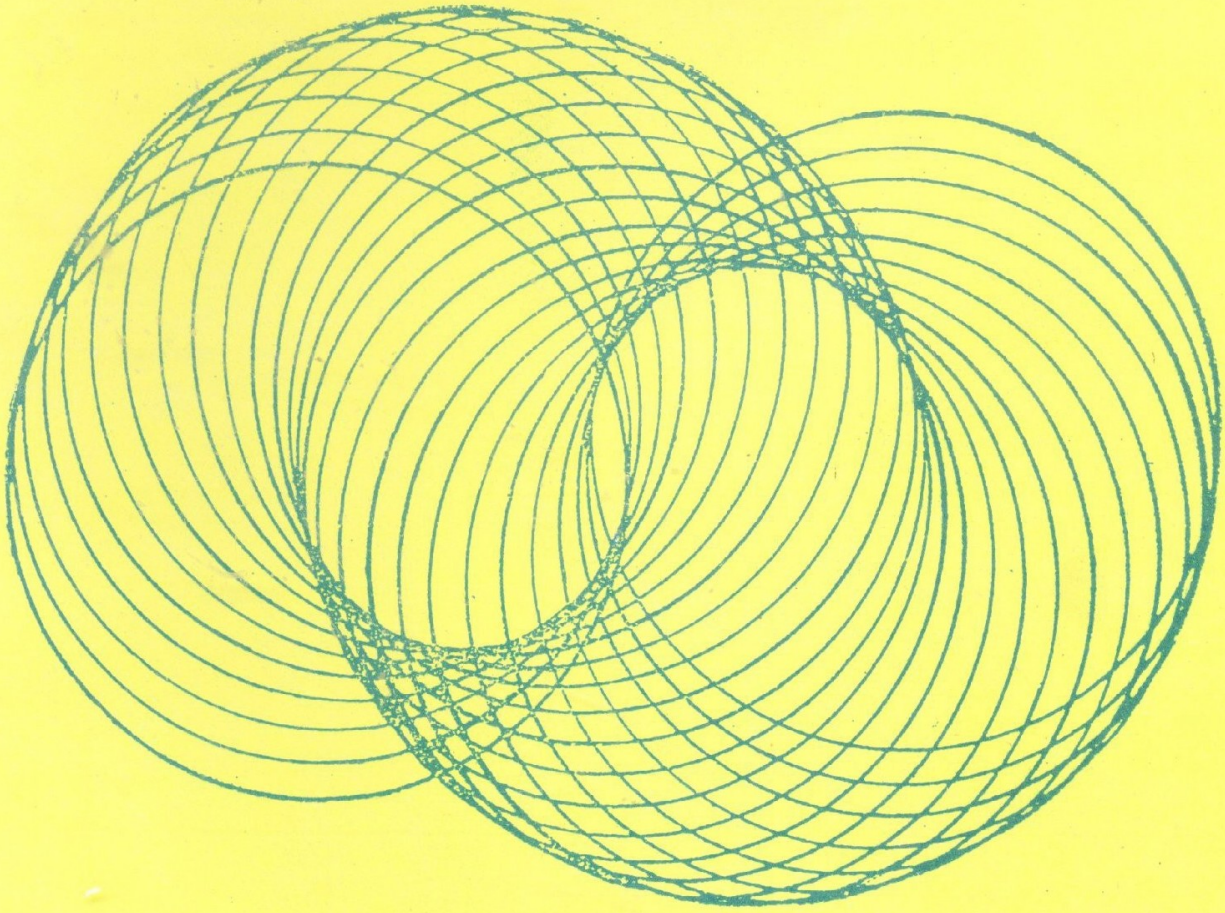
代数结构

侯广坤 编著



华南理工大学出版社

代　数　结　构

侯广坤　编著

华南理工大学出版社

内容提要

本书介绍了集合的最基本的概念，以及从这个最基本的概念出发生成的最基本的代数结构过程。全书分为四章，第一章是讨论朴素集合论的基本概念和由集合出发建立基本数学概念的过程和方法，特别介绍了从空集出发，用构造的方法建立自然数和自然数系，并阐述了用构造的方法与用公理方法建立的自然数和自然数系是一致的，同时指出了归纳法在构造性思维中的地位。第二章讨论了用集合的概念建立关系、函数、代数概念的过程。第三章和第四章介绍了半群、群、环、域、格、范畴等重要的代数结构，以及它们的同态关系和生成过程。

