Numbers, Ordinals and Cardinals

Klaus Sutner

Carnegie Mellon University

50-ordinals   2017/12/15 23:22

We have seen how to implement natural numbers as sets, using the successor function $S(x) = x \cup \{x\}$.

$$\underline{0} \rightsquigarrow \emptyset$$
$$\underline{n} \rightsquigarrow \underbrace{S(S(\ldots S(\emptyset)\ldots))}_{n}$$

Of course, we cannot define

$$\mathbb{N} = \{\, \underline{n} \mid n \in \mathbb{N} \,\}$$

but this problem is not hard to circumvent.

Let us say that a set X is inductive if $\emptyset \in X$ and $x \in X$ implies $S(x) \in X$.

Thus, an inductive set contains the empty set and is closed under successors. We can now define

$$\mathbb{N} = \bigcap \{ X \mid X \text{ inductive} \}$$

It is easy to check that the intersection produces the right set, inductive sets that are too large are being cut back.

If you want to quibble you can point out that this definition is not predicative: the set we define on the left is part of the big set on the right. Don't worry, be happy.

It is straightforward to check that $\langle \mathbb{N}, S, \emptyset \rangle$ is a model of the Peano axioms, at least with signature $(1, 0)$. If one wants to include addition, multiplication and order one needs to augment the structure in the obvious way.

The induction axiom schema

$$P(0) \wedge \forall x \, (P(x) \rightarrow P(x^{+})) \rightarrow \forall x \, P(x)$$

is, of course, directly justified by our construction of $\mathbb{N}$.

Using the Peano axioms we can check that $\langle \mathbb{N}, +, 0 \rangle$ is a commutative monoid with cancellation.

But, we cannot solve all equations $a + x = b$ in this monoid, for that we need the integers. At present, writing $x = b - a$ makes no sense if a and b are von Neumann ordinals.

So the question is, how should we represent the integers as sets?

One might be tempted to use a data structure approach and add a "sign bit" to a natural number:

$$\mathbb{Z} = \{ (a,b) \mid a \in N, b \in \mathbf{2} \}$$

with the intent that (a,b) represents $(-1)^b \cdot a$.

To be sure, this produces a perfectly good carrier set on which to define the necessary operations.

But: the actual constructions are very combinatorial in nature and really a major pain.

Exercise

Define addition and multiplication in this context.

Here is a better method. We would like to adjoin the solution of $a + x = b$ to $\mathbb{N}$, for all a, b.

To avoid visual clutter, lets just write (a, b) for this solution.

Intuitively, (a, b) stands for $b - a$ (but the latter is currently not properly defined).

So our first attempt will be to use $Z = \mathbb{N} \times \mathbb{N}$ as the set of integers.

Note that we do not lose the naturals, we can identify b with $(0, b)$.

Of course, for this to make sense we also need to explain how to add and multiply elements in Z.

A moment's thought shows that we need to define

$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b) \cdot (a', b') = (ab' + a'b, aa' + bb')$$

It is straightforward to check that these operations behave as expected.

Exercise

Show that both operations as defined above are associative and commutative, and they extend the operations on $\mathbb{N}$.

Alas, there is one glitch: different equations may have the same solution. In fact, we are representing each integer in infinitely many ways as $(a + c, b + c)$.

No problem, define the relation

$$(a, b) \sim (a', b') \iff a + b' = a' + b.$$

It is easy to check that $\sim$ is indeed an equivalence relation.

Claim: $\sim$ is a congruence in the sense that

$$(a, b) \sim (a', b'), (c, d) \sim (c', d') \implies (a + c, b + d) \sim (a' + c', b' + d')$$

A similar claim holds for multiplication.

It now follows from general algebra that the quotient structure

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$$

is another commutative monoid.

As a set, this version of $\mathbb{Z}$ is much more complicated than the "sign bit" version. But the operations are naturally inherited from $\mathbb{N}$.

And it is not hard to show that $\langle \mathbb{Z}, +, 0 \rangle$ is in fact a group.

A little more work shows that $\langle \mathbb{Z}, +, *, 0, 1 \rangle$ is a ring.

