Ordinals in Scunak

Chad E. Brown

cebrown@ags.uni-sb.de

Universität des Saarlandes, Saarbrücken, Germany

What is Scunak?

Scunak is

- Like Automath, Twelf and Coq: Dependent Type Theory, Proof Terms
- Like Coq, Isabelle, and TPS: Interactive Proving Facilities
- Like Mizar: Mathematics encoded in Set Theory

but

- not Automath, Twelf, Coq, TPS, Isabelle: Different Type Theory
- not TPS, Isabelle-HOL: Set Theory, not HOL
- not Isabelle-ZF, Mizar: Different Set Theory
- not Mizar: Computes Proof Objects.

Scunak Type Theory

Terms: x|c|$(\lambda x M)$|(MN)|$\langle M, N\rangle$ | $\pi_1(M)$ | $\pi_2(M)$

Types: `obj` | `prop` | $\vdash \phi$ | $\{x|\phi(x)\}$ | $\Pi x : A.B$

Like LF except:

- Restricted to three type families: `obj` (all mathematical objects); `prop` (all propositions); $\vdash \phi$ (proofs of ϕ)
- Proof irrelevance: at most one inhabitant of $\vdash \phi$
- Special sum types, the class type $\{x|\phi(x)\}$, equivalent to $\Sigma_{x:\mathtt{obj}} \vdash \phi(x)$
- Restricted to second-order λ-calculus.

Set Theory in Scunak

Axiomatic Basis: 30 basic concepts (propositional constructors, object constructors, proof constructors)

Mac Lane Set Theory, with (global) choice, plus universes, but without foundation.

Set Theory in Scunak

Axiomatic Basis: 30 basic concepts (propositional constructors, object constructors, proof constructors)

3 basic propositional constructors:

- Negation
  $\neg\phi$ where $\phi : \texttt{prop}$
- Equality between objects (i.e., sets)
  $x = y$ where $x, y : \texttt{obj}$
- Membership $x \in y$ where $x, y : \texttt{obj}$

Set Theory in Scunak

Axiomatic Basis: 30 basic concepts (propositional constructors, object constructors, proof constructors)

7 constructors for objects (sets):

- The empty set $\emptyset$
- Separation $\{x \in A | \phi(x)\}$
- **Set adjunction** $(x; A)$**, intuitively,** $\{x\} \cup A$
- Powerset $\mathcal{P}(A)$
- Set Union $\bigcup A$
- Universes $Univ(A)$
  A universe is a set containing A closed under the operations above.
- (Global) Choice...

Proof Rules

Remaining 20 basic concepts are natural deduction rules.

Proof Rules

Remaining 20 basic concepts are natural deduction rules.

For Example, Set Adjoin Elimination:

$$\dfrac{x \in (\{A\} \cup B) \qquad \begin{array}{c} \overline{x = A}^{\,u} \\ \vdots \\ \phi \end{array} \qquad \begin{array}{c} \overline{x \in B}^{\,v} \\ \vdots \\ \phi \end{array}}{\phi}\ \texttt{setadjoinE}^{u,v}$$

If $x \in (\{A\} \cup B)$ and ϕ is provable both under the assumption $x = A$ and under the assumption $x \in B$, then ϕ is provable.

Purity of Set Theory Axioms

All the basic concepts, including rules, are given without using *any* abbreviations.

1. All 30 constants are declared.
2. Everything after that is an abbreviation.

Some Defined Concepts

Logical Operators: $\wedge$, $\vee$, $\supset$

Bounded, Dependent, Quantifiers: $\forall x \in A.\phi(x)$ and $\exists x \in A.\phi(x)$

Set Theory Relations: $\subseteq$

Set Theory Operations: $\cup$, $\cap$

Ordinals

$\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}, \emptyset\}$, $\ldots$, ω, $\{\omega\} \cup \omega$, $\ldots$

Ordinals

$\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\},\emptyset\}$, $\ldots$, ω, $\{\omega\} \cup \omega$, $\ldots$

ω: Natural Numbers where $\in$ behaves like $<$.

Ordinals

$\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\},\emptyset\}$, $\ldots$, ω, $\{\omega\} \cup \omega$, $\ldots$

ω: Natural Numbers where $\in$ behaves like $<$.

$\emptyset$: Like 0

Ordinals

$\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\},\emptyset\}$, $\ldots$, ω, $\{\omega\} \cup \omega$, $\ldots$

ω: Natural Numbers where $\in$ behaves like $<$.

$\emptyset$: Like 0

$\{\emptyset\}$, i.e., $\{0\}$, like 1

Ordinals

$\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\},\emptyset\}$, $\ldots$, ω, $\{\omega\} \cup \omega$, $\ldots$

ω: Natural Numbers where $\in$ behaves like $<$.

$\emptyset$: Like 0

$\{\emptyset\}$, i.e., $\{0\}$, like 1

$\{\{\emptyset\},\emptyset\}$, i.e., $\{1,0\}$, like 2

Ordinals

$\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}, \emptyset\}$, $\ldots$, ω, $\{\omega\} \cup \omega$, $\ldots$

ω: Natural Numbers where $\in$ behaves like $<$.

$\emptyset$: Like 0

$\{\emptyset\}$, i.e., $\{0\}$, like 1

$\{\{\emptyset\}, \emptyset\}$, i.e., $\{1, 0\}$, like 2

Successors are formed by *adjoining* the set to itself:
$\{A\} \cup A$, i.e., $(A; A)$.

Ordinals

$\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\},\emptyset\}$, ..., ω, $\{\omega\} \cup \omega$, $\ldots$

ω: Natural Numbers where $\in$ behaves like $<$.

$\emptyset$: Like 0

$\{\emptyset\}$, i.e., $\{0\}$, like 1

$\{\{\emptyset\},\emptyset\}$, i.e., $\{1,0\}$, like 2

Successors are formed by *adjoining* the set to itself:
$\{A\} \cup A$, i.e., $(A;A)$.

Limit Ordinals (e.g., ω) equal $\bigcup X$ where X is an unbounded set of ordinals.

What is an Ordinal?

Defn: A set α is an *Ordinal* if

- α is "transitive" (it isn't *that* transitive)
  $y \in \alpha$ implies $y \subseteq \alpha$
- α is well-ordered by $\in$, i.e.:
  α is strictly totally ordered by $\in$
  Every nonempty subset Y of α has a $\in$-least element.

What is an Ordinal?

Defn: A set α is an *Ordinal* if

- α is "transitive" (it isn't *that* transitive)
  $y \in \alpha$ implies $y \subseteq \alpha$
- α is well-ordered by $\in$, i.e.:
  α is strictly totally ordered by $\in$
  Every nonempty subset Y of α has a $\in$-least element.

Ill-typed in HOL.

What is an Ordinal?

Defn: A set α is an *Ordinal* if

- α is “transitive” (it isn’t *that* transitive)
  $y \in \alpha$ implies $y \subseteq \alpha$
- α is well-ordered by $\in$, i.e.:
  α is strictly totally ordered by $\in$
  Every nonempty subset Y of α has a $\in$-least element.

Scunak Abbreviations:

```
[alpha:obj]
(transitiveset alpha):prop
=(forall y:alpha .  (y<=alpha)).
```

What is an Ordinal?

Defn: A set α is an *Ordinal* if

- α is "transitive" (it isn't *that* transitive)
  $y \in \alpha$ implies $y \subseteq \alpha$
- α is well-ordered by $\in$, i.e.:
  α is strictly totally ordered by $\in$
  Every nonempty subset Y of α has a $\in$-least element.

