Arithmetic of order types and ordinals

Franklin

August 4, 2022

1 Conceptual background

A **total order** or **linear order**, sometimes just called an **order**, is defined formally as a binary relation $\leq$ on a set A satisfying the following three axioms:

1. **Trichotomy.** For all $x, y \in A$, either $x \leq y$ or $y \leq x$ (or perhaps both).
2. **Antisymmetry.** For all $x, y \in A$, if $x \leq y$ and $y \leq x$, then $x = y$.
3. **Transitivity.** If $x \leq y$ and $y \leq z$, then $x \leq z$.

Intuitively, these three axioms are meant to encapsulate the essential nature of what it means to *compare* two things. The first axiom states that any two elements of a linear order can be compared; the second axiom is equivalent to stating that no element can be both less than and greater than any other element; and the third axiom states that if an element is at least as great as a second element, and that second element is at least as great as a third element, then the first element is also at least as great as that third element.

Much like set theory, the theory of abstract orderings often does not receive much attention on its own. Most often, we are concerned with algebraic structures that possess an ordering in addition to their other operations, such as $\mathbb{Z}$ (an ordered ring) or $\mathbb{R}$ (an ordered field). There are, however, plenty of tricky problems to be discovered just by focusing on the ordering of these structures (and others).

2 Order-isomorphism and order types

When defining cardinal numbers, the starting point is to define what it means for two sets to have "the same number of elements" or "the same size". Two sets A, B are said to have the same cardinality if there exists a **bijection** between them, i.e. a function $f : A \to B$ that is both an injection and a surjection, or a function that has an inverse. Intuitively, a bijection can be thought of as a "relabelling" of the elements of a set, and a cardinality can in some sense be thought of as a vague set-like object which is "left unlabelled". A bijection might also be referred to as an **isomorphism of sets**, expressing that two sets have "the same structure".

If we want to similarly characterize orderings, we need to define what it means for two orderings to have "the same order structure". We will similarly use a special kind of mapping $f : A \to B$ between two orderings $(A, \leq), (B, \leq)$ to establish that the have the same structure. Of course, if two orderings are to have the same structure, their underlying sets must also have the same structure, so f ought to be a bijection, so that it forms a correspondence between elements of A and elements of B. However, in order for f to constitute an **order isomorphism**, we will also require it to *preserve ordering*, so that

$$a \leq b \implies f(a) \leq f(b)$$

That is, we are forming a correspondence between the elements of A and the elements of B in such a way that elements of A and their corresponding elements of B *appear in the same order*. For example, if we let $A = \mathbb{N}$ with the usual ordering:

$$1 < 2 < 3 < 4 < \cdots$$

and if we let B be the set of powers of two:

$$2 \ < \ 4 \ < \ 8 \ < \ 16 \ < \ \cdots$$

Notice that these two orders have "the same structure" at a glance, even if their elements have "different names". In particular, $1 \in A$ and $2 \in B$ play the same role of being the smallest elements, and $2 \in A$ and $4 \in B$ are the second-smallest elements, and $3 \in A$ and $8 \in B$ are the third-smallest, and so on. In general, it seems like the element $n \in A$ would correspond to the element $2^n \in B$. This means that the order isomorphism we desire is the function $f(x) = 2^x$. Sure enough, this function is increasing (i.e. order-preserving) and comprises a bijection between the sets A and B, so we say that $(A, \leq)$ and $(B, \leq)$ are **order isomorphic** and write $(A, \leq) \cong (B, \leq)$, or sometimes just $A \cong B$ (since the specific ordering is clear from context).

Now let's think about a different pair of orderings $(A, \leq)$ and $(B, \leq)$. Again, let's take $A = \mathbb{N}$ with the usual ordering on the natural numbers:

$$1 \ < \ 2 \ < \ 3 \ < \ 4 \ < \ \cdots$$

but this time let's set $B = \mathbb{Z}$ with the usual ordering on the integers:

$$\cdots \ < \ -2 \ < \ -1 \ < \ 0 \ < \ 1 \ < \ 2 \ < \ \cdots$$

These two orderings certainly don't "look the same". They have several structural differences, such as the fact that A has a smallest element whereas for every element of B there is some smaller element. Can we make this intuition precise to prove that there cannot exist an order-isomorphism $f : A \to B$?

Well, if we suppose that there existed an order preserving bijection $f : A \to B$, we can show that $f(1)$ would have to be a smallest element of B. Any element $b \in B$ must equal $f(a)$ for some $a \in A$ because f is surjective, and we must have $1 \leq a$ because 1 is the least element of A, which would imply $f(1) \leq f(a) = b$ by the order preserving nature of f. Since b was arbitrary, we would have $f(1) \leq b$ for all $b \in B$, which is impossible since B has no least element! Hence, we may conclude that $(A, \leq)$ and $(B, \leq)$ are not isomorphic.

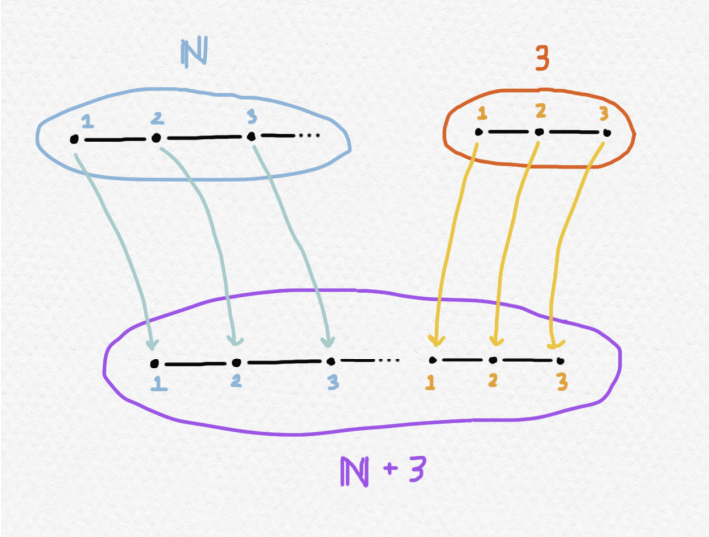
We might want to be able to refer to *only the structure* of an ordering, without ever referring to a specific instance of it, or ever having to "give names" to its elements. This can be accomplished by the notion of an **order type**. The relation $\cong$ of order isomorphism between ordered sets is an *equivalence relation*, and an order type is defined as an *equivalence class* of this equivalence relation, or a collection of orderings such that any two of them are order isomorphic. Here are the notations used for a couple of commonly-occurring order types:

