Implementation of Bourbaki’s Elements of Mathematics in Coq: Part Two
Ordered Sets, Cardinals, Integers

José Grimm

N° 7150 — version 2
initial version December 2009 — revised version April 2010

Programs, Verification and Proofs
Implementation of Bourbaki’s Elements of Mathematics in Coq:
Part Two
Ordered Sets, Cardinals, Integers

José Grimm∗

Theme : Programs, Verification and Proofs
Équipe-Projet Apics

Rapport de recherche n° 7150 — version 2 — initial version December 2009 — revised
version April 2010 — 304 pages

Abstract: We believe that it is possible to put the whole work of Bourbaki into a computer. One of the objectives of the Gaia project concerns homological algebra (theory as well as algorithms); in a first step we want to implement all nine chapters of the book Algebra. But this requires a theory of sets (with axiom of choice, etc.) more powerful than what is provided by Ensembles; we have chosen the work of Carlos Simpson as basis. This reports lists and comments all definitions and theorems of the Chapter “Ordered Sets, Cardinals, Integers”. The code (including some exercises) is available on the Web, under http://www-sop.inria.fr/apics/gaia.

Key-words: Gaia, Coq, Bourbaki, orders, cardinals, ordinals, integers

Work done in collaboration with Alban Quadrat

∗ Email: Jose.Grimm@sophia.inria.fr
Implémentation de la théorie des ensembles de Bourbaki dans Coq
partie 2
Ensembles Ordonnés, cardinaux, nombres entiers


Mots-clés : Gaia, Coq, Bourbaki, ordre, cardinaux, ordinaux, entiers
Chapter 1

Introduction

1.1 Objectives

Our objective (it will be called the Bourbaki Project in what follows) is to show that it is possible to implement the work of N. Bourbaki, “Éléments de Mathématiques” [3], into a computer, and we have chosen the Coq Proof Assistant, see [4,1]. All references are given to the English version “Elements of Mathematics” [2], which is a translation of the French version (the only major difference is that Bourbaki uses an axiom for the ordered pair in the English version and a theorem in the French one). We start with the first book: theory of sets. It is divided into four chapters, the first one describes formal mathematics (logical connectors, quantifiers, axioms, theorems). Chapters II describes sets, unions, intersections, functions, products, equivalences; Chapter III defines orders, integers, cardinals, limits. The last chapter describes structures. The first part of this report [5] describes Chapter I and Chapter II, we consider here Chapter III.

1.2 Content of this document

This document describes the code found in the files set5.v, set6.v, set7.v, set8.v, set9.v, and set10.v, corresponding to sections 1 to 6 of Chapter III. The first section describes order relations and associated properties (like upper bounds, greatest elements, increasing functions, order isomorphisms). The second section studies well-ordered sets, and introduces the notion of transfinite induction. We show Zermelo's theorem (which is equivalent to the axiom of choice). Section 3 defines cardinals, addition, multiplication and order on cardinals (a cardinal is a representative of a class of equipotent sets; this class is not a set, and the axiom of choice is required). Section 4 defines natural integers as cardinals such that \( x \neq x + 1 \). It introduces induction on natural integers, so that a natural integer is any cardinal obtained by applying a “finite” number of times \( x \mapsto x + 1 \) to the empty set. More formally, if \( E \) is a set containing zero and stable by \( x \mapsto x + 1 \), it contains all natural integers. If \( E \) is any set with cardinal \( x \), the set \( E \cup \{E\} \) has cardinal \( x + 1 \). As a consequence, one can define a mapping \( n \mapsto E_n \) that associates to each natural number \( n \) a set \( E_n \) of cardinal \( n \) (by transfinite induction, one can do this for any cardinal \( n \)). This set \( E_n \) is called an ordinal in [7] and pseudo-ordinal here (For Bourbaki, an ordinal is a representative of well-ordered sets). It allows one to define finite cardinals without the use of the axiom of choice. There is no set containing all cardinals (thus no set containing all ordinals) but given a cardinal (or ordinal) \( a \), there is a set containing all cardinals (or ordinals) less than \( a \), and it is well-ordered. Ev-
Every finite ordinal is a natural integer; infinite ordinals possess strange properties (addition and multiplication are non-commutative) studied in the Exercises. Section 5 studies some properties of integers (for instance division, expansion to base \( b \)) and computes the number of elements of various sets (for instance the number of subsets of \( p \) elements of a set of \( n \) elements, the number of permutations, etc). Section 6 studies infinite sets. If there exists an infinite set, then there exists a set \( N \) containing all natural integers. An axiom is required in Bourbaki; in Coq, there is an infinite set, namely \( nat \), and it is canonically isomorphic to the set of natural integers. We use this isomorphism in section 5 (for instance, the factorial function and binomial coefficient are defined by induction on the Coq type \( nat \), then shown to satisfy the Bourbaki definitions). There are few infinite cardinals (i.e., for any cardinal \( x \) there is a cardinal \( y \) such that \( y > x \), for instance \( 2^x \)), but one could add an axiom saying that \( y > x \) implies \( y \geq 2^x \), so that one gets result like: the number of permutations of \( E \) is the number of mapping \( N \to E \), it is also the number of orderings on \( E \) (see Exercises).

Section 6 defines direct limits and inverse limits. It is not yet implemented. There are many exercises, only a few of them are solved.

The reader is invited to read the introduction of the first part. It explains some implementation details (for instance, what is a set? what formulation of the axiom of choice is used?).

1.3 Terminology

Chapter III is much less formal than Chapter II. Let’s for instance quote Definition 9 [2, p. 146]: “Two elements of a preordered set \( E \) are said comparable if the relation “\( x \leq y \)” or “\( y \leq x \)” is true. A set \( E \) is said to be totally ordered if is is ordered and if any two elements of \( E \) are comparable. The ordering in \( E \) is then said to be a total ordering and the corresponding order relation a total order relation.”

One has to understand this as follows. A preordered set is a pair \((E, G)\) which satisfies the preorder condition. The notation \( x \leq y \) stands for \((x, y) \in G\). An ordered set is a preordered set where additional conditions are required for \( G \). The ordering is \( G \), the corresponding order relation is “\((x, y) \in G\)”. By definition, \( E \) is uniquely determined by \( G \). Instead of saying that \( E \) is totally ordered, one can say: \( G \) is a total ordering if it is an ordering and for every \( x \) and \( y \) in the substrate of \( G \) one has “\((x, y) \in G \)” or “\((y, x) \in G \)”.” This non ambiguous, and will be our definition. The following sentence is ambiguous “The set \( R \) of real numbers is totally ordered”, since the order is not specified. Note that a sentence like “\((R, \leq) \) is totally ordered” is ambiguous since \( \leq \) can denote any ordering. One must say “The set \( R \) of real numbers is totally ordered by the usual order on real numbers.” We shall use the notation \( x \leq_R y \); an alternative would be \( x \equiv y \mod R \) as in [7].

Bourbaki says: “a well-ordered set is totally ordered”. This is a short-hand for: for every \((E, \Gamma)\), if \( \Gamma \) is a well-ordering on \( E \), then \( \Gamma \) is a total ordering on \( E \). It is impossible to say “for every equivalence relation \( R \) we have...” since relations cannot be quantified; there is only one theorem in E.II.6, the chapter on equivalence relations. It is of the form: a correspondence \( \Gamma \) between \( X \) and \( X \) is an equivalence if and only if... This might explain why Bourbaki defines an order as a correspondence, rather than a graph. As a consequence, there are few criteria (C59 to C63 define normal and transfinite induction).
1.4 Tactics

We give here the list of tactics that are defined in the files associated to this document.

This is now the tactic that exploits properties of order relations.

```coq
Ltac order_tac:=
  match goal with
  | H1: gle ?r ?x _ |- inc ?x (substrate ?r)
    => exact (inc_arg1_substrate H1)
  | H1: glt ?r ?x _ |- inc ?x (substrate ?r)
    => nin H1; order_tac
  | H1:gle ?r _ ?x |- inc ?x (substrate ?r)
    => exact (inc_arg2_substrate H1)
  | H1:glt ?r _ ?x |- inc ?x (substrate ?r)
    => nin H1; order_tac
    => wrr order_reflexivity
  | H: order ?r |- inc (J ?u ?u) ?r
    => change (related r u u); wrr order_reflexivity
    => wrr order_reflexivity
    => exact (order_antisymmetry H H1 H2)
    => app (order_antisymmetry H H1 H2)
    => app (order_transitivity H H1 H2)
    => app (order_transitivity H H1 H2)
    => change (related r u w); app (order_transitivity H H1 H2)
    => elim (not_le_gt H H1 H2)
    => destruct H1 as [H1 _]; elim (not_le_gt H H1 H2)
    => exact (lt_leq_trans H1 H2 H3)
    => exact (leq_lt_trans H1 H2 H3)
    => exact (lt_trans H1 H2 H3)
    => exact (lt_trans H1 H2 H3)
  | H1:inc _ (Zo _ _), H2: (inc _ (Zo _ _)) |- _
    => nin (Z_all H1); nin (Z_all H2); clear H1; clear H2; ee
end.
```

This tactic is useful when we want to show \(\{x \in A, P(x)\} = \{x \in B, Q(x)\}\). It splits the goal into two subgoals, with assumptions \(x \in A\) and \(P(x)\) or \(x \in B\) and \(Q(x)\). The second tactic is useful to show \(\{x \in A, P(x)\} \cap \{x \in B, Q(x)\} = \{x \in C, R(x)\}\). It splits the goal in two. In the first case, we must show \(x \in C\) and \(R(x)\) in a context where \(x \in A\), \(P(x)\), \(x \in B\) and \(Q(x)\). In the second case, we assume \(x \in C\) and \(R(x)\), and must show the other properties.

```
Ltac zztac:=
```

RR n° 7150
José Grimm

set_extens; Ztac; ee; match goal with H: inc _ (Zo _ _) |- _ => clear H end.

Ltac zztac2:= uf_interval; set_extens;
[ match goal with H: inc _ (intersection2 _ _) |- _ =>
  nin (intersection2_both H) end;
match goal with
  H1:(inc _ (Zo _ _)), H2 :(inc _ (Zo _ _)) |- _
  => nin (Z_all H1); nin (Z_all H2); clear H1; clear H2; ee end;Ztac
| Ztac; match goal with H: inc _ (Zo _ _) |- _ => clear H end;
app intersection2_inc; Ztac; uf glt; ee; try order_tac].

This unfolds all definitions of intervals.

Ltac uf_interval :=
  uf interval_cc; uf interval_oo; uf interval_co; uf interval_oc;
  uf interval_uu; uf interval_uo; uf interval_ou;
  uf interval_uc; uf interval_cu.

This tactic uses transitivity and antisymmetry of ≤_{Card}.

Ltac co_tac := match goal with
    => ap (cardinal_le_transitive Ha Hb)
    => ap (cardinal_lt_le_trans Ha Hb)
    => ap (cardinal_le_lt_trans Ha Hb)
    => nin Ha; co_tac
    => elim (not_card_le_lt Ha Hb)
    => solve [ rw (cardinal_antisymmetry1 Ha Hb); fprops ]
end.

The first tactic uses the property that Card(x) = x if x is a cardinal.

Ltac eq_aux:= match goal with
  H: is_cardinal ?a |- cardinal ?b = ?a => wr (cardinal_le4 H); aw
  | H: is_cardinal ?a |- ?a = cardinal ?b => wr (cardinal_le4 H); aw
  | H: is_cardinal ?a |- cardinal ?a = ?b => wr (cardinal_le4 H); aw
end.
Ltac eqtrans u: apply equipotent_transitive with u.
Ltac eqsym:= apply equipotent_symmetric.

1.5 Removed theorems

The lemmas and definition shown here existed in previous version, but have been withdrawn.

A correspondence \( \Gamma = (G, E, E) \), whose graph G is an order on E, is also called an order by Bourbaki (this definition is in fact never used).
Definition order_c r :=
is_correspondence r & source r = target r & source r = substrate (graph r)
& order (graph r).

Theorem order_cor_pr: forall f,
is_correspondence f ->
order_c f =
(source f = target f & source f = (domain (graph f)) &
compose_graph (graph f) (graph f) = graph f &
intersection2 (graph f) (opposite_order (graph f))
= diagonal (substrate (graph f))).

Given two sets A and B, two distinct elements α and β, if I is the set that contains α and β, there is a family \{(X_i)\}_{i \in I} such that such that A = X_α and B = X_β. This family is Lvariant. We shall denote it by X_{αβ}(A,B). We show here uniqueness of the family.

Lemma two_terms_bij1: forall a b x y f,
y <> x -> fgraph f -> domain f = doubleton x y -> V x f = a -> V y f = b ->
rangle f = doubleton a b -> f = Lvariant x y a b.

Here are some trivial lemmas.

Lemma source_pfs:forall y x,
source (partition_fun_of_set y x) = y.

Lemma target_pfs: forall y x,
target (partition_fun_of_set y x) = powerset x.

Lemma source_graph_of_function: forall x y,
source (graph_of_function x y) = set_of_sub_functions x y.

Lemma target_graph_of_function: forall x y,
target (graph_of_function x y) = (set_of_graphs x y).

Lemma sup_interval_co_0a: forall n, inc n Bnat ->
supremum Bnat_order (interval_co_0a (succ n)) = n.

1.5.1 Definition of a function by induction

We explain here the initial implementation of section 7.2, more precisely the case when a function f is defined by (IND0), i.e., \( f(0) = a \) and \( f(n + 1) = h(n, f(n)) \) for \( n \in \mathbb{N} \), or variants of this formulation.

In Version 1 we had the following two definitions (compare with induction_defined0_set and induction_defined1_set). They are of the form choose IND0 and choose IND1'. We have two theorems saying that these objects satisfy (IND0) and (IND1') respectively, and two others stating existence and uniqueness of (IND0), and existence of (IND1'). Together with these four theorems, we show a variant of integer_induction_stable and the Bourbaki variant of (IND0).

Definition induction_defined1 E h a:= choosef(fun f=>
is_function f & source f = Bnat & target f = E & W card_zero f = a &
forall n, inc n Bnat -> W (succ n) f = h n (W n f)).

Definition induction_defined2 E h a p:= choosef(fun f=>
is_function f & source f = Bnat & target f = E & W card_zero f = a &
forall n, cardinal_lt n p -> W (succ n) f = h n (W n f)).

Lemma integer_induction_stable: forall E g a,
inc a E -> is_function g -> source g = E -> target g = E ->
Lemma induction_with_var: forall E h a,
   is_function h -> source h = product Bnat E -> target h = E -> inc a E ->
   exists_unique (fun f=> is_function f & source f = Bnat & target f= E &
   W card_zero f = a
   & forall n, inc n Bnat -> W (succ n) f = W (J n (W n f)) h).

Lemma induction_with_var1: forall E h a,
   (forall n x, inc n Bnat -> inc x E -> inc (h n x) E) -> inc a E ->
   exists_unique (fun f=> is_function f & source f = Bnat & target f= E &
   W card_zero f = a
   & forall n, inc n Bnat -> W (succ n) f = h n (W n f)).

Lemma induction_with_var2: forall E h a p,
   (forall n x, inc n Bnat -> inc x E -> cardinal_lt n p -> inc (h n x) E)
   -> inc a E -> inc p Bnat ->
   exists f, is_function f & source f = Bnat & target f= E &
   W card_zero f = a
   & forall n, cardinal_lt n p -> W (succ n) f = h n (W n f).

Lemma induction_defined_pr2: forall E h a p,
   (forall n x, inc n Bnat -> inc x E -> cardinal_lt n p -> inc (h n x) E)
   -> inc a E -> inc p Bnat ->
   let f := induction_defined2 E h a p in is_function f &
   source f = Bnat & target f= E & W card_zero f = a
   & forall n, cardinal_lt n p -> W (succ n) f = h n (W n f).

Lemma induction_defined_pr1: forall E h a,
   (forall n x, inc n Bnat -> inc x E -> inc (h n x) E)
   -> inc a E ->
   let f := inductionDefined1 E h a in is_function f &
   source f = Bnat & target f= E & W card_zero f = a
   & forall n, inc n Bnat -> W (succ n) f = h n (W n f).

### 1.5.2 Intervals

We give here the original proof that the intersection of two intervals is an interval.

Let's say that an interval is of type B if it is bounded, of type L' if it is left unbounded, of type R' if it is right unbounded, of type U if it is \(-\infty, -\infty\). Let's say that an interval is of type L if it is of type L' or U, of type R if it is of type L' or U.

Let's write L' \cap L' = U as a short-hand for: the intersection of two intervals of type L' is an interval of type L', this is lemma `intersection_i3` and will be explained later. If we consider the reverse ordering, an interval remains an interval, but the lemmas shown here are more precise (they say for instance that the opposite of L' is R').

Lemma opposite_interval_cc: forall r a b,
   order r -> interval_cc r a b = interval_cc (opposite_order r) b a.
Lemma opposite_interval_oo: forall r a b,
   order r -> interval_oo r a b = interval_oo (opposite_order r) b a.
Lemma opposite_interval_oc: forall r a b,
   order r -> interval_oc r a b = interval_co (opposite_order r) b a.
Lemma opposite_interval_co: forall r a b,
   order r -> interval_co r a b = interval_oc (opposite_order r) b a.
Lemma opposite_bounded_interval: forall r x, order r ->
There are 9 types of intervals, thus 81 cases to consider. The case of intervals of type U is trivial, so that the number of cases is really 64. The new proof replaces bounded intervals by unbounded intervals, so that there are only 16 cases to consider. Let’s start with these ones.

Case L′ ∩ R′ = R′ ∩ L′ = B. Consider X = |←, x] ∩ ]y, →]. If the intersection is non-empty, there is a such that y ≤ a ≤ x, thus y ≤ x, and X = ]y, x[. Otherwise X = ]x, x[. Similarly, if we consider intervals that contain the end-point x or y, the intersection is empty, or an interval that contains the end-point x or y.

Case L′ ∩ L′ = L′. Consider X(b) = |←, b] and Y(b) = |←, b]. Let d = inf(b, c). We have X(d) ⊆ X(b) ∩ X(c) ⊆ Y(d). If d is in the intersection, then the intersection is Y(d), otherwise it is X(d). Replacing one of X(b) or X(c) by Y(b) or Y(c) is similar. Note: the intersection of two closed intervals is empty or closed, and the intersection of two open intervals is open, only when the order is total.

Using the reverse order, it follows R′ ∩ R′ = R′, and this covers all unbounded intervals. All remaining cases are similar. We must consider what happens on the left, and what happens on the right. The big part of the proof (300 lines) consists in showing that the intersection of two bounded intervals is a bounded interval. This does not follow directly from our new theorem, but is easy (for instance, if X is a subinterval of [a, b], of the form ]a, b[, it is ]a, x[).
Lemma intersection_interval6: forall r x y, lattice r -> is_semi_open_interval r x -> is_semi_open_interval r y -> is_bounded_interval r (intersection2 x y).

Lemma intersection_interval7: forall r a b a’ b’, lattice r -> inc a (substrate r) -> inc a’ (substrate r) -> inc b (substrate r) -> inc b’ (substrate r) -> is_bounded_interval r (intersection2(interval_cc r a b)(interval_oo r a’ b’)). (* 30 *)

Lemma intersection_interval8: forall r a b a’ b’, lattice r -> inc a (substrate r) -> inc a’ (substrate r) -> inc b (substrate r) -> inc b’ (substrate r) -> is_bounded_interval r (intersection2(interval_cc r a b)(interval_oc r a’ b’)). (* 18 *)

Lemma intersection_interval9: forall r a b a’ b’, lattice r -> inc a (substrate r) -> inc a’ (substrate r) -> inc b (substrate r) -> inc b’ (substrate r) -> is_bounded_interval r (intersection2(interval_oo r a b)(interval_oc r a’ b’)). (* 34 *)

Lemma intersection_interval10: forall r a b a’ b’, lattice r -> inc a (substrate r) -> inc a’ (substrate r) -> inc b (substrate r) -> inc b’ (substrate r) -> is_bounded_interval r (intersection2(interval_oo r a b)(interval_co r a’ b’)).

Lemma intersection_interval11: forall r a b a’ b’, lattice r -> inc a (substrate r) -> inc a’ (substrate r) -> inc b (substrate r) -> inc b’ (substrate r) -> is_bounded_interval r (intersection2(interval_co r a b)(interval_cc r a’ b’)).

Lemma intersection_interval12: forall r x y, lattice r -> is_bounded_interval r x -> is_bounded_interval r y -> is_bounded_interval r (intersection2 x y).

We consider now the case of unbounded intervals.

Lemma intersection_interval13: forall r x, is_interval r x -> intersection2 x (interval_uu r) = x.

Lemma intersection_interval14: forall r x y, lattice r -> is_left_unbounded_interval r x -> is_left_unbounded_interval r y -> is_left_unbounded_interval r (intersection2 x y). (* 18 *)

Lemma intersection_interval15: forall r x y, lattice r -> is_right_unbounded_interval r x -> is_right_unbounded_interval r y -> is_right_unbounded_interval r (intersection2 x y).

Lemma intersection_interval16: forall r x y, lattice r -> is_left_unbounded_interval r x -> is_right_unbounded_interval r y -> is_bounded_interval r (intersection2 x y). (* 19 *)

Lemma intersection_interval17: forall r x y, lattice r -> is_unbounded_interval r x -> is_unbounded_interval r y -> is_interval r (intersection2 x y).

Lemma intersection_interval18: forall r x y, lattice r -> is_left_unbounded_interval r x -> is_bounded_interval r y -> is_bounded_interval r (intersection2 x y). (* 97 *)

Lemma intersection_interval19: forall r x y, lattice r -> is_right_unbounded_interval r x -> is_bounded_interval r y -> is_bounded_interval r (intersection2 x y).

Lemma intersection_interval20: forall r x y, lattice r -> is_unbounded_interval r x -> is_bounded_interval r y -> is_bounded_interval r (intersection2 x y).
The result is now obvious.

Theorem intersection_interval: \(\forall r \ x \ y,\)
\(\text{lattice } r \rightarrow \text{is_interval } r \ x \rightarrow \text{is_interval } r \ y \rightarrow \)
\(\text{is_interval } r \ (\text{intersection2 } x \ y).\)
Chapter 2

Order relations. Ordered sets

2.1 Definition of an order relation

In the last chapter of the first part of this document, we studied equivalence relations, that were reflexive, symmetric and transitive. If we replace symmetric by antisymmetric, we get an order relation. Remember that transitive means that if \( x \sim y \) and \( y \sim z \) then \( x \sim z \), and symmetric means that if \( x \sim y \) then \( y \sim x \). If a relation is symmetric and transitive, then \( x \sim y \) implies \( x \sim x \) and \( y \sim y \). The support of a relation is of the set of all \( x \) and \( y \) that are related by the relation. A relation is reflexive on a set \( E \) if \( x \in E \) is equivalent to \( x \sim x \).

We say that a relation (denoted here \( \prec \)) is antisymmetric if \( x \prec y \) and \( y \prec x \) imply \( x = y \). We say that it is reflexive if \( x \prec y \) implies \( x \prec x \) and \( y \prec y \) (this means that the relation is reflexive on the support). An order relation on \( E \) is an order relation whose support is \( E \) (or equivalently, that is reflexive on \( E \)). Bourbaki defines preorder relations later; giving the definition right now reduces a little bit the code. A preorder relation is reflexive and transitivie. The opposite relation of \( \prec \), denoted by \( \succ \), is such that \( x \prec y \) and \( y \succ x \) are equivalent.

```coq
Definition antisymmetric_r (r:EEP) :=
  forall x y, r x y -> r y x -> x = y.
Definition is_antisymmetric (r:Set) :=
  is_graph r & forall x y, related r x y -> related r y x -> x = y.
Definition reflexive_rr (r:EEP) :=
  forall x y, r x y -> (r x x & r y y).
Definition order_r(r:EEP) :=
  transitive_r r & antisymmetric_r r & reflexive_rr r.
Definition order_re (r:EEP) x :=
  order_r r & reflexive_r r x.
Definition preorder_r (r:EEP) :=
  transitive_r r & reflexive_rr r.
Definition opposite_relation (r:EEP) :=
  fun x y => r y x.

Equality and inclusion are order relations. The opposite of an order relation is an order relation.

Lemma equality_is_order: order_r(fun x y => x = y).
Lemma sub_is_order: order_r sub.
Lemma opposite_is_preorder_r: forall r, preorder_r r -> preorder_r (opposite_relation r).
```

RR n° 7150
Lemma opposite_is_order_r: forall r, 
order_r r -> order_r (opposite_relation r).

An order on a set E is a graph $G$ such that the relation $(x, y) \in G$ is an order relation between $x$ and $y$ with substrate $E$. A preorder is similarly defined. The opposite order relation corresponds to the inverse graph, which is thus called the opposite order.

