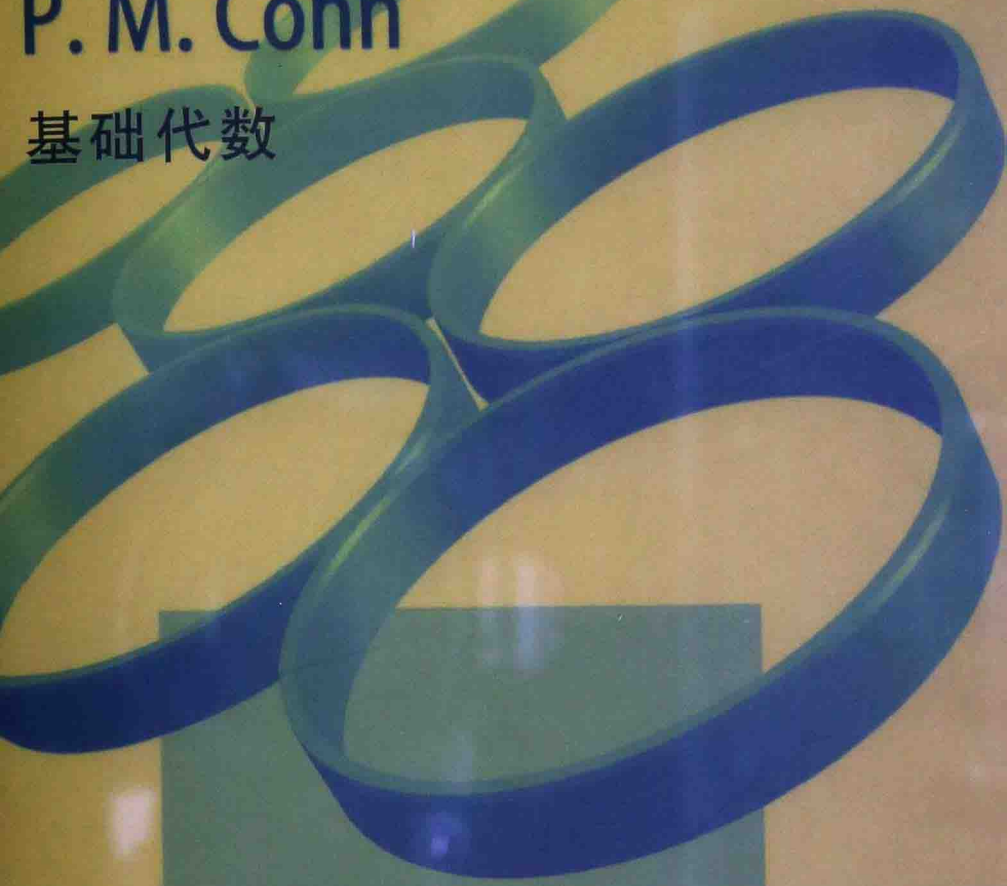
Basic Algebra

Groups, Rings and Fields

P. M. Cohn

基础代数



Springer

世界图书出版公司
www.wpcbj.com.cn

P.M. Cohn

Basic Algebra

Groups, Rings and Fields

Springer

图书在版编目（CIP）数据

基础代数 = Basic algebra：groups，rings and fields：英文/（英）卡恩（Cohn，P. M.）著. —影印本. —北京：世界图书出版公司北京公司，2015.3
ISBN 978-7-5100-9464-4

Ⅰ. ①基… Ⅱ. ①卡… Ⅲ. ①代数—英文 Ⅳ. ①015

中国版本图书馆 CIP 数据核字（2015）第 053765 号

书　　名：	Basic Algebra：Groups，Rings and Fields
作　　者：	P. M. Cohn
中 译 名：	基础代数
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河市国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街 137 号 100010）
联系电话：	010-64021602，010-64015659
电子信箱：	kjb@ wpcbj. com. cn
开　　本：	24 开
印　　张：	20
版　　次：	2015 年 5 月
版权登记：	图字：01-2014-7403
书　　号：	978-7-5100-9464-4　　定　　价：78.00 元