- **0** is the order type of the empty ordering
- **1** is the order type of the singleton ordering, **2** is the order type of the ordering with 2 elements, and so on
- ω is the order type of $(\mathbb{N}, \leq)$
- η is the order type of $(\mathbb{Q}, \leq)$
- λ is the order type of $(\mathbb{R}, \leq)$
- θ is the order type of the real irrationals $(\mathbb{R} \backslash \mathbb{Q}, \leq)$

If ξ is an order type and an ordering $(A, \leq)$ is in the equivalence class ξ, so that it is isomorphic to every ordering in ξ (or equivalently isomorphic to *some* ordering in ξ), then we say that $(A, \leq)$ **has order type** ξ. In the next section, we'll see how to combine some of these simpler order types to build up more complex and interesting ones.

3 Arithmetic of order types

We are now prepared to introduce a few operations on orderings and order types that are loosely analogous to arithmetical operations on numbers. For instance, if we intuitively think of addition as a way of "combining" two quantities, perhaps the most natural way of "combining" two ordered arrangements of points would be to *concatenate* them. For instance, if $(\mathbb{N}, \leq)$ is an ordering consisting of an infinite increasing sequence of points, and $([3], \leq)$ is an ordering consisting of three points in a sequence, then we might define $(\mathbb{N}, \leq) + ([3], \leq)$ to be an ordering consisting of an infinite increasing sequence of points *followed by* three points in a sequence, like this:



A more formal definition is as follows. Given two ordered sets A, B, we can define their **sum**, denoted $A + B$, to be the set of ordered pairs

$$\{(a, 0) : a \in A\} \cup \{(b, 1) : b \in B\}$$

endowed with an ordering defined by letting $(a_1, A) < (a_2, A)$ iff $a_1 < a_2$, and $(b_1, B) < (b_2, B)$ iff $b_1 < b_2$, and $(a, A) < (b, B)$ for all $a \in A$ and $b \in B$. We can then extend this definition to define the sum of two *order types*. If α is the order type of $(A, \leq)$ and β is the order type of $(B, \leq)$, then we may define $\alpha + \beta$ to be the order type of the ordering $(A, \leq) + (B, \leq)$. Notice that this is well-defined because the order type of $(A, \leq) + (B, \leq)$ depends only on the order types of $(A, \leq)$ and $(B, \leq)$. That is, if A, A', B, B' are ordered sets such that $(A, \leq) \cong (A', \leq)$ with isomorphism $f : A \to A'$, and $(B, \leq) \cong (B', \leq)$ with isomorphism $g : B \to B'$, then

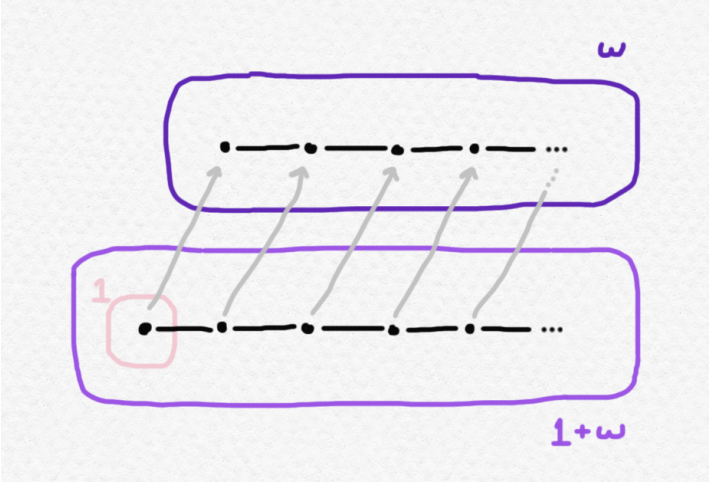
$$(A, \leq) + (B, \leq) \cong (A', \leq) + (B', \leq)$$

with this isomorphism being established by an order isomorphism h sending $(a, 0) \mapsto (f(a), 0)$ and $(b, 1) \mapsto (g(b), 1)$ for each $a \in A$ and $b \in B$.

If we start out by considering only sums of finite orderings, it may seem like addition of order types behaves much like addition of integers. Addition of finite order types behaves the same way as addition of the corresponding natural numbers, for instance, $\mathbf{3} + \mathbf{4} = \mathbf{7}$ (a sequence of 3 elements followed by a sequence of 4 elements is a sequence of 7 elements). However, when we begin to compute some sums involving infinite order types, it becomes clear that this "addition" is very different from integer addition. Consider, for instance, the identity

