**, s 叫 t 的**前象**.

例 1-2-1 设 S 为整数集, T 为实数集, 则我们有映射 $\mu:S\to$

T，对 $x\in S$，$x\mu=2x$.

例 1-2-2 设 S 是数域 P 上的 n 阶方阵的集，$T=P$，则我们有映射 $\mu:S\to T$，对 $x\in S$，$x\mu=|x|$ 是矩阵 x 的行列式.

例 1-2-3 对给定的 S，T 及 $t_0\in T$，我们有映射 $\mu:S\to T$，对 $x\in S$，$x\mu=t_0$.

例 1-2-4 对给定的 S 及 $T=S$，我们有映射 $I_s:S\to S$，对 $x\in S$，$xI_s=x$. 这个映射叫做 S 上的**恒等映射**. 当上下文中集 S 是清楚的时候，也简记为 I 或 ε.

例 1-2-5 设 $S=T=R$ 为实数集，令 $x\mu=\dfrac{1}{x}$，则 $\langle R,R,\mu\rangle$ 不是一个映射. 这是因为 0μ 不存在.

例 1-2-6 设 S 是有理数集，T 是整数集. 对 $x\in S$，若把 x 写成分数 $x=\dfrac{q}{p}$，令 $x\mu=q$，则 $\langle S,T,\mu\rangle$ 不是一个映射. 这是因为 $x\mu$ 不唯一. 例如，$x=1.5=\dfrac{3}{2}=\dfrac{6}{4}=\cdots$，从而 $x\mu=3$，$x\mu=6$，$\cdots$.

例 1-2-7 令 $S=R$ 是实数集，$T=N$ 是自然数集. 对 $x\in S$，令 $x\mu=|x|$ 是 x 的绝对值，则 $\langle R,N,\mu\rangle$ 不是一个映射. 这是因为对 $x=3.5\in R$，$x\mu=3.5\bar{\in} N$.

两个映射 $\langle S_1,T_1,\mu\rangle$，$\langle S_2,T_2,\eta\rangle$ 叫做相等的，是指 $S_1=S_2$，$T_1=T_2$，且对任何 $x\in S_1$，$x\mu=x\eta$.

例 1-2-8 设 $S_1=S_2=\{1,2\}$，$T_1=\{2,3,4\}$，$T_2=\{2,4\}$. 考虑映射 $\langle S_1,T_1,\mu\rangle$，其中 $1\mu=2$，$2\mu=4$；映射 $\langle S_2,T_2,\eta\rangle$，其中 $1\eta=2$，$2\eta=4$. 虽然 $S_1=S_2$，且对应法则也一样，但 $T_1\neq T_2$，从而这是两个不同的映射.

3° 映射的图形

定义 1-2-2 设有映射 $\mu:S\to T$，称

$$G(\mu)=\{(s,t)\mid t=s\mu, s\in S\}$$

为该映射的图形.

据定义立即得到$G(\mu)\subseteq S\times T$,且具有下述性质:

1) 对任何 $s\in S$,存在 $t\in T$,使$(s,t)\in G(\mu)$.

2) $(s,t_1),(s,t_2)\in G(\mu)\Rightarrow t_1=t_2$.

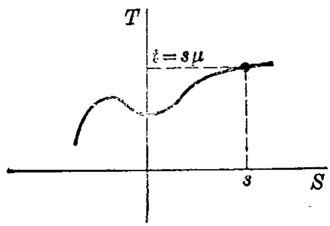

图 1-2-2

这两条性质完全刻划了 $S\times T$ 的一个子集能作为某一映射的图形的条件. 事实上,若 $G\subseteq S\times T$ 具有这两条性质,则可以定义映射 $\mu:S\to T$. 对 $s\in S$,按性质 1),存在 $t\in T$ 使 $(s,t)\in G$. 由性质 2)知这种 t 是唯一存在的. 令 $s\mu=t$,容易看到,$G=G(\mu)$.

这样,我们也可以把映射定义为有序三组$\langle S,T,G\rangle$,其中$G\subseteq S\times T$ 具有上述性质 1),2).

容易看到,两个映射$\langle S_1,T_1,\alpha\rangle$,$\langle S_2,T_2,\beta\rangle$相等的充要条件是 $S_1=S_2,T_1=T_2,G(\alpha)=G(\beta)$.

4° 几种特殊的映射

定义 1-2-3 映射 $\mu:S\to T$ 叫做**内射**或**1-1**的,是指 $s_1\neq s_2\Rightarrow s_1\mu\neq s_2\mu$.

由此,$\mu:S\to T$ 是内射的充要条件是:若 $t\in T$ 有前象,则前象是唯一的.

