Appunti di Fondamenti della Matematica

Silvio Valentini

versione (molto) provvisoria e (molto) incompleta
15 giugno 2014

Indice

Capitolo 1

Introduzione

La seconda parte del corso di Fondamenti della Matematica si propone di analizzare in qualche dettaglio due degli assiomi che compaiono nella usuale formalizzazione secondo Zermelo e Fraenkel della teoria degli insieme il cui ruolo è un po' diverso dagli altri visto che non si limitano a proporre opportune tecniche per costruire nuovi insieme a partire da insieme dati ma si preoccupano piuttosto di stabilire che esistono certi insiemi. Si tratta degli assiomi che sanciscono l'esistenza di un insieme infinito e l'esistenza di una funzione di scelta.

Ringraziamenti

???

Capitolo 2

Richiami di teoria degli insiemi

Per quanto riguarda la teoria degli insiemi è inutile presentare una nuova introduzione visto che si tratta di un argomento ampiamente trattato in letteratura. Per quel che serve a noi sono più che sufficienti le seguenti risorse che si possono trovare in internet e che vengono qui riportate solo per comodità di consultazione.

2.1 Introduction to set theory

Il primo testo, che fornisce una introduzione generale alla teoria degli insiemi pur non entrando nei dettagli, si può trovare qui:

`http://plato.stanford.edu/entries/set-theory`

Set Theory is the mathematical science of the infinite. It studies properties of sets, abstract objects that pervade the whole of modern mathematics. The language of set theory, in its simplicity, is sufficiently universal to formalize all mathematical concepts and thus set theory, along with Predicate Calculus, constitutes the true Foundations of Mathematics. As a mathematical theory, Set Theory possesses a rich internal structure, and its methods serve as a powerful tool for applications in many other fields of Mathematics. Set Theory, with its emphasis on consistency and independence proofs, provides a gauge for measuring the consistency strength of various mathematical statements. There are four main directions of current research in set theory, all intertwined and all aiming at the ultimate goal of the theory: to describe the structure of the mathematical universe. They are: inner models, independence proofs, large cardinals, and descriptive set theory.

2.1.1 The Essence of Set Theory

The objects of study of Set Theory are sets. As sets are fundamental objects that can be used to define all other concepts in mathematics, they are not defined in terms of more fundamental concepts. Rather, sets are introduced either informally, and are understood as something self-evident, or, as is now standard in modern mathematics, axiomatically, and their properties are postulated by the appropriate formal axioms.

The language of set theory is based on a single fundamental relation, called *membership*. We say that A is a member of B (in symbols $A \in B$), or that the set B contains A as its element. The understanding is that a set is determined by its elements; in other words, two sets are deemed equal if they have exactly the same elements. In practice, one considers sets of numbers, sets of points, sets of functions, sets of some other sets and so on. In theory, it is not necessary to distinguish between objects that are members and objects that contain members – the only objects one needs for the theory are sets (see the supplement 2.2 for further discussion).

Using the membership relation one can derive other concepts usually associated with sets, such as unions and intersections of sets. For example, a set C is the *union* of two sets A and B if its members are exactly those objects that are either members of A or members of B. The set C is uniquely determined, because we have specified what its elements are. There are more complicated

operations on sets that can be defined in the language of set theory (i.e. using only the relation $\in$), and we shall not concern ourselves with those. Let us mention another operation: the (unordered) *pair* $\{A, B\}$ has as its elements exactly the sets A and B. (If it happens that $A = B$, then the "pair" has exactly one member, and is called a *singleton* $\{A\}$.) By combining the operations of union and pairing, one can produce from any finite list of sets the set that contains these sets as members: $\{A, B, C, D, \ldots, K, L, M\}$. We also mention the *empty set* $\emptyset$, the set that has no elements. (The empty set is uniquely determined by this property, as it is the only set that has no elements – this is a consequence of the understanding that sets are determined by their elements.)

When dealing with sets informally, such operations on sets are self-evident; with the axiomatic approach, it is postulated that such operations can be applied: for instance, one postulates that for any sets A and B, the set $\{A, B\}$ exists. In order to endow set theory with sufficient expressive power one needs to postulate more general construction principles than those alluded to above. The guiding principle is that any objects that can be singled out by means of the language can be collected into a set. For instance, it is desirable to have the "set of all integers that are divisible by number 3", the "set of all straight lines in the Euclidean plane that are parallel to a given line", the "set of all continuous real functions of two real variables" etc. Thus one is tempted to postulate that given any property P, there exists a set whose members are exactly all the sets that have property P. As we shall see below, such an assumption is logically inconsistent, and the accepted construction principles are somewhat weaker than such a postulate.

One of the basic principles of set theory is the existence of an infinite set. The concept can be formulated precisely in the language of set theory, using only the membership relation, and the definition captures the accepted meaning of "infinite" (see the supplement 2.2 for further discussion).

Using the basic construction principles, and assuming the existence of infinite sets, one can define numbers, including integers, real numbers and complex numbers, as well as functions, functionals, geometric and topological concepts, and all objects studied in mathematics. In this sense, set theory serves as Foundations of Mathematics. The significance of this is that all questions of provability (or unprovability) of mathematical statements can be in principle reduced to formal questions of formal derivability from the generally accepted axioms of Set Theory.

While the fact that all of mathematics can be reduced to a formal system of set theory is significant, it would hardly be a justification for the study of set theory. It is the internal structure of the theory that makes it worthwhile, and it turns out that this internal structure is enormously complex and interesting. Moreover, the study of this structure leads to significant questions about the nature of the mathematical universe.

The fundamental concept in the theory of infinite sets is the cardinality of a set. Two sets A and B have the same cardinality if there exists a mapping from the set A onto the set B which is *one-to-one*, that is, it assigns each element of A exactly one element of B. It is clear that when two sets are finite, then they have the same cardinality if and only if they have the same number of elements. One can extend the concept of the "number of elements" to arbitrary, even infinite, sets. It is not apparent at first that there might be infinite sets of different cardinalities, but once this becomes clear, it follows quickly that the structure so described is rich indeed.

2.1.2 Origins of Set Theory

The birth of Set Theory dates to 1873 when Georg Cantor proved the uncountability of the real line. (One could even argue that the exact birthdate is December 7, 1873, the date of Cantor's letter to Dedekind informing him of his discovery.) Until then, no one envisioned the possibility that infinities come in different sizes, and moreover, mathematicians had no use for "actual infinity." The arguments using infinity, including the Differential Calculus of Newton and Leibniz, do not require the use of infinite sets, and infinity appears only as "a manner of speaking", to paraphrase Friedrich Gauss. The fact that the set of all positive integers has a proper subset, like the set of squares $\{1, 4, 9, 16, 25, \ldots\}$ of the same cardinality (using modern terminology) was considered somewhat paradoxical (this had been discussed at length by Galileo among others). Such apparent paradoxes prevented Bernhard Bolzano in 1840s from developing set theory, even though some of his ideas are precursors of Cantor's work. (It should be mentioned that Bolzano, an accomplished mathematician himself, coined the word *Menge* (= set) that Cantor used for objects of his theory.)

Motivation for Cantor's discovery of Set Theory came from his work on Fourier series (which led him to introduce ordinal numbers) and on transcendental numbers. Real numbers that are solutions of polynomial equations with integer coefficients are called algebraic, and the search was on for numbers that are not algebraic. A handful of these, called transcendental numbers, was discovered around that time, and a question arose how rare such numbers are. What Cantor did was to settle this question in an unexpected way, showing in one fell swoop that transcendental numbers are plentiful indeed. His famous proof went as follows: Let us call an infinite set A countable, if its elements can be enumerated; in other words, arranged in a sequence indexed by positive integers: a_1, a_2, a_3, ..., a_n, ... Cantor observed that many infinite sets of numbers are countable: the set of all integers, the set of all rational numbers, and also the set of all algebraic numbers. Then he gave his ingenious diagonal argument that proves, by contradiction, that the set of all real numbers is not countable. A consequence of this is that there exists a multitude of transcendental numbers, even though the proof, by contradiction, does not produce a single specific example (see the supplement 2.2 for further discussion).

Cantor's discovery of uncountable sets led him to the subsequent development of ordinal and cardinal numbers, with their underlying order and arithmetic, as well as to a plethora of fundamental questions that begged to be answered (such as the Continuum Hypothesis). After Cantor, mathematics has never been the same.

2.1.3 The Continuum Hypothesis

As the Continuum Hypothesis has been the most famous problem in Set Theory, let me explain what it says. The smallest infinite cardinal is the cardinality of a countable set. The set of all integers is countable, and so is the set of all rational numbers. On the other hand, the set of all real numbers is uncountable, and its cardinal is greater than the least infinite cardinal. A natural question arises: is this cardinal (the continuum) the very next cardinal. In other words, is it the case that there are no cardinals between the countable and the continuum? As Cantor was unable to find any set of real numbers whose cardinal lies strictly between the countable and the continuum, he conjectured that the continuum is the next cardinal: the Continuum Hypothesis. Cantor himself spent most of the rest of his life trying to prove the Continuum Hypothesis and many other mathematicians have tried too. One of these was David Hilbert, the leading mathematician of the last decades of the 19th century. At the World Congress of Mathematicians in Paris in 1900 Hilbert presented a list of major unsolved problems of the time, and the Continuum Hypothesis was the very first problem on Hilbert's list.

Despite the effort of a number of mathematicians, the problem remained unsolved until 1963, and it can be argued that in some sense the problem is still unsolved (see Section 2.1.7 on Independence Proofs).

2.1.4 Axiomatic Set Theory

In the years following Cantor's discoveries, development of Set Theory proceeded with no particular concern about how exactly sets should be defined. Cantor's informal "definition" was sufficient for proofs in the new theory, and the understanding was that the theory can be formalized by rephrasing the informal definition as a system of axioms. In the early 1900s it became clear that one has to state precisely what basic assumptions are made in Set Theory; in other words, the need has arisen to axiomatize Set Theory. This was done by Ernst Zermelo, and the immediate reasons for his axioms were twofold. The first one was the discovery of a paradox in Set Theory. This paradox is referred to as Russell's Paradox. Consider the *set* S of all sets that are not an element of itself. If one accepts the principle that all such sets can be collected into a set, then S should be a set. It is easy to see however that this leads to a contradiction (is the set S an element of itself?)

Russell's Paradox can be avoided by a careful choice of construction principles, so that one has the expressive power needed for usual mathematical arguments while preventing the existence of paradoxical sets (see the supplement 2.3 for further discussion). The price one has to pay for avoiding inconsistency is that some *sets* do not exist. For instance, there exists no "universal" set (the set of all sets), no set of all cardinal numbers, etc.

The other reason for axioms was more subtle. In the course of development of Cantor's theory of cardinal and ordinal numbers a question was raised whether every set can be provided with a certain structure, called *well-ordering* of the set. Zermelo proved that indeed every set can be well-ordered, but only after he introduced a new axiom that did not seem to follow from the other, more self-evident, principles. His *Axiom of Choice* has become a standard tool of modern mathematics, but not without numerous objections of some mathematicians and discussions in both mathematical and philosophical literature. The history of the Axiom of Choice bears strong resemblance to that of the other notorious axiom, Euclid's Fifth Postulate.

2.1.5 The Axiom of Choice

The Axiom of Choice states that for every set of mutually disjoint nonempty sets there exists a set that has exactly one member common with each of these sets. For instance, let S be a set whose members are mutually disjoint finite sets of real numbers. We can choose in each $X \in S$ the smallest number, and thus form a set that has exactly one member in common with each $X \in S$. What is not self-evident is whether we can make a choice every time, simultaneously for infinitely many sets X, regardless what these abstract sets are. The Axiom of Choice, which postulates the existence of a certain set (the choice set) without giving specific instructions how to construct such a set, is of a different nature than the other axioms, which all formulate certain construction principles for sets. It was this nonconstructive nature of the Axiom of Choice that fed the controversy for years to come.

An interesting application of the Axiom of Choice is the Banach-Tarski Paradox that states that the unit ball can be partitioned into a finite number of disjoint sets which then can be rearranged to form two unit balls. This is of course a paradox only when we insist on visualizing abstract sets as something that exists in the physical world. The sets used in the Banach-Tarski Paradox are not physical objects, even though they do exist in the sense that their existence is proved from the axioms of mathematics (including the Axiom of Choice).

The legitimate question is whether the Axiom of Choice is consistent, that is whether it cannot be refuted from the other axioms. (Notice the similarity with the non Euclidean geometry.) This question was answered by Gödel, and eventually the role of the Axiom of Choice has been completely clarified (see Section 2.1.7 on Independence Proofs).

2.1.6 Inner Models

In the 1930s, Gödel stunned the mathematical world by discovering that mathematics is incomplete. His Incompleteness Theorem states that every axiomatic system that purports to describe mathematics as we know it must be incomplete, in the sense that one can find a true statement expressible in the system that cannot be formally proved from the axioms. In view of this result one must consider the possibility that a mathematical conjecture that resists a proof might be an example of such an unprovable statement, and Gödel immediately embarked on the project of showing that the Continuum Hypothesis might be undecidable in the axiomatic set theory.

Several years after proving the Incompleteness Theorem, Gödel proved another groundbreaking result: he showed that both the Axiom of Choice and the Continuum Hypothesis are consistent with the axioms of set theory, that is that neither can be refuted by using those axioms. This he achieved by discovering a model of set theory in which both the Axiom of Choice and the Continuum Hypothesis are true.

Gödel's model $\mathcal{L}$ of "constructible sets" has since served as a blueprint for building so-called inner models. These models form a hierarchy and provide a glimpse into the as yet hidden structure of the mathematical universe. The advances in Inner Model Theory that have been made in the recent past owe much to the work of Ronald Jensen who introduced the study of the fine structure of constructible sets.

2.1.7 Independence Proofs

In 1963, Paul Cohen proved independence of the Axiom of Choice and of the Continuum Hypothesis. This he did by applying the method of forcing that he invented and constructing first a model of

set theory (with the axiom of choice) in which the Continuum Hypothesis fails, and then a model of set theory in which the Axiom of Choice fails. Together with Gödel's models, these models show that the Axiom of Choice can neither be proved nor refuted from the other axioms, and that the Continuum Hypothesis can neither be proved nor refuted from the axioms of set theory (including the Axiom of Choice).

Cohen's method proved extremely fruitful and led first to the solution of a number of outstanding problems (Suslin's Problem, the Lebesgue measurability Problem, Borel's Conjecture, Kaplansky's Conjecture, Whitehead's Problem and so on) and soon has become one of the cornerstones of modern set theory. The technique of forcing has to date been applied by hundreds of authors of numerous articles and has enormously advanced our knowledge of Foundations of Mathematics. Along with the theory of large cardinals it is used to gauge the consistency strength of mathematical statements.

2.2 Basic Set Theory

La prossima parte, che mostra come si possa ricostruire buona parte della matematica usuale a partire dalla teoria degli insiemi, si può trovare qui

`http://plato.stanford.edu/entries/set-theory/primer.html`

The following basic facts are excerpted from "Introduction to Set Theory", by Karel Hrbacek and Thomas Jech [HJ99].

2.2.1 Ordered Pairs

We begin by introducing the notion of the ordered pair. If a and b are sets, then the unordered pair $\{a, b\}$ is a set whose elements are exactly a and b. The "order" in which a and b are put together plays no role; $\{a, b\} = \{b, a\}$. For many applications, we need to pair a and b in a way making possible to "read off" which set comes "first" and which comes "second". We denote this ordered pair of a and b by (a, b); a is the first coordinate of the pair (a, b), b is the second coordinate.

As any object of our study, the ordered pair has to be a set. It should be defined in such a way that two ordered pairs are equal if and only if their first coordinates are equal and their second coordinates are equal. This guarantees in particular that $(a, b) \neq (b, a)$ if $a \neq b$.

Definition 2.2.1 $(a, b) = \{\{a\}, \{a, b\}\}$.

If $a \neq b$, (a, b) has two elements, a singleton $\{a\}$ and an unordered pair $\{a, b\}$. We find the first coordinate by looking at the element of $\{a\}$. The second coordinate is then the other element of $\{a, b\}$. If $a = b$, then $(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$ has only one element. In any case, it seems obvious that both coordinates can be uniquely "read off" from the set (a, b). We make this statement precise in the following theorem.

Theorem 2.2.2 *$(a, b) = (a', b')$ if and only if $a = a'$ and $b = b'$*

Proof. If $a = a'$ and $b = b'$, then, of course, $(a, b) = \{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\} = (a', b')$. The other implication is more intricate. Let us assume that $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$. If $a \neq b$, $\{a\} = \{a'\}$ and $\{a, b\} = \{a', b'\}$. So, first, $a = a'$ and then $\{a, b\} = \{a, b'\}$ implies $b = b$. If $a = b$, $\{\{a\}, \{a, a\}\} = \{\{a\}\}$. So $\{a\} = \{a'\}, \{a\} = \{a', b'\}$, and we get $a = a' = b'$, so $a = a'$ and $b = b'$ holds in this case, too.

With ordered pairs at our disposal, we can define ordered triples $(a, b, c) = ((a, b), c)$, ordered quadruples $(a, b, c, d) = ((a, b, c), d)$, and so on. Also, we define ordered "one-tuples" $(a) = a$.

2.2.2 Relations

A binary relation is determined by specifying all ordered pairs of objects in that relation; it does not matter by what property the set of these ordered pairs is described. We are led to the following definition.

Definition 2.2.3 *A set R is a binary relation if all elements of R are ordered pairs, i.e., if for any $z \in R$ there exist x and y such that $z = (x, y)$. It is customary to write $x\ R\ y$ instead of $(x, y) \in R$. We say that x is in relation R with y if $x\ R\ y$ holds.*

The set of all x which are in relation R with some y is called the *domain* of R and denoted by "$\mathsf{dom}(R)$". So $\mathsf{dom}(R) = \{x \mid \text{there exists } y \text{ such that } x\ R\ y\}$, namely $\mathsf{dom}(R)$ is the set of all first coordinates of ordered pairs in R.

The set of all y such that, for some x, x is in relation R with y is called the *range* of R, denoted by "$\mathsf{ran}(R)$". So $\mathsf{ran}(R) = \{y \mid \text{there exists } x \text{ such that } x\ R\ y\}$.

2.2.3 Functions

Function, as understood in mathematics, is a procedure, a rule, assigning to any object a from the domain of the function a unique object b, the value of the function at a. A function, therefore, represents a special type of relation, a relation where every object a from the domain is related to precisely one object in the range, namely, to the value of the function at a.

Definition 2.2.4 *A binary relation F is called a function (or mapping, correspondence) if $a\ F\ b_1$ and $a\ F\ b_2$ imply $b_1 = b_2$ for any a, b_1, and b_2. In other words, a binary relation F is a function if and only if for every a from $\mathsf{dom}(F)$ there is exactly one b such that $a\ F\ b$. This unique b is called the* value *of F at a and is denoted $F(a)$ or F_a. [$F(a)$ is not defined if $a \notin \mathsf{dom}(F)$]. If F is a function with $\mathsf{dom}(F) = A$ and $\mathsf{ran}(F) \subseteq B$, it is customary to use the notations $F : A \to B$, $\langle F(a) \mid a \in A\rangle$, $\langle F_a \mid a \mid A\rangle$, $\langle F_a\rangle_{a\in A}$ for the function F. The range of the function F can then be denoted $\{F(a) \mid a \in A\}$ or $\{F_a\}_{a\in A}$.*

The Axiom of Extensionality can be applied to functions as follows.

Lemma 2.2.5 *Let F and G be functions. $F = G$ if and only if $\mathsf{dom}(F) = \mathsf{dom}(G)$ and $F(x) = G(x)$ for all $x \in \mathsf{dom}(F)$.*

A function f is called *one-to-one* or *injective* if $a_1 \in \mathsf{dom}(f)$, $a_2 \in \mathsf{dom}(f)$, and $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$. In other words if $a_1 \in \mathsf{dom}(f)$, $a_2 \in \mathsf{dom}(f)$, and $f(a_1) = f(a_2)$, then $a_1 = a_2$.

2.2.4 Natural Numbers

In order to develop mathematics within the framework of the axiomatic set theory, it is necessary to define natural numbers. We all know natural numbers intuitively: 0, 1, 2, 3, ..., 17, ..., 324, etc., and we can easily give examples of sets having zero, one, two, or three elements.

To define number 0, we choose a representative of all sets having no elements. But this is easy, since there is only one such set. We define $0 = \emptyset$. Let us proceed to sets having one element (singletons): $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\emptyset, \{\emptyset\}\}\}$; in general, $\{x\}$. How should we choose a representative? Since we already defined one particular object, namely 0, a natural choice is $\{0\}$. So we define

$$1 = \{0\} = \{\emptyset\}$$

Next we consider sets with two elements: $\{\emptyset, \{\emptyset\}\}$, $\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, $\{\{\emptyset\}, \{\{\emptyset\}\}\}$, etc. By now, we have defined 0 and 1, and $0 \neq 1$. We single out a particular two-element set, the set whose elements are the previously defined numbers 0 and 1:

$$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$$

It should begin to be obvious how the process continues:

$$\begin{array}{lcl} 3 & = & \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\ 4 & = & \{0,1,2,3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\ 5 & = & \{0,1,2,3,4\} \end{array}$$

etc.

The idea is simply to define a natural number n as the set of all smaller natural numbers: $\{0, 1, \ldots, n-1\}$. In this way, n is a particular set of n elements.

This idea still has a fundamental deficiency. We have defined 0, 1, 2, 3, 4, and 5 and could easily define 17 and – not so easily – 324. But no list of such definitions tells us what a natural number is in general. We need a statement of the form: A set n is a natural number if .... We cannot just say that a set n is a natural number if its elements are all the smaller natural numbers, because such a "definition" would involve the very concept being defined.

Let us observe the construction of the first few numbers again. We defined $2 = \{0, 1\}$. To get 3, we had to adjoin a third element to 2, namely, 2 itself:

$$3 = 2 \cup \{2\} = \{0, 1\} \cup \{2\}$$

Similarly,

$$\begin{array}{lcl} 4 & = & 3 \cup \{3\} = \{0,1,2\} \cup \{3\}, \\ 5 & = & 4 \cup \{4\}, \end{array}$$

etc.

Given a natural number n, we get the "next" number by adjoining one more element to n, namely, n itself. The procedure works even for 1 and 2: $1 = 0 \cup \{0\}$, $2 = 1 \cup \{1\}$, but, of course, not for 0, the least natural number.

These considerations suggest the following.

Definition 2.2.6 *The* successor *of a set x is the set* $\mathsf{S}(x) = x \cup \{x\}$

Intuitively, the successor $S(n)$ of a natural number n is the "one bigger" number $n+1$. We use the more suggestive notation $n + 1$ for $\mathsf{S}(n)$ in what follows. We later define addition of natural numbers (using the notion of successor) in such a way that $n + 1$ indeed equals the sum of n and 1. Until then, it is just a notation, and no properties of addition are assumed or implied by it.

We can now summarize the intuitive understanding of natural numbers as follows:

1. 0 is a natural number.
2. If n is a natural number, then its successor $n + 1$ is also a natural number.
3. All natural numbers are obtained by application of (1) and (2), i.e., by starting with 0 and repeatedly applying the successor operation: 0, $0 + 1 = 1$, $1 + 1 = 2$, $2 + 1 = 3$, $3 + 1 = 4$, $4 + 1 = 5$, etc.

Definition 2.2.7 *A set I is called* inductive *if*

1. $0 \in I$.
2. *If* $n \in I$, *then* $(n + 1) \in I$.

An inductive set contains 0 and, with each element, also its successor. According to (3), an inductive set should contain all natural numbers. The precise meaning of (3) is that the set of natural numbers is an inductive set which contains no other elements but natural numbers, i.e., it is the smallest inductive set. This leads to the following definition.

Definition 2.2.8 *The set of all* natural numbers *is the set*

$$\mathsf{Nat} = \{x \mid x \in I \text{ for every inductive set } I\}$$

The elements of Nat are called *natural numbers*. Thus a set x is a natural number if and only if it belongs to every inductive set.

2.2.5 Cardinality of Sets

From the point of view of pure set theory, the most basic question about a set is: How many elements does it have? It is a fundamental observation that we can define the statement "sets A and B have the same number of elements" without knowing anything about numbers.

Definition 2.2.9 *Sets A and B have the* same cardinality *if there is a one-to-one function f with domain A and range B. We denote this by $\mid A \mid = \mid B \mid$.*

Definition 2.2.10 *The cardinality of A is less than or equal to the cardinality of B (notation: $\mid A \mid \leq \mid B \mid$) if there is a one-to-one mapping of A into B.*

Notice that $\mid A \mid \leq \mid B \mid$ means that $\mid A \mid = \mid C \mid$ for some subset C of B. We also write $\mid A \mid < \mid B \mid$ to mean that $\mid A \mid \leq \mid B \mid$ and not $\mid A \mid = \mid B \mid$, i.e., that there is a one-to-one mapping of A onto a subset of B, but there is no one-to-one mapping of A onto B.

Lemma 2.2.11 *Let A, B and C be sets. Then*

1. *If $\mid A \mid \leq \mid B \mid$ and $\mid A \mid = \mid C \mid$, then $\mid C \mid \leq \mid B \mid$.*
2. *If $\mid A \mid \leq \mid B \mid$ and $\mid B \mid = \mid C \mid$, then $\mid A \mid \leq \mid C \mid$.*
3. *$\mid A \mid \leq \mid A \mid$.*
4. *If $\mid A \mid \leq \mid B \mid$ and $\mid B \mid \leq \mid C \mid$, then $\mid A \mid \leq \mid C \mid$.*

Theorem 2.2.12 (Cantor-Bernstein Theorem) *If $\mid X \mid \leq \mid Y \mid$ and $\mid Y \mid \leq \mid X \mid$, then $\mid X \mid = \mid Y \mid$.*

2.2.6 Finite Sets

Finite sets can be defined as those sets whose size is a natural number.

Definition 2.2.13 *A set S is* finite *if it has the same cardinality as some natural number $n \in \mathsf{Nat}$. We then define $\mid S \mid = n$ and say that S* has *n* elements. *A set is* infinite *if it is not finite.*

2.2.7 Countable Sets

Definition 2.2.14 *A set S is* countable *if $\mid S \mid = \mid \mathsf{Nat} \mid$. A set S is* at most countable *if $\mid S \mid \leq \mid \mathsf{Nat} \mid$.*

Thus a set S is countable if there is a one-to-one mapping of Nat onto S, that is, if S is the range of an infinite one-to-one sequence.

Theorem 2.2.15 *An infinite subset of a countable set is countable.*

Proof. Let A be a countable set, and let $B \subseteq A$ be infinite. There is an infinite one-to-one sequence $\langle a_n \rangle_{n=0,\ldots}$, whose range is A. We let $b_0 = a_{k_0}$, where k_0 is the least k such that $a_k \in B$. Having constructed b_n, we let $b_{n+1} = a_{k_{n+1}}$, where k_{n+1} is the least k such that $a_k \in B$ and $a_k \neq b_i$ for every $i \leq n$. Such k exists since it is easily seen that $B = \{b_n \mid n \in \mathsf{Nat}\}$ and that $\langle b_n \rangle_{n=0,\ldots}$ is one-to-one. Thus B is countable.

Corollary 2.2.16 *A set is at most countable if and only if it is either finite or countable.*

The range of an infinite one-to-one sequence is countable. If $\langle a_n \rangle_{n=0,\ldots}$ is an infinite sequence which is not one-to-one, then the set $\{a_n\}_{n=0,\ldots}$ may be finite (e.g., this happens if it is a constant sequence). However, if the range is infinite, then it is countable.

Theorem 2.2.17 *The range of an infinite sequence $\langle a_n \rangle_{n=0,\ldots}$ is at most countable, i.e., either finite or countable. (In other words, the image of a countable set under any mapping is at most countable.)*

Proof. By recursion, we construct a sequence $\langle b_n \rangle_{n=0,\ldots}$ (with either finite or infinite domain) which is one-to-one and has the same range as $\langle a_n \rangle_{n=0,\ldots}$. We let $b_0 = a_0$, and, having constructed b_n, we let $b_{n+1} = a_{k_{n+1}}$, where k_{n+1} is the least k such that $a_k \neq b_i$ for all $i \leq n$. (If no such k exists, then we consider the finite sequence $\langle b_i \mid i \leq n \rangle$). The sequence $\langle b_i \rangle$ thus constructed is one-to-one and its range is $\{a_n\}_{n=0,\ldots}$.

One should realize that not all properties of size carry over from finite sets to the infinite case. For instance, a countable set S can be decomposed into two disjoint parts, A and B, such that $\mid A \mid = \mid B \mid = \mid S \mid$; that is inconceivable if S is finite (unless $S = \emptyset$).

Namely, consider the set $E = \{2k \mid k \in \mathsf{Nat}\}$ of all even numbers, and the set $O = \{2k + 1 \mid k \in \mathsf{Nat}\}$ of all odd numbers. Both E and O are infinite, hence countable; thus we have $\mid \mathsf{Nat} \mid = \mid E \mid = \mid O \mid$ while $\mathsf{Nat} = E \cup O$ and $E \cap O = \emptyset$.

We can do even better. Let p_n denote the n^{th} prime number (i.e., $p_0 = 2$, $p_1 = 3$, etc.). Let

$$S_0 = \{2^k \mid k \in \mathsf{Nat}\}, S_1 = \{3^k \mid k \in \mathsf{Nat}\}, \ldots, S_n = \{p_n^k \mid k \in \mathsf{Nat}\}, \ldots.$$

The sets $S_n (n \in \mathsf{Nat})$ are mutually disjoint countable subsets of Nat. Thus we have $\bigcup_{n=0,\ldots} S_n \subseteq \mathsf{Nat}$, where $\mid S_n \mid = \mid \mathsf{Nat}$ and the S_ns are mutually disjoint.

The following two theorems show that simple operations applied to countable sets yield countable sets.

Theorem 2.2.18 *The union of two countable sets is a countable set.*

Proof. Let $A = \{a_n \mid n \in \mathsf{Nat}\}$ and $B = \{b_n \mid n \in \mathsf{Nat}\}$ be countable. We construct a sequence $\langle c_n \rangle_{n=0,\ldots}$ as follows: $c_{2k} = a_k$ and $c_{2k+1} = b_k$ for all $k \in \mathsf{Nat}$. Then $A \cup B = \{c_n \mid n \in \mathsf{Nat}\}$ and since it is infinite, it is countable.

Corollary 2.2.19 *The union of a finite system of countable sets is countable.*

Proof. By induction (on the size of the system).

Theorem 2.2.20 *If A and B are countable, then $A \times B$ is countable.*

Proof. It suffices to show that $\mid \mathsf{Nat} \times \mathsf{Nat} \mid = \mid \mathsf{Nat} \mid$, i.e., to construct either a one-to-one mapping of $\mathsf{Nat} \times \mathsf{Nat}$ onto Nat or a one-to-one sequence with range $\mathsf{Nat} \times \mathsf{Nat}$. Consider the function

$$f(k, n) = 2^k \cdot (2n + 1) - 1.$$

It is easy to verify that f is one-to-one and that the range of f is Nat.

Corollary 2.2.21 *The cartesian product of a finite number of countable sets is countable. Consequently, Nat^m is countable, for every $m > 0$.*

Theorem 2.2.22 *Let $\langle A_n \mid n \in \mathsf{Nat} \rangle$ be a countable system of at most countable sets, and let $\langle a_n \mid n \in \mathsf{Nat} \rangle$ be a system of enumerations of A_n; i.e., for each $n \in \mathsf{Nat}$, $a_n = \langle a_n(k) \mid k \in \mathsf{Nat} \rangle$ is an infinite sequence, and $A_n = \{a_n(k) \mid k \in \mathsf{Nat}\}$. Then $\bigcup_{n=0,\ldots} A_n$ is at most countable.*

Proof. Define $f : \mathsf{Nat} \times \mathsf{Nat} \to \bigcup_{n=0,\ldots} A_n$ by $f(n, k) = a_n(k)$. Then, f maps $\mathsf{Nat} \times \mathsf{Nat}$ onto $\bigcup_{n=0,\ldots} A_n$, so the latter is at most countable.

As a corollary of this result we can now prove

Theorem 2.2.23 *If A is countable, then the set $\mathsf{Seq}(A)$ of all finite sequences of elements of A is countable.*

Proof. It is enough to prove the theorem for $A = \mathsf{Nat}$. As $\mathsf{Seq}(\mathsf{Nat}) = \bigcup_{n=0,\ldots} \mathsf{Nat}^n$, the theorem follows if we can produce a sequence $\langle a_n \mid n \geq 1\rangle$ of enumerations of Nat^n. We do that by recursion. Let g be a one-to-one mapping of Nat onto $\mathsf{Nat} \times \mathsf{Nat}$. Define recursively

$$\begin{array}{lcl} a_1(i) & = & \langle i\rangle \text{ for all } i \in \mathsf{Nat}; \\ a_{n+1}(i) & = & \langle b_0, \ldots, b_{n-1}, i_2\rangle \text{ where } g(i) = (i_1, i_2) \text{ and } \langle b_0, \ldots, b_{n-1}\rangle = a_n(i_1), \text{ for all } i \in \mathsf{Nat}. \end{array}$$

The idea is to let $a_{n+1}(i)$ be the $(n+1)$-tuple resulting from the concatenation of the $(i_1)^{\text{th}}$ n-tuple (in the previously constructed enumeration of n-tuples, a_n) with i_2. An easy proof by induction shows that a_n is onto Nat^n, for all $n \geq 1$, and therefore $\bigcup_{n=1,\ldots} \mathsf{Nat}^n$ is countable. Since $\mathsf{Nat}^0 = \{\langle\rangle\}$, $\bigcup_{n=0,\ldots} \mathsf{Nat}^n$ is also countable.

Corollary 2.2.24 *The set of all finite subsets of a countable set is countable.*

Proof. The function F defined by $F(\langle a_0, \ldots, a_{n-1}\rangle) = \{a_0, \ldots, a_{n-1}\}$ maps the countable set $\mathsf{Seq}(A)$ onto the set of all finite subsets of A.

Other useful results about countable sets are the following.

Theorem 2.2.25 *The set of all integers* Z *and the set of all rational numbers* Q *are countable.*

Proof. Z is countable because it is the union of two countable sets:

$$\mathsf{Z} = \{0, 1, 2, 3, \ldots\} \cup \{-1, -2, -3, \ldots\}.$$

Q is countable because the function $f : \mathsf{Z} \times (\mathsf{Z} - \{0\}) \to \mathsf{Q}$ defined by $f(p, q) = \frac{p}{q}$ maps a countable set onto Q.

2.2.8 Real Numbers

Definition 2.2.26 *An ordered set* $(X, <)$ *is* dense *if it has at least two elements and if for all* $a, b \in X$, $a < b$ *implies that there exists* $x \in X$ *such that* $a < x < b$.

Let us call the least and the greatest elements of a linearly ordered set (if they exist) the endpoints of the set.

The most important example of a countable dense linearly ordered set is the set Q of all rational numbers, ordered by size. The ordering is dense because, if r, s are rational numbers and $r < s$, then $x = \frac{(r+s)}{2}$ is also a rational number, and $r < x < s$. Moreover, $(\mathsf{Q}, <)$ has no endpoints (if $r \in \mathsf{Q}$ then $r + 1, r - 1 \in \mathsf{Q}$ and $r - 1 < r < r + 1$).

Definition 2.2.27 *Let* $(P, <)$ *be a dense linearly ordered set.* P *is* complete *if every non-empty* $S \subseteq P$ *bounded from above has a supremum.*

The ordered set $(\mathsf{Q}, <)$ of rationals has a unique completion (up to isomorphism); this is the ordered set of real numbers. The completion of $(\mathsf{Q}, <)$ is denoted $(\mathsf{R}, <)$; the elements of R are the real numbers.

Theorem 2.2.28 $(\mathsf{R}, <)$ *is the unique (up to isomorphism) complete linearly ordered set without endpoints that has a countable subset dense in it.*

2.2.9 Uncountable Sets

All infinite sets whose cardinalities we have determined up to this point turned out to be countable. Naturally, a question arises whether perhaps all infinite sets are countable. If it were so, this book might end with the preceding section. It was a great discovery of Georg Cantor that uncountable sets, in fact, exist. This discovery provided an impetus for the development of set theory and became a source of its depth and richness.

Theorem 2.2.29 *The set* R *of all real numbers is uncountable.*

Proof. Assume that R is countable, i.e., R is the range of some infinite sequence $\langle r_n \rangle_{n=0,\ldots}$. Let $a_0(n).a_1(n)a_2(n)a_3(n)\ldots$ be the decimal expansion of r_n. Let $b_n = 1$ if $a_n(n) = 0$, $b_n = 0$ otherwise; and let r be the real number whose decimal expansion is $0.b_1b_2b_3\ldots$. We have $b_n \neq a_n(n)$, hence $r \neq r_n$, for all $n = 1, 2, 3, \ldots$, a contradiction.

The combinatorial heart of the diagonal argument (quite similar to Russell's Paradox, which is of later origin) becomes even clearer in the next theorem.

Theorem 2.2.30 *The set of all sets of natural numbers is uncountable; in fact,* $| \mathcal{P}(\mathsf{Nat}) | > | \mathsf{Nat} |$.

Proof. The function $f : \mathsf{Nat} \to \mathcal{P}(\mathsf{Nat})$ defined by $f(n) = \{n\}$ is one-to-one, so $| \mathsf{Nat} | \leq | \mathcal{P}(\mathsf{Nat}) |$. We prove that for every sequence $\langle S_n \mid n \in \mathsf{Nat} \rangle$ of subsets of Nat there is some $S \subseteq \mathsf{Nat}$ such that $S \neq S_n$ for all $n \in \mathsf{Nat}$. This shows that there is no mapping of Nat onto $\mathcal{P}(\mathsf{Nat})$, and hence $| \mathcal{P}(\mathsf{Nat}) | > | \mathsf{Nat} |$.

We define the set $S \subseteq \mathsf{Nat}$ as follows: $S = \{n \in \mathsf{Nat} \mid n \notin S_n\}$. The number n is used to distinguish S from S_n: If $n \in S_n$, then $n? \notin S$, and if $n \notin S_n$, then $n \in S$. In either case, $S \notin S_n$, as required.

The set $2^{\mathsf{Nat}} = \{0, 1\}^{\mathsf{Nat}}$ of all infinite sequences of 0's and 1's is also uncountable, and, in fact, has the same cardinality as $\mathcal{P}(\mathsf{Nat})$ and R.

Theorem 2.2.31 $| \mathcal{P}(\mathsf{Nat}) | = | 2^{\mathsf{Nat}} | = | \mathsf{R} |$.

Proof. For each $S \subseteq \mathsf{Nat}$ define the characteristic function of S, $\chi_S : \mathsf{Nat} \to \{0, 1\}$, as follows:

$$\chi_{S(n)} = \begin{cases} 0 & \text{if } n \in S; \\ 1 & \text{if } n \notin S. \end{cases}$$

It is easy to check that the correspondence between sets and their characteristic functions is a one-to-one mapping of $\mathcal{P}(\mathsf{Nat})$ onto $\{0, 1\}^{\mathsf{Nat}}$.

To complete the proof, we show that $| \mathsf{R} | \leq | \mathcal{P}(\mathsf{Nat}) |$ and also $| 2^{\mathsf{Nat}} | \leq | \mathsf{R} |$ and use the Cantor-Bernstein Theorem.

1. We have constructed real numbers as cuts in the set Q of all rational numbers. The function that assigns to each real number $r = (A, B)$ the set $A \subseteq \mathsf{Q}$ is a one-to-one mapping of R into $\mathcal{P}(\mathsf{Q})$. Therefore $| \mathsf{R} | \leq | \mathcal{P}(\mathsf{Q}) |$. As $| \mathsf{Q} | = | \mathsf{Nat} |$, we have $| \mathcal{P}(\mathsf{Q}) | = | \mathcal{P}(\mathsf{Nat}) |$. Hence $| \mathsf{R} | \leq | \mathcal{P}(\mathsf{Nat}) |$.

2. To prove $| 2^{\mathsf{Nat}} | \leq | \mathsf{R} |$ we use the decimal representation of real numbers. The function that assigns to each infinite sequence $\langle a_n \rangle$ of 0s and 1s the unique real number whose decimal expansion is $0.a_0a_1a_2\ldots$ is a one-to-one mapping of 2^{Nat} into R. Therefore we have $| 2^{\mathsf{Nat}} | \leq | \mathsf{R} |$.

2.3 Zermelo-Fraenkel Set Theory

Infine la descrizione assiomatica della teoria degli insiemi si può trovare in

`http://plato.stanford.edu/entries/set-theory/ZF.html`

Axioms of ZF

Extensionality:

$$\forall x \forall y [\forall z (z \in x \equiv z \in y) \to x = y]$$

This axiom asserts that when sets x and y have the same members, they are the same set.

The next axiom asserts the existence of the empty set:
Null Set:

$$\exists x \neg \exists y (y \in x)$$

Since it is provable from this axiom and the previous axiom that there is a unique such set, we may introduce the notation '$\emptyset$' to denote it.

The next axiom asserts that if given any set x and y, there exists a pair set of x and y, i.e., a set which has only x and y as members:

Pairs:

$$\forall x \forall y \exists z \forall w (w \in z \equiv (w = x \vee w = y))$$

Since it is provable that there is a unique pair set for each given x and y, we introduce the notation '$\{x, y\}$' to denote it.

The next axiom asserts that for any given set x, there is a set y which has as members all of the members of all of the members of x:

Unions:

$$\forall x \exists y \forall z [z \in y \equiv \exists w (w \in x \wedge z \in w)]$$

Since it is provable that there is a unique 'union' of any set x, we introduce the notation '$\bigcup x$' to denote it.

The next axiom asserts that for any set x, there is a set y which contains as members all those sets whose members are also elements of x, i.e., y contains all of the subsets of x:

Power Set:

$$\forall x \exists y \forall z [z \in y \equiv \forall w (w \in z \rightarrow w \in x)]$$

Since every set provably has a unique 'power set', we introduce the notation $\mathcal{P}(x)$ to denote it. Note also that we may define the notion x is a subset of y ($x \subseteq y$) as: $\forall z (z \in x \rightarrow z \in y)$. Then we may simplify the statement of the Power Set Axiom as follows:

$$\forall x \exists y \forall z [z \in y \equiv z \subseteq x)$$

The next axiom asserts the existence of an infinite set, i.e., a set with an infinite number of members:

Infinity:

$$\exists x [\emptyset \in x \wedge \forall y (y \in x \rightarrow \cup \{y, \{y\}\} \in x)]$$

We may think of this as follows. Let us define the union of x and y ('$x \cup y$') as the union of the pair set of x and y, i.e., as $\cup\{x, y\}$. Then the Axiom of Infinity asserts that there is a set x which contains $\emptyset$ as a member and which is such that whenever a set y is a member of x, then $y \cup \{y\}$ is a member of x. Consequently, this axiom guarantees the existence of a set of the following form:

$$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots\}$$

Notice that the second element, $\{\emptyset\}$, is in this set because (1) the fact that $\emptyset$ is in the set implies that $\emptyset \cup \{\emptyset\}$ is in the set and (2) $\emptyset \cup \{\emptyset\}$ just is $\{\emptyset\}$. Similarly, the third element, $\{\emptyset, \{\emptyset\}\}$, is in this set because (1) the fact that $\{\emptyset\}$ is in the set implies that $\{\emptyset\} \cup \{\{\emptyset\}\}$ is in the set and (2) $\{\emptyset\} \cup \{\{\emptyset\}\}$ just is $\{\emptyset, \{\emptyset\}\}$. And so forth.

The next axiom asserts that every set is 'well-founded':

Regularity:

$$\forall x [x \neq \emptyset \rightarrow \exists y (y \in x \wedge \forall z (z \in x \rightarrow \neg (z \in y)))]$$

A member y of a set x with this property is called a 'minimal' element. This axiom rules out the existence of circular chains of sets (e.g., such as $x \in y$ and $y \in z$ and $z \in x$) as well as infinitely descending chains of sets (such as $\ldots x_3 \in x_2 \in x_1 \in x_0$).

The final axiom of ZF is the Replacement Schema. Suppose that $\phi(x, y, \overline{u})$ is a formula with x and y free, and let $\overline{u}$ represent the variables $u_1, \ldots, u_k$, which may or may not be free in ϕ. Furthermore, let $\phi_{x,y,\overline{u}}[s, r, \overline{u}]$ be the result of substituting s and r for x and y, respectively, in $\phi(x, y, \overline{u})$. Then every instance of the following schema is an axiom:

Replacement Schema:

$$\forall u_1 \ldots \forall u_k [\forall x \exists! y \phi(x, y, \overline{U}) \rightarrow \forall w \exists v \forall r (r \in v \equiv \exists s (s \in w \wedge \phi_{x,y,\overline{u}}[s, r, \overline{u}]))]$$

In other words, if we know that ϕ is a functional formula (which relates each set x to a unique set y), then if we are given a set w, we can form a new set v as follows: collect all of the sets to which the members of w are uniquely related by ϕ.