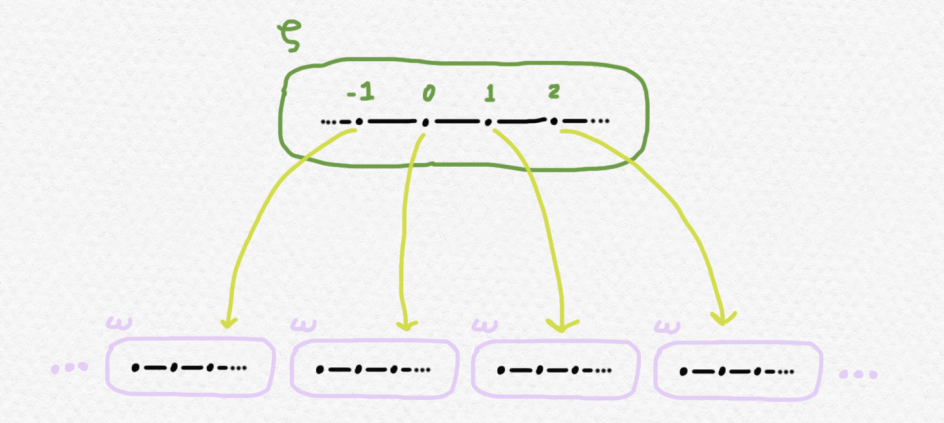
$$\mathbf{1} + \omega = \omega$$

which states "a single point followed by an increasing infinite sequence of points is just an increasing infinite sequence of points". This equality can be demonstrated by establishing an isomorphism between $(\mathbb{N}, \leq)$ and $([1], \leq) + (\mathbb{N}, \leq)$, namely the function that sends $1 \mapsto (1, 0)$ and $n \mapsto (n-1, 1)$ for all $n > 1$. We can visualize this phenomenon as follows:



The simple equality $\mathbf{1} + \omega = \omega$ in itself illustrates several differences between aritmetic in, say, a ring, and arithmetic with order types. For one, we have that $\omega + \mathbf{1} \neq \omega$, for an ordering of type $\omega + \mathbf{1}$ has a largest element, but an ordering of type ω does not. This means that $\omega + \mathbf{1} \neq \mathbf{1} + \omega$, and so *addition fails to be commutative*. We also have that $\omega = \mathbf{0} + \omega$, and so $\mathbf{1} + \omega = \mathbf{0} + \omega$, but clearly $\mathbf{1} \neq \mathbf{0}$, and thus addition *fails to be cancellable*. That is, if we have order types α, β, γ such that $\alpha + \gamma = \beta + \gamma$, we cannot necessarily conclude that $\alpha = \beta$! See the end of this section for some exercises that will help you explore how addition acts on some common order types.

We can also extend the operation of multiplication to order types. With natural numbers, we may interpret of $a \cdot b$ as "a added to itself b many times", or "b many copies of a". This interpretation extends well to infinite order types as well. We will define a product of orderings in such a way that $(A, \leq) \cdot (B, \leq)$ consists of "one copy of A" for each element of B, such that the ordering looks like the result of replacing each element of B with a miniature copy of A. Again, for finite order types, this agrees with multiplication of natural numbers. For products of infinite order types, such as $\omega \times \zeta$, we might visualize this operation as follows:



Given two ordered sets A, B, we define their **lexicographic product**, denoted $A \cdot B$, as the Cartesian Product $A \times B$ of ordered pairs (a, b) with $a \in A$ and $b \in B$ which are ordered according to the following rule. Given (a_1, b_1) and (a_2, b_2) in $A \times B$, we say that $(a_1, b_1) < (a_2, b_2)$ if $b_1 < b_2$, *or* if $b_1 = b_2$ and $a_1 < a_2$. That is, two pairs are compared first on the basis of their second elements, and if they have the same second element, the first element is used as a "tie breaker". We can show that if two pairs of ordered sets A, B and A', B' satisfy $A \cong A'$ and $B \cong B'$, then $A \times B \cong A' \times B'$. For if $f : A \to A'$ is an order isomorphism and $g : B \to B'$ is also an order isomorphism, then the mapping $h : A \times B \to A' \times B'$ defined by

$$h((a, b)) = (f(a), g(b))$$

is also an order isomorphism. Therefore, we can extend the lexicographic product to an operation on order types: if α is the order type of A and β is the order type of B, then we define the **product** $\alpha \cdot \beta$

to be the order type of $A \times B$. (Because the order type of $A \times B$ depends only on the order types of A and B, as shown above, this is not ill-defined.) If we just picture α and β as "abstract orderings" with unlabelled points, we can think of $\alpha \cdot \beta$ as consisting of "β many copies of α".

Similarly to the situation with addition, multiplication of order types does not enjoy the same agreeable properties of natural number multiplication. For instance, you may verify as an exercise that $\omega \cdot \mathbf{2} \neq \omega$, whereas $\mathbf{2} \cdot \omega = \omega$, meaning that *multiplication is not commutative*. We can prove that for any order types α, β, γ, we have that

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$

Proving this would also make a good exercise in the technical definitions of addition and multiplication of order types. Seeing this identity, we might rush into saying that multiplication distributes over addition. However, the above only tells us that multiplication is *left-distributive* over addition, and in the absence of commutativity, this is not necessarily the same as right-distributivity. Indeed, it is *not true in general* that $(\beta + \gamma) \cdot \alpha = (\beta \cdot \alpha) + (\gamma \cdot \alpha)$. Consider, for instance, the example of $\alpha = \omega$ and $\beta = \gamma = \mathbf{1}$. If you want, you can further explore the properties of order type multiplication by using the coming exercises to build intuition.

There is one more strange operation on order types that has no obvious analogues in ordinary arithmetic. Given an ordering $(A, \leq)$, the **dual ordering** is defined as the ordering $(A, \leq')$ with the same underlying set but a different ordering, such that $a_1 \leq' a_2$ iff $a_2 \leq a_1$. That is, the dual of $(A, \leq)$ "reverses the order" of each pair of elements, essentially "reflecting" the entire ordering. Given an ordering $(A, \leq)$, its dual is sometimes denoted $(A, \leq)^d$ or $(A, \leq)^*$. Similarly to the previous examples, we may extend this operation to order types, letting α^* be the order type of the dual of any ordering with type α.

Here are some exercises regarding the arithmetic of order types. Some of them are tricky!