Scunak Abbreviations:

```
[alpha:obj]
(transitiveset alpha):prop
=(forall y:alpha .  (y<=alpha)).
```

Parsed and Reconstructed into:

$\texttt{transitiveset} : \Pi\alpha : \texttt{obj}.\texttt{prop}$
$= \lambda\alpha(\texttt{dall}\,\alpha(\lambda y(\texttt{subset}\,\pi_1(y)\,\alpha)))$

What is an Ordinal?

Defn: A set α is an *Ordinal* if

- α is "transitive" (it isn't *that* transitive)
  $y \in \alpha$ implies $y \subseteq \alpha$
- α is well-ordered by $\in$, i.e.:
  α is strictly totally ordered by $\in$
  Every nonempty subset Y of α has a $\in$-least element.

Scunak Abbreviations:

```
(stricttotalorderedByIn alpha):prop
=((forall a b c:alpha .
     (((a::b) & (b::c)) => (a::c)))
& (forall a b:alpha .
     ((a==b)|((a::b)|(b::a))))
& (forall a:alpha .  (not (a::a)))).
```

What is an Ordinal?

Defn: A set α is an *Ordinal* if

- α is "transitive" (it isn't *that* transitive)
  $y \in \alpha$ implies $y \subseteq \alpha$
- α is well-ordered by $\in$, i.e.:
  α is strictly totally ordered by $\in$
  Every nonempty subset Y of α has a $\in$-least element.

Scunak Abbreviations:

```
(wellorderedByIn alpha):prop
=((stricttotalorderedByIn alpha)
& (forall Y:(powerset alpha) .
((nonempty Y) =>
(exists a:Y . (forall b:Y . ((a==b)|(a::b))))))
```

What is an Ordinal?

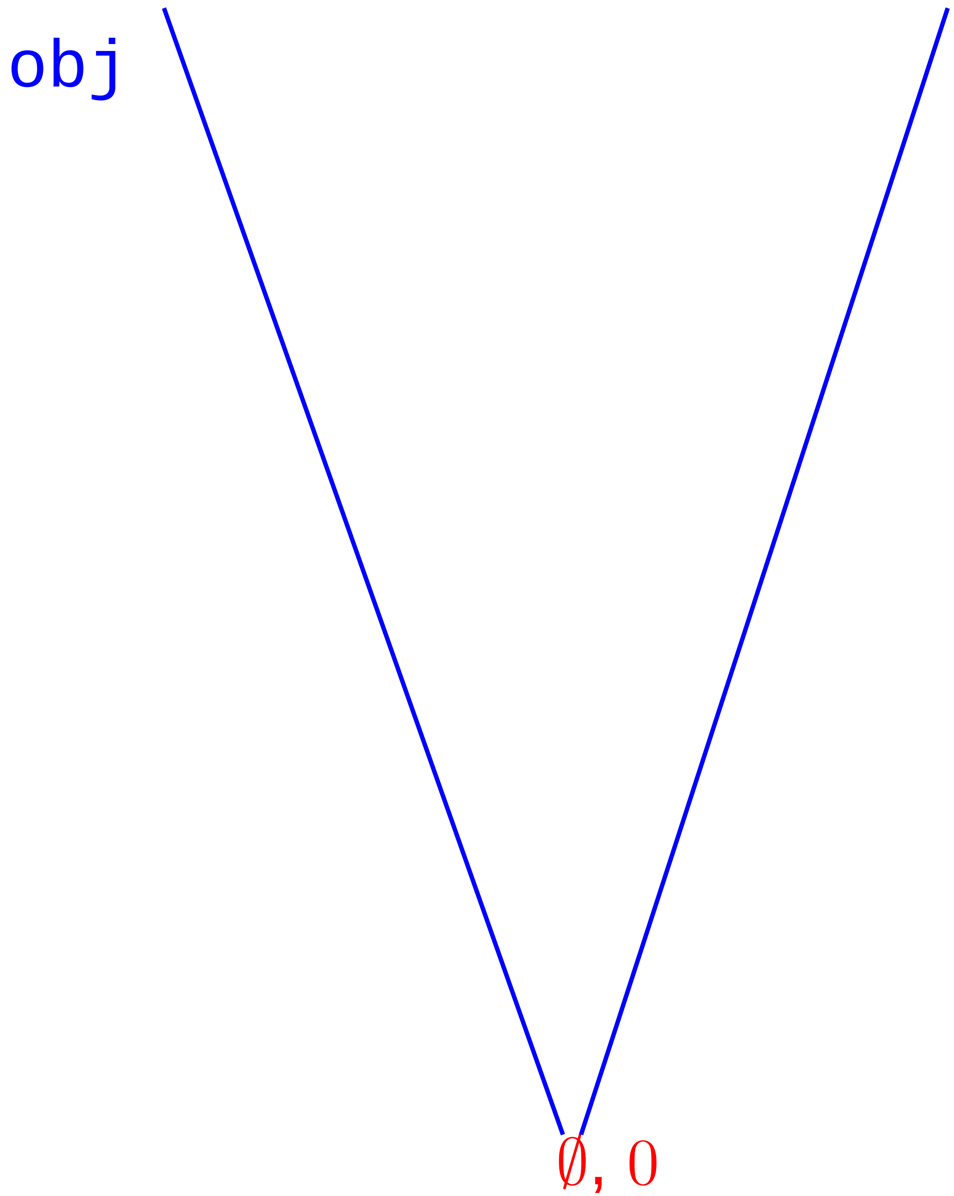
Defn: A set α is an *Ordinal* if

- α is "transitive" (it isn't *that* transitive)
  $y \in \alpha$ implies $y \subseteq \alpha$
- α is well-ordered by $\in$, i.e.:
  α is strictly totally ordered by $\in$
  Every nonempty subset Y of α has a $\in$-least element.