Definition order (r: Set) :=
is_reflexive r & is_transitive r & is_antisymmetric r.
Definition preorder (r: Set) :=
is_graph r & is_reflexive r & is_transitive r.
Definition opposite_order := inverse_graph.
Lemma order_is_graph: forall r, order r -> is_graph r.

If we have an order relation on $E$, we can take its graph, and this gives an order (this is the same construction as for equivalence relations).

Lemma order_has_graph0: forall r x, 
order_re r x -> is_graph_of (graph_on r x) r.
Lemma order_has_graph: forall r x, 
order_re r x -> exists g, is_graph_of g r.
Lemma order_if_has_graph: forall r g, 
is_graph g -> is_graph_of g r ->
order_r r -> order_re r (domain g).
Lemma order_if_has_graph2: forall r g, 
is_graph g -> is_graph_of g r ->
order_r r -> order g.
Lemma order_has_graph2: forall r x, 
order_re r x -> exists g, 
g = graph_on r x &
order g & (forall u v, r u v = related g u v).

The next two lemmas are more often used. They say that an order can be obtained from an order relation by taking its graph on a set.

Lemma preorder_from_rel: forall r x, 
preorder_r r -> preorder (graph_on r x).
Lemma order_from_rel: forall r x, 
order_r r -> order (graph_on r x).

The traditional notation for an order relation is $x \leq y$, or $y \geq x$, we shall use $gle$ and $gge$ in our code; if the elements are distinct, we shall use the notations $x < y$ and $y < x$. This last relation is not reflexive. It satisfies some transitivity properties. We give here some simple properties of orders.

Definition gle (r x y:Set) := related r x y.
Definition gge (r x y:Set) := related r y x.
Definition glt (r x y:Set) := gle r x y & x <> y.
Definition ggt (r x y:Set) := gge r x y & x <> y.
Lemma order_reflexivity_pr: forall r x u v, 
order_re r x -> inc u x & inc v x.

\(^1\)This condition has been removed; it is a consequence of the other properties
Lemma order_symmetricity_pr: forall r x u v,
    order_re r x -> (r u v & r v u) = (inc u x & inc v x & u = v).
Lemma order_reflexivity: forall r a,
    order r -> inc a (substrate r) = related r a a.
Lemma order_antisymmetry: forall r a b,
    order r -> related r a b -> related r b a -> a = b.
Lemma order_transitivity: forall r a b c,
    order r -> related r a b -> related r b c -> related r a c.
Lemma lt_leq_trans : forall r x y z,
    order r -> glt r x y -> gle r y z -> glt r x z.
Lemma leq_lt_trans : forall r x y z,
    order r -> gle r x y -> glt r y z -> glt r x z.
Lemma lt_lt_trans: forall r a b c, order r ->
    glt r a b -> glt r b c -> glt r a c.
Lemma not_le_gt: forall r x y, order r -> gle r x y -> glt r y x -> False.

Lemma order_is_order: forall r,
    order r -> order_r (related r).
Lemma order_is_graph: forall r, order r -> is_graph r.
Lemma substrate_domain_order: forall f,
    order f -> substrate f = domain f.
Lemma substrate_opposite_order: forall r,
    order r -> substrate(opposite_order r) = substrate r.
Lemma opposite_is_order: forall r,
    order r -> order (opposite_order r).

Remember that the diagonal of E is the graph of the equality relation on E. We know that
it is an equivalence. It is also an order.

Lemma diagonal_order : forall x, order(diagonal x).

¶ Given a relation \( \prec \) and a set X, we can consider the relation “\( x \in X \) and \( y \in X \) and \( x \prec y \)”. If
we assume \( x \prec x \) for all \( x \in X \), this gives an order relation on X. This is for instance the case of
inclusion, since \( x \subset x \) is always true. The set X can be \( \mathcal{P}(A) \), or any other set.

Definition induced_order_r (r:EEP) x :=
    fun u v => inc u x & inc v x & r u v.
Definition inclusion_order (a:Set) :=
    graph_on (fun u v => sub u a & sub v a & sub u v) (powerset a).
Definition inclusion_suborder (b:Set) :=
    graph_on (fun u v => inc u b & inc v b & sub u v) b.
Lemma induced_order_order_r: forall r x,
    order_r r -> (forall u, inc u x -> r u u) -> order_re (induced_order_r r x).
Lemma order_sub_on_set: forall a,
    order_re (fun u v => sub u a & sub v a & sub u v) (powerset a).
Lemma order_sub_on_subset: forall a,
    order_re (fun u v => inc u a & inc v a & sub u v) a.
Lemma inclusion_is_order: forall a,
    order (inclusion_order a).
Lemma inclusion_order_rw: forall a u v ,
    related (inclusion_order a) u v = (sub u a & sub v a & sub u v).
Lemma substrate_inclusion_order: forall a,
    substrate (inclusion_order a) = powerset a.
Lemma subinclusion_is_order: forall a,
order (inclusion_suborder a).
Lemma subinclusion_order_rw: forall a u v ,
related (inclusion_suborder a) u v = (inc u a & inc v a & sub u v).
Lemma substrate_subinclusion_order: forall a, 
substrate (inclusion_suborder a) = a.

¶ Second example. We consider the set \( \Phi(E,F) \) of functions from a subset of \( E \) to \( F \) and the extension relation. Remember that \( x \in \Phi(E,F) \) if and only if there is a function \( f \) whose source is a subset of \( E \), its target is \( F \) and its value as correspondence is \( x \). We say that \( g \) extends \( f \) if \( f \) and \( g \) are functions, the graph of \( f \) is a part of the graph of \( g \), the target of \( f \) is a part of the target of \( g \). If \( f \) and \( g \) are associated to two elements of \( \Phi(E,F) \), they have the same target, namely \( F \).

We can now define \( \text{extends}_\text{in} \) on the set \( \Phi(E,F) \), and simplify the definition: \( g \) extends \( f \) if and only if \( \text{pr}_1 f \subset \text{pr}_1 g \). This is an order; the only non trivial point is antisymmetry. If \( \text{pr}_1 x = \text{pr}_1 y \), we have \( x = y \) since the source of a function depends only on its graph \( \text{pr}_1 x \).

We then define \( \text{extension}_\text{order} \). This is an order on \( \Phi(E,F) \). Note that Bourbaki considers “\( g \) extends \( f \)” as a relation between \( f \) and \( g \). In our definition \( g \) comes before \( f \).

Definition \( \text{extends}_\text{in} \) x y := 
\( \text{fun } g \ f \Rightarrow \text{inc } f \left( \text{set_of_sub_functions } x \ y \right) \ & \ \text{inc } g \left( \text{set_of_sub_functions } x \ y \right) \) & 
\( \text{extends } \left( \text{inv_corr_value } g \right) \left( \text{inv_corr_value } f \right) \).
Definition \( \text{extension}_\text{order} \) x y := 
\( \text{graph_on } \left( \text{extends}_\text{in} \ x \ y \right) \left( \text{set_of_sub_functions } x \ y \right) \).

Lemma \( \text{extends}_\text{in}_\text{pr} \) : forall x y g f,
\( \text{extends}_\text{in} \ x \ y \ g \ f = \)
\( \left( \text{inc } f \left( \text{set_of_sub_functions } x \ y \right) \ & \ \text{inc } g \left( \text{set_of_sub_functions } x \ y \right) \ & \ 
\text{sub } \left( \text{P } f \right) \left( \text{P } g \right) \right) \).

Lemma \( \text{extends}_\text{refl} \) : forall f,
\( \text{is_function } f \Rightarrow \text{extends } f \ f \).

Lemma \( \text{extends}_\text{antisymmetric} \) : forall x y f g,
\( \text{inc } f \left( \text{set_of_sub_functions } x \ y \right) \Rightarrow \)
\( \text{inc } g \left( \text{set_of_sub_functions } x \ y \right) \Rightarrow \)
\( \text{P } f \Rightarrow \text{P } g \Rightarrow f = g \).

Lemma \( \text{extends}_\text{order} \) : forall x y,
\( \text{order}_\text{re} \left( \text{extends}_\text{in} \ x \ y \right) \left( \text{set_of_sub_functions } x \ y \right) \).

Lemma \( \text{extension}_\text{is_order} \) : forall x y,
\( \text{order } \left( \text{extension}_\text{order} \ x \ y \right) \).

Lemma \( \text{extension}_\text{order}_\text{rw} \) : forall x y u v ,
\( \text{related } \left( \text{extension}_\text{order} \ x \ y \right) \ u \ v = \left( \text{extends}_\text{in} \ x \ y \ u \ v \right) \).

Lemma \( \text{substrate}_\text{extension}_\text{order} \) : forall x y ,
\( \text{substrate } \left( \text{extension}_\text{order} \ x \ y \right) = \left( \text{set_of_sub_functions } x \ y \right) \).

¶ Third example. Let \( E \) be a set, and \( W \) the subset of \( \mathcal{P}(\mathcal{P}(E)) \) formed of all partitions of \( E \).
Recall that a partition \( \wp \) of \( E \) is a set of sets whose union is \( E \), so that \( \wp \subset \mathcal{P}(E) \). Additional conditions are: the empty set is not in \( \wp \), the elements of \( \wp \) are mutually disjoint. We say that \( \wp \) is \( \text{coarser} \) (or sometimes \( \text{not finer} \)) than \( \wp' \) if for every \( Y \in \wp' \) there exists \( X \in \wp \) such that \( Y \subset X \). We shall show that it is an order. But we start with another property: assume that \( X \) is a partition of \( E \); if \( x \in X \) then \( x \) is a subset of \( E \) hence \( x \in \mathcal{P}(E) \). We can consider the canonical injection from \( X \) to \( \mathcal{P}(E) \). The graph of this function is a family of sets; this family is a partition of \( E \).

Definition \( \text{set_of_partition_set} \) x := 
\( \text{Zo} \left( \text{powerset} \left( \text{powerset } x \right) \right) \left( \text{fun } z \Rightarrow \text{partition } z \ x \right) \).
Definition partition_fun_of_set y x :=
    canonical_injection y (powerset x).

Lemma partition_set_in_double_powerset: forall y x,
    partition y x -> inc y (powerset (powerset x)).
Lemma set_of_partition_pr: forall x y,
    inc y (set_of_partition_set x) = partition y x.
Lemma function_pfs: forall y x,
    partition y x -> is_function (partition_fun_of_set y x).
Lemma W_pfs: forall y x a,
    partition y x -> inc a y -> W a (partition_fun_of_set y x) = a.
Lemma partition_pfs: forall y x,
    partition y x -> partition_fam (graph (partition_fun_of_set y x)) x.

We now define coarser and show that it is an order on W.

Definition coarser x := graph_on coarser_c (set_of_partition_set x).

Lemma coarser_reflexive : forall y, coarser_c y y.
Lemma coarser_antisymmetricc : forall y y' x,
    partition y x -> partition y' x ->
    coarser_c y y' -> coarser_c y' y -> sub y y'.
Lemma coarser_antisymmetric : forall y y' x,
    partition y x -> partition y' x ->
    coarser_c y y' -> coarser_c y' y -> y = y'.
Lemma related_coarser: forall x y y',
    related (coarser x) y y' =
    (partition y x & partition y' x & coarser_c y y').
Lemma related_coarser_bis: forall x y y',
    related (coarser x) y y' =
    (partition y x & partition y' x &
     forall a, inc a y' -> exists b, inc b y & sub a b).
Lemma substrate_coarser : forall x,
    substrate (coarser x) = set_of_partition_set x.
Lemma coarser_order : forall x, order (coarser x).
Lemma smallest_partition_is_smallest: forall x y,
    nonempty x ->
    partition y x -> related (coarser x) (smallest_partition x) y.
Lemma largest_partition_is_largest: forall x y,
    partition y x -> related (coarser x) y (largest_partition x).

Let $\varnothing$ be a partition; consider the set formed of all $A \times A$ with $A \in \varnothing$; let $\tilde{\varnothing}$ be the union of all these sets. We pretend that this set is the graph of the equivalence associated to the partition. The relation "$\varnothing$ coarser than $\varnothing'$" is equivalent to $\tilde{\varnothing} \supset \tilde{\varnothing}'$. Bourbaki says that this shows that coarser is an order. The nontrivial point is antisymmetry: we must show that $\tilde{\varnothing} = \tilde{\varnothing}'$ implies $\varnothing = \varnothing'$. This is a consequence of the fact that the sets $A \times A$ are mutually disjoint. If $a$ and $b$ are in the same element of $\varnothing$ and in $A$ and $B$ for $\varnothing'$, the pair $(a, b)$ is in $\tilde{\varnothing}$, hence in $\tilde{\varnothing}'$, hence in $A \times A$ and $B \times B$, so that the intersection of $A$ and $B$ is not empty, and $A = B$. 

Definition partition_relation_set_aux y x :=
    Zo (powerset (coarse x)) (fun z => exists a, inc a y & z = coarse a).
Definition partition_relation_set y x :=
    partition_relation (partition_fun_of_set y x) x.
Lemma prs_is_equivalence: forall y x,
partition y x -> is_equivalence (partition_relation_set y x).

Lemma partition_relation_set_pr1: forall y x a,
partition y x ->
inc a y -> inc (coarse a) (partition_relation_set_aux y x).

Lemma partition_relation_set_pr: forall y x,
partition y x ->
partition_relation_set y x =
union (partition_relation_set_aux y x). (* 16 *)

Lemma sub_partition_relation_set_coarse: forall y x,
partition y x -> sub (partition_relation_set y x) (coarse x).

Lemma nondisjoint :forall a b c, inc a b -> inc a c -> disjoint b c -> False.

Lemma partition_relation_set_order: forall x y y',
partition_set y x -> partition_set y' x ->
sub (partition_relation_set y' x)(partition_relation_set y x) =
related (coarser x) y y'. (* 20 *)

Lemma partition_relation_set_order_anti: forall x y y',
partition y x -> partition y' x ->
(partition_relation_set y' x = partition_relation_set y x) ->
sub y y'. (* 34 *)

Lemma partition_relation_set_order_antisymmetric: forall x y y',
partition y x -> partition y' x ->
(partition_relation_set y' x = partition_relation_set y x) ->
y = y'.

Let G be a graph, Δ be the diagonal of the substrate of G. If Δ ⊂ G and G ◦ G ⊂ G then
G ◦ G = G. The two assumptions say that G is reflexive and transitive, this a preorder. Anti-
symmetry is G ∩ G = Δ, since Δ is symmetric (i.e., it is its inverse), reflexivity is also Δ ⊂ G⁻¹,
so that G is an order if and only if G ◦ G = G, G ∩ G⁻¹ = Δ (we know that G is an equivalence
if and only G ◦ G = G and G ∩ G⁻¹ = Δ). Proposition 1 of Bourbaki [2, p. 132] considers the case
of a correspondence (moved to the list of removed theorems).

Lemma preorder_prop1: forall g,
is_graph g ->
sub (diagonal (substrate g)) g -> sub (compose_graph g g) g ->
compose_graph g g = g.

Theorem order_pr: forall r,
order r =
(compose_graph r r = r &
intersection2 r (opposite_order r) = diagonal (substrate r)). (* 28 *)

Theorem order_cor_pr: forall f,
is_correspondence f ->
order_c f =
(source f = target f & source f = (domain (graph f)) &
compose_graph (graph f) (graph f) = graph f &
intersection2 (graph f) (opposite_order (graph f)) = diagonal (substrate (graph f))).

2.2 Preorder relations

Consider the relation “R is coarser than R’” in the set of all coverings of E. This is a pre-
order relation, since it is reflexive and transitive; it is not antisymmetric, for if R is a covering,
R' = R ∪ {X} with X ⊂ E, then R' is a covering which is coarser then R. Now, R is coarser than
If there is a $Y \in R$ such that $X \subset Y$. It can happen that $X \not\in R$; in such a case, $R$ is coarser than $R'$, $R'$ is coarser than $R$, but $R \neq R'$. In the case of a partition, $X \in R'$, $Y \in R'$ and $X \subset Y$ implies $X = Y$.

Here is the definition and the basic properties.

**Lemma preorder_is_preorder**: forall $r$, preorder $r$ -> preorder $r$ (related $r$).

**Lemma opposite_is_preorder1**: forall $r$, preorder $r$ -> preorder (opposite_order $r$).

The relation "$x \prec y$ and $y \prec x$" is an equivalence if $\prec$ is a preorder. Denote it by $\sim$. Then $x \prec y$ is compatible with $x \sim x'$ and $y \sim y'$. This means that if these three relations hold, then we have also $x' \prec y'$. If $\prec$ has a graph $G$, then $\sim$ has a graph, which is $G \cap G^{-1}$. If $G$ is a graph, it is a preorder if and only if $\Delta \subset G$ and $G \circ G \subset G$. We know that it implies $G \circ G = G$.

**Lemma equivalence_preorder**: forall $r$, preorder $r$ -> equivalence $r$ (fun $x$ $y$ => $r$ $x$ $y$ & $r$ $y$ $x$).

**Lemma compatible_equivalence_preorder**: forall $r$, let $s := (\text{fun } x \ y \Rightarrow r \ x \ y \ & \ r \ y \ x)$ in preorder $r$ -> preorder $r'$ (related $r$).

**Definition equivalence_associated_o r**: intersection2 $r$ (opposite_order $r$).

**Lemma equivalence_preorder1**: forall $r$, preorder $r$ -> is_equivalence (equivalence_associated_o $r$).

**Lemma substrate_equivalence_associated_o**: forall $r$, preorder $r$ -> substrate (equivalence_associated_o $r$) = substrate $r$.

**Lemma compatible_equivalence_preorder1**: forall $r$, preorder $r$ -> related (equivalence_associated_o $r$) $x$ $u$ -> related (equivalence_associated_o $r$) $y$ $v$ -> related $r$ $u$ $v$.

**Lemma preorder_prop**: forall $g$, is_graph $g$ -> preorder $g$ = (sub (diagonal (substrate $g$)) $g$ & sub (compose_graph $g$ $g$) $g$).

**Lemma preorder_prop2**: forall $g$, preorder $g$ -> compose_graph $g$ $g$ = $g$.

**Lemma preorder_reflexivity**: forall $r$ $a$, preorder $r$ -> inc $a$ (substrate $r$) = related $r$ $a$ $a$.

Let $\prec$ be a preorder on a set $E$, and $\sim$ the equivalence associated to it. Assume that $R$ is the graph of $\prec$, and let $\pi$ be the canonical projection $E/\sim$. Given two objects of the form $u = \pi(x)$ and $v = \pi(y)$ in the quotient, we can compare $u$ and $v$ via $x \prec y$, this is independent of the representatives $x$ and $y$. This relation has a graph, namely $S \circ G \circ S^{-1}$, where $S$ is the graph of $\pi$. This set is also $(\pi \times \pi)(G)$, where $\pi \times \pi$ maps $E \times E$ into $(E/\sim) \times (E/\sim)$. This relation is an order on the quotient; it is called the order relation $\text{associated}$ with $\prec$.

**Definition order_associated (r:Set)** :=
let $s := (\text{graph(canon_proj (equivalence_associated_o r))) in
compose_graph (compose_graph s r) (opposite_order s).

Lemma is_graph_order_associated: forall r,
  is_graph (order_associated r).
Lemma related_compose3: forall s r u v,
  related (compose_graph (compose_graph s r) (opposite_order s)) u v =
  exists x, exists y, related s x u & related s y v & related r x y.
Lemma related_graph_order_associated1: forall r u v,
  preorder r->
  related (order_associated r) u v =
  ( inc u (quotient (equivalence_associated_o r)) &
  inc v (quotient (equivalence_associated_o r)) &
  exists x, exists y, inc x u & inc y v & related r x y). (* 21 *)
Lemma related_graph_order_associated2: forall r u v,
  preorder r->
  related (order_associated r) u v =
  ( inc u (quotient (equivalence_associated_o r)) &
  inc v (quotient (equivalence_associated_o r)) &
  forall x y, inc x u -> inc y v -> related r x y).
Lemma substrate_order_associated: forall r,
  preorder r-> substrate (order_associated r) =
  (quotient (equivalence_associated_o r)). (* 15 *)
Lemma order_order_associated: forall r,
  preorder r-> order (order_associated r). (* 27 *)
Lemma graph_order_associated: forall r,
  preorder r ->
  order_associated r = image_by_fun (ext_to_prod(canon_proj (equivalence_associated_o r)) (canon_proj (equivalence_associated_o r))) r. (* 35 *)

2.3 Notation and terminology

For simplicity, we shall write \( x \leq y \) instead of \( x < y \), and \( x < y \) for “\( x \leq y \) and \( x \neq y \)”. In Coq, we do not want to overwrite the standard notations for comparison for natural numbers. For this reason, we shall use \( \text{gle} \), \( \text{gge} \), \( \text{ggt} \) and \( \text{glt} \). These are functions with three arguments: an order and two elements to be compared.

(* Definitions moved to section 1.1
Definition gle (r x y:Set) := related r x y.
Definition gge (r x y:Set) := related r y x.
Definition glt (r x y:Set) := gle r x y & x <> y.
Definition ggt (r x y:Set) := gge r x y & x <> y. *)

For Bourbaki an order on \( E \) satisfies

\((\text{RO}_i)\) The relation “\( x \leq y \) and \( y \leq z \)” implies \( x \leq z \).
\((\text{RO}_ii)\) The relation “\( x \leq y \) and \( y \leq x \)” implies \( x = y \).
\((\text{RO}_iii)\) The relation \( x \leq y \) implies “\( x \leq x \) and \( y \leq y \)”.
\((\text{RO}_iv)\) The relation \( x \leq x \) is equivalent to \( x \in E \).

Note the absence of quantifiers; in Bourbaki, if \( x \) is a free variable, \( \forall x \).1 is equivalent to \( (\forall x)(P1.x1) \). Hence the definition is correct if \( x \), \( y \) and \( z \) are three distinct letters that do not appear in \( E \) or \( \leq \). The first part of C58 is: let \( \leq \) be an order relation and let \( x \), \( y \) be two distinct
letters; the relation $x \leq y$ is equivalent to “$x < y$ or $x = y$”. Here, Bourbaki explicitly says that $x$ and $y$ are distinct. The statement is true only if $x = x$ implies $x \leq x$, for instance if $\leq$ is an order on $E$ and $x \in E$.

Definition order_axioms (r s:Set) :=
  (forall x y z, gle r x y -> gle r y z -> gle r x z) &
  (forall x y, gle r x y -> gle r y x -> x = y) &
  (forall x y, gle r x y -> (inc x s & inc y s)) &
  (forall x, gle r x x = inc x s) &
  is_graph r.

Lemma axioms_of_order: forall r,
  order r = (order_axioms r (substrate r)).

Lemma lt_leq_trans : forall r x y z,
  order r -> glt r x y -> gle r y z -> glt r x z.

Lemma leq_lt_trans : forall r x y z,
  order r -> gle r x y -> glt r y z -> glt r x z.

Lemma lt_lt_trans: forall r a b c, order r ->
  glt r a b -> glt r b c -> glt r a c.

Lemma le_pr: forall r x y,
  inc x (substrate r) -> order r -> gle r x y = (glt r x y / x = y).

We say that $f$ is a morphism or isomorphism for two orders denoted $\leq_E$ or $\leq_F$ on $E$ and $F$ if $f$ is a function from $E$ to $F$ compatible with the orders (this means the obvious: if $x \leq_E y$ then $f(x) \leq_F f(y)$ and conversely). A morphism is required to be injective, and an isomorphism is required to be bijective. Properties of morphisms will be studied later. A morphism is an isomorphism on its range.

Definition order_isomorphism f r r':=
  (order r) & (order r') &
  (bijective f) & (substrate r = source f) & (substrate r' = target f) &
  (forall x y, inc x (source f) -> inc y (source f) ->
    gle r x y = gle r' (W x f) (W y f)).

Definition order_morphism f r r':=
  (order r) & (order r') &
  (injective f) & (substrate r = source f) & (substrate r' = target f) &
  (forall x y, inc x (source f) -> inc y (source f) ->
    gle r x y = gle r' (W x f) (W y f)).

2.4 Ordered subsets. Product of ordered sets

Let $G$ be a graph, $A$ a set. Define $G_A = G \cap (A \times A)$. This is a graph, whose substrate is a subset of $A$. If $G$ is reflexive, with substrate $E$ and $A \subset E$, then the substrate of $G_A$ is $A$. As a consequence if $G$ is an order (or preorder) on $E$, then $G_A$ is an order (or preorder) on $A$. It is called the order induced by $G$. By abuse of notations, if the order relation associated to $G$ is denoted $x \leq y$ then the order relation associated to $G_A$ also denoted $x \leq_A y$ instead of $x \leq_A y$.

The first three lemmas here say that $x \leq_A y$ implies $x \leq y$, and $x \leq_A y$ implies $x < y$; moreover if $x \in A$ and $y \in A$, then $x \leq_A y$ is equivalent to $x \leq y$.