1. Can you show that $\omega + \omega \neq \omega$, but $\eta + \eta = \eta$? Can you prove that $\eta + \mathbf{1} + \eta = \eta$ and $\lambda + \mathbf{1} + \lambda = \lambda$?
2. Can you show that $\theta + \theta = \theta$, and that $\theta + \mathbf{1} + \theta = \theta$?
3. Prove that $(\alpha + \beta)^* = \beta^* + \alpha^*$ and $(\alpha \cdot \beta)^* = \alpha^* \cdot \beta^*$ for all order types α, β. Prove that if α is an arbitrary order type, then $\alpha^* = \alpha$ iff there exists an order type β such that $\alpha = \beta + \beta^*$ or $\alpha = \beta + \mathbf{1} + \beta^*$. Is it ever the case that $\alpha = \beta + \beta^* = \beta + \mathbf{1} + \beta^*$?
4. Can you prove that $\omega + \omega^2 = \omega^2$? Is $\omega^2 + \omega = \omega$? Can you show that $(\omega^3 + \omega)^5 = (\omega^5 + \omega^3)^3$?
5. Show that $(\omega + \mathbf{1})^2 = \omega^2 + \omega + \mathbf{1}$, and that $(\omega + \mathbf{1})^3 = \omega^3 + \omega^2 + \omega + \mathbf{1}$. Any conjectures?
6. Consider the following table of 25 order types:

$$\begin{array}{lllll} \omega \cdot \omega & \omega \cdot \zeta & \omega \cdot \eta & \omega \cdot \theta & \omega \cdot \lambda \\ \zeta \cdot \omega & \zeta \cdot \zeta & \zeta \cdot \eta & \zeta \cdot \theta & \zeta \cdot \lambda \\ \eta \cdot \omega & \eta \cdot \zeta & \eta \cdot \eta & \eta \cdot \theta & \eta \cdot \lambda \\ \theta \cdot \omega & \theta \cdot \zeta & \theta \cdot \eta & \theta \cdot \theta & \theta \cdot \lambda \\ \lambda \cdot \omega & \lambda \cdot \zeta & \lambda \cdot \eta & \lambda \cdot \theta & \lambda \cdot \lambda \end{array}$$

   Are any of these order types equal to each other? How many distinct order types appear in this table? Are any of them equal to $\omega, \zeta, \eta, \theta$ or λ?
7. We have seen that $\alpha + \gamma = \beta + \gamma$ does not necessarily imply that $\alpha = \beta$. Show, however, that $\alpha + \mathbf{1} = \beta + \mathbf{1}$ implies $\alpha = \beta$. Hence, there are *some order types* for which $\alpha + \gamma = \beta + \gamma$ implies $\alpha = \beta$. Can you find some other values of γ with this "cancellation property"? Can you find a necessary and sufficient condition characterizing *all* such order types γ?
8. We can naturally define the exponentiation of order types α^β when β is finite, i.e. $\beta = \mathbf{0}, \mathbf{1}, \mathbf{2}, \cdots$, using the "exponentiation as repeated multiplication" interpretation. Is there a "nice" way of defining exponentiation of order types α^β for some infinite order types β, such as $\beta = \omega$? Does your definition work for *arbitrary* order types α, or only under certain conditions? Why or why not?

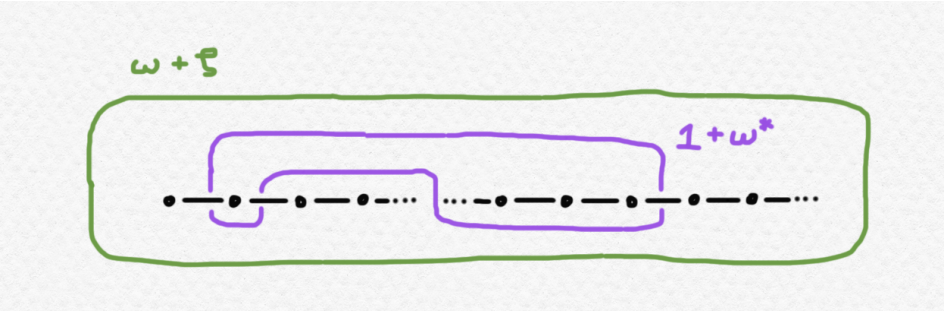
9. Can you prove that addition and multiplication are associative operations on order types? (You may have been assuming this fact on the previous exercises!)

4 Food for thought

In addition to the arithmetic operations introduced above, there are several other ways of studying order types and their relationships with each other. Simple operations or relationships involving order types such as the following can sometimes lead to unexpectedly deep or difficult questions. Below is a brief treatment of several different angles from which to study order types, each of which gives rise to interesting new puzzles.

4.1 Order embedding

We have defined an *order isomorphism* to be a bijective order-preserving function between two ordered sets. Similarly, we define an **order embedding** to be an *injective* order-preserving function between two ordered sets, and we say that the former ordering can be **embedded** in the latter. We use the same vocabulary to refer to their order types, saying that α can be embedded in β if any ordering of type α can be embedded in any ordering of type β, and denote this by writing $\alpha \hookrightarrow \beta$ or $\alpha \preceq \beta$. If one ordering can be embedded in another, then the latter "contains a copy" of the former, or contains some suborder which is isomorphic to the given order. For instance, $\omega \hookrightarrow \zeta$ because the integers have order type ζ and the natural numbers $\mathbb{N} \subset \mathbb{Z}$ comprise a subordering of type ω. Less trivially, $\mathbf{1} + \omega^* \hookrightarrow \omega + \zeta$, and the following picture shows how we can find "a copy of $\mathbf{1} + \omega^*$ inside of $\omega + \zeta$":

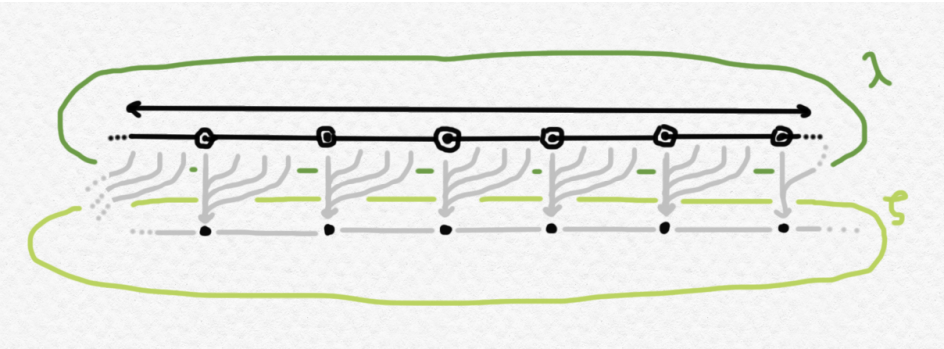


In general, determining whether $\alpha \hookrightarrow \beta$ for two given order types α, β comes down to "finding a copy of α inside β".