Note that the Replacement Schema can take you 'out of' the set w when forming the set v. The elements of v need not be elements of w. By contrast, the well-known Separation Schema of Zermelo yields new sets consisting only of those elements of a given set w which satisfy a certain condition ψ. That is, suppose that $\psi(x, \overline{u})$ has x free and may or may not have $u_1, \ldots, u_k$ free. And let $\psi_{x,\overline{u}}[r, \overline{u}]$ be the result of substituting r for x in $\psi(x, \overline{u})$. Then the Separation Schema asserts:

Separation Schema:

$$\forall u_1 \ldots \forall u_k[\forall w \exists v \forall r(r \in v \equiv r \in w \wedge \psi_{x,\overline{u}}[r, \overline{u}])]$$

In other words, if given a formula ψ and a set w, there exists a set v which has as members precisely the members of w which satisfy the formula ψ.

Capitolo 3

L'assioma dell'infinito

Non è difficile rendersi conto che nella formalizzazione di Zermelo e Fraenkel compaiono due tipi di assiomi. Ci sono assiomi come quello dell'insieme vuoto, della coppia, dell'unione, dell'insieme potenza, della separazione e dell'infinito che sostengono che certe collezioni sono insiemi (sotto opportune ipotesi), e che ci insegnano quindi come possiamo costruire gli insiemi di cui possiamo avere bisogno, e ci sono assiomi come quello di regolarità che richiedono dagli insiemi qualche proprietà.

Per quanto riguarda i primi una maniera molto semplice per capire la loro rilevanza è quella di chiedersi cosa *non* si potrebbe fare in loro assenza. Consideriamo quindi in questa prospettiva l'assioma dell'infinito: come sarebbe la teoria degli insiemi in sua assenza o addirittura in presenza di una qualche forma di assioma che neghi l'esistenza di insiemi infiniti? (esercizio: quale potrebbe essere un assioma per negare la presenza di insiemi infiniti?)

Per capire come rispondere a questa domanda possiamo provare a costruire un universo di insiemi che contenga esattamente quel che è necessario per rendere veri tutti gli assiomi della teoria degli insiemi che abbiamo visto nel capitolo precedente ma che non contenga nessun insieme con infiniti elementi. A tal fine possiamo dare la seguente definizione induttiva

$$\begin{aligned} V_0 &= \emptyset \\ V_{n+1} &= \mathcal{P}(V_n) \end{aligned}$$

e considerare l'insieme V che otteniamo come unione di tutti gli insiemi V_n al variare di n nei numeri naturali.

V contiene allora tutti i possibili sottoinsiemi finiti che possiamo ottenere con le operazioni insiemistiche richieste dagli assiomi dell'insieme vuoto, della coppia, dell'unione e dell'insieme potenza. Infatti

- (insieme vuoto) $\emptyset \in V$ perché $\emptyset \in V_1$,
- (coppia) se $x, y \in V$ allora, per qualche n e m, $x \in V_n$ e $y \in V_m$, ma possiamo supporre senza perdere di generalità che $n \leq m$ e quindi si può immediatamente dedurne che $V_n \subseteq V_m$ (esercizio!); perciò $x, y \in V_m$ e quindi $\{x, y\} \in V_{m+1} \subseteq V$,
- (unione) Se $x \in V$ allora per qualche n, $x \in V_n$ e quindi gli elementi di x stanno in V_{n-1} e i loro elementi in V_{n-2}; $\bigcup x$ è perciò un elemento di V_{n-1}, visto che è un sottoinsieme di V_{n-2}, e quindi anche di V.
- (potenza) se $x \in V$ allora $x \in V_n$ per qualche n, quindi tutti gli elementi di x stanno in V_{n-1}, tutti i sottoinsiemi di x stanno in V_n e perciò $\mathcal{P}(x) \in V_{n+1} \subseteq V$.

Tuttavia V non contiene nessun insieme con infiniti elementi visto che la cardinalità di V_0 è 0 e la cardinalità di V_{n+1} è $2^{|V_n|}$.

È facile dimostrare per induzione che ogni insieme V_n è *transitivo*, cioè ogni elemento x di V_n è anche un sottoinsieme di V_n (e quindi x è anche un elemento di V_{n+1}), e che la sequenza è *crescente*,

cioè $V_n \in V_{n+1}$. Per esempio abbiamo che

$$\begin{array}{lcl} V_0 & = & \emptyset \\ V_1 & = & \{\emptyset\} \\ V_2 & = & \{\emptyset, \{\emptyset\}\} \\ V_3 & = & \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\} \\ \ldots & & \end{array}$$

Definizione 3.0.1 *Gli insiemi* ereditariamente finiti *sono i membri di* V.

$(V, \in)$ soddisfa a tutti gli assiomi di $\mathsf{ZFC_{fin}}$, cioè *estensionalità*, *insieme vuoto*, *coppia*, *unione*, *potenza* e *separazione* (in symbols, $(V, \in) \vDash \mathsf{ZFC_{fin}}$). Possiamo quindi dire che la *matematica finitaria* è quella che si può sviluppare all'interno di $\mathsf{ZFC_{fin}}$; ad esempio tutti i numeri naturali si possono definire all'inteno di $\mathsf{ZFC_{fin}}$.

Vedremo nella prossime lezioni che la teoria degli insiemi che otteniamo escludendo gli insiemi infiniti è comunque ricca ed interessante visto che coincide sostanzialmente con quel che si può fare in una teoria dei numeri naturali.

3.1 L'interpretazione di PA in $\mathsf{ZFC_{fin}}$

Il difetto di $\mathsf{ZFC_{fin}}$ è che è una teoria poco conveniente per trattare di numeri naturali anche se essi si possono definire al suo interno. Ad ogni modo possiamo procurarci facilmente una teoria più adatta a questo scopo: si tratta di una piccola estensione dell'*aritmetica di Peano* (abbreviato in PA^+).

Dal punto di vista formale il linguaggio con cui si esprime PA^+ utilizza i simboli $\{0, \mathsf{s}, +, \times, \mathsf{exp}\}$ dove 0 è la costante *zero*, s è la funzione *successore* $\mathsf{s}(n) = n+1$, $+$ la funzione *somma*, $\times$ la funzione *prodotto* e exp la funzione *esponenziale*.

Definizione 3.1.1 (Aritmetica di Peano) PA^+ *è la teoria nel linguaggio* $\{0, \mathsf{s}, +, \times, \mathsf{exp}\}$ *con i seguenti assiomi*

1. $\forall x(\mathsf{s}(x) \neq 0)$.
2. $\forall x \forall y(\mathsf{s}(x) = \mathsf{s}(y) \to x = y)$.
3. $\forall x(x + 0 = x)$.
4. $\forall x \forall y(x + \mathsf{s}(y) = \mathsf{s}(x + y))$.
5. $\forall x(x \times 0 = 0)$.
6. $\forall x \forall y(x \times \mathsf{s}(y) = (x \times y) + x)$.
7. $\forall x(\mathsf{exp}(x, 0) = \mathsf{s}(0))$.
8. $\forall x \forall y(\mathsf{exp}(x, \mathsf{s}(y)) = \mathsf{exp}(x, y) \times x)$.
9. *(Induzione): per ogni formula* $\phi(x, \overline{y})$*:*

$$\forall \overline{y}((\phi(0, \overline{y}) \wedge \forall x(\phi(x, \overline{y}) \to \phi(\mathsf{s}(x), \overline{y}))) \to \forall x \phi(x, \overline{y})).$$

Non è ora difficile accorgersi che possiamo interpretare validamente PA^+ in $\mathsf{ZFC_{fin}}$. A tal fine basta infatti interpretare 0 in $\emptyset$ e il simbolo s nella funzione *successore* tra insiemi finiti S che associa ad un insieme finito x l'insieme $x \cup \{x\}$ sulla falsariga di quel che abbiamo visto nella sezione 2.2.4 dove abbiamo definito i numeri naturali all'interno degli insiemi. Inoltre il segno $+$ può essere interpretato in una qualsiasi funzione $+$ tra insiemi tale che

$$\begin{array}{lcl} x + \emptyset & = & x \\ x + \mathsf{S}(y) & = & \mathsf{S}(x + y) \end{array}$$

il segno $\times$ può essere interpretato in una qualsiasi funzione $\times$ tra insiemi finiti tale che

$$\begin{array}{lcl} x \times \emptyset & = & \emptyset \\ x \times \mathsf{S}(y) & = & (x \times y) + x \end{array}$$

mentre il segno exp può essere interpretato in una funzione exp tra insiemi finiti tale che

$$\begin{array}{lcl} \mathsf{exp}(x, \emptyset) & = & \{\emptyset\} \\ \mathsf{exp}(x, \mathsf{S}(y)) & = & \mathsf{exp}(x, y) \times x \end{array}$$

(notate che se restringiamo le funzioni $+$, $\times$ e exp ai soli *numeri naturali* allora quelle viste sopra possono essere considerate come le definizioni induttive di tali funzioni e si può dimostrare che esiste una sola funzione che soddisfa tali definizioni induttive).

Mentre i primi sei assiomi di PA^+ sono ovviamente validi in $\mathsf{ZFC_{fin}}$ con questa interpretazione, la dimostrazione del principio di induzione richiede qualche parola in più. Un modo per vedere che esso vale è quello di notare che ogni insieme non vuoto di *numeri naturali* ha un minimo elemento rispetto alla relazione d'ordine che sancisce che $n < m$ se e solo se $n \in m$. Infatti l'assioma di regolarità ci assicura che se X è un insieme non vuoto di *numeri naturali* allora esiste un suo elemento n tale che $n \cap X = \emptyset$, ma $n = \{0, 1, \ldots, n-1\}$ e quindi questo significa che $0 \notin X$, $\ldots$, $n-1 \notin X$, cioè n è il minimo elemento di X.

È ora un esercizio standard quello di ricavare la validità della proprietà di induzione a partire dal principio del minimo (sia X l'insieme dei *numeri naturali* che non soddisfano la proprietà P, se tale insieme non è vuoto allora ha minimo ma questo è impossibile visto che tale minimo non può essere 0 perché $P(0)$ vale e non può essere $n+1$ perché $P(n)$ implica $P(n+1)$; esercizio: dimostrare che vale anche l'altra implicazione).

Naturalmente questa dimostrazione funziona solo per quegli insiemi che sono fatti di *numeri naturali* e quindi non possiamo dire di aver dimostrato la validità della traduzione del principio di induzione senza modifiche quanto piuttosto la validità della formula seguente

$$\phi(\emptyset) \wedge \forall x(\mathsf{Nat}(x) \to (\phi(x) \to \phi(x \cup \{x\}))) \to \forall x(\mathsf{Nat}(x) \to \phi(x))$$

dove spponiamo per un momento di sapere come caratterizzare gi insieme che sono "numeri naturali" dentre V.

Sotto questa ipotesi possiamo allora dire che presa una qualunque formula ϕ nel linguaggio di PA^+ possiamo trasformarla in una formula di $\mathsf{ZFC_{fin}}$ in modo tale che se ϕ è un teorema di PA^+ la sua *traduzione* ϕ^* vale in $\mathsf{ZFC_{fin}}$ dove stiamo pensando di tradurre ϕ come segue

$$\begin{array}{lcl} (s = t)^* & \equiv & s^* = t^* \\ (\phi \wedge \psi)^* & \equiv & \phi^* \wedge \psi^* \\ (\phi \vee \psi)^* & \equiv & \phi^* \vee \psi^* \\ (\phi \to \psi)^* & \equiv & \phi^* \to \psi^* \\ (\neg\psi)^* & \equiv & \neg\psi^* \\ (\forall x\ \phi)^* & \equiv & \forall x(\mathsf{Nat}(x) \to \phi^*) \\ (\exists x\ \phi)^* & \equiv & \exists x(\mathsf{Nat}(x) \wedge \phi^*) \end{array}$$

Naturalmente affinché tutto funzioni bisogna capire come definire la formula Nat.

L'idea è quella di dire che i numeri naturali presenti in V sono tutti e soli gli insiemi *transitivi*, tali cioè da godere della seguente proprietà

$$\mathsf{Trans}(x) \equiv \forall y(y \in x \to y \subseteq x)(\equiv \forall z \forall y((z \in y \wedge y \in x) \to z \in x))$$

e *connessi*, cioè per cui valga la seguente proprietà

$$\mathsf{Conn}(x) \equiv \forall y \forall z((y \in x \wedge z \in x) \to (y \in z \vee z \in y \vee y = z))$$

Possiamo allora porre:

$$\mathsf{Nat}(x) \equiv \mathsf{Trans}(x) \wedge \mathsf{Conn}(x)$$

Naturalmente adesso sarà necessario dimostrare la correttezza della nostra intuizione: vogliamo cioè dimostrare che tutti i numeri naturali sono insiemi transitivi e connessi e, viceversa, che tutti gli insiemi transitivi e connessi delluniverso V sono numeri naturali.

Enunciamo preliminarmente la seguente proposizione.

Proposizione 3.1.2 *Sia $x \in V$ un insieme transitivo e connesso. Allora si ha che, se y è elemento di x, anche y è transitivo e connesso.*

Dimostrazione. Vediamo prima di tutto che vale $\mathsf{Trans}(y)$. Siano z e w tali che $z \in w \in y$. Per la tansitività di x si ha che $w \in x$ da cui, sempre per la transitività di x, segue che $z \in x$. Ora, per la connessione di x, si ha che $z \in y$ oppure $y \in z$ oppure $z = y$, ma $y \in z$ e $z = y$ sono entrambi da escludere per l'assioma di fondazione, per cui si ha necessariamente $z \in y$.

Dimostraiamo ora $\mathsf{Conn}(y)$. Se z e w sono elementi di y allora, per la transitività di x, essi sono anche elementi di x e sfruttando la connessione di x concludiamo che $z \in w$ oppure $w \in z$ oppure $z = w$.

Siamo ora pronti a dimostrare il seguente teorema.

Teorema 3.1.3 *Gli insiemi transitivi e connessi di V sono tutti e soli i numeri naturali.*

Dimostrazione. Il fatto che ogni numero naturale sia transitivo e connesso si può dimostrare per induzione.

Infatti $\emptyset$ è banalmente transitivo e connesso.

Consideriamo ora un qualunque numero naturale x tale che $x = y \cup \{y\}$ per qualche numero naturale y. Allora, per ipotesi induttiva, possiamo supporre che y sia transitivo e connesso. Sia ora $z \in x$ e $w \in z$. Allora $z \in y$ o $z = y$; ma se $z \in y$ allora per la transitività di y segue che $w \in y$ e quindi si deduce che $w \in x$, se invece $z = y$ allora chiaramente $w \in x$.

Anche la connessione di x si può dimostrare per induzione. $\mathsf{Conn}(\emptyset)$ ovviamente vale. Supponiamo ora che $x = y \cup \{y\}$ per qualche numero naturale y e che $z \in x$ e $w \in x$. Quindi o $z \in y$ e $w \in y$, e allora $z \in w$ o $w \in z$ o $w = z$ segue per ipotesi induttiva, o $z \in y$ e $w = y$, e allora $z \in w$, o $w \in y$ e $z = y$, e allora $w \in z$, o $z = y$ e $w = y$ e allora $z = w$.

Per dimostrare l'altra implicazione, cioè che un insieme x transitivo e connesso è un numero naturale, bisogna dimostrare che $x = \emptyset$ oppure che $x = y \cup \{y\}$ per qualche numero naturale y. Supponiamo quindi che x non sia vuoto e supponiamo che z e w siano due elementi di x massimali rispetto alla relazione di appartenenza; allora, a causa della connessione di x, otteniamo che $z = w$ visto che dobbiamo escludere sia $z \in w$ che $w \in z$ a causa della massimalità di z e w. Ma il numero di elementi in x è finito e quindi c'è un unico elemento massimale y rispetto alla relazione di appartenenza (ovviamente, in virtù della precedente proposizione 3.1.2, y è a sua volta transitivo e connesso in quanto elemento di x e quindi numero naturale per ipotesi induttiva sulla complessità dell'insieme rispetto alla relazione di appartenenza). Vediamo allora che $x = y \cup \{y\}$. Infatti se $z \in x$ allora, per la connessione di x, otteniamo che $z \in y \vee y \in z \vee z = y$, ma per la massimalità di y dobbiamo escludere che $y \in z$ e quindi abbiamo che $z \in y \cup \{y\}$; d'altra parte se $z \in y \cup \{y\}$ allora $z \in y$, e in questo caso $z \in x$ per la transitività di x, o $z = y$ e quindi $z \in x$ visto che $y \in x$.

3.2 L'interpretazione di $\mathsf{ZFC_{fin}}$ in PA

La cosa forse inaspettata è che c'è una traduzione che funziona anche nell'altra direzione: il problema sta naturalmente nel fatto che in $\mathsf{ZFC_{fin}}$ ci sono molti più insiemi finiti che *numeri naturali* e quindi è necessario inventarsi una traduzione che codifichi ogni insieme finito in un numero naturale in modo da poter definire una formula $B(x, y)$ di PA che codifichi la relazione di appartenenza dell'insieme codificato dal numero naturale x all'insieme codificato dal numero naturale y.

Un modo per ottenere questo risultato è quello di considerare l'espressione binaria del numero naturale y come la codifica dell'insieme finito i cui elementi sono gli insiemi finiti codificati dai numeri naturali x tali che al posto x nell'espressione binaria di y ci sia un 1. Formalmente, questo significa che possiamo definire una mappa ϕ dai numeri naturali agli insiemi finiti ponendo

$$\phi(n) \equiv \{\phi(k) \mid \text{il coefficiente di posto } k \text{ nell'espressione binaria di } n \text{ è uguale a } 1\}$$

Ad esempio la rappresentazione binaria di 21 è 10101_B e quindi 21 rappresenta l'insieme finito i cui elementi sono gli insiemi finiti rappresentati dai numeri naturali 0, 2 e 4; a sua volta $0 \equiv 0_B$ rappresenta l'insieme vuoto, $2 \equiv 10_B$ rappresenta l'insieme il cui unico elemento è l'insieme $\{\emptyset\}$

rappresentato dal numero $1 \equiv 1_B$ e $4 \equiv 100_B$ rappresenta l'insieme il cui unico elemento è l'insieme $\{\{\emptyset\}\}$ rappresentato dal numero 2. Quindi 21 rappresenta l'insieme $\{\emptyset, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\}$.

Se definiamo

$$B(x, y) \equiv \text{“al posto } x \text{ nella espressione binaria di } y \text{ c'è un 1”}$$

allora la definizione precedente diventa

$$\phi(n) \equiv \{\phi(k) \mid B(k, n)\}$$

In questa definizione il predicato $B(x, y)$ è quindi la controparte aritmetica, espressa cioè utilizzando i numeri naturali, della relazione di appartenenza tra insieme finiti. La cosa interessante è che, dal punto di vista teorico il predicato $B(x, y)$, al pari di qualsiasi altra relazione tra numeri naturali definibile per ricorsione primitiva, si può esprimere in PA^+; di fatto non è troppo difficile definire direttamente questa relazione utilizzando solo somme, prodotti ed esponenti.

Infatti $B(x, y)$ vale se e solo se dividendo y per 2^x otteniamo un numero dispari (dimostrarlo!) e quindi possiamo esprimere $B(x, y)$ in PA^+ ponendo

$$B(x, y) \equiv \exists z(\mathsf{div}(y, \mathsf{exp}(2, x), z) \wedge \mathsf{dispari}(z))$$

dove $\mathsf{div}(y, w, z)$ esprime il fatto che z è il risultato della divisione intera di y per w e si può esprimere in PA^+ ponendo

$$\mathsf{div}(y, w, z) \equiv (w \times z \leq y) \wedge (y < w \times \mathsf{s}(z))$$

e $\mathsf{dispari}(z)$ esprime il fatto che z è un numero dispari e si può definire ponendo

$$\mathsf{dispari}(z) \equiv \exists w\ (z = \mathsf{s}(\mathsf{s}(0)) \times w + \mathsf{s}(0))$$

(naturalmente stiamo supponendo che $s \leq t \equiv \exists w\ (s + w = t)$ e che $s < t \equiv \exists w\ (w \neq 0 \wedge s + w = t)$)

È ora ovvio che la mappa ϕ è iniettiva visto che la rappresentazione binaria di un numero naturale è univoca e che due insiemi sono uguali quando hanno gli stessi elementi.

Un po' meno immediato è vedere che la mappa ϕ è anche suriettiva, cioè che ogni insieme finito in $V = \bigcup_{n \in \mathsf{Nat}} V_n$ è immagine di qualche numero naturale. Visto però che gli elementi di V sono insieme finiti i cui elementi sono a loro volta insieme finiti possiamo trovare un numero naturale $\mathsf{cod}(x)$ tale che $\phi(\mathsf{cod}(x)) = x$ per ogni insieme $x \in V$ ponendo

$$\begin{cases} \mathsf{cod}(\emptyset) & = & 0 \\ \mathsf{cod}(x) & = & \Sigma_{y \in x} 2^{\mathsf{cod}(y)} \end{cases}$$

Quindi ogni formula di $\mathsf{ZFC_{fin}}$ si può trasformare in una formula di PA sostituendo ogni occorrenza della relazione di appartenenza $\in$ con una occorrenza del predicato $B(-, -)$ e ogni insieme finito con il numero naturale che lo codifica.

È allora chiaro che così facendo ogni assioma di $\mathsf{ZFC_{fin}}$ diventa un teorema di PA (questo è un lungo esercizio da dimostrare!) e quindi possiamo sviluppare in PA esattamente la stessa matematica che potevamo sviluppare in $\mathsf{ZFC_{fin}}$. Infatti l'*assioma dell'insieme vuoto* diventa

$$\exists n. \forall m. \neg B(m, n)$$

che chiaramente vale visto che PA è in grado di dimostrare che $\neg B(0, m)$ vale per ogni numero naturale m.

Inoltre l'*assioma della coppia* diventa

$$\forall m. \forall k. \exists n. \forall w. (B(w, n) \equiv w = m \vee w = k)$$

che possiamo dimostrare in PA ponendo $n = 2^m + 2^k$ se $m \neq k$ and $n = 2^m$ se $m = k$.

Anche la traduzione dell'*assioma dell'unione*

$$\forall m. \exists n. \forall w. (B(w, n) \equiv \exists v. B(w, v) \wedge B(v, m))$$

si può dimostrare in PA; infatti basta porre ...

Infine l'assioma della potenza diventa

$$\forall m.\exists n.\forall w.B(w,n) \equiv (\forall z.B(z,w) \rightarrow B(z,m))$$

che si dimostra in PA ponendo $n =$??? ...

Se mettiamo quindi insieme quel che abbiamo detto in questo paragrafo con quanto detto nel paragrafo precedente abbiamo visto che la teoria degli insiemi finiti altro non è che la teoria dei numeri naturali, un campo di studio sicuramente vasto ed interessante (la si può vedere come la matematica che si può sviluppare avendo a disposizione l'*infinito potenziale* invece dell'*infinito attuale* o se preferite l'illimitato invece dell'infinito).

Capitolo 4

Introduzione agli ordinali

Nel precedente capitolo abbiamo visto che pur limitandosi a $\mathsf{ZFC}_{\mathsf{fin}}$ di matematica possiamo farne molta e in particolare possiamo fare tutta la matematica che serve davvero per una qualsiasi applicazione (l'infinito attuale anche se necessario per trattare con oggetti matematici quali i numeri reali non sembra proprio necessario nella vita reale). Possiamo allora chiederci perché dovremmo desiderare di avere a disposizione l'assioma dell'infinito.

Vediamo cosa si può fare avendo a disposizione insiemi infiniti. La prima importante conseguenza è il fatto che i numeri naturali sono riconosciuti come insieme. L'assioma dell'infinito ci assicura infatti sull'esistenza di (almeno) un insieme contenente l'insieme vuoto e chiuso per l'operazione di successore che associa ad un insieme X l'insieme $X \cup \{X\}$. Possiamo allora definire i numeri naturali come la collezione degli elementi comuni a tutti gli insiemi che godono di tali proprietà e riconoscere che tale collezione è un insieme visto che è un sottoinsieme di un qualche insieme, anzi è proprio l'insieme che otteniamo facendo l'intersezione di tutti questi insiemi.

Ed essere i numeri naturali un insieme permette di utilizzare su di essi le operazioni insiemistiche.

Questo permette ad esempio di costruire l'insieme dei sottoinsiemi dei naturali e tutta una catena di insiemi che il teorema di Cantor ci assicura essere sempre più grandi senza fine (la situazione è quindi molto diversa rispetto al caso in cui non ci sia l'assioma dell'infinito dove la catena dei V_n che abbiamo visto nel capitolo precedente è tutto quello che ci serve).

Ma anche senza muoverci verso insiemi sempre più grandi possiamo comunque produrre nuovi insiemi che continuano ad essere numerabili e che si distinguono tra loro per il modo in cui sono ordinati i loro elementi. Ad esempio se indichiamo con $\omega = \{0, 1, 2, \ldots\}$ l'insieme dei numeri naturali abbiamo il diritto di definire il successore di ω e in tal modo di ottenere nuovi insiemi infiniti.

Se andiamo avanti per questa strada otteniamo quelli che si chiamano gli ordinali che possiamo trovare descritti con molto maggior dettaglio nei prossimi paragrafi.

4.1 Order type

Quanto segue è preso da

`http://en.wikipedia.org/wiki/Order_type`

In mathematics, especially in set theory, two ordered sets X, Y are said to have the same order type just when they are order isomorphic, that is, when there exists a bijection $f : X \to Y$ such that both f and its inverse are monotone (order preserving). (In the special case when X is totally ordered, monotonicity of f implies monotonicity of its inverse.)

For example, the set of integers and the set of even integers have the same order type, because the mapping sending n in $2n$ preserves the order. But the set of integers and the set of rational numbers (with the standard ordering) are not order isomorphic, because, even though the sets are of the same size (they are both countably infinite), there is no order-preserving bijective mapping between them. To these two order types we may add two more: the set of positive integers (which

has a least element), and that of negative integers (which has a greatest element). The open interval $(0, 1)$ of rationals is order isomorphic to the rationals (since

$$y = \frac{2x - 1}{1 - \mid 2x - 1 \mid}$$

provides a monotone bijection from the former to the latter); the half-closed intervals $[0, 1)$ and $(0, 1]$, and the closed interval $[0, 1]$, are three additional order type examples. Since order-equivalence is an equivalence relation, it partitions the class of all ordered sets into equivalence classes.

4.1.1 Order type of well-orderings

Every well-ordered set is order-equivalent to exactly one ordinal number. The ordinal numbers are taken to be the canonical representatives of their classes, and so the order type of a well-ordered set is usually identified with the corresponding ordinal. For example, the order type of the natural numbers is ω.

The order type of a well-ordered set V is sometimes expressed as $\mathsf{ord}(V)$

For example, consider the set of even ordinals less than $\omega \cdot 2 + 7$, which is:

$$V = \{0, 2, 4, 6, ...; \omega, \omega + 2, \omega + 4, ...; \omega \cdot 2, \omega \cdot 2 + 2, \omega \cdot 2 + 4, \omega \cdot 2 + 6\}.$$

Its order type is:

$$\mathsf{ord}(V) = \omega \cdot 2 + 4 = \{0, 1, 2, 3, ...; \omega, \omega + 1, \omega + 2, ...; \omega \cdot 2, \omega \cdot 2 + 1, \omega \cdot 2 + 2, \omega \cdot 2 + 3\}.$$

Because there are 2 separate lists of counting and 4 in sequence at the end.

4.2 Ordinal number

Quanto segue è preso da

`http://en.wikipedia.org/wiki/Ordinal_numbers`

In set theory, an ordinal number, or just ordinal, is the order type of a well-ordered set. They are usually identified with hereditarily transitive sets. Ordinals are an extension of the natural numbers different from integers and from cardinals. Like other kinds of numbers, ordinals can be added, multiplied, and exponentiated. Ordinals were introduced by Georg Cantor in 1883 to accommodate infinite sequences and to classify sets with certain kinds of order structures on them.[1] He discovered them by accident while working on a problem concerning trigonometric series -see Georg Cantor.

The finite ordinals (and the finite cardinals) are the natural numbers: 0, 1, 2, ..., since any two total orderings of a finite set are order isomorphic. The least infinite ordinal is ω, which is identified with the cardinal number $\aleph_0$. However in the transfinite case, beyond ω, ordinals draw a finer distinction than cardinals on account of their order information. Whereas there is only one countably infinite cardinal, namely itself, there are uncountably many countably infinite ordinals, namely

$$\omega, \omega + 1, \omega + 2, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \ldots, \omega^2, \ldots, \omega^3, \ldots, \omega^\omega, \ldots, \omega^{\omega^\omega}, \ldots, \epsilon_0, \ldots.$$

Here addition and multiplication are not commutative: in particular $1+\omega$ is ω rather than $\omega+1$ and likewise, $2\cdot\omega$ is ω rather than $\omega\cdot2$. The set of all countable ordinals constitutes the first uncountable ordinal ω_1, which is identified with the cardinal $\aleph_1$ (next cardinal after $\aleph_0$). Well-ordered cardinals are identified with their initial ordinals, i.e. the smallest ordinal of that cardinality. The cardinality of an ordinal defines a many to one association from ordinals to cardinals.

In general, each ordinal α, is the *order type of the set of ordinals* strictly less than the ordinal, α itself. This property permits every ordinal to be represented as the set of all ordinals less than it. Ordinals may be categorized as: zero, successor ordinals, and limit ordinals (of various cofinalities). Given a class of ordinals, one can identify the α-th member of that class, i.e. one can index (count)

them. Such a class is closed and unbounded if its indexing function is continuous and never stops. The Cantor normal form uniquely represents each ordinal as a finite sum of ordinal powers of ω. However, this cannot form the basis of a universal ordinal notation due to such self-referential representations as $\epsilon_0 = \omega^{\epsilon_0}$. Larger and larger ordinals can be defined, but they become more and more difficult to describe. Any ordinal number can be made into a topological space by endowing it with the order topology; this topology is discrete if and only if the ordinal is a countable cardinal, i.e. at most ω. A subset of $\omega + 1$ is open in the order topology if and only if either it is cofinite or it does not contain ω as an element.

4.2.1 Ordinals extend the natural numbers

A natural number (which, in this context, includes the number 0) can be used for two purposes: to describe the size of a set, or to describe the position of an element in a sequence. When restricted to finite sets these two concepts coincide; there is only one way to put a finite set into a linear sequence, up to isomorphism. When dealing with infinite sets one has to distinguish between the notion of size, which leads to cardinal numbers, and the notion of position, which is generalized by the ordinal numbers described here. This is because, while any set has only one size (its cardinality), there are many non-isomorphic well-orderings of any infinite set, as explained below.

Whereas the notion of cardinal number is associated with a set with no particular structure on it, the ordinals are intimately linked with the special kind of sets that are called well-ordered (so intimately linked, in fact, that some mathematicians make no distinction between the two concepts). A well-ordered set is a totally ordered set (given any two elements one defines a smaller and a larger one in a coherent way) in which there is no infinite decreasing sequence (however, there may be infinite increasing sequences); equivalently, every non-empty subset of the set has a least element. Ordinals may be used to label the elements of any given well-ordered set (the smallest element being labelled 0, the one after that 1, the next one 2, "and so on") and to measure the "length" of the whole set by the least ordinal that is not a label for an element of the set. This "length" is called the order type of the set.

Any ordinal is defined by the set of ordinals that precede it: in fact, the most common definition of ordinals identifies each ordinal as the set of ordinals that precede it. For example, the ordinal 42 is the order type of the ordinals less than it, i.e., the ordinals from 0 (the smallest of all ordinals) to 41 (the immediate predecessor of 42), and it is generally identified as the set $\{0, 1, 2, \ldots, 41\}$. Conversely, any set S of ordinals that is downward-closed – meaning that for any ordinal α in S and any ordinal $\beta < \alpha$, β is also in the set – is (or can be identified with) an ordinal.

So far we have mentioned only finite ordinals, which are the natural numbers. But there are infinite ones as well: the smallest infinite ordinal is ω, which is the order type of the natural numbers (finite ordinals) and that can even be identified with the set of natural numbers (indeed, the set of natural numbers is well-ordered – as is any set of ordinals – and since it is downward closed it can be identified with the ordinal associated with it, which is exactly how we define ω).

Perhaps a clearer intuition of ordinals can be formed by examining a first few of them: as mentioned above, they start with the natural numbers, 0, 1, 2, 3, 4, 5, ... After *all* natural numbers comes the first infinite ordinal, ω, and after that come $\omega+1$, $\omega+2$, $\omega+3$, and so on. (Exactly what addition means will be defined later on: just consider them as names.) After all of these come $\omega \cdot 2$ (which is $\omega + \omega$), $\omega \cdot 2 + 1$, $\omega \cdot 2 + 2$, and so on, then $\omega \cdot 3$, and then later on $\omega \cdot 4$. Now the set of ordinals we form in this way (the $\omega \cdot m + n$, where m and n are natural numbers) must itself have an ordinal associated with it: and that is ω^2. Further on, there will be ω^3, then ω^4, and so on, and ω^ω, then ω^{ω^2}, and much later on ϵ_0 (epsilon nought) (to give a few examples of relatively small-countable-ordinals). We can go on in this way indefinitely far ("indefinitely far" is exactly what ordinals are good at: basically every time one says "and so on" when enumerating ordinals, it defines a larger ordinal). The smallest uncountable ordinal is the set of all countable ordinals, expressed as ω_1.

4.2.2 Definitions

Well-ordered sets

In a well-ordered set, every non-empty subset has a smallest element. Given the axiom of dependent choice, this is equivalent to just saying that the set is totally ordered and there is no infinite decreasing sequence, something perhaps easier to visualize. In practice, the importance of well-ordering is justified by the possibility of applying transfinite induction, which says, essentially, that any property that passes on from the predecessors of an element to that element itself must be true of all elements (of the given well-ordered set). If the states of a computation (computer program or game) can be well-ordered in such a way that each step is followed by a "lower" step, then you can be sure that the computation will terminate.

Now we don't want to distinguish between two well-ordered sets if they only differ in the "labeling of their elements", or more formally: if we can pair off the elements of the first set with the elements of the second set such that if one element is smaller than another in the first set, then the partner of the first element is smaller than the partner of the second element in the second set, and vice versa. Such a one-to-one correspondence is called an *order isomorphism* and the two well-ordered sets are said to be order-isomorphic, or similar (obviously this is an equivalence relation). Provided there exists an order isomorphism between two well-ordered sets, the order isomorphism is unique: this makes it quite justifiable to consider the two sets as essentially identical, and to seek a "canonical" representative of the isomorphism type (class). This is exactly what the ordinals provide, and it also provides a canonical labeling of the elements of any well-ordered set.

So we essentially wish to define an ordinal as an isomorphism class of well-ordered sets: that is, as an equivalence class for the equivalence relation of "being order-isomorphic". There is a technical difficulty involved, however, in the fact that the equivalence class is too large to be a set in the usual ZermeloFraenkel (ZF) formalization of set theory. But this is not a serious difficulty. We will say that the ordinal is the order type of any set in the class.

Definition of an ordinal as an equivalence class

The original definition of ordinal number, found for example in *Principia Mathematica*, defines the order type of a well-ordering as the set of all well-orderings similar (order-isomorphic) to that well-ordering: in other words, an ordinal number is genuinely an equivalence class of well-ordered sets. This definition must be abandoned in ZF and related systems of axiomatic set theory because these equivalence classes are too large to form a set. However, this definition still can be used in type theory and in Quine's set theory New Foundations and related systems (where it affords a rather surprising alternative solution to the Burali-Forti paradox of the largest ordinal).

Von Neumann definition of ordinals

Rather than defining an ordinal as an equivalence class of well-ordered sets, we will define it as a particular well-ordered set that (canonically) represents the class. Thus, an ordinal number will be a well-ordered set; and every well-ordered set will be order-isomorphic to exactly one ordinal number.

The standard definition, suggested by John von Neumann, is: each ordinal is the well-ordered set of all smaller ordinals. In symbols, $\lambda = [0, \lambda)$.[2] Formally:

A set S is an ordinal if and only if S is strictly well-ordered with respect to set membership and every element of S is also a subset of S

Note that the natural numbers are ordinals by this definition. For instance, 2 is an element of $4 = \{0, 1, 2, 3\}$, and 2 is equal to $\{0, 1\}$ and so it is a subset of $\{0, 1, 2, 3\}$.

It can be shown by transfinite induction that every well-ordered set is order-isomorphic to exactly one of these ordinals, that is, there is an order preserving bijective function between them.

Furthermore, the elements of every ordinal are ordinals themselves. Whenever you have two ordinals S and T, S is an element of T if and only if S is a proper subset of T. Moreover, either S is an element of T, or T is an element of S, or they are equal. So every set of ordinals is totally ordered. Further, every set of ordinals is well-ordered. This generalizes the fact that every set of natural numbers is well-ordered.

Consequently, every ordinal S is a set having as elements precisely the ordinals smaller than S. For example, every set of ordinals has a supremum, the ordinal obtained by taking the union of all the ordinals in the set. This union exists regardless of the set's size, by the axiom of union.

The class of all ordinals is not a set. If it were a set, one could show that it was an ordinal and thus a member of itself, which would contradict its strict ordering by membership. This is the Burali-Forti paradox. The class of all ordinals is variously called Ord, ON, or ∞.

An ordinal is finite if and only if the opposite order is also well-ordered, which is the case if and only if each of its subsets has a maximum.

4.2.3 Transfinite sequence

If α is a limit ordinal and X is a set, an α-indexed sequence of elements of X is a function from α to X. This concept, a transfinite sequence or ordinal-indexed sequence, is a generalization of the concept of a sequence. An ordinary sequence corresponds to the case $\alpha \equiv \omega$.

4.2.4 Transfinite induction

What is transfinite induction?

Transfinite induction holds in any well-ordered set, but it is so important in relation to ordinals that it is worth restating here. Any property that passes from the set of ordinals smaller than a given ordinal α to α itself, is true of all ordinals. That is, if $P(\alpha)$ is true whenever $P(\beta)$ is true for all $\beta < \alpha$, then $P(\alpha)$ is true for all α. Or, more practically: in order to prove a property P for all ordinals α, one can assume that it is already known for all smaller $\beta < \alpha$.

Transfinite recursion

Transfinite induction can be used not only to prove things, but also to define them. Such a definition is normally said to be by *transfinite recursion* – the proof that the result is well-defined uses transfinite induction. Let F denote a (class) function F to be defined on the ordinals. The idea now is that, in defining $F(\alpha)$ for an unspecified ordinal α, one may assume that $F(\beta)$ is already defined for all $\beta < \alpha$ and thus give a formula for $F(\alpha)$ in terms of these $F(\beta)$. It then follows by transfinite induction that there is one and only one function satisfying the recursion formula up to and including α.

Here is an example of definition by transfinite recursion on the ordinals (more will be given later): define function F by letting $F(\alpha)$ be the smallest ordinal not in the class $\{F(\beta) \mid \beta < \alpha\}$, that is, the class consisting of all $F(\beta)$ for $\beta < \alpha$. This definition assumes the $F(\beta)$ known in the very process of defining F; this apparent vicious circle is exactly what definition by transfinite recursion permits. In fact, $F(0)$ makes sense since there is no ordinal $\beta < 0$, and the class $\{F(\beta) \mid \beta < 0\}$ is empty. So $F(0)$ is equal to 0 (the smallest ordinal of all). Now that $F(0)$ is known, the definition applied to $F(1)$ makes sense (it is the smallest ordinal not in the singleton class $\{F(0)\} = \{0\}$), and so on (the and so on is exactly transfinite induction). It turns out that this example is not very exciting, since provably $F(\alpha) = \alpha$ for all ordinals α, which can be shown, precisely, by transfinite induction.

Successor and limit ordinals

Any nonzero ordinal has the minimum element, zero. It may or may not have a maximum element. For example, 42 has maximum 41 and $\omega + 6$ has maximum $\omega + 5$. On the other hand, ω does not have a maximum since there is no largest natural number. If an ordinal has a maximum α, then it is the next ordinal after α, and it is called a *successor ordinal*, namely the successor of α, written α+1. In the von Neumann definition of ordinals, the successor of α is $\alpha \cup \{\alpha\}$ since its elements are those of α and α itself.

A nonzero ordinal that is not a successor is called a limit ordinal. One justification for this term is that a limit ordinal is indeed the limit in a topological sense of all smaller ordinals (under the order topology).

When $\langle \alpha_\iota \mid \iota < \gamma \rangle$ is an ordinal-indexed sequence, indexed by a limit γ and the sequence is increasing, i.e. $\alpha_\iota < \alpha_\rho$ whenever $\iota < \rho$ we define its limit to be the least upper bound of the set that is, the smallest ordinal (it always exists) greater than any term of the sequence. In this sense, a limit ordinal is the limit of all smaller ordinals (indexed by itself). Put more directly, it is the supremum of the set of smaller ordinals.

Another way of defining a limit ordinal is to say that α is a limit ordinal if and only if: There is an ordinal less than α and whenever ζ is an ordinal less than α, then there exists an ordinal ξ such that $\zeta < \xi < \alpha$.

So in the following sequence:

$$0, 1, 2, ..., \omega, \omega + 1$$

ω is a limit ordinal because for any smaller ordinal (in this example, a natural number) we can find another ordinal (natural number) larger than it, but still less than ω.

Thus, every ordinal is either zero, or a successor (of a well-defined predecessor), or a limit. This distinction is important, because many definitions by transfinite induction rely upon it. Very often, when defining a function F by transfinite induction on all ordinals, one defines $F(0)$, and $F(\alpha + 1)$ assuming $F(\alpha)$ is defined, and then, for limit ordinals δ one defines $F(\delta)$ as the limit of the $F(\beta)$ for all $\beta < \delta$ (either in the sense of ordinal limits, as we have just explained, or for some other notion of limit if F does not take ordinal values). Thus, the interesting step in the definition is the successor step, not the limit ordinals. Such functions (especially for F nondecreasing and taking ordinal values) are called *continuous*. We will see that ordinal addition, multiplication and exponentiation are continuous as functions of their second argument.

Indexing classes of ordinals

We have mentioned that any well-ordered set is similar (order-isomorphic) to a unique ordinal number α, or, in other words, that its elements can be indexed in increasing fashion by the ordinals less than α. This applies, in particular, to any set of ordinals: any set of ordinals is naturally indexed by the ordinals less than some α. The same holds, with a slight modification, for classes of ordinals (a collection of ordinals, possibly too large to form a set, defined by some property): any class of ordinals can be indexed by ordinals (and, when the class is unbounded in the class of all ordinals, this puts it in class-bijection with the class of all ordinals). So we can freely speak of the γ-th element in the class (with the convention that the "0-th" is the smallest, the "1-th" is the next smallest, and so on). Formally, the definition is by transfinite induction: the γ-th element of the class is defined (provided it has already been defined for all $\beta < \gamma$), as the smallest element greater than the β-th element for all $\beta < \gamma$.

We can apply this, for example, to the class of limit ordinals: the γ-th ordinal, which is either a limit or zero is $\omega \cdot \gamma$ (see ordinal arithmetic for the definition of multiplication of ordinals). Similarly, we can consider additively indecomposable ordinals (meaning a nonzero ordinal that is not the sum of two strictly smaller ordinals): the γ-th additively indecomposable ordinal is indexed as ω^γ. The technique of indexing classes of ordinals is often useful in the context of fixed points: for example, the γ-th ordinal α such that $\omega^\alpha = \alpha$ is written ϵ_γ. These are called the "epsilon numbers".

4.2.5 Ordinals and cardinals

Initial ordinal of a cardinal

Each ordinal has an associated cardinal, its cardinality, obtained by simply forgetting the order. Any well-ordered set having that ordinal as its order-type has the same cardinality. The smallest ordinal having a given cardinal as its cardinality is called the *initial ordinal* of that cardinal. Every finite ordinal (natural number) is initial, but most infinite ordinals are not initial. The axiom of choice is equivalent to the statement that every set can be well-ordered, i.e. that every cardinal has an initial ordinal. In this case, it is traditional to identify the cardinal number with its initial ordinal, and we say that the initial ordinal is a cardinal.

Cantor used the cardinality to partition ordinals into classes. He referred to the natural numbers as the *first number class*, the ordinals with cardinality $\aleph_0$ (the countably infinite ordinals) as the *second number class* and generally, the ordinals with cardinality $\aleph_{n-2}$ as the *n-th number class.*[3]

The α-th infinite initial ordinal is written ω_α. Its cardinality is written $\aleph_\alpha$. For example, the cardinality of $\omega_0 = \omega$ is $\aleph_0$, which is also the cardinality of ω^2 or ϵ_0 (all are countable ordinals). So (assuming the axiom of choice) we identify ω with $\aleph_0$, except that the notation $\aleph_0$ is used when writing cardinals, and ω when writing ordinals (this is important since, for example, $\aleph_0^2 = \aleph_0$ whereas $\omega^2 > \omega$). Also, ω_1 is the smallest uncountable ordinal (to see that it exists, consider the set of equivalence classes of well-orderings of the natural numbers: each such well-ordering defines a countable ordinal, and ω_1 is the order type of that set), ω_2 is the smallest ordinal whose cardinality is greater than $\aleph_1$, and so on, and ω_ω is the limit of the ω_n for natural numbers n (any limit of cardinals is a cardinal, so this limit is indeed the first cardinal after all the ω_n).