本书适合于从事数学、计算机科学工作的读者参考，也适于其它需要利用基于离散结构的构造性思维方法的读者参考。

［粤］新登字12号

代 数 结 构

侯广坤 编著

华南理工大学出版社出版发行

（广州 五山）

广东林业勘测设计院印刷厂印刷

开本787×1092 1/16 印张14.5 字数327千

1992年8月第1版 1992年8月第1次印刷

印数0001～1000

ISBN7－5623－0446－7/O・44

定价：7.50元

符　号　及　缩　写

$\{\mid\}$　使得...的集合

$\in$　属于

$\notin$　不属于

N　自然数集合(包括 0)

Q　有理数集合

I　整数集合

R　实数集合

C　复数集合

E_e　偶自然数的集合

O_d　奇自然数的集合

N_m　小于 m 的自然数的集合

I_+　正整数集合

I_-　负整数集合

R_+　正实数集合

R_-　负实数集合

$\varnothing$　空集

$\mathscr{A}$　集合类 $\mathscr{A}$

Σ　字符表

Λ　空字

A^*　集合 A 上的闭包

a^+　a 的后继

$\subset$　包含于

$\subseteqq$　包含于或等于

$\supset$　包含

$\supseteqq$　包含或等于

$\cup$　并

$\cap$　交

$-$　差

$\times$　笛卡尔乘

$\sim$　等价

$C_x(A)$　A 关于 X 的补(有时用 $\rightharpoonup A$ 表示

$\aleph_0$　等价于自然集的集合的基数

c　等价于实数集的集合的基数

$\aleph_1$　基数大于 $\aleph_0$ 最小基数

ω　自然数集的序数

$^{*}\omega$　负整数集的序数

$\equiv_m$　按模为 m 的等价

$+_m$　按模为 m 的加

$*_m$　按模为 m 的乘

$\approx$　同构

&　并且

$\vee$　或者

$\sum$　连加

$\prod$　连乘

$\neg$　否定，补

$f:X\to Y$　从集合 X 到集合 Y 的函数 f

dom$R$　R 在横坐标轴的投影

ron$R$　R 在纵坐标轴上的投影

$f(A)$　集合 A 在 f 下的象

$f^{-1}(B)$　集合 B 在 f 下的逆象

$f\cdot g$　f 与 g 的合成

$f|_A$　f 在 A 上的限制

aRb　aR—— 相关于 b

X/R　X 的等价类(X 关于 R 的商集)

X/A　X 关于 A 的商群

$A\oplus B$　A 与 B 的直和

$A\otimes B$　A 与 B 的张量积

$A\otimes_R B$　A 与 B 在 R 上的张量积

Im　像

Ker　核

Coim　余像

Coker　余核

deg　次数

dim　维数

Hom　同态群

$R[t]$　关于 t 的多项式

$E_\cdot(M)$　M 关于 R 的外代数

$S_\cdot(M)$　M 关于 R 的对称代数

$T_\cdot(M)$　M 关于 R 的张量代数

绪 论

计算机科学的许多研究方向都与代数，特别是抽象代数有着密切的关系，人们普遍地认为，抽象代数是计算机科学的理论基础之一。至少有如下三个理由来说明：(1)抽象代数研究的客体(对象)与计算机科学研究的客体都是一般的通用客体；(2)代数结构为计算机系统(包括理论系统、计算机系统组成的结构、工具与环境系统的结构、应用系统的结构、系统的结构分类和它们之间的关系等)提供必要的理论模型；(3)不论是计算机科学的基础学科、技术学科和应用学科，还是计算机科学的边缘学科，抽象代数都给它们提供了最基本的思维方法。

在绪论中我们讨论三个问题。

(一) 在这里所讲的代数系统，同以前所讨论的代数有相同的地方，也有不同的地方。在以前的代数学中研究的对象都是数(实数和复数)或用字母表示的数以及这些数的四则运算。