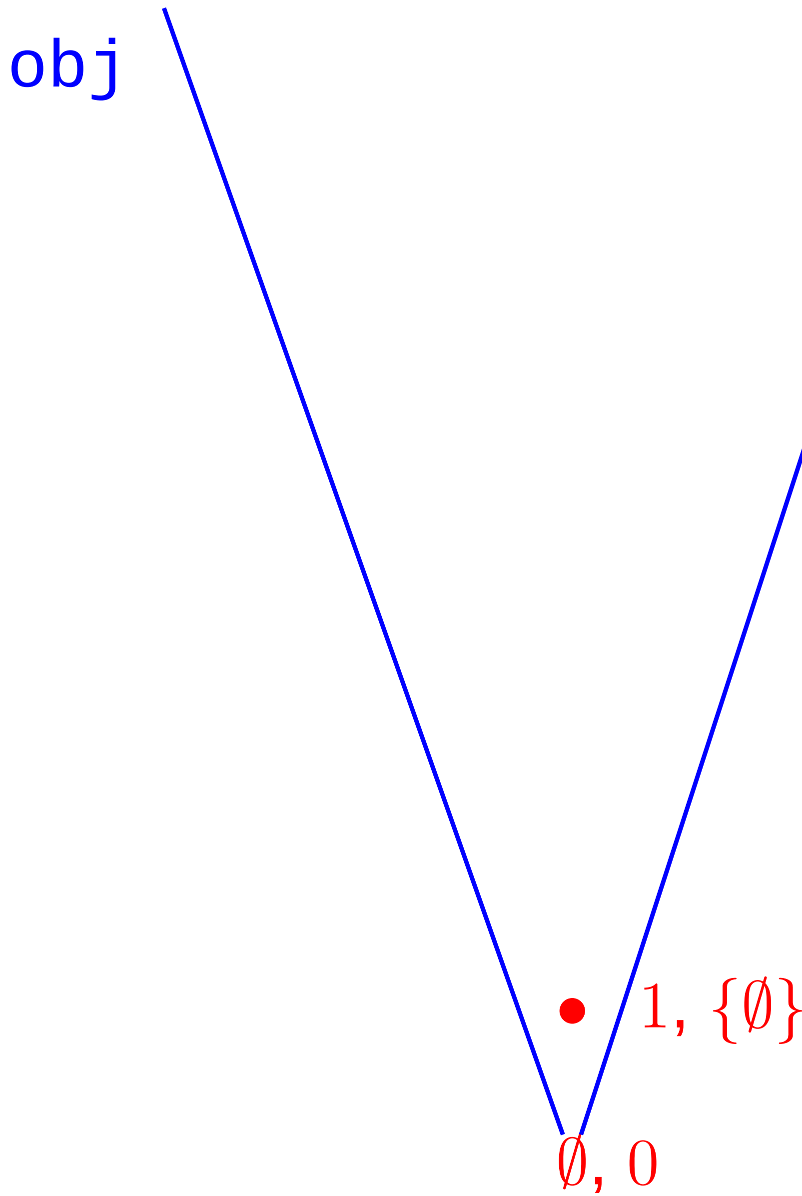
Scunak Abbreviations:

```
(ordinal alpha):prop
  =((transitiveset alpha) &
    (wellorderedByIn alpha)).
```

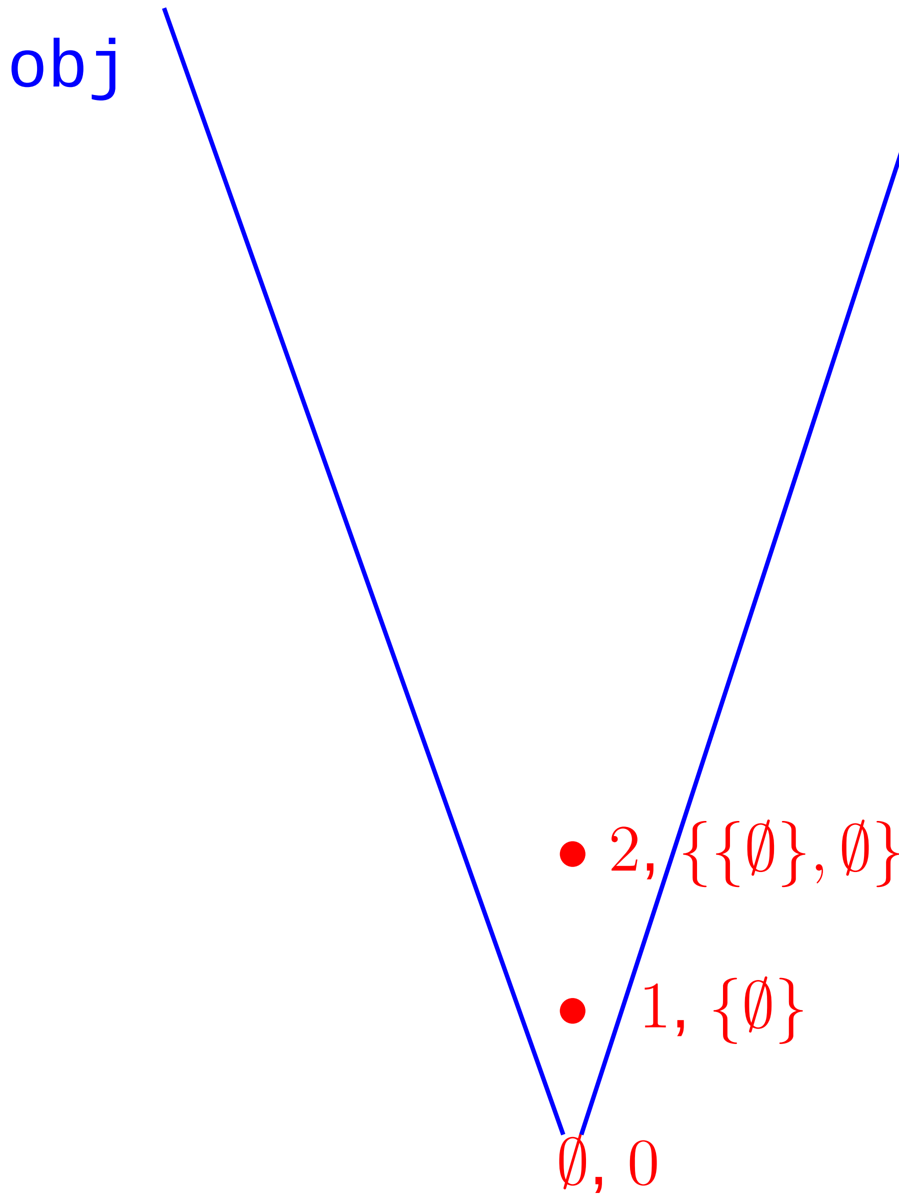
What is an Ordinal?



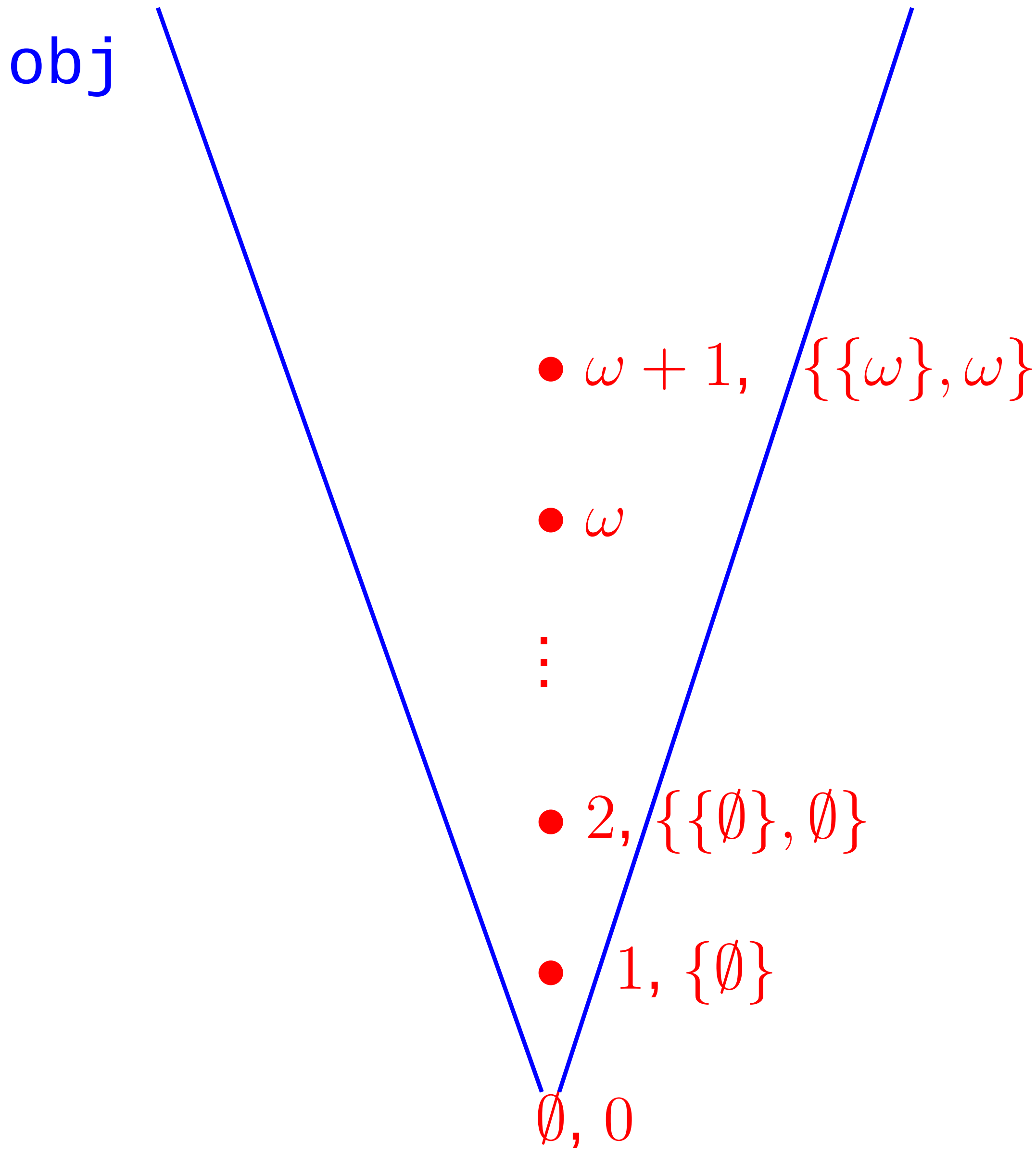
What is an Ordinal?