P.M. Cohn, MA, PhD, FRS
Department of Mathematics, University College London,
Gower Street, London WC1E 6BT, UK

British Library Cataloguing in Publication Data
Cohn, P. M. (Paul Moritz)
Basic algebra: groups, rings and fields
I. Algebra 2. Rings (Algebra) 3. Algebraic fields
I. Title
512
ISBN 978-1-4471-1060-6

Library of Congress Cataloging-in-Publication Data
Cohn, P.M. (Paul Moritz)
Basic algebra: groups, rings, and fields/P.M. Cohn.
p. cm.
Includes bibliographical references and indexes.
ISBN 978-1-4471-1060-6 ISBN 978-0-85729-428-9 (eBook)
DOI 10.1007/978-0-85729-428-9
1. Algebra. I. Title.

QA154.3.C64 2002
512–dc21 2002070686

springeronline.com

Originally published by Springer-Verlag London Berlin Heidelberg in 2003
Softcover reprint of the hardcover 1st edition 2003

2nd printing 2005

Reprint from English language edition:
Basic Algebra: Groups, Rings and Fields
by P. M. Cohn

Orginally published by Springer-Verlag London Berlin Heidelberg in 2003
Springer London is a part of Springer Science+Business Media

This reprint has been authorized by Springer Science & Business Media for distribution in China Mainland only and not for export therefrom.

Preface

Much of the second and third year undergraduate course in mathematics (as well as some graduate work) was covered by Volumes 2 and 3 of my book on algebra, now out of print.[1] So I was very pleased when Springer Verlag offered to bring out a new version of these volumes. The present book is based on both these volumes, complemented by the definitions and basic facts on groups and rings. Thus the volume is addressed to students who have some knowledge of linear algebra and who have met groups and fields, though all the essential facts are recalled here. My overall aim has been to present as many of the important results in algebra as would conveniently fit into one volume. It is my hope to collect the remaining parts of Volumes 2 and 3 into a second book, more oriented towards applications.[2]

Apart from chapters on groups (Chapter 2), rings and modules (Chapters 4, 5 and 6) and fields (Chapters 7 and 11), a number of concepts are treated that are less central but nevertheless have many uses. Chapter 1, on set theory, deals with countable and well-ordered sets, as well as Zorn's lemma and a brief section on graphs. Chapter 3 introduces lattices and categories, both concepts that form an important part of the language of modern algebra. The general theory of quadratic forms has many links with ordered fields, which are developed in Chapter 8. Chapters 9 and 10 are devoted to valuation theory and commutative rings, a subject that has gained in importance through its use in algebraic geometry.

On a first encounter some readers may find the style of this book somewhat concise, but they should bear in mind that mathematical texts are best read with paper and pencil, to work out the full consequences of what is being said and to check examples. The matter has been well put by Einstein, who said: "Everything should be explained as far as possible but no further." There are numerous exercises throughout, with occasional hints (but no solutions), and some historical remarks.

My thanks are due to the staff of Springer Verlag for the efficient way they have produced this volume.

University College London P.M. Cohn
June 2002

1 *Algebra*, Vol. 2 (2nd edn, 1989) and Vol. 3 (2nd edn, 1991), Wiley and Sons.

2 *Further Algebra and Applications*, Springer Verlag, London (2003). Referred to in the text as FA.

Conventions on Terminology

We assume that our readers are acquainted with the notion of a set (and even with groups and rings, though their definitions will be recalled in Chapters 2, 4). They will have seen notations such as $x \in S$ (x is a member of S), $S' \subseteq S$ or $S \supseteq S'$ (S' is a subset of S) and $T \subset S$ or $S \supset T$ (T is a proper subset of S) and $\varnothing$ for the empty set. For any propositions P, Q we write '$P \Rightarrow Q$' or '$Q \Leftarrow P$' to indicate that P implies Q, and '$P \Leftrightarrow Q$' to mean '$P \Rightarrow Q$ and $Q \Rightarrow P$', i.e. that P is equivalent to Q.

A property (of members of a set S) is said to hold for *almost all* members of S if it holds for all but a finite number of members of S. If T is a subset of S, its complement in S will be denoted by $S \backslash T$. This notation is also used occasionally for the left coset space (see Section 2.1); the risk of confusion is small.