We have a chain of constructions

$$\mathbb{N} \rightsquigarrow \mathbb{Z} \rightsquigarrow \mathbb{Q} \rightsquigarrow \mathbb{R} \rightsquigarrow \mathbb{C}$$

which forms the background for much of classical mathematics.

But there is another way in which we can extend $\mathbb{N}$, an extension towards infinity. More precisely, we do not add any negative numbers but transfinite numbers, numbers that are larger than all natural numbers.

Exercise

In $\mathbb{Z}$ all equations $a + x = b$ have a solution, but equations $a * x = b$ may not have solutions. Use a similar construction to adjoin solutions for these equations and construct the rational numbers $\mathbb{Q}$.

Exercise

$\mathbb{Q}$ is a field (there are multiplicative inverses), but it is not the right setting for calculus: there are too many holes in $\mathbb{Q}$ to form limits. Find a way to extend $\mathbb{Q}$ by filling the holes and obtain the real numbers $\mathbb{R}$.

This is no longer an algebraic construction and much harder. Look up Dedekind cuts on the web.

Exercise

Lastly, show how to extend $\mathbb{R}$ to $\mathbb{C}$, the field of complex numbers. This is again a purely algebraic construction and fairly straightforward.

Of course, the challenge here is not just to introduce some new sets and define them to be larger than all n, we need to carry over arithmetic.

In particular we have to make sense out of addition, multiplication and exponentiation of transfinite numbers.

As it turns out, this is a major project, in particular for the kinds of transfinite numbers that measure the size of a set (so-called cardinals).

Cantor's early work is in analysis. He was interested in exploring the limits of Fourier analysis. Suppose f is are real-valued function over $(-\pi, \pi)$. Then we can write f as a trigonometric series

$$f(x) = b_0/2 + \sum_{n \geq 1} a_n \sin(nx) + b_n \cos(nx).$$

Fourier discovered how to calculate the coefficients (via an integral involving f and trig functions).

As it turns out, this representation is unique: f determines the coefficients uniquely.

In fact, it was known that continuity over $(-\pi, \pi) - F$ where F is a finite set was sufficient for uniqueness.

Cantor realized that if the RHS converged for all $x \in (-\pi, \pi)$ the coefficients were also uniquely determined.

The question arose whether uniqueness could be guaranteed for functions that were defined only over

$$(-\pi, \pi) - U$$

where U is some suitable set.

Trying to identify the most general admissible kind of set U lead Cantor to consider the following construction.

Definition

Let $A \subseteq \mathbb{R}$ closed. A point $a \in \mathbb{R}$ is isolated (in A) if there exists a neighborhood of a that is disjoint from A. Otherwise a is a limit point or accumulation point. A is perfect if it has no isolated points.

Perfect sets can be constructed from arbitrary closed sets by removing isolated points. Write

$$X' = \{\, x \in X \mid x \text{ limit point} \,\}$$

Unfortunately, $A' \subseteq A$ may not be perfect, either. So we repeat the process: A'', A''' and so on. More precisely, we form a sequence $A^{(0)} = A$, $A^{(n+1)} = {A^{(n)}}'$ for all $n \in \mathbb{N}$.

Exercise

Show that it may happen that $A^{(n)}$ contains isolated points, for all n.

There is no guarantee that $A^{(n)}$ will be perfect for any $n \in \mathbb{N}$.

How do we continue our pruning process beyond the first infinitely many stages?

It's a fair guess that we should consider $\bigcap A_n$ next. We use ω to denote this next stage in the process.

$$A^{(\omega)} = \bigcap_{n < \omega} A^{(n)}$$

The weary reader might expect at this point that $A^{(\omega)}$ is not necessarily perfect either.

So we continue our pruning process with stages $\omega + 1$, $\omega + 2$, ... We get to a stage $\omega + \omega = 2\omega$, then 3ω, and even $\omega\omega = \omega^2$, and further to ω^3 and so on, ad nauseam.

This is just wild and woolly notation so far, we have not defined these stage objects, much less their arithmetic.

Exercise

Why must this process ultimately end?