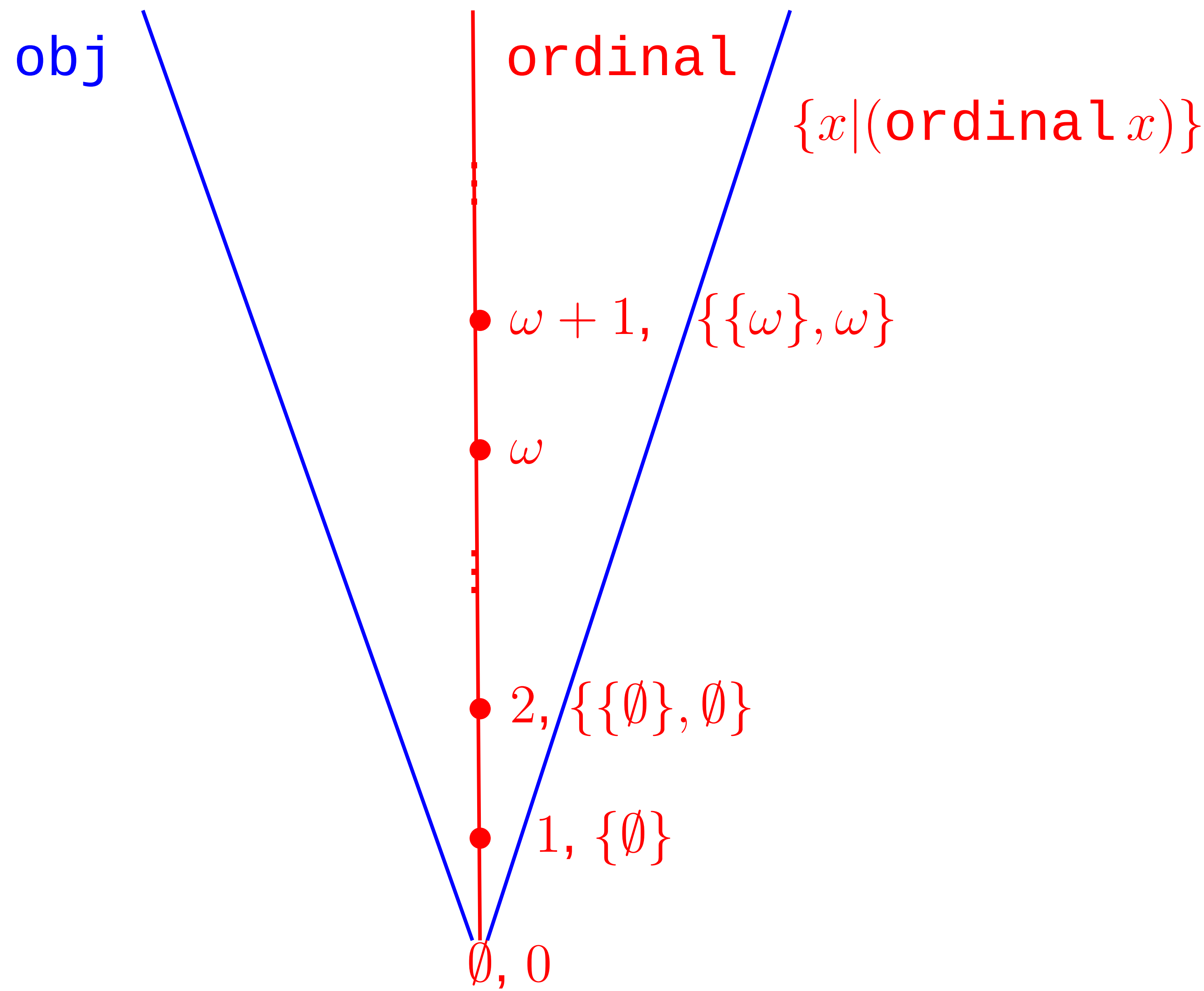
What is an Ordinal?



What is an Ordinal?