We can list the elements of a set S by indexing them, e.g. if S is finite, with n elements, we can write $S = \{x_1, x_2, \ldots, x_n\}$; we also write $|S| = n$. More generally, any set can be indexed by a suitable indexing set: $S = \{x_\lambda\}_{\lambda \in I}$, where I is the indexing set. A set in this form is often called a family indexed by I; it is in effect prescribing a mapping from I to S. This mapping is generally not assumed to be injective, thus x_λ may equal x_μ even if $\lambda \neq \mu$.

All mappings between sets are as a rule written on the right, so that fg means: first f, then g. If $f : S \to T$, i.e. f is a mapping from S to T and S' is a subset of S, then the restriction of f to S' is denoted by $f|S'$. A mapping $f : S \to T$ is called *injective* or *one–one* if different members of S have different images, *surjective* or *onto* if every member of T is an image of some member of S, and *bijective* if it is both injective and surjective. Mappings are often arranged as diagrams (see Section 4.2); a diagram is *commutative* if the different ways of going from one point to another along the arrows give the same result.

Frequently a two-index expression $f(i, j)$ is equal to 1 if $i = j$ and 0 otherwise. This is indicated by using the *Kronecker symbol* δ_{ij}; thus $f(i, j) = \delta_{ij}$.

A set S is *partially ordered*, often just called *ordered*, if there is a binary relation $\leq$, called a *partial ordering*, defined on S with the properties:

O.1 $x \leq x$ for all $x \in S$ (reflexive),
O.2 $x \leq y, y \leq z \Rightarrow x \leq z$ for all $x, y, z \in S$ (transitive),
O.3 $x \leq y, y \leq x \Rightarrow x = y$ for all $x, y \in S$ (antisymmetric).

If only **O.1** and **O.2** hold, we speak of a *preordering*.

The ordering is *total* if any two elements are comparable, i.e. $x \leq y$ or $y \leq x$ for any $x, y \in S$. If '$\leq$' is a partial ordering on a set S, we shall write '$x < y$' (x is *strictly*

less than y) to mean '$x \leq y$ and $x \neq y$', and we write $x \geq y$, $x > y$ for $y \leq x$, $y < x$ respectively. As is easily verified, the opposite ordering '$\geq$' again satisfies **O.1–O.3** and so is again a partial ordering. Thus any general statement about ordered sets has a dual, which is obtained by interpreting the original statement for the oppositely ordered set. This principle can often be used to shorten proofs.

A binary relation $\sim$ on a set S is called an *equivalence relation* if it is reflexive, transitive and *symmetric*, i.e. $x \sim y \Rightarrow y \sim x$, for all $x, y \in S$. For example, equality is an equivalence relation. Given an equivalence on S, we can list all members equivalent to a given one together in a class, and in this way obtain a *partition* of S into a collection of disjoint subsets, the *equivalence classes* or *blocks*. The set of equivalence classes is denoted by $S/\sim$ and is called the *quotient set* of S by the equivalence $\sim$.

Given sets S, T, their *Cartesian* or *direct product*, denoted by $S \times T$, is the set of pairs (x, y), where $x \in S$, $y \in T$. If S, T are any ordered sets, their direct product can again be ordered by writing $(x, y) \leq (x', y')$ to mean: $x \leq x'$ or $x = x'$ and $y \leq y'$. This is easily verified to be an ordering, called the *lexicographic ordering*; it is a total ordering whenever both S and T are totally ordered.

References to the bibliography are by the name of the author and the date. In each section all the results are numbered consecutively, e.g. in Section 4.7 we have Theorem 4.7.1, Lemma 4.7.2, Proposition 4.7.3. We shall also use iff as an abbreviation for 'if and only if' and ■ indicates the end (or absence) of a proof. Many exercises are provided with hints, and the harder ones are starred.

Contents

1 Sets

Much of algebra can be done using only very little set theory; all that is needed is a means of comparing infinite sets, and the axiom of choice in the form of Zorn's lemma. These topics occupy Sections 1.1 and 1.2. They are followed in Section 1.3 by an introduction to graph theory. This is an extensive theory with many applications in algebra and elsewhere; all we shall do here is to present a few basic results, some of which will be used later, which convey the flavour of the topic.