在研究的对象中有时出现代数式，数或代表数的字母按一定的法则连结起来构成的代数式，但代数式是数的另一种表示形式。在这里所讨论的对象除了数以外，还有其它的对象，这样可以说研究的对象是某集合元素的总体，甚至有时并不指出这个集合是什么，也不指出集合中的元素是什么。我们所研究的运算，也不仅仅是加、减、乘、除四则运算，而是满足一定抽象条件的运算，有时也可能不指出具体的运算是什么运算。以前所讨论的代数是代数系统的一个特例。

在 1900 年前后，被研究过的各种代数课题，不管是矩阵，二元，三元或 n 一 元二次型的代数，超数系，同余式，还是多项式方程的解的理论，都是建立在实数系和复数系之上的。但是数学家们发现，几乎对于任何代数课题和出现的问题，都可以用任何一种抽象结构去代替实数系和复数系，从而代数的抽象结构引起了人们的极大兴趣。

抽象代数的基本概念和目标在十九世纪就已经定下来了。十九世纪许多发明创造表明，代数能处理不一定是实数或复数的对象所组成的集合。向量、四元数、矩阵、二次型、各种形式的超复数、变换、替换或置换等等，都是这种对象的例子，这些对象在其各自集合所特有的运算和运算规律下联系起来。

本来为了数学发展而对代数研究的对象进行抽象，却给计算理论和计算机科学有很大的促进。无疑地，古典的计算概念往往地理解为计数或数值计算。上世纪末到本世纪初，人们在抽象代数和符号逻辑发展的影响下，一方面，去寻求更具有普遍意义的计算对象和作用于这些对象上的更具有普遍意义的法则(操作)，并在这个基础上建立起更具有普遍意义的最可靠的计算概念；另一方面，在解决了第一个问题的基础上建立更具有普遍意义的、实用的计算机和计算机系统。这种“具有普遍意义”后来被称为“通用性”。因此，计算机科学中的“通用性”和“可实现性”是与抽象代数研究的对象和法则的“通用性”和“可实现性”要求是一致的。

(二) 在抽象代数中，由于所讨论的对象以及在其中的运算是一般的，所以，在讨论的方法上有不同的地方。中学里的代数是用如下方法讨论的：首先，定义具体的对象，自然数、整数、有

理数、实数和复数，代数式等，这些对象都以最直观和最具体的方式，以它们所特有的个性加以定义。然后在这个具体对象上的定义具体的运算和具体地指出这些运算所满足的条件，而且最初并不讨论这些运算所具有的一般的性质(主要是逻辑思维的一般性质)。

例如，我们先给出包括零的所有自然数的整体，用 N 来表示，N 和零都是一个非常具体和直观的概念。在 N 上提出一个运算 +。不论是自然数也好，运算 + 也好，都有着十分具体的意义。而且对于集合 N 中的元素之间的关系 $>$、$<$、$=$ 等有十分明确的意义。因此我们就可以讨论在集合 N 上的运算 + 的性质：

(1) 运算 +，× 对于 N 的封闭性。假若 a 和 b 属于 N，则 a 和 b 使用运算 +，× 的结果称为它们的和与积也属于 N。

(2) 加法交换律。$a+b=b+a$。

(3) 加法结合律。$(a+b)+c=a+(b+c)$。

(4) 在 N 中存在着一元素 0，使得对于集合 N 中的任一元素 a 都有

$$a+0=0+a=a。$$

(5) 在 N 中存在一个元素 1，使得对于在 N 中任意两个不同的元素 x 和 y，其中的一个元素(譬如 x) 有限次地加上 1 后，等于另外一个。

还可以列举出其它的性质，例如分配律、乘法结合律和乘法交换律等。

这是一个初等算术系统，是初等算术系统的抽象结构。在这个系统中，可以从自然数的概念和运算 + 的性质产生新的概念。例如，偶数定义为可以分解为两个相同的元素(自然数) 的和的元素(自然数)，否则为奇数。偶数集合和奇数集合是自然数集合的子集合。如果我们将偶数集合和运算 + 再构成一个子系统并同原来的系统对应，则我们发现子系统同原来的初等算术系统有完全相同的性质，后面我们称为同构。

如果在初等算术系统中除讨论 + 外，同时考虑运算 ×，则得到更为丰富的系统。用 $\langle A; f_1, f_2, \ldots, f_n\rangle$ 表示一个代数系统，其中 $f_1, f_2, \ldots, f_n$ 是运算。不同的集合和不同的运算构成无穷的系统。可以用一些方法对它们进行分类。