4.2.6 Some "large" countable ordinals

We have already mentioned (see Cantor normal form) the ordinal ϵ_0, which is the smallest satisfying the equation $\omega^\alpha = \alpha$, so it is the limit of the sequence 0, 1, ω, ω^ω, ω^{ω^ω}, etc. Many ordinals can be defined in such a manner as fixed points of certain ordinal functions (the ι-th ordinal such that $\omega^\alpha = \alpha$ is called ϵ_ι, then we could go on trying to find the ι-th ordinal such that $\epsilon_\alpha = \alpha$, "and so on", but all the subtlety lies in the "and so on"). We can try to do this systematically, but no matter what system is used to define and construct ordinals, there is always an ordinal that lies just above all the ordinals constructed by the system. Perhaps the most important ordinal that limits a system of construction in this manner is the Church-Kleene ordinal ω_1^{CK}, (despite the ω_1 in the name, this ordinal is countable), which is the smallest ordinal that cannot in any way be represented by a computable function (this can be made rigorous, of course). Considerably large ordinals can be defined below ω_1^{CK}, however, which measure the "proof-theoretic strength" of certain formal systems (for example, ϵ_0 measures the strength of Peano arithmetic). Large ordinals can also be defined above the Church-Kleene ordinal, which are of interest in various parts of logic.

4.3 Transfinite induction

`http://en.wikipedia.org/wiki/Transfinite_induction`

Transfinite induction is an extension of mathematical induction to well-ordered sets, for instance to sets of ordinal numbers or cardinal numbers.

4.3.1 Transfinite induction

Let $P(\alpha)$ be a property defined for all ordinals α. Suppose that whenever $P(\beta)$ is true for all $\beta < \alpha$, then $P(\alpha)$ is also true (including the case that $P(0)$ is true given the vacuously true statement that $P(\alpha)$ is true for all $\alpha < 0$). Then transfinite induction tells us that P is true for all ordinals. That is, if $P(\alpha)$ is true whenever $P(\beta)$ is true for all $\beta < \alpha$, then $P(\alpha)$ is true for all α. Or, more practically: in order to prove a property P for all ordinals α, one can assume that it is already known for all smaller $\beta < \alpha$.

Usually the proof is broken down into three cases:

1. Zero case: Prove that $P(0)$ is true.
2. Successor case: Prove that for any successor ordinal $\alpha + 1$, $P(\alpha + 1)$ follows from $P(\alpha)$ (and, if necessary, $P(\beta)$ for all $\beta < \alpha$).
3. Limit case: Prove that for any limit ordinal λ, $P(\lambda)$ follows from $P(\beta)$ for all $\beta < \lambda$.

Notice that all three cases are identical except for the type of ordinal considered. They do not formally need to be considered separately, but in practice the proofs are typically so different as to require separate presentations. Zero is sometimes considered a limit ordinal and then may sometimes be treated in proofs in the same case as limit ordinals.

Un importante risultato che possiamo subito ottenere utilizzando l'induzione transfinita è il fatto che ogni sequenza decrescente di ordinali è finita. Possiamo dimostrare questa proprietà per un generico ordinale β per induzione transfinita nel modo che segue

- ($\beta = 0$) Ovvio visto che un cammino decrescente che parta da 0 è di lunghezza 0
- (β sucessore) In questo caso $\beta = \alpha + 1$ e per ipotesi induttiva sappiamo che ogni cammino discendente che parte da α è finito. Visto che un cammino discendente che parte da β è al più un passo più lungo di un cammino che parte da α ne segue che anche ogni cammino discendente che parte da β è finito.
- (β ordinale limite). In questo caso $\beta = \mathsf{sup}\{\alpha \mid \alpha < \beta\}$ e per ipotesi induttiva ogni cammino che parte da un ordinale $\alpha < \beta$ è finito. Consideriamo allora un qualsiasi cammino discendente che parta da β: con il primo passo esso deve portare ad un ordinale $\alpha < \beta$ e quindi per ipotesi induttiva deve arrivare a 0 in un numero finito di passi.

4.3.2 Transfinite recursion

Transfinite recursion is a method of constructing or defining something and is closely related to the concept of transfinite induction. As an example, a sequence of sets A_α is defined for every ordinal α, by specifying how to determine A_α from the sequence of A_β for $\beta < \alpha$.

More formally, we can state the Transfinite Recursion Theorem as follows. Given a class function $G : V \to V$, there exists a unique transfinite sequence $F : \mathsf{Ord} \to V$ (where Ord is the class of all ordinals) such that

$$F(\alpha) = G(F \upharpoonright \alpha) \text{ for all ordinals } \alpha.$$

As in the case of induction, we may treat different types of ordinals separately: another formulation of transfinite recursion is that given a set g_1, and class functions G_2, G_3, there exists a unique function $F : \mathsf{Ord} \to V$ such that

$$\begin{cases} F(0) & = & g_1, \\ F(\alpha+1) & = & G_2(F(\alpha)), \text{ for all } \alpha \in \mathsf{Ord}, \\ F(\lambda) & = & G_3(F \upharpoonright \lambda), \text{ for all limit } \lambda \neq 0. \end{cases}$$

Note that we require the domains of G_2, G_3 to be broad enough to make the above properties meaningful. The uniqueness of the sequence satisfying these properties can be proven using transfinite induction.

More generally, one can define objects by transfinite recursion on any well-founded relation R. (R need not even be a set; it can be a proper class, provided it is a set-like relation; that is, for any x, the collection of all y such that $y\,R\,x$ must be a set.)

4.4 Ordinal arithmetic

Quanto segue è preso da

`http://en.wikipedia.org/wiki/Ordinal_arithmetic`

In the mathematical field of set theory, ordinal arithmetic describes the three usual operations on ordinal numbers: addition, multiplication, and exponentiation. Each can be defined in essentially two different ways: either by constructing an explicit well-ordered set which represents the operation or by using transfinite recursion. Cantor normal form provides a standardized way of writing ordinals.

4.4.1 Addition

The union of two disjoint well-ordered sets S and T can be well-ordered. The order-type of that union is the ordinal which results from adding the order-types of S and T. If two well-ordered sets are not already disjoint, then they can be replaced by order-isomorphic disjoint sets, e.g. replace S by $S \times \{0\}$ and T by $T \times \{1\}$. Thus the well-ordered set S is written "to the left" of the well-ordered set T, meaning one defines an order on $S \cup T$ in which every element of S is smaller than every element of T. The sets S and T themselves keep the ordering they already have. This addition is associative and generalizes the addition of natural numbers.

The first transfinite ordinal is ω, the set of all natural numbers. Let's try to visualize the ordinal $\omega + \omega$: two copies of the natural numbers ordered in the normal fashion and the second copy completely to the right of the first. If we write the second copy as $\{0' < 1' < 2', \ldots\}$ then $\omega + \omega$ looks like

$$0 < 1 < 2 < 3 < \ldots < 0' < 1' < 2' < \ldots$$

This is different from ω because in ω only 0 does not have a direct predecessor while in $\omega + \omega$ the two elements 0 and $0'$ do not have direct predecessors. Here are $3 + \omega$ and $\omega + 3$:

$$0 < 1 < 2 < 0' < 1' < 2' < \ldots$$
$$0 < 1 < 2 < \ldots < 0' < 1' < 2'$$

After relabeling, the former just looks like ω itself while the latter does not: we have $3 + \omega = \omega$. But $\omega + 3$ is not equal to ω since $\omega + 3$ has a largest element (namely, $2'$) and ω does not. So our addition is not commutative.

One can see for example that $(\omega + 4) + \omega = \omega + (4 + \omega) = \omega + \omega$.

The definition of addition can also be given inductively (the following induction is on β):

$\alpha + 0 = \alpha$,

$\alpha + (\beta + 1) = (\alpha + \beta) + 1$ (here, "+1" denotes the successor of an ordinal),

and if δ is a limit ordinal then $\alpha + \delta$ is the limit of the $\alpha + \beta$ for all $\beta < \delta$.

Using this definition, we also see that $\omega + 3$ is a successor ordinal (it is the successor of $\omega + 2$) whereas $3 + \omega$ is the limit of $3 + 0 = 3$, $3 + 1 = 4$, $3 + 2 = 5$, etc., which is just ω.

Zero is an additive identity $\alpha + 0 = 0 + \alpha = \alpha$.

Addition is associative $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

Addition is strictly increasing and continuous in the right argument:

$$\alpha < \beta \Rightarrow \gamma + \alpha < \gamma + \beta$$

but the analogous relation does not hold for the left argument; instead we only have:

$$\alpha < \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$$

Ordinal addition is left-cancellative: if $\alpha + \beta = \alpha + \gamma$, then $\beta = \gamma$. Furthermore, one can define left subtraction for ordinals $\beta \leq \alpha$: there is a unique γ such that $\alpha = \beta + \gamma$. On the other hand, right cancellation does not work:

$$3 + \omega = 0 + \omega \text{ but } 3 \neq 0$$

Nor does right subtraction, even when $\beta \leq \alpha$: for example, there does not exist any γ such that $\gamma + 42 = \omega$.

4.4.2 Multiplication

The Cartesian product, $S \times T$, of two well-ordered sets S and T can be well-ordered by a variant of lexicographical order which puts the least significant position first. Effectively, each element of T is replaced by a disjoint copy of S. The order-type of the Cartesian product is the ordinal which results from multiplying the order-types of S and T. Again, this operation is associative and generalizes the multiplication of natural numbers.

Here is $\omega \cdot 2$:

$$00 < 10 < 20 < 30 < \ldots < 01 < 11 < 21 < 31 < \ldots$$

and we see: $\omega \cdot 2 = \omega + \omega$. But $2 \cdot \omega$ looks like this:

$$00 < 10 < 01 < 11 < 02 < 12 < 03 < 13 < \ldots$$

and after relabeling, this looks just like ω and so we get $2 \cdot \omega = \omega \neq \omega \cdot 2$. Hence multiplication of ordinals is not commutative.

Distributivity partially holds for ordinal arithmetic: $R(S + T) = RS + RT$. However, the other distributive law $(T + U)R = TR + UR$ is not generally true: $(1 + 1) \cdot \omega = 2 \cdot \omega = \omega$ while $1 \cdot \omega + 1 \cdot \omega = \omega + \omega$ which is different. Therefore, the ordinal numbers do not form a ring.

The definition of multiplication can also be given inductively (the following induction is on β):

$$\alpha \cdot 0 = 0,$$
$$\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha,$$
and if δ is limit then $\alpha \cdot \delta$ is the limit of the $\alpha \cdot \beta$ for all $\beta < \delta$.

The main properties of the product are:

- $\alpha \cdot 0 = 0 \cdot \alpha = 0$.
- One is a multiplicative identity $\alpha \cdot 1 = 1 \cdot \alpha =?$.
- Multiplication is associative $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.
- Multiplication is strictly increasing and continuous in the right argument: $(\alpha < \beta$ and $\gamma > 0) \Rightarrow \gamma \cdot \alpha < \gamma \cdot \beta$
- In the left argument, do not have the same as in the right argument. For example, $1 < 2$ but $1 \cdot \omega = 2 \cdot \omega = \omega$. Instead one gets $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$.
- There is a left cancellation law: If $\alpha > 0$ and $\alpha \cdot \beta = \alpha \cdot \gamma$, then $\beta = \gamma$.
- Right cancellation does not work e.g. $1 \cdot \gamma = 2 \cdot \omega = \omega$ but 1 and 2 are different.
- $\alpha \cdot \beta = 0 \Rightarrow \alpha = 0$ or $\beta = 0$.
- Distributive law on the left: $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.
- No distributive law on the right: e.g. $(\omega + 1) \cdot 2 = \omega + 1 + \omega + 1 = \omega + \omega + 1 = \omega \cdot 2 + 1$ which is not $\omega \cdot 2 + 2$.
- Left division with remainder: for all α and β, if $\beta > 0$, then there are unique γ and δ such that $\alpha = \beta \cdot \gamma + \delta$ and $\delta < \beta$. (This does not however mean the ordinals are a Euclidean domain, since they are not even a ring, and the Euclidean "norm" is ordinal-valued.)
- Right division does not work: there is no α such that $\alpha \cdot \omega \leq \omega^\omega \leq (\alpha + 1) \cdot \omega$.

4.4.3 Exponentiation

Exponentiation of well ordered sets is defined as follows. If the exponent is a finite set, the power is the product of iterated multiplication. For instance, $\omega^2 = \omega \cdot \omega$ using the operation of ordinal multiplication.

To generalize this to the case when the exponent is an infinite ordinal requires a different viewpoint. Note that $\omega \cdot \omega$ can be visualized as the set of functions from $2 = \{0, 1\}$ to $\omega = \{0, 1, 2, \ldots\}$, ordered lexicographically with the least significant position first:

$$(0,0) < (1,0) < (2,0) < (3,0) < \ldots < (0,1) < (1,1) < (2,1) < (3,1) < \ldots < (0,2) < (1,2) < (2,2) < \ldots$$

Here for brevity, we have replaced the function $\{(0, k), (1, m)\}$ by the ordered pair (k, m).

Similarly, for any finite exponent n, ω^n can be visualized as the set of functions from n (the domain) to the natural numbers (the range). These functions can be abbreviated as n-tuples of natural numbers.

For ω^ω, we might try to visualize the set of infinite sequences of natural numbers. However, if we try to use any absolutely defined ordering on this set, we find it is not well-ordered. Using the variant lexicographical ordering again, we restrict the set of sequences to those for which only a

finite number of elements of the sequence are different from zero. This is naturally motivated as the limit of the finite powers of the base (similar to the concept of coproduct in algebra). This can also be thought of as the infinite union $\bigcup_{n<\omega} \omega^n$.

The lexicographical order on this set is a well ordering that resembles the ordering of natural numbers written in decimal notation, except with digit positions reversed, and with arbitrary natural numbers instead of just the digits $0-9$:

$$(0,0,0,\ldots) < (1,0,0,0,\ldots) < (2,0,0,0,\ldots) < \ldots <$$
$$(0,1,0,0,0,\ldots) < (1,1,0,0,0,\ldots) < (2,1,0,0,0,\ldots) < \ldots <$$
$$(0,2,0,0,0,\ldots) < (1,2,0,0,0,\ldots) < (2,2,0,0,0,\ldots)$$
$$< \ldots <$$
$$(0,0,1,0,0,0,\ldots) < (1,0,1,0,0,0,\ldots) < (2,0,1,0,0,0,\ldots)$$
$$< \ldots$$

In general, any well ordered set B can be raised to the power of another well ordered set E, resulting in another well ordered set, the power B^E. Each element of B^E is a function from E to B such that only a finite number of elements of the domain E map to an element larger than the least element of the range B (essentially, we consider the functions with finite support). The order is lexicographic with the least significant position first.

We find $1^\omega = 1$, $2^\omega = \omega$, $2^{\omega+1} = \omega \cdot 2 = \omega + \omega$.

The order type of the power B^E is the ordinal which results from applying ordinal exponentiation to the order type of the base B and the order type of the exponent E.

The definition of exponentiation can also be given inductively (the following induction is on β, the exponent):

$$\alpha^0 = 1,$$
$$\alpha^{\beta+1} = (\alpha^\beta) \cdot \alpha, \text{ and}$$
$$\text{if } \delta \text{ is limit, then } \alpha^\delta \text{ is the limit of the } \alpha^\beta \text{ for all } \beta < \delta.$$

Properties of ordinal exponentiation:

- $\alpha^0 = 1$.
- If $0 < \alpha$, then $0^\alpha = 0$.
- $1^\alpha = 1$.
- $\alpha^1 = \alpha$.
- $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$.
- $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$.
- There are α, β, and γ for which $(\alpha \cdot \beta)^\gamma \neq \alpha^\gamma \cdot \beta^\gamma$. For instance, $(\omega \cdot 2)^2 = \omega^2 \cdot 2 \neq \omega^2 \cdot 4$.
- Ordinal exponentiation is strictly increasing and continuous in the right argument: If $\gamma > 1$ and $\alpha < \beta$, then $\gamma^\alpha < \gamma^\beta$.
- If $\alpha < \beta$, then $\alpha^\gamma \leq \beta^\gamma$. Note, for instance, that $2 < 3$ and yet $2^\omega = 3^\omega = \omega$.
- If $\alpha > 1$ and $\alpha^\beta = \alpha^\gamma$, then $\beta = \gamma$. If $\alpha = 1$ or $\alpha = 0$ this is not the case.
- For all α and β, if $\beta > 1$ and $\alpha > 0$ then there exist unique γ, δ, and ρ such that $\alpha = \beta^\gamma \cdot \delta + \rho$ such that $0 < \delta < \beta$ and $\rho < \beta^\gamma$.

Warning: Ordinal exponentiation is quite different from cardinal exponentiation. For example, the ordinal exponentiation $2^\omega = \omega$, but the cardinal exponentiation $2^{\aleph_0}$ is the cardinality of the continuum which is larger than $\aleph^0$. To avoid confusing ordinal exponentiation with cardinal exponentiation, one can use symbols for ordinals (e.g. ω) in the former and symbols for cardinals (e.g. $\aleph_0$) in the latter.

4.5 Cantor normal form

Quanto segue è preso da

`http://en.wikipedia.org/wiki/Ordinal_arithmetic`

Ordinal numbers present a rich arithmetic. Every ordinal number α can be uniquely written as $\omega^{\beta_1} \cdot c_1 + \omega^{\beta_2} \cdot c_2 + \ldots + \omega^{\beta_k} \cdot c_k$, where k is a natural number, c_1, c_2, ..., c_k are positive integers, and $\beta_1 > \beta_2 > \ldots > \beta_k$ are ordinal numbers (we allow $\beta_k = 0$). This decomposition of α is called the *Cantor normal form* of α, and can be considered the base-ω positional numeral system. The highest exponent β_1 is called the degree of α_1, and satisfies $\beta_1 \leq \alpha$. The equality $\beta_1 = \alpha$ applies if and only if $\alpha = \omega^\alpha$. In that case Cantor normal form does not express the ordinal in terms of smaller ones; this can happen as explained below.

A minor variation of Cantor normal form, which is usually slightly easier to work with, is to set all the numbers c_i equal to 1 and allow the exponents to be equal. In other words, every ordinal number α can be uniquely written as $\omega^{\beta_1} + \omega^{\beta_2} + \ldots + \omega^{\beta_k}$, where k is a natural number, and $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_k \geq 0$ are ordinal numbers.

The Cantor normal form allows us to uniquely express –and order– the ordinals α which are built from the natural numbers by a finite number of arithmetical operations of addition, multiplication and "raising ω to the power of": in other words, assuming $\beta_1 < \alpha$ in the Cantor normal form, we can also express the exponents β_i in Cantor normal form, and making the same assumption for the β_i as for α and so on recursively, we get a system of notation for these ordinals (for example,

$$\omega^{\omega^{\omega^7 \cdot 6 + \omega + 42} \cdot 1729 + \omega^9 + 88} \cdot 3 + \omega^{\omega^\omega} \cdot 5 + 65537$$

denotes an ordinal).

The ordinal ϵ_0 (epsilon nought) is the set of ordinal values of the finite arithmetical expressions of this form. It is the smallest ordinal that does not have a finite arithmetical expression, and the smallest ordinal such that $\epsilon_0 = \omega^{\epsilon_0}$, i.e. in Cantor normal form the exponent is not smaller than the ordinal itself. It is the limit of the sequence

$$0, 1 = \omega^0, \omega = \omega^1, \omega^\omega, \omega^{\omega^\omega}, \ldots$$

The ordinal ϵ_0 is important for various reasons in arithmetic (essentially because it measures the proof-theoretic strength of the first-order Peano arithmetic: that is, Peano's axioms can show transfinite induction up to any ordinal less than ϵ_0 but not up to ϵ_0 itself).

The Cantor normal form also allows us to compute sums and products of ordinals: to compute the sum, for example, one needs merely know that

$$\omega^\beta \cdot c + \omega^{\beta'} \cdot c' = \omega^{\beta'} \cdot c'$$

if $\beta' > \beta$ (if $\beta' = \beta$ one can obviously rewrite this as $\omega^\beta \cdot (c + c')$, and if $\beta' < \beta$ the expression is already in Cantor normal form); and to compute products, the essential facts are that when $\alpha = \omega^{\beta_1} \cdot c_1 + \ldots + \omega^{\beta_k} \cdot c_k$ is in Cantor normal form (and $\alpha > 0$) then

$$\alpha \cdot \omega^{\beta'} = \omega^{\beta_1 + \beta'}$$

and

$$\alpha \cdot n = \omega^{\beta_1} \cdot c_1 \cdot n + \omega^{\beta_2} \cdot c_2 + \ldots + \omega^{\beta_k} \cdot c_k$$

if n is a non-zero natural number.

To compare two ordinals written in Cantor normal form, first compare β_1, then c_1, then β_2, then c_2, etc.. At the first difference, the ordinal which has the larger component is the larger ordinal. If they are the same until one terminates before the other, then the one which terminates first is smaller.

4.5.1 Calcolare la forma normale di Cantor

To prove Cantor's normal form theorem we will need to make frequent use of the following important triviality

Lemma 4.5.1 *If $f : \mathsf{On} \to \mathsf{On}$ is normal, then for every $\beta \in \mathsf{On}$ there is a maximal $\alpha \in \mathsf{On}$ such that $f(\alpha) \leq \beta$.*

Proof. Let α_0 be $\mathsf{sup}\{\alpha \mid f(\alpha) \leq \beta\}$. Then

$$f(\alpha_0) = f(\mathsf{sup}\{\alpha \mid f(\alpha) \leq \beta\})$$

which by continuity of f is

$$\mathsf{sup}\{f(\alpha) \mid f(\alpha) \leq \beta\})$$

which of course is $\leq \beta$ since the ordinals are totally ordered. So α_0 is the largest element of $\{f(\alpha) \mid f(\alpha) \leq \beta\}$.

The way into Cantor Normal Forms is to think of the previous lemma as a rudimentary result of the kind "Given an ordinal β and a normal function f, $f(\alpha_0)$ is the best approximation to β from below that I can give using f." Cantor Normal form is an elaboration of this idea into a technique. Let us first minute a few normal functions to see what sort of things we can attack β with. For every $\alpha > 0$ the functions

$$\gamma \mapsto \alpha + \gamma; \qquad \gamma \mapsto \alpha \cdot \gamma; \qquad \gamma \mapsto \alpha^\gamma$$

are all normal, and each is obtained by iteration from the preceding one.

We are given β and we want to express it in terms of a normal function. Let α be some random ordinal below β. Then $\gamma \mapsto \alpha^\gamma$ is a normal function and since $\alpha < \beta$ we know by the lemma above that there is a largest γ such that $\alpha^\gamma \leq \beta$. Call this ordinal γ_0. Then $\alpha^{\gamma_0} \leq \beta$. If $\alpha^{\gamma_0} = \beta$ we stop there.

Now consider the case where $\alpha^{\gamma_0} < \beta$. By maximality of γ_0 we have

$$(*) \qquad \alpha^{\gamma_0} < \beta < \alpha^{\gamma_0+1} = \alpha^{\gamma_0} \cdot \alpha$$

We now attack β again, but this time not with the normal function $\gamma \mapsto \alpha^\gamma$ but the function $\theta \mapsto \alpha^{\gamma_0} \cdot \theta$. So by the lemma above there is a maximal θ such that $\alpha^{\gamma_0} \cdot \theta \leq \beta$. Call it θ_0. By $(*)$ we must have $\theta_0 < \alpha$.

If $\alpha^{\gamma_0} \cdot \theta_0 = \beta$ we stop there, so suppose $\alpha^{\gamma_0} \cdot \theta_0 < \beta$, and in fact

$$(**) \qquad \alpha^{\gamma_0} \cdot \theta_0 < \beta < \alpha^{\gamma_0} \cdot (\theta_0 + 1) = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_0}$$

by maximality of θ_0.

Now $\beta = \alpha^{\gamma_0} \cdot \theta_0 + \delta_0$, and we know $\delta_0 < \alpha^{\gamma_0}$ because of $(**)$. What we have proved is that, given ordinals $\alpha < \beta$, we can express β as $\alpha^{\gamma_0} \cdot \theta_0 + \delta_0$ with γ_0 and θ_0 maximal. If $\delta_0 < \alpha$ we stop. However if $\delta_0 > \alpha$ we continue, by attacking δ_0 with the normal function $\gamma \mapsto \alpha^\gamma$.

What happens if we do this? We then have $\delta = \alpha^{\gamma_1} \cdot \theta_1 + \delta_1$, which is to say

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \delta_1$$

One thing we can be sure of is that $\gamma_0 > \gamma_1$. This follows from the maximality θ_0.

We now go back and repeat the process, this time with δ_1 and α rather than α and β.

Therefore, when we repeat the process to obtain:

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \alpha^{\gamma_2} \cdot \theta_2 + \delta_3$$

and so on:

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \alpha^{\gamma_2} \cdot \theta_2 + \ldots + \alpha^{\gamma_n} \cdot \theta_n + \ldots$$

Now we do know that this process must terminate, because the sequence of ordinals

$$\{\gamma_0 > \gamma_1 > \gamma_2 > \ldots > \gamma_n > \ldots\}$$

is a descending sequence of ordinals and must be finite, because $<_{\mathsf{On}}$ is wellfounded.

So we have proved this:

Theorem 4.5.2 *For all α and β there are $\gamma_0 > \ldots > \gamma_n$ and $\theta_0 \ldots \theta_n$ with $\theta_i < \alpha$ for each i, such that*

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \alpha^{\gamma_2} \cdot \theta_2 + \ldots + \alpha^{\gamma_n} \cdot \theta_n$$

In particular, if $\alpha = \omega$ all the θ_i are finite. Since every finite ordinal is a sum $1 + 1 + 1 + \ldots$ this means that every ordinal is a sum of a decreasing finite sequence of powers of ω.

Quite how useful this fact is when dealing with an arbitrary ordinal β will depend on β. After all, if $\beta = \omega^\beta$ then –if we run the algorithm with ω and β– all Cantor's normal form theorem will tell us is that this is, indeed, the case. Ordinals β s.t. $\beta = \omega^\beta$ are around in plenty. They are called ϵ-numbers. They are moderately important because if β is an ϵ-number then the ordinals below β are closed under exponentiation. The smallest ϵ-number is called 'ϵ_0'. For the moment what concerns us about ϵ_0 is that if we look at the proof of Cantor's Normal Form theorem in the case where β is an ordinal below ϵ_0 and $\alpha = \omega$ the result is something sensible. This is because, ϵ_0 being the *least* fixed point of $\alpha \mapsto \omega^\alpha$, if we apply the technique of lemma 4.5.1 to some $\alpha < \epsilon_0$ the output of this process must be an expression containing only ordinals below α.

4.5.2 Unicità della forma normale di Cantor

The ordinals below ϵ_0 can be built up from 0 using *successor*, $+$, and the function $\alpha \mapsto \omega^\alpha$. The build-up is unique if one uses the *Cantor normal form*:

Theorem 4.5.3 *For every ordinal $\alpha > 0$ there are* unique *$\alpha_1 \geq \ldots \geq \alpha_n$ such that*

$$\alpha = \omega^{\alpha_1} + \ldots + \omega^{\alpha_n}$$

Proof. (*Uniqueness*) Suppose that

$$(1) \qquad \omega^{\alpha_1} + \ldots + \omega^{\alpha_n} = \omega^{\beta_1} + \ldots + \omega^{\beta_m}$$

Let i be minimal such that $\alpha_i \neq \beta_i$. If such i does not exist and $n \neq m$ then clearly (1) cannot hold, so $n = m$ in this case and we have uniqueness. If i exists, without loss of generality $\alpha_i > \beta_i$. But then

$$\omega^{\alpha_i} \geq \omega^{\beta_i + 1} = \omega^{\beta_i} \cdot \omega = \mathsf{sup}\{\omega^{\beta_i} \cdot n \mid n \in \omega\} > \omega^{\beta_i} \cdot n$$

for every n. Hence $\omega^{\alpha_i} > \omega^{\beta_i} + \ldots + \omega^{\beta_m}$, contradicting (1).

(*Existence*). We prove by induction on β that every α with $0 < \alpha < \omega^\beta$ has a Cantor normal form.

- $\beta = 0$. Since $\omega^0 = 1$ there is nothing to prove.
- β sucessor. We have $\omega^{\beta+1} = \omega_\beta \cdot \omega = \mathsf{sup}\{\omega^\beta \cdot n \mid n \in \omega\}$. By the induction hypothesis, every $\alpha < \omega^\beta$ has a Cantor normal form. We prove by induction on n that every $0 < \alpha < \omega^\beta \cdot n$ has a Cantor normal form. The base case $n = 1$ holds by induction hypothesis. Induction step $n + 1$: Suppose $\alpha < \omega^\beta \cdot (n + 1) = \omega^\beta \cdot n + \omega^\beta$. If $\alpha < \omega^\beta \cdot n$ we are done by induction hypothesis. Otherwise $\omega^\beta \cdot n \leq \alpha < \omega^\beta \cdot n + \omega^\beta$. But then $\alpha = \omega^\beta \cdot n + \xi$ for some $\xi < \omega^\beta$. By induction hypothesis ξ has a Cantor normal form $\omega^{\xi_1} + \ldots + \omega^{\xi_m}$. By $\xi < \omega^\beta$ all the exponents ξ_i have $\xi_i < \beta$, so it follows that α also has a Cantor normal form.
- β a limit. In this case $\omega^\beta = \mathsf{sup}\{\omega^\gamma \mid \gamma < \beta\}$. If $\alpha < \omega^\beta$ then there is $\gamma < \beta$ such that $\alpha < \omega^\gamma$, so by induction hypothesis α has a Cantor normal form.

4.6 Ordinali e ipergioco

Sia α_0 un ordinale. Possiamo allora pensare al seguente processo di cui descriviamo il passo i-mo:

1. scegliamo un qualsiasi elemento α_{i+1} di α_i
2. incrementiamo i

3. torniamo al passo (1)

In questo modo costruiamo una successione decrescente di ordinali (l'ordinale α_{i+1} è minore dell'ordinale α_i visto che è un suo elemento) e quindi il processo è destinato a terminare in un numero finito di passi visto che ogni catena discendente di ordinali deve necessariamente arrivare a 0, cioè a $\emptyset$.

Se partiamo ora da un qualsiasi insieme di ordinali la situazione non cambia visto che appena ne scegliamo un elemento cadiamo nella situazione precedente.

La situazione è quindi molto simile a quella che si incontra quando si analizza il paradosso dell'ipergioco (vedi appendice A). Infatti un ordinale si può considerare come la descrizione astratta di un gioco finito in cui ad ogni stato del gioco teniamo conto solo delle mosse possibili in quello stato (alcuni stati possono ammettere anche un numero infinito di mosse ma il gioco è da considerarsi ancora come finito nel senso che ogni sviluppo di mosse prima o poi termina). Quel che ci insegna in paradosso dell'ipergioco è che se consideriamo la collezione di tutti i giochi finiti e ci chiediamo se essa definisce un gioco finito allora ci troviamo in una situazione paradossale.

Nel nostro caso, qualcosa di analogo capita se consideriamo la collezione di tutti gli ordinali: da un certo punto di vista quel che otteniamo dovrebbe essere un ordinale (il supremo di tutti gli ordinali) ma questo ci porta ad una situazione paradossale perchè questo *ordinale* dovrebbe essere un elemento della collezione di tutti gli ordinali e quindi a partire da lui sarebbe possibile definire una successione infinita di ordinali sempre più piccoli (basterebbe scegliere sempre come elemento la collezione di tutti gli ordinali come nel caso del paradosso dell'ipergioco come prima mossa si sceglie sempre di giocare all'ipergioco). La via di uscita da tale situazione è quella di dire che la collezione di tutti gli ordinali non è un insieme e quindi tanto meno può essere un ordinale (gli ordinali sono insiemi!).

Se nel caso della collezione di tutti gli ordinali la soluzione sembra un po' un trucco per evitare il problema (ma proprio per evitare situazioni di questo tipo è importante distinguere tra collezioni e insiemi), se usiamo lo stesso approccio con collezioni che non siano paradossali possiamo ricavare informazioni utili (come d'altra parte succede anche con il paradosso dell'ipergioco che può essere utilizzato per dimostrare la non esistenza di una funzione biunivoca tra un insieme e la sua potenza).

Ad esempio se consideriamo la collezione di tutti gli ordinali numerabili ne deduciamo che il suo supremo non può essere un ordinale numerabile, ma questa volta la via di uscita è semplicemente quella di considerare questa informazione come una dimostrazione del fatto che il supremo della collezione degli ordinali numerabili è il più piccolo ordinale non numerabile (sulla cui cardinalità poco si può dire, vedi la sezione 2.1.3).

4.7 References

Cantor, G., (1897), *Beitrage zur Begrundung der transfiniten Mengenlehre.* II (tr.: Contributions to the Founding of the Theory of Transfinite Numbers II), Mathematische Annalen 49, 207-246 English translation.

Conway, J. H. and Guy, R. K., *Cantor's Ordinal Numbers.* In The Book of Numbers. New York: Springer-Verlag, pp. 266-267 and 274, 1996.

Dauben, Joseph Warren, (1990), *Georg Cantor: his mathematics and philosophy of the infinite.* Chapter 5: The Mathematics of Cantor's Grundlagen. ISBN 0691024472

Hamilton, A. G. (1982), *Numbers, Sets, and Axioms : the Apparatus of Mathematics*, New York: Cambridge University Press, ISBN 0521245095 See Ch. 6, Ordinal and cardinal numbers

Kanamori, A., *Set Theory from Cantor to Cohen*, to appear in: Andrew Irvine and John H. Woods (editors), The Handbook of the Philosophy of Science, volume 4, Mathematics, Cambridge University Press.

Levy, A. (1979), *Basic Set Theory*, Berlin, New York: Springer-Verlag Reprinted 2002, Dover. ISBN 0-486-42079-5

Jech, Thomas (2003), *Set Theory*, Springer Monographs in Mathematics, Berlin, New York: Springer-Verlag

Sierpinski, W. (1965). *Cardinal and Ordinal Numbers (2nd ed.)*. Warszawa: Pastwowe Wydawnictwo Naukowe.

Suppes, P. (1960), *Axiomatic Set Theory*, D.Van Nostrand Company Inc., ISBN 0-486-61630-4

Capitolo 5

Vero ma non dimostrabile (in PA)

In questo capitolo vedremo alcuni esempi di proposizioni matematiche

- che si possono esprimere nell'aritmetica di Peano (o equivalentemente nella teoria degli insiemi finiti),
- che, utilizzando la teoria degli insiemi (incluso l'assioma dell'infinito), si possono dimostrare essere valide
- ma che non si possono dimostrare nell'aritmetica di Peano (e quindi neppure nella teoria degli insiemi finiti).

In questo senso esse si possono considerare *vere*, visto che in qualche modo le possiamo dimostrare, ma *non dimostrabili*, visto che non le possiamo dimostrare nella teoria in cui sono esprimibili.

5.1 Il teorema di Goodstein

Da Wikipedia, l'enciclopedia libera.

`http://it.wikipedia.org/wiki/Teorema_di_Goodstein`

In matematica, il Teorema di Goodstein è un teorema sui numeri naturali, relativamente semplice da enunciare, la cui particolarità consiste nel fatto di essere indecidibile dall'aritmetica di Peano ma dimostrabile nella teoria assiomatica degli insiemi. Esso può essere considerato un esempio di enunciato indecidibile dagli usuali assiomi dell'aritmetica più "naturale" rispetto alle complicate costruzioni dei teoremi di incompletezza di Gödel.

Per enunciare il Teorema di Goodstein occorre dare alcune definizioni preliminari.

5.1.1 Notazione ereditaria in base n

Definiamo innanzitutto una speciale notazione numerica. Dato un numero naturale n chiamiamo notazione ereditaria in base n di un numero a l'espressione costruita mediante la seguente procedura:

- Scriviamo a in base n, ottenendo un'espressione del tipo:

  $$a_k n^k + a_{k-1} n^{k-1} + \ldots + a_0$$

  dove tutti gli a_i sono compresi tra 0 e $n-1$.
- Scriviamo tutti gli esponenti in base n e sostituiamo l'espressione di ciascuno di essi nell'espressione sopra.
- Consideriamo ora tutti gli esponenti che compaiono negli esponenti e ancora li rimpiazziamo con la loro scrittura in base n

- E così via per gli esponenti degli esponenti degli esponenti, eccetera ... fino ad arrivare ad una espressione in cui compaiono solamente numeri compresi tra 0 e n.

Per esempio: scriviamo 35 nella notazione ereditaria in base 2:

- Scriviamo inizialmente 35 in base 2:

$$35 = 2^5 + 2^1 + 2^0$$

- Gli esponenti sono 5, 1 e 0. Gli esponenti 1 e 0 sono già in base 2, per quanto riguarda 5 la sua espressione in base 2 è data da 2^2+1, quindi rimpiazziamo questa espressione nell'espressione che avevamo prima e otteniamo

$$35 = 2^{2^2+1} + 2^1 + 2^0$$

- La scrittura ottenuta è quella finale, poiché compaiono solamente numeri compresi tra 0 e 2.

5.1.2 Sequenza di Goodstein associata ad un numero

La sequenza di Goodstein associata ad un numero m è una successione $G(1, m)$, $G(2, m)$, $G(3, m)$, ... definita per ricorrenza nel seguente modo:

$$\begin{aligned} G(1, m) &= m \\ G(k + 1, m) &= d(G(k, m)) - 1 \end{aligned}$$

ove $d(G(k, m))$ è l'operazione di dilatazione su $G(k, m)$ ottenuta sostituendo il numero $k+2$ a tutti le occorrenze del numero $k + 1$ presenti nella notazione ereditaria in base $k + 1$.

Vediamo ora passo passo:

- il primo elemento $G(1, m)$ della sequenza è il numero m stesso
- per ottenere il secondo $G(2, m)$ si procede così:
  - si scrive m nella notazione ereditaria in base 2
  - si sostituisce il numero 3 al posto di ogni 2
  - si sottrae 1
- per ottenere il terzo elemento $G(3, m)$ si procede così:
  - si scrive $G(2, m)$ nella notazione ereditaria in base 3
  - si sostituisce il numero 4 al posto di ogni 3
  - si sottrae 1
- più in generale, una volta ottenuto il k-esimo numero della sequenza $G(k, m)$, per ottenere il termine $(k + 1)$-esimo si procede così:
  - si scrive $G(k, m)$ nella notazione ereditaria in base $k + 1$
  - si sostituisce il numero $k + 2$ al posto di ogni $k + 1$
  - si sottrae 1

La sequenza termina in corrispondenza del primo valore del passo k tale che $G(k, m) = 0$.
Ad esempio i primi tre termini della sequenza di Goodstein di 35 sono:

- $G(1, 35) = 35$
- poiché $35 = 2^{2^2+1} + 2^1 + 2^0$ rimpiazzando 2 con 3 e sottraendo 1 otteniamo:

$$G(2, 35) = 3^{3^3+1} + 3^1 + 3^0 - 1 = 3^{28} + 3 = 22876792454964$$

- per calcolare $G(3, 35)$ dobbiamo scrivere in notazione ereditaria in base 3 il numero 22876792454964, tale scrittura risulta essere $3^{3^3+1} + 3^1$; quando rimpiazziamo 4 al posto di 3 otteniamo circa 5363×10^{136}, un numero enorme a cui dobbiamo sottrarre 1.

Il calcolo dei termini di una sequenza di Goodstein

Per calcolare effettivamente i termini di una sequenza di Goodstein possono essere utili le seguenti considerazioni. Supponiamo di avere un numero m scritto in base a ereditaria

$$m = n_0 a^{k_0} + n_1 a^{k_1} + \ldots + n_s a^{k_s}$$

dove $n_0, \ldots n_s$ sono numeri naturali minori di a e $k_0, \ldots, k_s$ sono numeri scritti in base a ereditaria.

Allora la più complessa operazione che dobbiamo fare per portare calcolare il prossimo termine della successione è quella di sottrarre 1 da m e riscrivere il risultato in base a. Tuttavia per fare questo passo, se m è già espresso in base a, non abbiamo alcun bisogno di calcolarne il valore in base 10, operare la sottrazione e riportare il risultato in base a visto che possiamo procedere come segue:

- (caso $k_s = 0$) In questo caso

$$\begin{aligned} m-1 &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + n_s a^0 - 1 \\ &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + (n_s - 1) a^0 \end{aligned}$$

- (caso $k_s > 0$ e $n_s = 1$) In questo caso

$$\begin{aligned} m-1 &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + a^{k_s} - 1 \\ &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + a a^{k_s - 1} - 1 \\ &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + (a-1) a^{k_s - 1} + a^{k_s - 1} - 1 \\ &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + (a-1) a^{k_s - 1} + (a-1) a^{k_s - 2} + a^{k_s - 2} - 1 \\ &\ldots \\ &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + (a-1) a^{k_s - 1} + \ldots + (a-1) a^{k_s - (k_s - 1)} + (a-1) a^{k_s - k_s} - 1 \\ &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + (a-1) a^{k_s - 1} + \ldots + (a-1) a^1 + (a-1) a^0 \end{aligned}$$

- (caso $k_s > 0$ e $n_s > 1$) In questo caso possiamo facilmente ridurci al caso precedente per poi ripetere gli stessi passi

$$\begin{aligned} m-1 &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + n_s a^{k_s} - 1 \\ &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + (n_s - 1) a^{k_s} + a^{k_s} - 1 \\ &\ldots \\ &= n_0 a^{k_0} + n_1 a^{k_1} + \ldots + (n_s - 1) a^{k_s} + (a-1) a^{k_s - 1} + \ldots + (a-1) a^1 + (a-2) a^0 \end{aligned}$$

Una volta che abbiamo capito come eseguire questo passo del calcolo risulta molto naturale pensare che un numero m espresso in base a iterata si può rappresentare in generale come una terna

$$m \equiv \langle n_0, k_0, r_0 \rangle_a$$

dove n_0 è il coefficiente della potenza di grado più alto (si tratta di un numero minore di a), k_0 è a sua volta una terna, che rappresenta un numero in base a iterata, che è l'esponete di grado massimo e r_0 è ancora una terna che rappresenta il *resto* del numero in base a iterata.

Vale la pena di notare che in questa rappresentazione la base non compare mai esplicitamente eccetto che a pedice della terna.

Dato quindi un qualsiasi numero espresso come terna $\langle n_0, k_0, r_0 \rangle_a$ della sequenza di Goodstein, diverso da $0 \equiv \langle 0, 0, 0 \rangle_a$, per passare al termine successivo basta cambiare la base a pedice ed effettuare l'operazione $\stackrel{*}{-}$ di decremento di 1 con il metodo suggerito qui sopra che manipola solamente gli elementi delle terne, cioè possiamo utilizzare la seguente definizione ricorsiva:

$$\begin{aligned} \langle 1, k_0, 0 \rangle_a \stackrel{*}{-} 1 &\Rightarrow \langle a-1, k_0 \stackrel{*}{-} 1, \langle 1, k_0 \stackrel{*}{-} 1, 0 \rangle \stackrel{*}{-} 1 \rangle_a \\ \langle n_0, 0, 0 \rangle_a \stackrel{*}{-} 1 &\Rightarrow \langle n_0 - 1, 0, 0 \rangle_a \\ \langle n_0, k_0, 0 \rangle_a \stackrel{*}{-} 1 &\Rightarrow \langle n_0 - 1, k_0, \langle 1, k_0, 0 \rangle \stackrel{*}{-} 1 \rangle_a \\ \langle n_0, k_0, r_0 \rangle_a \stackrel{*}{-} 1 &\Rightarrow \langle n_0, k_0, r_0 \stackrel{*}{-} 1 \rangle_a \end{aligned}$$

5.1.3 Altri esempi di sequenze di Goodstein

La sequenza di Goodstein che si ha partendo da 3 raggiunge presto il valore 0:

Base	Ereditaria	Valore	Note
2	$2^1 + 1$	3	1 sta per 2^0.
3	$3^1 + 1 - 1$	3	Rimpiazziamo i 2 nella precedente espressione con dei 3 e poi sottraiamo 1. Quello che otteniamo è 3 che è già espresso nella nuova base, che è appunto 3.
4	$4^1 - 1$	3	Rimpiazziamo i 3 nella precedente espressione con 4 e sottraiamo 1. Poiché il valore da rappresentare in base 4 è 3 che è minore della base, la rappresentazione è ancora 3.
5	$3 - 1$	2	Dovremmo rimpiazzare i 4 della precedente espressione con dei 5, ma non ce ne sono, quindi l'espressione rimane 3 a cui dobbiamo sottrarre 1.
6	$2 - 1$	1	
7	$1 - 1$	0	

È sufficiente considerare la successione di Goodstein associata a 4 per vedere invece i valori della successione crescere a lungo:

Base	Ereditaria	Valore
2	2^2	4
3	$2 \cdot 3^2 + 2 \cdot 3 + 2$	26
4	$2 \cdot 4^2 + 2 \cdot 4 + 1$	41
5	$2 \cdot 5^2 + 2 \cdot 5$	60
6	$2 \cdot 6^2 + 6 + 5$	83
7	$2 \cdot 7^2 + 7 + 4$	109
...	...	...
11	$2 \cdot 11^2 + 11$	253
12	$2 \cdot 12^2 + 11$	299
...	...	...
1000	$1000^{+}18 \cdot 1000 + 535$	1018535
1001	$1001^2 + 18 \cdot 1001 + 534$	1020553
...	...	...

Gli elementi di questa successione continuano a crescere fino a raggiungere in corrispondenza della base $3 \cdot 2^{402653209}$ il valore massimo di $3 \cdot 2^{402653210} - 1$, poi la successione rimane stazionaria per altri $3 \cdot 2^{402653209}$ passi e infine inizia a decrescere fino a raggiungere lo zero in corrispondenza della base $3 \cdot 2^{402653211} - 1$.