1.1 Finite, Countable and Uncountable Sets

Most of our readers will have met sets before; a *set* for us is a collection of objects, its members or *elements*. These elements may themselves be sets; of course one has to be careful to avoid situations like Russell's paradox: 'the set Ω of all sets that are not members of themselves'; this quickly leads to a contradiction when one asks if $\Omega \in \Omega$. There are several ways of resolving this paradox, but they will not concern us here; all that is needed is some care in forming 'large' sets.

Given two sets, we may wish to compare them for size, i.e. the number of elements in each. We can use the natural numbers to count the members, but this may not be necessary. When Man Friday wanted to tell Robinson Crusoe that he had seen a boat with 17 men in it, he did this by exhibiting another 17-element set, and he could do this without being able to count up to 17. Even for a fully numerate person it may be easier to compare two sets rather than to count each; e.g. in a full lecture room a brief glance may suffice to convince us that there are as many people as seats. This suggests that it may be easier to determine when two sets have the same 'number of elements' than to find that number. Let us call two sets *equipotent* if there is a bijection (i.e. a one–one correspondence) between them. This relation of equipotence is an equivalence relation on any given collection of sets; here we avoid talking about the collection of *all* sets, as that would bring us dangerously close to the paradox mentioned above.

A set S is said to be *finite*, of *cardinal* n, if S is equipotent to the set $\{1, 2, \ldots, n\}$ consisting of the natural numbers from 1 to n. By convention the empty set, having no elements, is reckoned among the finite sets; its cardinal is 0 and it is denoted by $\varnothing$.

It is clear that two finite sets are equipotent if they have the same cardinal, and this may be regarded as the basis of counting. It is also true that sets of different finite cardinalities are not equipotent. This may seem intuitively obvious; we shall assume it here and defer to FA its derivation from the axioms for the natural numbers. More generally, we shall assume that for any natural numbers m, n, if there is an injective mapping from $\{1, 2, \ldots, m\}$ to $\{1, 2, \ldots, n\}$, then $m \leq n$. Let us abbreviate $\{1, 2, \ldots, n\}$ by $[n]$, for any $n \in \mathbf{N}$. It follows that if there is a bijection between $[m]$ and $[n]$, then $m \leq n$ and $n \leq m$, hence $m = n$. Thus for any finite set, the natural number which indicates its cardinal is uniquely determined. The contrapositive form of the above assertion states that if $m > n$, then there can be no injective mapping from $[m]$ to $[n]$. A more illuminating way of expressing this observation is Dirichlet's celebrated

Box Principle (Schubfachprinzip). *If $n + 1$ objects are distributed over n boxes, then some box must contain more than one of the objects.*

Although intuitively obvious, this principle is of great use in number theory and elsewhere.

Having given a formal definition of finite sets, we now define a set to be *infinite* if it is not finite. Until relatively recent times the notion of 'infinity' was surrounded by a good deal of mystery and uncertainty, even in mathematics. Thus towards the middle of the 19th century, Bernard Bolzano propounded as a paradox the fact that (in modern terms) an infinite set might be equipotent to a proper subset of itself. A closer study reveals the fact that every infinite set has this property, and this has even been taken as the basis of a definition of infinite sets; it certainly no longer seems a paradox. The work of Georg Cantor, Richard Dedekind and others from 1870 onwards has dispelled most of the uncertainties, and though mysteries remain, they will not hamper us in the relatively straightforward use we shall make of the theory.

In order to extend the notion of counting to infinite sets, we associate with every set X, finite or not, an object $|X|$ called its *cardinal* or cardinal *number*, defined in such a way that two sets have the same cardinal iff they are equipotent. Such a definition is possible because, as we have seen, equipotence is an equivalence relation on any collection of sets.