定义 1-2-4 映射 $\mu:S\to T$ 叫做**满射**或**到上**的,是指对任何

$t\in T$，都存在 $s\in S$，使 $t=s\mu$，即 T 中的每个元素都有前象.

定义 1-2-5 映射 $\mu:S\to T$ 叫做**双射**或 **1-1 到上的**，是指 μ 既是内射又是满射.

按定义，例 1-2-1 是内射但不是满射. 例 1-2-2 是满射但不是内射. 例 1-2-3 既不是内射也不是满射. 例 1-2-4 是双射.

一般称集 S 到其自身的映射为**变换**. 称 S 到其自身的双射为 S 上的**置换**. 特别地，当 S 是由 n 个元素组成的有限集时，S 上的置换常叫做 n **阶置换**.

例 1-2-9 考虑映射 $\mu:Z\to Z$，对 $x\in Z$，$x\mu=x+3$. 它是一个置换.

例 1-2-10 令 $S=\{1,2,3,4,5\}$，考虑映射 $\mu:S\to S$，其中 $1\mu=2$，$2\mu=3$，$3\mu=4$，$4\mu=1$，$5\mu=5$. 它是一个 5 阶置换.

一般地，$S=\{1,2,\cdots,n\}$的一个置换 μ 常用一个"表"来表示：

$$\mu=\begin{pmatrix}1 & 2 & \cdots & n\\ 1\mu & 2\mu & \cdots & n\mu\end{pmatrix}.$$

而以 S_n 表示 S 上的所有 n 阶置换的集. 这样，例 1-2-10 中的 5 阶置换 μ 可以表示为

$$\mu=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 4 & 1 & 5\end{pmatrix}.$$

5° 映射的积

定义 1-2-6 设有映射 $\alpha:S\to T$，$\beta:T\to U$，称映射 $\gamma:S\to U$，对 $s\in S$，$s\gamma=(s\alpha)\beta$，为 $\alpha:S\to T$，$\beta:T\to U$ 的积，简记为 $\gamma=\alpha\beta$.

由定义，对 $s\in S$，我们有 $s(\alpha\beta)=(s\alpha)\beta$.

应该注意，在映射的积的定义中，要求 α 的余区域就是 β 的区域.

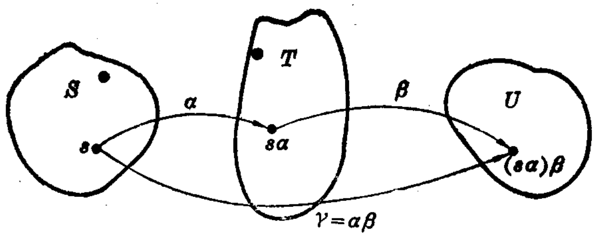

图 1-2-3

例 1-2-11 设 $S=T=U=R$ 是实数集，$x\alpha=\sin x, y\beta=y^2+1$，则 $x(\alpha\beta)=\sin^2 x+1$；$x(\beta\alpha)=\sin(x^2+1)$.

由此看到，映射的积正是通常数学分析中复合函数概念的推广.

例 1-2-12 设 $S=\{1,2,3\}, T=\{n,p,q,r\}, U=\{x,y,z\}$. 考虑映射

$$
\begin{array}{ll}
\alpha: S\to T & \beta: T\to U \\
1\alpha=p, & n\beta=x, \\
2\alpha=n, & p\beta=y, \\
3\alpha=q, & q\beta=z, \\
 & r\beta=z.
\end{array}
$$

则得积 $\alpha\beta: S\to U$

$$
\begin{aligned}
1(\alpha\beta)&=(1\alpha)\beta=p\beta=y,\\
2(\alpha\beta)&=(2\alpha)\beta=n\beta=x,\\
3(\alpha\beta)&=(3\alpha)\beta=q\beta=z.
\end{aligned}
$$

例 1-2-13 设

$$\alpha=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad \beta=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

则

$$\alpha\beta=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},\quad \beta\alpha=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}.$$

这些例子表明，对于映射的积 $\alpha\beta$，一般来说，$\beta\alpha$ 并不一定有意义，因为 S,U 可以不相同. 即使 $S=T=U$，$\alpha\beta$ 与 $\beta\alpha$ 也不一定相等. 从而关于映射的积，因子的顺序是重要的，即交换律不成立. 但有下述定理：

定理 1-2-1 设有映射 $\alpha:S\to T$，$\beta:T\to U$，$\gamma:U\to V$，则 $(\alpha\beta)\gamma=\alpha(\beta\gamma)$，即映射的积满足结合律.