从上面看出，要讨论代数系统，先定义一些概念，并以此来确定构成系统的对象集合，指出对象的性质和对象与对象之间的关系，然后确定由现有对象出发构成新的对象的运算。研究运算的性质和系统的结构；研究子系统以及它们之间的关系；研究系统从内容上和范围上的扩充以及产生新的系统的方法；研究系统间的关系和分类；等等。上面已经讲过，在讨论代数系统时，所讨论的对象是一般的对象集合，也就是说，给出的并不是一个集合，而是一般地满足一定抽象条件的集合。另外，运算也是满足一定抽象条件运算。所以，在定义一个代数系统时，并不是一个具体的代数系统，而是满足一定抽象条件的一类代数系统的总体。因此研究的是代数系统的总体结构，提出一个同属于某一大类的所有代数结构的理论模型。而且如果对其中的对象和运算进行不同的解释时，只要在这个解释下可满足这种抽象的结构，则形成一个具体的代数系统。

计算机是一个通用的计算模型，它的通用性在于：任何一个可计算的问题，如果问题本身是有结果的(例如，最后总是能回答“是”或“非”的)，只要不考虑时间和空间的可能性，原则上都可以在计算机上得到结果。计算机的结构也是一个通用的结构。只要根据某具体需求解的问题，而对计算机系统的对象(数据模型) 和运算(所做的操作) 进行解释，则计算机系统就成为解决这个问题的具体理论模型。

（三）根据上面两点，不难决定代数结构的思维方法。根据计算机科学构造性和通用性的需要，在讨论基本思维方法时应非常注重构造的方法和公理的方法，这不仅是数学的基本思维方法，而且也是计算机科学的基本思维方法。所谓构造的方法是提供一个由原生概念开始来构造整个理论系统的方法。构造方法的第一步是确定所研究的对象，首先非常直观地陈述一些不经定义的原始概念，例如，欧基里得几何的点、直线、平面，在本课程里的集合的概念等等。然后指出由已知概念产生新的概念的过程和规则及方法。例如，在本课程中怎样由集合的概念产生元素、空集、有限集、直观的无穷集等，继而属于、包含等概念。第二步是定义作用于对象的操作，这样，操作的结果又是新的对象。例如，并集、交集、幂集、函数、自然数、整数、有理数、实数、笛卡尔乘积、关系、部分函数、运算、代数等。第三步对所定义的操作进行认真的分析，研究这些操作作用于这些对象上所表现出来的性质。第四步是讨论分类问题以及系统与系统之间的关系问题，例如，在课程中关系是集合，为笛卡尔乘积的子集，而提出一些条件（根据这个关系所包含的有序对）来定义等价关系、序关系、相容关系等等的特殊关系；部分函数是一个特殊的关系，根据这个关系的有序对的第一个元素与第二个元素的对应关系分类为内射、满射、双射等。第五步是讨论层次较高的理论问题和哲学问题，例如，存在性、唯一性问题；协调性、完全性问题等，这个问题较深，不是本课程的重点。

在研究构造的方法时，有两点是十分关键的思维范畴的问题：第一. 系统中任何一个对象都可以由原始对象通过有限次地使用系统中的操作而得到，因此这里的存在性问题成为可构造性问题，唯一性问题是极小化问题；第二. 思维范畴应该是在有限的范畴中的，但当必须牵涉无穷时也只是潜在的无穷性，能够通过第一归纳法和第二归纳法将思维的范畴从有限延伸到潜在无穷。

从课程的第三章开始使用了公理的方法。所谓公理的方法不像构造的方法那样去定义具体的对象和去定义具体的操作，而是只用抽象的符号表示对象和操作，提出一系列的断言，那么所研究的系统只是满足这些断言的系统。例如，在第四章研究群时，首先给出集合和运算，这集合和运算并非具体给出，那么群是满足四个断言（封闭性、结合律、存在单位元、存在逆元）的所有集合和运算。当然，公理方法必须有构造方法的思维基础和古典数学的思维基础的。