Definition induced_order (r a:Set):=
  intersection2 r (coarse a).
Lemma related_induced_order: forall r a x y, 
\[ \text{inc} \ x \ a \ \rightarrow \ \text{inc} \ y \ a \ \rightarrow \ \text{gle} \ (\text{induced_order} \ r \ a) \ x \ y = \text{gle} \ r \ x \ y. \]

Lemma related_induced_order1: forall r a x y, 
\[ \text{gle} \ (\text{induced_order} \ r \ a) \ x \ y \ \rightarrow \ \text{gle} \ r \ x \ y. \]

Lemma related_induced_order2: forall r a x y, 
\[ \text{glt} \ (\text{induced_order} \ r \ a) \ x \ y \ \rightarrow \ \text{glt} \ r \ x \ y. \]

Lemma relation_induced_order:forall r a, 
\[ \text{is_graph} \ r \ \rightarrow \ \text{is_graph} \ (\text{induced_order} \ r \ a). \]

Lemma substrate_induced_order1 :forall r a, 
\[ \text{is_reflexive} \ r \ \rightarrow \ \text{sub} \ a \ (\text{substrate} \ r) \ \rightarrow \ \text{substrate} \ (\text{induced_order} \ r \ a) = a. \]

Lemma substrate_induced_order :forall r a, 
\[ \text{order} \ r \ \rightarrow \ \text{sub} \ a \ (\text{substrate} \ r) \ \rightarrow \ \text{substrate} \ (\text{induced_order} \ r \ a) = a. \]

Lemma reflexive_induced_order: forall r a, 
\[ \text{is_reflexive} \ r \ \rightarrow \ \text{sub} \ a \ (\text{substrate} \ r) \ \rightarrow \ \text{is_reflexive} \ (\text{induced_order} \ r \ a). \]

Lemma transitive_induced_order: forall r a, 
\[ \text{is_transitive} \ r \ \rightarrow \ \text{is_transitive} \ (\text{induced_order} \ r \ a). \]

Lemma preorder_induced_order: forall r a, 
\[ \text{preorder} \ r \ \rightarrow \ \text{preorder} \ (\text{induced_order} \ r \ a). \]

Lemma order_induced_order: forall r a, 
\[ \text{order} \ r \ \rightarrow \ \text{order} \ (\text{induced_order} \ r \ a). \]

Lemma order_substrate: forall r, 
\[ \text{order} \ r \ \rightarrow \ (\text{OK if } r \text{ is graph}) \text{ induced_order} \ r \ (\text{substrate} \ r) = r. \]

Lemma opposite_induced: forall r x, order r -> 
\[ \text{induced_order} \ (\text{opposite_order} \ r) x = \text{opposite_order} \ (\text{induced_order} \ r x). \]

Let \( \Phi(E, F) \) be the set of all mappings of subsets of \( E \) into \( F \). Recall that the set of triples \( \Gamma = (G, A, B) \) is termed set_of_sub_functions. We first show that \( \Gamma \rightarrow G \) is a function from \( \Phi(E, F) \) to the set of functional graphs included in \( E \times F \). This function is in fact an isomorphism of ordered sets, where the first set is endowed with the relation “\( g \) extends \( f \)” between \( f \) and \( g \) (this is the opposite order of extension_order) and the second set with the inclusion order.

Definition set_of_graphs(x y :Set):= 
\[ (\text{Zo}(\text{powerset} \ (\text{product} \ x \ y)) \ (\text{fun} \ z \ \rightarrow \ \text{functional_graph} \ z)). \]

Definition graph_of_function (x y:Set):= 
\[ \text{BL} \ (\text{fun} \ g \ \rightarrow \ (P \ g)) \ (\text{set_of_sub_functions} \ x \ y) \ (\text{set_of_graphs} \ x \ y). \]

Lemma sub_graph_of_function: forall x y z, 
\[ \text{inc} \ z \ (\text{set_of_sub_functions} \ x \ y) \ \rightarrow \ \text{sub} \ (P \ z) \ (\text{product} \ x \ y). \]

Lemma set_of_graphs_pr: forall x y z, 
\[ \text{inc} \ z \ (\text{set_of_sub_functions} \ x \ y) \ \rightarrow \ \text{inc} \ (P \ z) \ (\text{set_of_graphs} \ x \ y). \]

Lemma axioms_graph_of_function: forall x y,
Lemma fonction_graph_of_function: forall x y, 
is_function (graph_of_function x y).
Lemma W_graph_of_function: forall x y f, 
inc f (set_of_sub_functions x y) -> W f (graph_of_function x y) = P f.
Lemma injective_graph_of_function: forall x y, 
injective (graph_of_function x y).
Lemma surjective_graph_of_function: forall x y, 
surjective (graph_of_function x y).
Lemma isomorphism_graph_of_function: forall x y, 
order_isomorphism (graph_of_function x y) 
(opposite_order (extension_order x y)) 
(inclusion_suborder (set_of_graphs x y)).

¶ If E is a set, we consider the mapping \( \varpi \rightarrow \tilde{\varpi} \), that maps a partition to the graph of the associated equivalence. We know that “\( \varpi \) coarser than \( \varpi' \)” is equivalent to \( \tilde{\varpi} \supset \tilde{\varpi}' \). This mapping is an isomorphism on its image (when the source is endowed with the opposite of the coarse relation, and the target with \( \subset \)). The source is the set of partitions, the target is some subset of \( \mathcal{P}(E \times E) \).

Definition graph_of_partition x := 
fun_function(fun y => partition_relation_set y x) 
(set_of_partition_set x)(powerset (coarse x)).
Lemma axioms_gop: forall x, 
transf_axioms (fun y => partition_relation_set y x) 
(set_of_partition_set x) (powerset (coarse x)).
Lemma W_gop: forall x y, 
partition y x -> W y (graph_of_partition x) = partition_relation_set y x.
Lemma function_gop: forall x, is_function(graph_of_partition x).
Lemma injective_gop: forall x, injective(graph_of_partition x).
Lemma isomorphism_gop: forall x, 
order_morphism (graph_of_partition x) (coarser x) 
(opposite_order (inclusion_order (coarse x))).

¶ We consider the set of all preorders on E; more precisely the set of all graphs that are preorders, and order them by inclusion. A preorder \( s \) is finer than \( t \) if \( s \subseteq t \); this is the same as to say that elements related by \( s \) are related by \( t \).

Definition set_of_preorders x := 
Zo (powerset (coarse x))(fun z => substrate z = x & preorder z).
Definition coarser_preorder (x:E) := 
inclusion_suborder (set_of_preorders x).
Lemma set_of_preorders_pr: forall x z, 
inc z (set_of_preorders x) = (substrate z = x & preorder z).
Lemma order_coarser_preorder: forall x, 
order (coarser_preorder x).
Lemma substrate_coarser_preorder: forall x, 
substrate (coarser_preorder x) = set_of_preorders x.
Lemma related_coarser_preorder: forall x u v, 
related (coarser_preorder x) u v =
Lemma related_coarser_preorder1: forall x u v,
related (coarser_preorder x) u v =
(preorder u & preorder v & substrate u = x & substrate v = x & forall a b, inc a x -> inc b x -> related u a b -> related v a b).

Consider now a family of sets $E_\iota$, a family of orders $\Gamma_\iota$ with graphs $G_\iota$. Denote the relation associated to $G_\iota$ by $\leq_\iota$. On the product $\prod E_\iota$, we can consider the relation: $\forall \iota, x_\iota \leq_\iota x'_\iota$ between $(x_\iota)$ and $(x'_\iota)$. This is an order relation; it will be called the *product* of the order relations and its graph will be called the *product* of the orders. The graph is $\prod G_\iota$ transported from $\prod(E_\iota \times E_\iota)$ to $\prod E_\iota \times \prod E_\iota$ via the canonical bijection.

Definition product_order_r(f g:Set): EEP :=
fun x x' =>
inc x (productb f) & inc x' (productb f) &
forall i, inc i (domain f) -> gle (V i g) (V i x)(V i x').

Definition product_order f g:=
graph_on (product_order_r f g)(productb f).

Definition axioms_product_order f g:=
fgraph f & fgraph g & domain f = domain g &
(f forall i, inc i (domain f) -> order (V i g)) &
(f forall i, inc i (domain f) -> substrate (V i g) = V i f).

Lemma order_r_product_order: forall f g,
axioms_product_order f g -> order_r (product_order_r f g).

Lemma order_re_product_order: forall f g,
axioms_product_order f g -> order_re (product_order_r f g)(productb f).

Lemma order_product_order: forall f g,
axioms_product_order f g -> order(product_order f g).

Lemma related_product_order: forall f g x x',
axioms_product_order f g ->
related(product_order f g) x x' =
(inc x (productb f) & inc x' (productb f) &
forall i, inc i (domain f) -> related (V i g) (V i x)(V i x')).

Lemma substrate_product_order: forall f g,
axioms_product_order f g -> substrate(product_order f g) = productb f.

Lemma product_order_def: forall f g, axioms_product_order f g ->
image_by_fun (prod_of_products_canon f f)(product_order f g) = (productb g). (* 36 *)

Since $F^{E_\iota}$ is a product, an order on $F$ gives an order on the set of graphs of functions. We can compare two functions $f$ and $g$ via $f(x) \leq g(x)$, which is not an order because we cannot consider the set of all functions. However, this gives a natural order on $F^{(E; F)}$ via *sof_value*.

The function that associates to a triple of $F^{(E; F)}$ its graph in $F^{E_\iota}$ is an isomorphism.
Definition graph_order x y g :=
  graph_on(graph_order_r x y g) (set_of_gfunctions x y).

Definition function_order x y r :=
  graph_on(fun u v => function_order_r x y r(sof_value x y u)(sof_value x y v))
  (set_of_functions x y).

Definition cst_graph x y:= L x (fun _ => y).

Lemma axioms_product_order_x:forall x y g, order g -> substrate g = y ->
  axioms_product_order (cst_graph x y) (cst_graph x g).

Lemma cst_graph_pr: forall x y,
  productb (cst_graph x y) = set_of_gfunctions x y.

Lemma graph_order_r_pr: forall x y g z z', order g -> substrate g = y ->
  graph_order_r x y g z z' =
  product_order_r (cst_graph x y) (cst_graph x g) z z'.

Lemma order_graph_order: forall x y g, order g -> substrate g = y ->
  order (graph_order x y g).

Lemma graph_order_pr:forall x y g, order g -> substrate g = y ->
  graph_order x y g = product_order (cst_graph x y) (cst_graph x g).

Lemma preorder_r_product2_order: forall f g,
  preorder f -> preorder g -> preorder_r (product2_order_r f g).

Lemma order_r_product2_order: forall f g,
  order f -> order g -> order_r (product2_order_r f g).

¶ We consider now the product of two order relations (it is similar to the product of a family
of order that has two elements).

Definition product2_order_r f g :=
  fun x x' =>
  inc x (product (substrate f)(substrate g)) &
  inc x' (product (substrate f)(substrate g)) &
  related f (P x) (P x') & related g (Q x) (Q x').

Definition product2_order f g:=
  graph_on (product2_order_r f g)(product (substrate f)(substrate g)).

Lemma preorder_r_product2_order: forall f g,
  preorder f -> preorder g -> preorder_r (product2_order_r f g).

Lemma order_r_product2_order: forall f g,
  order f -> order g -> order_r (product2_order_r f g).

RR n° 7150
Lemma preorder_product2_order: forall f g, preorder f -> preorder g -> preorder (product2_order f g).
Lemma order_product2_order: forall f g, order f -> order g -> order (product2_order f g).
Lemma product2_order_pr: forall f g x y, related (product2_order f g) x y = product2_order_r f g x y.
Lemma substrate_preorder_product2_order: forall f g, preorder f -> preorder g -> substrate (product2_order f g) = product (substrate f) (substrate g).
Lemma substrate_order_product2_order: forall f g, order f -> order g -> substrate (product2_order f g) = product (substrate f) (substrate g).

2.5 Increasing mappings

We say that a function is increasing if \( x \leq y \) implies \( f(x) \leq f(y) \) and decreasing if \( x \leq y \) implies \( f(x) \geq f(y) \). Bourbaki defines increasing when \( \leq \) is a preorder. A function is strictly increasing or strictly decreasing if \( x < y \) implies \( f(x) < f(y) \) or \( f(x) > f(y) \). A function that is increasing or decreasing is monotone.

Define increasing_map f src r r':=
forall x y, inc x src -> inc y src -> gle r x y -> gle r' (f x) (f y).
Definition decreasing_map f src r r':=
forall x y, inc x src -> inc y src -> gle r x y -> gge r' (f x) (f y).
Definition strict_increasing_map f src r r':=
forall x y, inc x src -> inc y src -> glt r x y -> glt r' (f x) (f y).
Definition strict_decreasing_map f src r r':=
forall x y, inc x src -> inc y src -> glt r x y -> ggt r' (f x) (f y).

Definition increasing_fun f r r':=
is_function f & order r & order r' & substrate r = source f & substrate r' = target f & increasing_map (fun w => W w f) (source f) r r'.
Definition decreasing_fun f r r':=
is_function f & order r & order r' & substrate r = source f & substrate r' = target f & decreasing_map (fun w => W w f) (source f) r r'.
Definition monotone_fun f r r':=
increasing_fun f r r' / decreasing_fun f r r'.
Definition strict_increasing_fun f r r':=
is_function f & order r & order r' & substrate r = source f & substrate r' = target f & strict_increasing_map (fun w => W w f) (source f) r r'.
Definition strict_decreasing_fun f r r':=
is_function f & order r & order r' & substrate r = source f & substrate r' = target f & strict_decreasing_map (fun w => W w f) (source f) r r'.
Definition strict_monotone_fun f r r':=
strict_increasing_fun f r r' / strict_decreasing_fun f r r'.

Some consequences when we replace one order by its opposite.

Lemma increasing_fun_reva : forall f r r', increasing_fun f r r' -> decreasing_fun f r (opposite_order r').
Lemma increasing_fun_revb : forall f r r',
  increasing_fun f r r' -> decreasing_fun f (opposite_order r) r'.

Lemma decreasing_fun_reva : forall f r r',
  decreasing_fun f r r' -> increasing_fun f r (opposite_order r').

Lemma decreasing_fun_revb : forall f r r',
  decreasing_fun f r r' -> increasing_fun f (opposite_order r) r'.

Lemma monotone_fun_reva : forall f r r',
  monotone_fun f r r' -> monotone_fun f r (opposite_order r').

Lemma monotone_fun_revb : forall f r r',
  monotone_fun f r r' -> monotone_fun f (opposite_order r) r'.

Same for strictly monotone.

Lemma opposite_gle: forall r x y, order r ->
  gle (opposite_order r) x y = gle r y x.

Lemma opposite_gge: forall r x y, order r ->
  gge (opposite_order r) x y = gle r x y.

Lemma glt_inva: forall r x y,
  order r -> glt r x y = ggt (opposite_order r) x y.

Lemma ggt_inva: forall r x y,
  order r -> ggt r x y = glt (opposite_order r) x y.

Lemma ggt_invb: forall r x y,
  order r -> ggt r x y = glt r y x.

Lemma strict_increasing_fun_reva : forall f r r',
  strict_increasing_fun f r r' -> strict_decreasing_fun f r (opposite_order r').

Lemma strict_increasing_fun_revb : forall f r r',
  strict_increasing_fun f r r' -> strict_decreasing_fun f (opposite_order r) r'.

Lemma strict_decreasing_fun_reva : forall f r r',
  strict_decreasing_fun f r r' -> strict_increasing_fun f r (opposite_order r').

Lemma strict_decreasing_fun_revb : forall f r r',
  strict_decreasing_fun f r r' -> strict_increasing_fun f (opposite_order r) r'.

Lemma strict_monotone_fun_reva : forall f r r',
  strict_monotone_fun f r r' -> strict_monotone_fun f r (opposite_order r').

Lemma strict_monotone_fun_revb : forall f r r',
  strict_monotone_fun f r r' -> strict_monotone_fun f (opposite_order r) r'.

If \( f \) is constant, then \( f \) is increasing and decreasing. Conversely, the identity function is increasing and decreasing on a set ordered by equality. This function is not constant when the set has more than one element. Let \( E \) be set, \( f \) the function that maps \( X \subset E \) to its complement. This is a strictly decreasing function when the powerset is ordered by inclusion.

Lemma constant_fun_increasing: forall f r r',
  order r -> order r' -> substrate r = source f ->
  substrate r' = target f -> is_constant_function f ->
  increasing_fun f r r'.

Lemma constant_fun_decreasing: forall f r r',
  order r -> order r' -> substrate r = source f ->
  substrate r' = target f -> is_constant_function f ->
  decreasing_fun f r r'.

Lemma identity_increasing_decreasing : forall x,
  let r := diagonal x in
  (increasing_fun (identity_fun x) r r & decreasing_fun (identity_fun x) r r).

Lemma complementary_decreasing: forall E, 
  strict_decreasing_fun(Bl (fun X => complement E X)(powerset E)(powerset E))
  (inclusion_order E) (inclusion_order E).
Let $U_x$ be the set of upper bounds of $\{x\}$ (the case of a non-singleton will be studied later). We have $x \leq y$ if and only if $U_y \subset U_x$. The function $x \mapsto U_x$ is strictly decreasing.

**Definition set_of_majorants1**: $x \mapsto$

\[
\text{Zo (substrate } r)(\text{fun } y \Rightarrow \text{related } r x y).
\]

**Lemma set_of_majorants1_pr**: $\forall x y r, \text{order } r \Rightarrow \text{inc } x (\text{substrate } r) \Rightarrow \text{inc } y (\text{substrate } r) \Rightarrow$

\[(\text{related } r x y = \text{sub (set_of_majorants1 } y r) (\text{set_of_majorants1 } x r)).
\]

**Lemma set_of_majorants1_decreasing**: $\forall r, (*) 15 (*)$

\[\text{order } r \Rightarrow \text{strict_decreasing_fun (BL (fun } x \Rightarrow (\text{set_of_majorants1 } x r)) (\text{substrate } r)(\text{powerset (substrate } r))) r (\text{inclusion_order (substrate } r)).\]

If a function is injective, monotone implies strictly monotone. If a function is bijective, it is an isomorphism if and only if the function and its inverse are increasing. An isomorphism remains one if the ordering on the source and target are replaced by the opposite ones.

**Lemma strict_increasing_from_injective**: $\forall f r r', \text{injective } f \Rightarrow \text{increasing_fun } f r r' \Rightarrow \text{strict_increasing_fun } f r r'$.

**Lemma strict_decreasing_from_injective**: $\forall f r r', \text{injective } f \Rightarrow \text{decreasing_fun } f r r' \Rightarrow \text{strict_decreasing_fun } f r r'$.

**Lemma strict_monotone_from_injective**: $\forall f r r', \text{injective } f \Rightarrow \text{monotone_fun } f r r' \Rightarrow \text{strict_monotone_fun } f r r'$.

**Lemma order_isomorphism_increasing**: $\forall f r r', \text{order_isomorphism } f r r' \Rightarrow$

\[\text{strict_increasing_fun } f r r'.\]

**Lemma order_morphism_increasing**: $\forall f r r', \text{order_morphism } f r r' \Rightarrow$

\[\text{strict_increasing_fun } f r r'.\]

**Lemma order_isomorphism_pr**: $\forall f r r', \text{order_r } r \Rightarrow \text{order_r' } r' \Rightarrow \text{bijective } f \Rightarrow \text{substrate } r = \text{source } f \Rightarrow \text{substrate } r' = \text{target } f \Rightarrow$

\[(\text{increasing_fun } f r r' & \text{increasing_fun (inverse_fun } f) r' r)).\]

**Lemma order_isomorphism_opposite**: $\forall g r r', \text{order_isomorphism } g r r' \Rightarrow$

\[\text{order_isomorphism } g (\text{opposite_order } r) (\text{opposite_order } r').\]

Assume that we have two ordered sets $E$ and $E'$, decreasing functions $u$ and $v$ from $E$ to $E'$ and $E'$ to $E$. Assume $u(v(x)) \geq x$ and $v(u(x')) \geq x'$ for all $x$ and $x'$. Proposition 2 [2 p. 139] says $u \circ v \circ u = u$ and $v \circ u \circ v = v$.

**Theorem decreasing_composition**: $\forall u v r r', \text{decreasing_fun } u r r' \Rightarrow \text{decreasing_fun } v r' r \Rightarrow$

\[(\text{forall } x, \text{inc } x (\text{substrate } r) \Rightarrow \text{related } r (W (W x u) v) x) \Rightarrow\]

\[(\text{forall } x', \text{inc } x' (\text{substrate } r') \Rightarrow \text{related } r' (W (W x' v) u) x') \Rightarrow\]

\[(\text{compose } u (\text{compose } v u) = u & \text{compose } v (\text{compose } u v) = v). (*) 21 (*)\]

### 2.6 Maximal and minimal elements

Bourbaki says: if $E$ is a set with a preorder, then $a \in E$ is minimal (resp. maximal) in $E$ if $x \leq a$ (resp. $x \geq a$) implies $x = a$. In the definition given here, we do not say that $r$ is an order or a preorder.
Definition maximal_element r a :=
  inc a (substrate r) & forall x, inc x (substrate r) -> gle r a x -> x = a.
Definition minimal_element r a :=
  inc a (substrate r) & forall x, inc x (substrate r) -> gle r x a -> x = a.

¶ Given a correspondence \( f \) and a pair \((x, y)\), we can extend \( f \) as \( f' \) by imposing \( f'(x) = y \); this is a correspondence, it is a function if \( x \) is not in the source of \( f \). This extension is unique if we merely add \( x \) to the source, \( y \) to the target and \((x, y)\) to the graph. The extension is a surjective function if \( f \) is surjective.

Definition tack_on_f f x y :=
  corresp (tack_on (source f) x) (tack_on (target f) y) (tack_on (graph f) (J x y)).

Lemma corresp_tack_on: forall f x y,
  is_correspondence f -> is_correspondence (tack_on_f f x y).
Lemma function_tack_on: forall f x y,
  is_function f -> ~(inc x (source f)) -> is_function (tack_on_f f x y).
Lemma W_tack_on_in: forall f x y u,
  is_function f -> ~(inc x (source f)) -> inc u (source f) ->
  W u (tack_on_f f x y) = W u f.
Lemma W_tack_on_out: forall f x y,
  is_function f -> ~(inc x (source f)) -> W x (tack_on_f f x y) = y.
Lemma surjective_tack_on: forall f x y,
  is_function f -> ~(inc x (source f)) -> surjective (tack_on_f f x y).
Lemma tack_on_f_injective: forall x f g a b,
  is_function f -> is_function g -> target f = target g ->
  source f = source g -> ~(inc x (source f)) ->
  (tack_on_f f x a = tack_on_f g x b) -> f = g.

Examples. In \( \mathcal{P}(E) \), the empty set is the least element for inclusion. If we remove it, minimal elements are singletons. On the set of partial functions ordered by extension, maximal elements are total functions (because non-total functions can be extended).

Lemma maximal_element_opp: forall r a,
  order r -> maximal_element r a -> minimal_element (opposite_order r) a.
Lemma minimal_element_opp: forall r a,
  order r -> minimal_element r a -> maximal_element (opposite_order r) a.
Lemma maximal_opposite: forall r x,
  order r -> maximal_element (opposite_order r) x = minimal_element r x.

Lemma minimal_inclusion: forall E y, (* 14 *)
  let F := complement (powerset E) (singleton emptyset) in
  inc y F -> (minimal_element (inclusion_suborder F) y = is_singleton y).
Lemma maximal_prolongation: forall E F x, (* 32 *)
  nonempty F -> inc x (set_of_sub_functions E F) ->
  maximal_element (opposite_order (extension_order E F)) x = (P (Q x) = E).

2.7 Greatest element and least element

We start with the definition of the greatest and least element of an order relation (sometimes called the largest or smallest). Trivial properties follow. If \( \leq \) is an order on \( E \), then \( a \)
is a greatest element for the order if \( a \in E \) and if for all \( x \in E \) we have \( x \leq a \) (the condition \( a \in E \) could be relaxed in \( E \) is not empty). A greatest element may not exist, but is unique. It is maximal. A set that has a greatest element has a unique maximal element. The greatest (resp.least) element is sometimes denoted max (resp. min). We give two properties: if \( E \) has a least element then min\( E \) is a least element, and if \( x \) is a least element of \( E \) then min\( E \) = \( x \). If \( E' \subset E \) then min\( E \) = min\( E' \) provided that the big set has a greatest element that belongs to the small set. If min\( E \) = max\( E \), then \( E \) has a single element.