1. Prove that $\alpha \hookrightarrow \alpha'$ and $\beta \hookrightarrow \beta'$ implies $\alpha + \beta \hookrightarrow \alpha' + \beta'$ and $\alpha \cdot \beta \hookrightarrow \alpha' \cdot \beta'$.
2. Does $\lambda \cdot \lambda \hookrightarrow \lambda$? Does $\theta \cdot \theta \hookrightarrow \theta$? Does $\lambda \cdot \theta \hookrightarrow \lambda$?
3. Prove or disprove that if $\alpha \preceq \beta$ and $\beta \preceq \alpha$, then $\alpha = \beta$.
4. Prove that if $\alpha + \mathbf{1} \hookrightarrow \omega \cdot \beta$ then $\alpha + \omega \hookrightarrow \omega \cdot \beta$, for arbitrary order types α, β.

4.2 Homomorphic images

There is another class of functions between ordered sets which are required to preserve order *non-strictly*. A function f between ordered sets is called an **order homomorphism** if $x \leq y$ implies $f(x) \leq f(y)$. Hence, if $x < y$, f might map x and y to two distinct points appearing in the same order, *or* to the same point so that $f(x) = f(y)$. We can think of non-injective order homomorphisms as "collapsing" some different intervals of a ordering into single points. If there exists a surjective order homomorphism from any ordering of type α onto any ordering of type β, then we say that β is a **homomorphic image** of α and denote this by writing $\beta \precsim \alpha$. For instance, any nonempty order type α satisfies $\mathbf{1} \precsim \alpha$, since the constant function from any ordering of type α onto $([1], \leq)$ is a surjective homomorphism. For a more complex example, we also have that $\zeta \preceq \lambda$ because the floor function $x \mapsto \lfloor x \rfloor$ is a surjective homomorphism from $\mathbb{R}$ onto $\mathbb{Z}$, collapsing each interval $[n, n+1)$ to the point n like this:



If $\alpha \precsim \beta$, we can think of β as being "capable of covering α". Here are some questions to ponder concerning homomorphic images:

1. Given an ordering of type **6** and another ordering of type **3**, how many distinct order homomorphisms are there from the former to the latter? What about *surjective* order homomorphisms?
2. Is $\eta \precsim \lambda$? Is $\theta \precsim \lambda$? Is $\eta \precsim \theta$?
3. Does $\alpha \preceq \beta$ imply $\alpha \precsim \beta$? Does $\alpha \precsim \beta$ imply $\alpha \preceq \beta$?
4. Find an order type α such that for every *proper* homomorphic image $\alpha' \precsim \alpha$ with $\alpha' \neq \alpha$, there exists β such that $\alpha' \precsim \beta \precsim \alpha$ and $\beta \neq \alpha, \alpha'$.

4.3 Automorphism groups

Given an ordering of type α, an order isomorphism from that ordering to itself is called an **order automorphism**. If $f, g : A \to A$ are two automorphisms of the ordered set $(A, \leq)$, then we may compose them to form a second automorphism $f \circ g$. Additionally, given an automorphism $f : A \to A$, we may consider its inverse $f^{-1} : A \to A$ since it is a bijection, and this function will also be an automorphism. This means that the set of automorphisms of $(A, \leq)$ constitutes a *group* under the operation of function composition, since this operation satisfies the group laws of being associative (function composition is associative), having an identity element (the identity function $A \to A$), and having an inverse for each element. Since the structure of this group depends only on the order type of $(A, \leq)$, we may use $\mathrm{Aut}(\alpha)$ to denote the **automorphism group** of an ordering of type α. For instance, we have that $\mathrm{Aut}(\zeta) \cong (\mathbb{Z}, +)$, the additive group of integers, because the order automorphisms of the ordering $(\mathbb{Z}, \leq)$ are the translation maps $x \mapsto x + n$ for fixed n.

1. What is $\mathrm{Aut}(\zeta)$? What is $\mathrm{Aut}(\zeta \cdot \mathbf{2})$? What is $\mathrm{Aut}(\eta)$?
2. Prove or disprove that $\mathrm{Aut}(\eta) \cong \mathrm{Aut}(\theta)$.
3. Prove or disprove that the automorphism group of an ordering is always Abelian.
4. Prove or disprove that the automorphism group of an ordering is always torsion-free. Given a (torsion-free) group, can you always come up with an ordering whose automorphism group is isomorphic to that group?

4.4 Elementary equivalence

If you came to my talk on *model theory* or saw the minicourse notes, you might have considered the problem of distinguishing between orderings using sentences of first-order logic with the language $\mathcal{L} = \{\leq\}$. For instance, we can discriminate between the orderings $(\mathbb{N}, \leq)$ and $(\mathbb{Z}, \leq)$ using the first-order sentence

$$\varphi \;=\; \big(\exists x\ \forall y\ x \leq y\big)$$

which says, in plain English, that there exists an element which is less than or equal to all other elements, so that φ is true in $(\mathbb{N}, \leq)$ but not in $(\mathbb{Z}, \leq)$. If it is possible to write down a first-order sentence in the language $\mathcal{L} = \{\leq\}$ that discriminates between a model consisting of an ordering of

type α and one of type β, then we write $\alpha \not\equiv \beta$ (so, based on the above sentence φ, we may conclude that $\omega \not\equiv \zeta$). Otherwise, we may say that α and β are **elementarily equivalent**. The problem of determining whether two orderings are elementarily equivalent can be very difficult. Two isomorphic orderings are guaranteed to be elementarily equivalent, but not the other way around! (Proving two orderings to be elementarily equivalent is difficult, but one tool to approach this problem is something called an **Ehrenfeucht-Fraisse game**, which you can look up if you're interested.)