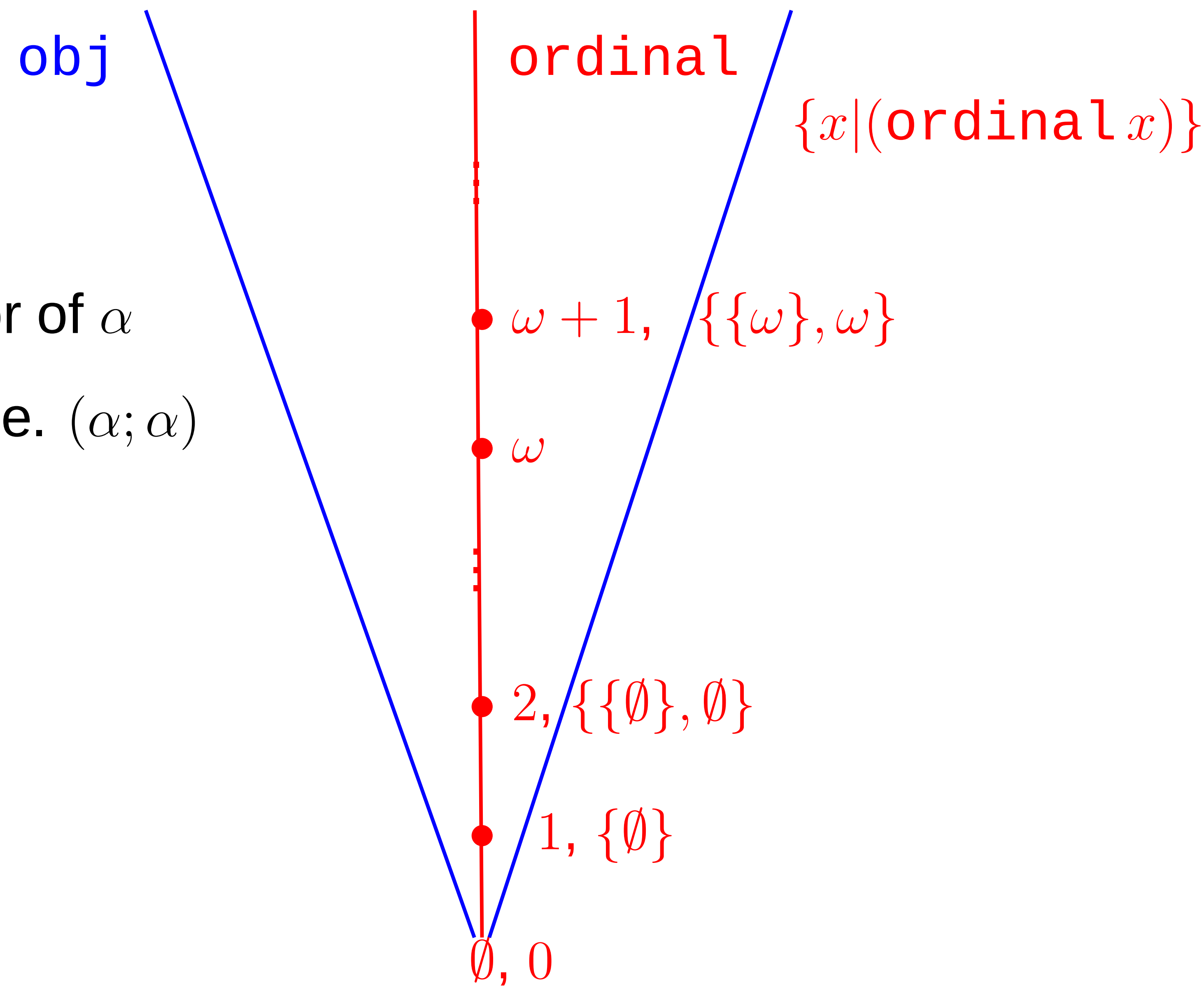
What is an Ordinal?