Definition greatest_element \( r \ a := \\
\quad \text{inc} \ a \ (\text{substrate} \ r) \ & \ \text{forall} \ x, \ \text{inc} \ x \ (\text{substrate} \ r) \ \rightarrow \ \text{gle} \ r \ x \ a.
\)

Definition least_element \( r \ a := \\
\quad \text{inc} \ a \ (\text{substrate} \ r) \ & \ \text{forall} \ x, \ \text{inc} \ x \ (\text{substrate} \ r) \ \rightarrow \ \text{gle} \ r \ a \ x.
\)

Definition the_least_element \( r := \\
\quad \text{choose} \ (\text{fun} \ x \Rightarrow \ \text{least_element} \ r \ x).
\)

Definition the_greatest_element \( r := \\
\quad \text{choose} \ (\text{fun} \ x \Rightarrow \ \text{greatest_element} \ r \ x).
\)

Lemma unique_greatest: \( \forall \ a \ b \ r, \ \text{order} \ r \ \rightarrow \ \text{greatest_element} \ r \ a \ \rightarrow \ \text{greatest_element} \ r \ b \ \rightarrow \ a = b. \)

Lemma unique_least: \( \forall \ a \ b \ r, \ \text{order} \ r \ \rightarrow \ \text{least_element} \ r \ a \ \rightarrow \ \text{least_element} \ r \ b \ \rightarrow \ a = b. \)

Lemma the_least_element_pr: \( \forall \ r, \ \text{order} \ r \ \rightarrow \ (\exists \ u, \ \text{least_element} \ r \ u) \ \rightarrow \ \text{least_element} \ r \ (\text{the_least_element} \ r). \)

Lemma the_greatest_element_pr: \( \forall \ r, \ \text{order} \ r \ \rightarrow \ (\exists \ u, \ \text{greatest_element} \ r \ u) \ \rightarrow \ \text{greatest_element} \ r \ (\text{the_greatest_element} \ r). \)

Lemma greatest_induced: \( \forall \ r \ s \ x, \ \text{order} \ r \ \rightarrow \ \text{sub} \ s \ (\text{substrate} \ r) \ \rightarrow \ \text{inc} \ x \ s \ \rightarrow \ \text{greatest_element} \ r \ x \ \rightarrow \ \text{the_greatest_element} \ r = \text{the_greatest_element} \ (\text{induced_order} \ r \ s). \)

Lemma least_induced: \( \forall \ r \ s \ x, \ \text{order} \ r \ \rightarrow \ \text{sub} \ s \ (\text{substrate} \ r) \ \rightarrow \ \text{inc} \ x \ s \ \rightarrow \ \text{least_element} \ r \ x \ \rightarrow \ \text{the_least_element} \ r = \text{the_least_element} \ (\text{induced_order} \ r \ s). \)

Lemma least_not_greatest: \( \forall \ r \ x, \ \text{order} \ r \ \rightarrow \ \text{least_element} \ r \ x \ \rightarrow \ \text{greatest_element} \ r \ x \ \rightarrow \ \text{is_singleton} \ (\text{substrate} \ r). \)

More simple properties.

Lemma greatest_reverse: \( \forall \ a \ r, \ \text{order} \ r \ \rightarrow \ \text{greatest_element} \ r \ a \ \rightarrow \ \text{least_element} \ (\text{opposite_order} \ r) \ a. \)

Lemma least_reverse: \( \forall \ a \ r, \ \text{order} \ r \ \rightarrow \ \text{least_element} \ r \ a \ \rightarrow \ \text{greatest_element} \ (\text{opposite_order} \ r) \ a. \)

Lemma the_least_reverse: \( \forall \ r, \ \text{order} \ r \ \rightarrow \ (\exists \ a, \ \text{greatest_element} \ r \ a) \ \rightarrow \ \text{the_least_element} \ (\text{opposite_order} \ r) = \text{the_greatest_element} \ r. \)
Lemma greatest_maximal: forall a r,  
  order r -> greatest_element r a -> maximal_element r a.
Lemma least_minimal: forall a r,  
  order r -> least_element r a -> minimal_element r a.
Lemma greatest_unique_maximal: forall a b r,  
  greatest_element r a -> maximal_element r b -> a = b.
Lemma least_unique_minimal: forall a b r,  
  least_element r a -> minimal_element r b -> a = b.

Now some examples. If $\mathcal{G}$ is a subset of $\mathcal{P}(E)$, then the upper and lower bounds of $\mathcal{G}$ are the intersection and union; we anticipate a bit: for the moment being, we just say that the least and greatest elements are the intersection and union, provided they are in $\mathcal{G}$. Note that $E$ need not be mentioned in the theorems.

Lemma least_is_intersection: forall s a,  
  least_element (inclusion_suborder s) a ->  
  nonempty s -> a = intersection s.
Lemma greatest_is_union: forall s a,  
  greatest_element (inclusion_suborder s) a -> a = union s.
Lemma intersection_is_least: forall s,  
  inc (intersection s) s ->  
  least_element (inclusion_suborder s) (intersection s).
Lemma union_is_greatest: forall s,  
  inc (union s) s -> greatest_element (inclusion_suborder s) (union s).

Some applications. On $\mathcal{P}(E)$, the least element is $\emptyset$, the greatest is $E$. On the set of partial functions from $E$ to $F$, there is no greatest element if $F$ has at least two elements (constant functions defined on the whole of $E$ are maximal; if there is a greatest element, all constants are equal).

Lemma emptyset_is_least: forall E,  
  least_element (inclusion_order E) emptyset.
Lemma wholeset_is_greatest: forall E,  
  greatest_element (inclusion_order E) E.
Definition empty_function_tg F := BL (fun x => x) emptyset F.
Lemma function_empty_function_tg: forall F,  
  is_function (empty_function_tg F).
Lemma least_prolongation: forall E F,  
  least_element (opposite_order (extension_order E F))  
  (corr_value (empty_function_tg F)).
Lemma greatest_prolongation: forall E F x,  
  greatest_element (opposite_order (extension_order E F)) x ->  
  nonempty E -> small_set F. (* 17 *)

Bourbaki notices that if $E$ is a set, $\Delta$ the diagonal of $E$, then $\Delta$ is the smallest of equivalences or preorders on $E$ (for the inclusion order induced on $\mathcal{P}(E \times E)$). This a consequence of the next lemma. Note: We have defined finer_equivalence and shown that if $S$ and $R$ are equivalences on a same set, then $S$ is finer than $R$ if and only if $S \subset R$. Thus, on the set of equivalences on $E$, the inclusion order is finer_equivalence and we have already shown that the least element is the diagonal and the greatest one is $E \times E$.

Lemma least_equivalence: forall r,  
  is_reflexive r -> sub (diagonal (substrate r)) r.
Proposition 3 [2, p. 140] in Bourbaki says: Let $E$ be an ordered set and let $E'$ be the disjoint union of $E$ and a set $\{a\}$ consisting of a single element. Then there exists a unique ordering on $E'$ which induces the given ordering on $E$ and for which $a$ is the greatest element of $E'$.

There is no definition of “disjoint union”, but section II.4.8 defines the sum of a family of sets as the union of a family of mutually disjoint sets. Thus, given $E$ and $A = \{a\}$, there exists $\bar{E}$ and $\bar{A}$, two disjoint sets, two bijections $f : E \to \bar{E}$ and $g : A \to \bar{A}$, and $E'$ is the union of $\bar{E}$ and $\bar{A}$. Because $g$ is a bijection, there is an element $a'$ such that $\{a'\} = \bar{A}$. The proposition is now: if $G$ is the given order, then $(f \times f)(G)$ is an order, its substrate is $f(E)$, namely $\bar{E}$, and there is a unique order on $\bar{E} \cup \{a'\}$, extending $(f \times f)(G)$ and with $a'$ as greatest element. In our implementation we consider two separate lemmas.

Definition order_with_greatest r a :=  
union2 r (product (tack_on (substrate r) a) (singleton a)).

Lemma singleton_pr1: forall a x, nonempty x ->  
(forall z, inc z x -> z = a) -> x = singleton a.

Lemma order_with_greatest_pr: forall r a, (* 44 *)  
let r' := order_with_greatest r a in  
order r -> ~ (inc a (substrate r)) ->  
(order r' & substrate r' = tack_on (substrate r) a &  
r = intersection2 r' (coarse (substrate r)) & greatest_element r' a).

Lemma order_transportation: forall f r,  
let r' := image_by_fun (ext_to_prod f f) r in  
bijection f -> order r -> substrate r = source f ->  
(order r' & substrate r' = target f). (* 42 *)

Theorem adjoin_greatest: forall r a E,  
order r -> substrate r = E -> ~ (inc a E) ->  
exists_unique (fun r' => order r' & substrate r' = tack_on E a &  
r = intersection2 r' (coarse E) & greatest_element r' a). (* 39 *)

If $r$ is an order on $E$ (Bourbaki considers the case of pre-orders) we say that a part $A$ of $E$ is \textit{cofinal} (or \textit{coinitial}) if for all $x \in E$ there is a $y \in A$ such that $x \leq y$ (or $y \leq x$) if the order is denoted $\leq$. Bourbaki says “To say that an ordered set $E$ has a greatest element therefore means that $E$ has a cofinal subset consisting of a single element”. The lemmas given here talk about an object $r$ and its substrate $E$. We do not assume that $r$ is an order: we do not even assume that $r$ is a graph (what happens is the following: if $r'$ is the set of pairs $(x, y)$ in $r$, then $r'$ is the the graph of the relation associated to $r$, for which $x$ and $y$ are related if and only if $(x, y) \in r$).

Definition cofinal_set r a :=  
sub a (substrate r) &  
(forall x, inc x (substrate r) -> exists y, inc y a & gle r x y).

Definition coinitial_set r a :=  
sub a (substrate r) &  
(forall x, inc x (substrate r) -> exists y, inc y a & gle r y x).

Lemma exists_greatest_cofinal: forall r,  
exists x, greatest_element r x) =  
(exists a, cofinal_set r a & is_singleton a).

Lemma exists_least_coinitial: forall r,  
exists x, least_element r x) =  
(exists a, coinitial_set r a & is_singleton a).
2.8 Upper and lower bounds

Given an order \( r \) on a set \( E \) denoted by \( \leq \) and a set \( X \), an element \( x \) is said to be an upper bound for \( r \) and \( X \) if \( y \in X \) implies \( y \leq x \). A lower bound is an element \( x \) such that \( y \in X \) implies \( x \leq y \). If the set \( X \) is not empty, we deduce that \( x \in E \); in order to cover the case \( X = \emptyset \), we add the condition \( x \in E \); the set of upper bounds of the empty set is thus \( E \). Note that Bourbaki assumes that \( r \) is a preorder (but in most examples, and in the next section, it will be an order).

Definition upper_bound \( r \ X \ x := \)
\[ \text{inc } x \ (\text{substrate } r) \ & \ \text{forall } y, \ \text{inc } y \ X \to \ \text{gle } r \ y \ x. \]
Definition lower_bound \( r \ X \ x := \)
\[ \text{inc } x \ (\text{substrate } r) \ & \ \text{forall } y, \ \text{inc } y \ X \to \ \text{gle } r \ x \ y. \]

The first properties given here are trivial. If we have an order on \( E \) and if \( X \) is a subset of \( E \), we can consider the order induced on \( X \); this may have a least element \( m \) or a greatest element \( M \). If these quantities exist, they are in \( X \) and are an upper or lower bound of \( X \) for the relation on \( E \). Converse holds: if \( X \) has an upper bound in \( X \), it is \( M \).

Lemma opposite_upper_bound: forall \( x \ X \ r \), order \( r \to \)
upper_bound \( r \ X \ x \) = lower_bound (opposite_order \( r \)) \( X \ x \).
Lemma opposite_lower_bound: forall \( x \ X \ r \), order \( r \to \)
lower_bound \( r \ X \ x \) = upper_bound (opposite_order \( r \)) \( X \ x \).
Lemma smaller_lower_bound: forall \( x y \ X \ r \), preorder \( r \to \)
lower_bound \( r \ X \ x \) \to gle \( r \ y \ x \) \to lower_bound \( r \ X \ y \).
Lemma greater_upper_bound: forall \( x y \ X \ r \), preorder \( r \to \)
upper_bound \( r \ X \ x \) \to gle \( r \ x \ y \) \to upper_bound \( r \ X \ y \).

Lemma sub_lower_bound: forall \( x \ X \ Y \ r \),
lower_bound \( r \ X \ x \) \to sub \( Y \ X \to \) lower_bound \( r \ Y \ x \).
Lemma sub_upper_bound: forall \( x \ X \ Y \ r \),
upper_bound \( r \ X \ x \) \to sub \( Y \ X \to \) upper_bound \( r \ Y \ x \).
Lemma least_element_pr: forall \( X \ r \), order \( r \to \) sub \( X \ (\text{substrate } r) \to \)
(exists \( a \), least_element (induced_order \( r \) \( X \)) \( a \) =
(exists \( x \), lower_bound \( r \ X \ x \ & \ \text{inc } x \ X \)).
Lemma greatest_element_pr: forall \( X \ r \), order \( r \to \) sub \( X \ (\text{substrate } r) \to \)
(exists \( a \), greatest_element (induced_order \( r \) \( X \)) \( a \) =
(exists \( x \), upper_bound \( r \ X \ x \ & \ \text{inc } x \ X \)).

We consider now bounded sets, that are sets that have a bound.

Definition bounded_above \( r \ X \) := exists \( x \), upper_bound \( r \ X \ x \).
Definition bounded_below \( r \ X \) := exists \( x \), lower_bound \( r \ X \ x \).
Definition bounded_both \( r \ X \) := bounded_above \( r \ X \ & \ bounded_below \( r \ X \).

Lemma bounded_above_sub: forall \( X Y \ r \),
sub \( Y \ X \to \) bounded_above \( r \ X \ \to \) bounded_above \( r \ Y \).
Lemma bounded_below_sub: forall \( X Y \ r \),
sub \( Y \ X \to \) bounded_below \( r \ X \ \to \) bounded_below \( r \ Y \).
Lemma bounded_both_sub: forall \( X Y \ r \),
sub \( Y \ X \to \) bounded_both \( r \ X \ \to \) bounded_both \( r \ Y \).
Lemma singleton_bounded:forall \( x \ r \),
is_singleton \( x \to \) order \( r \to \) sub \( x \ (\text{substrate } r) \to \) bounded_both \( r \ x \).
2.9 Least upper bound and greatest lower bound

The Bourbaki definition is: \textit{let E be an ordered set and let X be a subset of E. An element of E is said to be greatest lower bound of X in E if it is the greatest element of the set of lower bounds of X in E.} Let \( W_X \) be the set of lower bounds of \( X \); it is a subset of \( E \), hence can be ordered with the order induced from \( E \). This may have a greatest element \( x \). This is in \( W_X \) hence is a lower bound of \( X \) and if \( z \) is another lower bound we have \( z \leq x \). The converse is true, hence we have a characterization of the greatest lower bound that does not involve the set \( W_X \). Similarly the \textit{least upper bound} of \( X \) is an upper bound \( x \) such that if \( z \) is another upper bound, then \( x \leq z \).

\[
\text{Definition greatest_lower_bound } r \ X \ x := \text{greatest_element (induced_order } r (\text{Zo (substrate } r) (\text{fun } z \Rightarrow \text{lower_bound } r X z))) x. \\
\text{Definition least_upper_bound } r \ X \ x := \text{least_element (induced_order } r (\text{Zo (substrate } r) (\text{fun } z \Rightarrow \text{upper_bound } r X z))).
\]

\[
\text{Lemma greatest_lower_bound_pr: forall } r \ X \ x, \text{order } r \rightarrow \text{sub } X (\text{substrate } r) \rightarrow \text{greatest_lower_bound } r \ X \ x = (\text{lower_bound } r X x \& \text{forall } z, \text{lower_bound } r X z \Rightarrow \text{gle } r z x). \\
\text{Lemma least_upper_bound_pr: forall } r \ X \ x, \text{order } r \rightarrow \text{sub } X (\text{substrate } r) \rightarrow \text{least_upper_bound } r \ X \ x = (\text{upper_bound } r X x \& \text{forall } z, \text{upper_bound } r X z \Rightarrow \text{gle } r x z).
\]

The greatest lower bound and least upper bound are also called supremum and infimum and denoted by \( \text{sup}_E X \) and \( \text{inf}_E X \). As usual, the order is \( \leq \) and the substrate is \( E \); in some cases the set \( E \) is not mentioned. If \( X = \{x, y\} \) we often write \( \text{sup}(x, y) \) and \( \text{inf}(x, y) \). The sup does not always exists, but is unique since there is a unique least element. We give a characterization of the sup and the inf when they exist. The case of two arguments is also provided.

\[
\text{Lemma supremum_unique: forall } x \ y \ X \ r, \text{order } r \rightarrow \text{least_upper_bound } r X x \rightarrow \text{least_upper_bound } r X y \rightarrow x = y. \\
\text{Lemma infimum_unique: forall } x \ y \ X \ r, \text{order } r \rightarrow \text{greatest_lower_bound } r X x \rightarrow \text{greatest_lower_bound } r X y \rightarrow x = y.
\]

\[
\text{Definition supremum } r \ X := \text{choose (fun x=> least_upper_bound } r X x). \\
\text{Definition infimum } r X := \text{choose (fun x=> greatest_lower_bound } r X x). \\
\text{Definition has_supremum } r X := (\exists x, \text{least_upper_bound } r X x). \\
\text{Definition has_infimum } r X := (\exists x, \text{greatest_lower_bound } r X x). \\
\text{Definition sup } r x y := \text{supremum } r \text{ (doubleton } x y). \\
\text{Definition inf } r x y := \text{infimum } r \text{ (doubleton } x y).
\]

\[
\text{Lemma supremum_pr1: forall } X r, \text{order } r \rightarrow \text{sub } X (\text{substrate } r) \rightarrow \text{has_supremum } r X \rightarrow \text{least_upper_bound } r X (\text{supremum } r X). \\
\text{Lemma infimum_pr1: forall } X r, \text{order } r \rightarrow \text{sub } X (\text{substrate } r) \rightarrow \text{has_infimum } r X \rightarrow \text{greatest_lower_bound } r X (\text{infimum } r X). \\
\text{Lemma inc_supremum_substrate : forall } X r, \text{order } r \rightarrow \text{sub } X (\text{substrate } r) \rightarrow \text{has_supremum } r X \rightarrow \text{inc } (\text{supremum } r X) (\text{substrate } r).
\]

José Grimm
Lemma inc_infimum_substrate :forall X r,
  order r -> sub X (substrate r) -> has_infimum r X ->
  inc (infimum r X) (substrate r).

Lemma supremum_pr: forall X r,
  order r -> sub X (substrate r) -> has_supremum r X ->
  (upper_bound r X (supremum r X) &
   forall z, upper_bound r X z -> gle r (supremum r X) z).

Lemma infimum_pr: forall X r,
  order r -> sub X (substrate r) -> has_infimum r X ->
  (lower_bound r X (infimum r X) &
   forall z, lower_bound r X z -> gle r z (infimum r X)).

Lemma sup_pr: forall a b r,
  order r -> inc a (substrate r) -> inc b (substrate r)
  -> has_supremum r (doubleton a b) ->
  (gle r a (sup r a b) & gle r b (sup r a b) &
   forall z, gle r a z -> gle r b z -> gle r (sup r a b) z).

Lemma inf_pr: forall a b r,
  order r -> inc a (substrate r) -> inc b (substrate r)
  -> has_infimum r (doubleton a b) ->
  (gle r (inf r a b) a & gle r (inf r a b) b &
   forall z, gle r z a -> gle r z b -> gle r (inf r a b) z).

Lemma least_upper_bound_doubleton: forall r x y z,
  order r -> gle r x z -> gle r y z ->
  (forall t, gle r t x -> gle r t y -> gle r t z) ->
  least_upper_bound r (doubleton x y) z.

Lemma greatest_lower_bound_doubleton: forall r x y z,
  order r -> gle r x z -> gle r y z ->
  (forall t, gle r t x -> gle r t y -> gle r t z) ->
  greatest_lower_bound r (doubleton x y) z.

We show here the following claim: if a subset X of E has a greatest element a, then a is the
least upper bound of X in E.

Lemma greatest_is_sup: forall r X a,
  order r -> sub X (substrate r) ->
  greatest_element (induced_order r X) a -> least_upper_bound r X a.

Lemma least_is_inf: forall r X a,
  order r -> sub X (substrate r) ->
  least_element (induced_order r X) a -> greatest_lower_bound r X a.

The roles of inf and sup are exchanged if we replace the order by its opposite.

Lemma inf_sup_opp: forall r X a,
  order r -> sub X (substrate r) ->
  greatest_lower_bound r X a = least_upper_bound (opposite_order r) X a.

Lemma sup_inf_opp: forall r X a,
  order r -> sub X (substrate r) ->
  least_upper_bound r X a = greatest_lower_bound (opposite_order r) X a.

Examples. We study the sup and inf of the empty set.

Lemma set_of_lower_bounds_emptyset: forall r ,
  Zo (substrate r) (fun z => lower_bound r emptyset z) = substrate r.

Lemma set_of_upper_bounds_emptyset: forall r ,
  Zo (substrate r) (fun z => upper_bound r emptyset z) = substrate r.
Lemma least_upper_bound_emptyset: forall r x, order r ->
       least_upper_bound r emptyset x = least_element r x.
Lemma greatest_lower_bound_emptyset: forall r x, order r ->
       greatest_lower_bound r emptyset x = greatest_element r x.

If $\mathcal{G}$ is a subset of $\mathcal{P}(E)$, then the upper and lower bounds of $\mathcal{G}$ are the union and intersection, as claimed before. Is $S$ is empty, the intersection is undefined, and the greatest lower bound is the greatest element, namely $E$. Assume $\mathcal{G} \subseteq \mathfrak{F}$ and $\mathfrak{F} \subseteq \mathcal{P}(E)$; then the upper and lower bounds of $\mathcal{G}$ in $\mathfrak{F}$ are the union and intersection, provided that these elements are in $\mathfrak{F}$.

Lemma intersection_is_inf: forall s E, sub s (powerset E) ->
       greatest_lower_bound (inclusion_order E) s
       (Yo (nonempty s) (intersection s) E). (* 14 *)
Lemma union_is_sup: forall s E, sub s (powerset E) ->
       least_upper_bound (inclusion_order E) s (union s).
Lemma union_is_sup1: forall s F E, sub F (powerset E) ->
       sub s F -> inc (union s) F ->
       least_upper_bound (inclusion_suborder F) s (union s).
Lemma intersection_is_inf1: forall s F E, sub F (powerset E) ->
       sub s F -> inc (Yo (nonempty s) (intersection s) E) F ->
       greatest_lower_bound (inclusion_suborder F) s
       (Yo (nonempty s) (intersection s) E).

Third example. If $u$ is in $\Phi(E,F)$, the set of partial functions from $E$ to $F$, we denote its domain by $D(u)$. If $\Theta$ is subset of $\Phi(E,F)$, it has a least upper bound if and only if for all $u$ and $v$ in the family, for all $x \in D(u) \cap D(v)$ we have $u(x) = v(x)$. Denote this property by $P(u,v)$. We use an auxiliary result: if $u \leq w$, the condition $x \in D(u) \cap D(w)$ is equivalent to $x \in D(u)$, and $P(u,w)$ is true. Thus, if $u$ and $v$ are bounded by $w$, $P(u,v)$ is true. Conversely, we know that if $P$ is true on $T$ there is a function defined on the union of the $D(u)$ such that $u \leq f$. This is the least upper bound.

Lemma extension_order_pr : forall E F f g x,
       related (opposite_order (extension_order E F)) f g ->
       inc x (P (Q f)) -> inc x (Q g) = inc x (inv_corr_value g).
Lemma sup_extension_order1: forall E F T f,
       sub T (set_of_sub_functions E F) ->
       least_upper_bound (opposite_order (extension_order E F)) T f ->
       forall u v x, inc u T -> inc v T ->
       inc x (Q u) -> inc x (Q v) ->
       W x (inv_corr_value u) = W x (inv_corr_value v).
Lemma sup_extension_order2: forall E F T,
       sub T (set_of_sub_functions E F) ->
       (forall u v x, inc u T -> inc v T -> inc x (Q u) -> inc x (Q v) ->
       W x (inv_corr_value u) = W x (inv_corr_value v)) ->
       exists x, least_upper_bound (opposite_order (extension_order E F)) T x &
       (P (Q x) = unionf T (fun u => (P (Q u)))) &
       (range (P x) = unionf T (fun u => (range (P u)))) &
       (P x) = unionf T (fun u => (P u)). (* 28 *)

If $f$ is a function with source $A$ and if its target is an ordered set, the supremum of the image $f(A)$ is denoted by $\sup_{x \in A} f(x)$. The infimum is denoted by $\inf_{x \in A} f(x)$. For typographical
reasons, for in-text formulas, the notations \( \sup_{x \in A} f(x) \), \( \inf_{x \in A} f(x) \) are preferred. If \( f \) is the identity function, one can write \( \sup x \) or \( \inf x \). We give a characterization of the sup and inf of a function.