A non-empty finite set has as its cardinal a natural number; the empty set has cardinal 0. All other sets are infinite; their cardinals are said to be *transfinite* or *infinite*. In particular, the set $\mathbf{N}$ of all natural numbers is infinite; its cardinal is denoted by $\aleph_0$. The letter aleph, $\aleph$, the first of the Hebrew alphabet, is customarily used for infinite cardinal numbers. A set of cardinal $\aleph_0$ is also said to be *countable* (or *enumerable*); thus A is countable iff there is a bijection from $\mathbf{N}$ to A. If a set A is countable, it can be written in the form

$$A = \{a_1, a_2, a_3, \ldots\}, \tag{1.1.1}$$

where the a_i are distinct. Such a representation of A is called an *enumeration* of A, and a proof that a set is countable will often consist in giving an enumeration. Sometimes the term 'enumeration' is used for a set written as in (1.1.1) even if the a_i

are not all distinct; in that case we can always produce a strict enumeration by going through the sequence and omitting all repetitions. The set so obtained is finite or countable.

Many sets formed from countable sets are again countable, as our first result shows:

Theorem 1.1.1. *Any subset and any quotient of a countable set is countable or finite. If A and B are countable sets, then the union $A \cup B$ and Cartesian product $A \times B$ are again countable; more generally, the Cartesian product of any finite number of countable sets is countable. Further, a countable union of countable sets is countable and the collection of all finite subsets of a countable set is countable.*

We recall that a *quotient set* of A is the set of all blocks, i.e. equivalence classes, of some equivalence on A.

Proof. Any countable set A may be taken in the form (1.1.1); if A' is a subset, we go through the sequence $a_1, a_2, \ldots$ of elements of A and omit all terms not in A' to obtain an enumeration of A'. If A'' is a quotient set, and $x \mapsto \bar{x}$ is the natural mapping from A to A'', then $\{\bar{a}_1, \bar{a}_2, \ldots\}$ is an enumeration of A'', possibly with repetitions; hence A'' is countable (or finite).

Next let A be given by (1.1.1) and let $B = \{b_1, b_2, \ldots\}$; then $A \cup B$ may be enumerated as $\{a_1, b_1, a_2, b_2, \ldots\}$, where repetitions (which will occur if $A \cap B \neq \varnothing$) may be discarded. Similarly we can enumerate $A \times B$ as $\{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_1, b_3), (a_2, b_2), (a_3, b_1), \ldots\}$ by writing $A \times B$ as a square table and going along the finite diagonals. Now the result for a product of r countable sets follows by induction on r. If we have a countable family $\{A_n\}$ of countable sets, say $A_n = \{a_{ni}\}$, then we can enumerate the union $\cup A = \{a_{ni} | n, i \in \mathbf{N}\}$ by writing the elements a_{ni} as a matrix and going again along the diagonals.

Finally let A be any countable set and denote by A_r for $r = 1, 2, \ldots$ the set of all r-element subsets of A. Clearly A_r is countable, for it may be mapped into the Cartesian power A^r by the rule

$$\{a_{i_1}, \ldots, a_{i_r}\} \mapsto (a_{j_1}, \ldots, a_{j_r}),$$

where $j_1, \ldots, j_r$ is the sequence $i_1, \ldots, i_r$ arranged in ascending order. This provides a bijection of A_r with a subset of A^r, and it follows that A_r is countable. Now the earlier proof shows that the union $\cup A_r$ is countable, and adding $\varnothing$ as a further member we still have a countable set. ∎

With the help of this result many sets can be proved to be countable which do not at first sight appear to be so. Thus the set $\mathbf{Z}$ of all integers can be written as a union of $\mathbf{N} = \{1, 2, \ldots\}$ and $\mathbf{N}' = \{0, -1, -2, \ldots\}$; both $\mathbf{N}$ and $\mathbf{N}'$ are countable hence so is $\mathbf{Z}$. The set $\mathbf{Q}_+$ of all positive rational numbers is countable, as the image of $\mathbf{N}^2$ under the mapping $(a, b) \mapsto ab^{-1}$. Now $\mathbf{Q}$ itself can be written as the union of the set of all positive rational numbers, the negative rational numbers and 0; therefore $\mathbf{Q}$ is countable. The set of all algebraic numbers (see Section 7.1 below) is countable:

for a given degree n, the set of all monic equations of degree n over $\mathbf{Q}$ is equipotent to $\mathbf{Q}^n$, if we map

$$(a_1, \ldots, a_n) \mapsto x^n + a_1 x^{n-1} + \ldots + a_n = 0.$$

Each equation has at most n complex roots, so the set S_n of all roots of equations of degree n is countable, and now the set of all algebraic numbers is $S_1 \cup S_2 \cup \ldots$, which is again countable.