We want to define a class On of stage objects, henceforth called ordinals. The conditions are

- There is a unique least ordinal, denoted 0.

- For every ordinal α there is a unique least larger ordinal, denoted $\alpha + 1$.

- For every increasing sequence (α_i) of ordinals, there is a unique least upper bound, denoted $\sup \alpha_i$.

We are cheating a bit, of course: we also need to define an order relation $<$ on On.

Disregarding 0, there are two types of ordinals:

- Successor ordinals of the form $\alpha + 1$. These indicate the step immediately following step α.
- Limit ordinals of the form $\lambda = \sup X$. These indicate the collection of all prior steps into one super-step.

For example, for any limit ordinal λ we have

$$\alpha < \lambda \text{ implies } \alpha + 1 < \lambda.$$

It is customary to write ω for the smallest limit ordinal.

Note that we can identify $\mathbb{N}$ with an initial segment of this order: 0 is the least ordinal, 1 its successor, 2 the successor of 1, and so on. It is tempting to think of ω as just being $\mathbb{N}$, but it's helpful to have special notation for this number.

There is another problem: sequences are usually indexed by $\mathbb{N}$, but we need much larger index sets. To get around this, we need to insist that $\sup X$ exists for any set $X \subseteq On$.

Careful, On is not a set but a proper class, so there is no contraction between the two conditions (On does not have a largest element).

Disregarding 0, there are two types of ordinals:

- Successor ordinals of the form $\alpha + 1$. These indicate then next step immediately following step α.
- Limit ordinals of the form $\lambda = \sup X$. These indicate the collection of all prior steps into one super-step.

For example, for any limit ordinal λ we have

$$\alpha < \lambda \text{ implies } \alpha + 1 < \lambda.$$

It is customary to write ω for the smallest limit ordinal.

It is tempting to think of ω as just being $\mathbb{N}$, but it's helpful to have special notation for this number.

Definition

A structure $\langle A, \lhd \rangle$ is a well-order if $\lhd$ is a total order on A and every non-empty subset of A has a $\lhd$-minimal element.

The classical example of a well-order is $\langle \mathbb{N}, < \rangle$. The integers and the positive rationals are the standard counterexample.

Lemma

$\langle A, \lhd \rangle$ *is a well-order if, and only if, there are no infinite descending chains in this order.*

In other words, we must not have a sequence

$$a_0 \rhd a_1 \rhd a_2 \rhd \ldots \rhd a_n \rhd \ldots$$

Exercise

Prove the lemma (using intuitive set theory).

A key question in the early development of set theory was whether every set can be well-ordered. In fact, Hilbert on his famous list of open problems placed well-ordering the reals (think of them as Cantor space $2^{\mathbb{N}}$ in this context) on top of the list.

Cantor thought this was "self-evident" because we construct the required order in stages. To well-order A construct a sequence a_α in stages

$$a_\alpha = \text{ pick some } x \in (A - \{\, x_\beta \mid \beta < \alpha \,\})$$

The problem is the "pick some" operations: A is an abstract set and there is no clear mechanism how this choice should be made. We need some high-powered axiom to make the selection of an element in an arbitrary, non-empty set possible: the Axiom of Choice.

The following principles are equivalent to the Axiom of Choice, but often easier to apply in concrete situations.

- The Well-Ordering Principle: every set can be well-ordered.

- Zorn's lemma: every partial order in which every chain has an upper bound contains a maximal element.

- Hausdorff's Maximality Principle: every partial order has a maximal chain.

- Every equivalence relation has a set of representatives.

Zorn's lemma was popularized in particular by Bourbaki.

We won't worry about foundational issues and simply assume either and all of the above.

Well-orders are centrally important to termination of recursive procedures. Suppose some recursive function f when called on x makes a recursive call to y, where x and y belong to some ground set A.

If we can find a well-order $\lhd$ on A such that $y \lhd x$ then any call is always guaranteed to terminate: otherwise we would have an infinite descending chain.