Operations On Ordinals

Successor of α

$\{\alpha\} \cup \alpha$, i.e. $(\alpha;\alpha)$



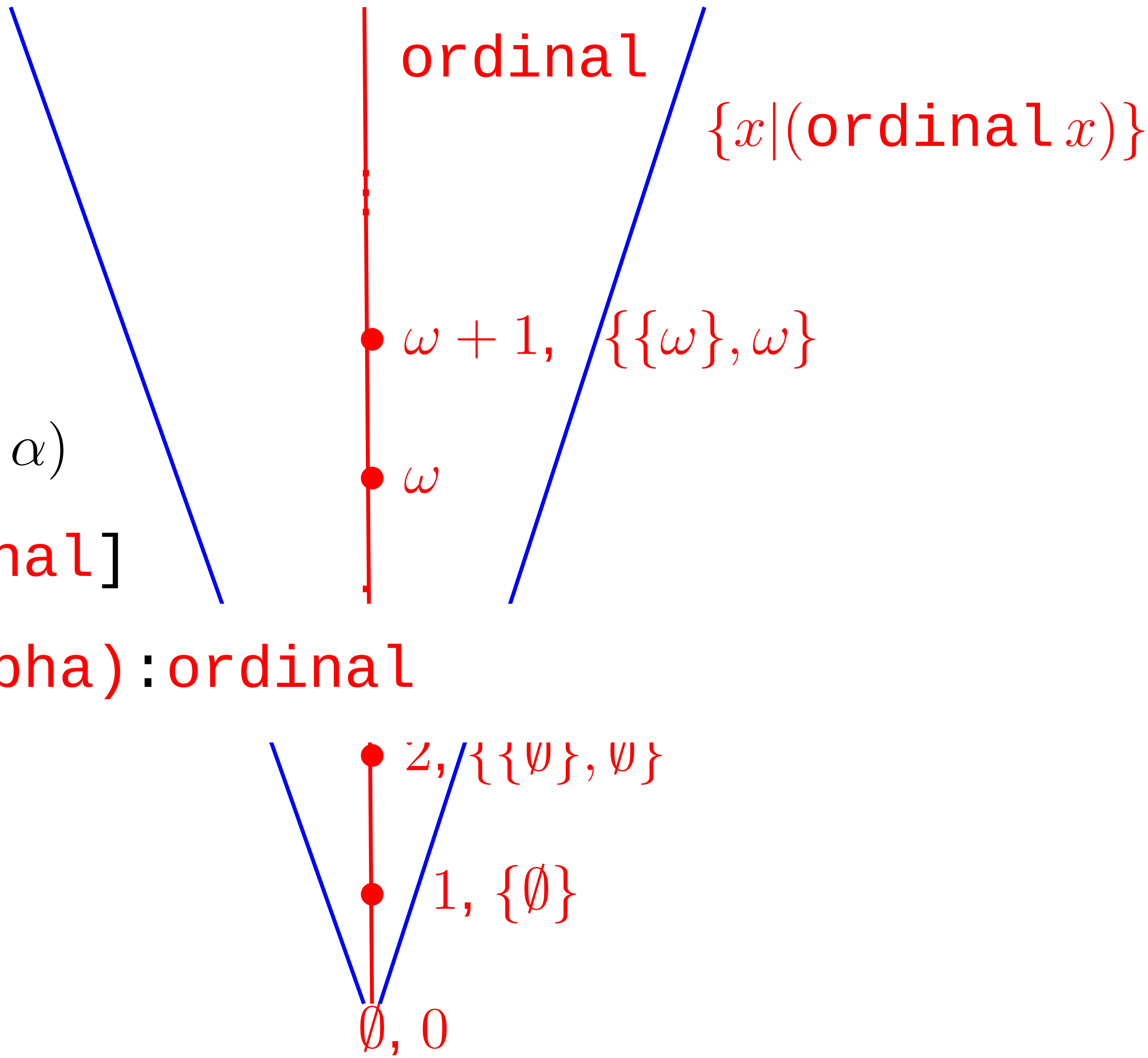
Operations On Ordinals

Successor of α

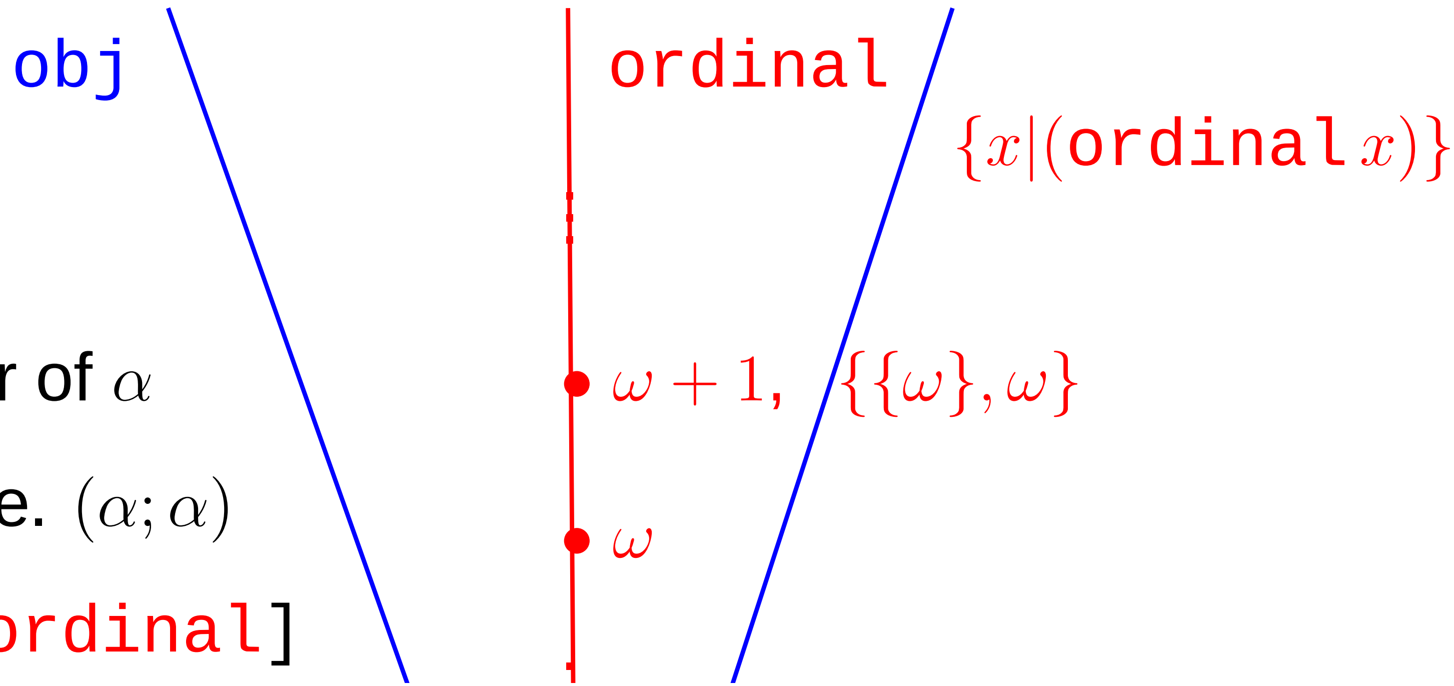
$\{\alpha\} \cup \alpha$, i.e. $(\alpha; \alpha)$

`[alpha:ordinal]`

`(ordsucc alpha):ordinal`



Operations On Ordinals



Successor of α

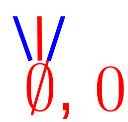
$\{\alpha\} \cup \alpha$, i.e. $(\alpha;\alpha)$

`[alpha:ordinal]`

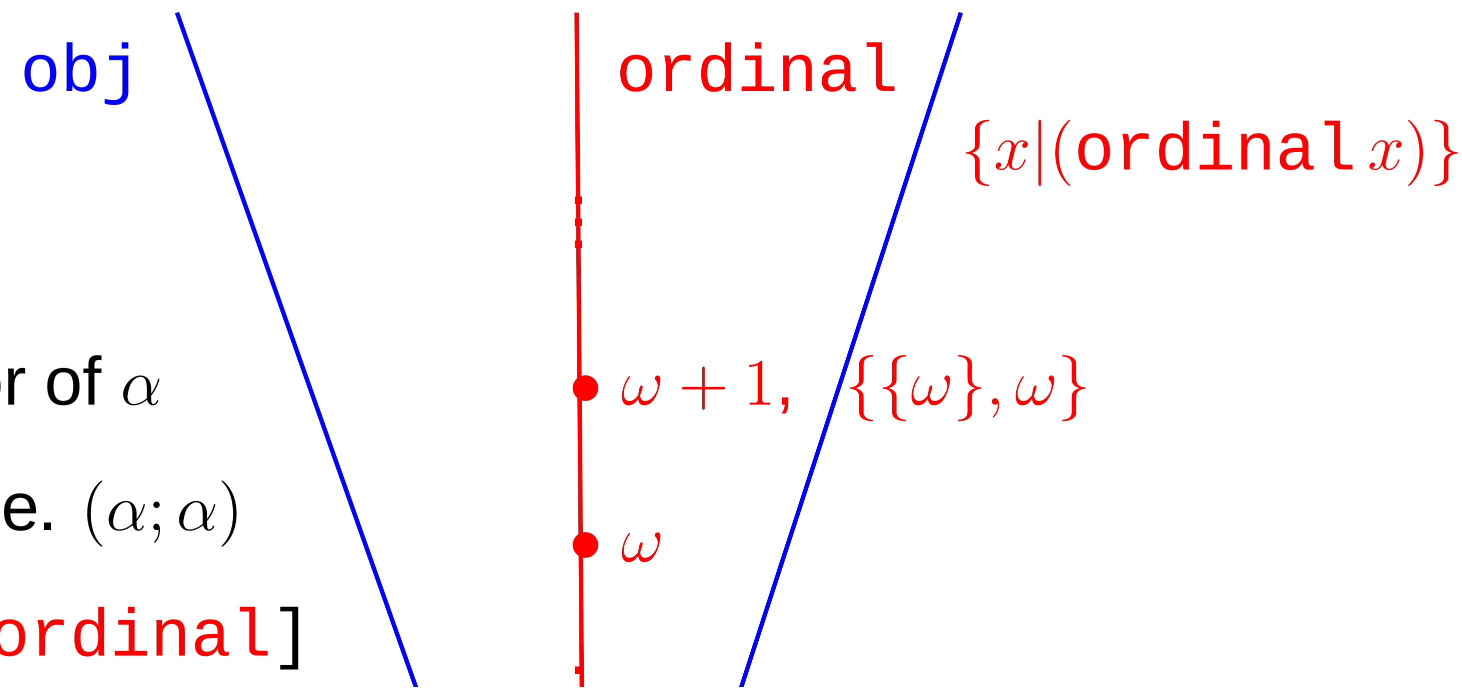
`(ordsucc alpha):ordinal`

`<(alpha;alpha),(ordsuccOrdinal alpha)>`

`(alpha;alpha)` corresponds to $(\texttt{setadjoin}\ \pi_1(\alpha)\ \pi_1(\alpha))$