在计算机科学中，语言代数的建立是利用构造方法和公理方法的。现代许多有关计算机系统的生成方面的问题，也非常注重生成的方法，往往以构造的方法和公理的方法作为基础。

我们用公理方法来研究一些理论问题时，要讨论一个问题，即是系统的协调性问题。即在给出的抽象条件之间是否是矛盾的。例如所讨论的代数系统，对于用来确定对象和在这对象系统上的运算的抽象条件之间是否有矛盾。这是数学基础研究的问题，在这里不讨论这个问题。但在构造代数系统时有必要注意它的逻辑结构。

如何学好代数结构呢？首先，要充分了解对象及系统的结构，对象系统中的所有对象的构造过程。构造的方法是抽象代数的基础。

其次，在充分了解对象系统中的对象后，非常重要的一点是用什么方法来确立一个抽象系统。往往会提出一系列的公理，这些公理应该是平常已十分了解的一些逻辑规律和数学规则。我们所讨论的抽象系统是同时满足这些公理的那些对象所组成的系统。

这两步是学好抽象代数的关键。为了掌握这部分知识，一定要找到这些抽象系统的解释。包括如下三方面的内容：第一，找到一个（一些）具体的原始对象和具体的从原始对象和已定义的对象而产生新的对象的方法，我们还要说明这些对象的数学意义或物理意义，也要阐明这

些方法的数学意义；第二，这些对象以及从这些对象产生新的对象的过程必须满足所列出的公理。所谓满足这些公理应有明确的逻辑意义；第三，同一个定义有着不同的解释，我们要明白，不同的解释所产生的不同的系统，在逻辑上都是遵循着同一个定义的。

再其次，从所定义的系统出发，产生新的系统的构造方法。如子系统、以系统作为对象进行运算产生新系统、陪系统、商系统等等。

第四，要讨论系统与系统之间的关系和系统的分类。它们是同构、同态、同余？用那一种关系来对它们分类？

这是掌握抽象代数的一般方法，读者在学习的过程中会更有体会。

书中的内容比较丰富，在目录中带有星号 * 的内容是作为研究生和对抽象代数有进一步兴趣的读者阅读用的。

目　　录

第一章　集合论基础

我们首先讨论集合论基础是基于如下两个原因：

一是集合是现代数学的基础之一，几乎所有数学理论和计算机科学的理论都可以在集合论中找到解释。当然也是抽象代数的基础之一。在十九世纪中叶以前，数学其中包括代数，都建立在几何的基础上。人们发现建立在几何上的分析是不可靠的，当然建立在几何上的代数也并非可靠。人们力求将分析建立在算术的基础上，作为这个副产品，代数也应建立在算术的基础上。在这个过程中，人们不仅弄清了实数系的逻辑结构，同时产生了朴素集合论。朴素集合论的最基本原则是将集合作为一个数学对象来讨论，从集合论出发建立其它的数学理论。因此讨论集合论基础为后面几章讨论最基本的代数结构提供基本思维方法。

二是已在绪论中讲过，讨论代数结构是从最基本的概念开始，代数结构中的一切概念都是从集合出发通过构造的方法和公理的方法而得到。通过对这个过程的讨论分析计算机科学的基本思维方法之一 —— 基于离散结构的构造性思维方法。

因此，在这一章要解决如下的两个问题：一是确立将集合作为一个独立的数学对象来讨论的思想和讨论从集合出发构造新的集合的方法，命题法和元数学法具有普遍的意义；二是如何从集合论出发构造其它的数学理论，又古典的数学理论作为现代数学和计算机科学的基础，而且它是以自然数为出发点的，所以着重讨论自然数和自然数集的构造，而且指出第一归纳法和第二归纳法在基于离散结构的构造性思维方法中的意义，然后略论其它数和数系的构造。

§1.1　一般集合概念

首先考虑集合的一般概念。众所诸知，要建立一个数学理论，总是利用已知的概念定义新的概念。但任何一种数学理论中，不可能对其中的每一个概念都有严格的定义。比如说，数学的第一个概念就无法定义，因为已没有能用于定义这个概念的更原始的概念了。我们称这种不能严格地定义的概念为该数学理论的原始概念，而称由此原始概念生成的其它概念为派生概念。把“集合”也看作不能严格定义的原始概念。最为原始的东西最具有同一性，最简单的、最少约束的概念为最广泛的概念。除此之外，在确立集合这个原始概念时，只用了一个最基本的逻辑原则 —— 排中律，排中律同样具有原始的意义。正因为如此，集合才能作为代数结构和其它数学对象中的最简单、最基本、最原始、而又最广泛的概念。