Definition \( \text{is\_sup\_fun} \ r \ f \ x := \text{least\_upper\_bound} \ r \ (\text{image\_of\_fun} \ f) \ x \).
Definition \( \text{is\_inf\_fun} \ r \ f \ x := \text{greatest\_lower\_bound} \ r \ (\text{image\_of\_fun} \ f) \ x \).

Lemma \( \text{is\_sup\_fun\_pr} : \forall r \ f \ x, \text{order} \ r \rightarrow \text{substrate} \ r = \text{target} \ f \rightarrow \) 
\( \text{is\_function} \ f \rightarrow \) 
\( \text{is\_sup\_fun} \ r \ f \ x = (\text{inc} \ x \ (\text{target} \ f) \) 
\& (\forall a, \text{inc} \ a \ (\text{source} \ f) \rightarrow \text{gle} \ r \ (W \ a \ f) \ x) 
\& (\forall z, \text{inc} \ z \ (\text{target} \ f) \rightarrow (\forall a, \text{inc} \ a \ (\text{source} \ f) 
\rightarrow \text{gle} \ r \ (W \ a \ f) \ z) \rightarrow \text{gle} \ r \ x \ z) \).

Lemma \( \text{is\_inf\_fun\_pr} : \forall r \ f \ x, \text{order} \ r \rightarrow \text{substrate} \ r = \text{target} \ f \rightarrow \) 
\( \text{is\_function} \ f \rightarrow \) 
\( \text{is\_inf\_fun} \ r \ f \ x = (\text{inc} \ x \ (\text{target} \ f) \) 
\& (\forall a, \text{inc} \ a \ (\text{source} \ f) \rightarrow \text{gle} \ r \ (W \ a \ f)) \) 
\& (\forall z, \text{inc} \ z \ (\text{target} \ f) \rightarrow (\forall a, \text{inc} \ a \ (\text{source} \ f) 
\rightarrow \text{gle} \ r \ z \ (W \ a \ f)) \rightarrow \text{gle} \ r \ z \ x) \).

In general, we consider a family rather than a function (i.e., a functional graph instead of a function).

Definition \( \text{is\_sup\_graph} \ r \ f \ x := \text{least\_upper\_bound} \ r \ (\text{range} \ f) \ x \).
Definition \( \text{is\_inf\_graph} \ r \ f \ x := \text{greatest\_lower\_bound} \ r \ (\text{range} \ f) \ x \).
Definition \( \text{has\_sup\_graph} \ r \ f := \text{has\_supremum} \ r \ (\text{range} \ f) \).
Definition \( \text{has\_inf\_graph} \ r \ f := \text{has\_infimum} \ r \ (\text{range} \ f) \).
Definition \( \text{sup\_graph} \ r \ f := \text{supremum} \ r \ (\text{range} \ f) \).
Definition \( \text{inf\_graph} \ r \ f := \text{infimum} \ r \ (\text{range} \ f) \).

Here are the characteristic properties.

Lemma \( \text{is\_sup\_graph\_pri} : \forall r \ f, \) 
\( \text{order} \ r \rightarrow \text{sub} \ (\text{range} \ f) \ (\text{substrate} \ r) \rightarrow \text{has\_sup\_graph} \ r \ f \rightarrow \) 
\( \text{least\_upper\_bound} \ r \ (\text{range} \ f) \ (\text{sup\_graph} \ r \ f) \).
Lemma \( \text{is\_inf\_graph\_pri} : \forall r \ f, \) 
\( \text{order} \ r \rightarrow \text{sub} \ (\text{range} \ f) \ (\text{substrate} \ r) \rightarrow \text{has\_inf\_graph} \ r \ f \rightarrow \) 
\( \text{greatest\_lower\_bound} \ r \ (\text{range} \ f) \ (\text{inf\_graph} \ r \ f) \).

Lemma \( \text{is\_sup\_graph\_pr} : \forall r \ f \ x, \text{order} \ r \rightarrow \text{sub} \ (\text{range} \ f) \ (\text{substrate} \ r) \rightarrow \) 
\( \text{fgraph} \ f \rightarrow \) 
\( \text{is\_sup\_graph} \ r \ f \ x = (\text{inc} \ x \ (\text{substrate} \ r) \) 
\& (\forall a, \text{inc} \ a \ (\text{domain} \ f) \rightarrow \text{gle} \ r \ (V \ a \ f) \ x) 
\& (\forall z, \text{inc} \ z \ (\text{substrate} \ r) \rightarrow (\forall a, \text{inc} \ a \ (\text{domain} \ f) 
\rightarrow \text{gle} \ r \ (V \ a \ f) \ z) \rightarrow \text{gle} \ r \ x \ z) \).

Lemma \( \text{is\_inf\_graph\_pr} : \forall r \ f \ x, \text{order} \ r \rightarrow \text{sub} \ (\text{range} \ f) \ (\text{substrate} \ r) \rightarrow \) 
\( \text{fgraph} \ f \rightarrow \) 
\( \text{is\_inf\_graph} \ r \ f \ x = (\text{inc} \ x \ (\text{substrate} \ r) \) 
\& (\forall a, \text{inc} \ a \ (\text{domain} \ f) \rightarrow \text{gle} \ r \ (V \ a \ f)) \) 
\& (\forall z, \text{inc} \ z \ (\text{substrate} \ r) \rightarrow (\forall a, \text{inc} \ a \ (\text{domain} \ f) 
\rightarrow \text{gle} \ r \ z \ (V \ a \ f)) \rightarrow \text{gle} \ r \ z \ x) \).

Assume that \( A \subset E \) is a set that has an infimum and a supremum. If \( A \) is empty, we know that these elements are the least and greatest elements; otherwise, if \( y \in A \) we have \( \inf A \leq y \leq \sup A \), hence \( \inf A \leq \sup A \). This is Proposition 4 [2, p. 142].
Theorem compare_inf_sup1: forall r A, order r -> sub A (substrate r) ->
  has_supremum r A -> has_infimum r A ->
  A = emptyset ->
  (greatest_element r (infimum r A) & least_element r (supremum r A)).

Theorem compare_inf_sup2: forall r A, order r -> sub A (ssetubstrate r) ->
  has_supremum r A -> has_infimum r A ->
  nonempty A -> gle r (infimum r A) (supremum r A).

Proposition 5 [2, p. 142] says that sup is increasing and inf is decreasing (as a function
from \( P(E) \) into \( E \), where \( P \) is ordered by inclusion). Of course, these are only partial func-
tions. As a corollary, consider a family \((x_i)_{i \in I} \) and \( J \subset I \); we have \( \sup_{i \in I} x_i \leq \sup_{i \in J} x_i \) if both quan-
tities are defined. Note that the first term is the supremum of the restriction of the family
to \( J \).

Theorem sup_increasing: forall r A B, order r -> sub A (substrate r) ->
  sub B (substrate r) -> sub A B ->
  has_supremum r A -> has_supremum r B ->
  gle r (supremum r A) (supremum r B).

Theorem inf_decreasing: forall r A B, order r -> sub A (substrate r) ->
  sub B (substrate r) -> sub A B ->
  has_infimum r A -> has_infimum r B ->
  gge r (infimum r A) (infimum r B).

Lemma sup_increasing1: forall r f j,
  order r -> fgraph f -> sub (range f) (substrate r) -> sub j (domain f) ->
  has_sup_graph r f -> has_sup_graph r (restr f j) ->
  gle r (sup_graph r (restr f j)) (sup_graph r f).

Lemma inf_decreasing1: forall r f j,
  order r -> fgraph f -> sub (range f) (substrate r) -> sub j (domain f) ->
  has_inf_graph r f -> has_inf_graph r (restr f j) ->
  gge r (inf_graph r (restr f j)) (inf_graph r f).

Proposition 6 [2, p. 143] says that if \( f \) and \( g \) are two functions of type \( F \rightarrow E \), if \( f(x) \leq g(x) \)
for all \( x \in F \) then \( \sup f \leq \sup g \), provided that both quantities are defined. In fact, it is stated
as: if for all \( i \in I \) we have \( x_i \leq y_i \), then \( \sup_{i \in I} x_i \leq \sup_{i \in I} y_i \), and \( \inf_{i \in I} x_i \leq \inf_{i \in I} y_i \).

Lemma sup_increasing2: forall r f f',
  order r -> fgraph f -> fgraph f' -> domain f = domain f' ->
  sub (range f) (substrate r) -> sub (range f') (substrate r) ->
  has_sup_graph r f -> has_sup_graph r f' ->
  (forall x, inc x (domain f) -> gle r (V x f) (V x f')) ->
  gle r (sup_graph r f) (sup_graph r f').

Lemma inf_increasing2: forall r f f',
  order r -> fgraph f -> fgraph f' -> domain f = domain f' ->
  sub (range f) (substrate r) -> sub (range f') (substrate r) ->
  has_inf_graph r f -> has_inf_graph r f' ->
  (forall x, inc x (domain f) -> gle r (V x f) (V x f')) ->
  gle r (inf_graph r f) (inf_graph r f').

Proposition 7 [2, p. 143] is the following. Consider a family \((x_i)_{i \in I} \), and let \((J_{\lambda})_{\lambda \in L} \) be a
covering of \( I \). The family \((x_i)_{i \in J_{\lambda}} \) is the restriction of \((x_i) \) to \( J_{\lambda} \); we assume that it has a supre-
mum \( \sup_{i \in J_{\lambda}} x_i \), and we consider the family \((\sup_{i \in J_{\lambda}} x_i)_{\lambda \in L} \). This family has a supremum if and only
if \((x_i)_{i \in I} \) has one, and the values are the same; the second equality in (1) is true under similar
conditions.

\[(1) \quad \sup_{i \in I} x_i = \sup_{\lambda \in L} \left( \sup_{i \in I} x_i \right), \quad \inf_{i \in I} x_i = \inf_{\lambda \in I} \left( \inf_{i \in I} x_i \right).\]

The first lemma here says that if \(x\) is a least upper bound for one family, it is also the least upper bound for the other one. Finally, since the supremum is a least upper bound, we get the result by uniqueness.

**Lemma sup_distributive:** forall \(r f c x\), \((*) 45 (*)\)
order \(r \to fgraph f \to \text{sub (range } f \text{) (substrate } r \text{) \to}
covering c (domain f) \to
(\forall l, \text{inc } l \text{ (domain } c \text{)} \to \text{has_sup_graph } r \text{ (restr } f \text{ (V } l \text{ c)}) \to
\text{is_sup_graph } r \text{ f x } =
\text{is_sup_graph } r \text{ (L (domain } c \text{) (fun } l \to \text{sup_graph } r \text{ (restr } f \text{ (V } l \text{ c)})\)) x.

**Lemma inf_distributive:** forall \(r f c x\), \((*) 44 (*)\)
order \(r \to fgraph f \to \text{sub (range } f \text{) (substrate } r \text{) \to}
covering c (domain f) \to
(\forall l, \text{inc } l \text{ (domain } c \text{)} \to \text{has_inf_graph } r \text{ (restr } f \text{ (V } l \text{ c)}) \to
\text{is_inf_graph } r \text{ f x } =
\text{is_inf_graph } r \text{ (L (domain } c \text{) (fun } l \to \text{inf_graph } r \text{ (restr } f \text{ (V } l \text{ c)})\)) x.

**Lemma sup_distributive1:** forall \(r f c\), \((*) 45 (*)\)
order \(r \to fgraph f \to \text{sub (range } f \text{) (substrate } r \text{) \to}
covering c (domain f) \to
(\forall l, \text{inc } l \text{ (domain } c \text{)} \to \text{has_sup_graph } r \text{ (restr } f \text{ (V } l \text{ c)}) \to
\text{has_sup_graph } r \text{ f =}
\text{has_sup_graph } r \text{ (L (domain } c \text{) (fun } l \to \text{sup_graph } r \text{ (restr } f \text{ (V } l \text{ c)})\)) .

**Lemma inf_distributive1:** forall \(r f c\), \((*) 44 (*)\)
order \(r \to fgraph f \to \text{sub (range } f \text{) (substrate } r \text{) \to}
covering c (domain f) \to
(\forall l, \text{inc } l \text{ (domain } c \text{)} \to \text{has_inf_graph } r \text{ (restr } f \text{ (V } l \text{ c)}) \to
\text{has_inf_graph } r \text{ f =}
\text{has_inf_graph } r \text{ (L (domain } c \text{) (fun } l \to \text{inf_graph } r \text{ (restr } f \text{ (V } l \text{ c)})\)) .

**Theorem sup_distributive2:** forall \(r f c\), \((*) 19 (*)\)
order \(r \to fgraph f \to \text{sub (range } f \text{) (substrate } r \text{) \to}
covering c (domain f) \to
(\forall l, \text{inc } l \text{ (domain } c \text{)} \to \text{has_sup_graph } r \text{ (restr } f \text{ (V } l \text{ c)}) \to
(\text{has_sup_graph } r \text{ f =}
\text{has_sup_graph } r \text{ (L (domain } c \text{) (fun } l \to \text{sup_graph } r \text{ (restr } f \text{ (V } l \text{ c)})\)) \&
(\text{sup_graph } r \text{ f \to sup_graph } r \text{ f =}
\text{sup_graph } r \text{ (L (domain } c \text{) (fun } l \to \text{sup_graph } r \text{ (restr } f \text{ (V } l \text{ c)})\)) .

**Theorem inf_distributive2:** forall \(r f c\), \((*) 19 (*)\)
order \(r \to fgraph f \to \text{sub (range } f \text{) (substrate } r \text{) \to}
covering c (domain f) \to
(\forall l, \text{inc } l \text{ (domain } c \text{)} \to \text{has_inf_graph } r \text{ (restr } f \text{ (V } l \text{ c)}) \to
(\text{has_inf_graph } r \text{ f =}
\text{has_inf_graph } r \text{ (L (domain } c \text{) (fun } l \to \text{inf_graph } r \text{ (restr } f \text{ (V } l \text{ c)})\)) \&
(\text{inf_graph } r \text{ f \to inf_graph } r \text{ f =}
\text{inf_graph } r \text{ (L (domain } c \text{) (fun } l \to \text{inf_graph } r \text{ (restr } f \text{ (V } l \text{ c)})\)) .

¶ Corollary. Let \((x_{\lambda \mu})_{(\lambda, \mu) \in L \times M}\) be a double family of elements of an ordered set \(E\) such that for each \(\mu \in M\) the family \((x_{\lambda \mu})_{\lambda \in L}\) has a least upper bound in \(E\). This family is the restriction of the double family to \(L \times \{\mu\}\). For the double family to have a least upper bound in \(E\) it is
necessary and sufficient that \((\sup_{\lambda \in L} x_{\lambda \mu})_{\mu \in M}\) has a least upper bound, and the bounds are the same. The second equality in (2) holds under similar conditions.

\[
\begin{align*}
\sup_{(\lambda, \mu) \in L \times M} x_{\lambda \mu} &= \sup_{\mu \in M} (\sup_{\lambda \in L} x_{\lambda \mu}), \\
\inf_{(\lambda, \mu) \in L \times M} x_{\lambda \mu} &= \inf_{\mu \in M} (\inf_{\lambda \in L} x_{\lambda \mu}).
\end{align*}
\]

Definition partial_fun f x m := restr f (product x (singleton m)).

Lemma sup_distributive3: forall r f x y, order r -> fgraph f -> sub (range f) (substrate r) -> domain f = product x y -> (forall m, inc m y -> has_sup_graph r (partial_fun f x m)) -> (has_sup_graph r f = has_sup_graph r (L y (fun m => sup_graph r (partial_fun f x m)))) & (has_sup_graph r f -> sup_graph r f = sup_graph r (L y (fun m => sup_graph r (partial_fun f x m)))).

Lemma inf_distributive3: forall r f x y, order r -> fgraph f -> sub (range f) (substrate r) -> domain f = product x y -> (forall m, inc m y -> has_inf_graph r (partial_fun f x m)) -> (has_inf_graph r f = has_inf_graph r (L y (fun m => inf_graph r (partial_fun f x m)))) & (has_inf_graph r f -> inf_graph r f = inf_graph r (L y (fun m => inf_graph r (partial_fun f x m)))).

Proposition 8 [2, p. 144] says that if we have a family of ordered sets \(E_i\), a subset \(A\) of \(\prod E_i\), and if \(A_{i} = \text{pr}_i A\), then \(A\) has a least upper bound of the form \((x_i)_{i \in I}\), if and only if each \(A_i\) has one, and there is equality; a similar property holds for the greatest lower bound.

\[
\sup A = (\sup_{A_i})_{i \in I} = \left(\sup_{x \in A_{i}} x_{i}\right)_{i \in I}, \quad \inf A = (\inf_{A_i})_{i \in I} = \left(\inf_{x \in A_{i}} x_{i}\right)_{i \in I}.
\]

Theorem sup_in_product: forall f g A, (* 60 *)
let Ai := fun i => (image_by_fun (pr_i f i) A) in
let has_sup :=
forall i, inc i (domain f) -> has_supremum (V i g) (Ai i) in
axioms_product_order f g -> sub A (productb f) ->
((has_sup = has_supremum (product_order f g) A) &
(has_sup -> supremum (product_order f g) A = L (domain f) (fun i => supremum(V i g) (Ai i)))).

Theorem inf_in_product: forall f g A, (* 60 *)
let Ai := fun i => (image_by_fun (pr_i f i) A) in
let has_inf :=
forall i, inc i (domain f) -> has_infimum (V i g) (Ai i) in
axioms_product_order f g -> sub A (productb f) ->
((has_inf = has_infimum (product_order f g) A) &
(has_inf -> infimum (product_order f g) A = L (domain f) (fun i => infimum(V i g) (Ai i)))).

Proposition 9 [2, p. 144] assumes that \(E\) is an ordered set, \(F\) is a subset of \(E\) and \(A\) is a subset of \(F\). It can happen that one of \(\sup_E A\) and \(\sup_F A\) exists, but not the other; they may be unequal. If the objects exist we have

\[
\sup_E A \leq \sup_F A, \quad \inf_E \geq \inf_F A \quad (F \subseteq E).
\]

If \(\sup_E A\) exists and is in \(F\), it is \(\sup_F A\).
Theorem sup_induced1: \(\forall r \ A \ F, \text{order } r \implies \text{sub } F (\text{substrate } r) \implies \text{sub } A \ F \implies\)
\[\text{has_supremum } r A \implies \text{has_supremum } (\text{induced_order } r F) A \implies\]
\[\text{gle } r (\supremum r A) (\supremum (\text{induced_order } r F) A).\]

Theorem inf_induced1: \(\forall r \ A \ F, \text{order } r \implies \text{sub } F (\text{substrate } r) \implies \text{sub } A \ F \implies\)
\[\text{has_infimum } r A \implies \text{has_infimum } (\text{induced_order } r F) A \implies\]
\[\text{gge } r (\infimum r A) (\infimum (\text{induced_order } r F) A).\]

Theorem sup_induced2: \(\forall r \ A \ F, \text{order } r \implies \text{sub } F (\text{substrate } r) \implies \text{sub } A \ F \implies\)
\[\text{has_supremum } r A \implies \text{inc } (\supremum r A) F \implies\]
\[\text{has_supremum } (\text{induced_order } r F) A \implies\]
\[\supremum r A = \supremum (\text{induced_order } r F) A.\]

Theorem inf_induced2: \(\forall r \ A \ F, \text{order } r \implies \text{sub } F (\text{substrate } r) \implies \text{sub } A \ F \implies\)
\[\text{has_infimum } r A \implies \text{inc } (\infimum r A) F \implies\]
\[\text{has_infimum } (\text{induced_order } r F) A \implies\]
\[\infimum r A = \infimum (\text{induced_order } r F) A.\]

2.10 Directed sets

An ordered set is said left or right directed if every doubleton is bounded (above or below).

Definition right_directed \(r\) :=
\[\text{order } r \land \forall x, \forall y, \text{inc } x (\text{substrate } r) \implies \text{inc } y (\text{substrate } r) \implies\]
\[\text{bounded_above } r (\text{doubleton } x y).\]

Definition left_directed \(r\) :=
\[\text{order } r \land \forall x, \forall y, \text{inc } x (\text{substrate } r) \implies \text{inc } y (\text{substrate } r) \implies\]
\[\text{bounded_below } r (\text{doubleton } x y).\]

We rewrite the definition as: for all \(x\) and \(y\) there is a \(z\) such that \(x \leq z\) and \(y \leq z\). A set that has a greatest element is right directed. A product of directed sets is directed. A cofinal set of a directed set is directed for the induced order.

Lemma right_directed_pr: \(\forall r, \text{right_directed } r = (\text{order } r \land \forall x, \forall y, \text{inc } x (\text{substrate } r) \implies \text{inc } y (\text{substrate } r) \implies \exists z, \text{inc } z (\text{substrate } r) \land \text{gle } r x z \land \text{gle } r y z).\)

Lemma left_directed_pr: \(\forall r, \text{left_directed } r = (\text{order } r \land \forall x, \forall y, \text{inc } x (\text{substrate } r) \implies \text{inc } y (\text{substrate } r) \implies \exists z, \text{inc } z (\text{substrate } r) \land \text{gle } r z x \land \text{gle } r z y).\)

Lemma greatest_right_directed : \(\forall r, \text{order } r \implies\)
\[(\exists a, \text{greatest_element } r a) \implies \text{right_directed } r.\]

Lemma least_left_directed : \(\forall r, \text{order } r \implies\)
\[(\exists a, \text{least_element } r a) \implies \text{left_directed } r.\]

Lemma opposite_right_directed : \(\forall r, \text{is_graph } r \implies\)
\[\text{right_directed } r = \text{left_directed } (\text{opposite_order } r).\]

Lemma opposite_left_directed : \(\forall r, \text{is_graph } r \implies\)
\[\text{left_directed } r = \text{right_directed } (\text{opposite_order } r).\]

Lemma product_right_directed: \(\forall f g, (\ast 14 \ast)\)
\[\text{axioms_product_order } f g \implies\]
\[(\forall i, \text{inc } i (\text{domain } f) \implies \text{right_directed } (V i g)) \implies \text{right_directed } (\text{product_order } f g).\]

Lemma product_left_directed: \(\forall f g, (\ast 14 \ast)\)
\[\text{axioms_product_order } f g \implies\]
\[(\forall i, \text{inc } i (\text{domain } f) \implies \text{left_directed } (V i g))\]

RR n° 7150
-> left_directed (product_order f g).
Lemma cofinal_right_directed: forall r A,
  right_directed r -> cofinal_set r A -> right_directed (induced_order r A).
Lemma cofinal_left_directed: forall r A,
  left_directed r -> cofinal_set r A -> left_directed (induced_order r A).

Proposition 10 [2, p. 145] says that in a right directed set, a maximal element is the greatest element.
Theorem right_directed_maximal: forall r x,
  right_directed r -> maximal_element r x -> greatest_element r x.
Theorem left_directed_minimal: forall r x,
  left_directed r -> minimal_element r x -> least_element r x.

2.11 Lattices

A lattice is an ordered set on which each pair has a least upper bound and a greatest lower bound.
Definition lattice r := order r &
  forall x, forall y, inc x (substrate r) -> inc y (substrate r) ->
  (has_supremum r (doubleton x y) & has_infimum r (doubleton x y)).

Lemma lattice_sup_pr: forall r a b,
  lattice r -> inc a (substrate r) -> inc b (substrate r) ->
  (gle r a (sup r a b) & gle r b (sup r a b) &
  forall z, gle r a z -> gle r b z -> gle r (sup r a b) z).

Lemma lattice_inf_pr: forall r a b,
  lattice r -> inc a (substrate r) -> inc b (substrate r) ->
  (gle r (inf r a b) a & gle r (inf r a b) b &
  forall z, gle r z a -> gle r z b -> gle r z (inf r a b)).

The powerset is a lattice. In fact each set has a supremum and an infimum.
Lemma inf_inclusion: forall A x y, sub x A -> sub y A ->
  greatest_lower_bound (inclusion_order A) (doubleton x y) (intersection2 x y).
Lemma sup_inclusion: forall A x y, sub x A -> sub y A ->
  least_upper_bound (inclusion_order A) (doubleton x y) (union2 x y).
Lemma powerset_lattice: forall A, lattice (inclusion_order A).

The product of lattices is a lattice. This is an easy consequence of Proposition 8, and the fact that pr A is a doubleton if A is a doubleton. A lattice is a directed set.

Lemma product_lattice: forall f g,
  axioms_product_order f g ->
  (forall i, inc i (domain f) -> lattice (V i g))
  -> lattice (product_order f g). (* 29 *)

Lemma lattice_directed: forall r,
  lattice r -> (right_directed r & left_directed r).

Other examples. The set of integers, with the order “x divides y” is a lattice. The set of subgroups of a group (ordered by inclusion) is a lattice. The set of topologies on a set is a lattice. The set of real functions on an interval is a lattice. The opposite of a lattice is a lattice.