L'esempio della successione che inizia da 4 tuttavia non è ancora un buon esempio di quanto rapidamente può crescere una successione di Goodstein. Se partiamo da 19 otteniamo la sequenza

di valori:

Notazione ereditaria	Valore
$2^{2^2}+2+1$	19
$3^{3^3}+3$	7625597484990
$4^{4^4}+3$	circa 1.3×10^{154}
$5^{5^5}+2$	circa 1.8×10^{2184}
$6^{6^6}+1$	circa 2.6×10^{36305}
7^{7^7}	circa 3.8×10^{695974}
$7\times8^{7\times8^7+7\times8^6+7\times8^5+7\times8^4+7\times8^3+7\times8^2+7\times8+7}$ $+7\times8^{7\times8^7+7\times8^6+7\times8^5+7\times8^4+7\times8^3+7\times8^2+7\times8+6}+\dots$ $+7\times8^{8+2}+7\times8^{8+1}+7\times8^8+7\times8^7+7\times8^6$ $+7\times8^5+7\times8^4+7\times8^3+7\times8^2+7\times8+7$	circa 6×10^{15151335}
$7\times9^{7\times9^7+7\times9^6+7\times9^5+7\times9^4+7\times9^3+7\times9^2+7\times9+7}$ $+7\times9^{7\times9^7+7\times9^6+7\times9^5+7\times9^4+7\times9^3+7\times9^2+7\times9+6}+\dots$ $+7\times9^{9+2}+7\times9^{9+1}+7\times9^9+7\times9^7+7\times9^6$ $+7\times9^5+7\times9^4+7\times9^3+7\times9^2+7\times9+6$	circa 4.3×10^{369693099}
...	...

5.1.4 L'enunciato del teorema

Nonostante questa crescita vertiginosa il teorema di Goodstein asserisce che

Teorema 5.1.1 *Tutte le sequenze di Goodstein, qualunque sia il valore iniziale, raggiungono lo 0.*

Dimostrazione. Data una successione di Goodstein associata ad un qualsiasi numero m costruiamo una successione "parallela" di numeri ordinali. Abbiamo visto che ad ogni termine della sequenza è associata una base partendo da 2 per il primo (cioè m) e aumentando progressivamente di 1. Accanto alla sequenza dei valori possiamo quindi considerare la sequenza delle loro rappresentazioni nella corrispondente base come abbiamo visto nelle tabelle sopra rappresentate.

La successione parallela di ordinali è costruita considerando la successione di tutte le rappresentazioni ereditarie e sostituendo alle corrispondenti basi il numero ordinale ω. Ricordiamo che per i numeri ordinali sono ben definite le operazioni di addizione, moltiplicazione e potenza.

Nell'esempio considerato precedentemente con $m = 4$ abbiamo quindi:

Not. ereditaria	Valore	Base	Succ. parallela
2^2	4	2	ω^ω
$2 \cdot 3^2 + 2 \cdot 3 + 2$	26	3	$\omega^2 \cdot 2 + \omega \cdot 2 + 2$
$2 \cdot 4^2 + 2 \cdot 4 + 1$	41	4	$\omega^2 \cdot 2 + \omega \cdot 2 + 1$
$2 \cdot 5^2 + 2 \cdot 5$	60	5	$\omega^2 \cdot 2 + \omega \cdot 2$
$2 \cdot 6^2 + 6 + 5$	83	6	$\omega^2 \cdot 2 + \omega + 5$
$2 \cdot 7^2 + 7 + 4$	109	7	$\omega^2 \cdot 2 + \omega + 4$
...	...	...	...
$2 \cdot 11^2 + 11$	253	11	$\omega^2 \cdot 2 + \omega$
$2 \cdot 12^2 + 11$	299	12	$\omega^2 \cdot 2 + 11$
...	...	...	...
$1000^2 + 18 \cdots 1000 + 535$	1018535	1000	$\omega^2 + \omega \cdot 18 + 535$
$1001^2 + 18 \cdot 1001 + 534$	1020553	1001	$\omega^2 + \omega \cdot 18 + 534$
...	...	...	...

Nel caso in cui un termine delle due successioni fosse uguale a 0 deve essere 0 anche il termine della successione parallela. Dunque l'idea per la dimostrazione del teorema è dimostrare che la sequenza parallela di ordinali converge a 0.

Un primo passo consiste nell'osservare che la successione parallela, quando è non nulla, è strettamente decrescente rispetto alla relazione d'ordine di cui sono dotati naturalmente gli ordinali. A tale scopo ricordiamo che gli ordinali espressi nella forma che stiamo considerando corrispondono a tutti gli ordinali minori di ϵ_0, la cui struttura di insieme ordinato è isomorfa all'insieme delle funzioni reali di una variabile reale che si hanno considerando le analoghe espressioni con la variabile x al posto di ω e dotandolo della seguente relazione d'ordine:

$$p(x) <_{\text{psf}} q(x) \equiv \text{il grafico di } p(x) \text{ si stabilizza al di sotto del grafico di } q(x) \text{ da un certo } x \text{ in poi}$$

(le lettere "psf" abbreviano "per segmenti finali").

Come si può vedere, nell'esempio la successione di ordinali è decrescente rispetto a questa relazione d'ordine, ovvero:

$$x^x >_{\text{psf}} 2x^2 + 2x + 2 >_{\text{psf}} 2x^2 + 2x + 1 >_{\text{psf}} \cdots >_{\text{psf}} x^2 + 18x + 535 >_{\text{psf}} \cdots$$

dunque a differenza della successione originale, la successione parallela degli ordinali è decrescente. Questo accade perché l'operazione di cambiamento di base non ha alcun effetto sulla successione parallela, mentre quando scriviamo un termine della successione nella base corrispondente e sottraiamo 1 e lo riscriviamo nuovamente nella stessa base, l'ordinale associato sarà in ogni caso minore del precedente.

In generale se abbiamo una successione strettamente decrescente di numeri naturali possiamo concludere che questa deve raggiungere lo 0 in un numero finito di passi grazie al principio di induzione. Nel nostro caso abbiamo a che fare con una successione decrescente di numeri ordinali, e per concludere che questa deve raggiungere lo 0 possiamo avvalerci del principio di induzione transfinita.

5.1.5 Indipendenza dall'Aritmetica di Peano

Alle sequenze di Goodstein si può associare una funzione g dai naturali ai naturali che manda un qualunque numero naturale n nel numero di passi k necessari affinché la sequenza di Goodstein che da quel numero naturale parte arrivi a 0. Ad esempio abbiamo che i valori della sequenza di

Goodstein che parte da 3 con base 2 sono $3 \to 3 \to 3 \to 2 \to 1 \to 0$ e quindi $g(3) = 5$ mentre come abbiamo visto il valore di $g(4)$ è enormemente più grande (per non parlare dei valori successivi!).

Ora cosa interessante è che la funzione g è esprimibile nell'aritmetica di Peano tramite una qualche proposizione G tale che $g(n) = k$ se e solo se l'interpretazione della proposizione G nei numeri naturali è tale che $G(n, k)$ vale (possiamo esprimere G utilizzando solo successore, somme, prodotti e il predicato di uguaglianza) e sappiamo inoltre che si tratta di una funzione totale, cioè per ogni numero naturale n esiste un numero naturale k tale che l'interpretazione $G(n, k)$ nei numeri naturali vale.

Tuttavia, la dimostrazione sopra esposta di questo fatto fa uso di un principio (l'induzione transfinita sugli ordinali minori di ϵ_0) che non è formalizzabile nell'Aritmetica di Peano e per questo motivo non possiamo sperare di dimostrare la proposizione $\forall n.\exists k.G(n, k)$ usando la formalizzazione della prova che abbiamo dato utilizzando gli ordinali.

Questa è una conseguenza di due teoremi dovuti a Gödel e Gentzen: il primo ha dimostrato che se una teoria sufficientemente potente è coerente allora non può dimostrare la propria coerenza, il secondo ha dimostrato che la coerenza dell'Aritmetica di Peano si può dimostrare tramite il principio di induzione transfinita fino all'ordinale ϵ_0. Dunque a meno che l'aritmetica di Peano non sia incoerente non può essere in grado di formalizzare il principio di induzione transfinita fino all'ordinale ϵ_0.

È naturale quindi chiedersi se il teorema sia o no dimostrabile nell'Aritmetica di Peano (eventualmente in altri modi). La questione è stata risolta dal Teorema di Kirby e Paris (la cui dimostrazione è considerevolmente più tecnica e difficile di quella del Teorema di Goodstein) il quale sfrutta il teorema di Goodstein per dimostrare che l'aritmetica di Peano è una teoria coerente. La dimostrazione di Kirby e Paris assieme con i teoremi di incompletezza di Gödel implica che il teorema di Goodstein è indecidibile nell'aritmetica di Peano.

5.2 Il teorema delle idre

È noto dal famoso teorema di incompletezza di Gödel che esistono proposizioni valide che sono esprimibili ma non dimostrabili nell'Aritmetica di Peano (PA). Il risultato che ci interessa qui è una di tali proposizioni scoperta da Kirby e Paris nel 1982: la battaglia tra Ercole e l'idra. Ne diamo una esposizione informale tratta quasi integralmente dal loro lavoro originale.

Un'idra è un albero finito, che può essere considerato una collezione finita di segmenti ciascuno congiungente due nodi, tale che ogni nodo sia connesso da un unico cammino di segmenti ad un nodo fisso detto *radice* (vedi figura 5.1).

Una *testa* di un'idra è un nodo da cui esca un unico segmento e che non sia la radice.

Una battaglia tra Ercole e un'idra data si svolge così: al passo n-mo (con $n \geq 1$) Ercole taglia una testa dell'idra. L'idra quindi fa spuntare una quantità di nuove teste nel modo seguente: partendo dal nodo a cui era attaccata la testa appena tagliata, si percorre un segmento verso la radice finché si raggiunge il prossimo nodo. Da questo spuntano n nuove copie della parte dell'idra (dopo la decapitazione) che sta "sopra" il segmento appena percorso, cioè quei nodi e segmenti da cui, per raggiungere la radice, sarebbe necessario attraversare questo segmento. Se la testa appena tagliata era attaccata direttamente alla radice, l'idra non genera alcuna nuova testa (vedi figura 5.2).

Ercole vince se dopo un qualche numero finito di passi, non rimane niente dell'idra a parte la sua radice. Ercole combatte seguendo una *strategia*, ovvero una funzione che per ogni idra sceglie che testa tagliare. Non è difficile dimostrare che, per quanto la cosa sia sorprendente, Ercole può vincere.

Possiamo infatti dare un esempio di strategia per una battaglia tra Ercole e una generica idra che si può provare essere vincente per induzione sugli ordinali minori di ω^3.

Cominciamo con l'introdurre un po' di terminologia. L'*altezza* di un nodo di un albero è il numero minimo di segmenti che bisogna percorrere per andare da essa alla radice. I *figli* di un nodo sono i nodi che sono collegati alla radice attraverso tale nodo e che hanno altezza uguale all'altezza del nodo più uno. Infine la *larghezza* di un nodo è il numero dei suoi figli.

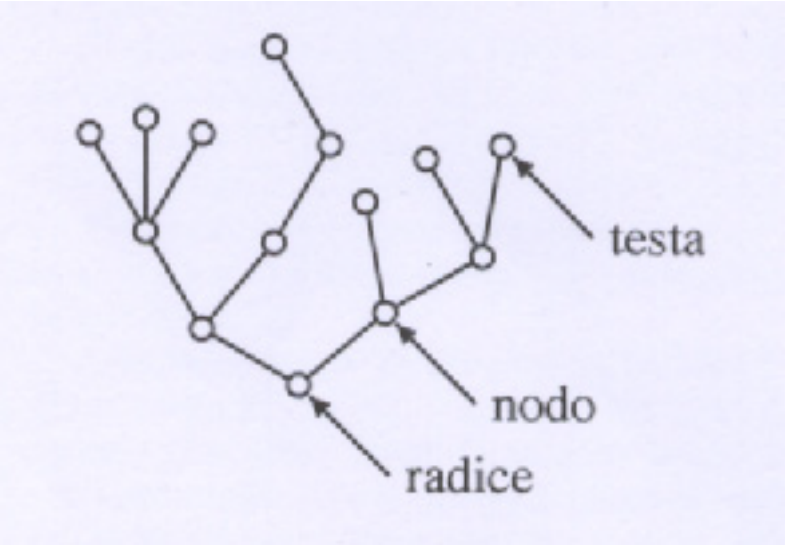

Figura 5.1: esempio di idra

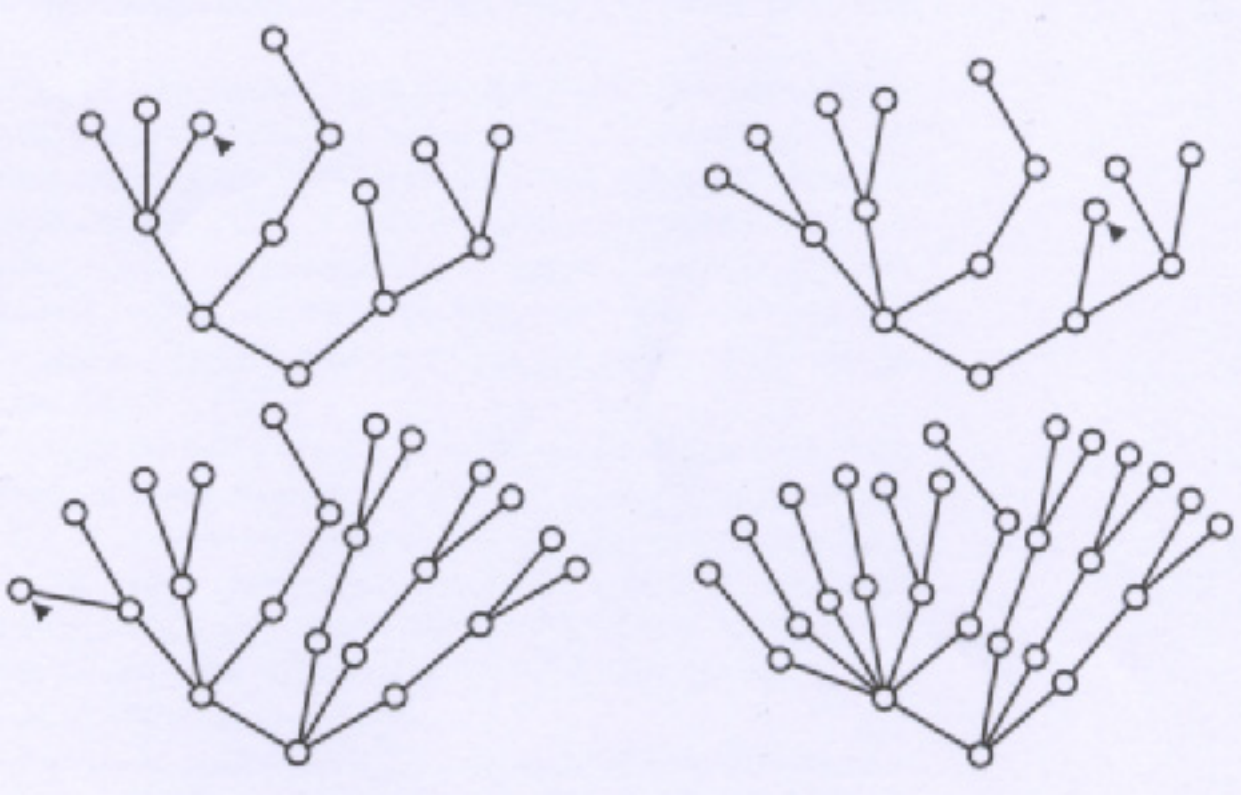

Figura 5.2: primi passi di una battaglia tra Ercole e l'idra

Introduciamo ora dei parametri associati ad un idra. Sia n l'altezza massima dei nodi dell'idra, m la larghezza massima dei nodi di altezza $n-1$ e k il numero di nodi di altezza $n-1$ e larghezza m. Sia quindi $\omega^2 \cdot n + \omega \cdot m + k$ l'ordinale *associato* a tale idra.

La strategia da impiegare è allora quella di tagliare ad un qualsiasi passo un figlio (che è certamente una testa) di un nodo di altezza $n-1$ e larghezza m. La prova che tale strategia è vincente consiste allora nel verificare che l'ordinale associato ad un'idra decresce strettamente quando si taglia la testa indicata dalla strategia. Lasciamo tale verifica al lettore; osserviamo solo che k è il parametro che decresce più rapidamente; quando k arriva a zero allora tocca ad m diminuire e k può aumentare; quando $m = 0$ allora è n a calare (e k e m possono crescere). Il combinare questi parametri nell'ordinale associato è un modo per assegnare un peso ai vari parametri: n pesa più di m e k e questo si traduce nel fatto che una diminuzione di n fa diminuire l'ordinale associato anche se m e k crescono.

In realtà è forse ancora più sorprendente scoprire che Ercole non può evitare di vincere (a patto che non si stanchi di tagliar teste!). Infatti la proposizione che vogliamo provare è che ogni strategia è una strategia vincente. Prima di passare ad analizzare come questo risultato si possa ottenere è forse il caso di notare che l'affermazione "ogni strategia è vincente" è sostanzialmente più forte dell'affermazione "esiste una strategia vincente". Per convincere il lettore di questo, descriviamo un problema più semplice ma per molti aspetti simile a quello della battaglia tra Ercole e l'idra.

5.2.1 Uccidere una lista di numeri

Consideriamo liste finite di numeri naturali. Una riduzione di una lista data si svolge nel modo seguente: al passo n-mo, dove $n \geq 1$, si scegli un elemento positivo k della lista e lo sostituisce con n ripetizioni del valore $k-1$. La riduzione termina quando tutti gli elementi della lista sono zeri. Diremo che una strategia (cioè una regola per scegliere un elemento ad ogni passo) è vincente se per ogni lista iniziale la riduzione che segue tale strategia termina dopo un numero finito di passi.

Per esempio se si inizia con la lista [352031] e scegliamo il quinto elemento, applicare la regola data sopra per $n = 1$ dà come risultato la lista [352021]. Se scegliamo ora il secondo elemento della lista così ottenuta, al termine del secondo passo la riduzione restituisce [3442021].

Mostriamo ora che la strategia *del massimo*, cioè la strategia che consiste nello scegliere ad ogni passo uno degli elementi di valore massimo, è una strategia vincente. Per farlo costruiremo una funzione che ad ogni lista associa un ordinale minore di ω^2. Data una lista sia n_0 il suo massimo e m_0 il numero di volte che n_0 compare nella lista. Allora l'ordinale associato alla lista è $\omega \cdot n_0 + m_0$. È facile vedere che ogni volta che una lista viene ridotta secondo la strategia del massimo il suo ordinale decresce strettamente e quindi la riduzione deve terminare dopo un numero finito di passi. Quindi per mostrare che esiste una strategia vincente è sufficiente l'induzione sugli ordinali minori di ω^2.

Per provare invece che ogni strategia è vincente abbiamo bisogno dell'induzione sugli ordinali minori di ω^ω. Dobbiamo infatti introdurre un'altra funzione che mappa ogni lista in un ordinale nel modo seguente:

- data una lista riordiniamola in modo che sia decrescente.
- se dopo averla riordinata essa si scrive come $[x_0, \ldots, x_k]$, l'ordinale associato è $\omega^{x_0} + \ldots + \omega^{x_k}$.

È abbastanza semplice mostrare che se una lista viene ridotta (scegliendo un qualsiasi elemento), allora anche l'ordinale associato da questa nuova funzione decresce strettamente e quindi si può concludere che ogni strategia è vincente.

5.2.2 Uccidere un'idra

La dimostrazione anche in questo caso, come per il teorema di Goodstein o per le liste di numeri naturali, si basa sull'idea di definire una funzione che associa un ordinale ad ogni idra in modo tale che l'ordinale associa ad un idra sia maggiore dell'ordinale associato all'idra che da questa si ottiene tagliandone una qualsiasi testa.

A questo scopo possiamo assegnare ad un idra un ordinale minore di ϵ_0 nel modo che segue:

- ad ogni foglia assegnamo 0.

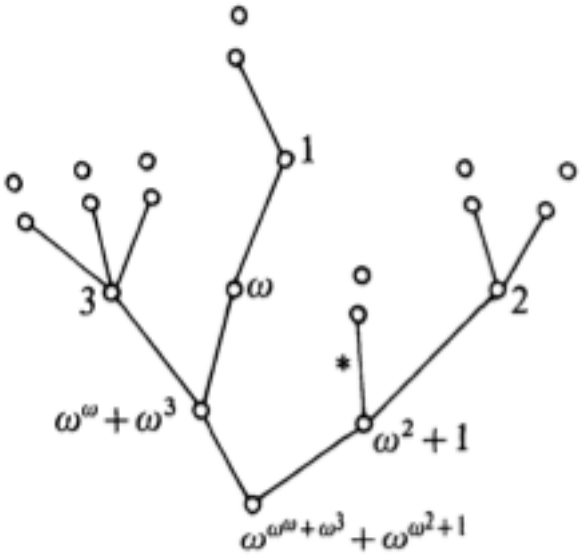

Figura 5.3: assegnazione di ordinali

- Ad ogni altro nodo assegnamo $\omega^{\alpha_i}+\ldots+\omega^{\alpha_n}$, dove $\alpha_1 \geq \ldots \geq \alpha_n$ sono gli ordinali assegnati ai nodi immediatamente "sopra" tale nodo (ricordate che $\omega^0 = 1$).

Un esempio di assegnazione di ordinali ad un idra è quello che si vede in figura 5.3. Infine diremo che l'ordinale di un'idra è quello assegnato alla sua radice. È allora abbastanza facile vedere che qualsiasi sia la testa che si decide di tagliare l'ordinale associato in questo modo all'idra "ridotta" è minore di quello che viene assegnato all'idra di partenza.

Anche se non sviluppiamo la dimostrazione completa della impossibilità di formalizzare nell'aritmetica di Peano questa dimostrazione che richiede di usare l'induzione fino all'ordinale ϵ_0, vale la pena di notare che il modo per vedere che essa non è formalizzabile nell'aritmetica di Peano consiste nel determinare una strategia che si comporti così male che la funzione che associa una particolare idra con il numero di passi necessari per ucciderla utilizzando tale strategia cresce così in fretta da essere al di là di quel che l'aritmetica può formalizzare (si tratta dello stesso problema che avevamo già dovuto affrontare quando abbiamo analizzato la funzione che associa un numero naturale n con il numero di passi necessari alla procedura di Goodstein ad arrivare a 0 partendo da n).

Una strategia di questo genere è la seguente: per decidere quale testa tagliare si parta dalla radice e ci si muova verso l'alto scegliendo sempre il nodo sopra quello dove siamo arrivati cui sia stato assegnato l'ordinale più piccolo (se più di un nodo ha lo stesso ordinale possiamo scegliere quello più a sinistra tra quelli minimi). In questo modo arriviamo prima o poi ad una testa e quella tagliamo. Ad esempio nella figura 5.4 si vedono i primi passi dell'uso di tale strategia sull'idra di figura 5.3.

5.3 Bibliografia

Goodstein, R., *On the restricted ordinal theorem*, Journal of Symbolic Logic, 9 (1944), 33-41.

Kirby, L. and Paris, J., *Accessible independence results for Peano arithmetic*, Bull. London. Math. Soc., 14 (1982), 285-93.

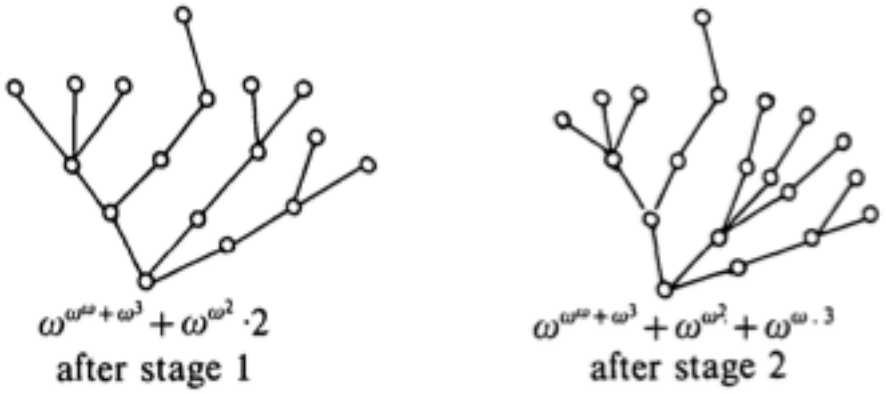

Figura 5.4: i primi passi di una battaglia

Capitolo 6

Assioma della scelta

Rispetto agli altri assiomi della teoria degli insieme ben diversa è la situazione per quanto riguarda l'assioma di scelta; qui non si tratta di escogitare un utile metodo per costruire nuovi insiemi a partire da insiemi vecchi quanto piuttosto della pretesa che esista sempre una funzione in grado di scegliere un elemento da ciascun insieme di una arbitraria famiglia non vuota di insiemi non vuoti.

Da un certo punto di vista l'assioma è del tutto ovvio (sapere che i vari insiemi considerati nella famiglia sono non vuoti vuol dire proprio sapere che contengono un qualche elemento e basta quindi scegliere proprio quello che ci ha convinto che l'insieme non è vuoto).

Pretendere tuttavia di sapere fare questa scelta in generale, per qualsiasi famiglia di insiemi non vuoti e soprattutto senza fissare dei chiari criteri per convincerci che gli insiemi non sono vuoti, è il vero contenuto dell'assioma di scelta.

6.1 Discussione generale sull'assioma di scelta

Ecco alcune considerazioni su tale assioma che abbiamo preso da

`http://www.math.vanderbilt.edu/~schectex/ccc/choice.html`

The *Axiom of Choice* (AC) was formulated about a century ago, and it was controversial for a few of decades after that; it might be considered the last great controversy of mathematics. It is now a basic assumption used in many parts of mathematics. In fact, assuming AC is equivalent to assuming any of these principles (and many others):

- Given any two sets, one set has cardinality less than or equal to that of the other set – i.e., one set is in one-to-one correspondence with some subset of the other. (Historical remark: It was questions like this that led to Zermelo's formulation of AC, see section 6.2.2)
- Any vector space over a field F has a basis – i.e., a maximal linearly independent subset – over that field. (Remark: If we only consider the case where F is the real line, we obtain a slightly weaker statement; it is not yet known whether this statement is also equivalent to AC, see section 7.2)
- Any product of compact topological spaces is compact. (This is now known as Tychonoff's Theorem, though Tychonoff himself only had in mind a much more specialized result that is not equivalent to the Axiom of Choice, see section 9.6)

AC has many forms; here is one of the simplest:

Definition 6.1.1 (Axiom of Choice) *Let C be a nonempty collection of nonempty sets. Then we can choose a member from each set in that collection. In other words, there exists a function f defined on C with the property that, for each set S in the collection, $f(S)$ is a member of S. The function f is then called a* choice function.

To understand this axiom better, let's consider a few examples.

- If C is the collection of all nonempty subsets of $\{1, 2, 3, \ldots\}$, then we can define f quite easily: just let $f(S)$ be the smallest member of S.
- If C is the collection of all intervals of real numbers with positive, finite lengths, then we can define $f(S)$ to be the midpoint of the interval S.

If C is some more general collection of subsets of the real line, we may be able to define f by using a more complicated rule. However, if C is the collection of all nonempty subsets of the real line, it is not clear how to find a suitable function f. In fact, no one has ever found a suitable function f for this collection C, and there are convincing model-theortic arguments that no one ever will. (Of course, to prove this requires a precise definition of "find," etc.)

The controversy was over how to interpret the words "choose" and "exists" in the axiom:

- If we follow the constructivists, and "exist" means "find," then the axiom is false, since we cannot find a choice function for the nonempty subsets of the reals.
- However, most mathematicians give "exists" a much weaker meaning, and they consider the Axiom to be true: To define $f(S)$, just arbitrarily "pick any member" of S.

In effect, when we accept the *Axiom of Choice*, this means we are agreeing to the convention that we shall permit ourselves to use a hypothetical choice function f in proofs, as though it "exists" in some sense, even in cases where we cannot give an explicit example of it or an explicit algorithm for it.

To assert that a mathematical object "exists," even when you cannot give an example of it, is a little bit like this: Suppose that one day you go to a football game by yourself. There are thousands of other people in the stadium, but you don't know the names of any of them. (And let's suppose you're shy, so you're not about to ask anyone their name.) Then you know those people have names, but you cannot give any of those names. (Admittedly, this is only a metaphor, and not a perfect one; don't make too much of it.)

The "existence" of f – or of any mathematical object, even the number "3" – is purely formal. It does not have the same kind of solidity as your table and your chair; it merely exists in the mental universe of mathematics. Many different mathematical universes are possible. When we accept or reject the *Axiom of Choice*, we are specifying something about which mental universe we're choosing to work in. Both possibilities are feasible – i.e., neither accepting nor rejecting AC yields a contradiction; that fact follows from models devised by Gödel and Cohen. However, most "ordinary" mathematicians – i.e., most mathematicians who are not logicians or set theorists – accept the *Axiom of Choice* chiefly because their work is simpler with the *Axiom of Choice* than without it.

Bertrand Russell was more famous for his work in philosophy and political activism, but he was also an accomplished mathematician. His book *Introduction to Mathematical Philosophy* includes some discussion of AC. Here is my paraphrasing of part of what he said:

"To choose one sock from each of infinitely many pairs of socks requires the *Axiom of Choice*, but for shoes the Axiom is not needed."

The idea is that the two socks in a pair are identical in appearance, and so we must make an arbitrary choice if we wish to choose one of them. For shoes, we can use an explicit algorithm – e.g., "always choose the left shoe." Why does Russell's statement mention infinitely many pairs? Well, if we only have finitely many pairs of socks, then AC is not needed – we can choose one member of each pair using the definition of "nonempty," and we can repeat an operation finitely many times using the rules of formal logic.

Jerry Bona once said,

"The *Axiom of Choice* is obviously true; the *Well Ordering Principle* is obviously false; and who can tell about *Zorn's Lemma*?"

This is a joke. In the setting of ordinary set theory, all three of those principles are mathematically equivalent – i.e., if we assume any one of those principles, we can use it to prove the

other two. However, human intuition does not always follow what is mathematically correct. The *Axiom of Choice* agrees with the intuition of most mathematicians; the *Well Ordering Principle* is contrary to the intuition of most mathematicians; and *Zorn's Lemma* is so complicated that most mathematicians are not able to form any intuitive opinion about it.

For another indication of the controversy that initially surrounded the *Axiom of Choice*, consider this anecdote (recounted by Jan Mycielski in Notices of the AMS vol. 53 no. 2 page 209). Tarski, one of the early great researchers in set theory and logic, proved that AC is equivalent to the statement that any infinite set X has the same cardinality as the Cartesian product $X \times X$. He submitted his article to *Comptes Rendus Acad. Sci. Paris*, where it was refereed by two very famous mathematicians, Fréchet and Lebesgue. Both wrote letters rejecting the article. Fréchet wrote that an implication between two well known truths is not a new result. And Lebesgue wrote that an implication between two false statements is of no interest. Tarski said that he never again submitted a paper to the *Comptes Rendus*.

AC permits arbitrary choices from an arbitrary collection of nonempty sets. Some mathematicians have investigated some weakened forms of AC, such as

- CC (Countable Choice), which permits arbitrary choices from a sequence of nonempty sets.
- DC (Dependent Choice), which permits the more general process of selecting arbitrarily from a sequence of nonempty sets where only the first set is specified in advance; each subsequent set of options may depend somehow on the previous choices. This is precisely what is needed for some choice processes in topology and analysis – e.g., for the proof of the Baire Category Theorem.

The full strength of the *Axiom of Choice* does not seem to be needed for applied mathematics. Some weaker principle such as CC or DC generally would suffice. To see this, consider that any application is based on measurements, but humans can only make finitely many measurements. We can extrapolate and take limits, but usually those limits are sequential, so even in theory we cannot make use of more than countably many measurements. The resulting spaces are separable. Even if we use a nonseparable space such as L^∞, this may be merely to simplify our notation; the relevant action may all be happening in some separable subspace, which we could identify with just a bit more effort. (Thus, in some sense, nonseparable spaces exist only in the imagination of mathematicians.) If we restrict our attention to separable spaces, then much of conventional analysis still works with AC replaced by CC or DC. However, the resulting exposition is then more complicated, and so this route is only followed by a few mathematicians who have strong philosophical leanings against AC.

A few pure mathematicians and many applied mathematicians (including, e.g., some mathematical physicists) are uncomfortable with the *Axiom of Choice*. Although AC simplifies some parts of mathematics, it also yields some results that are unrelated to, or perhaps even contrary to, everyday "ordinary" experience; it implies the existence of some rather bizarre, counterintuitive objects. Perhaps the most bizarre is the Banach-Tarski Paradox: It is possible to take the 3-dimensional closed unit ball,

$$B = \{(x, y, z) \in \mathsf{R}^3 \mid x^2 + y^2 + z^2 \leq 1\}$$

and partition it into finitely many pieces, and move those pieces in rigid motions (i.e., rotations and translations, with pieces permitted to move through one another) and reassemble them to form two copies of B.

At first glance, the Banach-Tarski result seems to contradict some of our intuition about physics – e.g., the Law of Conservation of Mass, from classical Newtonian physics. If we assume that the ball has a uniform density, then the Banach-Tarski Paradox seems to say that we can disassemble a one-kilogram ball into pieces and rearrange them to get two one-kilogram balls. But actually, the contradiction can be explained away: Only a set with a defined volume can have a defined mass. A "volume" can be defined for many subsets of R^3 – spheres, cubes, cones, icosahedrons, etc. – and in fact a "volume" can be defined for nearly any subset of R^3 that we can think of. This leads beginners to expect that the notion of "volume" is applicable to every subset of R^3. But it's not. In particular, the pieces in the Banach-Tarski decomposition are sets whose volumes cannot be defined.

More precisely, Lebesgue measure is defined on *some* subsets of R^3, but it cannot be extended to all subsets of R^3 in a fashion that preserves two of its most important properties: the measure of the union of two disjoint sets is the sum of their measures, and measure is unchanged under translation and rotation. The pieces in the Banach-Tarski decomposition are not Lebesgue measurable. Thus, the Banach-Tarski Paradox gives as a corollary the fact that there exist sets that are not Lebesgue measurable. That corollary also has a much shorter proof (not involving the Banach-Tarski Paradox) which can be found in every introductory textbook on measure theory, but it too uses the *Axiom of Choice*.

6.1.1 Alcune formulazioni dell'assioma di scelta

Quelle che seguono sono alcune considerazioni introduttive sull'assioma di scelta prese da

`http://www.science.unitn.it/~vigna/scelta.pdf`

L'assioma della scelta è una di quelle cose a cui tutti credono e che tutti usano senza accorgersene: non ho mai trovato nessuno studente che abbia fatto obiezioni alla semplice dimostrazione del fatto che ogni funzione suriettiva abbia un'inversa a destra; tale inversa viene trovata scegliendo un elemento in ognuno degli insiemi non vuoti costituiti dalle controimmagini degli elementi del codominio. Neanche i matematici fondatori della teoria degli insiemi avevano niente da ridire su questa procedura finchè uno di loro, Zermelo, ha dimostrato nel 1904 che su ogni insieme si può mettere un ordine tale che ogni sottoinsieme non vuoto abbia un primo elemento. Questa è sembrata un po' grossa, tanto più che proprio pochi mesi prima che Zermelo tirasse fuori questa trovata König aveva dimostrato che su R un ordine con tale proprietà non esiste. Il vespaio che ne venne fuori convinse i matematici a guardare con più cura la dimostrazione di Zermelo, e uno di loro, Erhard Schmidt, si accorse che tale prova usava il principio di poter pescare un elemento in ogni insieme non vuoto anche se la famiglia di tali insiemi è infinita. Quando si rese conto di aver usato questo fatto (a cui aveva abboccato esattamente come gli studenti del primo anno abboccano alla dimostrazione dell'esistenza dell'inversa destra delle funzioni suriettive) Zermelo produsse un'altra dimostrazione del suo teorema citato sopra molto più semplice dell'originale. È la dimostrazione riportata in queste note. Per la cronaca König, stimolato dal trambusto, si accorse dell'errore della sua dimostrazione. Dopo questa erudita dissertazione storica veniamo alla matematica.

Teorema 6.1.2 *I seguenti tre enunciati sono equivalenti:*

- *(AC_1) Siano X un insieme non vuoto e $\mathcal{P}^*(X) = \mathcal{P}(X) - \{\emptyset\}$ l'insieme delle parti non vuote di X. Allora esiste una funzione, detta* funzione di scelta, *$f : \mathcal{P}^*(X) \to X$ tale che $f(A) \in A$, per ogni $A \in \mathcal{P}^*(X)$. In altre parole si può scegliere un elemento in ogni sottoinsieme non vuoto di X.*
- *(AC_2) Ogni funzione suriettiva ha un'inversa a destra; cioè se A, B sono insiemi e $g : A \to B$ è suriettiva allora esiste $h : B \to A$ tale che $g \circ h(b) = b$, per ogni $b \in B$.*
- *(AC_3) Siano I, X insiemi non vuoti e $A : I \to \mathcal{P}^*(X)$ una funzione; allora il prodotto cartesiano $\Pi_{i\in I} A_i$ non è vuoto.*

Dimostrazione Per dimostrare l'equivalenza seguiamo questo schema:

$$\mathsf{AC}_1 \Rightarrow \mathsf{AC}_2 \Rightarrow \mathsf{AC}_3 \Rightarrow \mathsf{AC}_1.$$

- ($\mathsf{AC}_1 \Rightarrow \mathsf{AC}_2$) È facile perché $g^{-1}(b) \in \mathcal{P}^*(X)$, per ogni $b \in B$ e, se f è una funzione di scelta, basta porre $h(b) = f(g^{-1}(b))$, per ogni $b \in B$ e siamo a posto.
- ($\mathsf{AC}_2 \Rightarrow \mathsf{AC}_3$) Ricordiamo innanzitutto che

  $$\Pi_{i\in I} A_i = \{f : I \to \bigcup_{i\in I} A_i \mid f(i) \in A_i, \text{ per ogni } i \in I\}$$

  Definiamo $A'_i = A_i \times \{i\}$ e sia $g : \bigcup_{i\in I} A'_i \to I$ definita da $g(x, i) = i$; allora g è suriettiva perché per ogni $i \in I$, $A_i \neq \emptyset$ e quindi, per AC_2, g ha un'inversa a destra h la quale soddisfa quindi $h(i) \in A'_i$ per ogni $i \in I$; basta allora porre $f(i) = \mathsf{pr}_1(h(i))$ dove $\mathsf{pr}_1 : \bigcup_{i\in I} A'_i \to \bigcup_{i\in I} A_i$ è data da $\mathsf{pr}_1(x, i) = x$ e siamo a posto.

- ($\mathsf{AC}_3 \Rightarrow \mathsf{AC}_1$) Grazie a AC_3 sappiamo che $\Pi_{A\in\mathcal{P}^*(X)}A \neq \emptyset$ cioè esiste $f : \mathcal{P}^*(X) \to \bigcup_{A\in\mathcal{P}^*(X)} A = X$ tale che $f(A) \in A$ per ogni $A \in \mathcal{P}^*(X)$. Ecco trovata una funzione di scelta.

Chiameremo assioma della scelta, e lo indicheremo con AC uno qualunque dei tre enunciati equivalenti appena visti.

6.2 Alcuni equivalenti dell'assioma della scelta

Per convincerci dell'ambiguità contenuta nell'enunciato della'*assioma della scelta* proveremo a studiarne delle formulazioni equivalenti o delle conseguenze che possono essere più o meno convincenti.

6.2.1 Assioma di scelta implica Lemma di Zorn

Parliamo ora di insiemi ordinati. Sia $(X, \leq)$ un insieme parzialmente ordinato. Un sottoinsieme C non vuoto di X è detto *catena* se è totalmente ordinato dalla relazione $\leq$, cioè presi comunque due elementi x e y in X o $x \leq y$ o $y \leq x$. Un elemento $x \in X$ viene detto *elemento massimale* se non esiste $y \in X$ tale che $y > x$. Se C è un sottoinsieme non vuoto di X e $x \in X$ si dice che x è un maggiorante di C se, per ogni $y \in C$, $y \leq x$; si dice che $a \in C$ è il *primo elemento* di C se, per ogni $y \in C$, $a \leq y$.

Per esempio

- se A è un insieme non vuoto e $X = \mathcal{P}(A) - \{A\}$ è ordinato mediante l'inclusione allora gli insiemi della forma $A - \{a\}$, per qualche $a \in A$, sono tutti e soli gli elementi massimali e l'insieme vuoto è il primo elemento di X.
- Il primo elemento di Nat con il solito ordine è 0 mentre Z e l'insieme dei numeri reali positivi non hanno primo elemento.
- 21 è un maggiorante per il sottoinsieme di Z formato dai numeri interi negativi.
- Ogni sottoinsieme di un insieme totalmente ordinato è una catena.

$(X, \leq)$ è detto *induttivo* se ogni sua catena ha un maggiorante. $(X, \leq)$ è detto *bene ordinato* e $\leq$ un *buon ordine* su X se ogni sottoinsieme non vuoto di X ha un primo elemento.

Il lemma di Zorn afferma che:

Lemma 6.2.1 (Lemma di Zorn) *Se X è un insieme non vuoto su cui è definita una relazione d'ordine parziale tale che ogni sua catena possiede un maggiorante, allora contiene almeno un elemento massimale.*

Cenno storico e ruolo

Il lemma di Zorn viene detto anche Lemma di Kuratowski-Zorn; in effetti esso fu scoperto da Kazimierz Kuratowski nel 1922 e riscoperto indipendentemente da Max Zorn nel 1935.

Si dimostrò poi che il Lemma di Zorn è equivalente all'assioma della scelta e al teorema del buon ordinamento. Più precisamente, assunto il sistema di assiomi di Zermelo-Fraenkel, se si assume anche uno dei tre suddetti enunciati si possono dedurre i due rimanenti.

In conseguenza dei lavori di Kurt Gödel e di Paul Cohen si è dimostrato che l'assioma della scelta (o equivalentemente il lemma di Zorn, oppure il principio di buon ordinamento) è logicamente indipendente da un sistema di assiomi per la teoria degli insiemi, ad esempio dagli assiomi di Zermelo-Fraenkel. Risulta impossibile da questi assiomi dimostrare il lemma di Zorn o la sua negazione; quindi si possono avere teorie degli insiemi che includono il lemma di Zorn e altre che includono la sua negazione.

Nella maggior parte dei lavori matematici che affrontano queste tematiche generali il lemma di Zorn viene richiesto, in quanto esso rende possibile stabilire un insieme più ampio di proprietà e di individuare una gamma più estesa di oggetti matematici che conducono a costruzioni teoriche più soddisfacenti, cioè a sistemi di teoremi con caratteristiche di maggiore completezza. Ad esempio grazie all'assunzione del lemma di Zorn si possono enunciare il teorema di Hahn-Banach in analisi

funzionale, l'esistenza di una base per ogni spazio vettoriale, il teorema di Tychonoff in topologia, cioè la compattezza di ogni prodotto di spazi compatti, l'esistenza di un ideale massimale per ogni anello e il fatto che ogni campo possiede una chiusura algebrica.

Dimostrazione del lemma di Zorn con l'assioma della scelta

L'idea della dimostrazione consiste nel trovare le catene "più lunghe possibile" visto che il loro maggiorante, che esiste per ipotesi, dovrà essere un elemento massimale perché altrimenti la catena si potrebbe estendere.

Dato un insieme X su cui sia definita una relazione d'ordine $\leq$, per l'assioma della scelta (applicato all'insieme delle parti non vuote di X) sappiamo che esiste una funzione di scelta $f : \mathcal{P}^*(X) \to X$ tale che, per ogni $Y \in \mathcal{P}^*(X)$, $f(Y) \in Y$.

Data allora una tale f, definiamo *f-catena* una catena C su X tale che:

- $(C, <)$ sia ben ordinata
- per ogni $a \in C$, $a = f(\{x \in X \mid (\forall b \in C)\ b < a \to x > b\})$

ovvero ogni elemento della catena è l'immagine tramite f dell'insieme non vuoto degli elementi che maggiorano tutti gli elementi precedenti nella catena.

Per capire che tra le catene di X ci sono delle f-catene possiamo considerare la catena costituita dal solo elemento $f(X)$, la catena costituita da $f(X)$ e $f(\{x \in X \mid f(X) < x\})$ e in generale tutte le catene che si possono ottenere, partire dall'insieme vuoto, aggiungendo ogni volta un elemento scelto nell'insieme dei maggioranti degli elementi già aggiunti.

Si verifica facilmente che date due f-catene C e D una sarà sempre un segmento iniziale dell'altra, e quindi che un'unione di f-catene è ancora una f-catena.

Sia ora F l'unione di tutte le f-catene contenute in X. F sarà una f-catena. Supponiamo che ogni catena abbia un maggiorante (ipotesi del Lemma di Zorn): allora in particolare esiste un m maggiore o uguale a tutti gli elementi di F. Ma se esistesse $n \in X$ tale che $n > m$, avremmo che l'insieme M dei maggioranti di m (e quindi di ogni elemento di F) è non vuoto (contiene almeno n) e quindi la catena ottenuta estendendo F con l'elemento $f(M)$ è una f-catena. Ma questo è un assurdo perché F è definito come l'unione di *tutte* le f-catene.