1. Can you come up with a first-order sentence that is true of any ordering of type ζ, but not of any ordering of type η? What about η versus λ?

2. Can you think of a first-order sentence distinguishing between orderings of type ω^3 and ω^4, showing that $\omega^3 \not\equiv \omega^4$? In general, can you come up with a way of discriminating between ω^m and ω^n when $m \neq n$?

3. Prove that there exists an order type α of a countably infinite ordering such that $\alpha \equiv \lambda$.

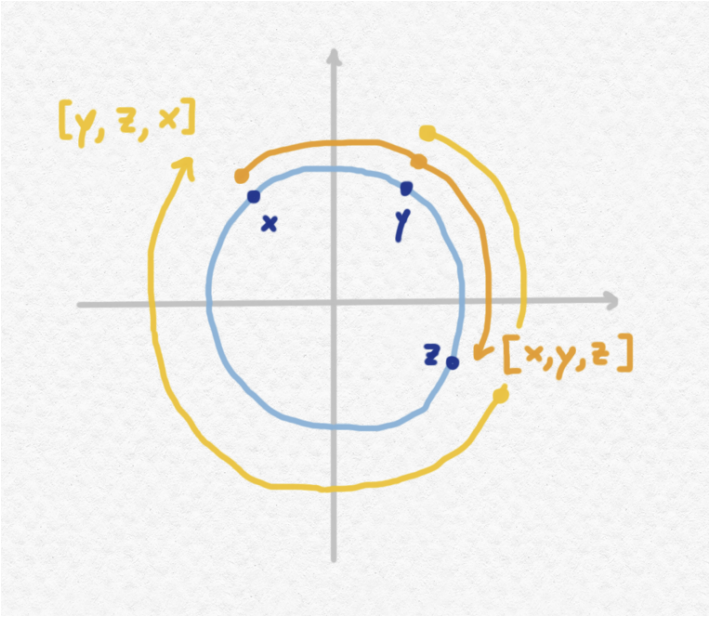
4. Is $\omega \equiv \omega + \zeta$? Is $\zeta \equiv \zeta + \zeta$? Is $\zeta \equiv \zeta \cdot \zeta$? Is $\zeta \equiv \zeta \cdot \lambda$? Any conjectures?

4.5 Cyclic orders

A **cyclic order** is a modification of the concept of a linear ordering in which two elements cannot be compared in an absolute way, but they can be compared *relative* to some other element, as a way of formalizing "circular" structures that linear orders cannot capture. For instance, if we wanted to order the points on the unit circle, we might want to say something like "let $x \leq y$ if y is clockwise from x". But any two points on the circle can be mapped onto each other by either a clockwise *or* a counterclockwise rotation, so this would not define an ordering at all - $\leq$ would just be a trivial relation which relates any pair of points on the unit circle. However, if we *first fix a point* on the unit circle, we can then compare two points based on which is "more clockwise" from that basepoint. Thus, cyclic orderings are formalized using a *ternary relation* in place of the usual binary relation $\leq$. In particular, we write

$$[x, y, z]$$

to assert that "starting from x, z is at least as far clockwise as y".



In place of the usual axioms for the binary relation $\leq$, we have three axioms for the ternary relation $[-,-,-]$. Firstly, for all x, y, z in the cyclic ordering, we require that either $[x, y, z]$ or $[x, z, y]$ be true. (This is analogous to requiring that either $y \leq z$ or $z \leq y$.) Secondly, we require that for all

w, x, y, z in the cyclic ordering, $[w, x, y]$ and $[w, y, z]$ together imply that $[w, x, z]$ holds. (This is analogous to transitivity.) Finally, we require that for all x, y, z in the cyclic ordering, $[x, y, z]$ implies $[y, z, x]$.

Similarly to how we defined isomorphisms of linear orderings, we can define isomorphisms of cyclic orderings, and analogously define *cyclic order types*. Additionally, from any ordinary linear ordering $(A, \leq)$, we can define a cyclic linear ordering by "wrapping A around into a circle". That is, for any $x, y, z \in A$, we may define $[x, y, z]$ to be true iff either $x \leq y \leq z$, or $y \leq z \leq x$, or $z \leq x \leq y$. If α is an order type, we may denote by $\text{cyc}(\alpha)$ the cyclic order type of the cyclic order defined in this way from any linear ordering of type α. For instance, the structure of the unit circle can be expressed as $\text{cyc}(\mathbf{1}+\lambda)$, since $\mathbf{1}+\lambda$ is the order type of the half-open interval $[0, 1)$, which can be "wrapped around" to form the unit circle.

1. Prove that $\text{cyc}(\eta) = \text{cyc}(\eta + \mathbf{1})$. Are there any more order types α such that $\text{cyc}(\alpha) = \text{cyc}(\eta)$? How many order types α are there such that $\text{cyc}(\alpha) = \text{cyc}(\mathbf{1} + \lambda)$?

2. Show that $\text{cyc}(\alpha + \beta) = \text{cyc}(\beta + \alpha)$ for all order types $\alpha + \beta$. Show further that if f is a function defined on order types such that $f(\alpha + \beta) = f(\beta + \alpha)$ for all order types α, β, then there exists a function g defined on cyclic order types such that $f(\gamma) = g(\text{cyc}(\gamma))$ for all order types γ.