1.1.1 集合及其表示

因为集合是不能严格定义地原始概念，所以它只能对它作直观的描述。这种直观的描述在逻辑上是必须基于排中律的。通俗地讲，排中律是“非此即彼”、“二者必居其一”、“三者必居其一”等意义。所谓集合，乃是由某些可以互相区分的任何客观存在的对象，如数、变量、函数、符号、字母、数字、图、语言、程序或事件等或者没有任何对象，汇集在一起所组成一个整体。首先排中律体现在“有”和“无”问题上。在汇集若干个对象的情况下的可区分性有两方面的意义，排中律就体现在两处：(1) 这个整体中的任何两个对象，都有一个方法在有限步内区分其相同或不同；(2) 任何对象(若干个对象) 都有一个方法在有限步内判定它(它们) 是否具有或者不具有某个性质(或关系)。这里所涉及的各个对象，统称为元素。组成一个集合的各个对象，称为这个集合的元素或成员。

在这里陈述的有关集合的概念中会发现，首先直观地陈述某些可区分的对象，这些对象(或客体 —— 客观存在的实体)，这些对象称为集合的元素，因此元素的概念直接由集合的概念产生，在这里同样具有直观和原始的意义。在陈述集合和其中所包含的元素的概念时，对于组成集合的成员是什么并不需要指出，以什么样的方式汇集在一块也不必阐述。即是说不论是什么，只要满足可区分性，不管是什么方式将它们汇集在一起，都是集合。这种陈述的集合的概念具有最大的广泛性。

下面一些不同的客体以各种不同的方式汇集在一起所构成的集合：

例 1.1.1　以下是一些集合的例子：

① 中国人的集合；

② 中国的山和河的集合；

③1000 以内的素数的集合；

④ 方程 $x^2 + x + 1 = 0$ 的实根的集合；

⑤ 自然数(在这指的是非负整数) 的集合；

⑥ 直线 $y = 2x - 5$ 上的点的集合。

例 1.1.2　在以下集合的元素中，有的就是集合：

① 例 1.1.1 中列举的集合的集合；

② 由字母 a,b 和自然数的集合一起所组成的集合。

对例 1.1.2 的 ①，集合的每一个元素都是集合；对于例 1.1.2 的 ②，集合的一些元素是集合，另一些元素可能不是集合。

通常，用大写拉丁字母 $A,B,C,\cdots\cdots$ 表示集合，用小写的拉丁字母 $a,b,c,\cdots\cdots$ 表示元素。用如下的字母表示固定的集合：

N—— 自然数的集合；

Q—— 有理数的集合；

I—— 整数的集合；

R—— 实数的集合；

C—— 复数的集合；

E_e—— 偶自然数集合；

O_d—— 奇自然数集合；

N_m—— 小于 m 的自然数集合；

I_+ —— 正整数的集合；

I_- —— 负整数的集合；

R_+ —— 正实数的集合；

R_- —— 负实数的集合。

从集合和元素的概念出发来定义“属于”概念。在集合概念中使用排中律还表现为如下的意义：设 a 为任一个对象，A 为任意一个集合，则在 a 和 A 之间有且仅有以下两种情况中的一个出现：

(1) a 为 A 的元素，记作“$a \in A$”，并称为“a 属于 A” 或“A 含有 a”；

(2) a 不为 A 的元素，记作“$a \notin A$”，并称“a 不属于 A”。

二者必居其一。

元素对于某集合的从属性是继陈述集合及属于它的元素的概念之后所陈述的另一个基本概念，陈述时也只用到排中律。

当 $a_1 \in A, a_2 \in A, \ldots, a_n \in A$ 时，常简写为 $a_1, a_2, \ldots, a_n \in A$。