6.2.2 Lemma di Zorn implica buon ordinamento

L'assioma della scelta ha conseguenze sorprendenti. Una di queste è il teorema di buon ordinamento. Un *buon ordinamento* su un insieme X è un ordinamento con la proprietà che ogni sottoinsieme non vuoto di X ha minimo. Un *insieme bene ordinato* è un insieme munito di un buon ordinamento. Ad esempio Nat, con l'ordinamento usuale, è bene ordinato; questo equivale al principio di induzione (esercizio).

Teorema 6.2.2 (Teorema del buon ordinamento) *Ogni insieme ammette un buon ordinamento.*

La dimostrazione che daremo usa il lemma di Zorn. Sia X un insieme non vuoto, e sia $\mathcal{X}$ l'insieme delle coppie $(A, \leq_A)$, dove A è un sottoinsieme non vuoto di X e $\leq_A$ è un buon ordinamento su A. L'insieme $\mathcal{X}$ non è vuoto, perché i singoletti $\{a\}$, per $a \in X$, muniti dell'unico ordine possibile, i.e. $a \leq a$, ci appartengono.

Introduciamo un ordinamento su $\mathcal{X}$ ponendo $(A, \leq_A) \preccurlyeq (B, \leq_B)$ se e solo se $A \subseteq B$, la restrizione di $\leq_B$ ad A è $\leq_A$, e inoltre $x \leq_B y$ ogni volta che $x \in A$ e $y \in B - A$.

Vediamo che $\mathcal{X}$ è induttivo, cioè ogni catena su $\mathcal{X}$ ha un maggiorante. Sia $\mathcal{C}$ una catena in $\mathcal{X}$. Poniamo $A = \bigcup_{(C, \leq_C) \in \mathcal{C}} C$. Consideriamo poi gli ordinamenti $\leq_C$ come relazioni su C, cioè come sottoinsiemi di $C \times C$ e definiamo un ordinamento su A ponendo $\leq_A = \bigcup_{(C, \leq_C) \in \mathcal{C}} \leq_C$. È chiaro che $\leq_A$ è un ordinamento totale su A che, per ogni $(C, \leq_C) \in \mathcal{C}$, induce l'ordinamento $\leq_C$ su C.

Mostriamo ora che $\leq_A$ è anche un buon ordinamento su A (e quindi che $(A, \leq_A)$ è un maggiorante nell'ordine $\preccurlyeq$ per la catena $\mathcal{C}$). Supponiamo quindi che D sia un sottoinsieme non vuoto di A e vediamo che esso ha minimo rispetto all'ordine $\leq_A$. Supponiamo quindi che x sia un qualsiasi elemento di D. Allora esiste $(C_1, \leq_{C_1}) \in \mathcal{C}$ tale che $x \in C_1$. Se adesso consideriamo un qualsiasi y di D

tale che $y \leq_A x$, abbiamo che esiste $(C_2, \leq_{C_2}) \in \mathcal{C}$ tale che $y \in C_2$. Vediamo allora che deve aversi $y \in C_1$. Infatti sia $(C_1, \leq_{C_1})$ che $(C_2, \leq_{C_2})$ stanno nella catena $\mathcal{C}$ e quindi o $(C_2, \leq_{C_2}) \preccurlyeq (C_1, \leq_{C_1})$, e in questo caso y appartiene a C_1 perché $C_2 \subseteq C_1$, o $(C_1, \leq_{C_1}) \preccurlyeq (C_2, \leq_{C_2})$, e y deve comunque appartenere ad C_1 altrimenti, per la definizione dell'ordinamento $\preccurlyeq$ su $\mathcal{X}$, non potrebbe essere minore di x.

Quindi tutti gli elementi y di D tali che $y \leq_A x$ stanno in C_1 e sono tali che $y \leq_{C_1} x$; ma $\leq_{C_1}$ è un buon ordine per cui l'insieme degli elementi di D che stanno in C_1 hanno minimo rispetto alla relazione $\leq_{C_1}$ ma tale minimo è un minimo anche rispetto alla relazione $\leq_A$ visto $\leq_{C_1} \subseteq \leq_A$.

È ora chiaro che $(A, \leq_A)$ è l'estremo superiore di $\mathcal{C}$. Dunque $\mathcal{X}$ è induttivo, e quindi per il Lemma di Zorn ammette un elemento massimale $(F, \leq_F)$. Se F fosse strettamente contenuto in X, cioè se vi fosse un elemento x di X non appartenente a F, potremmo estendere F a un ordinamento di $F \cup \{x\}$ imponendo a x di seguire ogni elemento di F. Questo sarebbe un buon ordinamento su $F \cup \{x\}$, contro la massimalità di $(F, \leq_F)$. In conclusione, $\leq_F$ è un buon ordinamento su $X (= F)$.

Vale la pena di osservare che il sapere che, sotto l'ipotesi dell'assioma della scelta, ogni insieme è ben ordinabile risolve il problema di Zermelo che voleva essere in grado di confrontare la cardinalità di due insieme qualsiasi per vedere quale dei due è più grande dell'altro. Basta infatti ben ordinarli e confrontare quindi i buoni ordini così ottenuti.

6.2.3 Buon ordinamento implica assioma della scelta

Dimostriamo infine che se ogni insieme è bene ordinabile, vale l'assioma della scelta. Data una famiglia non vuota F di insiemi non vuoti, vorremmo trovare una funzione $f : F \to \bigcup_{X \in F} X$ tale che, per ogni $X \in F$, $f(X) \in X$.

Ma su $\bigcup_{X \in F} X$ possiamo stabilire un buon ordine $<$. Allora, per la definizione di buon ordine, dato un insieme $X \in F$, che è un sottoinsieme di $\bigcup_{X \in F} X$, possiamo trovarne un elemento minimo. Allora

$$f(X) = \mathsf{min}(X)$$

è una funzione di scelta, dato che è definita per ogni $X \in F$ e $f(X) \in X$.

Capitolo 7

Prime conseguenze dell'assioma di scelta

L'assioma di scelta ha varie conseguenze nello sviluppo dell'intera matematica. Già nel precedente capitolo abbiamo visto alcuni suoi equivalenti. In questo capitolo vedremo alcune delle sue conseguenze più immediate mentre rimandiamo ai prossimi capitoli quei risultati che per essere presentati richiedono un po' di lavoro preliminare per richiamare le nozioni necessarie.

Early applications of AC include:

- Every infinite set has a denumerable subset. This principle, again weaker than AC, cannot be proved without it in the context of the remaining axioms of set theory.
- Every infinite cardinal number is equal to its square. This was proved equivalent to AC in Tarski 1924.
- Every vector space has a basis (initiated by Hamel 1905). This was proved equivalent to AC in Blass 1984.
- Every field has an algebraic closure (Steinitz 1910). This assertion is weaker than AC, indeed is a consequence of the (weaker) compactness theorem for first-order logic (see below).
- There is a Lebesgue nonmeasurable set of real numbers (Vitali 1905). This was shown much later to be a consequence of BPI (see below) and hence weaker than AC. Solovay (1970) established its independence of the remaining axioms of set theory.

A significant "folklore" equivalent of AC is

The Set-Theoretic Distributive Law. For an arbitrary doubly-indexed family of sets $\{M_{i,j} \mid i \in I, j \in J\}$, and where J^I is the set of all functions with domain I and which take values in J:

$$\bigcap_{i\in I}\bigcup_{j\in J} M_{i,j} = \bigcup_{f\in J^I}\bigcap_{i\in I} M_{i,f(i)}$$

A much-studied special case of AC is the

Principle of Dependent Choices (Bernays 1942, Tarski 1948). For any nonempty relation R on a set A for which $\mathsf{range}(R) \subseteq \mathsf{domain}(R)$, there is a function $f : \omega \to A$ such that, for all $n \in \omega$, $R(f(n), f(n+1))$.

This principle, although (much) weaker than AC, cannot be proved without it in the context of the remaining axioms of set theory.

Mathematical equivalents of AC include:

- Tychonov's Theorem (1930): the product of compact topological spaces is compact. This was proved equivalent to AC in Kelley 1950. But for compact Hausdorff spaces it is equivalent to BPI (see below) and hence weaker than AC

- Löwenheim-Skolem-Tarski Theorem (Löwenheim 1915, Skolem 1920, Tarski and Vaught 1957): a first-order sentence having a model of infinite cardinality α also has a model of any infinite cardinality β such that $\beta \leq \alpha$. This was proved equivalent to AC by Tarski.
- Every distributive lattice has a maximal ideal. This was proved equivalent to AC in Klimovsky 1958, and for lattices of sets in Bell and Fremlin 1972.
- Every commutative ring with identity has a maximal ideal. This was proved equivalent to AC by Hodges 1979.

There are a number of mathematical consequences of AC which are known to be weaker than it, in particular:

- The Boolean Prime Ideal Theorem (BPI): every Boolean algebra has a maximal (or prime) ideal. This was shown to be weaker than AC in Halpern and Levy 1971.
- The Stone Representation Theorem for Boolean algebras (Stone 1936): every Boolean algebra is isomorphic to a field of sets. This is equivalent to BPI and hence weaker than AC
- Compactness Theorem for First-Order Logic (Gödel 1930, Malcev 1937, others): if every finite subset of a of a set of first-order sentences has a model, then the set has a model. This was shown, in Henkin 1954, to be equivalent to BPI, and hence weaker than AC.
- Completeness Theorem for First-Order Logic (Gödel 1930, Henkin 1954): each consistent set of first-order sentences has a model. This was shown by Henkin in 1954 to be equivalent to BPI, and hence weaker than AC.

7.1 Assioma di scelta e ultrafiltri

Quanto segue è preso da ???

I want to classify all subsets of $\{1, 2, 3, 4, 5, \ldots\}$ as "small" or not "small," defining the word "small" in such a way that

1. any set with zero or one members is "small";
2. any union of two "small" sets is "small"; and
3. a set is "small" if and only if its complement isn't "small."

Now, without much difficulty I can give examples satisfying any two of those three rules:

- Define "small" to mean "finite." This satisfies rules 1 and 2. But it does not satisfy rule 3, since the even numbers and the odd numbers are complements of each other, and neither of those sets is finite.
- Say that a set is "small" if the number 1 is not a member of that set. This definition satisfies rules 2 and 3, but it classifies the set $\{1\}$ as "not small," thus failing rule 1.
- Say that a set is "small" if it contains at most one of the three numbers 1, 2, 3. That satisfies rules 1 and 3. But it classifies the sets $\{1\}$ and $\{2\}$ as small and the set $\{1, 2\}$ as not small, thus failing rule 2.

Does there exist a classification scheme satisfying all three rules? It turns out that such a classification scheme exists, but an example of such a classification scheme does not exist (which makes it a bit hard to visualize!). And by that I do not mean just that we haven't found an example yet. I mean that the proofs of existence are inherently nonconstructive – i.e., they cannot be replaced by constructive proofs – so no examples can ever be given. But the proof of that fact is very deep, and it raises interesting philosophical questions: In what sense does that classification scheme "exist"? (My own attitude is that I'm not really working with the classification schemes themselves; I'm just working with sentences about hypothetical classification schemes.)

To prove the existence of such a classification scheme, just call "large" the members of some nonprincipal ultrafilter on the positive integers, and call their complements "small." Note that, with this scheme, any superset of a "large" set is also "large." The converse is slightly more complicated: If you have a "small/large" classification, the "large" sets do not necessarily form a nonprincipal ultrafilter, but the supersets of "large" sets do. An introduction to nonprincipal ultrafilters can be found in my book and in many other places in the literature.

The existence of nonprincipal ultrafilters follows easily from Zorn's Lemma, by arguments that will be obvious once you've digested all definitions involved (admittedly not a small task).

La questione è infatti quella di capire quali sono le proprietà rilevanti per decidere se un sottoinsieme dei numeri naturali N è *grande*.

Sicuramente non ci sono troppi problemi a decidere che se chiamiamo G la collezione dei sottoinsiemi *grandi* di N le seguenti proprietà dovrebbero valere (si ricordi che un sottoinsieme di N è *co-finito* se e solo se il suo complementare è finito):

$$\text{(cofinitezza)} \qquad \frac{X \text{ co-finito}}{X \in G}$$

$$\text{(chiusura in su)} \qquad \frac{X \in G \qquad X \subseteq Y}{Y \in G}$$

$$\text{(consistenza)} \qquad \emptyset \notin G$$

Appena un po' più difficile è riconoscere che anche la seguente proprietà dovrebbe essere soddisfatta dai sottoinsiemi *grandi*

$$\text{(completezza)} \qquad \frac{X \cup Y \in G}{X \in G \text{ oppure } Y \in G}$$

visto che essa sostiene che mettendo assieme due cose *piccole* non posso ottenere qualcosa di *grande*.

In conseguenza di questa proprietà otteniamo subito che X sta in G oppure ci sta il suo complemento X^C visto che tutto l'insieme N sta sicuramente in G in quanto è un co-finito.

Sembra inoltre ragionevole pretendere che il complemento di un insieme *grande* non sia a sua volta *grande*, cioè che G deva essere in grado di decidere sempre tra un sottoinsieme ed il suo complemento visto che uno dei due lo deve prendere ma non entrambi (cosa potrà mai fare con i pari e i dispari lo sa solo G!)

Da queste proprietà si deduce immediatamente (esercizio) la

$$\text{(chiusura per intersezione)} \qquad \frac{X \in G \quad Y \in G}{X \cap Y \in G}$$

che sostiene che l'intersezione di due sottoinsiemi *grandi* è ancora un sottoinsieme *grande* (proprietà questa non del tutto intuitiva).

Nel seguito chiameremo *filtro proprio* una famiglia non vuota di sottoinsiemi di N che, come G, soddisfa *chiusura in su*, *chiusura per intersezione* e *consistenza* e *ultrafiltro* un filtro proprio che soddisfi anche *completezza* o equivalentemente il fatto che un sottoinsieme o il suo complemento vi appartengono (esercizio: verificare l'equivalenza tra queste due condizioni).

Quindi se consideriamo la collezioni di tutti i filtri sull'insieme delle parti di N essa può essere ordinata dall'inclusione e gli ultrafiltri sono gli elementi massimali in tale relazione d'ordine (esercizio: verificare quest'ultima affermazione facendo vedere che nessun sottoinsieme di numeri naturali può essere aggiunto ad un ultrafiltro senza distruggerne la consistenza).

Quindi la questione adesso è come fare per costruire un ultrafiltro che contenga tutti i sottoinsiemi cofiniti e la soluzione ci viene dal lemma di Zorn.

Non è infatti difficile vedere che la collezione di tutti i sottoinsiemi cofiniti di numeri naturali è un filtro proprio (esercizio). Richiede invece un po' di lavoro in più verificare che l'unione di una qualsiasi catena di filtri contenenti i cofiniti (ordinata per inclusione) è a sua volta un filtro proprio (esercizio) e quindi che ogni catena ha un maggiorante.

Ma appena fatto questo lavoro il lemma di Zorn può fare la sua *magia* e assicurarci dell'esistenza di una collezione massimale di sottoinsiemi di numeri naturali che gode di tutte le proprietà che abbiamo richiesto per G.

But showing that the existence proof is inherently nonconstructive is much harder, and requires some definitions that I've made up. By an "example" I mean anything whose existence can be proved using just ZF+DC — that is, I'll allow Dependent Choice but no higher relatives of AC.

Let BP be the statement that "every subset of the reals has the Baire property." The existence of a nonpricipal ultrafilter on the integers implies not-BP (by fairly straightforward functional analysis and topology). But in 1984 Shelah proved that the consistency of ZF implies the consistency of ZF + DC + BP. Therefore, if ordinary set theory is free of contradictions, then ZF + DC cannot be used to prove ¬BP. I say "if" because we don't know that for sure, and Gödel's Incompleteness Theorem assures us that we never will know the consistency of ZF for sure. However, I would say that ZF is *empirically consistent*: In a century of study, mathematicians have not yet found any contradictions in ZF, despite the incentive that any mathematician finding such an important proof would instantly be promoted to full professor at any university in the world.

7.2 Assioma di scelta e base di uno spazio vettoriale

In matematica, e più precisamente in algebra lineare, la base di uno spazio vettoriale è un insieme di vettori linearmente indipendenti che generano lo spazio. In modo equivalente, ogni elemento dello spazio vettoriale può essere scritto in modo unico come combinazione lineare dei vettori appartenenti alla base.

Se la base di uno spazio vettoriale è composta da un numero finito di elementi allora la dimensione dello spazio è finita. In particolare, il numero di elementi della base è la dimensione dello spazio.

7.2.1 Definizione

Sia V uno spazio vettoriale su un campo K. L'insieme $\{v_1, v_2, \ldots, v_n\}$ di elementi di V è una base di V se valgono entrambe le seguenti proprietà:

- I vettori v_1, v_2, …, v_n sono linearmente indipendenti in K, ovvero
$$\Sigma_{i=1}^{n} a_i v_i = a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0$$
è verificata solo se i numeri a_1, a_2, …, a_n sono tutti uguali a zero.
- I vettori v_1, v_2, …, v_n generano V, ovvero:
$$V = \{a_1 v_1 + a_2 v_2 + \ldots + a_n v_n \mid a_1, a_2, \ldots, a_n \in K\}$$
In particolare, per ogni vettore v di V i numeri a_1, a_2, …, a_n sono le sue *coordinate* rispetto alla base scelta.

Si dice anche che i vettori v_1, v_2, …, v_n appartenenti ad una qualsiasi base di V costituiscono un sottoinsieme massimale di vettori linearmente indipendenti dello spazio. Questo significa che i vettori v_1, v_2, …, v_n sono tali che esistono a_1, a_2, …, a_n tali che:

$$\Sigma_{i=1}^{n} a_i v_i + w = 0 \qquad \text{per ogni } w \in V \text{ diverso da tutti i } v_i \text{ della base}$$

ovvero l'aggiunta al sottoinsieme massimale di un qualsiasi altro elemento dello spazio determina la dipendenza lineare degli elementi del sottoinsieme.

Una base è dunque composta dal minimo numero di vettori linearmente indipendenti che genera lo spazio. Un insieme di infiniti elementi possiede infinite possibili basi diverse.

7.2.2 Dimensione di uno spazio vettoriale

Uno spazio vettoriale in generale non ha una sola base, e solitamente si trattano spazi con infinite basi possibili. Il teorema della dimensione per spazi vettoriali afferma che tutte le possibili basi di uno stesso spazio hanno la stessa cardinalità, sono formate cioè sempre dallo stesso numero di vettori. Questo numero è la dimensione dello spazio, e permette di definire spazi di dimensione arbitrariamente alta. La dimensione dello spazio è inoltre pari sia al massimo numero di vettori indipendenti che esso contiene, sia al minimo numero di vettori necessari per generare lo spazio stesso.

Esistenza

Qualsiasi sia lo spazio vettoriale V, è sempre possibile trovarne una base. La dimostrazione richiede l'uso del lemma di Zorn nel caso generale, mentre nel caso particolare degli spazi finitamente generati esistono dimostrazioni più semplici.

Si consideri la collezione $I(V)$ dei sottoinsiemi di V linearmente indipendenti. È immediato dedurre che l'inclusione è un ordine parziale su $I(V)$, e che per ogni catena $\{B_i\}$ l'insieme $\bigcup_i B_i$ ne è un maggiorante (è linearmente indipendente in quanto unione di elementi di una catena ordinata per inclusione). Applicando il lemma di Zorn, esiste un insieme massimale linearmente indipendente B in $I(V)$. Dunque B è una base, infatti se $v \in V$ ma non appartiene a B allora per la massimalità di B l'insieme $B \cup \{v\}$ deve essere linearmente dipendente, cioè esistono degli scalari a_1, a_2, ..., a_n non tutti nulli tali che

$$av + \Sigma_{i=1}^{n} a_i w_i = 0 \qquad \text{per ogni } w_i \in B$$

con $a \neq 0$, dal momento che se fosse nulla allora anche gli altri a_i dovrebbero esserlo, essendo gli elementi di B linearmente indipendenti. Quindi v può essere scritto come combinazione lineare finita di elementi di B, che oltre a essere linearmente indipendenti generano V. Dunque B è una base.

Capitolo 8

Assioma di scelta, aree e volumi

Quanto segue è preso da "La matematica del novecento" di P. Odifreddi.

A volte parliamo di oggetti in matematica senza conoscerne l'esatta definizione. Proviamo a capire di più il concetto di area (intesa come misura).

8.1 Il concetto di area

Euclide non ha mai dato una definizione di area né di una sua misura. Enunciò alcune "nozioni comuni" dalle quali si deducono le seguenti proprietà:

1. (invarianza) superfici uguali hanno aree uguali;
2. (addittività finita) sommando fra loro un numero finito di superfici si ottiene una superficie che ha un'area pari alla somma delle aree di quelle;
3. (monotonicità) una superficie contenuta in un'altra ha un'area minore o uguale di questa.

In base a queste proprietà è possibile assegnare un'area ad ogni poligono:

1. dividendo (scomponendo) il poligono in tanti triangoli;
2. calcolando l'area di ciascun triangolo;
3. sommando le loro aree

Il fatto è che Euclide non dimostrò in modo rigoroso (in verità non dimostrò in alcun modo) che l'area di un triangolo non dipende dalla scelta della base e dell'altezza, e che l'area di un poligono non dipende dal modo con cui si viene scomposto in triangoli. Per una rigorosa sistemazione della geometria euclidea dobbiamo aspettare il 1899, anno in cui David Hilbert pubblicò i "Fondamenti della geometria" ("Grundlagen der Geometrie").

A tale proposito è interessante riportare il teorema pubblicato nel 1833 da Janos Bolyai: "Due poligoni che hanno la stessa area si possono decomporre in un numero finito di triangoli equivalenti".

In particolare ogni poligono si può "quadrare", cioè si può scomporre in un numero finito di triangoli che ricomposti costituiscono un quadrato.

Questo nel piano. E nello spazio? Vale un teorema analogo a quello di Bolyai? È possibile, cioè, decomporre un poliedro in un numero finito di tetraedri di modo che ricomposti diano un cubo con lo stesso volume? (questo rappresenta il "terzo problema di Hilbert"). La risposta fu data da Max Dehn, il quale dimostrò che non è possibile nemmeno per i tetraedri stessi.

8.1.1 Nozione generale di misura di Peano-Jordan

Venne spontaneo porsi il problema (siamo già alla fine dell'800) di come calcolare l'area di una superficie il cui bordo è curvilineo. Nel 1887 Giuseppe Peano e poi nel 1893 Camille Jordan introdussero la seguente nozione generale:

Data una figura curvilinea, la sua area può approssimarsi mediante poligoni, sia dall'interno, sia dall'esterno. Essa è compresa tra le aree di queste approssimazioni, e se queste tendono ad uno stesso limite, allora l'area della figura curvilinea coinciderà con questo limite.

A tale proposito è opportuno ricordare:

- Metodo di esaustione: usato prima da Eudosso (IV sec.a.C.) e poi da Archimede nel 225 a.C., per calcolare l'area del cerchio e la superficie della sfera.
- L'integrale di RIEMANN (mediante rettangoli): introdotto da Bernhard Riemann nel 1854, che permette di calcolare l'area di una figura curvilinea il cui bordo sia delimitato da funzioni continue.

  In realtà dal '600 all'800 si dava per scontato l'esistenza dell'area di una superficie e l'integrale era uno strumento per calcolarla.
- A. Cauchy nel 1823 pensò bene di definire l'area come l'integrale stesso.

  Ma questo non bastò finché c'erano funzioni che non erano integrabili (si pensi alle funzioni con infinite discontinuità). Ci si accorse che era necessario precisare una misura dell'insieme di discontinuità. La nozione di Peano-Jordan non era più sufficiente.
- Ci pensò nel 1902 H. Lebesgue con il concetto di "misura di Lebesgue".

  L'additività finita di Euclide fu sostituita con l'additività numerabile: "Sommando fra loro una quantità numerabile di superfici dà una superficie con un'area uguale alla somma delle aree di quelle".

  Oggi i matematici considerano una superficie dotata di area quand'essa è misurabile secondo Lebesgue. L'integrale di Riemann è un caso particolare della nozione di misura secondo Peano- Jordan; l'integrale di Lebesgue è un caso particolare della misura di Lebesgue.
- Ne deriva che le funzioni integrabili secondo Riemann sono integrabili anche secondo Lebesgue, mentre ci sono integrali di Lebesgue che non sono di Riemann.

  Dunque la nozione di misura di Lebesgue è più generale rispetto a tutte le definizioni precedenti.

8.2 Rettificazioni e quadrature

Quanto segue è preso da ???

Il problema che vogliamo affrontare in questa pagina è composto da due parti:

1. data una linea piana di lunghezza finita, costruire, con riga e compasso, un segmento avente la stessa lunghezza (rettificazione di una linea);
2. data una regione piana di area finita, costruire, con riga e compasso, un quadrato avente la stessa area della regione (quadratura di una regione piana).

Tratteremo questo problema solo a livello elementare, per cui supporremo che le linee e le regioni in esame siano prive di patologie strane. In particolare ci occuperemo di regioni con contorno costituito da segmenti o archi di cerchio, in numero finito. In molti casi ci limiteremo a semplici commenti alle figure proposte. Segnaliamo altresì che le costruzioni proposte non sono le uniche possibili e invitiamo lo studente a cercarne altre, magari più efficienti.

Problema 1: Data una spezzata con un numero finito di lati costruire un segmento avente la stessa lunghezza

Si tratta di un problema di banale soluzione: basta riportare ciascun lato della spezzata su una retta come indicato nella figura 8.1 (attenzione però alla questione del "compasso molle", vedi sezione 8.3). Questa costruzione permette di rettificare il contorno di un qualunque poligono (problema della misura di un perimetro).

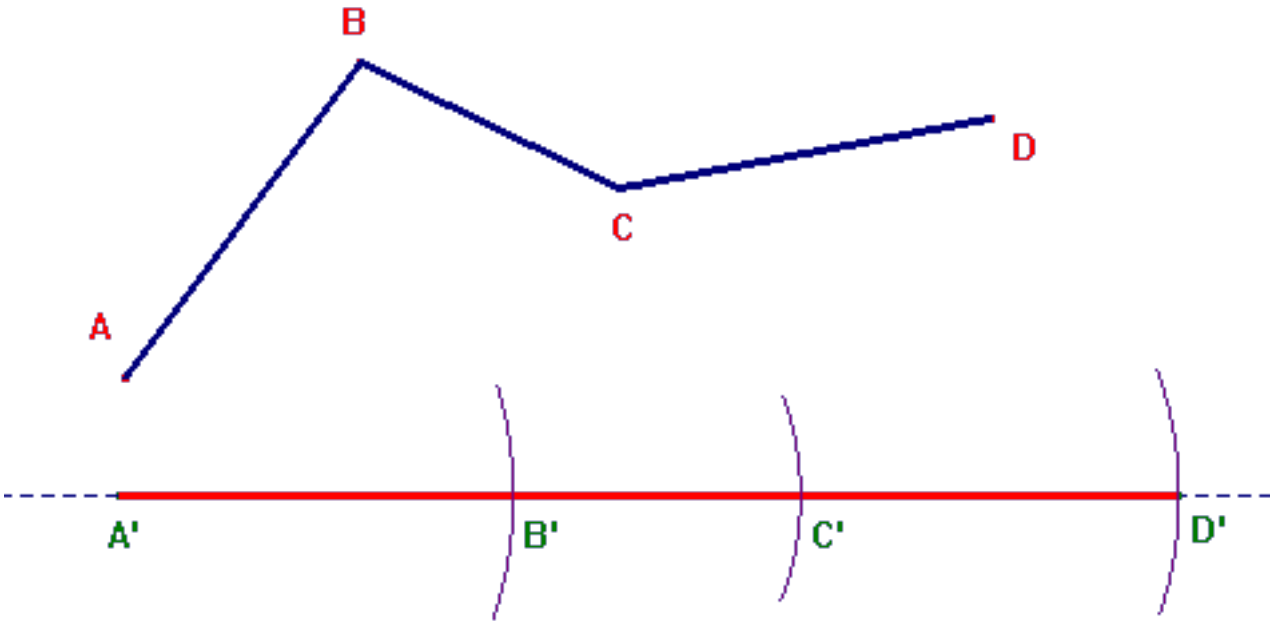

Figura 8.1: rettificazione di una linea

Problema 2: Dato un rettangolo ABCD costruire un quadrato ad esso equivalente

Si tratta semplicemente di applicare il teorema di Euclide come in figura 8.2: riportato BC in BC′ e costruito il semicerchio di diametro AC′ (e centro O), il quadrato BEFG, costruito sull'altezza relativa all'ipotenusa del triangolo rettangolo AGC′, è il quadrato cercato.

Problema 3: Dato un quadrato ABCD costruire un rettangolo ad esso equivalente e avente un lato assegnato

Si tratta del problema inverso del precedente (vedi figura 8.3). Basta riportare il lato assegnato sul prolungamento di AD, in DE, e di costruire il triangolo rettangolo ECH. Il quadrato dato è quello costruito sull'altezza relativa all'ipotenusa, per cui il rettangolo richiesto avrà dimensioni HD e DE. Nella figura 8.3 HD è riportato in DG.

Problema 4: Dato un triangolo ABC costruire un rettangolo ad esso equivalente

Si esamini solo la figura 8.4, tenendo conto che M è il punto medio di AB.

I problemi 2 e 4 ci consentono di quadrare un qualsiasi triangolo, prima trasformandolo in un rettangolo e poi in un quadrato. Poiché ogni poligono si può decomporre in triangoli possiamo trasformare ogni poligono nella somma di tanti rettangoli: se trasformiamo tutti i rettangoli in rettangoli aventi la stessa altezza otterremo un unico rettangolo equivalente al poligono dato e quindi potremo facilmente quadrare il poligono.

Dunque ogni poligonale (con un numero finito di lati) è rettificabile elementarmente e ogni regione chiusa a contorno poligonale (con un numero finito di lati) è quadrabile elementarmente.

Si pone ora il problema di risolvere lo stesso problema per altre figure, in particolare per la circonferenza e il cerchio. Il problema della quadratura del cerchio o quello, equivalente, della rettificazione della circonferenza è di quelli che hanno più a lungo angustiato i matematici e solo Lindemann nel 1882 risolse definitivamente il problema in un celebre articolo dal titolo "Über

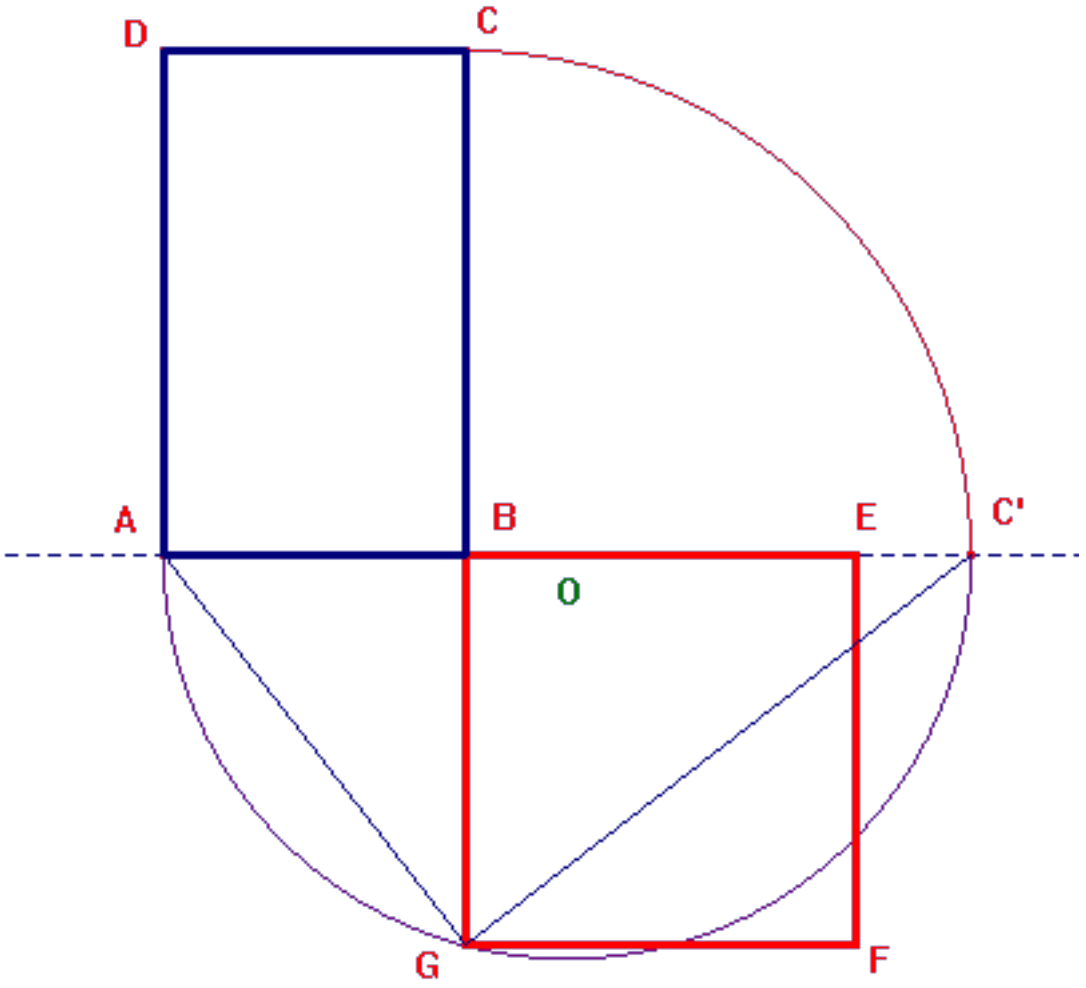

Figura 8.2: quadratura di un rettangolo

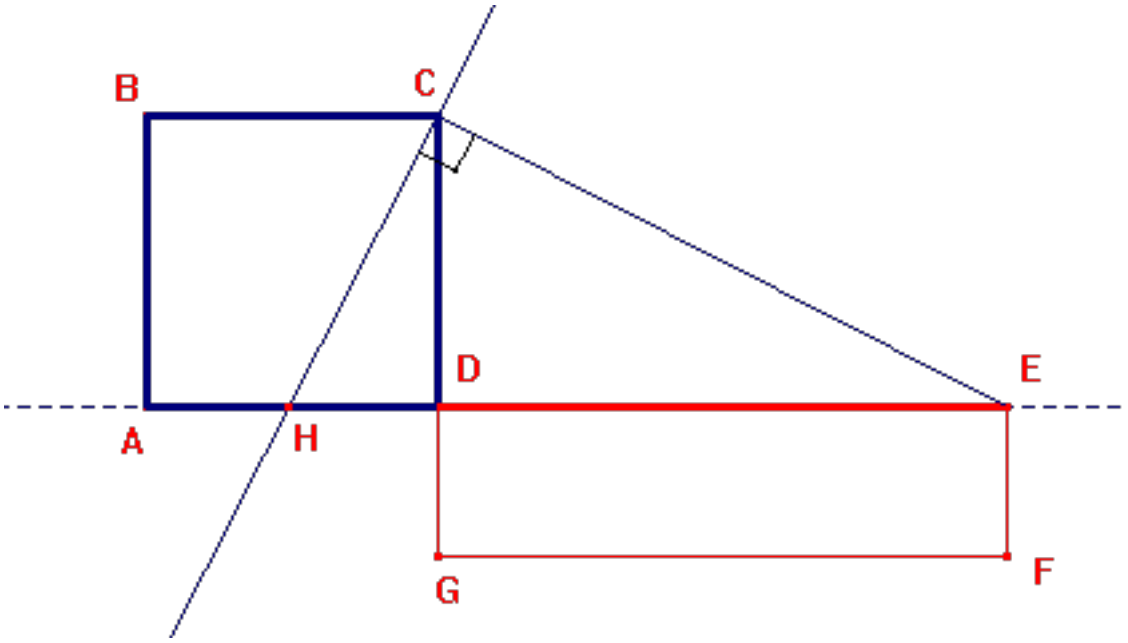

Figura 8.3: rettangolatura di un quadrato

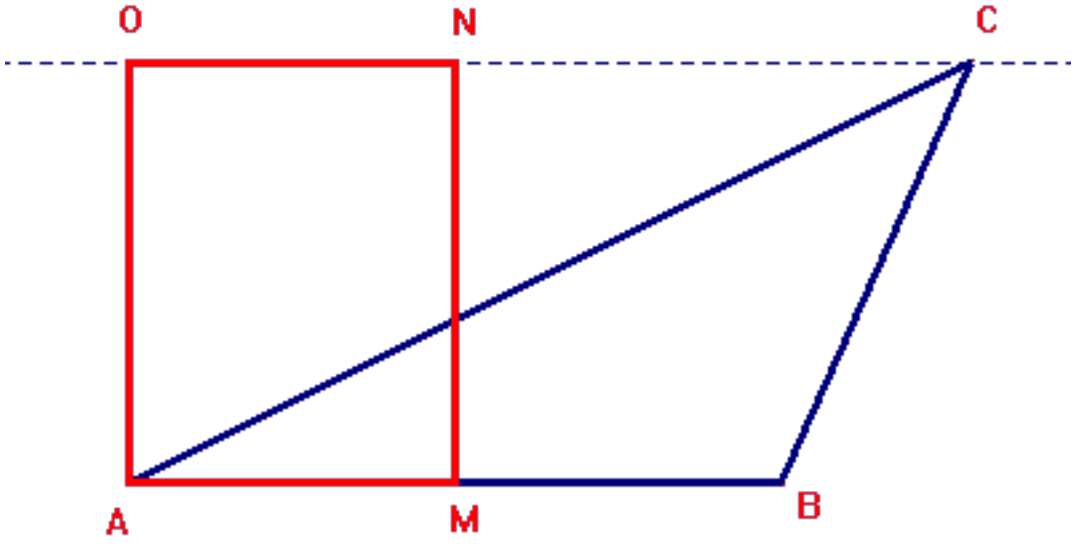

Figura 8.4: quadratura di un triangolo

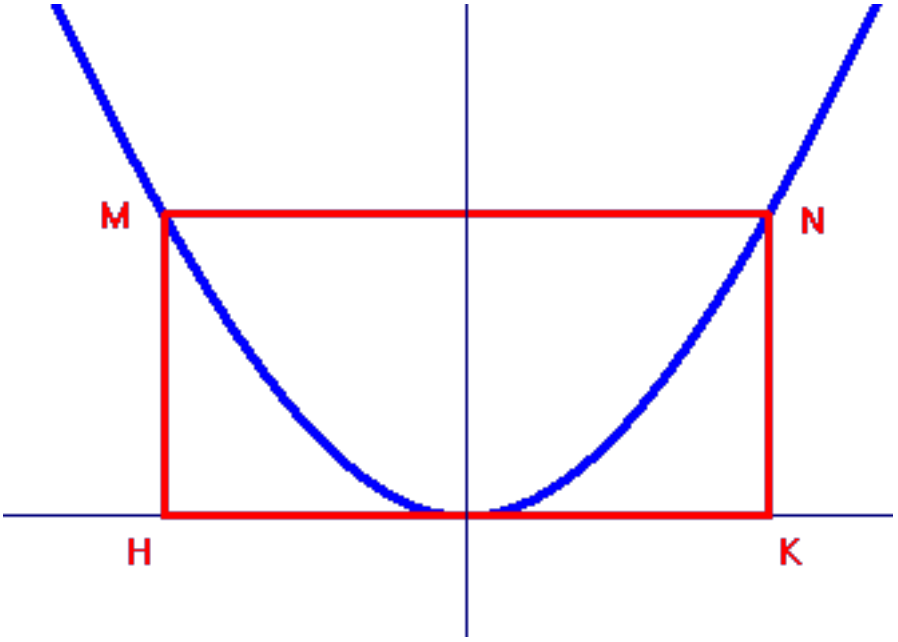

Figura 8.5: quadratura di una parabola

die Zahl π", pubblicato sui Matematische Annalen. Questo articolo è noto universalmente come la dimostrazione della trascendenza di π, e la conclusione è che la quadratura del cerchio è impossibile con riga e compasso.

Questo non significa affatto che sia impossibile quadrare, con riga e compasso figure dal contorno curvilineo. Ricordiamo qui solo i due casi più famosi: il segmento di parabola (problema risolto da Archimede) e le lunule di Ippocrate.

Per quanto riguarda il segmento di parabola Archimede ha provato che esso è equivalente ai 2/3 del parallelogramma costruito come in figura 8.5. Il risultato rimane valido anche se la corda MN non è perpendicolare all'asse, purché HK sia tangente alla parabola.

Per quanto riguarda le lunule di Ippocrate consideriamo il quadrato ABCD e i due archi di cerchio ABC e APC, aventi centro rispettivamente in O e D (vedi figura 8.6). La regione tra essi compresa è una lunula. L'area della lunula è determinabile con un calcolo elementare, osservando che si può ottenere per differenza tra il semicerchio OABC e il segmento circolare OAPC, il quale ultimo è la differenza tra il quarto di cerchio DAPC e il triangolo ADC. Si ottiene facilmente: $Area_{lunula} = \frac{\pi \mathsf{OA}^2}{2} - (\frac{\pi \mathsf{AD}^2}{4} - \frac{\mathsf{AD}^2}{2})$, ovvero, tenendo conto che $\mathsf{AD}^2 = 2\mathsf{OA}^2$ (per Pitagora), $Area_{lunula} = \frac{\mathsf{AD}^2}{2}$, che è come dire che l'area della lunula è metà del quadrato.

Anche se questo non è il ragionamento fatto da Ippocrate, si conclude subito che la lunula è quadrabile. La quadrabilità di questa e altre lunule fece nascere nei matematici la speranza che anche il cerchio fosse quadrabile, cosa che, come abbiamo visto, non è possibile.

8.2.1 Quadratura dei poligoni

Quanto segue è preso da ???

"I greci erano in grado di costruire un quadrato equivalente a un qualunque poligono dato".
"Indipendentemente dal numero dei lati del poligono?".
"Sì, con un procedimento molto bello e generale".
"Mh, interessante".
"Tutto è basato sul fatto che triangoli aventi la stessa base e la stessa altezza sono equivalenti".
"Cioè hanno la stessa area?".
"Sì, anche se il concetto di equivalenza è un po' più astratto. Quando parli di area, usi i numeri, quando parli di equivalenza no".

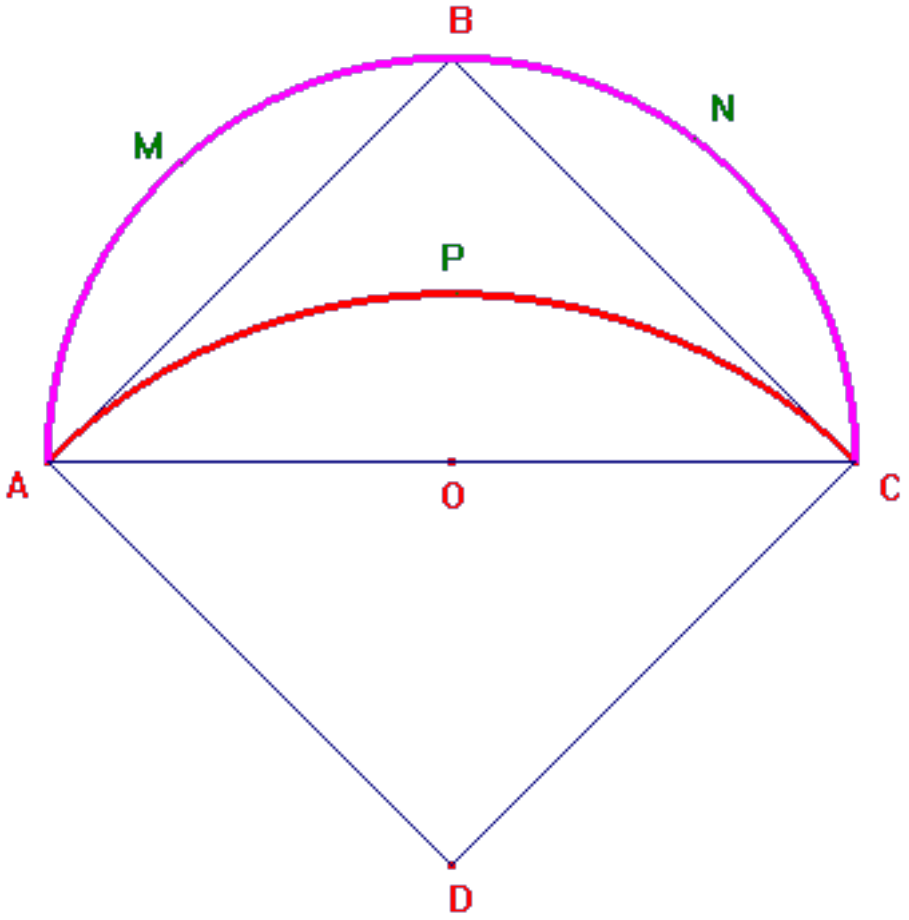

Figura 8.6: la lunula di Ippocrate

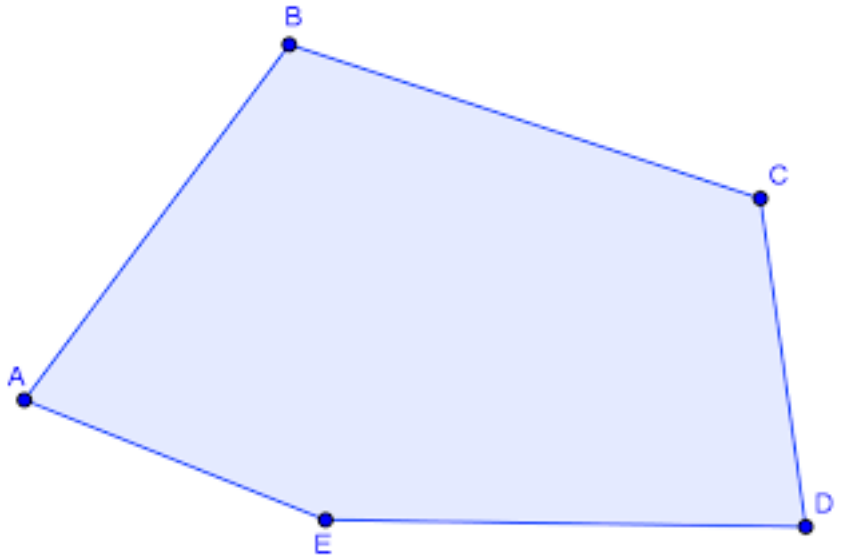

Figura 8.7: poligono con cinque lati

"E cosa uso?".