Lemma lattice_inverse: forall r, lattice r -> lattice (opposite_order r).
2.12 Totally ordered sets

Two elements of a preordered set $E$ are said comparable if the relation “$x \leq y$ or $y \leq x$” is true. A set $E$ is said to be totally ordered if it is ordered and if any two elements of $E$ are comparable.

Definition total_order $r :=$

\[
\text{order } r \land \forall x \ y, \text{inc } x (\text{substrate } r) \to \text{inc } y (\text{substrate } r) \to \\
(\text{gle } r \ x \ y \lor \text{gge } r \ x \ y).
\]

An order satisfies $G \circ G = G$ and $G \cap G^{-1} \subset \Delta_E$. It is total if moreover $G \cup G^{-1} = E \times E$. We have $x < y$ or $x > y$. We have $x \leq y$ or $y \leq x$. A subset of a totally ordered set is totally ordered. A small set is totally ordered. The opposite of a totally ordered set is totally ordered.

Lemma total_order_pr: forall $r$,

\[
\text{total_order } r = \\
(\text{compose_graph } r \times r = r \land \\
\text{intersection2 } r (\text{opposite_order } r) = \text{diagonal } (\text{substrate } r) \land \\
\text{union2 } r (\text{opposite_order } r) = \text{coarse } (\text{substrate } r)).
\]

Lemma total_order_pr1 : forall $r \ x \ y$,

\[
\text{total_order } r \to \text{inc } x (\text{substrate } r) \to \text{inc } y (\text{substrate } r) \to \\
(\text{glt } r \ x \ y \lor \text{ggt } r \ x \ y \lor \ x = y).
\]

Lemma total_order_pr2 : forall $r \ x \ y$,

\[
\text{total_order } r \to \text{inc } x (\text{substrate } r) \to \text{inc } y (\text{substrate } r) \to \\
(\text{glt } r \ x \ y \lor \text{gle } r \ y \ x).
\]

Lemma total_order_sub : forall $r \ x$,

\[
\text{total_order } r \to \text{sub } x (\text{substrate } r) \to \text{total_order } (\text{induced_order } r \ x).
\]

Lemma total_order_conterexample:

\[- (\text{total_order } (\text{inclusion_order } \text{two_points})).
\]

Lemma total_order_opposite: forall $r$,

\[
\text{total_order } r \to \text{total_order } (\text{opposite_order } r).
\]

If $x \leq y$, then $\sup(x, y) = y$ and $\inf(x, y) = x$, hence a totally ordered set is a lattice.

Lemma sup_comparable: forall $r \ x \ y$, $\text{gle } r \ x \ y \to$

\[
\text{order } r \to \text{least_upper_bound } r (\text{doubleton } x \ y) \ y.
\]

Lemma inf_comparable: forall $r \ x \ y$, $\text{gle } r \ x \ y \to$

\[
\text{order } r \to \text{greatest_lower_bound } r (\text{doubleton } x \ y) \ x.
\]

Lemma sup_comparable1: forall $r \ x \ y$, $\text{order } r \to \text{gle } r \ x \ y \to \sup r \times y = y$.

Lemma inf_comparable1: forall $r \ x \ y$, $\text{order } r \to \text{gle } r \ x \ y \to \inf r \times y = x$.

Lemma total_order_lattice: forall $r$,

\[
\text{total_order } r \to \text{total_order } (\text{induced_order } r \ x). \to \text{lattice } r.
\]

Lemma total_order_directed: forall $r$,

\[
\text{total_order } r \to \text{(right_directed } r \land \text{left_directed } r).
\]

Proposition 11 [2, p. 147] says that if $f$ is strictly monotone and the ordering on the source is total, then $f$ is injective. If $f$ is strictly increasing, it is a morphism (an isomorphism onto the image). We first show that if $f$ is strictly increasing, then it is increasing.

Lemma increasing_fun_from_strict: forall $f \ r \ r'$,

\[
\text{strict_increasing_fun } f \ r \ r' \to \text{increasing_fun } f \ r \ r'.
\]

Lemma decreasing_fun_from_strict: forall $f \ r \ r'$,

\[
\text{strict_decreasing_fun } f \ r \ r' \to \text{decreasing_fun } f \ r \ r'.
\]

Theorem total_order_monotone_injective: forall $f \ r \ r'$,
total_order r -> strict_monotone_fun f r r' -> injective f.

Theorem total_order_increasing_morphism: forall f r r',
  total_order r -> strict_increasing_fun f r r' -> order_morphism f r r'.

Proposition 12 \[2, p. 147\] says that in a totally ordered set \( E \), an element \( x \) is the least upper bound of a subset \( X \) if and only if it is an upper bound and, for all \( y < x \), there is a \( z \in X \) such that \( y < z \) and \( z \leq x \).

Theorem sup_in_total_order:forall r X x, total_order r -> sub X (substrate r)->
  least_upper_bound r X x = (upper_bound r X x &
  (forall y, glt r y x -> exists z, inc z X & glt r y z & gle r z x)).

Theorem inf_in_total_order:forall r X x, total_order r -> sub X (substrate r)->
  greatest_lower_bound r X x = (lower_bound r X x &
  (forall y, glt r x y -> exists z, inc z X & glt r z y & gle r x z)).

2.13 Intervals

There are many definitions of an interval. The set of all \( x \) such that \( a \leq x \leq b \) is called the closed interval and denoted \([a,b]\); the set of all \( x \) such that \( a < x < b \) is called the open interval and denoted \((a,b)\); intervals can be semi open. One can drop one of the conditions, for instance the set of all \( x \) such that \( x < b \) is denoted by \([a,)\), this is an unbounded interval.

The letters o, c, u stand for open, close, and unbounded.

Definition interval_oo r a b := Zo(substrate r)(fun z => glt r a z & glt r z b).
Definition interval_oc r a b := Zo(substrate r)(fun z => glt r a z & gle r z b).
Definition interval_ou r a := Zo (substrate r) (fun z => glt r a z).
Definition interval_co r a b := Zo(substrate r)(fun z => gle r a z & glt r z b).
Definition interval_cu r a := Zo (substrate r) (fun z => gle r a z).
Definition interval_uo r b := Zo (substrate r) (fun z => glt r z b).
Definition interval_uc r a := Zo (substrate r) (fun z => gle r a z).
Definition interval_uu r := Zo (substrate r) (fun z => True).

Definition is_closed_interval r x := exists a, exists b,
  inc a (substrate r) & inc b (substrate r) & gle r a b & x = interval_cc r a b.
Definition is_open_interval r x := exists a, exists b,
  inc a (substrate r) & inc b (substrate r) & gle r a b & x = interval_oo r a b.
Definition is_semi_open_interval r x := exists a, exists b,
  inc a (substrate r) & inc b (substrate r) & gle r a b &
  (x = interval_oc r a b) / x = interval_co r a b).
Definition is_bounded_interval r x := exists b, inc b (substrate r) &
  x = interval_uo r b / x = interval_oo r b.
Definition is_left_unbounded_interval r x :=
  exists b, inc b (substrate r) & (x = interval_uc r b) / x = interval_uo r b.
Definition is_right_unbounded_interval r x :=
  exists a, inc a (substrate r) & (x = interval_cu r a) / x = interval_or u a).
Definition is_unbounded_interval r x :=
  is_left_unbounded_interval r x / is_right_unbounded_interval r x \ /
  x = interval_uu r.
Definition is_interval r x :=
  is_bounded_interval r x / is_unbounded_interval r x.

A non-empty interval \([a,b]\) has a least and greatest elements, which are \(a\) and \(b\) respectively.
Lemma the_least_interval: forall r a b, order r -> gle r a b -> the_least_element (induced_order r (interval_cc r a b)) = a.
Lemma the_greatest_interval: forall r a b, order r -> gle r a b -> the_greatest_element (induced_order r (interval_cc r a b)) = b.

A closed interval is never empty; however [a,a], [a,a], and [a,a] are empty.

Lemma nonempty_closed_interval: forall r x, order r -> is_closed_interval r x -> nonempty x.
Lemma singleton_interval: forall r a, order r -> inc a (substrate r) -> is_singleton (interval_cc r a a).
Lemma empty_interval: forall r a, order r -> inc a (substrate r) -> (empty (interval_co r a a) & empty (interval_oc r a a) & empty (interval_oo r a a)).

The only non trivial result here is Proposition 13 [2, p. 148] that says that, in a lattice, the intersection of two intervals is an interval. We start with a short proof.

Let's say that an interval is of type L if it is left unbounded, of type R if it is right unbounded (the interval \( U = [\rightarrow, \rightarrow] \) is of both types, and \( U \cap X = X \) for any interval \( X \)). Obviously, each interval is the intersection of two intervals of type L and R (if the interval is unbounded, consider intersection with \( U \)). The intersection of two intervals is thus of the form \( (L_1 \cap R_1) \cap (L_2 \cap R_2) = (L_1 \cap L_2) \cap (R_1 \cap R_2) \). This is of the form \( L_3 \cap R_3 \).

Definition is_lu_interval r x := x = interval_uu r \| is_left_unbounded_interval r x.
Definition is_ru_interval r x := x = interval_uu r \| is_right_unbounded_interval r x.
Lemma intersection4: forall A B C D, intersection2 (intersection2 A B) (intersection2 C D) = intersection2 (intersection2 A C) (intersection2 B D).
Lemma intersection_i1: forall r x, is_interval r x -> intersection2 x (interval_uu r) = x. (* 13 *)
Lemma intersection_i2: forall r x, is_interval r x -> \exists u, \exists v, is_lu_interval r u & is_ru_interval r v & intersection2 u v = x). (* 17 *)
Lemma intersection_i3: forall r x y, lattice r -> is_left_unbounded_interval r x -> is_left_unbounded_interval r y -> is_left_unbounded_interval r (intersection2 x y). (* 18 *)
Theorem intersection_interval: forall r x y, lattice r -> is_interval r x -> is_interval r y -> is_interval r (intersection2 x y). (* 47 *)

The total size of the proof of the theorem is 150 lines, including the tactics designed for this theorem. Originally, its size was 841 lines, reduced to 615 by using adequate tactics. Details can be found in section 1.5.
Chapter 3

Well-ordered sets

This chapter defines the notion of a well-ordering, and the lexicographic ordering (we compare two sequences $x_i$ and $y_i$ according to the least index $j$ such that $x_j \neq y_j$.) We show Zermelo’s theorem (there exists a well-ordering) and Zorn’s lemma (every inductive ordered set has a maximal element). These theorems are equivalent to the axiom of choice, thus non-constructive. Ordinals (first, second, third, etc.) are introduced at the end of the chapter, cardinals (one, two, three, etc.) are defined in the next chapter. To each finite ordinal corresponds a unique cardinal (see Chapter 4 for the definition of “finite”). The “etc.” in the sentence above suggests that there is a unique way to add a new term to the sequence (for instance fourth and four). This is called “induction” in the case of finite cardinals; it is called “transfinite induction” in the case of well-ordered sets.

3.1 Segments of a well-ordered set

A relation $R \mid x, y \mid$ is said to be a well-ordering relation between $x$ and $y$ if $R$ is an order relation between $x$ and $y$ and if for each non-empty set $E$ on which $R \mid x, y \mid$ induces an order relation, the ordered by this relation, has a least element. A set $E$ ordered by an ordering $\Gamma$ is said to be well-ordered if the relation $y \in \Gamma(x)$ is a well ordering between $x$ and $y$; $\Gamma$ is then said to be a well-ordering on $E$. The definition that follows corresponds to $\Gamma$.

Definition worder r :=
  order r & forall x, sub x (substrate x) -> nonempty x ->
  exists y, least_element (induced_order r x) y.

Bourbaki notes that a totally ordered set with two elements is well-ordered. In fact, it contains $a$ and $b$ such that $a < b$, so that the graph is the set with three elements $(a, a), (a, b)$ and $(b, b)$. All total orders on sets with two elements are isomorphic. We consider here the case where $a$ and $b$ are the elements of the doubleton two_points.

Definition canonical_doubleton_order :=
  union2 (doubleton (J TPa TPa) (J TPb TPb)) (singleton (J TPa TPb)).

Lemma canonical_doubleton_order_pr: forall x y, 
  related canonical_doubleton_order x y = 
  (x= TPa & y = TPa) / (x= TPb & y = TPb) / (x= TPa & y = TPb).

Lemma one_not_zero: (singleton emptyset) <> emptyset.

Lemma substrate_canonical_doubleton_order:

RR n° 7150
José Grimm

\begin{verbatim}
substrate canonical_doubleton_order = two_points.

Lemma worder_canonical_doubleton_order:
  worder canonical_doubleton_order. (* 23 *)

By considering the least element of the doubleton \{x, y\}, one deduces that a well-ordering is a total ordering. Every subset that is bounded above has a least upper bound. A subset of a well-ordered set is well-ordered. Adjoining a greatest element to a well-ordered set gives a well-ordered set. A nonempty well-ordered set has a least element.

Lemma worder_total:forall r, worder r -> total_order r.
Lemma worder_hassup:forall r A, worder r -> sub A (substrate r) ->
  bounded_above r A -> has_supremum r A.
Lemma induced_trans:forall r x y,
  order r -> sub x y -> sub y (substrate r) ->
  induced_order r x = induced_order (induced_order r y) x.
Lemma worder_restriction:forall r A, worder r -> sub A (substrate r) ->
  worder (induced_order r A).
Lemma worder_adjoin_greatest:forall r a, worder r -> ~ (inc a (substrate r))
  -> worder (order_with_greatest r a). (* 23 *)
Lemma worder_least:forall r, worder r -> nonempty (substrate r) ->
  exists y, least_element r y.

Some useful small lemmas. If \leq is a relation on E, then \lt means \leq and \neq. Thus \lt is false and \leq and \lt implies that \leq and \lt are in E. If we have a total order on E, if \in E and \in E then \lt or \leq; in the case of an order, one of these relations is false.

Lemma inc_lt1_substrate:forall r x y, glt r x y -> inc x (substrate r).
Lemma inc_lt2_substrate:forall r x y, glt r x y -> inc y (substrate r).
Lemma not_le_gt:forall r x y, order r -> gle r x y -> glt r y x -> False.
Lemma not_lt_self:forall r x, glt r x x -> False.

Consider two strictly increasing functions f and g, with the same source and range. These functions are equal provided that the source is well-ordered (on \Z, the mapping \(x \mapsto x + 1\) is a strictly increasing bijection, different from the identity, so that the condition on the order is necessary). Assume \(f \neq g\), and let \(x\) be the smallest element such that \(f(x) \neq g(x)\). Since \(f(x)\) is in the range of \(g\), there is \(z\) such that \(f(x) = g(z)\). If \(z < x\) then \(f(z) < f(x) = g(z)\), contradicting the definition of \(x\). Since the source is totally ordered, we get \(x < z\) (since \(x \neq z\)), hence \(g(x) < g(z) = f(x)\). Since \(g(x)\) is in the range of \(f\), the same argument gives \(f(x) < g(x)\), absurd.

Lemma strict_increasing_extens: forall f g r r',
  strict_increasing_fun f r r' -> strict_increasing_fun g r r' ->
  range (graph f) = range (graph g) ->
  f = g. (* 33 *)

A segment \(S\) in an ordered set \(E\) is such that, if \(x \in S\) and \(y \in E\) and \(y \leq x\), then \(y \in S\). Note that if \(E\) is the substrate of \(\leq\) then \(y \leq x\) implies \(y \in E\). An interval of the form \([-, x]\) is a segment; it will be denoted by \(S_x\), and is called the segment with endpoint \(x\). The interval \([-, x]\) will be called the closed segment.

Definition is_segment r s :=
  sub s (substrate r) & forall x y, inc x s -> gle r y x -> inc y s.
Definition segment r x := interval_uo r x.
Definition segment_c r x := interval_uc r x.
\end{verbatim}
The 20-some following lemmas sometimes assume that we have an order \( \leq \) on \( E \), and that \( S \) is a segment. We assume \( x' \in E \). They state that if \( x \in S \) and \( y < x \) then \( y \in S \). If \( y \in [\neg, x] \) then \( y \in S \). We have \( S \subseteq E \). We have \( |\neg, x| \subseteq E \). We have \( x \notin |\neg, x'| \). We have \( y < x' \) if and only if \( y \in |\neg, x'| \). We have \( |\neg, x'| = |\neg, x'| \cup \{x'\} \). We have \( |\neg, x'| \subseteq F \), where the notation \( W \) means that we restrict \( \leq \) to \( F \). The empty set and \( E \) are segments. Intersections and unions of segments are segments. If \( S' \) is a segment for the order induced on \( S \), then \( S' \) is a segment. Finally \( |\neg, x'| \) is a segment.

**Lemma** \( \text{lt\_in\_segment} \): \( \forall r, s, x, y, \text{is\_segment } r, s \rightarrow \text{inc } x, s \rightarrow \text{glt } r, y, x \rightarrow \text{inc } y, s \).

**Lemma** \( \text{inc\_segment} \): \( \forall r, x, y, \text{inc } y, (\text{segment } r, x) \rightarrow \text{glt } r, y, x \).

**Lemma** \( \text{not\_in\_segment} \): \( \forall r, x, \text{inc } x, (\text{segment } r, x) \rightarrow \text{False} \).

**Lemma** \( \text{sub\_segment} \): \( \forall r, x, \text{sub } (\text{segment } r, x) \rightarrow (\text{substrate } r) \).

**Lemma** \( \text{sub\_segment1} \): \( \forall r, s, \text{is\_segment } r, s \rightarrow \text{sub } s, (\text{substrate } r) \).

**Lemma** \( \text{sub\_segment2} \): \( \forall r, x, y, \text{sub } (\text{induced\_order } r, x, y) \rightarrow \text{y} \).

**Lemma** \( \text{segment\_inc} \): \( \forall r, x, y, \text{inc } x, (\text{substrate } r) \rightarrow \text{glt } r, y, x \rightarrow \text{inc } y, (\text{segment } r, x) \).

**Lemma** \( \text{segment\_rw} \): \( \forall r, x, y, \text{inc } y, (\text{substrate } r) \rightarrow \text{inc } y, (\text{segment } r, x) = \text{glt } r, y, x \).

**Lemma** \( \text{segment\_c\_rw} \): \( \forall r, x, y, \text{inc } y, (\text{substrate } r) \rightarrow \text{inc } y, (\text{segment\_c } r, x) = \text{gle } r, y, x \).

**Lemma** \( \text{inc\_bound\_segmentc} \): \( \forall r, x, \text{order } r \rightarrow \text{inc } x, (\text{substrate } r) \rightarrow \text{inc } x, (\text{segment\_c } r, x) \).

**Lemma** \( \text{sub\_segmentc} \): \( \forall r, x, \text{sub } (\text{segment\_c } r, x) \rightarrow (\text{substrate } r) \).

**Lemma** \( \text{segment\_c\_pr} \): \( \forall r, x, \text{order } r \rightarrow \text{inc } x, (\text{substrate } r) \rightarrow \text{tack\_on } (\text{segment } r, x) = \text{segment\_c } r, x \).

**Lemma** \( \text{empty\_is\_segment} \): \( \forall r, \text{is\_segment } r, \text{emptyset} \).

**Lemma** \( \text{substrate\_is\_segment} \): \( \forall r, \text{order } r \rightarrow \text{is\_segment } r, \text{substrate } r \).

**Lemma** \( \text{intersection\_is\_segment} \): \( \forall r, s, \text{order } r \rightarrow \text{nonempty } s \rightarrow (\forall x, \text{inc } x, s \rightarrow \text{is\_segment } r, x) \rightarrow \text{is\_segment } r, (\text{intersection } s) \).

**Lemma** \( \text{union\_is\_segment} \): \( \forall r, s, \text{order } r \rightarrow (\forall x, \text{inc } x, s \rightarrow \text{is\_segment } r, x) \rightarrow \text{is\_segment } r, (\text{union } s) \).

**Lemma** \( \text{union\_f\_is\_segment} \): \( \forall r, j, s, \text{order } r \rightarrow (\forall x, \text{inc } x, j \rightarrow \text{is\_segment } r, x) \rightarrow \text{is\_segment } r, (\text{union\_f } j, s) \).

**Lemma** \( \text{subsegment\_is\_segment} \): \( \forall r, s, s', \text{order } r \rightarrow \text{is\_segment } r, s, \text{order } r \rightarrow \text{is\_segment } r, s', \text{order } r \rightarrow \text{is\_segment } r, (\text{induced\_order } r, s) s' \rightarrow \text{is\_segment } r, s' \).

**Lemma** \( \text{segment\_is\_segment} \): \( \forall r, x, \text{order } r \rightarrow \text{inc } x, (\text{substrate } r) \rightarrow \text{is\_segment } r, (\text{segment } r, x) \).

Proposition 1 [2] p. 149] is the converse of the previous lemma. In a well-ordered set, a segment is either the whole set or of the form \( S_x = [a, x] \); hence in a well-ordered set \( E \), a segment \( S \) is either \( E \), or else \( E \) is not empty, has a least element \( a \) and \( S = [a, x] \).

**Theorem** \( \text{well\_ordered\_segment} \): \( \forall r, s, \text{worder } r \rightarrow \text{is\_segment } r, s \rightarrow s = \text{substrate } r \setminus (\text{exists } x, \text{inc } x, (\text{substrate } r) \& s = \text{segment } r, x) \). (* 15 *)

**Lemma** \( \text{segment\_alt} \): \( \forall r, x, a, \text{order } r \rightarrow \text{least\_element } r, a \rightarrow \text{segment } r, x = \text{interval\_co } r, a, x \).

**Lemma** \( \text{segment\_alt1} \): \( \forall r, s, \text{worder } r \rightarrow \text{is\_segment } r, s \rightarrow s = \text{substrate } r \setminus (\text{exists } x, \text{exists } a, s = \text{interval\_co } r, a, x) \).

Some useful lemmas. We consider a well-ordered set. If \( S \) and \( S' \) are segments, then \( S \subseteq S' \) or \( S' \subseteq S \). If \( S \subseteq S' \), if \( x \in S \), the segments with endpoint \( x \) in \( S \) or \( S' \) coincide. If \( x \leq y \), then
$S_x \subset S_y$ and $S_x \times S_x \subset S_y \times S_y$. If $z \leq y$ and $y \in S_x$ then $z \in S_x$. The set $\{ - ,y \}$ is a segment. If $S$ is a segment and $x \in S$, then $S_x$ is the segment with endpoint $x$ for the order induced on $S$. It is also the segment with endpoint $x$ for the order induced on $\{ - ,y \}$ or $\{ - ,y \}$ if $x < y$.

Lemma segment_dichot_sub: forall $r \ x \ y$, 
\[ \text{worder } r \rightarrow \text{is_segment } r \ x \rightarrow \text{is_segment } r \ y \rightarrow \]
\[ \text{(sub } x \ y \lor \text{ sub } y \ x). \]

Lemma segments_induced_order: forall $r \ s' \ s'' \ x$, 
\[ \text{worder } r \rightarrow \text{is_segment } r \ s' \rightarrow \text{is_segment } r \ s'' \rightarrow \text{sub } s' \ s'' \rightarrow \text{inc } x \ s' \rightarrow \]
\[ \text{segment } (\text{induced_order } r \ s') \ x = \text{segment } (\text{induced_order } r \ s'') \ x. \]

Lemma segment_monotone: forall $r \ x \ y$, order $r \rightarrow \text{gle } r \ x \ y \rightarrow \]
\[ \text{sub } (\text{segment } r \ x) \ (\text{segment } r \ y). \]

Lemma le_in_segment: forall $r \ x \ y \ z$, worder $r \rightarrow \text{inc } x \ (\text{substrate } r) \rightarrow \]
\[ \text{inc } y \ (\text{segment } r \ x) \rightarrow \text{gle } r \ x \ y \rightarrow \text{inc } z \ (\text{segment } r \ x). \]

Lemma coarse_segment_monotone: forall $r \ x \ y$, worder $r \rightarrow \text{gle } r \ x \ y \rightarrow \]
\[ \text{sub } (\text{coarse } (\text{segment } r \ x)) \ (\text{coarse } (\text{segment } r \ y)). \]

Lemma tack_on_segment: forall $r \ x$, 
\[ \text{worder } r \rightarrow \text{inc } x \ (\text{substrate } r) \rightarrow \]
\[ \text{is_segment } r \ (\text{segment } c \ r \ x). \]

Lemma segment_induced_a: forall $r \ s \ x$, 
\[ \text{worder } r \rightarrow \text{is_segment } r \ s \rightarrow \text{inc } x \ s \rightarrow \]
\[ \text{segment } (\text{induced_order } r \ s) \ x = \text{segment } r \ x. \]

Lemma segment_induced: forall $r \ x \ x_0$, worder $r \rightarrow \text{glt } r \ x_0 \ x \rightarrow \]
\[ \text{segment } (\text{induced_order } r \ (\text{segment } r \ x)) \ x_0 = \text{segment } r \ x_0. \]

Lemma segment_induced1: forall $r \ x \ x_0$, worder $r \rightarrow \text{glt } r \ x_0 \ x \rightarrow \]
\[ \text{segment } (\text{induced_order } r \ (\text{segment } c \ r \ x)) \ x_0 = \text{segment } r \ x_0. \]

In a totally ordered set $E$, the union of all segments is $E$ minus its greatest elements (there is at most one such element). In fact the union is the set of all $x$ for which there is a $y$ such that $x < y$ (remember that $x \leq y$ implies $x \in E$ and $y \in E$).