As an example, consider the Ackermann function $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$A(0, y) = y^+$$
$$A(x^+, 0) = A(x, 1)$$
$$A(x^+, y^+) = A(x, A(x^+, y))$$

The standard proof for A being total is by induction on x and subinduction on y. This is a perfectly civilized approach, but it obscures some of the finer points.

It may seem that any recursive definition along the lines of Ackermann's is automatically guaranteed to produce a well-defined, total function. Alas, that's most emphatically not the case.

$$f(0, 0) = 0$$
$$f(x + 1, y) = f(x, y + 1)$$

$$g(x, 0) = x + 1$$
$$g(x, y + 1) = g(x + 1, y)$$
$$g(x + 1, y + 1) = g(x, g(x, y))$$

Exercise

Explain what goes wrong in the definitions of f and g above.

The ground set here is $A = \mathbb{N} \times \mathbb{N}$. There is a natural order on A, namely the lexicographic order:

$$(a, b) \prec (c, d) \iff (a < c) \vee (a = c \wedge b < d).$$

This order is a well-order and it is easy to see that whenever a call to Y is nested inside a call to X we have $Y \prec X$:

$(x, 0) \succ (x - 1, 1),$

$(x, y) \succ (x, y - 1), (x - 1, z).$

Thus termination is guaranteed.

Exercise

Prove that $\langle A, \prec \rangle$ is indeed a well-order.

Unlike arbitrary total orders, well-orders are always comparable in a very strict sense.

Suppose $\langle A, \lhd \rangle$ is a well-order. We can enumerate the elements of A by constructing a partial function $f : On \to A$ defined by

$$f(0) = \min_{\lhd}(A)$$

$$f(\alpha + 1) = \min_{\lhd}(A - \{f(0), \ldots, f(\alpha)\})$$

$$f(\lambda) = \min_{\lhd}(A - \{\, f(\nu) \mid \nu < \lambda \,\}$$

Note the domain of f is an initial segment of On, so we get an order isomorphism

$$f : \{\, \alpha \in On \mid \alpha < \beta \,\} \to A$$

The ordinal β is uniquely determined by A, so we can propose the following measure of the length of a well-order.

Definition

The ordinal β such that that there is an order isomorphism from $\{\, \alpha \in On \mid \alpha < \beta \,\}$ to A is the order type or length of A.

Note that any two well-orders are comparable in the sense that one must be isomorphic to an initial segment of the other.

The length of a well-order is a successor ordinal if the order has a largest element, and a limit ordinal otherwise.

So, in a sense all well-orders reduce to initial segments of the ordinals. This fact is particularly useful since we can naturally define arithmetic of ordinals – which produces a handy notation system for well-orders.

We can extend the classical principle of induction on the naturals to induction on On.

Definition

Let $\Phi(x)$ be some formula where x is supposed to range over ordinals. Φ is inductive if $\forall\, \beta < \alpha\; \Phi(\beta) \Rightarrow \Phi(\alpha)$.

Theorem

If $\Phi(x)$ is inductive then $\Phi(\alpha)$ holds for all $\alpha \in On$.

Likewise, we can define "recursive" functions on the ordinals, using recursion much in the same way as for natural numbers.

Here is the version with an additional set parameter.

Theorem (von Neumann, 1923, 1928)

Given a function $F(x,y)$ defined on sets, there is a unique function $f : V \times On \to V$ defined by

$$f(x,\alpha) = F(x, \lambda z f(x,z) \restriction \alpha).$$

Note that this definition works for all ordinals α. In practice, it may still be convenient to distinguish between arguments 0, successor ordinals and limit ordinals.

Consider the well-ordering $A = \langle \mathbb{N} \times \mathbb{N}, < \rangle$ with the usual lexicographic order. We can define an order isomorphism $f : \lambda \to A$ for some limit ordinal λ by transfinite recursion:

$$f(\nu) = \min{}_< (A - \{\, f(\alpha) \mid \alpha < \nu \,\})$$

The right hand side is well-defined as long as $A \neq \{\, f(\alpha) \mid \alpha < \nu \,\}$. In other words, we can think of $f \colon On \hookrightarrow A$ as a partial function whose domain is some initial segment λ of On.