证明 因为 $(\alpha\beta)\gamma$ 及 $\alpha(\beta\gamma)$ 的区域都是 S，余区域都是 V，所以只需证明对任何 $s\in S$ 有 $s[(\alpha\beta)\gamma]=s[\alpha(\beta\gamma)]$ 就可以了. 事实上

$$s[(\alpha\beta)\gamma]=[s(\alpha\beta)]\gamma=[(s\alpha)\beta]\gamma,$$

$$s[\alpha(\beta\gamma)]=(s\alpha)(\beta\gamma)=[(s\alpha)\beta]\gamma.$$

从而 $(\alpha\beta)\gamma=\alpha(\beta\gamma)$.

根据这个定理，我们可以讨论三个映射的积 $\alpha\beta\gamma=(\alpha\beta)\gamma=\alpha(\beta\gamma)$ 以及三个以上映射的积，而它们与括号的添加方式无关.

定义 1-2-7 一个由映射组成的图形叫做**交换图**，是指沿着任何一条从同一个始点到同一个终点的路径，把这些映射乘起来，得到的结果相同.

例 1-2-14 设有映射 $\alpha:S\to T$，$\beta:T\to U$，$\gamma:S\to U$. 考虑图 1-2-4，则它是交换图的充要条件是 $\gamma=\alpha\beta$.

$$\begin{tikzcd} S \arrow[r, "\alpha"] \arrow[dr, "\gamma"'] & T \arrow[d, "\beta"] \\ & U \end{tikzcd}$$

图 1-2-4

$$\begin{tikzcd} S \arrow[r, "\alpha"] \arrow[d, "\gamma"'] & T \arrow[d, "\beta"] \\ V \arrow[r, "\delta"] & U \end{tikzcd}$$

图 1-2-5

例 1-2-15 设有映射 $\alpha: S\to T$, $\beta: T\to U$, $\gamma: S\to V$, $\delta: V\to U$ 且 $\alpha\beta=\gamma\delta$，则图 1-2-5 是交换图.

例 1-2-16 图 1-2-6 是交换图是指 $\alpha\beta=\eta=\gamma\delta$.

这样，映射积的结合律可以用交换图叙述如下：
对于图 1-2-7，$\triangle STU$ 是交换图及 $\triangle TUV$ 是交换图 $\Rightarrow$ 整个图形是交换图.

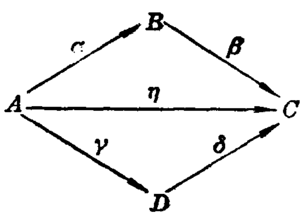

图 1-2-6

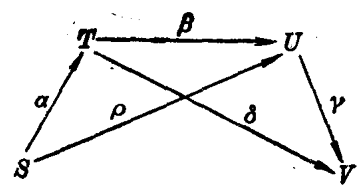

图 1-2-7

定理 1-2-2 对映射 $\alpha: S\to T$ 有

$$I_S\alpha=\alpha,\quad \alpha I_T=\alpha.$$

证明 对任何 $s\in S$，$s(I_S\alpha)=(sI_S)\alpha=s\alpha$，故 $I_S\alpha=\alpha$. 又 $s(\alpha I_T)=(s\alpha)I_T=s\alpha$，故 $\alpha I_T=\alpha$.

定理 1-2-3 $\alpha: S\to T$ 是双射 $\Longleftrightarrow$ 存在 $\beta: T\to S$，使 $\alpha\beta=I_S$，$\beta\alpha=I_T$.

证明 $\Rightarrow$ 因为 α 是双射，故对每一 $t\in T$，有唯一的 $s\in S$，使 $s\alpha=t$. 令 $t\beta=s$. 于是得到映射 $\beta: T\to S$. 我们来证明 $\alpha\beta=I_S$，$\beta\alpha=I_T$. 事实上，对任何 $s\in S$，$s(\alpha\beta)=(s\alpha)\beta$. 设 $s\alpha=t$. 由 β 的定义，$t\beta=s$，从而 $s(\alpha\beta)=(s\alpha)\beta=t\beta=s=sI_S$，故 $\alpha\beta=I_S$；又对任何 $t\in T$，$t(\beta\alpha)=(t\beta)\alpha$. 设 $t\beta=s$，即 $s\alpha=t$，从而 $t(\beta\alpha)=(t\beta)\alpha=s\alpha=t=tI_T$，故 $\beta\alpha=I_T$.

$\Leftarrow$ 首先，α 是满射. 事实上，对任何 $t\in T$，$t=tI_T=t(\beta\alpha)=(t\beta)\alpha$，从而 t 有前象 $t\beta$. 其次，α 是内射. 事实上，若 $s_1\alpha=s_2\alpha$，