有了集合、元素和从属性概念，可以建立关于集合的其它概念。

定义 1.1.1　设 A 为任一集合，用 $n(A)$ 表示 A 含有元素的个数。

① 若 $n(A) = 0$，则称 A 为空集；

② 若 $n(A)$ 为某自然数，则称 A 为有限集；

③ 若 $n(A)$ 为无穷大，则称 A 为无穷集；

④ 若 $n(A) \neq 0$，则称 A 为非空。

这个定义的基于集合概念的两点：① 对于集合的元素的计数时集于可区分性上；② 在 $n(A)$ 为无穷大时，必须有对集合 A 中的可区分性元素数是无穷大能得到证明。空集是不包含任何元素的有限集有限集，常用符号 $\varnothing$ 来表示。

在例 1.1.1 中所列举的集合中，①、② 和 ③ 都是非空有限集(即为有限集，且不为空集的集合)，④ 为空集，而 ⑤ 和 ⑥ 都是无穷集。

在上面所给出的常用集合中，只有 N_m 为有限集，其余的都是无穷集。

定义 1.1.2　设 A, B 为任意两个集合。

(1) A 为空集，或 A 非空，且对于每个 $a \in A$ 皆有 $a \in B$，那么称 A 为 B 的子集或 B 包含 A，也称 B 为 A 的母集，记作 $A \subseteq B$ 或 $B \supseteq A$。

(2) 若 $A \subseteq B$ 且 $B \subseteq A$，则称 A 和 B 相等，记作 $A = B$；否则，称 A 和 B 不相等，并记作 $A \neq B$。(这里作为定义，其实在许多有关集合论的论著中，这一点是要证明的)。

(3) 若 $A \subset B$ 且 $A \neq B$，则称 A 为 B 的真子集或 B 真包含 A，记作 $A \subset B$ 或 $B \supset A$。

由此可见，两个集合相等，仅指它们所含有的元素完全相同。所以，要想确定一个集合，只需确定：哪些元素属于这个集合，哪些元素不属于这个集合。至于这些元素用什么方法描述或指定，并无关紧要。

在这里便可以严格定义空集：存在着一个集合，它能作为任意集合的子集，这个集合称为空集。

定义了集合，定义了集合的元素、空集、子集，还定义集合与它所包含的元素，集合与集合之间的一般联系。从这里看来初步确定集合（包括无穷集，但比较严格的是有限集）是一个独立的数学对象存在，那么存在的方法是怎样的呢？即用什么方式表示集合？可以用种种不同的方法描述一个集合。常用的方法有以下四种：

(1) 列举法

依照任意一种次序，不重复地列举出集合的全都元素，并用一对花括号括起来。例如 10 以内的素数的集合 $=\{2,3,5,7\}$。列举法只适用于元素不太多的有限集。

(2) 部分列举法

依照任一种次序，不重复地列举出集合的一部分元素。但是，这部分元素要能充分体现该集合在上述次序下的构造规律，从而能够很容易地获得集合中的任何一个未列举的元素。未列举出的元素用"..."代替。然后，用一对花括号把已列举出的元素和"..."一起括起来。例如

$$N=\{0,1,2,\ldots\}$$

$$E_+=\{0,2,4,\ldots\}$$

$$O_+=\{1,3,5,\ldots\}$$

部分列举法仅适用于元素的构造规律比较明显的简单的集合。它们可以是无穷的集合，但所表示的这些无穷集合的每一个元素都可以用简单的方式构造，简单到无需写出规律人们都能清楚。也可以是所含有的元素个数较多的有限集。

(3) 命题法

用这种方法定义一个集合 A 时，要给出一个与 x 有关的命题 $P(x)$，使得 $x\in A$ 当且仅当 $P(x)$ 为真，并称 A 为使 $P(x)$ 为真的 x 的集合，记为

$$A=\{x\mid P(x)\}\qquad 或\qquad A=\{x;P(x)\}$$

通俗的讲，这种集合的定义方法是一个性质决定一个集合，这个性质一般用谓词来表示。例如

$$N_m=\{n\mid n\in N\text{ 且 }0\leqslant n<m\}$$

$$\{1,2\}=\{x\mid x\in R\text{ 且 }x^2+3x+2=0\}$$

用这个方法来表示一个集合实际上是定义了一个具体的集合，用来定义集合的命题（准确地讲是谓词）可能不止一个而是多个，而且在这些谓词之间有一定的关系，例如这些谓词同时成立来确定一个集合；也可能这些谓词中只有其中的一个成立来确定一个集等等。在后面会看到，代数结构中的任何一个对象都可以看成一个或一组集合，因此命题法就成为本课程用来建立概念的最基本方法之一，公理方法也是在命题法上发展起来的。希望同学们特别注意。