3. Does $\text{cyc}(\alpha) = \text{cyc}(\beta)$ imply that $\alpha \cdot \zeta = \beta \cdot \zeta$? Does $\alpha \cdot \zeta = \beta \cdot \zeta$ imply that $\text{cyc}(\alpha) = \text{cyc}(\beta)$?

4. Can you think of a way of defining the "sum" of two cyclic order types? How about a "product"? How about a "dual"?

5 Intro to well-ordering and ordinals

In our attempts to axiomatize the arithmetic of the integers, we've noticed that they contain a special subset $\mathbb{N} \subset \mathbb{Z}$ which has a very powerful property. Namely, $\mathbb{N}$ is **well-ordered**, meaning that *each of its nonempty subsets has a least element*. Not all orderings have this property. For instance, $\mathbb{Z}$ fails to be well-ordered because the subset consisting of all negative integers has no least element. The orderings of $\mathbb{Q}$ and $\mathbb{R}$, and even $\mathbb{Q}^+$ and $\mathbb{R}^+$, also fail to have this property. Among orderings, we certainly cannot take the well-ordering property for granted!

However, $\mathbb{N}$ is evidently not the only ordered set which is well-ordered. Of course, each of the finite orderings $([n], \leq)$ are also well-ordered, because any finite set of elements of an ordered set must have a least element, and every subset of a finite ordering is finite! A little bit of investigation will, however, reveal that there are also other *infinite orderings*, not isomorphic to $(\mathbb{N}, \leq)$, which are also well-ordered. A simple example is $(\mathbb{N}, \leq) + ([1], \leq)$, an ordering which consists of a copy of the natural numbers followed by a single additional element greater than each natural number. To see why this is well-ordered, consider an arbitrary nonempty subset S of this ordering. Either it consists of only the largest element, in which case the least element of S is that element, or S contains some of the natural numbers as well, in which case the least element of S is the least natural number in S.

As a matter of fact, although many of the orderings we have thus far considered were not well-ordered, there are quite a few different (non-isomorphic) well-orderings. At this point, it will be beneficial for us to refer once more to classes of isomorphic orderings, rather than particular orderings on sets, so we will use the word **ordinal** to refer to an order type of a well-ordered set. (Can you prove that if two orderings are isomorphic, then one is well-ordered iff the other is well-ordered?) The ordinals currently among our repertoire are ω, the finite orderings $\mathbf{n}$, and $\omega + \mathbf{1}$. The following properties allow us to construct a great many more ordinals to play with:

1. If α and β are ordinals, then $\alpha + \beta$ is an ordinal.

2. If α and β are ordinals, then $\alpha \cdot \beta$ is an ordinal.

3. If α is an ordinal and $\beta \hookrightarrow \alpha$, then β is an ordinal.

If you can prove these facts, then you will suddenly have access to a great many more ordinals, such as $\omega \cdot \mathbf{2}$ and ω^2 and $\omega^3 + \omega^2 \cdot \mathbf{5} + \mathbf{4}$. We know that well-ordering was useful when it came to proving

number-theoretic facts about the integers - can it be used to prove any new properties about the arithmetic of ordinals? How does the arithmetic of ordinals compare to the arithmetic of order types in general?

In fact, the ordinals satisfy many useful properties, including but not limited to the following:

1. **Trichotomy.** For any two ordinals σ, τ, either $\sigma < \tau$ or $\tau < \sigma$ or $\sigma = \tau$. (This is not true for general orderings: consider, for instance, ω and ω^*.)
2. **Left-cancellable addition.** Ordinal addition satisfies a left-cancellation law. That is, if $\rho + \sigma = \rho + \tau$ for three ordinals ρ, σ, τ, then $\sigma = \tau$ necessarily. (We have seen that this is not true of general order types.)
3. **Left-cancellable multiplication.** Ordinal multiplication also satisfies left-cancellability. That is, if $\rho \cdot \sigma = \rho \cdot \tau$ and $\rho \neq \mathbf{0}$, then $\sigma = \tau$, for any ordinals ρ, σ, τ. (Not true for general order types, for instance $\eta \cdot \mathbf{2} = \eta \cdot \eta$ but $\mathbf{2} \neq \eta$.)
4. **Finite number of right-hand divisors.** We say that ρ is a **right-hand divisor** of σ if there exists τ such that $\sigma = \tau \cdot \rho$. It is an amazing fact that every ordinal has at most finitely many distinct many right-hand divisors.
5. **Well-ordering.** Every set of ordinal numbers is well-ordered.

We will come nowhere near close to proving all of these pleasant properties of ordinal arithmetic, but we will sketch the proofs of a few propositions leading up to the proof of the left-cancellability of addition. If you'd like to see a more rigorous treatment that also covers more of the properties of ordinal arithmetic, see W. Sierpinski's fantastic (but rather old) book *Cardinal and Ordinal Arithmetic*, or J. G. Rosenstein's book *Linear Orderings*.

Proposition 1. *An ordering $(A, \leq)$ is a well-ordering iff $(\mathbb{N}, \leq)^*$, the dual of the usual ordering of the natural numbers, cannot be embedded in $(A, \leq)$.*

Proof. Suppose that $f : \mathbb{N} \to A$ is an order embedding of $(\mathbb{N}, \leq)^*$ into $(A, \leq)$, so that it is injective and order-preserving. If we let $S \subset A$ be the image of f, i.e. the set

$$S = \{f(n) \ : \ n \in \mathbb{N}\}$$

then we have that S has no smallest element, for if $f(k)$ is some arbitrary element, then $f(k+1)$ is even smaller. Hence $(A, \leq)$ is not well-ordered.