This ordinal λ is the order type of our well-order. Note that λ must be a limit ordinal since A fails to have a largest element.

In this case it is not hard to given an explicit description of f and λ.

Note that any ordinal below ω^2 can be written uniquely in the form $\alpha = \omega^n + m$ for $n, m < \omega$. Then

$$f(\alpha) = (n, m)$$

and $\lambda = \omega^2$: we have $A = \{\, f(\alpha) \mid \alpha < \omega^2 \,\}$ and the recursion stops.

Exercise

What is the order type of $\mathbb{N}^k$ under lexicographic order?

Here is another well-order: $B = \langle \mathbb{N}_+, \prec \rangle$ where

$$n \prec m \iff \nu_2(n) < \nu_2(m) \vee \nu_2(n) = \nu_2(m) \wedge n < m.$$

Here $\nu_2(x)$ is the dyadic valuation of x, the highest power of 2 which divides x.
Thus

$$1 \prec 3 \prec 5 \prec \ldots 2 \prec 6 \prec 10 \prec \ldots 4 \prec 12 \prec 20 \prec \ldots$$

Exercise

Determine the order type of B.

Arithmetic operations are straightforward to define by induction, following exactly the Dedekind definitions for addition and multiplication on the natural numbers. For clarity, we write α' for the successor of α.

$$\alpha + 0 = \alpha$$
$$\alpha + \beta' = (\alpha + \beta)'$$
$$\alpha + \lambda = \sup\{\, \alpha + \beta \mid \beta < \lambda \,\}$$
$$\alpha \cdot 0 = 0$$
$$\alpha \cdot \beta' = \alpha \cdot \beta + \alpha$$
$$\alpha \cdot \lambda = \sup\{\, \alpha \cdot \beta \mid \beta < \lambda \,\}$$
$$\alpha^0 = 0'$$
$$\alpha^{\beta'} = \alpha^{\beta} \cdot \alpha$$
$$\alpha^{\lambda} = \sup\{\, \alpha^{\beta} \mid \beta < \lambda \,\}$$

One can show that addition and multiplication of ordinals are both associative but they fail to be commutative.

For example, letting $1 = 0'$, $2 = 1'$, we have

$$1 + \omega = \omega \neq \omega + 1$$

and

$$2 \cdot \omega = \omega \neq \omega \cdot 2 = \omega + \omega$$

Exercise

Show that addition and multiplication are associative.

Exercise

Show that multiplication is left-distributive but not right-distributive.

Exercise

Show that $\alpha^{\beta+\gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$.

The definitions of ordinal arithmetic above may seem obvious, but it is worth pointing out that they faithfully represent certain natural operations on well-orders.

Suppose A and B are well-orders of order type α and β, respectively.

Let

$$C = \{\,(0, a) \mid a \in A\,\} \cup \{\,(1, b) \mid b \in B\,\}$$

be the disjoint union of A and B. Order C by "first A, then B". Then C is a well-order of order type of C is $\alpha + \beta$.

Likewise, setting $C = A \times B$ and ordering this set lexicographically produces a well-order of order type $\alpha \cdot \beta$.

Fill in the details for these constructions.

Invent a similar justification for ordinal exponentiation in terms of constructing well-orders from given ones.

Ordinary induction on $\mathbb{N}$ uses a well-order of order type ω.

But the argument for the Ackermann function requires order type ω^2. We can still establish the well-ordering property of this well-order using nested ordinary induction. In particular, we could carry out the proof in Peano arithmetic.

We could also establish induction of order type ω^3 and so forth. In fact, we can get quite far within Peano arithmetic.

An ordinal α is an ε-number if $\alpha = \omega^\alpha$. Note that an ε-number is closed with respect to exponentiation.

One can show that there are lots of ε-numbers, in fact just as many as there ordinals. The least ε-number is usually called ε_0 (epsilon naught).

For ordinals $\alpha < \varepsilon_0$ Cantor has established the following normal form:

$$\alpha = \omega^{\alpha_1} + \omega^{\alpha_2} + \ldots + \omega^{\alpha_k}$$

where $\alpha > \alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_k$.