"Niente. Cioè, usi il concetto di avere la stessa estensione, occupare la stessa superficie. Un concetto che, senza numeri, non è ulteriormente definibile. Negli Elementi di Euclide è un concetto primitivo, cioè non ulteriormente definibile. Ma se vuoi parlare di area, va benissimo".

"Sì, ho parlato di area perché mi è venuto in mente che l'area di un triangolo dipende proprio solo dalla base e dall'altezza".

"Infatti, è così, la formula per il calcolo dell'area di un triangolo funziona proprio perché tutti i triangoli aventi stessa base e stessa altezza sono equivalenti, e quindi l'area è sempre quella".

"Va bene. Vediamo questo procedimento, allora".

"Ecco qua, prendiamo un poligono qualsiasi, composto da un certo numero di lati. In figura 8.7, ne prendiamo cinque".

"Ok, un pentagono irregolare. Adesso?".

"Adesso scegliamo due vertici non adiacenti, ma tali che se percorriamo il bordo della figura, ci sia un solo vertice tra i due".

"Per esempio A e C?".

"Esatto: tra A e C abbiamo solo il vertice B. Congiungiamo A con C e, a partire da B, tracciamo una parallela ad AC" (vedi figura 8.8).

"Ok, fin qua ci sono. So che con riga e compasso si riesce a tracciare una parallela a una retta data".

"Infatti. Ora prolunghiamo il lato DC verso C, fino ad incontrare la retta che abbiamo tracciato prima. Chiamiamo F il punto di intersezione". (vedi figura 8.9)

"Ok, adesso?".

"Adesso abbiamo finito: il poligono $AFDE$ è equivalente al precedente".

"Perché?".

"Perché i due triangoli ABC e AFC hanno la stessa base e la stessa altezza, mentre la parte composta dal poligono $ACDE$ non è stata toccata dalla nostra costruzione".

"Ah, ecco. Sì, è vero, ma perché dici che abbiamo finito?".

"Perché questo è il procedimento: siamo partiti dal poligono $ABCDE$, cinque lati, e siamo arrivati al poligono $AFDE$, quattro lati".

"Ah! Quindi possiamo partire da un poligono di n lati, e arrivare a un poligono di $n-1$ lati".

"Certo, poi possiamo proseguire così fino ad arrivare a un poligono di tre lati, cioè un triangolo. E lì ci fermiamo".

"Bene, ci sono. Cioè, no, non avevi detto che dovevamo costruire un quadrato?".

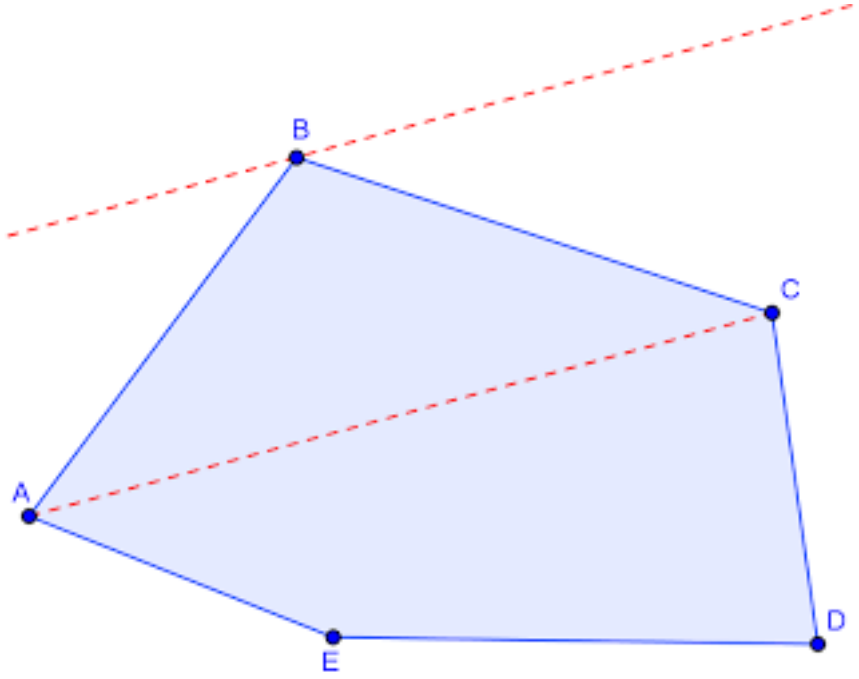

Figura 8.8: quadratura di un poligono con cinque lati

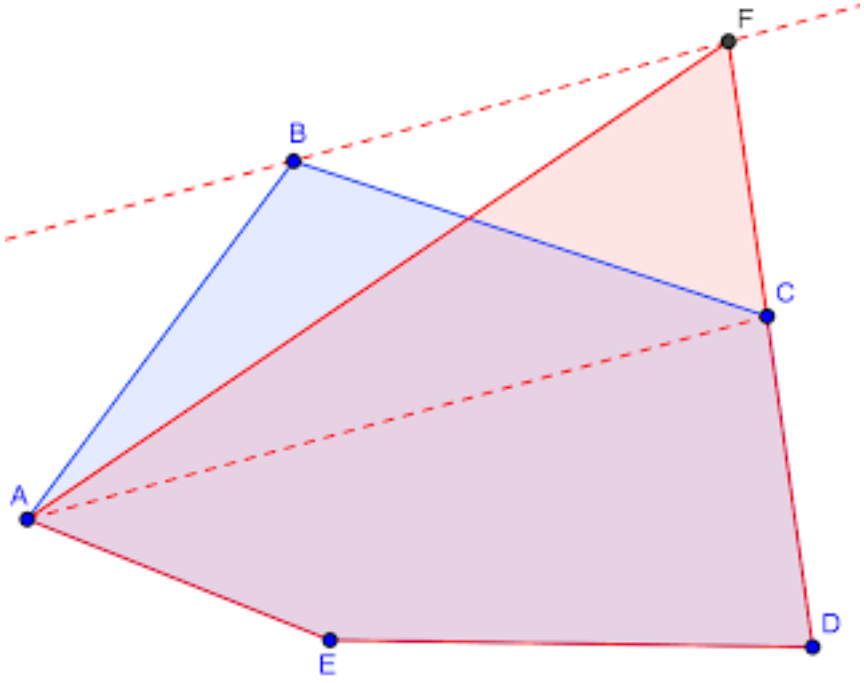

Figura 8.9: quadratura di un poligono con cinque lati (continua)

"Sì, è vero. Per ora abbiamo ricondotto tutti i poligoni ai triangoli, e questo è giè un passo notevole. Ora ricordati che puoi ricondurre un triangolo a un quadrato (vedi sezione 8.2).

8.3 Costruzioni con riga e compasso

Tutte le costruzioni che abbiamo visto nei capitoli precedenti sono state fatte con il vincolo di utilizzare solamente due strumenti, vale a dire la *riga* e il *compasso*, che erano gli unici che sembravano validi dal punto di vista della matematica greca.

In questo capitolo vogliamo studiare come questi vincoli influenzano la possibilità di portare avanti una costruzione geometrica.

Quanto segue è preso da

`http://web.unife.it/utenti/fabio.stumbo/didattica/varie/costruzioni.pdf`

8.3.1 Note storiche

I problemi di costruzioni con riga e compasso sono stati un argomento chiave nella matematica greca, e quindi in tutta la matematica fino a tempi recenti: la soluzione di alcuni problemi classici, tramandatici dai greci, ha dato un forte impulso per lo sviluppo di nuove discipline della matematica moderna come, ad esempio, la teoria dei campi.

Eseguire una costruzione con riga e compasso vuol dire, in parole povere, determinare oggetti geometrici a partire da altri oggetti dati, utilizzando come unici strumenti la riga ed il compasso.

Naturalmente, ciò già richiede un primo livello di astrazione: le figure che noi possiamo tracciare sono inevitabilmente approssimative. Si pensi, ad esempio, allo spessore del tratto lasciato dalla matita: una retta, o un segmento, secondo i greci deve essere formato da "punti" che sono, per definizione stessa, indivisibili. Quel che però è importante, non è il disegno in sè quanto la correttezza del procedimento che descriveremo: se diremo che un tale segmento è lungo 5 unità, all'interno della nostra costruzione ciò avrà un valore esatto, anche se nella pratica il segno tracciato sarà 5 più o meno qualcosa.

Un'altra precisazione necessaria riguarda gli strumenti da utilizzare. Con riga non si intende uno strumento per misurare o segnare distanze, ma sempre e soltanto un'asta rigida che permetta solo di tracciare una retta, che sarà sempre determinata da due punti che le appartengono. Un'osservazione più delicata, e spesso sorvolata, riguarda il compasso. Si tende ad utilizzare il compasso, tacitamente, come uno strumento *rigido* mentre invece, almeno in principio, è da considerarsi *molle*. Spieghiamo meglio questa sottile, ma delicata, differenza. Il compasso è utilizzato per disegnare delle circonferenze. Una circonferenza è determinata dal suo centro e da un punto su di essa: si punta il compasso nel centro, si apre fino a raggiungere con la matita del compasso il punto della circonferenza e si traccia la circonferenza. Questo è il compasso *molle*. Più spesso, però, la circonferenza è determinata assegnandone il centro ed il raggio. Il problema è allora di andare a rilevare tale lunghezza con il compasso (ricordiamo che la riga non permette di misurare le distanze) e poi trasportare il compasso fino a poter puntare nel centro e tracciare con l'apertura determinata. In questo procedimento si presuppone che il compasso sia *rigido*, vale a dire che sia in grado di mantenere inalterata, in modo perfetto, l'apertura impostata. È evidente come questa sia una restrizione rispetto alluso del compasso nel modo più abituale. Se quindi si vuole restare nella massima generalità possibile, bisogna solo considerare il compasso *molle*; ad ogni modo, il problema si aggira facilmente dimostrando come prima cosa che utilizzando riga e compasso *molle* è possibile costruire una circonferenza una volta che siano assegnati il centro ed un segmento qualsiasi del piano che funga da raggio, autorizzando in questo modo un utilizzo accettabile allinterno della teoria del compasso *rigido*.

Fra i vari problemi considerati dai greci ve ne sono alcuni che si distinguono per la brillantezza e labilità necessaria per arrivare alla soluzione e altri per la difficoltà della soluzione stessa, fino ad arrivare a quelli che hanno impegnato per secoli, se non millenni, generazioni di matematici, portando a soluzioni talvolta sorprendenti.

Un problema classico è il cosiddetto problema di contatto di Apollonio (circa 250 a.C.): sono date nel piano tre circonferenze arbitrarie e si chiede di tracciare una quarta circonferenza tangente a tutte e tre. Di questo problema, poi, esistono parecchie varianti, perché si ammette che una o

più delle circonferenze date possa degenerare ad un punto o ad una retta. Per esempio, nel caso in cui tutte e tre le circonferenza degenerano ad un punto si deve determinare una circonferenza passante per tre punti dati: questo è, naturalmente, il caso più facile tra tutti. I casi particolari sono in genere non troppo difficili, ma il caso generale è notevolmente più difficile. Altri problemi classici e famosissimi (anzi, in un certo senso, *i problemi classici*) tramandatici dai greci, sono la duplicazione del cubo, la trisezione dellangolo e la quadratura del cerchio. A questi possiamo senz'altro aggiungere il problema di determinare una costruzione del poligono regolare di n lati, dove n è un intero maggiore o uguale a 3. Per quest'ultimo problema la soluzione era nota fin dallantichità per alcuni valori particolari, come per esempio $n = 3, 4, 5, 6$.

Come già sottolineato, la soluzione di tali problemi ammette solo luso della riga e del compasso: includendo l'uso di altri strumenti si allarga notevolmente il campo delle figure costruibili. Del resto, è naturale aspettarsi che l'insieme delle figure costruibili aumenti all'aumentare degli strumenti ammissibili: già i greci, per esempio, avevano risolto il problema della duplicazione del cubo in più modi diversi, usando vari strumenti.

Per contro, come ha sorprendentemente dimostrato Mascheroni, ogni costruzione eseguibile con riga e compasso può essere eseguita col solo compasso. Naturalmente, non sarà possibile tracciare materialmente una retta, ma la si dovrà considerare nota tramite due suoi punti. Osserviamo, per amor di precisione, che questo risultato comunemente attribuito a Mascheroni è stato dimostrato in realtà per la prima volta dal matematico danese Georg Mohr che lo pubblicò nel libro *Euclides Danicus* nel 1672. Tale libro però venne pubblicato solo in danese ed olandese e rimase sostanzialmente sconosciuto alla comunità fino al 1928, quando uno studente di matematica ne trovò una copia in un negozio di libri usati e venne divulgato.

Se invece si cerca un *analogo* del risultato di Mascheroni-Mohr relativamente all'uso della sola riga, ci si convince subito che ciò non è possibile: usando solo la riga si possono costruire solo curve lineari (i.e., rette) e, col linguaggio che useremo nella dimostrazione del teorema, le intersezioni restano allinterno del campo di definizione delle curve. Ciò che invece è possibile, come ha dimostrato Jacob Steiner nel 1833, è che tutte le costruzioni con riga e compasso sono effettuabili con la sola riga a patto che sia data anche una circonferenza (fissa) con il suo centro. Non è però possibile prescindere dal centro: se è data solo la circonferenza senza il centro, non si possono più effettuare tutte le costruzioni.

I problemi classici sono stati accanitamente studiati per secoli, e senza risultati, al punto da entrare addirittura nel lessico quotidiano: basti pensare che quando si dice che si affronta qualcosa di difficilissimo si dice che si sta cercando di *quadrare il cerchio* (ciò, in realtà, ha anche originato delle incomprensioni tra i matematici e i non matematici, come vedremo).

Dopo lungo tempo di tentativi infruttuosi, ha iniziato ad insinuarsi l'idea, tra i matematici, che tali problemi fossero irrisolubili. Si affacciò dunque un problema diverso: *come si può dimostrare che una data costruzione non possa essere eseguita?*

Per arrivare a studiare la risolubilità o meno dei problemi classici fu però necessario aspettare che venissero gettate le fondamenta per lalgebra moderna. Anche in algebra vi era, in particolare, un problema antico che attirava lattenzione degli studiosi: si trattava di determinare le soluzioni di un polinomio utilizzando solo espressioni che contenessero dei radicali. La soluzione di questo problema era ben nota da lungo tempo per le equazioni di grado 2 e nel XVI secolo si era scoperto che esiste una soluzione per le equazioni di terzo e quarto grado. Ciò aveva dato nuovo vigore alle ricerche finché i lavori di Ruffini (1765-1822), Abel (1802-29) (per le equazioni di quinto grado), e Galois (1811-32) (per la teoria generale relativa alle equazioni di grado superiore al quinto) non conclusero la questione dimostrando che, in generale, non è possibile determinare un'espressione che contenga solo radicali e che dia tutte le radici di un polinomio avente grado fissato, se questo grado è maggiore o uguale a 5. Ciò comunque non vuol dire che il polinomio non abbia radici: Gauss aveva già dimostrato, nella sua tesi di laurea nel 1799, che ogni polinomio di grado n ha esattamente n radici nel campo dei numeri complessi. Tali radici possono essere determinate con un grado arbitrario di precisione mediante metodi di approssimazione opportuni, e ciò ha grande importanza nelle applicazioni, ma *non* possono essere determinate in modo esatto tramite radicali.

La teoria utilizzata per ottenere questo risultato risultò molto efficace anche per studiare i problemi con riga e compasso. Efficace al punto tale che, in colpo solo, quasi tutti i problemi principali furono risolti! Questo, tra l'altro, è un bellissimo esempio dellinterdipendenza che hanno tra loro le varie discipline matematiche (algebra, geometria, analisi, ecc.): spesso i problemi sollevati

nell'ambito di una disciplina trovano soluzione in un'altra disciplina, oppure servono da motivazione per lo sviluppo di discipline completamente nuove (nella matematica moderna, un esempio mirabile di ciò lo si ha con il *Teorema di Fermat*, che ha dato impulso, negli ultimi decenni, allo sviluppo di settori completamente nuovi).

Tornando alle costruzioni con riga e compasso, iniziamo col considerare il problema di costruire il poligono regolare con n lati. I greci sapevano già costruire i poligoni regolari con 3, 4 e 5 lati. Dato che era noto come bisecare un angolo, a partire da questi era possibile costruire i poligoni regolari con un numero di lati pari a $2n$, $3 \cdot 2n$ e $5 \cdot 2n$. Inoltre, dato che $24 = 2 \cdot 12 = 2 \cdot (72 - 60)$, si potevano anche costruire tutti i poligoni regolari con $15 \cdot 2n$ lati. A parte questi valori ben noti ai greci, nessun altro risultato era stato raggiunto nel corso dei secoli. Fu Gauss il primo a dare un nuovo esempio: a 18 anni dimostrò la costruibilità, con riga e compasso, del poligono regolare di 17 lati, e si dice che questa scoperta lo convinse che la matematica avrebbe dovuto essere il suo mestiere. Dopo la sua morte a Gottinga gli fu eretta una statua avente, come base, un poligono regolare di 17 lati. In seguito, Gauss dimostrò che un poligono regolare con p lati, con p numero primo dispari, è costruibile se p è un primo di Fermat, vale a dire $p = 2^{2^m} + 1$ per qualche intero m. Gauss affermò anche il viceversa, ma non si trovò tra le sue carte una dimostrazione di ciò, dimostrazione che fu data da Wantzel. Infine, utilizzando i risultati di Galois, fu possibile dimostrare che il poligono regolare di n lati (con n primo) è costruibile se, e solo se, $n = 2^m p_1 \dots p_s$, con p_i primi di Fermat distinti.

I "primi di Fermat" son chiamati in questo modo in quanto Fermat notò che per $m = 0, 1, 2, 3, 4$ tale intero è un primo e congetturò che fosse primo per ogni valore di m; ma già nel 1732 Eulero si accorse che $n = 2^{2^5} + 1 = 6416700417$ non è primo. Di più, tutti gli altri valori di m fino ad ora calcolati hanno dato numeri non primi, al punto che adesso la congettura è esattamente opposta: si pensa che tali numeri siano primi solo per $m = 0, 1, 2, 3, 4$. Ad ogni modo, il problema geometrico è risolto: sono completamente caratterizzati quegli interi per cui il poligono regolare è costruibile anche se, di fatto, questi interi non sono completamente noti.

Passiamo ora ai tre problemi classici dei greci.

Il problema della duplicazione del cubo chiede di costruire un cubo che abbia volume doppio rispetto ad un cubo dato. La leggenda vuole che in occasione di una grande epidemia la peste si era diffusa a Delo e i cittadini, non trovando altro rimedio, si rivolsero alloracolo di Delfi. La sentenza fu che per far cessare la peste si doveva costruire un altare grande il doppio di quello consacrato ad Apollo nellisola di Delo. Tale altare era, per l'appunto, di forma cubica. Naturalmente tutti i tentativi fatti dai greci furono vani, a partire da quelli più ingenui come costruire un cubo di lato doppio (che dava un cubo con un volume uguale a 8 volte il volume originale) o come costruire un altare di volume effettivamente doppio di quello originale ma che non era più di forma cubica, essendo un parallelepipedo in cui un lato era lungo due volte quello originale e gli altri lati invece erano invariati. Il problema della duplicazione del cubo si riduce, numericamente, alla costruzione con riga e compasso del numero $\sqrt[3]{2}$: grazie alla teoria dei campi sappiamo che ciò è impossibile.

Per quel che riguarda la trisezione dellangolo, bisogna osservare che la risolubilità o meno del problema dipende dallangolo considerato: effettivamente, in alcuni casi particolari trisecare langolo dato è possibile, se non addirittura semplice, come per esempio nel caso degli angoli di 180 e 90 gradi. D'altra parte, risolvere in generale il problema vuol dire che dato un qualsiasi angolo si deve avere una costruzione con riga e compasso che come risultato dia un angolo pari ad un terzo dellangolo dato. Sempre utilizzando la teoria dei campi, si può dimostrare che nel caso dellangolo di 60 gradi non è possibile effettuare la trisezione usando solo riga e compasso.

Infine, il problema più famoso: la quadratura del cerchio, vale a dire, dato un cerchio determinare un quadrato che abbia la sua stessa area. È evidente come ciò si riduca immediatamente a costruire con riga e compasso il numero $\sqrt{\pi}$. Per poter dimostrare che ciò è impossibile è stato necessario attendere che Lindemann nel 1882, riadattando la dimostrazione della trascendenza di e di Hermite, dimostrasse la trascendenza di π.

Concludiamo con unosservazione sul concetto di *impossibilità* di una dimostrazione. Spesso, nel linguaggio comune, si dice che qualcosa è *impossibile* intendendo con ciò dire che sia "estremamente difficile", se non, addirittura, che sia così difficile che nessuno sappia come fare. Quindi cercare di fare qualcosa etichettata in tal modo come *impossibile* può essere considerato come una sfida per il proprio ingegno, tramite la quale dimostrare la propria superiorità nei confronti degli altri. Tale era la soluzione del problema della quadratura del cerchio prima della dimostrazione di Lindemann.

Dopo tale dimostrazione, tuttavia, il termine *impossibile* ha preso il suo significato matematico: all'interno della teoria assiomatica che presupponiamo valere, dire che qualcosa è impossibile vuol dire che è stata dimostrata la falsità di una proposizione o, se si preferisce, la verità della sua negazione. Se quindi si riuscisse anche a dimostrare la verità della proposizione ciò vorrebbe dire che nella nostra teoria sarebbe possibile dimostrare sia una proposizione che la sua negazione: una catastrofe! Nonostante tutto questo, a tutt'oggi esistono ancora persone che si ingegnano di scovare costruzioni della quadratura del cerchio che si rivelano, ovviamente, invariabilmente errate: spesso sono delle ottime, anzi eccellenti, approssimazioni, ma mai costruzioni esatte, naturalmente. Per trovare lerrore può essere necessario anche molto tempo, per cui può capitare che quando un aspirante "quadratore" sottopone alla comunità matematica internazionale una presunta quadratura del cerchio, la sua soluzione venga direttamente inoltrata al... cestino! E a nulla valgono, né possono valere, le vibranti proteste dell'aspirante quadratore contro la "lobby" dei matematici ufficiali che non vuole riconoscere il suo genio!

8.3.2 Costruzioni fondamentali

Iniziamo con individuare quelle che sono le operazioni di base: le regole fondamentali che si usano per qualunque altra costruzione e che verranno poi sempre utilizzate senza ulteriori riferimenti. Alla base di queste costruzioni ci sono le più elementari definizioni e proprietà geometriche come, ad esempio, il fatto che il luogo dei punti equidistanti da due punti dati è la retta passante per il punto medio del segmento individuato dai due punti e ad esso perpendicolare (il cosiddetto *asse del segmento*). Oppure, il fatto che la bisettrice di un angolo è il luogo dei punti equidistanti da due semirette (uscenti da uno stesso punto) date. E così via, senza dimenticare i teoremi fondamentali sui triangoli: proporzioni, similitudini, Euclide, Pitagora ...

Definizione e notazioni

Inizieremo, come già osservato, supponendo che il compasso sia molle, vale a dire che non sia in grado di mantenere inalterata la sua apertura quando lo si trasporta a zonzo per il piano. Con esso è quindi possibile costruire una circonferenza solo una volta che ne siano dati il centro ed un suo punto.

Appena possibile vedremo che, in realtà, usando il compasso molle e la riga è possibile "simulare" il compasso rigido e quindi, a partire da quel punto in poi, faremo un uso libero del compasso: per definire una circonferenza andrà bene sia il centro ed un suo punto, che il centro ed un segmento qualsiasi che ne sia il raggio.

Per prima cosa, cerchiamo di capire come si può passare a codificare in termini algebrici il concetto di "costruzione con riga e compasso", in modo da poter tradurre un problema geometrico in uno algebrico, e viceversa.

Per effettuare una costruzione con riga e compasso si effettua una successione di operazioni scelte tra quattro operazioni fondamentali. Le operazioni sono:

1. congiungere due punti (già costruiti) con una retta;
2. trovare il punto di intersezione di due rette (già costruite);
3. tracciare una circonferenza, dato il centro ed un suo punto;
4. trovare i punti di intersezione di una circonferenza con un'altra circonferenza (già costruita) o con una retta (già costruita).

Una figura sarà determinata nel piano dai punti necessari a definirla: due punti per un segmento, 5 punti per un pentagono, i due fuochi ed i due assi per un'ellissi, eccetera.

Una costruzione $\mathcal{C}$ è, per definizione, una successione di punti, rette e circonferenza

$$\{\Gamma_0 = (0,0), \Gamma_1 = (1,0), \Gamma_2, \ldots, \Gamma_m; \Gamma_{m+1}, \ldots, \Gamma_n\}$$

in cui gli elementi Γ_i, $i \leq m$, sono dati mentre per ogni Γ_i, $i > m$, vale una delle seguenti condizioni:

1. se Γ_i è un punto esso o è un punto già presente nella costruzione (uno dei Γ_h, con $h < i$) oppure esistono due curve distinte Γ_h, Γ_k, con $h, k < i$, tali che Γ_i sia uno dei loro punti di intersezione;

2. se Γ_i è una retta esistono due punti distinti Γ_h, Γ_k, con $h, k < i$, tali che Γ_i sia la retta che li unisce;

3. se Γ_i è una circonferenza esistono due punti Γ_h, Γ_k, con $h, k < i$, tali che Γ_i sia la circonferenza con centro Γ_h e raggio $\overline{\Gamma_h\Gamma_k}$ (questo, si osservi, è il compasso molle).

Un punto $P = (\alpha, \beta)$ del piano è detto costruibile a partire da $\mathcal{C} = \{\Gamma_0, \ldots, \Gamma_m\}$ se esiste una costruzione $\mathcal{C}' = \{\Gamma_0, \ldots, \Gamma_m; \Gamma_{m+1}, \ldots, \Gamma_n\}$ in cui esso compaia. P è semplicemente detto costruibile nel caso in cui $\mathcal{C}$ sia formata solo dal segmento unitario: $\mathcal{C} = \{(0,0), (1,0)\}$. Il numero complesso $z = \alpha + \mathrm{i}\beta$ si dice costruibile se è costruibile il punto (α, β) oppure equivalentemente (come vedremo) se lo sono i punti $(\alpha, 0)$ e $(0, \beta)$. Osserviamo che i numeri reali vengono considerati come caso particolare dei complessi: $a = a + \mathrm{i} \cdot 0$ è quindi costruibile se è costruibile il punto $(a, 0)$, essendo $(0, 0)$ costruibile per ipotesi.

Abbiamo quindi dato una definizione soddisfacente dal punto di vista matematico del concetto intuitivo di "costruibilità". Il problema è ora capire quali siano le figure costruibili.

In questi appunti, useremo la seguente notazione:

- AB: retta passante per A e B;
- $\overline{AB}$: lunghezza del segmento avente come estremi A e B;
- $O(A)$ (oppure anche O_A): cerchio di centro O e passante per A;
- $O(AB)$ (oppure anche O_{AB}): cerchio di centro O e raggio $\overline{AB}$.

Un accorgimento che può semplificare la lettura di una costruzione è quello di indicare i punti in ordine alfabetico via via che vengono costruiti: in questo modo diventa più agevole, anche solo guardando una figura, capire quali sono, ed in quale sequenza, le operazioni fatte.

Dato che in una costruzione si costruiscono punti successivi come intersezioni di curve passanti per punti precedenti, una convenzione che può rendere più compatta e schematica una costruzione altrimenti prolissa da descrivere è quella di usare una tabella in cui sulla prima riga si mettono i punti dati e nella seconda i (nuovi) punti risultanti come intersezione delle curve determinati dai punti dati. Per esempio, la tabella

$$\frac{|A(BC), DF|}{E, G}$$

indica che i punti E, G sono l'intersezione del cerchio di centro A e raggio $\overline{BC}$ con la retta DF. Useremo la prima colonna per indicare i punti dati della costruzione, da cui si parte, mentre nellultima colonna indicheremo i punti che individuano la soluzione al problema.

Operazioni elementari

- Asse di un segmento.

  Dato il segmento $\overline{AB}$, costruire $A(B)$ e $B(A)$. I due punti C e D di intersezione delle due circonferenze individuano una retta che è lasse del segmento dato.

- Cerchio passante per tre punti. Dati i 3 punti (non allineati)

  A, B e C, costruire come nel punto precedente gli assi dei segmenti $\overline{AB}$ e $\overline{BC}$. Lintersezione D di queste due rette è il centro della circonferenza cercata.

- Perpendicolare ad una retta per un punto della retta stessa.

  Data la retta a ed il punto A su di essa, centrare il compasso in A. Sia B un punto dato su a diverso da A e costruire $A(B)$. Sia C laltro punto di intersezione della circonferenza con la retta; la perpendicolare cercata è lasse DE del segmento $\overline{BC}$.

- Perpendicolare ad una retta per un punto esterno (o, anche, simmetrico di un punto rispetto ad una retta).

  Dati una retta a ed un punto A ad essa esterno, sia B un punto dato della retta. Costruire $A(B)$. Se $A(B) \cap a = \{B\}$, allora $A(B)$ è tangente ad a e AB è perpendicolare ad a. Altrimenti, sia C l'ulteriore punto di intersezione: la retta cercata è lasse del segmento BC. Pertanto, costruire $B(A)$ e $C(A)$; tali circonferenze si intersecheranno in A ed in un ulteriore punto D, che è simmetrico di D rispetto ad a. La retta AD è la perpendicolare richiesta.

- Parallela ad un retta per un punto esterno.

  Siano dati una retta a ed un punto A ad essa esterno. Una prima costruzione è quella che prevede di costruire la perpendicolare b ad a passante per A e, successivamente, la perpendicolare a b in A.

  Per una costruzione più rapida ed elegante, scegliere un qualsiasi punto dato B su a. Costruire $B(A)$. Sia C un punto di intersezione con a. Costruire $A(B)$ e $C(B)$. Lulteriore intersezione D di queste ultime due circonferenze è tale che il quadrilatero $ABCD$ ha tutti i lati di lunghezza uguale, quindi è un rombo e dunque la retta AD è parallela ad a.

- Dal compasso molle al compasso rigido.

  Dati un punto A ed un segmento BC, si deve costruire la circonferenza con centro A e raggio BC. Per far ciò, tracciare la retta AB e costruire le parallele ad AB e BC passanti per C e per A rispettivamente. Il punto D di intersezione tra queste due rette è sul centro cercato.

  Quanto appena visto mostra come con l'uso della riga e del compasso "molle" sia possibile simulare un compasso rigido. A partire da ora, quindi, non faremo più distinzione tra compasso rigido e compasso molle, per cui una circonferenza per noi sarà data dal centro ed un suo punto oppure, indifferentemente, dal centro ed una lunghezza che determini il raggio.

- Bisezione di un angolo.

  Sia dato langolo $B\hat{A}C$. Costruire $A(B)$ e sia D il suo punto di intersezione con AC. Costruire $D(B)$ e $B(D)$. I punti di intersezione E ed F delle due circonferenze individuano una retta che passa per A ed è la bisettrice dellangolo dato.

- Trasporto di un angolo.

  Sia dato langolo $B\hat{A}C$ e lo si voglia trasportare sul segmento $\overline{DE}$, con langolo in D. Costruire $A(B)$ e determinare la sua intersezione F con AC. Costruire $D(AB)$ e determinare la sua intersezione G su DE. Costruire $G(BF)$ e determinare H, intersezione di $G(BF)$ e $D(G)$. La retta DH è tale che $B\hat{A}C = E\hat{D}H$.

Operazioni aritmetiche

Conoscendo alcune costruzioni elementari, vediamo come fare le operazioni aritmetiche usando la riga ed il compasso. Naturalmente, nel riferirci a costruzioni già esposte non daremo tutti i dettagli, ma diremo solo quale costruzione è usata.

Le operazioni aritmetiche possibili con riga e compasso sono solo quelle che definiscono un campo (somma, differenza, prodotto e divisione) e la costruzione della radice quadrata di un numero dato: ciò è alla base del teorema di costruibilità e ne spiega, sostanzialmente, il significato.

- Somma di due numeri (positivi) dati a e b.

  Su una retta costruibile scegliere un punto costruibile A e, con centro in tale punto e apertura a, determinare un segmento terminante in B. Con centro in questultimo punto e raggio b, determinare un punto C sulla retta fissata che stia nella semiretta uscente da B opposta rispetto a quella in cui si trova A: il segmento $\overline{AC}$ ha lunghezza $a + b$.

- Differenza di due numeri (positivi) dati a e b ($a > b$).

  Su una retta costruibile scegliere un punto costruibile A e, con centro in tale punto e apertura a, determinare un segmento terminante in A. Con centro in questultimo punto e raggio b,

determinare un punto B sulla retta fissata allinterno del segmento $\overline{AC}$: il segmento $\overline{AB}$ ha lunghezza $a - b$.

- Prodotto di due numeri (positivi) dati a e b.

  Su una retta costruibile scegliere un punto costruibile A e costruire B tale che $\overline{AB} = 1$. Costruire un'altra semiretta passante per A (per esempio, la perpendicolare in A). Sulla prima trovare C e sulla seconda D tali che $\overline{AC} = a$ e $\overline{AD} = b$. Tracciare la retta passante per C parallela ad BD: il punto E di intersezione di tale retta con la retta AD è tale che $\overline{AE} = ab$.

- Divisione fra due numeri (positivi) dati a e b.

  Come nella costruzione precedente, fissare due semirette uscenti da A e, su una di essa, individuare tramite il compasso due punti B, C tali che $\overline{AB} = 1$ e $\overline{AC} = a$. Sulla seconda retta fissare un punto D a distanza b da A. Tracciare la retta passante per B parallela a CD: il punto E di intersezione di tale retta con la retta AD è tale che $\overline{AE} = \frac{a}{b}$.

  Osserviamo che se in queste operazioni almeno uno dei numeri dati è negativo, bisogna modificare le costruzioni di conseguenza cambiando lorientazione sulla relativa semiretta.

- Costruzione della radice di a.

  Sia $\overline{AB} = a$, un segmento dato; aggiungere 1 e costruire la semicirconferenza di diametro $a + 1 = \overline{BC}$. Nel punto A dove si è aggiunto il segmento unitario costruire la perpendicolare che intersecherà la semicirconferenza nel punto D: il segmento $\overline{AD}$ ha lunghezza $\sqrt{a}$.

Da quanto visto, segue che tutti i punti P di coordinate $P = (a, b)$ dove $a, b \in Q$ sono punti costruibili. Tali punti formano un insieme denso nel piano; questo permette di giustificare un'apparente imprecisione che capita di trovare sovente nelle costruzioni: a volte si può vedere una costruzione che richieda, per la soluzione, la costruzione di una retta o di una circonferenza caratterizzata da una qualche proprietà ma che, a parte, ciò, può essere in una posizione "generica". Per esempio, "dato il segmento $[A, B]$ ed un punto P fuori dalla retta AB, tracciare una retta passante per P che intersechi il segmento in un punto interno".

Secondo la definizione che abbiamo dato, ciò non è necessariamente possibile: se nella costruzione sono dati solo i punti A, B, P, seguendo la definizione non si sa dove prendere un altro punto per cui far passare la retta richiesta. La soluzione sta nel fatto che la definizione sottintende la costruibilità dei punti $(0, 0)$ e $(1, 0)$ e quindi, grazie alle costruzioni elementari viste, di tutti i punti a coordinate razionali, per cui diventa facile integrare i punti di partenza A, B, P con altri punti costruibili che soddisfino le proprietà richieste.

A volte, cercheremo di far vedere come anche a partire dai punti dati nella costruzione stessa si possano costruire altri punti che permettono di procedere secondo le proprietà richieste.

Risultati principali

In virtù delle costruzioni elementari viste, dati due numeri a, b è possibile costruire $a + b$, $a - b$, $a \cdot b$ e $\frac{a}{b}$ (quando $b \neq 0$). Questo già ci dice che tutto il campo dei numeri razionali Q è costruibile. Inoltre, dato a è possibile costruire anche $\sqrt{a}$.

Introduciamo alcune notazioni utili nel teorema che vedremo. Se K è un sottocampo di C e $P = (\alpha, \beta)$ è un punto del piano, diremo che P è definito su K se $\alpha, \beta \in K$. La retta di equazione $ax + by + c = 0$ si dice definita su K se $a, b, c \in K$ e lo stesso dicasi per il cerchio di equazione $x^2 + y^2 + a^x + b^y + c = 0$.

Adesso siamo pronti per enunciare il teorema di costruibilità.

Teorema 8.3.1 *Un numero complesso $z = \alpha + \mathsf{i} \cdot \beta \in \mathsf{C}$ è costruibile se, e solo se, esiste un campo $K \subseteq \mathsf{R}$ tale che:*

1. $\alpha, \beta \in K$;

2. esiste una catena finita di campi compresa tra Q *e* K

$$Q = K_0 \subset K_1 \subset \ldots \subset K_n = K$$

tale che

$$[K_i : K_{i-1}] = 2 \qquad 1 \leq i \leq n.$$

Prima di vedere la dimostrazione di questo teorema facciamo alcune osservazioni che aiutano a comprenderne il significato.

Come è noto, una retta nel piano si rappresenta tramite un'equazione di primo grado mentre per una circonferenza è necessaria un'equazione di secondo grado in cui i coefficienti di x^2 e y^2 sono entrambi 1. Ciò vuol dire che per determinare il punto di intersezione di due rette è necessario risolvere un sistema formato da due equazioni lineari in due incognite, mentre il punto di intersezione tra una circonferenza ed una retta è dato da un sistema ancora di due equazioni con due incognite ma in cui unequazione ha grado 1 e l'altra ha grado 2. Infine, l'intersezione di due circonferenze è data dalla soluzione di un sistema di due equazioni di secondo grado con due incognite: mediante un semplice passaggio, ciò si può ridurre ad un sistema due equazioni una avente grado 1 e l'altra grado 2. Un sistema del primo tipo (equazioni di grado 1), si risolve semplicemente con operazioni di somme, moltiplicazioni e divisioni: la soluzione apparterrà allo stesso campo al quale appartengono i coefficienti delle due equazioni. Un sistema del secondo tipo (in cui un'equazione ha grado 2) alla fine si riduce a risolvere un'equazione di secondo grado e quindi è necessario estrarre una radice quadrata. Quindi se i coefficienti appartengono ad un dato campo H, non è detto che anche la soluzione sia in H ma, più generalmente, apparterrà ad un'estensione $H(\sqrt{\alpha})$ di grado 2 di H. Ciò spiega il motivo per cui compare una catena di estensioni di grado 2 nel teorema: si ha un'estensione non banale ogni volta che si interseca una circonferenza con un'altra curva e l'intersezione non può essere determinata nel campo in cui ci si trova in quel dato momento.

Dimostrazione. ($\Rightarrow$) Supponiamo che il numero complesso $z = \alpha + \mathrm{i}\beta$ sia costruibile e sia $\mathcal{C} = \{\Gamma_0 \equiv (0,0), \Gamma_1 \equiv (1,0), \ldots, \Gamma_h\}$ una costruzione con riga e compasso del punto $\Gamma_h \equiv (\alpha, \beta)$. Nella costruzione $\mathcal{C}$ compare un numero positivo s di punti. Per ogni j, $1 \leq j \leq h$, consideriamo la costruzione euclidea (parziale) $\mathcal{C}_j = \{\Gamma_0, \ldots, \Gamma_j\}$: in essa comparirà un numero t di punti, con $t \leq s$. Indichiamo tali punti con $\Gamma_{j_1} \equiv (\alpha_1, \beta_1), \ldots, \Gamma_{j_t} \equiv (\alpha_t, \beta_t)$ e definiamo il campo $K_j = \mathsf{Q}(\alpha_1, \beta_1, \ldots, \alpha_t, \beta_t)$. Definiamo anche $K_0 = \mathsf{Q}$. Otteniamo così una catena di campi

$$K_0 \subset K_1 \subset \ldots \subset K_h.$$

Dimostriamo che

- se Γ_j è una curva, essa è definita su K_{j-1};
- $[K_j : K_{j-1}] \leq 2$.

Dopo aver dimostrato ciò, sopprimendo i campi intermedi in cui la dimensione resta invariata si ottiene la tesi.

Dimostriamo la prima. Se Γ_j è una retta passante per i punti $\Gamma_k \equiv (1,1)$ e $\Gamma_r \equiv (\alpha_2, \beta_2)$ allora la sua equazione è

$$x(\beta_2 - 1\beta_1) + y(\alpha_1 - \alpha_2) + \beta_1\alpha_2 - \alpha_1\beta_2 = 0$$

e tutti i coefficienti appartengono a K_{j-1}.

Analogamente, se Γ_j è un cerchio di centro $\Gamma_k \equiv (\alpha_1, \beta 1)$ e passante per il punto $\Gamma_r \equiv (\alpha_2, \beta_2)$ allora la sua equazione è

$$(x - \alpha_1)^2 + (y - \beta_1)^2 = (\alpha_2 - \alpha_1)^2 + (\beta_2 - \beta_1)^2$$

che, quindi, è definito su K_{j-1}.

Passiamo ora al secondo punto. Se Γ_j non è un punto, allora $K_j = K_{j-1}$ e non cè niente da dimostrare. Supponiamo dunque che Γ_j sia un punto, intersezione delle due curve Γ_r, Γ_s con $r, s < j$. Supponiamo che entrambe le curve siano due cerchi. Per trovare le intersezioni tra i due cerchi bisogna risolvere il sistema

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 &= 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 &= 0 \end{cases}$$

dove le due equazioni sono, rispettivamente, le equazioni di Γ_r e Γ_s. Dato che $r, s < j$, entrambe le curve sono definite su K_{j-1} e quindi a_1, b_1, c_1 e a_2, b_2, c_2 appartengono tutti a K_{j-1}, per il punto precedente. Sottraendo, il sistema diventa

$$\begin{cases} x^2 + y^2 + a_1 x + b_1 y + c_1 & = & 0 \\ (a_1 - a_2)x + (b_1 - b_2)y + c_1 - c_2 & = & 0 \end{cases}$$

Per risolvere, si ricava dunque x oppure y dalla seconda equazione e si sostituisce nella prima, ottenendo così un'equazione in un'incognita di secondo grado. Le sue radici si trovano in un'estenzione di grado minore od uguale a 2 di K_{j-1} e nello stesso campo si trova l'altra incognita, dato che poi resta da risolvere unequazione lineare.

È evidente che nello stesso modo si studia il caso in cui una delle due curve è una retta: si parte direttamente da un sistema simile al secondo.

Ancora più banale è il caso di due rette: stavolta il sistema è formato da due equazioni lineari e quindi le soluzioni restano all'interno del campo.

($\Leftarrow$) Siano $z = \alpha + \mathrm{i}\beta \in \mathsf{C}$ e $K = K_n$ un campo verificante le ipotesi del teorema. Dobbiamo dimostrare che il punto $P \equiv (\alpha, \beta)$ è costruibile. Lo faremo per induzione su n.

- $n = 0$: in questo caso, $\alpha, \beta \in K_0 = \mathsf{Q}$ ed in base alle costruzioni elementari viste z è costruibile.
- $(n-1) \Rightarrow n$: possiamo supporre che $\alpha \notin K_{n-1}$, di modo che $K_{n-1}(\alpha) \neq K_{n-1}$. Per il teorema della torre

  $$[K_n : K_{n-1}(\alpha)][K_{n-1}(\alpha) : K_{n-1}] = [K_n : K_{n-1}] = 2$$

  e quindi $K_n = K_{n-1}(\alpha)$, pertanto è algebrico di grado 2 su K_{n-1}. Sia $x^2 + a^x + b$ il suo polinomio minimo ($a, b \in K_{n-1}$). In virtù della costruibilità della radice quadrata di un numero costruibile, le radici del polinomio sono costruibili su K_{n-1}. Per ipotesi induttiva tutti i numeri di K_{n-1} sono costruibili e quindi anche α è costruibile. Analogamente si ragiona per β.