Lemma union_segments: forall $r$, total_order $r$ \rightarrow \]
\[ \text{let } E := \text{substrate } r \text{ in} \]
\[ \text{let } A := \text{union } (\text{fun_image } E \ (\text{fun } x \rightarrow \text{segment } r \ x))) \text{ in} \]
\[ (\forall x, \neg (\text{greatest_element } r \ x) \rightarrow A = E) \]
\[ k (\forall x, \text{greatest_element } r \ x \rightarrow A = \text{complement } E \ (\text{singleton } x)). \]

If $\{ - ,x[= ]\rightarrow \}, y[\text{then } x = y \text{ if } x < y, \text{then } x \in ]\rightarrow, y[ \text{et } x \notin ]\rightarrow, x\}$.

Lemma segment_injective: forall $r \ x \ y$, total_order $r$ \rightarrow \]
\[ \text{inc } x \ (\text{substrate } r) \rightarrow \text{inc } y \ (\text{substrate } r) \rightarrow \text{segment } r \ x = \text{segment } r \ y \rightarrow \]
\[ x = y. \]

Lemma segment_injective1: forall $r \ x \ y$, worder $r$ \rightarrow \]
\[ \text{inc } x \ (\text{substrate } r) \rightarrow \text{inc } y \ (\text{substrate } r) \rightarrow \text{segment } r \ x = \text{segment } r \ y \rightarrow \]
\[ x = y. \]

Assume that $E$ is well-ordered. The mapping $x \rightarrow S_x$ is a bijection on the set $E^* \setminus \{E\}$ where $E^*$ is the set of all segments of $E$. This mapping is an order isomorphism. From this, we deduce that $E^* \setminus \{E\}$, hence $E^*$, is well-ordered. This is Proposition 2 in [2, p. 149].

Definition set_of_segments_strict $r$= \]
\[ \text{fun_image } (\text{substrate } r) \ (\text{fun } x \rightarrow \text{segment } r \ x). \]

Definition set_of_segments $r$= \]
\[ \text{tack_on } (\text{set_of_segments_strict } r) \ (\text{substrate } r). \]

Definition set_of_segments_iso $r$= \]

INRIA
Lemma BL(segment r) (substrate r) (set_of_segments_strict r).

Lemma is_segment r x = inc x (set_of_segments r).
Lemma sub_set_of_segments: forall r x, worder r ->
  inc x (set_of_segments r) -> sub x (substrate r).
Lemma set_of_segments_axiom: forall r, worder r ->
  transf_axioms (segment r) (substrate r) (set_of_segments_strict r).
Lemma bijective_set_of_segments_iso: forall r, worder r ->
  bijective (set_of_segments_iso r).
Theorem isomorphism_set_of_segments_iso:forall r, worder r ->
  order_isomorphism (set_of_segments_iso r) r
  (inclusion_suborder (set_of_segments_strict r)).

Theorem set_of_segments_worder: forall r, worder r ->
  worder (inclusion_suborder (set_of_segments r)). (* 64 *)

We state Lemma 1 [2, p. 150]. Let \((X_\alpha)_{\alpha \in A}\) be a family of ordered sets, directed with respect to the relation \(\subset\). Suppose that, for each pair of indices \((\alpha, \beta)\) such that \(X_\alpha \subset X_\beta\), the ordering induced on \(X_\alpha\) by that of \(X_\beta\) is identical with the given ordering on \(X_\alpha\). Under these conditions there exists a unique ordering on then set \(E = \bigcup_{\alpha \in A} X_\alpha\) which induces the given ordering on each \(X_\alpha\). In the lemma that follows, \(g\) is the family of orders \((G_\alpha)\) and the resulting order is the union of the family.

Definition common_prolongation_order g h:=
  order h & substrate h = unionf (domain g) (fun a => (substrate (V a g))) &
  (forall a, inc a (domain g) -> V a g = induced_order h (substrate (V a g))).
Definition common_prolongation_order_axiom g :=
  fgraph g &
  (forall x, inc x (domain g) -> order (V x g)) &
  (forall a b, inc a (domain g) -> inc b (domain g) -> exists c,
    inc c (domain g) & sub (substrate (V a g)) (substrate (V c g)) &
    sub (substrate (V b g)) (substrate (V c g))) &
  (forall a b, inc a (domain g) -> inc b (domain g) ->
    sub (substrate (V a g)) (substrate (V b g)) ->
    V a g = induced_order (V b g) (substrate (V a g))).

Lemma order_merge1: forall g, common_prolongation_order_axiom g ->
  common_prolongation_order g (unionb g). (* 34 *)
Lemma order_merge2: forall g h1 h2, common_prolongation_order_axiom g ->
  common_prolongation_order g h1 ->
  common_prolongation_order g h2 -> (h1 = h2).

We consider now Proposition 3 [2, p. 149]. It says \((X_\iota)_{\iota \in I}\) be a family of well-ordered sets such that for each pair of indices \((\iota, \kappa)\) one of the sets \(X_\iota, X_\kappa\) is a segment of the other. Then there exists a unique ordering on the set \(E = \bigcup_{\iota \in I} X_\iota\) which induces the given ordering on each of the \(X_\iota\). Endowed with this ordering, \(E\) is a well-ordered set. Every segment of \(X_\iota\) is a segment of \(E\); for each \(x \in X_\iota\), the segment with endpoint \(x\) in \(X_\iota\) is equal to the segment with endpoint \(x\) in \(E\); and each segment of \(E\) is either \(E\) itself or a segment of one of the \(X_\iota\). Note that if \(X_\alpha = X_\beta\), then each set is a segment of the other; the orderings \(G_\alpha\) and \(G_\beta\) may differ, in which case (since orders are total) there is a pair \((x, y)\) such that \(x < y\) for one order and \(y < x\) for the other one, and no compatible order exists on the union. Thus an additional condition is needed (the same one as in the previous lemma). With this definition, the next lemmas become trivial.
Definition common_worder_axiom g :=
  fgraph g &
  (forall x, inc x (domain g) -> worder (V x g)) &
  (forall a b, inc a (domain g) -> inc b (domain g) ->
    is_segment (V a g) (substrate (V b g))
  \ /
  is_segment (V b g) (substrate (V a g))) &
  (forall a b, inc a (domain g) -> inc b (domain g) ->
    sub (substrate (V a g)) (substrate (V b g)) ->
    V a g = induced_order (V b g) (substrate (V a g))).

Lemma order_merge3: forall g,
  common_worder_axiom g -> common_prolongation_order_axiom g.

Lemma order_merge4: forall g,
  common_worder_axiom g -> common_prolongation_order g (unionb g).

Lemma order_merge5: forall g h1 h2, common_worder_axiom g ->
  common_prolongation_order g h1 ->
  common_prolongation_order g h2 -> (h1 = h2).

Theorem worder_merge: forall g, common_worder_axiom g ->
  ( (common_prolongation_order g (unionb g)) &
    worder (unionb g) &
  (forall a x, inc a (domain g) -> is_segment (V a g) x
  -> is_segment (unionb g) x ) &
  (forall a x, inc a (domain g) -> inc x (substrate (V a g)) ->
    segment (V a g) x = segment (unionb g) x) &
  (forall x, is_segment (unionb g) x ->
    x = substrate (unionb g) \/
    exists a, inc a (domain g) & is_segment (V a g) x)). (* 54 *)

3.2 The principle of transfinite induction

The next result is Lemma 2 [2, p. 151]. It says that, given a well-ordered set E and a set $\mathcal{S}$ of segments of E, all segments are in $\mathcal{S}$ if $\mathcal{S}$ is stable by union and by adjunction of a greatest element (i.e., if the segment $S_x$ belongs to $\mathcal{S}$ then $S_x \cup \{x\}$ belongs to $\mathcal{S}$). As a consequence, the substrate of the order is in $\mathcal{S}$.

Lemma transfinite_principle1: forall r s,
  worder r -> (forall x, inc x s -> is_segment r x) ->
  (forall s', sub s' s -> inc (union s') s) ->
  (forall x, inc x (substrate r) -> inc (segment r x) s
  -> inc (segment_c r x) s) ->
  (forall x, is_segment r x -> inc x s). (* 42 *)

Lemma transfinite_principle2: forall r s,
  worder r -> (forall x, inc x s -> is_segment r x) ->
  (forall s', sub s' s -> inc (union s') s) ->
  (forall x, inc x (substrate r) -> inc (segment r x) s
  -> inc (segment_c r x) s) ->
  inc (substrate r) s.

Let $H(x)$ be the assumption: “$x \in E$, and for all $y \in E$ such that $y < x$, then $p(y)$ is true”. Assume that $\leq$ is a well-ordering on E. Assume that, for all $x$, $H(x)$ is true; then $p(x)$ is true. This is C59 (“Principle of transfinite induction”), [2, p. 151]. The Bourbaki Proof is the following: because of the previous lemma, the set of segments $S$ such that $p$ is true on $S$ contains
E. Other proof: the assumption say that the set of elements not satisfying \( p \) has no least element.

**Theorem transfinite_principle:** \( \forall r \ (p: E \times P), \ \)  
worder \( r \to \)  
(\( \forall x, \) inc \( x \) (substrate \( r \)) \to \)  
(\( \forall y, \) inc \( y \) (substrate \( r \)) \to glt \( r \) \( y \) \( x \) \to \( p \) \( y \))  
\( \to \) \( p \) \( x \))  
\( \to \) \( \forall x, \) inc \( x \) (substrate \( r \)) \to \( p \) \( x \)).

We now define a mapping by transfinite induction. We consider a well-ordered set \( E \), a function \( g \), and an element \( x \in E \). Let \( g^{(x)} \) denote the restriction of \( g \) to \( \{ x \} \) as a surjective function.

**Definition restriction_to_segment \( r \times g := \)  
restriction1 \( g \) (segment \( r \times x \)).**

**Definition restriction_to_segment_axiom \( r \times g := \)  
worder \( r \) & inc \( x \) (substrate \( r \)) & is_function \( g \) & sub (segment \( r \times x \)) (source \( g \)).**

**Lemma sub_image_target:** \( \forall g \ x, \) is_function \( g \to \)  
sub (image_by_fun \( g \) \( x \)) (target \( g \)).

**Lemma function_rts:** \( \forall r \times g, \) restriction_to_segment_axiom \( r \times g \to \)  
is_function (restriction_to_segment \( r \times g \)).

**Lemma W_rts:** \( \forall r \times g a, \) restriction_to_segment_axiom \( r \times g \to \)  
glt \( r \) \( a \) \( x \) \to \( W \ a \) (restriction_to_segment \( r \times g \)) = \( W \ a \) \( g \).

**Lemma surjective_rts:** \( \forall r \times g, \) restriction_to_segment_axiom \( r \times g \to \)  
surjective (restriction_to_segment \( r \times g \)).

**Lemma rts_extensionality:** \( \forall r \ s \ x \ f \ g, \)  
worder \( r \to \) inc \( x \) (substrate \( r \)) \to \( \) worder \( s \to \) inc \( x \) (substrate \( s \)) \to \)  
segment \( r \times x = \) segment \( s \times x \) RA  
is_function \( f \to \) sub (segment \( r \times x \)) (source \( f \)) \to \)  
is_function \( g \to \) sub (segment \( s \times x \)) (source \( g \)) \to \)  
(forrall \( a \), inc \( a \) (segment \( r \times x \)) \to \( W \ a \ f = W \ a \) \( g \)) \to \)  
restriction_to_segment \( r \times f = \) restriction_to_segment \( s \times g \)).

We can now state Criterion C60 (Definition of a mapping by transfinite induction) \( \{2, p. 151\} \): Let \( u \) be a letter, \( T \) a term in the theory \( T \) (in which \( E \) is a set well-ordered by a relation denoted \( \leq \)). There exists a set \( U \) and a mapping \( f \) of \( E \) onto \( U \) such that for all \( x \in E \) we have \( f(x) = T(f^{(x)}) \). Furthermore the set \( U \) and the mapping \( f \) are uniquely determined by these conditions.

We shall denote by \( f^{(x)}_S \) the restriction of \( f \) to the segment \( x \) for the ordering \( S \) (more precisely, the ordering induced on \( S \) by the given ordering). Let's denote by \( S(T, f) \) the property of the criterion, namely, that \( f \) is a surjective function defined on \( S \) such that \( f(x) = T(f^{(x)}) \) for every \( x \in S \).

Assume that \( S(E, T, f) \) and \( S(E, T, f') \) are true. Assume \( x \in E \), \( f \) and \( f' \) agree on \( S_x \). Then \( f^{(x)}_E = f'^{(x)}_E \) (the functions have the same target, because they are surjective, and take the same value). By assumption, \( T(f^{(x)}_E) = T(f'^{(x)}_E) \), so that \( f \) and \( f' \) agree on \( S_x \cup \{x\} \) (this transfinite_unique1). We consider the set of all segments \( \mathcal{S} \) on which \( f \) and \( f' \) agree. This set is clearly stable by union, and we have seen that, if it contains \( S_x \), then it contains \( S_x \cup \{x\} \). Hence it contains \( E \). Since \( f \) and \( f' \) agree on \( E \), they are equal (same reasoning as above).

Assume now that \( S'(S', T, f') \) and \( S''(S'', T, f'') \) are true, and \( S' \) and \( S'' \) are segments such that \( S' \subset S'' \). Let \( f \) be the restriction of \( f'' \) on \( S' \). This is a surjective function. We have
\[ f^{(x)}_{S'} = f^{(x)}_{S''} \] (because the functions are surjective and take the same values on \( S' \)). We have \[ f^{(x)}_{S} = f^{(x)}_{S'} \] because these are two restrictions to identical segments. We have \( f(x) = f''(x) \).

Assumption \( \mathcal{I}(S'', T, f'') \) gives thus \( f(x) = T f^{(x)}_{S'} \), in other words, \( \mathcal{I}(S', T, f) \), hence \( f = f' \) by uniqueness. This is transfinite_aux1.

Assume we have a set of segments \( \mathcal{S} \) and, for \( S \in \mathcal{S} \), we have a function \( f_S \) such that \( \mathcal{I}(s, T, f_S) \). We use our axiom of choice to select such a function \( f_S \). Let \( t \) be the union of the targets of the functions \( f_S \), and let \( g_T \) be the function that has the same source as \( f_S \) (namely \( s \)), same graph as \( f_S \), but target \( t \). If \( s \) and \( s' \) are two segments, we have \( s \subset s' \) or \( s' \subset s \); in the first case \( g_T \) and \( g_{s' \subset s} \) agree on \( s \) (previous result). By symmetry \( g_T \) and \( g_{s' \subset s} \) agree on \( s' \) in the other case. Using prolongation_covering, we get a function \( g \) that coincides with every \( g_T \). The target of this function is \( t \), so that the function is surjective. Assume \( x \in S \) and \( S \in \mathcal{S} \). We have \( g(x) = f_S(x) \) because \( f_S(x) = g_S(x) \). Thus the quantities \( g_T^{(x)} \) and \( f_S^{(x)} \) are well defined and equal. We have \( f^{(x)}_{S'} = f^{(x)}_{S''} \) because these two functions are restriction of \( f_S \) to the segment defined by \( x \), and whether this segment is defined by the ordering on \( t \) or \( S \) is irrelevant (we have \( x \in S \subset t \)). We have \( f_S(x) = T f^{(x)}_{S'} \) by assumption. Thus \( g(x) = T f^{(x)}_{S'} \). This means that \( \mathcal{I}(t, T, g) \) is true. This is transfinite_aux2. We changed a bit the theorem; initially it was: if, for \( S \in \mathcal{S} \), there exists a function \( f \) such that \( \mathcal{I}(s, T, f) \), there is a function \( g \) such that \( \mathcal{I}(t, T, g) \).

It is now: given functions \( f_S \) such that \( \mathcal{I}(s, T, f) \), there exists a function \( g \) such that \( \mathcal{I}(t, T, g) \) whose target is the union of the targets of the functions \( f_S \) (this target has to be the union, by uniqueness).

Assume now that \( \mathcal{I}(S_T, T, f) \). Let’s extend \( f \) to \( f' \) via to \( S_T \cup \{ y \} \) via the formula \( f'(y) = T f(y) \). This function takes the same values as \( f \) on subsets of \( S_T \) hence \( f'(x) = T f^{(x)}_{S_T} \) for every \( x \in S_T \). The formula is also true for \( y = x \), hence \( \mathcal{I}(S_T \cup \{ y \}, T, f') \). These facts allow us to use the transfinite induction principle, to show the existence of a function defined everywhere. Assume that for some \( F \) we have \( T f | u | \in F \). If we change the definition of \( \mathcal{I}(S, T, f) \) by adding the condition that the target of \( f \) is a subset of \( F \), we can easily show that the target of the unique function defined by transfinite induction is a subset of \( F \).

Definition transfinite_def r p f :=
  surjective f & source f = substrate r &
  forall x, inc x (substrate r) -> \( \mathcal{W} x f = p \) (restriction_to_segment r x f).

Definition transfinite_defined r p := choosef (fun f => transfinite_def r p f).

Lemma transfinite_unique1: forall r p f f' z, worder r ->
  inc z (substrate r) ->
  transfinite_def r p f -> transfinite_def r p f' ->
  (forall x : Set, inc x (segment r z) -> \( \mathcal{W} x f = \mathcal{W} x f' \)) ->
  restriction_to_segment r z f = restriction_to_segment r z f'.

Lemma transfinite_unique: forall r p f f', worder r ->
  transfinite_def r p f -> transfinite_def r p f' -> f = f'. (* 21 *)

Lemma transfinite_pr: forall r x p, worder r -> transfinite_def r p x ->
  transfinite_defined r p = x.

Lemma transfinite_aux1: forall r p s' s'' f' f'',
  worder r -> is_segment r s' -> is_segment r s'' -> sub s' s'' ->
  transfinite_def (induced_order r s') p f' ->
  transfinite_def (induced_order r s'') p f'' ->
  f'' = restriction1 f' s'. (* 26 *)

(* old version
Lemma transfinite_aux2: forall r p s, worder r -> (* 70 *)

INRIA
Lemma transfinite_aux2: forall r p s tdf, worder r -> (* 67 *)
(forall z, inc z s -> is_segment r z) ->
(forall z, inc z s -> transfinite_def (induced_order r z) p (tdf z)) ->
exists f : correspondenceC, (transfinite_def (induced_order r (union s)) p f &
  target f = unionf s (fun z => target (tdf z))).

Lemma transfinite_aux3: forall r p x g,
  worder r -> inc x (substrate r) ->
  transfinite_def (induced_order r (segment r x)) p g
  -> transfinite_def (induced_order r (segment_c r x)) p (tack_on_f g x (p (restriction_to_segment r x g))). (* 37 *)

Theorem transfinite_definition: forall r p,
  worder r -> exists_unique (fun f => transfinite_def r p f).

Lemma transfinite_defined_pr: forall r p, worder r ->
  transfinite_def r p (transfinite_defined r p).

Theorem transfinite_definition_stable: forall r p F,
  worder r ->
  (forall f, is_function f -> is_segment r (source f) -> sub (target f) F ->
    inc (p f) F) ->
  sub (target (transfinite_defined r p)) F. (* 35 *)

3.3 Zermelo's theorem

We show here that every set is the substrate of a well-ordering. This requires quite a number of small results. Consider two well-orderings, $\Gamma$ and $\Gamma'$ on $E$ and $E'$; denote by $S_x$ and $S'_x$ the segments with endpoints $x$ in $\Gamma$ and $\Gamma'$ (these are subsets of $E$ and $E'$). Let $V$ be the set of all $x \in E \cap E'$ such that $S_x = S'_x$ and $(S_x \times S_x) \cap \Gamma = (S'_x \times S'_x) \cap \Gamma'$; the last condition says that $\Gamma$ and $\Gamma'$ induce the same ordering on $S_x$. This set is a segment for $\Gamma$ and $\Gamma'$, and both orderings coincide.

Definition common_ordering_set r r' :=
Zo (intersection2 (substrate r) (substrate r'))
  (fun x => segment r x = segment r' x &
    induced_order r (segment r x) = induced_order r' (segment r' x)).

Lemma Zermelo_aux0: forall r r',
  common_ordering_set r r' = common_ordering_set r' r.
Lemma Zermelo_aux1: forall r r', worder r -> worder r' ->
  is_segment r (common_ordering_set r r').
Lemma Zermelo_aux2: forall r r' v, worder r -> worder r' ->
  v = common_ordering_set r r' -> sub(induced_order r v)(induced_order r' v).

Let $Q(\Gamma)$ denote the following property: $\Gamma$ is a well-ordering of a subset of $E$, and if $S_x$ denotes the segment of $\Gamma$ with endpoint $x$, we have $S_x \in \mathcal{S}$ and $p(S_x) = x$. RR n° 7150
Definition Zermelo_axioms E p s r :=
  worder r &
  sub (substrate r) E &
  (forall x, inc x (substrate r) -> inc (segment r x) s) &
  (forall x, inc x (substrate r) -> p (segment r x) = x).

Let \( q(\Gamma, \Gamma') \) be the property that, if \( E \) and \( E' \) are the substrates of \( \Gamma \) and \( \Gamma' \), then \( E \subseteq E' \), \( E \) is a segment of \( \Gamma' \), and \( \Gamma \) is the ordering induced by \( \Gamma' \) on \( E \). We pretend that if \( Q(\Gamma) \) and \( Q(\Gamma') \) are true, then either \( q(\Gamma, \Gamma') \) or \( q(\Gamma', \Gamma) \) is true. The previous lemmas show that this is true if \( V \) is either \( E \) or \( E' \). Otherwise, we may consider \( x \) and \( x' \) the smallest element of \( E \) or \( E' \) not in \( V \), so that \( V = S_x \) and \( V = S_{x'} \) (for the orderings \( \Gamma \) and \( \Gamma' \)). By application of \( p \) we get \( x = x' \). This implies \( x \in V \), absurd.

Lemma Zermelo_aux3: forall E s p r r',
  let q := fun r r' => sub (substrate r) (substrate r')
  & r = induced_order r' (substrate r) & is_segment r' (substrate r) in
  Zermelo_axioms E p s r -> Zermelo_axioms E p s r' ->
  q r r' / q r' r.

Let \( \Gamma \) be a well-ordering and \( x \) an element not in the substrate. We can extend \( \Gamma \) as \( \Gamma' \) by adjoining \( x \) as greatest element. This is a well-ordering, a segment of this order is either the substrate of \( \Gamma' \), the substrate of \( \Gamma \), or a segment \( S_x \) of \( \Gamma \).

Lemma Zermelo_aux4: forall r a, worder r ->
  let owg := order_with_greatest r a in
  ~(inc a (substrate r)) ->
  (worder owg & segment owg a = (substrate r) &
   forall x, inc x (substrate owg) -> x = a \/
   segment owg x = segment r x). (* 13 *)

Let \( E \) be a set, \( S \) a part of \( \wp(E) \) and \( p \) a function from \( S \) into \( E \) such that \( p(X) \notin X \). Consider \( M \), the set of orderings \( \Gamma \) that satisfy property \( Q \); by virtue of Zermelo_aux3, there is a well-ordering \( \Gamma \) (the union of the elements of \( M \)) that extends the orderings of \( M \). It satisfies \( Q \). Its substrate \( M \) is not in \( S \). Proof: if \( M \in S \), and \( a = p(M) \), we know \( a \notin M \), so that we can extend \( \Gamma \) to \( \Gamma' \) by adjoining \( a \) as greatest element. This new order satisfies \( Q \) (for all \( y, S_y \in S \) and \( p(S_y) = y \); this is true if \( y \) is in the support of \( \Gamma \), otherwise \( y = a \) and \( S_a = M \in S \), \( p(S_a) = p(M) = a \)). This means that the new order is in \( M \), its support is a subset of \( M \), and \( a \in M \), absurd.

Lemma Zermelo_aux: forall E s p, sub s (powerset E) ->
  (forall x, inc x s -> inc (p x) E & - (inc (p x) x)) ->
  exists r, Zermelo_axioms E p s r & ~ (inc (substrate r) s)). (* 52 *)

Let now \( S \) be the set of all subsets of \( E \) but \( E \) itself. If \( p \) is the representative of the complement of \( x \) in \( E \), the order defined by the lemma Zermelo_aux has its substrate in \( \wp(E) - S \). Thus, it is a well-ordering on \( E \). This is Theorem 1 [2, p. 153].