At this point a newcomer might be forgiven for thinking that perhaps every infinite set is countable. If that were so, there would of course be no need for an elaborate theory of cardinal numbers. In fact the existence of uncountable sets is one of the key results of Cantor's theory, and we shall soon meet examples of such sets.

Our next task is to extend the natural order on $\mathbf{N}$ to cardinal numbers. If α, β are any cardinals, let A, B be sets such that $|A| = \alpha$, $|B| = \beta$. We shall write $\alpha \leq \beta$ whenever there is an injective mapping from A to B. Whether such a mapping exists clearly depends only on α, β and not on A, B themselves, so the notation is justified. Further, $\alpha \leq \alpha$ holds for all α, because the identity mapping on A is injective, and since the composition of two injections is an injection, it follows that $\alpha \leq \beta$, $\beta \leq \gamma$ implies $\alpha \leq \gamma$. Thus we have a preordering; this will in fact turn out to be a total ordering, but for the moment we content ourselves with proving that it is an ordering, i.e. that '$\leq$' is antisymmetric. In terms of sets we must establish

Theorem 1.1.2 (Schröder–Bernstein theorem). *Let A, B be any sets and $f : A \to B$, $g : B \to A$ be any injective mappings. Then there is a bijection $h : A \to B$.*

Proof. By alternating applications of f and g we produce an infinite sequence of successive images starting from $a \in A$: $a, af, afg, afgf, \ldots$. Further, each element $a \in A$ is the image of at most one element of B under g, which may be written ag^{-1}, and each $b \in B$ is the image of at most one element bf^{-1} of A under f, so from $a \in A$ we obtain a sequence of inverse images which may or may not break off: ag^{-1}, $ag^{-1}f^{-1}, \ldots$. If we trace a given element $a \in A$ as far back as possible we find one of three cases: (i) there is a first 'ancestor' in A, i.e. $a_0 \in A \backslash Bg$, such that $a = a_0(fg)^n$ for some $n \geq 0$; (ii) there is a first ancestor in B, i.e. $b_0 \in B \backslash Af$, such that $a = b_0(gf)^n g$ for some $n \geq 0$; (iii) the sequence of inverse images continues indefinitely.

Each element of A comes under one of these headings, and likewise each element of B. Thus A is partitioned into three subsets A_1, A_2, A_3; similarly B is partitioned into $B_1 = A_1 f$, $B_2 = A_2 g^{-1}$ and $B_3 = A_3 f = A_3 g^{-1}$. It is clear that the restriction of f to A_1 is a bijection between A_1 and B_1, for each element of B_1 comes from one element of A_1. For the same reason the restriction of g to B_2 provides a bijection between B_2 and A_2, and we can use either f restricted to A_3 or g restricted to B_3 to obtain a bijection between A_3 and B_3. Thus we have found a bijection between A_i and B_i $(i = 1, 2, 3)$ and putting these together we obtain the desired bijection between A and B. ∎

This proof is essentially due to Gyula König (in 1906).

The sum and product of cardinals may be defined as follows. Let α, β be any cardinals, say $\alpha = |A|$, $\beta = |B|$, and assume that $A \cap B = \varnothing$. Then it is easily seen that $|A \cup B|$ depends only on α, β, not on A, B and we may define

$$\alpha + \beta = |A \cup B|.$$

Similarly we put

$$\alpha\beta = |A \times B|.$$

It is easy to verify that these operations satisfy the commutative and associative laws, and a distributive law, as in the case of the natural numbers. Moreover, for finite cardinals these operations agree with the usual operations of addition and multiplication. On the other hand, the cancellation law does not hold, thus we may have $\alpha + \beta = \alpha' + \beta$ or $\alpha\beta = \alpha'\beta$ for $\alpha \neq \alpha'$, and there is nothing corresponding to subtraction or division. In fact, it can be shown that if $\alpha, \beta \neq 0$ and at least one of α, β is infinite, then