Per concludere, vediamo come tutto ciò si applichi alla soluzione dei problemi classici. Dal teorema otteniamo subito il

Corollario 8.3.2 *Se $z \in \mathsf{C}$ è costruibile, allora esso è algebrico su Q e il suo grado è una potenza di due.*

Dimostrazione. Sia $z = \alpha + \mathrm{i}\beta$ costruibile e sia $K \subseteq \mathsf{R}$ tale che $\alpha, \beta \in K$. z è radice del polinomio $x^2 - 2\alpha x + \alpha^2 + \beta^2$ a coefficienti in K, pertanto $[K(z) : K] \leq 2$. Per il teorema della torre, $[K(z) : \mathsf{Q}] = [K(z) : K][K : \mathsf{Q}]$ e quindi anche $[K(z) : \mathsf{Q}]$ è una potenza di 2. Dato che $\mathsf{Q}(z) \subseteq K(z)$, ancora per il teorema della torre otteniamo che $[\mathsf{Q}(z) : \mathsf{Q}]$ è una potenza di 2.

Spesso si usa quest'ultimo corollario, però nella sua forma negata:

Corollario 8.3.3 *Se il polinomio minimo su Q di $z \in \mathsf{C}$ ha grado che non è una potenza di due, allora z non è costruibile.*

Teorema 8.3.4 *Non è possibile duplicare il cubo con riga e compasso.*

Dimostrazione. Per duplicare il cubo, bisogna costruire il numero $\sqrt[3]{2}$. Tale numero è soluzione su Q del polinomio $x^3 - 2$, che è irriducibile. Infatti, se fosse riducibile, essendo di grado 3 dovrebbe avere (almeno) un fattore di grado 1, cioè dovrebbe avere una radice in Q. Sia $\frac{a}{b}$ una radice, con $a, b \in \mathsf{Z}$, $\mathsf{MCD}(a, b) = 1$ e $(\frac{a}{b})^3 = 2$. Allora $2b^3 = a^3$ pertanto $2|a^3$, quindi $2|a$ che implica $2^3|a^3$ e da ciò si ricava $2|b$, contro l'ipotesi che a e b siano primi tra loro.

Pertanto $x^3 - 2$ è il polinomio minimo di $\sqrt[3]{2}$ su Q e $[\mathsf{Q}(\sqrt[3]{2}) : Q] = 3$.

Per quello che riguarda la quadratura del cerchio, abbiamo già osservato che il problema si risolve utilizzando il Teorema di Lindemann, che afferma la trascendenza di π: non essendo algebrico, non è possibile costruirlo con riga e compasso.

8.4 Insieme di Vitali

Quanto segue è preso da ???

L'insieme di Vitali prende il nome dal matematico italiano Giuseppe Vitali e fornisce un esempio di sottoinsieme di R che non è misurabile da nessuna misura che sia positiva, invariante per traslazioni e sigma-finita (in particolare dalla misura di Lebesgue). Per la costruzione dell'insieme di Vitali è indispensabile l'assioma della scelta.

La costruzione procede nel seguente modo:

- Definiamo sui numeri reali dell'intervallo $[0, 1]$ la seguente relazione di equivalenza: diciamo che x è equivalente a y se la loro differenza è un numero razionale;
- Consideriamo l'insieme di tutte le classi di equivalenza indotte dalla relazione appena definita. Queste devono essere una infinità non numerabile poiché se fossero un'infinità numerabile avremmo che l'insieme $[0, 1]$ stesso sarebbe numerabile (in quanto unione numerabile di insiemi numerabili).
- L'assioma della scelta ci dice che esiste un insieme che contiene esattamente un rappresentante di ogni classe, chiamiamolo V: questo è l'insieme di Vitali (notate che V contiene una quantità più che numerabile di punti).

8.4.1 Dimostrazione della non misurabilità di V

L'insieme di Vitali ha le seguenti proprietà:

1. Se lo trasliamo di una quantità pari ad un qualsiasi numero razionale strettamente positivo, occuperà punti completamente diversi da quelli che occupava inizialmente. Più formalmente stiamo dicendo che l'insieme V e il suo traslato $\mathsf{T}_q(V) \equiv V + q$ sono disgiunti per qualsiasi $q \in \mathsf{Q} - \{0\}$. Questo perché se per assurdo fosse $V \cap \mathsf{T}_q(V) \neq \emptyset$, con $q \in \mathsf{Q} - \{0\}$, esisterebbero $x, y \in V$ distinti, e quindi con $(y - x) \notin \mathsf{Q}$ essendo rappresentanti di diverse classi di equivalenza, tali che $y = \mathsf{T}_q(x)$. Ma allora, $y = x + q$, ovvero $(y - x) = q \in \mathsf{Q}$, che è assurdo avendo osservato che $(y - x) \notin \mathsf{Q}$ per ogni $x, y \in V$ distinti.
2. Dato un qualunque punto $x \in [0, 1]$ questo apparterrà a qualcuna delle traslazioni $V + q$ con $q \in \mathsf{Q}$: infatti apparterrà a qualcuna delle classi di equivalenza definite sopra, e sappiamo che in V c'è un rappresentante di ogni classe, quindi in V c'è un punto che dista da x una quantità pari ad un numero razionale.

Dalle proprietà enunciate discende la non misurabilità di V nel caso in cui la misura μ verifichi le seguenti proprietà:

- (invarianza per traslazioni) per ogni insieme A, $\mu(A + x) = \mu(A)$
- (positività) $\mu(\mathsf{R}) \neq 0$
- (sigma-finitezza) $\mu([a, b]) < \infty$ per ogni a e b
- (inclusione) Se $U \subseteq V$ allora $\mu(U) \leq \mu(V)$
- (addittività numerabile) Se $U = \bigcup V_i$, con $V_i \cap V_j = \emptyset$ se $i \neq j$, allora $\mu(U) = \Sigma_{i>0}\mu(V_i)$

Per dimostrare la non misurabilità di V rispetto alla misura μ assumiamo che sia definito il valore di $\mu(V)$ e deriviamo una contraddizione con le ipotesi.

Consideriamo l'insieme ottenuto unendo tutte le possibili traslazioni di V di numeri razionali compresi tra -1 e 1. A tale scopo consideriamo prima una enumerazione dei razionali di $[-1, 1]$: q_1, q_2, q_3, ... e definiamo l'insieme

$$U \equiv (V + q_1) \cup (V + q_2) \cup \ldots \cup (V + q_n) \cup \ldots$$

Osserviamo subito che, per *inclusione* e *sigma-finitezza* di μ, $\mu(U) < \infty$ perché U è un insieme limitato visto che $U \subseteq [-1, 2]$. Poiché U è un'unione disgiunta di insiemi (esercizio: verificare che

gli insiemi $V + q_i$ e $V + q_j$ sono davvero disgiunti se $i \neq j$), per le proprietà delle misure abbiamo che

$$\mu(U) = \mu(V + q_1) + \mu(V + q_2) + \ldots + \mu(V + q_n) + \ldots$$

e per l'invarianza di μ per traslazioni

$$\mu(U) = \mu(V) + \mu(V) + \ldots + \mu(V) + \ldots$$

ma poiché la quantità a sinistra dell'uguaglianza è finita, la relazione appena scritta implica che $\mu(V) = 0$, e quindi anche $\mu(U) = 0$.

Abbiamo osservato prima, però, che ogni $x \in [0, 1]$ si trova in uno dei $V + q_n$, quindi U deve includere tutto l'intervallo $[0, 1]$, ma allora, di nuovo per *inclusione*, $\mu([0, 1] \leq \mu(U)$, e abbiamo visto poco fa che quest'ultima è nulla, quindi $\mu([0, 1]) = 0$, e per l'*invarianza per traslazioni* e la *addittività numerabile* dovremo avere anche $\mu(\mathsf{R}) = 0$ (visto che tutti gli intervalli di lunghezza unitaria hanno misura nulla e una quantità numerabile di intervalli copre tutto R), il che contraddice le ipotesi su μ.

8.5 Paradosso di Banach-Tarski e non misurabilità

Quanto segue è preso da

`http://en.wikipedia.org/wiki/Banach-Tarski_paradox`

The Banach-Tarski paradox is a theorem in set theoretic geometry which states the following: Given a solid ball in 3-dimensional space, there exists a decomposition of the ball into a finite number of non-overlapping pieces (i.e. subsets), which can then be put back together in a different way to yield two identical copies of the original ball. The reassembly process involves only moving the pieces around and rotating them, without changing their shape. However, the pieces themselves are not "solids" in the usual sense, but infinite scatterings of points. A stronger form of the theorem implies that given any two "reasonable" solid objects (such as a small ball and a huge ball), either one can be reassembled into the other. This is often stated colloquially as "a pea can be chopped up and reassembled into the Sun".

The reason the Banach-Tarski theorem is called a paradox is that it contradicts basic geometric intuition. "Doubling the ball" by dividing it into parts and moving them around by rotations and translations, without any stretching, bending, or adding new points, seems to be impossible, since all these operations preserve the volume, but the volume is doubled in the end.

Unlike most theorems in geometry, this result depends in a critical way on the axiom of choice in set theory. This axiom allows for the construction of non-measurable sets, collections of points that do not have a volume in the ordinary sense and for their construction would require performing an uncountably infinite number of choices.

It was shown in 2005 that the pieces in the decomposition can be chosen in such a way that they can be moved continuously into place without running into one another.[1]

8.5.1 Banach and Tarski publication

In a paper published in 1924 (see [2]) Stefan Banach and Alfred Tarski gave a construction of such a "paradoxical decomposition", based on earlier work by Giuseppe Vitali concerning the unit interval (see section 8.4) and on the paradoxical decompositions of the sphere by Felix Hausdorff, and discussed a number of related questions concerning decompositions of subsets of Euclidean spaces in various dimensions. They proved the following more general statement, the strong form of the Banach-Tarski paradox:

Given any two bounded subsets A and B of a Euclidean space in at least three dimensions, both of which have a non-empty interior, there are partitions of A and B into a finite number of disjoint subsets, $A = A_1 \cup \ldots \cup A_k$, $B = B_1 \cup \ldots \cup B_k$, such that for each i between 1 and k, the sets A_i and B_i are congruent.

Now let A be the original ball and B be the union of two translated copies of the original ball. Then the proposition means that you can divide the original ball A into a certain number of pieces

and then rotate and translate these pieces in such a way that the result is the whole set B, which contains two copies of A.

The strong form of the Banach-Tarski paradox is false in dimensions one and two, but Banach and Tarski showed that an analogous statement remains true if countably many subsets are allowed. The difference between the dimensions 1 and 2 on the one hand, and three and higher, on the other hand, is due to the richer structure of the group G_n of the Euclidean motions in the higher dimensions, which is solvable for $n = 1, 2$ and contains a free group with two generators for $n \geq 3$. John von Neumann studied the properties of the group of equivalences that make a paradoxical decomposition possible, identifying the class of amenable groups, for which no paradoxical decompositions exist. He also found a form of the paradox in the plane which uses area-preserving affine transformations in place of the usual congruences.

8.5.2 Formal treatment

The Banach-Tarski paradox states that a ball in the ordinary Euclidean space can be doubled using only the operations of partitioning into subsets, replacing a set with a congruent set, and reassembly. Its mathematical structure is greatly elucidated by emphasizing the role played by the group of Euclidean motions and introducing the notions of *equidecomposable sets* and *paradoxical set*. Suppose that G is a group acting on a set X. In the most important special case, X is an n-dimensional Euclidean space, and G consists of all isometries of X, i.e. the transformations of X into itself that preserve the distances. Two geometric figures that can be transformed into each other are called *congruent*, and this terminology will be extended to the general G-action. Two subsets A and B of X are called *G-equidecomposable*, or *equidecomposable* with respect to G, if A and B can be partitioned into the same finite number of respectively G-congruent pieces. It is easy to see that this defines an equivalence relation among all subsets of X. Formally, if

$$A = \bigcup_{i=1}^{k} A_i \qquad B = \bigcup_{i=1}^{k} B_i \qquad A_i \cap A_j = \emptyset = B_i \cap B_j \text{ for all } i, j \text{ such that } 1 \leq i < j \leq k$$

and there are elements $g_1, \ldots, g_k$ of G such that for each i between 1 and k, $g_i(A_i) = B_i$, then we will say that A and B are G-equidecomposable using k pieces. If a set E has two disjoint subsets A and B such that A and E, as well as B and E, are G-equidecomposable then E is called paradoxical.

Using this terminology, the Banach-Tarski paradox can be reformulated as follows:

A three-dimensional Euclidean ball is equidecomposable with two copies of itself

In fact, there is a sharp result in this case, due to Robinson[3]: doubling the ball can be accomplished with five pieces, and fewer than five pieces will not suffice. The strong version of the paradox claims:

Any two bounded subsets of 3-dimensional Euclidean space with non-empty interiors are equidecomposable

While apparently more general, this statement is derived in a simple way from the doubling of a ball by using a generalization of the Bernstein-Schroeder theorem due to Banach that implies that if A is equidecomposable with a subset of B and B is equidecomposable with a subset of A, then A and B are equidecomposable.

The Banach-Tarski paradox can be put in context by pointing out that for two sets in the strong form of the paradox, there is always a bijective function that can map the points in one shape into the other in a one-to-one fashion. In the language of Georg Cantor's set theory, these two sets have equal cardinality. Thus, if one enlarges the group to allow arbitrary bijections of X then all sets with non-empty interior become congruent. Likewise, we can make one ball into a larger or smaller ball by stretching, in other words, by applying similarity transformations. Hence if the group G is large enough, we may find G-equidecomposable sets whose "size" varies. Moreover, since a countable set can be made into two copies of itself, one might expect that somehow, using countably many pieces could do the trick. On the other hand, in the Banach-Tarski paradox the number of pieces is finite and the allowed equivalences are Euclidean congruences, which preserve

the volumes. Yet, somehow, they end up doubling the volume of the ball! While this is certainly surprising, some of the pieces used in the paradoxical decomposition are non-measurable sets, so the notion of volume (more precisely, Lebesgue measure) is not defined for them, and the partitioning cannot be accomplished in a practical way. In fact, the Banach-Tarski paradox demonstrates that it is impossible to find a finitely-additive measure (or a Banach measure) defined on all subsets of a Euclidean space of three (and greater) dimensions that is invariant with respect to Euclidean motions and takes the value one on a unit cube. In his later work, Tarski showed that, conversely, non-existence of paradoxical decompositions of this type implies the existence of a finitely-additive invariant measure.

The heart of the proof of the "doubling the ball" form of the paradox presented below is the remarkable fact that by a Euclidean isometry (and renaming of elements), one can divide a certain set (essentially, the surface of a unit sphere) into four parts, then rotate one of them to become itself plus two of the other parts. This follows rather easily from a F_2-paradoxical decomposition of F_2, the free group with two generators. Banach and Tarski's proof relied on an analogous fact discovered by Hausdorff some years earlier: the surface of a unit sphere in space is a disjoint union of three sets B, C, D and a countable set E such that, on the one hand, B, C, D are pairwise congruent, and, on the other hand, B is congruent with the union of C and D. This is often called the Hausdorff paradox.

8.5.3 Connection with earlier work and the role of the axiom of choice

Banach and Tarski explicitly acknowledge Giuseppe Vitali's 1905 construction of the set bearing his name, Hausdorff's paradox (1914), and an earlier (1923) paper of Banach as the precursors to their work. Vitali's and Hausdorff's constructions depend on Zermelo's axiom of choice ("AC"), which is also crucial to the Banach-Tarski paper, both for proving their paradox and for the proof of another result:

Two Euclidean polygons, one of which strictly contains the other, are not equidecomposable

They remark: "Le röle que joue cet axiome dans nos raisonnements nous semble meriter l'attention (The role this axiom plays in our reasoning seems to us to deserve attention)" and point out that while the second result fully agrees with our geometric intuition, its proof uses AC in an even more substantial way than the proof of the paradox. Thus Banach and Tarski imply that AC should not be rejected simply because it produces a paradoxical decomposition, for such an argument also undermines proofs of geometrically intuitive statements.

However, in 1949 A.P. Morse showed that the statement about Euclidean polygons can be proved in ZF set theory and thus does not require the axiom of choice. In 1964, Paul Cohen proved that the axiom of choice cannot be proved from ZF. A weaker version of an axiom of choice is the axiom of dependent choice, DC. It has been shown that the Banach-Tarski paradox is not a theorem of ZF, nor of ZF + DC (Wagon, Corollary 13.3).

Large amounts of mathematics use AC. As Stan Wagon points out at the end of his monograph, the Banach-Tarski paradox has been more significant for its role in pure mathematics than for foundational questions: it motivated a fruitful new direction for research, the amenability of groups, which has nothing to do with the foundational questions.

In 1991, using then-recent results by Matthew Foreman and Friedrich Wehrung,[4] Janusz Pawlikowski proved that the Banach-Tarski paradox follows from ZF plus the Hahn-Banach theorem.[5] The Hahn-Banach theorem doesn't rely on the full axiom of choice but can be proved using a weaker version of AC called the ultrafilter lemma. So Pawlikowski proved that the set theory needed to prove the Banach-Tarski paradox, while stronger than ZF, is weaker than full ZFC.

8.5.4 A sketch of the proof

Here we sketch a proof which is similar but not identical to that given by Banach and Tarski. Essentially, the paradoxical decomposition of the ball is achieved in four steps:

1. Find a paradoxical decomposition of the free group in two generators.

2. Find a group of rotations in 3-d space isomorphic to the free group in two generators.

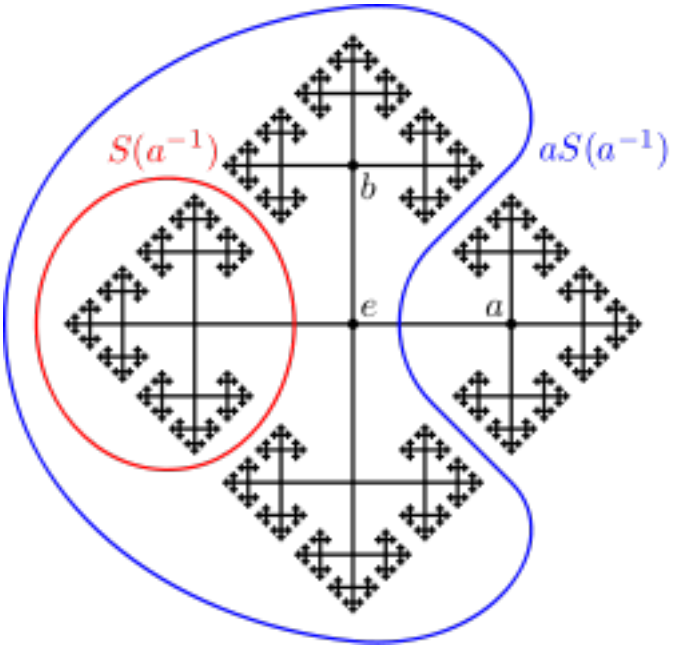

Figura 8.10: The sets $S(a^{-1})$ and $aS(a^{-1})$ in the Cayley graph of F_2

3. Use the paradoxical decomposition of that group and the axiom of choice to produce a paradoxical decomposition of the hollow unit sphere.

4. Extend this decomposition of the sphere to a decomposition of the solid unit ball.

We now discuss each of these steps in more detail.

Step 1

The free group with two generators a and b consists of all finite strings that can be formed from the four symbols a, a^{-1}, b and b^{-1} such that no a appears directly next to an a^{-1} and no b appears directly next to a b^{-1}. Two such strings can be concatenated and converted into a string of this type by repeatedly replacing the "forbidden" substrings with the empty string. For instance: $abab^{-1}a^{-1}$ concatenated with $abab^{-1}a$ yields $abab^{-1}a^{-1}abab^{-1}a$, which contains the substring $a^{-1}a$, and so gets reduced to $abaab^{-1}a$. One can check that the set of those strings with this operation forms a group with identity element the empty string e. We will call this group F_2.

The group F_2 can be "paradoxically decomposed" as follows: let $S(a)$ be the set of all strings that start with a and define $S(a^{-1})$, $S(b)$ and $S(b^{-1})$ similarly. Clearly,

$$\mathsf{F}_2 = \{e\} \cup S(a) \cup S(a^{-1}) \cup S(b) \cup S(b^{-1})$$

but also

$$\mathsf{F}_2 = aS(a^{-1}) \cup S(a)$$

and

$$\mathsf{F}_2 = bS(b^{-1}) \cup S(b)$$

The notation $aS(a^{-1})$ means take all the strings in $S(a^{-1})$ and concatenate them on the left with a.

Make sure that you understand this last line, because it is at the core of the proof. For example, there may be a string $aa^{-1}b$ in the set $aS(a^{-1})$ which, because of the rule that a must not appear next to a^{-1}, reduces to the string b. In this way, $aS(a^{-1})$ contains all the strings that start with b. Similarly, it contains all the strings that start with a^{-1} (for example the string $aa^{-1}a^{-1}$ which reduces to a^{-1}). We have cut our group F_2 into four pieces (plus the singleton $\{e\}$), then "shifted"

two of them by multiplying with a or b, then "reassembled" two pieces to make one copy of F_2 and the other two to make another copy of F_2. That is exactly what we want to do to the ball.

Step 2

In order to find a group of rotations of 3D space that behaves just like (or "isomorphic to") the group F_2, we take two orthogonal axes, e.g. the x and z axes, and let A be a rotation of $\arccos(1/3)$ about the first, x axis, and B be a rotation of $\arccos(1/3)$ about the second, z axis (there are many other suitable pairs of irrational multiples of π, that could be used here instead of $\arccos(1/3)$ and $\arccos(1/3)$, as well). It is somewhat messy but not too difficult to show that these two rotations behave just like the elements a and b in our group F_2. We shall skip it, leaving the exercise to the reader. The new group of rotations generated by A and B will be called H. We now also have a paradoxical decomposition of H. (This step cannot be performed in two dimensions since it involves rotations in three dimensions. If we take two rotations about the same axis, the resulting group is commutative and doesn't have the property required in step 1.)

Step 3

The unit sphere S^2 is partitioned into orbits by the action of our group H: two points belong to the same orbit if and only if there's a rotation in H which moves the first point into the second. (Note that the orbit of a point is a dense set in S^2.) We can use the axiom of choice to pick exactly one point from every orbit; collect these points into a set M. Now (almost) every point in S^2 can be reached in exactly one way by applying the proper rotation from H to the proper element from M, and because of this, the paradoxical decomposition of H then yields a paradoxical decomposition of S^2 into four pieces A_1, A_2, A_3, A_4 as follows:

$$\begin{aligned} A_1 &= S(a)M \cup M \cup B \\ A_2 &= S(a^{-1})M - B \\ A_3 &= S(b)M \\ A_4 &= S(b^{-1})M \end{aligned}$$

where:

$$B = a^{-1}M \cup a^{-2}M \cup \ldots$$

(We didn't use the five "paradoxical" parts of F_2 directly, as they would leave us with M as an extra piece after doubling, due to the presence of the singleton $\{e\}$!)

The (majority of the) sphere has now been divided into four sets (each one dense on the sphere), and when two of these are rotated, we end up with double what we had before:

$$\begin{aligned} aA_2 &= A_2 \cup A_3 \cup A_4 \\ bA_4 &= A_1 \cup A_2 \cup A_4 \end{aligned}$$

Step 4

Finally, connect every point on S^2 with a ray to the origin; the paradoxical decomposition of S^2 then yields a paradoxical decomposition of the solid unit ball minus the point at the ball's centre (this center point needs a bit more care).

N.B. This sketch glosses over some details. One has to be careful about the set of points on the sphere which happen to lie on the axis of some rotation in H. However, there are only countably many such points, and like the point at the centre of the ball, it is possible to patch the proof to account for them all.

References

1. Wilson, Trevor M. (September 2005). "A continuous movement version of the BanachTarski paradox: A solution to De Groot's problem". Journal of Symbolic Logic 70 (3): 946-952. doi:10.2178/jsl/1122038921. JSTOR 27588401.

2. Banach, Stefan; Tarski, Alfred (1924). "Sur la decomposition des ensembles de points en parties respectivement congruentes" (in French). Fundamenta Mathematicae 6: 244277.

3. Robinson, R. M. (1947). "On the Decomposition of Spheres." Fund. Math. 34:246-260. This article, based on an analysis of the Hausdorff paradox, settled a question put forth by von Neumann in 1929.

4. Foreman, M.; Wehrung, F. (1991). "The Hahn-Banach theorem implies the existence of a non-Lebesgue measurable set". Fundamenta Mathematicae 138: 13-19.

5. Pawlikowski, Janusz (1991). "The Hahn-Banach theorem implies the Banach-Tarski paradox". Fundamenta Mathematicae 138: 21-22.

6. Churkin, V. A. (2010). "A continuous version of the Hausdorff-Banach-Tarski paradox". Algebra and Logic 49 (1): 81-89. doi:10.1007/s10469-010-9080-y.

7. On p. 85. Neumann, J. v. (1929). "Zur allgemeinen Theorie des Masses". Fundamenta Mathematica 13: 73-116.

8. Laczkovich, Miklös (1999). "Paradoxical sets under SL2(R)". Ann. Univ. Sci. Budapest. Etvos Sect. Math. 42: 141-145.

9. Satö, Kenzi (2003). "A locally commutative free group acting on the plane". Fundamenta Mathematica 180 (1): 25-34.

10. Edward Kasner and James Newman (1940) Mathematics and the Imagination, pp 205-7, Simon and Schuster.

11. Kuro5hin. "Layman's Guide to the Banach-Tarski Paradox".

12. Stromberg, Karl (March 1979). "The Banach-Tarski paradox". The American Mathematical Monthly (Mathematical Association of America) 86 (3): 151-161. doi:10.2307/2321514. JSTOR 2321514.

13. Su, Francis E.. "The Banach-Tarski Paradox".

14. von Neumann, John (1929). "Zur allgemeinen Theorie des Masses". Fundamenta Mathematicae 13: 73-116.

15. Wagon, Stan (1994). The Banach-Tarski Paradox. Cambridge: Cambridge University Press. ISBN 0-521-45704-1.

16. Wapner, Leonard M. (2005). The Pea and the Sun: A Mathematical Paradox. Wellesley, Mass.: A.K. Peters. ISBN 1-56881-213-2.

Capitolo 9

Assioma di scelta e topologia

Quanto segue è preso da "Notes on Introductory Point-Set Topology" di Allen Hatcher

One way to describe the subject of Topology is to say that it is *qualitative geometry*. The idea is that if one geometric object can be continuously transformed into another, then the two objects are to be viewed as being topologically the same. For example, a circle and a square are topologically equivalent. Physically, a rubber band can be stretched into the form of either a circle or a square, as well as many other shapes which are also viewed as being topologically equivalent. On the other hand, a figure eight curve formed by two circles touching at a point is to be regarded as topologically distinct from a circle or square. A qualitative property that distinguishes the circle from the figure eight is the number of connected pieces that remain when a single point is removed: When a point is removed from a circle what remains is still connected, a single arc, whereas for a figure eight if one removes the point of contact of its two circles, what remains is two separate arcs, two separate pieces.

The term used to describe two geometric objects that are topologically equivalent is *homeomorphic*. Thus a circle and a square are homeomorphic. Concretely, if we place a circle C inside a square S with the same center point, then projecting the circle radially outward to the square defines a function $f : C \to S$, and this function is continuous: small changes in x produce small changes in $f(x)$. The function f has an inverse $f^{-1} : S \to C$ obtained by projecting the square radially inward to the circle, and this is continuous as well. One says that f is a homeomorphism between C and S.

One of the basic problems of Topology is to determine when two given geometric objects are homeomorphic. This can be quite difficult in general.

Our first goal will be to define exactly what the 'geometric objects' are that one studies in Topology. These are called *topological spaces*. The definition turns out to be extremely general, so that many objects that are topological spaces are not very geometric at all, in fact.

9.1 Topological Spaces

Rather than jump directly into the definition of a topological space we will first spend a little time motivating the definition by discussing the notion of continuity of a function. One could say that topological spaces are the objects for which continuous functions can be defined.

For the sake of simplicity and concreteness let us talk about functions $f : R \to R$. There are two definitions of continuity for such a function that the reader may already be familiar with, the $\epsilon\delta$ definition and the definition in terms of limits. But it is a third definition, equivalent to these two, that is the one we want here. This definition is expressed in terms of the notion of an open set in R, generalizing the familiar idea of an open interval (a, b).

Definition 9.1.1 *A subset O of R is open if for each point $x \in O$ there exists an interval (a, b) that contains x and is contained in O.*

With this definition an open interval certainly qualifies as an open set. Other examples are:

- R itself is an open set, as are semi-infinite intervals (a, ∞) and $(-\infty, a)$.
- The complement of a finite set in R is open.
- If A is the union of the infinite sequence $x_n = \frac{1}{n}$, $n = 1, 2, \ldots$, together with its limit 0 then $R - A$ is open.
- Any union of open intervals is an open set. The preceding examples are special cases of this. The converse statement is also true: every open set O is a union of open intervals since for each $x \in O$ there is an open interval (a_x, b_x) with $x \in (a_x, b_x) \subseteq O$, and O is the union of all these intervals (a_x, b_x).
- The empty set $\emptyset$ is open, since the condition for openness is satisfied vacuously as there are no points x where the condition could fail to hold.

Here are some examples of sets which are not open:

- A closed interval $[a, b]$ is not an open set since there is no open interval about either a or b that is contained in $[a, b]$. Similarly, half-open intervals $[a, b)$ and $(a, b]$ are not open sets when $a < b$.
- A nonempty finite set is not open.

Now for the nice definition of a continuous function in terms of open sets:

Definition 9.1.2 *A function $f : R \to R$ is continuous if for each open set O in R the inverse image $f^{-1}(O) = \{x \in R \mid f(x) \in O\}$ is also an open set.*

To see that this corresponds to the intuitive notion of continuity, consider what would happen if this condition failed to hold for a function f. There would then be an open set O for which $f^{-1}(O)$ was not open. This means there would be a point $x_0 \in f^{-1}(O)$ for which there was no interval (a, b) containing x_0 and contained in $f^{-1}(O)$. This is equivalent to saying there would be points x arbitrarily close to x_0 that are in the complement of $f^{-1}(O)$. For x to be in the complement of $f^{-1}(O)$ means that $f(x)$ is not in O. On the other hand, x_0 was in $f^{-1}(O)$ so $f(x_0)$ is in O. Since O was assumed to be open, there is an interval (c, d) about $f(x_0)$ that is contained in O. The points $f(x)$ that are not in O are therefore not in (c, d) so they remain at least a fixed positive distance from $f(x_0)$. To summarize: there are points x arbitrarily close to x_0 for which $f(x)$ remains at least a fixed positive distance away from $f(x_0)$. This certainly says that f is discontinuous at x_0.

This reasoning can be reversed. A reasonable interpretation of discontinuity of f at x_0 would be that there are points x arbitrarily close to x_0 for which $f(x)$ stays at least a fixed positive distance away from $f(x_0)$. Call this fixed positive distance ϵ. Let O be the open set $(f(x_0) - \epsilon, f(x_0) + \epsilon)$. Then $f^{-1}(O)$ contains x_0 but it does not contain any points x for which $f(x)$ is not in O, and we are assuming there are such points x arbitrarily close to x_0, so $f^{-1}(O)$ is not open since it does not contain all points in some interval (a, b) about x_0.

The definition we have given for continuity of functions $R \to R$ can be applied more generally to functions $R^n \to R^n$ and even $R^m \to R^n$ once one has a notion of what open sets in R^n are. The natural definition generalizing the case $n = 1$ is to say that a set O in R^n is open if for each $x \in O$ there exists an open ball containing x and contained in O, where an open ball of radius r and center x_0 is defined to be the set of points x of distance less than r from x_0. Here the distance from x to x_0 is measured as in linear algebra, as the length of the vector $x - x_0$, the square root of the dot product of this vector with itself.

This definition of open sets in R^n does not depend as heavily on the notion of distance in R^n as might appear. For example in R^2 where open balls become open disks, we could use open squares instead of open disks since if a point $x \in O$ is contained in an open disk contained in O then it is also contained in an open square contained in the disk and hence in O, and conversely, if x is contained in an open square contained in O then it is contained in an open disk contained in the open square and hence in O. In a similar way we could use many other shapes besides disks and squares, such as ellipses or polygons with any number of sides.

After these preliminary remarks we now give the definition of a topological space.

Definition 9.1.3 *A topological space is a set X together with a collection $\mathcal{O}$ of subsets of X, called* open sets*, such that:*

1. *The union of any collection of sets in $\mathcal{O}$ is in $\mathcal{O}$.*
2. *The intersection of any finite collection of sets in $\mathcal{O}$ is in $\mathcal{O}$.*
3. *Both $\emptyset$ and X are in $\mathcal{O}$.*

The collection $\mathcal{O}$ of open sets is called a topology *on X.*

All three of these conditions hold for open sets in R as defined earlier. To check that (1) holds, suppose that we have a collection of open sets O_α where the index α ranges over some index set I, either finite or infinite. A point $x \in \bigcup_\alpha O_\alpha$ lies in some O_α, which is open so there is an interval (a, b) with $x \in (a, b) \subseteq O_\alpha$, hence $x \in (a, b) \subseteq \bigcup_\alpha O_\alpha$, so $\bigcup_\alpha O_\alpha$ is open. To check (2) it suffices by induction to check that the intersection of two open sets O_1 and O_2 is open. If $x \in O_1 \cap O_2$ then x lies in open intervals in O_1 and O_2, and there is a smaller open interval in the intersection of these two open intervals that contains x. This open interval lies in $O_1 \cap O_2$, so $O_1 \cap O_2$ is open. Finally, condition (3) obviously holds for open sets in R.

In a similar fashion one can check that open sets in R^2 or more generally R^n also satisfy $(1)-(3)$.

Notice that the intersection of an infinite collection of open sets in R need not be open. For example, the intersection of all the open intervals $(-\frac{1}{n}, \frac{1}{n})$ for $n = 1, 2, \ldots$ is the single point $\{0\}$ which is not open. This explains why condition (2) is only for finite intersections.

It is always possible to construct at least two topologies on every set X by choosing the collection $\mathcal{O}$ of open sets to be as large as possible or as small as possible:

- The collection $\mathcal{O}$ of all subsets of X defines a topology on X called the *discrete topology.*
- If we let $\mathcal{O}$ consist of just X itself and $\emptyset$, this defines a topology, the *trivial topology.*

Thus we have three different topologies on R, the usual topology, the discrete topology, and the trivial topology. Here are two more, the first with fewer open sets than the usual topology, the second with more open sets:

- Let $\mathcal{O}$ consist of the empty set together with all subsets of R whose complement is finite. The axioms $(1) - (3)$ are easily verified, and we leave this for the reader to check. Every set in $\mathcal{O}$ is open in the usual topology, but not vice versa.
- Let $\mathcal{O}$ consist of all sets O such that for each $x \in O$ there is an interval $[a, b)$ with $x \in [a, b) \subseteq O$. Properties $(1) - (3)$ can be checked by almost the same argument as for the usual topology on R, and again we leave this for the reader to do. Intervals $[a, b)$ are certainly in $\mathcal{O}$ so this topology is different from the usual topology on R. Every interval (a, b) is in $\mathcal{O}$ since it can be expressed as a union of an increasing sequence of intervals $[a_n, b)$ in $\mathcal{O}$. It follows that $\mathcal{O}$ contains all sets that are open in the usual topology since these can be expressed as unions of intervals (a, b).

These examples illustrate how one can have two topologies $\mathcal{O}$ and $\mathcal{O}'$ on a set X, with every set that is open in the $\mathcal{O}$ topology is also open in the $\mathcal{O}'$ topology, so $\mathcal{O} \subseteq \mathcal{O}'$. In this situation we say that the topology $\mathcal{O}'$ is *finer* than $\mathcal{O}$ and that $\mathcal{O}$ is *coarser* than $\mathcal{O}'$. Thus the discrete topology on X is finer than any other topology and the trivial topology is coarser than any other topology. In the case $X = R$ we have interpolated three other topologies between these two extremes, with the finite complement topology being coarser than the usual topology and the half-open-interval topology being finer than the usual topology. Of course, given two topologies on a set X, it need not be true that either one is finer or coarser than the other.

Here is another piece of basic terminology:

Definition 9.1.4 *A subset A of a topological space X is* closed *if its complement $X - A$ is open.*

For example, in R with the usual topology a closed interval $[a, b]$ is a closed subset. Similarly, in R^2 with its usual topology a closed disk, the union of an open disk with its boundary circle, is a closed subset.

Instead of defining a topology on a set X as a collection of open sets satisfying the three axioms, one could equally well consider the collection of complementary closed sets, and define a topology on X to be a collection of subsets called closed sets, such that the intersection of any collection of closed sets is closed, the union of any finite collection of closed sets is closed, and both the empty set and the whole set X are closed. Notice that the role of intersections and unions is switched compared with the original definition. This is because of the general set theory fact that the complement of a union is the intersection of the complements, and the complement of an intersection is the union of the complements.

9.2 Basis for a Topology

Many arguments with open sets in R reduce to looking at what happens with open intervals since open sets are defined in terms of open intervals. A similar statement holds for R^2 and R^n with open disks and balls in place of open intervals. In each case arbitrary open sets are unions of the special open sets given by open intervals, disks, or balls. This idea is expressed by the following terminology:

Definition 9.2.1 *A collection $\mathcal{B}$ of open sets in a topological space X is called a* basis *for the topology if every open set in X is a union of sets in $\mathcal{B}$.*

A topological space can have many different bases. For example, in R^2 another basis besides the basis of open disks is the basis of open squares with edges parallel to the coordinate axes. Or we could take open squares with edges at 45 degree angles to the coordinate axes, or all open squares without restriction. Many other shapes besides squares could also be used.

If $\mathcal{B}$ is a basis for X and Y is a subspace of X, then we can obtain a basis for Y by taking the collection B_Y of intersections $Y \cap B$ as B ranges over all the sets in $\mathcal{B}$. This gives a basis for Y because an arbitrary open set in the subspace topology on Y has the form $Y \cap (\bigcup_\alpha B_\alpha) = \bigcup_\alpha (Y \cap B_\alpha)$ for some collection of basis sets $B_\alpha \in \mathcal{B}$. In particular this says that for any subspace X of R^n, a basis for the topology on X is the collection of open sets $X \cap B$ as B ranges over all open balls in R^n. For example, for a circle in R^2 the open arcs in the circle form a basis for its topology.

If $\mathcal{B}$ is a basis for a topology on X, then $\mathcal{B}$ satisfies the following two properties:

1. Every point $x \in X$ lies in some set $B \in \mathcal{B}$.

2. For each pair of sets B_1, B_2 in $\mathcal{B}$ and each point $x \in B_1 \cap B_2$ there exists a set B_3 in $\mathcal{B}$ with $x \in B_3 \subseteq B_1 \cap B_2$.

The first statement holds since X is open and is therefore a union of sets in $\mathcal{B}$. The second statement holds since $B_1 \cap B_2$ is open and hence is a union of sets in $\mathcal{B}$.

Theorem 9.2.2 *If $\mathcal{B}$ is a collection of subsets of a set X satisfying* (1) *and* (2) *above then $\mathcal{B}$ is a basis for a topology on X.*

The open sets in this topology have to be exactly the unions of sets in $\mathcal{B}$ since $\mathcal{B}$ is a basis for this topology.

Proof. Let $\mathcal{O}$ be the collection of subsets of X that are unions of sets in $\mathcal{B}$. Obviously the union of any collection of sets in $\mathcal{O}$ is in $\mathcal{O}$. To show the corresponding result for finite intersections it suffices by induction to show that $O_1 \cap O_2 \in \mathcal{O}$ if $O_1, O_2 \in \mathcal{O}$. For each $x \in O_1 \cap O_2$ we can choose sets $B_1, B_2 \in \mathcal{B}$ with $x \in B_1 \subseteq O_1$ and $x \in B_2 \subseteq O_2$.

By (2) there exists a set $B_3 \in \mathcal{B}$ with $x \in B_3 \subseteq B_1 \cap B_2 \subseteq O_1 \cap O_2$. The union of all such sets B_3 as x ranges over $O_1 \cap O_2$ is $O_1 \cap O_2$, so $O_1 \cap O_2 \in \mathcal{O}$.

Finally, X is in $\mathcal{O}$ by (1), and $\emptyset \in \mathcal{O}$ since we can regard $\emptyset$ as the union of the empty collection of subsets of $\mathcal{B}$.

9.3 Continuity and Homeomorphisms

Recall the definition: A function $f : X \to Y$ between topological spaces is continuous if $f^{-1}(O)$ is open in X for each open set O in Y. For brevity, continuous functions are sometimes called *maps* or *mappings*. (A map in the everyday sense of the word is in fact a function from the points on the map to the points in whatever region is being represented by the map.)

Lemma 9.3.1 *A function $f : X \to Y$ is continuous if and only if $f^{-1}(C)$ is closed in X for each closed set C in Y.*

Proof An evident set-theory fact is that $f^{-1}(Y - A) = X - f^{-1}(A)$ for each subset A of Y. Suppose now that f is continuous. Then for any closed set $C \subseteq Y$, we have $Y - C$ open, hence the inverse image $f^{-1}(Y - C) = X - f^{-1}(C)$ is open in X, so its complement $f^{-1}(C)$ is closed. Conversely, if the inverse image of every closed set is closed, then for O open in Y the complement $Y - O$ is closed so $f^{-1}(Y - O) = X - f^{-1}(O)$ is closed and thus $f^{-1}(O)$ is open, so f is continuous.

Here is another useful fact:

Lemma 9.3.2 *Given a function $f : X \to Y$ and a basis $\mathcal{B}$ for Y, then f is continuous if and only if $f^{-1}(B)$ is open in X for each $B \in \mathcal{B}$.*

Proof. One direction is obvious since the sets in $\mathcal{B}$ are open. In the other direction, suppose $f^{-1}(B)$ is open for each $B \in \mathcal{B}$. Then any open set O in Y is a union $\bigcup_\alpha B_\alpha$ of basis sets B_α, hence $f^{-1}(O) = f^{-1}(\bigcup_\alpha B_\alpha) = \bigcup_\alpha f^{-1}(B_\alpha)$ is open in X, being a union of the open sets $f^{-1}(B_\alpha)$.

Lemma 9.3.3 *If $f : X \to Y$ and $g : Y \to Z$ are continuous, then their composition $gf : X \to Z$ is also continuous.*

Proof. This uses the easy set-theory fact that $(gf)^{-1}(A) = f^{-1}(g^{-1}(A))$ for any $A \subseteq Z$. Thus if f and g are continuous and A is open in Z then $g^{-1}(A)$ is open in Y so $f^{-1}(g^{-1}(A))$ is open in X. This means gf is continuous.

Definition 9.3.4 *A continuous map $f : X \to Y$ is a homeomorphism if it is one-to-one and onto, and its inverse function $f^{-1} : Y \to X$ is also continuous.*

9.4 Product Spaces

Given two sets X and Y, their product is the set $X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}$. For example $R^2 = R \times R$, and more generally $R^m \times R^n = R^{m+n}$. If X and Y are topological spaces, we can define a topology on $X \times Y$ by saying that a basis consists of the subsets $U \times V$ as U ranges over open sets in X and V ranges over open sets in Y. The criterion for a collection of subsets to be a basis for a topology is satisfied since $(U_1 \times V_1) \cap (U_2 \times V_2) = (U_1 \cap U_2) \times (V_1 \cap V_2)$. This is called the *product topology* on $X \times Y$. The same topology could also be produced by taking the smaller basis consisting of products $U \times V$ where U ranges over a basis for the topology on X and V ranges over a basis for the topology on Y. This is because $(\bigcup_\alpha U_\alpha) \times (\bigcup_\beta V_\beta) = \bigcup_{\alpha,\beta}(U_\alpha \times V_\beta)$.

For example, a basis for the product topology on $R \times R$ consists of the open rectangles $(a_1, b_1) \times (a_2, b_2)$. This is also a basis for the usual topology on R^2, so the product topology coincides with the usual topology.

More generally one can define the product $X_1 \times \ldots \times X_n$ to consist of all ordered n-tuples $(x_1, \ldots, x_n)$ with $x_i \in X_i$ for each i. A basis for the product topology on $X_1 \times \ldots \times X_n$ consists of all products $U_1 \times \ldots \times U_n$ as each U_i ranges over open sets in X_i, or just over a basis for the topology on X_i. Thus R^n with its usual topology is also describable as the product of n copies of R, with basis the open 'boxes' $(a_1, b_1) \times \ldots \times (a_n, b_n)$.

A product space $X \times Y$ has two projection maps $p_1 : X \times Y \to X$ and $p_2 : X \times Y \to Y$ defined by $p_1(x, y) = x$ and $p_2(x, y) = y$. These maps are continuous since if $U \subseteq X$ is open then so is $p_1^{-1}(U) = U \times Y$, and if $V \subseteq Y$ is open then so is $p_2^{-1}(V) = X \times V$.

9.5 Compactness

Compactness is a sort of finiteness property that some spaces have and others do not. The rough idea is that spaces which are 'infinitely large' such as R or $[0, \infty)$ are not compact. However, we want compactness to depend just on the topology on a space, so it will have to be defined purely in terms of open sets. This means that any space homeomorphic to a noncompact space will also be noncompact, so finite intervals (a, b) and $[a, b)$ will also be noncompact in spite of their 'finiteness'. On the other hand, closed intervals $[a, b]$ will be compact - they cannot be stretched to be 'infinitely large'.

How can this idea be expressed just in terms of open sets rather than in some numerical measure of size? This would seem to be difficult since open sets themselves can be large or small. But large open sets can be expressed as unions of small open sets, so perhaps we should think about counting how many small open sets are needed when a large open set in a space X, such as the whole space X itself, is expressed as a union of small open sets. The most basic question in this situation is whether the number of small open sets needed is finite or infinite. This leads to the following general definition:

Definition 9.5.1 *A space X is* compact *if for each collection of open sets O_α in X whose union is X, there exist a finite number of these O_α's whose union is X.*

More concisely, one says that every open cover of X has a finite subcover, where an *open cover* of X is a collection of open sets in X whose union is X, and a *finite subcover* is a finite subcollection whose union is still X.