Given this constraint, the normal form is indeed unique.

We can exploit Cantor normal form to define, for each limit ordinal $\lambda < \varepsilon_0$, a "natural" increasing sequence $[\lambda_n]$ where $n < \omega$ such that $\lambda = \lim \lambda[n]$.

- For $\lambda = \omega^{\alpha_1} + \omega^{\alpha_2} + \ldots + \omega^{\alpha_k}$ we set
  $\alpha[n] = \omega^{\alpha_1}[n] + \omega^{\alpha_2}[n] + \ldots + \omega^{\alpha_k}[n]$.

- For $\lambda = \omega^{\alpha+1}$ we set $\lambda[n] = \omega^\alpha \cdot n$.

- For $\lambda = \omega^\alpha$ we set $\lambda[n] = \omega^{\alpha[n]}$.

We can now define functions $W_\alpha : \mathbb{N} \to \mathbb{N}$ for all $\alpha < \varepsilon_0$.

$$W_0(x) = x + 1$$
$$W_{\alpha+1}(x) = W_\alpha^x(x)$$
$$W_\lambda(x) = W_{\lambda[x]}(x)$$

The first ω levels are quite similar to the classical Ackermann function.

Note that one can define W_{ε_0} in a similar fashion, one just needs to fix a fundamental sequence for ε_0.

For $\alpha < \beta$, W_β dominates W_α: for all sufficiently large x we have $W_\beta(x) > W_\alpha(x)$. Much larger, indeed.

All the W_α are computable, and can be shown to be total in (PA).

But W_{ε_0} is also total, but this is no longer provable in (PA).

One can show that Peano arithmetic can handle inductions of length λ for any $\lambda < \varepsilon_0$ but not to ε_0 itself. In fact, induction of length ε_0 suffices to prove the consistency of Peano arithmetic. Hence, by Gödel's theorem, one cannot establish ε_0-induction in Peano arithmetic.

Let's return to the issue of measuring the sizes of sets. Any well-order of order type ω requires a countably infinite carrier set.

But countable sets suffice to build well-orders of higher order types such as $\omega + \omega$, $\omega \cdot \omega$, ω^ω. Even ε_0 can easily be squeezed into a countable carrier set.

This suggests the following definition.

Definition

An ordinal κ is a cardinal if the carrier set of any well-order of length κ is larger than the carrier set of any well-order of length $\alpha < \kappa$.

This comes down to insisting that there is no injection

$$\{\,\alpha \in On \mid \alpha < \kappa\,\} \to \{\,\alpha \in On \mid \alpha < \beta\,\}$$

for any $\beta < \kappa$.

Informally, cardinalities jump when the length of a well-order reaches κ.

What can we say about cardinals $Card \subseteq On$?

First off, there are the finite cardinals which consist of all ordinals less than ω – if you like, you can identify these with the natural numbers.

The first infinite cardinal is ω, though in its capacity as a cardinal rather than just plain ordinal it is often written

$$\aleph_0 \qquad \text{aleph naught}$$

This notation is, of course, due to Cantor.

But things do not end there. In fact, one can show that $Card$ is a well-ordered subclass of On, so we actually have a sequence

$$\aleph_0, \aleph_1, \ldots \aleph_\omega, \ldots \aleph_{\omega+\omega}, \ldots \aleph_{\omega^2}, \ldots \aleph_{\varepsilon_0}, \ldots, \aleph_{\aleph_1}, \ldots$$

If you find this vertigo-inducing you are quite right.

Note that for our examples, $\aleph_\alpha$ is always much, much larger than α.

Alas, one can prove in ordinary set theory that there is a cardinal κ such that

$$\alpha_\kappa = \kappa$$

To wit, κ can be chosen to be the least ordinal larger than $f(n)$ for all $n < \omega$ where $f(0) = 0$ and $f(n+1) = \aleph_{f(n)}$.

Take a moment to figure out what this means. This number is mind-numbingly large.

In set-theory κ would be considered fairly small.

One studies inaccessible cardinals $\alpha = \aleph_\alpha$:

- for all $\beta < \alpha$: $2^{\alpha_\beta} < \alpha$,
- α is regular: no sequence of length $\lambda < \alpha$ has limit α.