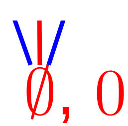
Operations On Ordinals



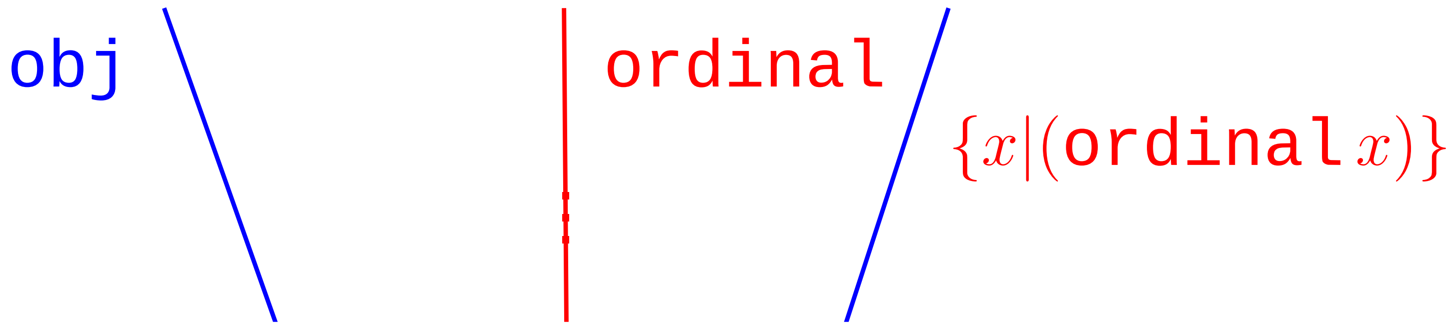
Successor of α

$\{\alpha\} \cup \alpha$, i.e. $(\alpha;\alpha)$

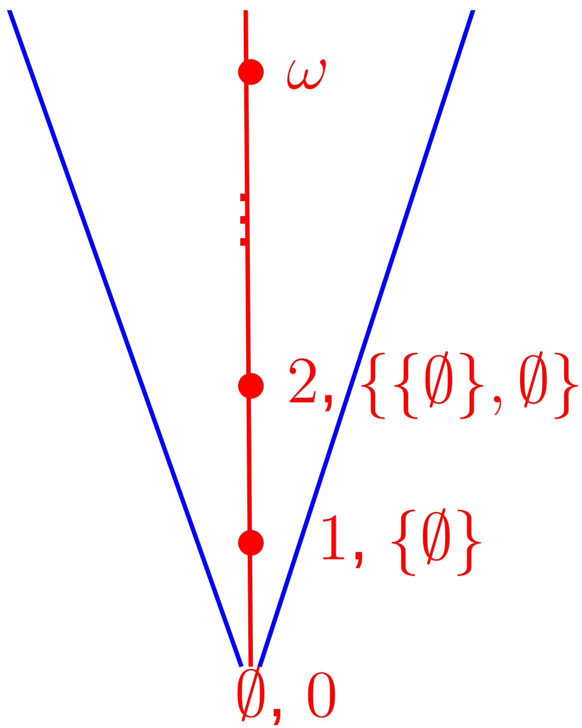
```
[alpha:ordinal]
(ordsucc alpha):ordinal
<(alpha;alpha),(ordsuccOrdinal alpha)>
(ordsuccOrdinal alpha):⊢ (ordinal (alpha;alpha))
```



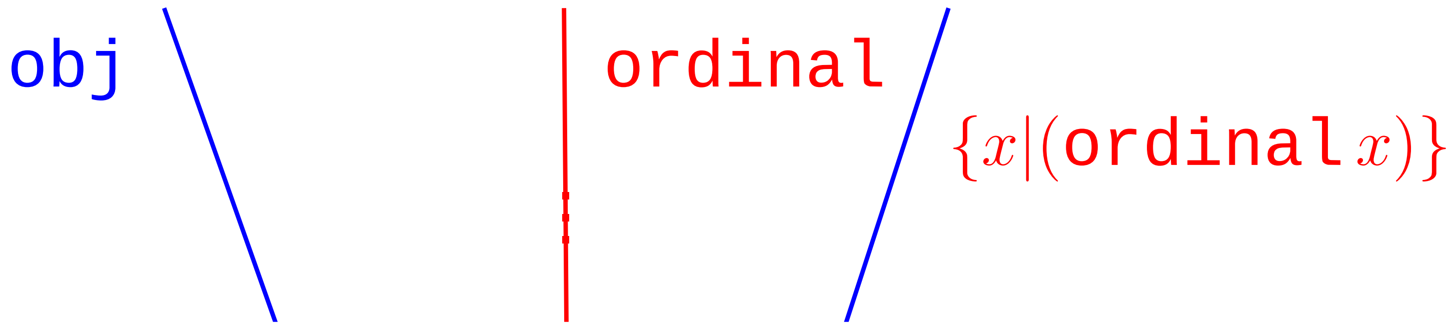
Operations On Ordinals



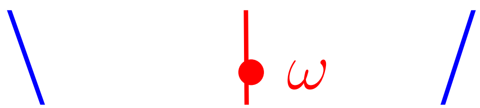
Supremum of a set X of ordinals: $\bigcup X$



Operations On Ordinals

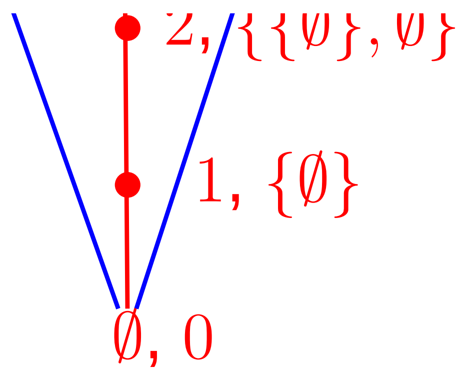


Supremum of a set X of ordinals: $\bigcup X$

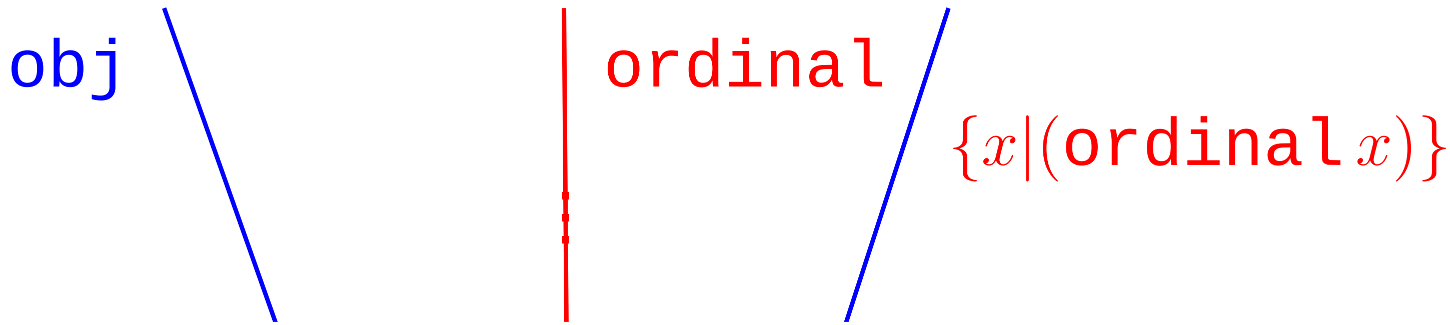


[X:{A | ∀ x ∈ A . (ordinal x)}]

(ordsup X):ordinal



Operations On Ordinals

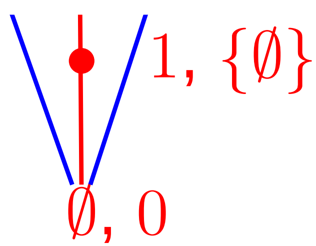


Supremum of a set X of ordinals: $\bigcup X$

[X:{A | ∀ x ∈ A . (ordinal x)}]

(ordsup X):ordinal

<(⋃ X),(setunionOrdinal X)>



Operations On Ordinals

obj ordinal

$\{x | (\texttt{ordinal}\, x)\}$

Supremum of a set X of ordinals: $\bigcup X$

ω

[X:{A | ∀ x ∈ A . (ordinal x)}]

(ordsup X):ordinal

<(⋃ X),(setunionOrdinal X)>

(setunionOrdinal alpha):⊢ (ordinal (⋃ X))

$\emptyset$, 0

Making Claims

To define successor on ordinals, we used a proof term.

This can be declared as a claim:

```
[alpha:ordinal]
(ordsuccOrdinal alpha):⊢ (ordinal
                              (alpha;alpha))?
```

We then prove the claim interactively to obtain the proof term.