$$\alpha + \beta = \alpha\beta = \max\{\alpha, \beta\}. \tag{1.1.2}$$

For any cardinals α, β we define β^α as $|B^A|$, where A, B are sets such that $|A| = \alpha$, $|B| = \beta$ and B^A denotes the set of all mappings from A to B. It is again clear that β^α is independent of the choice of A, B, and we note that for finite cardinals, β^α has its usual meaning: if A has m elements and B has n elements, then there is a choice of n elements to which to map each element of A, and these choices are independent, so there are $n.n \ldots n$ (m factors) $= n^m$ choices. Of course this interpretation applies only to finite sets.

If B is a 1-element set, then so is B^A, for any set A: each element of A is mapped to the unique element of B, and this applies even if A is empty, for a mapping $A \to B$ is defined as soon as we have specified the images of the elements of A; so when $A = \varnothing$, nothing needs to be done. When B is empty, then so is B^A, unless also $A = \varnothing$, for there is nowhere for the elements of A to map to. Hence we have

$$1^\alpha = 1, 0^\alpha = \begin{cases} 0 & \text{if } \alpha \neq 0, \\ 1 & \text{if } \alpha = 0. \end{cases} \tag{1.1.3}$$

Let us now assume that B has more than one element. Then we necessarily have

$$|B^A| \geq |A|. \tag{1.1.4}$$

For let b, b' be distinct elements of B; we can map A to B^A by the rule $a \mapsto \delta_a$, where

$$x\delta_a = \begin{cases} b & \text{if } x = a, \\ b' & \text{if } x \neq a. \end{cases}$$

This mapping is injective because for $a \neq a'$, δ_a differs from $\delta_{a'}$ at a. It is a remarkable fact that the inequality (1.1.4) is always strict. As usual we write $\alpha < \beta$ or $\beta > \alpha$ to mean '$\alpha \leq \beta$ and $\alpha \neq \beta$'.

Theorem 1.1.3. *For any cardinals α, β, if $\beta > 1$, then $\alpha < \beta^\alpha$. In particular,*

$$\alpha < 2^\alpha \tag{1.1.5}$$

for any cardinal α.

Proof. We have just seen that $\alpha \leq \beta^\alpha$ and it only remains to show that equality cannot hold. Taking sets A, B such that $|A| = \alpha$, $|B| = \beta$, we shall show that there is no surjective mapping from A to B^A; it then follows that these sets are not equipotent. Thus let $f : A \to B^A$ be given; in detail, f associates with each $a \in A$ a mapping from A to B, which may be denoted by f_a. We must show that f is not surjective, i.e. we must find $g : A \to B$ such that $g \neq f_a$ for all $a \in A$. This may be done very simply by constructing a mapping g to differ from f_a at a. By hypothesis, B has at least two elements, say b, b', where $b \neq b'$. We put

$$ag = \begin{cases} b' & \text{if } af_a = b, \\ b & \text{otherwise.} \end{cases}$$

Then g is well-defined and for each $a \in A$, $g \neq f_a$ because $ag \neq af_a$. ■

If in this theorem we take A to be countable and B a 2-element set, simply denoted by 2, then 2^A is again infinite, but uncountable. Moreover, we can in this way obtain arbitrarily large cardinals by starting from any infinite cardinal α and forming in succession $2^\alpha, 2^{2^\alpha}, \ldots$.

Theorem 1.1.3 again illustrates the dangers of operating with the 'set of all sets'. If we could form the union of all sets, U say, then U would contain 2^U as a subset, and it would follow that $|2^U| \leq |U|$, in contradiction to Theorem 1.1.3. This paradox was discussed by Cesare Burali-Forti and others in the closing years of the 19th century, and it provided the impetus for much of the axiomatic development that followed. Any axiomatic system now in use is designed to avoid the possibility of such paradoxes. For our purpose it is sufficient to note that we can avoid the paradoxes by not admitting constructions involving 'all sets' without further qualification.