For example, R is not compact because the cover by the open intervals $(-n, n)$ for $n = 1, 2, \ldots$ has no finite subcover, since infinitely many of these intervals are needed to cover all of R. Another open cover which has no finite subcover is the collection of intervals $(n - 1, n + 1)$ for $n \in Z$.

In a similar vein, the interval $(0, 1)$ fails to be compact since the cover by the open intervals $(\frac{1}{n}, 1)$ for $n \geq 1$ has no finite subcover. Of course, there do exist open covers of $(0, 1)$ which have finite subcovers, for example the cover by $(0, 1)$ itself, or a little less trivially, the cover by all open subintervals of fixed length, say $\frac{1}{4}$, which has the finite subcover $(0, \frac{1}{4})$, $(\frac{1}{8}, \frac{3}{8})$, $(\frac{1}{4}, \frac{1}{2})$, $(\frac{3}{8}, \frac{5}{8})$, $(\frac{1}{2}, \frac{3}{4})$, $(\frac{5}{8}, \frac{7}{8})$, $(\frac{3}{4}, 1)$. To be compact means that every possible open cover has a finite subcover. This could be difficult to check in individual cases, so we will develop general theorems to test for compactness.

9.5.1 Compact Sets in Euclidean Space

Spaces with only finitely many points are obviously compact, or more generally spaces whose topology has only finitely many open sets. However, such spaces are not very interesting. Our goal in this section will be to characterize exactly which subspaces of R^n are compact. We start with an important special case:

Theorem 9.5.2 *A closed interval $[a, b]$ is compact.*

Proof. The case $a = b$ is trivial, so we may assume $a < b$. Let a cover of $[a, b]$ by open sets O_α in $[a, b]$ be given. Since $a \in O_\alpha$ for some α, there exists $c > a$ such that the interval $[a, c]$ is contained in this O_α, and hence $[a, c]$ is contained in the union of finitely many O_α's. Let L be the least upper bound of the set of numbers $c \in [a, b]$ such that $[a, c]$ is contained in the union of finitely many O_α's. We know that $L > a$ by the preceding remarks, and by the definition of L we certainly have $L \leq b$.

There is some O_α, call it O_β, that contains L. This O_β is open in $[a, b]$, so since $L > a$ there is an interval $[L - \epsilon, L]$ contained in O_β for some $\epsilon > 0$. By the definition of L there exist numbers $c < L$ arbitrarily close to L such that $[a, c]$ is contained in the union of finitely many O_α's. In particular, there are such numbers c in the interval $[L - \epsilon, L]$. For such a c we can take a finite collection of O_α's whose union contains $[a, c]$ and add the set O_β containing $[L - \epsilon, L]$ to this collection to obtain a finite collection of O_α's containing the interval $[a, L]$. If $L = b$ we would now be done, so it remains only to show that $L < b$ is not possible.

If $L < b$, the number ϵ could have been chosen so that not only is $[L - \epsilon, L] \subseteq O_\beta$ but also $[L - \epsilon, L + \epsilon] \subseteq O_\beta$, since O_β is open in $[a, b]$. Then by adding O_β to the finite collection of O_α's

whose union contains $[a, c]$, as in the preceding paragraph, we would have a finite collection of O_α's whose union contains $[a, L + \epsilon]$. However, this means that L is not an upper bound for the set of c's such that $[a, c]$ is contained in a finite union of O_α's. This contradiction shows that $L < b$ is not possible, so we must have $L = b$.

For a subspace A of a space X to be compact means of course that every open cover of A has a finite subcover. The open cover of A would consist of sets of the form $A \cap O_\alpha$ for O_α open in X. To say that $A = \bigcup_\alpha (A \cap O_\alpha)$ is equivalent to saying that $A \subseteq \bigcup_\alpha O_\alpha$. Thus for A to be compact means that for every collection of open sets in X whose union contains A, there is a finite subcollection whose union contains A. So it does no harm to interpret 'every open cover of A has a finite subcover' to mean precisely this.

Lemma 9.5.3 *A closed subset of a compact space is compact, in the subspace topology.*

Proof. Let $\{O_\alpha\}$ be a cover of A by open sets in X. We then obtain an open cover of X by adding the set $X - A$, which is open if A is closed. If X is compact this open cover of X has a finite subcover. The sets O_α in this finite subcover then give a finite cover of A since the set $X - A$ contributes nothing to covering A.

Here is another way to show that a space is compact:

Lemma 9.5.4 *If $f : X \to Y$ is continuous and onto, and if X is compact, then so is Y.*

Proof Let a cover of Y by open sets O_α be given. Then the sets $f^{-1}(O_\alpha)$ form an open cover of X. If X is compact, this cover has a finite subcover. Call this finite subcover $f^{-1}(O_1)$, ..., $f^{-1}(O_n)$. Assuming that f is onto, the corresponding sets O_1, ..., O_n then cover Y since for each $y \in Y$ there exists $x \in X$ with $f(x) = y$, and this x will be in some set $f^{-1}(O_i)$ of the finite cover of X, so y will be in the corresponding set O_i.

This implies for example that a circle is compact since it is the image of a continuous map $f : [0, 1] \to R^2$.

In order to expand our range of compact spaces we use the notion of product spaces, introduced in section 9.4.

Theorem 9.5.5 *If X and Y are compact then so is their product $X \times Y$.*

By induction this implies that the product of any finite collection of compact spaces is compact.

Proof. Let a cover of $X \times Y$ by open sets O_α in $X \times Y$ be given. Each point $(x, y) \in X \times Y$ lies in some O_α, and this O_α is a union of basis sets $U \times V$, so there exists a basis set $U_{xy} \times V_{xy}$ containing (x, y) and contained in some O_α.

Suppose we choose a fixed x and let y vary. Then the sets $U_{xy} \times V_{xy}$ cover $\{x\} \times Y$, so the sets V_{xy} with fixed x and varying y form an open cover of Y. Since Y is compact, this cover has a finite subcover V_{xy_1}, ..., V_{xy_n}, where n may depend on x. The intersection $U_x = \bigcap_{j=1}^n U_{xy_j}$ is then an open set containing x with two key properties: The sets $U_x \times V_{xy_1}$, ..., $U_x \times V_{xy_n}$ cover $U_x \times Y$, and each $U_x \times V_{xy_j}$ is contained in some O_α.

Now we let x vary. The sets U_x form an open cover of X, so since X is compact there is a finite subcover $U_{x_1}, \ldots, U_{x_m}$. The products $U_{x_i} \times V_{x_i y_j}$ of the sets U_{x_i} with the corresponding sets $V_{x_i y_j}$ chosen earlier then form a finite cover of $X \times Y$. Each set in this finite cover is contained in some O_α, so by choosing an O_α containing each $U_{x_i} \times V_{x_i y_j}$ we obtain a finite cover of $X \times Y$.

We can use this result to determine exactly which subspaces of R^n are compact. The result is usually called the Heine-Borel Theorem.

Theorem 9.5.6 *A subspace $X \subseteq R^n$ is compact if and only if it is closed and bounded.*

For a subset $X \subseteq R^n$ to be bounded means that it lies inside some ball of finite radius centered at the origin.

Proof. First let us assemble previously-proved results to show the 'if' half of the theorem. If we assume X is bounded, then it lies in a ball of finite radius and hence in some closed cube

$[-r, r] \times \ldots \times [-r, r]$. This cube is compact, being a product of closed intervals which are compact. Since X is a closed subset of a compact space, it is also compact.

Now for the converse, suppose X is compact. The collection of all open balls in R^n centered at the origin and of arbitrary radius forms an open cover of X, so there is a finite subcover, which means X is contained in a single ball of finite radius, the largest radius of the finitely many balls covering X. Hence X is bounded.

To show X is closed if it is compact, suppose x is a limit point of X that is not in X. Then every neighborhood of x contains points of X. In particular each open ball $B_r(x)$ of radius r centered at x contains points of X, so the same is true also for the closed balls $\overline{B}_r(x)$. The complements $R^n - \overline{B}_r(x)$ form an open cover of X as r varies over $(0, \infty)$ since their union is $R^n - \{x\}$ and $x \in X$. This open cover of X has no finite subcover since each $\overline{B}_r$ contains points of X. Thus we have shown that if X is not closed, it is not compact.

9.6 Teorema di Tychonoff sul prodotto topologico

Quanto segue è preso da "Prodotti infiniti e teorema di Tychonoff" di Denis Nardin.

Questo articolo è scritto con lo scopo di dare una rapida illustrazione dei prodotti infiniti di spazi topologici e, in particolare, una dimostrazione essenzialmente elementare del teorema di Tychonoff. L'ispirazione sono stati gli ottimi appunti di Allen Hatcher (http://www.math.cornell.edu/ hatcher/ Top/Topdownloads.html), di cui raccomando la lettura a chiunque voglia approfondire.

9.6.1 Prodotti infiniti

Come è noto, dati due spazi topologici X e Y si può definire sul prodotto $X \times Y$ una topologia, detta *topologia prodotto*, prendendo come base i cosiddetti *rettangoli aperti*, cioè gli insiemi della forma $A \times B$, dove A e B sono aperti in X e Y. Adesso vedremo come estendere questa nozione ad una famiglia di spazi topologici indicizzata da un insieme qualsiasi I. Sia quindi $\{X_i\}_{i \in I}$ una famiglia di spazi. Vorremmo quindi dare una topologia all'insieme

$$X = \Pi_{i \in I} X_i$$

L'osservazione chiave è che, nel caso di due spazi, la topologia prodotto è esattamente la topologia meno fine che rende le due proiezioni $\pi_X : X \times Y \to X$ e $\pi_Y : X \times Y \to Y$ continue. Quindi il minimo che vorremmo chiedere è che per ogni $i \in I$, la proiezione sulla i-esima coordinata $\pi_i : X \to X_i$ sia continua.

Ci chiediamo dunque: qual'è la topologia meno fine tale che le proiezioni siano continue? Serve esattamente che gli insiemi $\pi_i^{-1}(A_i)$ siano aperti, per ogni $i \in I$ e $A_i \subseteq X_i$ aperto. Come topologia prodotto prendiamo perciò la più piccola topologia che contiene questi insiemi.

Purtroppo gli insiemi della forma $\pi_i^{-1}(A_i)$ non sono una base di aperti per la topologia, ma quello che si dice una *sottobase*, cioè una famiglia $\mathcal{F}$ di insiemi per cui si considera la più piccola topologia che li contiene (la cosa ha senso, perché l'intersezione di una famiglia di topologie è ancora una topologia). Per ottenere una base bisogna considerare le intersezioni finite degli elementi della sottobase. Quindi come base per la topologia prodotto si considerano gli insiemi della forma

$$\pi_{i_1}^{-1}(A_{i_1}) \cap \ldots \cap \pi_{i_n}^{-1}(A_{i_n})$$

dove $i_1, \ldots, i_n \in I$ e $A_{i_j} \subseteq X_{i_j}$ sono aperti. Questi insiemi sono detti *insiemi cilindrici*. In altri termini, sul prodotto X mettiamo la topologia che ha per base gli insiemi cilindrici, che sono quelli della forma

$$U = \Pi_{i \in I} U_i$$

dove $U_i \subseteq X_i$ aperti tali che solo un numero finito di loro non sono banali (cioè non coincidono con tutto lo spazio).

9.6.2 Teorema di Tychonoff

Lo scopo di questa sezione è dimostrare il teorema di Tychonoff: se $\{X_i\}_{i\in I}$ è una famiglia di spazi topologici compatti, allora il prodotto

$$X = \Pi_{i\in I} X_i$$

è ancora uno spazio topologico compatto.

Com'è noto, per dimostrare il teorema di Tychonoff è necessario utilizzare l'assioma di scelta in qualche sua forma (vedi sezione 9.7). Qui l'uso che ne faremo si limiterà a supporre che l'insieme I degli indici sia ben ordinabile, e quindi senza perdita di generalità un ordinale γ.

Supponiamo che $\mathcal{U}$ sia un ricoprimento aperto privo di sottoricoprimenti finiti. L'idea di questa semplice dimostrazione consiste nel costruire per ricorsione transfinita un punto $x = \{x_\alpha\}_{\alpha<\gamma}$ tale che ogni suo intorno di base non abbia sottoricoprimenti finiti. Questo è ovviamente assurdo, in quanto il punto x deve stare in qualche aperto di $\mathcal{U}$, che ovviamente conterrà un suo intorno di base.

Per comodità di notazione, introduciamo le seguenti abbreviazioni

$$Y_\lambda \equiv \Pi_{\alpha<\lambda} X_\alpha \text{ e } Z_\lambda \equiv \Pi_{\lambda\leq\alpha<\gamma} X_\alpha$$

per ogni $\lambda \leq \gamma$.

Vogliamo costruire una successione $\{x_\alpha\}_{\alpha<\gamma}$ tale che per ogni $\lambda \leq \gamma$, se $y_\lambda = \{x_\alpha\}_{\alpha<\lambda}$ ogni aperto della forma

$$U \times Z_\lambda$$

con U intorno di base di y_λ in Y_λ, non abbia sottoricoprimenti finiti in X.

Costruiamola per ricorsione transfinita, una componente alla volta.

- Per $\lambda = 0$ la successione vuota soddisfa la tesi
- Se è vero per λ, troviamo x_λ in modo che $y_{\lambda+1} = \{x_\alpha\}_{\alpha\leq\lambda}$ verifichi la proprietà. Supponiamo per assurdo che non esista un tale x. Questo vuol dire che per ogni $x \in X_\lambda$ esiste un intorno di base V_x di y_λ e un intorno U_x di x tale che l'aperto

  $$V_x \times U_x \times Z_{\lambda+1}$$

  abbia un sottoricoprimento finito. Ma $\{U_x\}_{x\in X}$ è un ricoprimento di X_λ, che è uno spazio topologico compatto. Allora deve esistere un sottoricoprimento finito $U_{x_1}, \ldots, U_{x_n}$.

  Perciò esistono $x_1, \ldots, x_n$ tali che $U_{x_1}, \ldots, U_{x_n}$ ricoprono X_λ e

  $$V_{x_i} \times U_{x_i} \times Z_{\lambda+1}$$

  ha un sottoricoprimento finito per ogni $i = 1, \ldots, n$. Ma allora, posto $V = V_{x_1} \cap \ldots \cap V_{x_n}$, anche V è un aperto di base per Y_λ, e inoltre $V \times U_{x_i} \times Z_{\lambda+1}$ ha un sottoricoprimento finito per ogni $i = 1, \ldots n$. Ma quindi l'unione finita

  $$\bigcup_{i=1\ldots n} V \times U_{x_i} \times Z_{\lambda+1} = V \times Z_\lambda$$

  ha un sottoricoprimento finito (basta prendere l'unione dei sottoricoprimenti finiti dei singoli termini). Ma questo è assurdo, perché l'ipotesi induttiva su y_λ era che per nessun intorno di base V, l'insieme $V \times Z_\lambda$ ha sottoricoprimenti finiti. Perciò è possibile prolungare y_λ a $y_{\lambda+1}$.
- Supponiamo ora che λ sia un ordinale limite. Allora abbiamo una successione $\{x_\alpha\}_{\alpha<\lambda}$ tale che per ogni $\beta < \lambda$, $y_\beta = \{x_\alpha\}_{\alpha<\beta}$. Allora, se pongo $y_\lambda = \{x_\alpha\}_{\alpha<\lambda}$ posso scrivere ogni suo intorno di base come

  $$U \times \Pi_{\beta\leq\alpha<\lambda} X_\alpha$$

  dove $\beta < \lambda$ e U è un intorno di base di y_β. Questo perché ogni intorno di base di y_λ ha solo un numero finito di intorni non banali e λ è un ordinale limite. Ma allora per l'ipotesi induttiva ogni intorno di base di y_λ non ha, una volta completato, un sottoricoprimento finito. Quindi y_λ è il punto che stavamo cercando.

Perciò se poniamo $x = y_\gamma$, abbiamo che ogni intorno di base di x non ha sottoricoprimenti finiti. Ma questo è assurdo, per quanto visto prima.

9.7 Teorema di Tychonoff implica assioma della scelta

Quanto segue è preso da

`planetMath.org`

We prove that Tychonoff's theorem implies that product of non-empty set of non-empty sets is non-empty, which is equivalent to the axiom of choice (AC). This fact, together with the fact that AC implies Tychonoff's theorem, shows that Tychonoff's theorem is equivalent to AC (under ZF). The proof was first discovered by John Kelley in 1950, and is now an exercise in axiomatic set theory.

Proof. Let C be a non-empty collection of non-empty sets. Let Y be the generalized cartesian product of all the elements in C, namely, $Y = \{g : C \to \bigcup_{A\in C} A \mid g(A) \in A\}$. Our objective is show that Y is non-empty.

First, some notations: for each $A \in C$, set $X_A := A \cup \{A\}$, $D := \{X_A \mid A \in C\}$, X the generalized cartesian product of all the X_A's, and p_A the projection from X onto X_A.

We break down the proof into several steps:

1. Y is equipollent to $Z := \bigcap\{\mathsf{p}_A^{-1}(A) \mid A \in C\}$.

   An element of X is a function $f : D \to \bigcup D$, such that $f(X_A) \in X_A$ for each $A \in C$. In other words, either $f(X_A) \in A$, or $f(X_A) = A$. An element of Y is a function $g : C \to \bigcup C$ such that $g(A) \in A$ for each $A \in C$. Finally, $h \in \mathsf{p}_A^{-1}(A)$ iff $h(X_A) \in A$.

   Given $g \in Y$, define $g^* \in X$ by $g^*(X_A) := g(A) \in A$. Since A is arbitrary, $g^* \in Z$. Conversely, given $h \in Z$, define $h' \in Y$ by $h'(A) := h(X_A)$, which is well-defined, since $h(X_A) \in A$. Now, it is easy to see that the function $\phi : Y \to Z$ given by $\phi(g) = g^*$ is a bijection, whose inverse $\phi^{-1} : Z \to Y$ is given by $\phi^{-1}(h) = h'$. This shows that Y and Z are equipollent.

2. Next, we topologize each X_A in such a way that X_A is compact. Let τ_A be the coarsest topology containing the cofinite topology on X_A and the singleton $\{A\}$. A typical open set of X_A is either the empty set, or has the form $S \cup \{A\}$, where S is cofinite in A.

   To show that X_A is compact under τ_A, let $\mathcal{D}$ be an open cover for X_A. We want to show that there is a finite subset of $\mathcal{D}$ covering X_A. If $X_A \in \mathcal{D}$, then we are done. Otherwise, pick a non-empty element $S \cup \{A\}$ in $\mathcal{D}$, so that $A - S \neq \emptyset$, and is finite. By assumption, each element in $A - S$ belongs to some open set in $\mathcal{D}$. So to cover $A - S$, only a finite number of open sets in $\mathcal{D}$ are needed. These open sets, together with $S \cup \{A\}$, cover X_A. Hence X_A is compact.

3. Finally, we prove that Z, and therefore Y, is non-empty.

   Apply Tychonoff's theorem, X is compact under the product topology. Furthermore, π_A is continuous for each $A \in C$. Since $\{A\}$ is open in X_A, and $A = X_A - \{A\}$, A is closed in X_A, and thus so is $\mathsf{p}_A^{-1}(A)$ closed in X.

   To show that Z is non-empty, we employ a characterization of compact space: X is compact iff every collection of closed sets in X having FIP has non-empty intersection (esercizio: dimostrare che questa caratterizzazione della compattezza di uno spazio topologico è equivalente a quella data nella sezione 9.5). Let us look at the collection $\mathcal{S} := \{\mathsf{p}_A^{-1}(A) \mid A \in C\}$. Given $A_1, \ldots, A_n \in C$, pick an element $a_i \in A_i$, since $A_i \neq \emptyset$ by assumption. Note that this is possible, since there are only a finite number of sets. Define $f : D \to \cup D$ as follows:

$$f(X_A) := \begin{cases} a_i & \text{if } A = A_i \text{ for some } i = 1, \ldots, n \\ A & \text{otherwise} \end{cases}$$

   Since $f(X_{A_i}) = a_i \in A_i$, $f \in \mathsf{p}_{A_i}^{-1}(A_i)$ for each $i = 1, \ldots, n$. Therefore,

$$f \in \mathsf{p}_{A_1}^{-1}(A_1) \cap \ldots \cap \mathsf{p}_{A_n}^{-1}(A_n)$$

   Since $\mathsf{p}_{A_1}^{-1}(A_1)$, $\ldots$, $\mathsf{p}_{A_n}^{-1}(A_n)$ are arbitrarily picked from $\mathcal{S}$, the collection $\mathcal{S}$ has finite intersection property, and since X is compact, $Z = \bigcap S$ must be non-empty.

This completes the proof.

Remark. In the proof, we see that the trick is to adjoin the set $\{A\}$ to each set $A \in C$. Instead of $\{A\}$, we could have picked some arbitrary, but fixed singleton $\{B\}$, as long as $B \notin A$ for each $A \in C$, and the proof follows essentially the same way.

Bibliography

1. T. J. Jech, The Axiom of Choice. North-Holland Pub. Co., Amsterdam, 1973.

2. J. L. Kelley, The Tychonoff's product theorem implies the axiom of choice. Fund. Math. 37, pp. 75-76, 1950.

Appendice A

Il paradosso dell'ipergioco

Consideriamo due giocatori A e B che decidano di giocare tra loro solamente giochi che prima o poi finiscano. Essi decidono di considerare anche il seguente *ipergioco*: il primo giocatore sceglie un gioco finito e il secondo giocatore comincia poi con la prima mossa del gioco scelto dal primo giocatore. Ma sorge un problema: l'ipergioco è finito o no? Infatti se non lo consideriamo finito allora esso non può essere scelto dal primo giocatore e una partita all'ipergioco entra quindi dopo il primo passo in un gioco sicuramente finito e quindi anche una partita all'ipergioco sicuramente finisce; d'altra parte se l'ipergioco è finito allora esso può essere scelto dal primo giocatore alla sua prima mossa e a questo punto la prima mossa del secondo giocatore consiste nello scegliere un gioco finito, ma anch'egli può scegliere l'ipegioco e andando avanti in tal modo non si finisce mai una partita.

A.1 Formalizziamo l'ipergioco

Si può ottenere una controparte formale del paradosso dell'ipergioco che fornisce un utile strumento per fare dimostrazioni matematiche. A questo scopo consideriamo un qualsiasi insieme X e una qualsiasi relazione R tra gli elementi di X e introduciamo la seguente definizione.

Definition A.1.1 (R-fondatezza) *Sia X un insieme, R una relazione tra elementi di X e x un elemento di X. Allora x è R-fondato se e solo se non esiste alcuna funzione f dall'insieme dei numeri naturali N in X tale che $f(0) = x$ e, per ogni $n \in \mathsf{N}$, $f(n+1)\ R\ f(n)$, i.e.*

$$R\text{-}fondato(x) \equiv \neg(\exists f : \mathsf{N} \to X)\ (f(0) = x)\ \&\ (\forall n \in \mathsf{N})\ f(n+1)\ R\ f(n)$$

Possiamo ora dimostrare il seguente teorema.

Theorem A.1.2 *Sia X un insieme e sia R una relazione tra gli elementi di X. Allora non esiste alcun elemento $i \in X$ tale che, per ogni $x \in X$, $x\ R\ i$ se e solo se x è R-fondato.*

Dimostrazione. Supponiamo che esista $i \in X$ tale che, per ogni $x \in X$, $x\ R\ i$ se e solo se x è R-fondato.

Allora i sarebbe R-fondato perchè se supponiamo che esista una funzione $f : \mathsf{N} \to X$ tale che $f(0) = i$ e, per ogni $n \in \mathsf{N}$, $f(n+1)\ R\ f(n)$, allora varrebbe che $f(1)\ R\ f(0) = i$ e quindi l'implicazione da sinistra a destra della nostra assunzione darebbe che $f(1)$ è R-fondato. D'altra parte, se definiamo $g(n) \equiv f(n+1)$ otteniamo subito che $g(0) = f(1)$ e che, per ogni $n \in \mathsf{N}$, $g(n+1)\ R\ g(n)$ e quindi $f(1)$ non può essere ben fondato contro il risultato precedente.

Ma allora, la R-fondatezza di i, assieme con l'implicazione da destra a sinistra della nostra assunzione, implica $i\ R\ i$ e quindi dà la possibilità, ponendo $h(n) = i$, per ogni $n \in \mathsf{N}$, di definire una funzione costante $h : \mathsf{N} \to X$ tale che $h(0) = i$ e, per ogni $n \in \mathsf{N}$, $h(n+1)\ R\ h(n)$ che contraddice la R-fondatezza di i.

È forse il caso di notare che la prova vale intuizionisticamente.

A.2 Applicazioni

Vediamo subito alcune applicazioni del precedente teorema.

Theorem A.2.1 (Teorema di Cantor 1) *Sia X un insieme, $\mathcal{P}(X)$ sia la collezione dei sottoinsiemi di X e h sia una mappa da X in $\mathcal{P}(X)$. Allora esiste un elemento di $\mathcal{P}(X)$ che non è immagine secondo h di alcun elemento di X.*

Dimostrazione. Sia R la relazione tra elementi di X definita ponendo

$$x\ R\ y \equiv x \in h(y)$$

e consideriamo il sottoinsieme F degli elementi di X che sono R-fondati. Non può allora esistere alcun elemento $i \in X$ tale che $F = h(i)$ perchè altrimenti avremmo che $x\ R\ i$ se e solo se $x \in h(i)$ se e solo se x è R-fondato.

Theorem A.2.2 (Teorema di Cantor 2) *Sia N l'insieme dei numeri naturali, $\mathsf{N} \to \mathsf{N}$ sia l'insieme delle funzioni da N in se e h sia una mappa da N in $\mathsf{N} \to \mathsf{N}$. Allora esiste una funzione in $\mathsf{N} \to \mathsf{N}$ che non è immagine secondo h di alcun elemento di N.*

Dimostrazione. Sia R la relazione tra elementi di N definita ponendo

$$x\ R\ y \equiv h(y)(x) = 0$$

e consideriamo la funzione $f : \mathsf{N} \to \mathsf{N}$ definita ponendo $f(x) = 0$ se x è R-fondato, $f(x) = 1$ altrimenti, i.e., f è la funzione caratteristica degli R-fondati. Non può allora esistere alcun elemento $i \in \mathsf{N}$ tale che $f = h(i)$ perchè altrimenti avremmo che $x\ R\ i$ se e solo se $h(i)(x) = 0$ se e solo se $f(x) = 0$ se e solo se x è R-fondato.

Theorem A.2.3 (Teorema di Cantor 3) *Sia X un insieme, $X \to \mathsf{Boole}$ sia l'insieme delle funzioni da X in $\mathsf{Boole} \equiv \{\mathsf{true}, \mathsf{false}\}$ e h sia una mappa da X in $X \to \mathsf{Boole}$. Allora esiste una funzione in $X \to \mathsf{Boole}$ che non è immagine secondo h di alcun elemento di X.*

Dimostrazione. Sia R la relazione tra elementi di X definita ponendo

$$x\ R\ y \equiv h(y)(x) = \mathsf{true}$$

e consideriamo la funzione $f : X \to \mathsf{Boole}$ definita ponendo $f(x) = \mathsf{true}$ se x è R-fondato, $f(x) = \mathsf{false}$ altrimenti, i.e., f è la funzione caratteristica degli R-fondati. Non può allora esistere alcun elemento $i \in X$ tale che $f = h(i)$ perchè altrimenti avremmo che $x\ R\ i$ se e solo se $h(i)(x) = \mathsf{true}$ se e solo se $f(x) = \mathsf{true}$ se e solo se x è R-fondato.

Appendice B

Buoni ordini sui numeri naturali

Quanto segue è preso da ???

In this document I attempt to build some intuition for the ordinals by constructing several concrete well-orderings of the naturals with order types up to (and including!) ϵ_0.

Ordinals are all about well-orderings. A well ordering of the naturals is an ordering – call it $\prec$ – on the naturals that has no infinitely descending chains. So the *reverse ordering*, i.e. $x \prec y$ iff $y < x$, is obviously not a well-ordering because it has the infinitely descending chain $1 \succ 2 \succ 3 \succ \ldots$.

However, the usual ordering is a well-ordering, because if you start at n, you only get at most n steps before you have to hit 0. The usual ordering is called "omega", which I denote ω.

However, let's take zero out and put it at the top. So 0 is greater than all other numbers, and the other numbers use the usual ordering:

$$1\ 2\ 3\ 4\ 5\ 6\ \ldots\ 0$$

This is also a well-ordering, but a bit more subtly. If you start at n, you only get at most $n-1$ steps to get to the least element 1. But if you start at 0, there is no longer a bound on how many steps it will take. But you have to choose some number less than 0 to descend to, and that number will be finite, giving a finite number of steps. We call this ordering $\omega + 1$.

Ordinals are equivalence classes of well-orderings; that is, if you make an order isomorphism between the naturals and themselves with a different order, those will be represented by the same ordinal. So we are really interested in seeing the structure of what is less than what, rather than the specific numbers. But I wanted to use specific numbers to make it more "real"; what does an order of type ω^2 look like, after all? And we will go far beyond w^2.

When I'm writing these down, I try to use a number of dots corresponding to the number of "levels of iteration" that I am hand waving over. This kind of breaks down when we get to w^w, so it turns into more of a suggestive intuition than something formal.

Without further ado! The simplest ordinals:

$$\begin{array}{lcl}
\omega & = & 0\ 1\ 2\ \ldots \\
\omega + 1 & = & 1\ 2\ 3\ \ldots 0 \\
\omega + \omega (= \omega \cdot 2) & = & 0\ 2\ 4\ \ldots\ 1\ 3\ 5\ \ldots \\
\omega \cdot 2 + 1 & = & 1\ 3\ 5\ \ldots\ 2\ 4\ 6\ \ldots 0 \\
\omega \cdot 3 & = & 0\ 3\ 6\ \ldots\ 1\ 4\ 7\ \ldots\ 2\ 5\ 8\ \ldots
\end{array}$$

For $\omega \cdot \omega$, we need to get a copy of ω at each point in ω; that is, an infinite series of infinite sequences.

Let

$$B(n) = \text{ the increasing sequence of binary numbers with } n \text{ 1s.}$$

Then

$$\begin{array}{rcl}
\omega \cdot \omega (= \omega^2) & = & 0\ 1\ 2\ 4\ 8\ \ldots\ \ 3\ 5\ 6\ 9\ \ldots\ \ 7\ 11\ 13\ 14\ \ldots\ \ldots \\
& \equiv & [B(1)\ \ \ \ \ ]\ [B(2)\ \ \ \ \ ]\ [B(3)\ \ \ \ \ \ \ ]\ \ldots
\end{array}$$

For ω^3, we need to get a copy of ω at each point in ω^2. $B^*(S)$ gets the sequence for each number in S and "concatenates" them.

$$
\begin{array}{lcccccccccccccccc}
\omega^3 & = & 0\ 1\ 2\ 4\ \ldots & & 3\ 5\ 6\ 9\ \ldots & & 15\ 23\ \ldots\ \ldots & & 7\ 11\ \ldots & & 31\ 47\ \ldots\ \ldots & & 127\ 191\ \ldots & & 2047\ 3071\ \ldots\ \ldots \\
 & & [B(1) &] & [B(2) &] & [B(4) &] \ldots & [B(3) &] & [B(5) &] \ldots & [B(7) &] & [B(11) &] \ldots \\
 & & [B^*(B(1)) & & & & &] & [B^*(B(2)) & & &] & [B^*(B(3)) & & &] \ldots
\end{array}
$$

For order type ω^ω, we need to construct an ordering which contains ω^n for each natural n. Order lexicographically by prime decomposition, comparing larger primes before smaller ones.

$$
\begin{array}{ll}
1 & = 1 \\
2^1 & = 2 \\
2^2 & = 4 \\
2^3 & = 8 \\
\ldots & \\
3^1 & = 3 \\
3^1 * 2^1 & = 6 \\
3^1 * 2^2 & = 12 \\
3^1 * 2^3 & = 24 \\
\ldots & \\
3^2 & = 9 \\
3^2 * 2^1 & = 18 \\
3^2 * 2^2 & = 36 \\
\ldots & \\
5^1 & = 5 \\
5^1 * 2^1 & = 10 \\
5^1 * 2^2 & = 20 \\
\ldots & \\
5^1 * 3^1 & = 15 \\
5^1 * 3^1 * 2^1 & = 30\ldots \\
5^2 & = 25 \\
5^2 * 3^1 & = 75 \\
5^2 * 3^1 * 2^1 & = 150\ldots \\
7^1 & = 7 \\
\ldots & \\
\ldots &
\end{array}
$$

Note that a number is a successor if and only if it has a factor of 2. If n is the p-th prime, then the order type of all numbers less than n in this ordering is ω^p.

For $\omega^{\omega^\omega} (= \omega^{(\omega^\omega)})$, we still use the prime decomposition, but we compare the primes according the ω^ω ordering above as opposed to the usual ω ordering, by acting on their prime *index*.

So factors of 2 (the 1-st prime) are still successors, the next limit is 3 (the 2-nd prime), the

next limit is 7 (the 4-th(!) prime), etc.

$$
\begin{array}{lcll}
1 & = & 1 & \\
2^1 & = & 2 & \text{(prime 1)} \\
2^2 & = & 4 & \\
\ldots & & & \\
3^1 & = & 3 & \text{(prime 2)} \\
3^1 \cdot 2^1 & =^6 & & \\
3^1 \cdot 2^2 & = & 12 & \\
\ldots & & & \\
3^2 & = & 9 & \\
3^2 \cdot 2^1 & = & 18 & \\
\ldots & & & \\
7^1 & = & 7 & \text{(prime 4)} \\
7^1 \cdot 2^1 & = & 14 & \\
\ldots & & & \\
7^1 \cdot 3^1 & = & 21 & [\ldots] \\
7^1 \cdot 3^2 & = & 63 & \\
\ldots & & & \\
7^2 & = & 49 & \\
\ldots & & & \\
5^1 & = & 5 & \text{(prime 3)} \\
5^1 \cdot 2^1 & = & 10 & [\ldots] \\
5^1 \cdot 3^1 & = & 15 & [\ldots] \\
5^1 \cdot 7^1 & = & 35 & [\ldots] \\
\ldots & & & \\
13^1 & = & 13 & \text{(prime 6)} \\
\ldots & & & \\
23^1 & = & 23 & \text{(prime 9)} \\
\ldots & & & \\
11^1 & = & 11 & \text{(prime 5)} \\
\ldots & & &
\end{array}
$$

And so on, with the primes following the ω^ω ordering. The number 5 in this ordering has a copy of ω^ω below it (5 is the 3-rd prime, 3 is the first limit ordinal in ω^ω).

We can iterate this process to get all the ordinals below ϵ_0 (all $\omega^{\omega^{\omega^{\cdots^\omega}}}$ some finite number of times), by using the previous ordering O to order the primes ω^O.

We are almost to understanding ϵ_0, the proof theoretic ordinal of Peano Arithmetic (that is, the least ordinal that PA cannot prove is well-ordered). That means that the ordering we construct for ϵ_0, assuming we get there, will be beyond PA's grasp.

ϵ_0 is the least fixed point of $(\omega^\cdot)$, that is, $\omega^{\epsilon_0} = \epsilon_0$. So if we do this crazy relabeling-of-primes-and-lexicographic-ordering process using ϵ_0 as the ordering on prime indices, what we get back has the same order type as ϵ_0. That doesn't really help us construct a concrete ordering, since the numbers may be different; all we know is their order type is the same.

How shall we compute a concrete ordering for ϵ_0? It must contain all the orderings constructed above, ω, ω^ω, ω^{ω^ω}. There is a straightforward construction from this idea, that we could have used for taking limits at earlier stages (but it would give rise to less-understandable simple orderings). Prime-decompose the number, and let the exponent on the power of 2 select which of these orderings we will use on *the rest*. To construct the rest, shift all the primes down by one. So for example:

$$84 = 2^2 \cdot 3^1 \cdot 7^1$$

2^2 means interpret from ω^{ω^ω}

$3^1 \cdot 7^1$ "shifted down" is $2^1 \cdot 3^1 = 6$

So 84 has the same position as 6 in ω^{ω^ω} (the successor of 3, which is the first limit ordinal, so $84'' ='' \omega + 1$)

We will denote this $(2, 6)$

And we say that first we compare on the power of 2. So $2^6 \cdot$ stuff $> 2^4 \cdot$ stuff . It's only when they are equal that we compare them according to that power's associated "omega tower" ordering.

(all odd numbers appear below in ω ordering)

$$\begin{array}{lcll} (0,1) & = & 2^0 & = 1 \\ (0,2) & = & 2^0 \cdot 3^1 & = 3 \\ (0,3) & = & 2^0 \cdot 5^1 & = 5 \\ (0,4) & = & 2^0 \cdot 3^2 & = 9 \\ (0,5) & = & 2^0 \cdot 7^1 & = 7 \\ \ldots & & & \end{array}$$

(numbers with exactly one factor of 2 appear below in ω^ω ordering)

$$\begin{array}{lcll} (1,1) & = & 2^1 & = 2 \\ (1,2) & = & 2^1 \cdot 3^1 & = 6 \\ (1,4) & = & 2^1 \cdot 3^2 & = 18 \\ (1,8) & = & 2^1 \cdot 3^3 & = 54 \\ \ldots & & & \\ (1,3) & = & 2^1 \cdot 5^1 & = 10 \\ (1,6) & = & 2^1 \cdot 3^1 \cdot 5^1 & = 30 \\ \ldots & & & \\ (1,5) & = & 2^1 \cdot 7^1 & = 14 \\ (1,10) & = & 2^1 \cdot 3^1 \cdot 7^1 & = 42 \\ \ldots & & & \end{array}$$

(numbers with exactly 2 factors of 2 appear below in ω^{ω^ω} ordering)

$$\begin{array}{lcll} (2,1) & = & 2^2 & = 4 \\ (2,2) & = & 2^2 \cdot 3^1 & = 12 \\ (2,4) & = & 2^2 \cdot 3^2 & = 36 \\ \ldots & & & \\ (2,3) & = & 2^2 \cdot 5^1 & = 20 \\ (2,6) & = & 2^2 \cdot 3^1 \cdot 5^1 & = 60 \\ \ldots & & & \\ (2,7) & = & 2^2 \cdot 11^1 & = 44 \\ \ldots & & & \end{array}$$

(numbers with 3 factors of 2 appear in $\omega^{\omega^{\omega^\omega}}$ ordering)

$$\ldots$$

This is a concrete ordering of the integers with order type ϵ_0. It is computable (for fun, write a program that computes it!). You can start from any number and pick a number at random (or equivalently, according to some input) that is less than it in this ordering, and you will always eventually hit 1. However, the axioms of Peano arithmetic are not strong enough to prove this fact; so really you will only always hit 1 if you believe in axioms stronger than PA. Real question, philosophical answer :-)

Appendice C

Prigionieri e cappelli

Quanto segue è preso da ???

Imagine a queue of infinitely many prisoners numbered 0, 1, 2, ... Randomly, each of them is assigned a black or a white hat. Each prisoner can only see the hats of the fellow inmates in front of him (i.e. the hats of the inmates who have a higher number than he has). The guard asks each prisoner in turn to guess the color of his hat, without the other prisoners being able to hear his reply.

If the prisoner answers correctly, he will be released. If not, he has to stay in prison for the rest of his life. After being given the rules of the game, the prisoners get one hour to determine their strategy. One of them, a classical mathematician accepting the Axiom of Choice, says 'I have a plan that ensures at most finitely many of us guess wrongly'.

C.1 La soluzione

As said, the classical mathematician accepting the Axiom of Choice, claims they can ensure that at most finitely many guess wrong. His plan is as follows. Consider the equivalence relation on C, the set of all the possible sequences of hats, namely, the set of functions from Nat to $\{\text{black}, \text{white}\}$, defined by, for all $\alpha, \beta \in C$,

$$\alpha \sim \beta \equiv \exists n \forall m > n[\alpha(m) = \beta(m)]$$

In other words: α and β are equivalent if and only if they are almost everywhere the same.

How does this relation help the prisoners? Each distribution of hats can be seen as a sequence of zeros and ones (saying each black hat is a one and each white hat a zero). Before they line up, the prisoners together select, using the Axiom of Choice(!), one representative from each equivalence class. During the game there are only finitely many hats a prisoner cannot see, so he can decide in which equivalence class the actual hat distribution is. He guesses the hat color he would have if the chosen representative of that class were the actual situation. As the sequence resulting from the guesses of the prisoners and the actual sequence are in the same equivalence class, they differ only in finitely many positions. This means at most finitely many prisoners guess wrong.

A nice puzzle: change the situation to 100 prisoners, each of them being able to hear the answers of the inmates behind him. How can they ensure (without cheating or using the Axiom of Choice!) at most one of them guesses wrong?

Risposta: il primo prigioniero dice il colore del cappello del prigioniero di fronte a lui (e se è fortunato questo è anche il colore del suo cappello, altrimenti ...); a questo punto il prossimo prigioniero sa il colore x del suo cappello e può quindi rispondere correttamente "Il mio cappello è x" se intende comunicare che il cappello di fronte a lui è ancora di colore x oppure "È x il mio cappello" se intende comunicare che il cappello di fronte al suo non è di colore x.

Bibliografia

[A63] K.J. Arrow, *Social choice and individual values*, John Wiley and Sons, Inc., New York, London, Sydney 1963

[BM77] J. L. Bell and M. Machover, *A course in mathematical logic*, Amsterdam : North-Holland Pub. Co. ; New York : Elsevier Pub. Co., 1977

[Bir67] Birkhoff, G., *Lattice Theory*, 3rd ed. Vol. 25 of American Mathematical Society Colloquium Publications. American Mathematical Society, 1967.

[Bolz1817] Bolzano, B., *Rein analytischer Beweis.*

[BBJ07] Boolos G., Burgess J., Jeffrey R., *Computability and Logic*, Cambridge University Press

[Can32] Cantor, G., *Gesammelte Abhandlungen*, Berlin: Springer-Verlag, 1932

[Coh66] Cohen, P., *Set theory and the continuum hypothesis*, New York (1966)

[D82] G. dall'Aglio, *Decisioni di gruppo: il paradosso di Arrow*, Archimede, vol. XXXIV n. 1-2 (1982), pp 3-14

[Gal79] Gale, D., *The game of Hex and the Brouwer Fixed-Point Theorem*, The American Mathematical Monthly, vol. 86 (10), 1979, pp. 818–827.

[Gar59] Gardner, M., *The Scientific American Book of Mathematical Puzzels and Diversions*, Simon and Schuster, New York, 1959, pp. 73–83.

[God38] Gödel, K., *The consistency of the axiom of choice and the generalized continuum hypothesis*, Proceedings of the National Academy of Sciences (U.S.A), 24(1938), pp. 556-557.

[HJ99] Hrbacek, K. and Jech, T., *Introduction to Set Theory*, New York: Marcel Dekker, Inc. (1999)

[Jec2011] Jech, Thomas, *Set Theory*, The Stanford Encyclopedia of Philosophy (Winter 2011 Edition), Edward N. Zalta (ed.), URL = ¡http://plato.stanford.edu/archives/win2011/entries/set-theory/¿.

[Jen72] Jensen, R., *The fine structure of the constructible hierarchy*, Ann. Math. Logic, 4 (1972), pp. 229-308.

[EK09] C. Klamler and D. Eckert, *A Simple Ultrafilter Proof For an Impossibility Theorem in Judgment Aggregation*, Economics Bulletin, 2009

[LL94] L. Lawers and L. Van Liedekerke, *Ultraproducts and Aggregation*, Journal of Mathematical Economics, 1994

[LeoTof07] Leonesi, S., Toffalori, C., *Matematica, miracoli e paradossi*, Bruno Mondadori editore

[MS89] Martin, D. and Steel, J., *A proof of projective determinacy*, J. Amer. Math. Soc., 2 (1989), pp. 71-125.

[Mat1970] Y. Matiyasevich, *Enumerable sets are Diophantine*, Doklady Akademii Nauk SSSR, 191, pp. 279-282, 1970, Traduzione inglese in Soviet Mathematics. Doklady, vol. 11, no. 2, 1970

[MV11] A. Montino and S. Valentini, *Generalizing Arrow's theorem: a logical point of view*, in corso di pubblicazione

[Rasiowa-Sikorski 63] H. Rasiowa, R. Sikorski, *The mathematics of metamathematics*, Polish Scientific Publishers, Warsaw, 1963

[Sco61] Scott, D., *Measurable cardinals and constructible sets*, Bull. Acad. Pol. Sci., 9 (1961), pp. 521-524.

[Smullyan81] R. Smullyan, *Quale è il titolo di questo libro?* Zanichelli, Bologna, 1981

[Smullyan85] R. Smullyan, *Donna o tigre?* Zanichelli, Bologna, 1985

[Smullyan92] R. Smullyan, *Gödel incompleteness Theorems* Oxford University Press, Oxford, 1992

[Takeuti 75] G. Takeuti *Proof Theory*, North Holland, 1975

[Ula30] Ulam, S., *Zur Masstheorie in der allgemeinen Mengenlehre, Fund. Math., 16 (1930, pp. 140-150.*