Note that our κ is the limit of a sequence of puny length ω.

One huge difference here is that ZFC cannot prove the existence of an inaccessible cardinal.

This never-ending stream of alephs is important in axiomatic set-theory, but for us only the first few items are relevant.

The natural numbers aka finite ordinals form the first number class. The countable ordinals form the second number class.

Thus $\aleph_1$ is the least uncountable ordinal, the least ordinal that does not belong to the second number class.

One can show that

$$\aleph_1 \leq |\mathbb{R}|$$

but equality, Cantor's famous Continuum Hypothesis, the other top entry on Hilbert's list, can not be settled in the framework of standard set theory. So it is safe to assume that $\aleph_1 = |\mathbb{R}|$ or that $\aleph_1 < |\mathbb{R}|$. Unlike with the Axiom of Choice, neither option seems to be particularly natural or consequential, so the Continuum Hypothesis has not been adopted as a standard axiom.

One should note the arithmetic of cardinals is different from the arithmetic of ordinals. We won't give a detailed definition of the arithmetic operations; they are supposed to represent the effect on cardinality of disjoint union, Cartesian product and function space formation. For example, $\aleph_0 + \aleph_0 = \aleph_0$: it is easy to construct a bijection between $\mathbb{N}$ and two disjoint copies of $\mathbb{N}$.

One can show that addition and multiplication of cardinals are associative, commutative operations. Moreover

Lemma

Let λ and κ be two cardinals, at least one of them infinite and neither 0. Then

$$\lambda + \kappa = \lambda \cdot \kappa = \max(\lambda, \kappa).$$

Note that exponentiation is not mentioned here; in fact $2^\kappa > \kappa$ for all cardinals κ as Cantor's diagonal argument shows.

One can also derive some basic properties of inequalities between cardinalities.

Lemma

Let $\lambda \leq \kappa$ and $\lambda' \leq \kappa'$. Then

$$\lambda + \lambda' \leq \kappa + \kappa' \text{ and } \lambda \cdot \lambda' \leq \kappa \cdot \kappa'$$

Unless $\lambda = \lambda' = \kappa = 0 < \kappa'$ we also have

$$\lambda^{\lambda'} \leq \kappa^{\kappa'}.$$

There are also infinitary version of the arithmetic operations. Here is one famous result.

Lemma (König)

Let $\lambda_i < \kappa_i$ for all $i \in I$. Then

$$\prod_i \lambda_i < \sum_i \kappa_i.$$

One interesting property of the second number class is that all its elements can be approximated by sequences of length ω.

Definition

Define the cofinality of a limit ordinal α to be the length of a shortest sequence that is cofinal in $\{\, \beta \in On \mid \beta < \alpha \,\}$. Ordinal α is regular if it has cofinality α.

In symbols: $\operatorname{cof}\alpha$.

Note that $\omega + \omega$, ω^2 and the like all have cofinality ω.

Lemma

All limit ordinal in the second number class have cofinality ω. But $\aleph_1$ is regular.

So far we have carefully avoided explaining how to represent ordinals and cardinals as sets and instead used concepts such as "stage of construction", "well-ordering" and so on. Here is one way to represent ordinals as ordinary pure sets due to von Neumann. All the assertions we have made above can then be proven in set-theory.

We want to define a set N_α for each ordinal α that represents α in some natural way.

First off, what is meant by natural here is that the structure

$$\langle N_\alpha, \in \rangle$$

ought to be a well-ordering of order type α.

So, for any well-ordering $\langle A, < \rangle$ there is an isomorphic order of the form $\langle N_\alpha, \in \rangle$, we don't need any order relation more complicated than $\in$.

If we use $\in$ as the underlying order we must have the following (order relations are transitive):

$$z \in y \in x \text{ implies } z \in x.$$

This property warrants a definition of its own.

Definition
A set x is transitive if $z \in y \in x$ implies $z \in x$.

Thus, x is transitive iff $\bigcup x \subseteq x$ iff $x \subseteq \mathfrak{P}(x)$.