We conclude this section with some applications of Theorem 1.1.3. Given any set A, we denote by $\mathscr{P}(A)$ the set whose members are all the subsets of A; e.g. $\mathscr{P}(\varnothing) = \{\varnothing\}$, $\mathscr{P}(\{x\}) = \{\varnothing, \{x\}\}$. This set $\mathscr{P}(A)$ is often called the *power set* of A; it is equipotent with 2^A. To obtain a bijection we associate with each subset C of A its *characteristic function* $\chi_C \in 2^A$; taking $2 = \{0, 1\}$, we have

$$\chi_C(x) = \begin{cases} 1 & \text{if } x \in C, \\ 0 & \text{if } x \notin C. \end{cases}$$

It is easily seen that the mapping $C \mapsto \chi_C$ provides a bijection between $\mathscr{P}(A)$ and 2^A. The inverse mapping is obtained by associating with each $f \in 2^A$ the inverse image of 1: $1f^{-1} = \{x \in A | xf = 1\}$. Now Theorem 1.1.3 shows the truth of

Corollary 1.1.4. *No set is equipotent with its power set. More precisely, given any set A, there is no surjection from A to $\mathscr{P}(A)$.* ■

As a further application we determine the cardinal of the set $\mathbf{R}$ of all real numbers. This cardinal is usually denoted by $\mathfrak{c}$ and is called the *cardinal* (or *power*) of the *continuum*.

Proposition 1.1.5. $\mathfrak{c} = 2^{\aleph_0}$.

Proof. We can replace $\mathbf{R}$ by the open interval $(0, 1) = \{x \in \mathbf{R} | 0 < x < 1\}$, for there is a bijection, e.g.

$$x \mapsto \frac{1}{2} + \frac{x}{2(1+x^2)^{1/2}}.$$

If we express each number in the binary scale: $a = 0.a_1a_2\ldots(a_i = 0 \text{ or } 1)$, then $a \mapsto f_a$, where $f_a(n) = a_n$, is a mapping $(0, 1) \to 2^{\mathbf{N}}$ which is injective, for distinct real numbers have distinct binary expansions. Indeed, some have more than one, e.g. $0.0111\ldots = 0.1000\ldots$, but we can achieve uniqueness by excluding representations in which only finitely many digits are 0. It follows that $\mathfrak{c} \leq 2^{\aleph_0}$. On the other hand, there is an injective mapping from $2^{\mathbf{N}}$ to $(0, 1)$, obtained by mapping f_a, defined as before, to $0.a_1a_2\ldots$ in the decimal scale; thus the image consists of the real numbers between 0 and 1 whose decimal expansion contains only 0's and 1's. This shows that $2^{\aleph_0} \leq \mathfrak{c}$, and the desired equality follows. ■

It was conjectured by Cantor that $\mathfrak{c}$ is the least cardinal greater than $\aleph_0$; this is known as *Cantor's continuum hypothesis* (CH). In 1939 Kurt Gödel showed that it is consistent with the usual axioms of set theory; thus if the usual system of axioms (which we have not given explicitly) is consistent, then it remains consistent when CH is added. In 1963 Paul J. Cohen showed CH to be independent of the usual axioms of set theory. Thus if the negation of CH is added to the axioms of set theory (assumed consistent), we again get a consistent system. This means that within the usual axiom system of set theory CH is undecidable.

Exercises

1. Show that the set of all intervals in $\mathbf{R}$ with rational endpoints is countable.
2. Let A be an infinite set, A' be a finite subset and B be its complement in A. By picking a countable subset of B, show that $|A| = |B|$ without assuming Equation (1.1.2).
3. Let A be an uncountable set, A' be a countable subset and B be its complement in A. Show that $|A| = |B|$ without assuming Equation (1.1.2).
4. Fill in the details of the following proof that the interval $(0, 1)$ is uncountable. If the real numbers in binary form (as in the proof of Proposition 1.1.5) could be enumerated as $a^{(1)}, a^{(2)}, \ldots$, we can find a number not included in the enumeration by putting $a = 0.b_1b_2\ldots$, where $b_n = 0$ or 1 according as $a^{(n)}$ has 1 or 0 in