Conversely, suppose that $(A, \leq)$ is not well-ordered, so that there exists a nonempty subset $S \subset A$ with no smallest element. Therefore, we may define a function $g : S \to S$ which assigns to each element $x \in S$ some element $y \in S$ that is *smaller* than x, or $y < x$. (Caution! This step implicitly makes use of something called the *Axiom of Choice*, which not all set theorists are comfortable taking for granted.) Then, given some $x_0 \in S$, we may recursively define a sequence (x_n) by letting $x_{n+1} = g(x_n)$ for each $n \in \mathbb{N}$, so that we have

$$\cdots < x_3 < x_2 < x_1 < x_0$$

Then we have that the mapping $n \mapsto x_n$ is an order embedding of $(\mathbb{N}, \leq)^*$ into $(A, \leq)$, as desired. $\square$

Proposition 2. *If $(A, \leq)$ is a well-ordering and $f : A \to A$ is an order embedding of A into itself, then $f(x) \geq x$ for all x.*

Proof. Suppose that $(A, \leq)$ is a well-ordering, and that $f : A \to A$ is an order embedding. Then f strictly preserves order, so that $x < y$ implies $f(x) < f(y)$ for all $x, y \in A$. If we assume for the sake of contradiction that

$$f(x) < x$$

for some $x \in A$, then we may apply f to both sides of this inequality to obtain

$$f(f(x)) < f(x) < x$$

and apply f again to obtain

$$f(f(f(x))) < f(f(x)) < f(x) < x$$

and so on. More generally, we may define a strictly decreasing sequence recursively by letting $x_0 = x$ and $x_{n+1} = f(x_n)$, and prove inductively that $x_{n+1} < x_n$ for all $n \in \mathbb{N}$. But this means that the map $n \mapsto x_n$ is an order embedding of $(\mathbb{N}, \leq)^*$, contradicting the fact that $(A, \leq)$ was a well-ordering by the previous proposition. □

Proposition 3. *If $(A, \leq)$ is a well-ordering, then it has no non-identity order automorphisms.*

Proof. Suppose that $f : (A, \leq) \to (A, \leq)$ is a non-identity order automorphism. Then, for some $a \in A$, we have that $f(a) \neq a$, since f is not the identity function by hypothesis. This means that either $f(a) > a$ or $f(a) < a$. The latter is impossible by the previous proposition, and the former implies that $a > f^{-1}(a)$ because f is a bijection and f^{-1} is another order automorphism, which also contradicts the previous proposition. Thus, there are no non-identity automorphisms of a well-ordering. □

Proposition 4. *If α is an ordinal and $\alpha + \beta = \alpha + \gamma$ for some order types β, γ, then $\beta = \gamma$.*

Proof. Suppose that $(A, \leq)$ has order type α so that it is a well-ordering, and suppose $(B, \leq)$ has order type β and $(C, \leq)$ has order type γ. Then, since $\alpha + \beta = \alpha + \gamma$, there exists an order isomorphism

$$f : (A, \leq) + (B, \leq) \ \to \ (A, \leq) + (C, \leq)$$

Let A_B be the subset of $(A, \leq) + (B, \leq)$ consisting of elements of the form $(a, 0)$, and let A_C be the subset of $(A, \leq) + (C, \leq)$ consisting of elements of the form $(a, 0)$.

We will show that the image of A_B under f is equal to A_C. Since A_B is an initial segment of the former ordering, we have that $f(A_B)$ must be an initial segment of the latter. Hence, if we assume for the sake of contradiction that $f(A_B) \neq A_C$, then either $f(A_B)$ is a proper initial segment of A_C, or A_C is a proper initial segment of $f(A_B)$. If the former is the case, then we may construct an order preserving function $g : (A, \leq) \to (A, \leq)$ defined by letting $g(a)$ be the first coordinate of $f((a, 0))$. But because $f(A_B)$ is a proper initial segment of A_C, we would have that there exists a such that $g(a) < a$, contradicting a previous proposition. Similarly, if A_C is a proper initial segment of $f(A_B)$, then we can define $g : (A, \leq) \to (A, \leq)$ by letting $g(a)$ be the first coordinate of $f^{-1}((a, 0))$, so that we will again have $a \in A$ such that $f(a) < a$, leading to the same contradiction. We must therefore have that $f(A_B) = A_C$.

Since f must map the $(A, \leq)$ component of $(A, \leq)+(B, \leq)$ to the $(A, \leq)$ component of $(A, \leq)+(C, \leq$), we have that in must also map the $(B, \leq)$ component of the former to the $(C, \leq)$ component of the latter. But since f is an order isomorphism, it restricts to an order isomorphism between $(B, \leq)$ and $(C, \leq)$, establishing that $\beta = \gamma$ as claimed. □

The wild world of ordinal numbers contains many exotic order types, and there just isn't enough time to go into them in-depth in this minicourse. If you want to dive deeper into the properties of ordinal arithmetic and some of the less intuitive facts about them, have a look at the following exercises.

1. Prove that ordinal multiplication is left-cancellable.
2. Prove that every ordinal number has finitely many right-hand divisors. Which ordinals have finitely many left-hand divisors?
3. Let A be the set of all finite sequences of natural numbers, ordered in such a way that $x < y$ for any finite sequences x, y where the length of x is less than the length of y, and such that any two sequences of *the same length* are compared using the lexicographic ordering. Prove that this is a well-ordering. Its order type is an ordinal denoted ω^ω.
4. Prove that $\alpha \cdot \omega > \alpha$ for any ordinal $\alpha > \mathbf{1}$. Then find a nonzero ordinal α such that $\omega \cdot \alpha = \alpha$.
5. We know that $\mathbf{1} + \omega = \omega$. Can you find an ordinal α such that $\omega + \alpha = \alpha$? Can you find α such that $\omega^5 + \alpha = \alpha$? Can you find α such that $\omega^n + \alpha = \alpha$ for all $n \in \mathbb{N}$?
6. Prove that $\omega^\omega \hookrightarrow \lambda$. Show also that there exists an ordinal α such that $\alpha \not\hookrightarrow \lambda$.