Structures that can be represented by transitive sets together with $\in$ play an important role in set theory, but we won't pursue the issue here.

As an aside, we note that for any set x we can construct the least transitive superset y, by induction on $\in$.

Definition

The transitive closure of x is defined to be

$$\mathsf{TC}(x) = \bigcap \{\, y \supseteq x \mid y \text{ transitive} \,\}.$$

We can define the transitive closure operator in by recursion along $\in$:

$$\mathsf{TC}(\emptyset) = \emptyset$$
$$\mathsf{TC}(x) = x \cup \bigcup_{z \in x} \mathsf{TC}(z)$$

Exercise

Show that $y \subseteq x$ implies $\mathsf{TC}(y) \subseteq \mathsf{TC}(x)$.

Exercise

Show that the recursive definition works as advertised.

So, what should the von Neumann ordinals look like?

Needless to say, we start with $N_0 = \emptyset$.

The successor function on sets is defined by
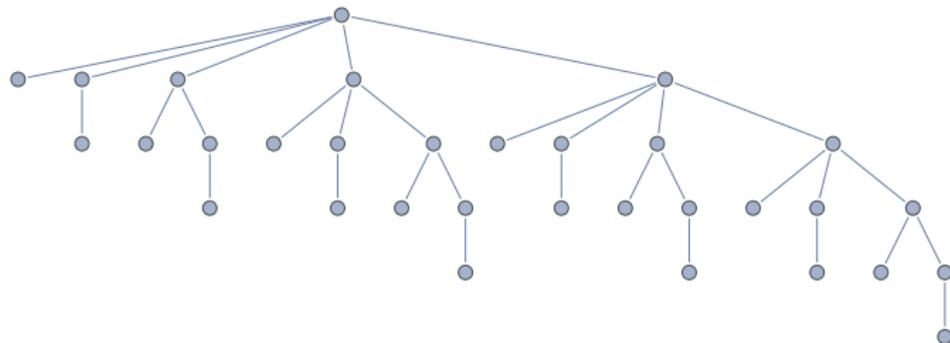
$$S(x) = x \cup \{x\}$$

and $S(N_\alpha)$ is the successor of N_α.

So the question is what to do with limit ordinals. The answer is fairly simple: take the union of all earlier von Neumann ordinals. So

$$N_\lambda = \bigcup_{\alpha < \lambda} N_\alpha$$

Exercise

Show that the von Neumann ordinals are in fact well-ordered by $\in$.

The leaves correspond to ∅, the edges indicate membership. This tree emphatically does not share common subexpressions.

Not every transitive set represents an ordinal, but there is a nice way to characterize these sets.

Lemma

The von Neumann ordinals are precisely the transitive sets that are well-ordered by the element relationship $\in$.

Proof.

An easy induction shows that all von Neumann ordinals are well-ordered by $\in$.

For the opposite direction use induction on α to show that the element in $\langle A, \in \rangle$ of rank α must be N_α (transitivity is crucial).

$\square$

Exercise

Show that every element of a von Neumann ordinal is a von Neumann ordinal using as definition "transitive and $\in$-well-ordered".

The last lemma is rather neat; to represent well-orders in set theory we can dispense with specific order relations and just use ε. The only thing that changes is the carrier set, which has rather nice properties itself.

We note that some authors define ordinals in terms of their set-theoretic implementation. While formally correct, this approach is rather dubious since it obscures the intended properties of ordinals – they all have to be tediously discovered after the fact. Some would also gripe that this method over-emphasizes set theory.

At any rate, the crucial idea is to generalize inductive proofs and/or definitions to well-orderings other than just the natural numbers. Ordinals represent the stages in these arguments and constructions.

- Ordinals capture the notion of stages in an inductive process, including the transfinite case.

- Alternatively, we can think of them as the order types of all well-orderings.

- Ordinals can be implemented in set theory as transitive sets that are well-ordered by ε.

- Using transitive induction, one can define ordinal arithmetic which corresponds naturally to operations on the well-orderings.

- Cardinals are special types of ordinals, and carry their own arithmetic.