Making Claims

Actually, we split this into three lemmas.

```
(ordsuccOrdinalLem1 alpha):⊢
     (transitiveset (alpha ; alpha))?

(ordsuccOrdinalLem2 alpha):⊢
   (stricttotalorderedByIn (alpha ; alpha))?

(ordsuccOrdinalLem3 alpha):⊢

     (wellorderedByIn (alpha ; alpha))?
```

Proving Claims Interactively

Consider First Claim:

```
(ordsuccOrdinalLem1 alpha):⊢
     (transitiveset (alpha ; alpha))?
```

“If α is an ordinal, then $\{\alpha\} \cup \alpha$ is a transitive set.”

Proving Claims Interactively

```
prove ordsuccOrdinalLem1

Give name for ordinal>alpha

>pplan

Support (Objects, Assumptions and Derived
Facts in Context):

alpha:ordinal

fact0:|- (ordinal alpha)

Goal (What you need to show):  |-
(transitiveset (alpha;alpha))
```

The goal has an abbreviation `transitiveset` at the head.

Unfold it, working backwards.

Proving Claims Interactively

```
>foldhead

OK

>pplan

Support (Objects, Assumptions and Derived
Facts in Context):

alpha:ordinal

fact0:|- (ordinal alpha)

Goal (What you need to show):  |- (dall
(alpha;alpha) (λ x2.(x2<=(alpha;alpha))))
```

New Goal: $\forall x \in \{\alpha\} \cup \alpha \,.\, (x \subseteq (\{\alpha\} \cup \alpha))$.

Proving Claims Interactively

New Goal: $\forall x \in \{\alpha\} \cup \alpha \,.\, (x \subseteq (\{\alpha\} \cup \alpha))$.
Introduce the quantifier.

```
>intro
OK

Give name for (in (alpha;alpha))>x
```

Proving Claims Interactively

```
>pplan
Support ...:
alpha:ordinal
fact0:|- (ordinal alpha)
x:(in (alpha;alpha))
fact2:|- (x::(alpha;alpha))
Goal (What you need to show):  |-
(x<=(alpha;alpha))
```

Assume $x \in (\{\alpha\} \cup \alpha)$

Show $x \subseteq (\{\alpha\} \cup \alpha)$

Split into cases: $x = \alpha$ or $x \in \alpha$.

Proving Claims Interactively

```
>adjcases
OK
>pplan
Support ...:
alpha:ordinal
fact0:|- (ordinal alpha)
x:(in (alpha;alpha))
fact2:|- (x::(alpha;alpha))
ass0:|- (x==alpha)
```

New Assumption $x = \alpha$.

```
Goal (What you need to show): |-
(x<=(alpha;alpha))
```

Proving Claims Interactively

```
>pstatus
0) (ass0 fact2 x fact0 alpha) |-
(x<=(alpha;alpha))
1) (fact2 x fact0 alpha) x4:|- (x::alpha)|-
(x<=(alpha;alpha))
```

There are now two gaps to fill corresponding to the two cases:

0) $x = \alpha$

1) $x \in \alpha$

Proving Claims Interactively

Current Case: $x = \alpha$

Current Goal: $x \subseteq (\{\alpha\} \cup \alpha)$

Idea: Use $\alpha \subseteq (\{\alpha\} \cup \alpha)$.

```
>fact
Enter Proposition>(alpha<=(alpha;alpha))
Correct.
```

The `fact` command tells Scunak to look for something to justify the given proposition in context.

Proving Claims Interactively

```
>pplan
Support ...:
alpha:ordinal
fact0:|- (ordinal alpha)
x:(in (alpha;alpha))
fact2:|- (x::(alpha;alpha))
ass0:|- (x==alpha)
fact4:|- (alpha<=(alpha;alpha))
Goal (What you need to show):  |-
(x<=(alpha;alpha))
>d

Done with subgoal!
```

$x = \alpha$

$\alpha \subseteq (\alpha;\alpha)$

Show: $x \subseteq (\alpha;\alpha)$

Scunak finishes

Proving Claims Interactively

Next Case: $x \in \alpha$

Goal: $x \subseteq (\{\alpha\} \cup \alpha)$

Idea: Use transitivity of ordinal α.

```
>fact
Enter Proposition>(x<=alpha)
Correct.
```

Scunak justifies $x \subseteq \alpha$ using $x \in \alpha$ and the fact that α is an ordinal.

Proving Claims Interactively

```
>pplan
Support ...:
alpha:ordinal
fact0:|- (ordinal alpha)
x:(in (alpha;alpha))
fact2:|- (x::(alpha;alpha))
ass1:|- (x::alpha)
fact5:|- (x<=alpha)
Goal (What you need to show):  |-
(x<=(alpha;alpha))
```

$x \subseteq \alpha$

Show: $x \subseteq (\{\alpha\} \cup \alpha)$

This gap is trivial enough...

Proving Claims Interactively

```
>d                                                    Scunak Finishes
Done with subgoal!
Successful Term:                                           Proof Term
(λ x0.transitiveset#F (x0;x0) (dallI (x0;x0)
(λx1.(x1<=(x0;x0))) (λx1.setadjoinE x0
x0 x1 x1 (x1<=(x0;x0)) (λx2.equivEimp1
(x0<=(x0;x0)) (x1<=(x0;x0)) (subset#Cong
x0 x1 (symeq x1 x0 x2) (x0;x0) (x0;x0)
(eqI (x0;x0))) (setadjoinSub x0
x0)) (λx2.setadjoinSub2 x1 x0 x0
(ordinalTransSet1 x0 x1 x2)))))
```

Proving Claims Interactively

What facts were used in the proof?

`transitiveset#F` : Definition of `transitiveset`

`dallI` : Forall introduction

`setadjoinE` : Cases rule for $x \in (A; B)$

`setadjoinSub` : $B \subseteq (A; B)$.

`setadjoinSub2` : If $Y \subseteq B$, then $Y \subseteq (A; B)$

`ordinalTransSet1` : If β is an ordinal and $y \in \beta$, then $y \subseteq \beta$.

+ some equality reasoning

Currently Proven

- $\emptyset$ is an ordinal.
- If α is an ordinal, then $\alpha \notin \alpha$.
- If α is an ordinal, then $(\alpha; \alpha)$ is an ordinal.
- If α is an ordinal and $x \in \alpha$, then x is an ordinal.
- Every ordinal is a successor or a limit ordinal.
- If α is an ordinal and $\alpha \in x$, then $x \notin \alpha$.
- If α and β are ordinals and α is a proper subset of β, then $\alpha \in \beta$.
- If α and β are ordinals, then $\alpha \cap \beta$ is an ordinal.
- If α and β are ordinals, then $\alpha = \beta$, $\alpha \in \beta$, or $\beta \in \alpha$.

Currently Proven

- Any set of ordinals is well-ordered by $\in$.
- No ordinal is between α and the successor of α.
- If X is a set of ordinals, then $\bigcup X$ is an ordinal.
- **Ordinal Induction:** Let ϕ be a property. Assume for every ordinal α, $\phi(\alpha)$ holds if $\phi(x)$ holds for every $x \in \alpha$. Then $\phi(\alpha)$ holds for all ordinals α.

Conclusion

Scunak can encode ordinals nicely because:

- The untyped set theory allows the “ill-typed” definition of the ordinals.
- The dependent type theory allows the class of ordinals to be used as a type.

Also,

- The interactive prover allows reuse of previously proven facts without explicit mention of the names of the facts.

Future Work:

- Counting as high as I can.