(4) 归纳定义法或元数学定义法

用这种方法定义一个非空集合 A 时，一般包括以下三步：

① 基本项

已知某些元素（常用 S_0 表示由这些元素组成的非空集合）属于 A，即 $S_0\subseteq A$。这是构造 A 的基础，并保证 A 非空。

② 归纳项

给出一组规则，从 A 中元素出发，依据这些规则所获得的元素，仍然都是 A 中的元素。这是构造 A 的关键步骤。

③ 极小化

如果集合 $S \subseteq A$ 也满足 ① 和 ②，则 $S = A$。这说明，A 中每一个元素都可以通过有限次地使用 ① 和 ② 来获得，它保证所构造出的集合 A 是唯一的。

归纳定义法中有如下几点是值得注意的：(1) 这个方法是从有限出发用无穷次重复的构造可得到无穷的对象，这样只需将出发的基（基本项）给出和可重复的构造方法给出（归纳项），而且这些方法（规律）只是有限个；(2) 只要给出的基本项和归纳项是相同的，那么所得到的无穷对象也是相同的，这就是极小化；(3) 将我们的思维论域从有限过渡到无穷。

用归纳定义法定义自然数集合 N，乃是数学归纳法的理论基础，在后面还要详细论述。由于步骤 ③ 在每次使用时都一样，毫无变化，所以常常省略不写，这并不是说没有这一步。

命题法和归纳法表示集合是建立代数结构以及其它数学理论的基础，也是建立计算机科学理论的基础。在数学中有两个最基本的问题：存在性问题和唯一性问题，命题法和归纳法都表现出解决这学基本问题的基本思维方法。在命题法中的存在性问题表现为存在满足一个或一组命题（谓词）的域（集合），命题法中的唯一性问题表现为用同一个或同一组命题（谓词）所确定的域（集合）满足一定的不变性（相同、相似、同构、同态等）。在归纳法中的存在性表现为存在某集合，使得它有一个子集是 S，而且集合中的元素或属于 S，或从 S 中的元素出发通过有限次地使用规则而得到。在归纳法中的唯一性问题表现在极小化。在计算机科学中也有相对应的两个最基本的问题：可构造性和构造的唯一性或有限（有效）问题。同样在命题法和归纳法中也充分地表现出决这些基本问题的思维方法。

基于命题法和归纳法的思维是代数结构的基本思维，是本课程的核心，在整个课程中贯穿着这种思维方法，希望读者注意。

还是回到集合论的最基本概念的构造上来。

例 1.1.3　设 $k \in I_+$，若用 A_k 表示能够被 k 整除的自然数的集合，则 Ak 可以用归纳法定义如下：

① $0 \in A_k$；

② 若 $n \in A_k$，则 $(n + k) \in A_k$。

例 1.1.4　设 Σ 为任意一个字符表，即由一个由符号组成的非空有限集。我们称由 Σ 中的有限多个字符并置在一起所组成的字符串为 Σ 上的字，不含任何符号的空符号串称为空字，用 Λ 来表示。若用 Σ^* 表示 Σ 上的字的集合，则 Σ^* 可以用归纳定义法定义如下：

① $\Lambda \in \Sigma^*$；

② 若 $\alpha \in \Sigma^*$ 且 $a \in \Sigma$，则 $a\alpha \in \Sigma^*$。

若用 Σ^+ 表示 Σ 上所有非空的字的集合，则 Σ^+ 可以用归纳定义法定义如下：

① $\Sigma \subset \Sigma^+$；

② 若 $\alpha, \beta \in \Sigma^+$，则 $\alpha\beta \in \Sigma^+$。

不难看出，$\Sigma^* = \Sigma^+ \cup \{\Lambda\}$。

定理 1.1.1　设 A，B 和 C 为任意三个集合，则有

(1) $\varnothing \subseteq A$；

(2) $A \subseteq A$；

(3) 若 $A \subseteq B$ 且 $B \subseteq C$，则 $A \subseteq C$；

(4) 若 $A \supseteq B$ 且 $B \supseteq C$，则 $A \supseteq C$。

证明　只证 ①，其余留作练习。