Theorem Zermelo: forall E, exists r, worder r & substrate r = E. (* 17 *)

3.4 Inductive sets

An ordered set is said to be inductive if every totally ordered subset of \( E \) has an upper bound in \( E \). More precisely, let \( r \) be an order and \( E \) its substrate, then every subset \( X \) of \( E \),
for which the order induced by \( r \) is total, has an upper bound for \( r \). The set \( \Phi(A, B) \) of partial functions is inductive, another example is given page 158.

Definition \( \text{inductive\_set\_r} := \)
\[
\forall X, \text{sub} X (\text{substrate} r) \rightarrow \text{total\_order} (\text{induced\_order} r X) \rightarrow \\
\exists x, \text{upper\_bound} r X x.
\]

Lemma \( \text{inductive\_graphs}: \forall a, b, \)
\[
\text{inductive\_set} (\text{opposite\_order} (\text{extension\_order} a b)). (* 32 *)
\]

Consider an ordered set \( E \); assume that each well-ordered subset of \( E \) is bounded above. Let \( p(S) \) be an upper bound of \( S \) that is not in \( S \). Let \( \mathcal{S} \) be the set of sets \( S \subset E \) for such a \( p(S) \) exists. By \( \text{Zermelo\_aux} \), there is \( \Gamma \) that satisfies \( Q \), i.e. \( \Gamma \) is a well-ordering of a subset \( M \) of \( E \), and if \( S_x \) denotes the segment of \( \Gamma \) with endpoint \( x \), we have \( S_x \in \mathcal{S} \) and \( p(S_x) = x \). This last condition says that if \( y < x \) for \( \Gamma \), it is true for the ordering on \( E \); hence \( \Gamma \) is the restriction to \( M \) of the ordering of \( E \). By assumption, \( M \) is bounded, say by \( m \). This element is maximal (this is Proposition 4 [2, p. 154]).

Theorem 2 [2, p. 154] says that every inductive ordered set has a maximal element. This is a trivial consequence of the previous result.

Theorem \( \text{Zorn\_aux}: \forall r, \text{order } r \rightarrow \\
(\forall s, \text{sub} s (\text{substrate} r) \rightarrow \text{worder} (\text{restriction\_order} r s) \rightarrow \\
(\text{bounded\_above} r s) \rightarrow \\
\exists a, \text{maximal\_element} r a). (* 35 *)
\]

Theorem \( \text{Zorn\_lemma}: \forall r, \text{order } r \rightarrow \text{inductive\_set } r \rightarrow \\
\exists a, \text{maximal\_element} r a.
\]

Corollary. If \( E \) is inductive, \( a \in E \), \( F \) is the set of all \( x \geq a \), then \( F \) is inductive (if \( X \) is a totally ordered set in \( F \), then \( X \cup \{a\} \) is totally ordered; an upper bound \( m \) is in \( F \) since it satisfies \( a \leq m \)). Hence there is a maximal element \( m \) such that \( a \leq m \). Second corollary: if \( \mathcal{A} \) is a subset of the powerset of \( E \) such that for every subset \( \mathcal{S} \) of \( \mathcal{A} \) which is totally ordered by inclusion, the union (resp. intersection) of the sets of \( \mathcal{S} \) belongs to \( \mathcal{A} \), then \( \mathcal{A} \) has a maximal or minimal element. The trick with the intersection is that the intersection is not defined if \( \mathcal{S} \) is empty. The set is nevertheless inductive, provided that \( \mathcal{A} \) is not empty (in the case of the union, it contains the empty set).

Lemma \( \text{inductive\_max\_greater}: \forall r, a, \text{order } r \rightarrow \text{inductive\_set } r \rightarrow \\
\text{inc } a (\text{substrate } r) \rightarrow \\
\exists m, \text{maximal\_element } r m \& \text{gle } r a m. (* 26 *)
\]

Lemma \( \text{inductive\_powerset}: \forall A, F, \text{sub } A (\text{powerset } F) \rightarrow \\
(\forall S, (\forall x y, \text{inc } x S \rightarrow \text{inc } y S \rightarrow \text{sub } x y \lor \text{sub } y x) \rightarrow \\
\text{sub } S A \rightarrow \text{inc } (\text{union } S) A) \rightarrow \\
\text{inductive\_set } (\text{inclusion\_suborder } A).
\]

Lemma \( \text{maximal\_in\_powerset}: \forall A, F, \text{sub } A (\text{powerset } F) \rightarrow \\
(\forall S, (\forall x y, \text{inc } x S \rightarrow \text{inc } y S \rightarrow \text{sub } x y \lor \text{sub } y x) \rightarrow \\
\text{sub } S A \rightarrow \text{inc } (\text{union } S) A) \rightarrow \\
\exists a, \text{maximal\_element } (\text{inclusion\_suborder } A) a.
\]

Lemma \( \text{minimal\_in\_powerset}: \forall A, F, \text{sub } A (\text{powerset } F) \rightarrow \text{nonempty } A \rightarrow \\
(\forall S, (\forall x y, \text{inc } x S \rightarrow \text{inc } y S \rightarrow \text{sub } x y \lor \text{sub } y x) \rightarrow \\
\text{sub } S A \rightarrow \text{inc } (\text{intersection } S) A) \rightarrow \\
\exists a, \text{minimal\_element } (\text{inclusion\_suborder } A) a.
3.5 Isomorphisms of well-ordered sets

Assume that $E$ and $F$ are two well-ordered sets. We show Theorem 3 [2, p. 155]: Let $I(u, v, f)$ be the property that $f$ is an order isomorphism from $u$ onto a segment $w$ of $v$. We claim that there exists a unique $f$ such that $I(E, F, f)$, or there exists a unique $f$ such that $I(F, E, f)$. Note: The two cases are not excluded; in that case, $f$ is bijection between $E$ and $F$.

Recall that an order isomorphism is a bijection such that $x \leq y$ is equivalent to $f(x) \leq f(y)$. In the proof of the theorem we use the set $\mathcal{S}$ of triples $(A, B, C)$ associated to a function $f$, satisfying the following properties: The source $A$ of $f$ is a subset of $E$, the target $B$ is the set $F$ (this is also called a partial function from $E$ to $F$). We assume that the source and the range of $f$ are segments of $E$ and $E'$; Finally, we assume that $f$ is an isomorphism onto its range. In other terms, $a \leq b$ is equivalent to $f(a) \leq f(b)$. The definition of order_morphism requires $f$ to be injective. We start with a lemma that says that this condition is not needed.

Lemma order_morphism_pr1: \( \forall f \ r \ r' \in \mathcal{S}, \) \( \text{order} \ r \rightarrow \text{order} \ r' \rightarrow \text{is_function} \ f \rightarrow \text{substrate} \ r = \text{source} \ f \rightarrow \text{substrate} \ r' = \text{target} \ f \rightarrow \forall x \ y, \text{inc} \ x (\text{source} \ f) \rightarrow \text{inc} \ y (\text{source} \ f) \rightarrow \text{gle} \ r \ x \ y = \text{gle} \ r' \ (W \ x \ f) \ (W \ y \ f) \rightarrow \text{order_morphism} \ f \ r \ r'. \)

In order to show uniqueness we start with a lemma: if $f$ is increasing and $g$ is strictly increasing, if the image of $f$ is a segment of $F$, then $f(x) \leq g(x)$ for all $x$. The proof is by contradiction. If $a$ is the smallest element such that $g(a) < f(a)$, since the image of $f$ is a segment there is a $z$ such that $g(a) = f(z)$. Since $f$ is increasing this gives $z < a$, hence $f(z) \leq g(z) < g(a)$, absurd.

Lemma increasing_function_segments: \( \forall r \ r' \ f \ g, \) \( \text{worder} \ r \rightarrow \text{worder} \ r' \rightarrow \text{increasing_fun} \ f \ r \rightarrow \text{strict_increasing_fun} \ g \ r' \rightarrow \text{is_segment} \ r' (\text{range} \ (\text{graph} \ f)) \rightarrow \forall x, \text{inc} \ x (\text{source} \ f) \rightarrow \text{gle} \ r' \ (W \ x \ f) \ (W \ x \ g). \) \[ (* 31 *) \)

Lemma isomorphism_worder_unique: \( \forall r \ r' \ x \ y, \) \( \text{worder} \ r \rightarrow \text{worder} \ r' \rightarrow \text{is_segment} \ r' (\text{range} \ (\text{graph} \ x)) \rightarrow \text{is_segment} \ r' (\text{range} \ (\text{graph} \ y)) \rightarrow \text{order_morphism} \ x \ r \rightarrow \text{order_morphism} \ y \ r' \rightarrow x = y. \)

Lemma induced_order_trans: \( \forall a \ b \ c, \) \( \text{subc} \ b \rightarrow \text{induced_order} \ (\text{induced_order} \ a \ b) \ c = \text{induced_order} \ a \ c. \)

Given a totally ordered subset $X$ of $\mathcal{S}$, we can apply lemma sup_extension_order2, that says that there exists a function $f$ that extends all elements in $X$; we know that the source and range of $f$ are the union of the sources and ranges of the elements of $X$, hence are segments. Given $a$ and $b$ in the source of $f$, there is a function $g$ that is defined for both $a$ and $b$ (because $X$ is totally ordered); since $a \leq b$ is equivalent to $g(a) \leq g(b)$ and $f(a) = g(a)$ and $f(b) = g(b)$ we deduce that $a \leq b$ is equivalent to $f(a) \leq f(b)$. As a consequence, $f$ is increasing and hence is a morphism. Consider now a maximal element $f$. If the source of $f$ is $E$, then $I(E, F, f)$ is true. If the range of $f$ is $F$, then $f^{-1}$ is a bijection from $F$ onto a subset of $E$, hence $I(F, E, f^{-1})$. Otherwise, if $a$ is the smallest element of $E$ not in the source of $f$ and $b$ the smallest element not in the range of $b$, we can extend $f$ to a function $g$ by saying $g(a) = b$. This function is in $\mathcal{S}$. This contradicts the maximality of $f$.

Theorem isomorphism_worder: \( \forall r \ r', \) \[ (* 157 *) \)
worder r -> worder r' ->
let iso:= (fun u v f =>
is_segment v (range (graph f)) & order_morphism f u v)
in exists_unique (fun f => iso r r' f) / exists_unique (fun f => iso r' r f).

Corollary 1. The only isomorphism from a well ordered set into a segment of itself is the identity.

Lemma identity_isomorphism: forall r, order r ->
order_isomorphism (identity_fun (substrate r)) r r.
Lemma identity_morphism: forall r, order r ->
order_morphism (identity_fun (substrate r)) r r.
Lemma unique_isomorphism_onto_segment: forall r f, worder r ->
is_segment r (range (graph f)) -> order_morphism f r r ->
f = identity_fun (substrate r).

Corollary 2. If E and F are two well ordered sets, f an isomorphism of E onto a segment of F, g an isomorphism of F onto a segment of E, then f and g are inverse bijections.

Lemma inverse_order_isomorphism: forall r r' f ,
order_isomorphism f r r' -> order_isomorphism (inverse_fun f) r' r.
Lemma compose_order_isomorphism: forall r r' r'' f f',
composable f' f -> order_isomorphism f r r' -> order_isomorphism f' r' r''
-> order_isomorphism (compose f' f) r r''.
Lemma compose_order_morphism: forall r r' r'' f f',
composable f' f -> order_morphism f r r' -> order_morphism f' r' r''
-> order_morphism (compose f' f) r r''.
Lemma bij_pair_isomorphism_onto_segment: forall r r' f f',
worder r -> worder r' ->
is_segment r' (range (graph f)) -> order_morphism f r r' ->
is_segment r (range (graph f')) -> order_morphism f' r' r
(order_isomorphism f r r' & order_isomorphism f' r' r &
f = inverse_fun f'). (* 35 *)

Finally, we show that every subset of a well-ordered set is isomorphic to a segment of E.

Lemma isomorphic_subset_segment: forall r a,
worder r -> sub a (substrate r) ->
events w, exists f, is_segment r w &
order_isomorphism f (induced_order r a) (induced_order r w). (* 46 *)

3.6 Lexicographic products

Consider the follow definition. We assume that \((X_i)_{i \in I}\) is a family of sets, with domain I, \(g\) is a family of orderings (for each \(i\), \(g_i\) is an ordering on \(f_i\)) and \(r\) is a well-ordering in I. Denote the order relation associated to \(r\) by \(\leq\), and the order relation associated to \(g\) by \(\leq\).
The lexicographic product is the order associated to the relation: \(x\) and \(y\) are elements of the product \(\prod X_\i\), and either \(x = y\), or, if \(i\) is the smallest index (for the relation \(\leq\)) such that \(x_i \neq y_i\) then \(x_i \leq y_i\).

Definition lexicographic_order_r (r f g: Set): EEP :=
fun x x' =>
inc x (productb f) & inc x' (productb f) &
forall j, least_element (induced_order r (Zo (domain f)) (fun i => V i x <> V i x')) j -> glt (V j g) (V j x) (V j x').

Definition lexicographic_order_axioms r f g :=
  worder r & substrate r = domain f &
  fgraph f & fgraph g & domain f = domain g &
  (forall i, inc i (domain f) -> order (V i g)) &
  (forall i, inc i (domain f) -> substrate (V i g) = V i f).

Definition lexicographic_order r f g :=
  graph_on (lexicographic_order_r r f g) (productb f).

It is obvious that the lexicographic product is well-defined; it is a bit more longish to prove that it is an order on the product.

Lemma order_lexproduct_order: forall r f g,
  lexicographic_order_axioms r f g -> order (lexicographic_order r f g).

Lemma related_lexicographic_order: forall r f g x x',
  lexicographic_order_axioms r f g ->
  related (lexicographic_order r f g) x x' =
  (inc x (productb f) & inc x' (productb f) &
   forall j, least_element (induced_order r (Zo (domain f)) (fun i => V i x <> V i x')) j -> glt (V j g) (V j x) (V j x')).

Lemma substrate_lexicographic_order: forall r f g,
  lexicographic_order_axioms r f g ->
  substrate(lexicographic_order r f g) = productb f.

If all orders are total so is the lexicographic product.

Lemma total_lexicographic_order: forall r f g,
  lexicographic_order_axioms r f g ->
  (forall i, inc i (domain g) -> total_order (V i g)) ->
  total_order(lexicographic_order r f g). (* 23 *)

3.7 Ordinals

What follows is not part of the main text of Bourbaki, but may come from exercises. Recall that the disjoint union of a family of sets \((X_i)_{i \in I}\) is the union of the sets \(X_i \times \{i\}\). If \(x\) is in the union, it has the form \((y, \lambda)\), where \(y \in E_\lambda\), and \(\lambda \in I\). This quantity will be denoted by \(\lambda(x)\).

Assume that we have an order \(\leq\) on \(I\), and an order \(\leq_i\) on each \(X_i\). We can compare two elements via: either \(\lambda(x) < \lambda(y)\), or \(x = (x', \lambda)\) and \(y = (y', \lambda)\) and \(x' \leq_\lambda y'\) in \(E_\lambda\). In some cases, we may assume the base sets non-empty.

Definition ordinal_sum_axioms r f g :=
  order r & substrate r = domain f &
  fgraph f & fgraph g & domain f = domain g &
  (forall i, inc i (domain f) -> order (V i g)) &
  (forall i, inc i (domain f) -> substrate (V i g) = V i f).

Definition ordinal_sum_axioms1 r f g:
  ordinal_sum_axioms r f g & (forall i, inc i (domain f) -> nonempty (V i f)).

Definition ordinal_sum_r (r f g: Set): EEP :=
fun x x' =>
  inc x (disjoint_union f) & inc x' (disjoint_union f) &
  (glt r (Q x) (Q x') \ (Q x = Q x' & gle (V (Q x) g) (P x) (P x'))).

Definition ordinal_sum r f g :=
  graph_on (ordinal_sum_r r f g)(disjoint_union f).

We show here that this induces an order on the disjoint union. This is the ordinal sum of
the family and denoted by \( \sum_{i \in I} X_i \). As is customary, this notation hides the relations \( \leq \) and \( \leq_i \).
Note that the same notation is used for the cardinal of the disjoint union.

Lemma du_index_pr:forall f x, inc x (disjoint_union f) ->
  (inc (Q x) (domain f) & inc (P x) (V (Q x) f) & is_pair x).

Lemma lt_lt_trans: forall r a b c, order r ->
  glt r a b & glt r b c -> glt r a c.

Lemma order_ordinal_sum: forall r f g,
  ordinal_sum_axioms r f g -> order (ordinal_sum r f g).

Lemma related_ordinal_sum_order: forall r f g x x',
  ordinal_sum_axioms r f g ->
  related (ordinal_sum r f g) x x' =
  (inc x (disjoint_union f) & inc x' (disjoint_union f) &
  (glt r (Q x) (Q x') \ (Q x = Q x' & gle (V (Q x) g) (P x) (P x')))).

Lemma related_ordinal_sum_order_id: forall r f g x x',
  ordinal_sum_axioms r f g ->
  related (ordinal_sum r f g) x x' -> gle r (Q x) (Q x').

Lemma inc_disjoint_union: forall f x y,
  inc y (domain f) -> inc x (V y f) ->
  inc (J x y) (disjoint_union f).

Lemma substrate_ordinal_sum: forall r f g,
  ordinal_sum_axioms r f g ->
  substrate(ordinal_sum r f g) = disjoint_union f.

Given two sets \( a \) and \( b \) the disjoint union of the family \( x \mapsto E_1 \) and \( y \mapsto E_2 \) is \( E_1 \times \{x\} \cup E_2 \times \{y\} \). In the special case where \( x \) and \( y \) are TPa and TPb, we call this the canonical disjoint union. We have a canonical ordering on the index set with \( x < y \).

Definition canonical_du2 a b :=
  disjoint_union (Lvariantc a b).

Lemma disjoint_union2_rw: forall a b x y, y <> x ->
  disjoint_union (Lvariant x y a b) =
  union2 (product a (singleton x)) (product b (singleton y)).

Lemma disjoint_union2_rw1: forall a b,
  disjoint_union (Lvariantc a b) =
  union2 (product a (singleton TPa)) (product b (singleton TPb)).

Lemma canonical_du2_rw: forall a b,
  canonical_du2 a b = union2 (product a (singleton TPa))
  (product b (singleton TPb)).

Lemma canonical_du2_pr: forall a b x,
  inc x (canonical_du2 a b) = (is_pair x &
  (((inc (P x) a & Q x = TPa) \ (inc (P x) b & Q x = TPb))).

We define the ordinal sum of the two sets \( E_1 \) and \( E_2 \) as the ordinal sum of the family \( \alpha \mapsto E_1 \) and \( \beta \mapsto E_2 \), defined on the canonical doubleton ordered by \( \alpha < \beta \). This is an ordered set, it will be denoted by \( E_1 + E_2 \).
Definition \(\text{ordinal}_2 \ r \ r' :=\)
\[
\text{ordinal} \ (\text{canonical}_2 \ r \ r')
\]
\[
(\text{L} \ r \ r')
\]

Lemma \(\text{ordinal}_2\) _axioms_: \(\forall r \ r',\ \text{order} \ r \rightarrow \text{order} \ r' \rightarrow \)
\[
\text{axioms}_2 \ (\text{canonical}_2 \ r \ r') \ (\text{L} \ r \ r')
\]

Lemma \(\text{order}_2\) _axioms_: \(\forall r \ r',\ \text{order} \ r \rightarrow \text{order} \ r' \rightarrow \)
\[
\text{order} \ (\text{ordinal}_2 \ r \ r')
\]

Lemma \(\text{substrate}_2\) _axioms_: \(\forall r \ r',\ \text{order} \ r \rightarrow \text{order} \ r' \rightarrow \)
\[
\text{substrate} \ (\text{ordinal}_2 \ r \ r') = \text{canonical}_2 \ (\text{substrate}_2 \ r \ r')
\]

The ordering on \(E_1 + E_2\) is defined by \(x \leq y\) if and only if either \(\text{pr}_2 x = \text{pr}_2 y = \alpha\) and \(\text{pr}_1 x \leq \text{pr}_1 y\) or \(\text{pr}_2 x = \text{pr}_2 y = \beta\) and \(\text{pr}_1 x \leq \text{pr}_1 y\), or \(\text{pr}_2 x < \text{pr}_2 y\) (where \(\{\alpha, \beta\}\) is the canonical doubleton, < its ordering, \(\text{pr}_2 x < \text{pr}_2 y\) is the same as \(\text{pr}_2 x = \alpha\) and \(\text{pr}_2 y \neq \alpha\), while \(\text{pr}_2 x = \text{pr}_2 y = \beta\) is the same as \(\text{pr}_2 x \neq \alpha\) and \(\text{pr}_2 y \neq \alpha\)).

If we identify \(E_1\) and \(E_2\) as subsets of \(E_1 + E_2\), we can restate this as: for all \(x \in E_1\) and \(y \in E_2\) we have \(x < y\), and the ordering induced by the sum on \(E_1\) or \(E_2\) is the original ordering.

Lemma \(\text{related}_{\text{ordinal}_2}\): \(\forall r \ r' \ x \ x',\ \text{order} \ r \rightarrow \text{order} \ r' \rightarrow \)
\[
\text{related} \ (\text{ordinal}_2 \ r \ r') \ x \ x' =
\]
\[
(\text{inc} \ x \ (\text{canonical}_2 \ r \ r') \ (\text{substrate}_2 \ r \ r') \ &
\text{inc} \ x' \ (\text{canonical}_2 \ r \ r') \ (\text{substrate}_2 \ r \ r') \ &
(Q x = \text{TPa} \ & \ Q x' = \text{TPa} \ & \ \text{gle} \ r \ (P x) \ (P x') \)
\&
(\text{inc} \ x \ (\text{canonical}_2 \ r \ r') \ (\text{substrate}_2 \ r \ r') \ &
\text{inc} \ x' \ (\text{canonical}_2 \ r \ r') \ (\text{substrate}_2 \ r \ r') \ &
(Q x = \text{TPa} \ & \ Q x' = \text{TPa} \ & \ \text{gle} \ r' \ (P x) \ (P x') \)
\&
(Q x = \text{TPa} \ & \ Q x' = \text{TPa})).
\]

Lemma \(\text{related}_{\text{ordinal}_2}\) _spec_: \(\forall r \ r' \ x \ x',\ \text{order} \ r \rightarrow \text{order} \ r' \rightarrow \)
\[
\text{inc} \ x \ (\text{substrate}_2 \ r \ r') \rightarrow \text{inc} \ x' \ (\text{substrate}_2 \ r \ r') \rightarrow
\]
\[
\text{glt} \ (\text{ordinal}_2 \ r \ r') \ (J x \ TPa) \ (J x' \ TPb).
\]

Lemma \(\text{order}_2\) _totalorder_: \(\forall r \ f \ g,
\text{order} \ r \rightarrow \text{order} \ f \ &
\text{order} \ r \rightarrow \text{order} \ g \rightarrow
\]
\[
\text{total} \ (\text{order} \ r \ f \ g) = \text{total} \ (\text{order} \ r \ &
\text{order} \ f \ g \rightarrow \text{total} \ (\text{order} \ (V i \ f \ g))
\]

We want to show the associativity of the ordinal sum.
\[
\sum_{i \in I} E_i = \sum_{\lambda \in L} \sum_{i \in \lambda} E_i, \quad I = \sum_{\lambda \in L} \lambda.
\]

There is an abuse of notations here. Since \(I\) is an ordinal sum, it is an ordering, and \(i \in I\) has to be interpreted as \(i\) belongs to the support. On the other hand \(\lambda\) is a set, but not a subset of the support (the support if the union of the \(\lambda \times \{\lambda\}\)).

Assume that \(E = \sum E_i\) is the sum associated to the triple \((r, f, g)\) (where \(f\) is the family \(E_i\), \(g\) the family of orderings and \(r\) and ordering on the index set \(I\)). Assume \(I = \sum \lambda\). This means that we have a triple \((r, f', g')\), and \(r\) is the ordinal sum associated to this triple. An element of \(E\) is a pair \((x, i)\) with \(x \in I\) and \(x \in f(i)\). Since \(I\) is a disjoint union, \(i\) is a pair, hence our element has the form
\[
(*) \quad y = (x, (i, \lambda)), \quad \lambda \in L, \quad i \in f'(\lambda), \quad x \in f(i, \lambda).
\]

Let \(F_{\lambda}\) be the ordinal sum of the sets \(E_i\) for \(i \in \lambda\). It is the ordinal sum of \((r_{\lambda}, f_{\lambda}, g_{\lambda})\), where \(f_{\lambda}(i) = f((i, \lambda))\) and \(g_{\lambda}(i) = g((i, \lambda))\) (composition of \(i \rightarrow (i, \lambda)\) and the restrictions of \(f\) and \(g\)).
Moreover $r_\lambda$ is the obvious ordering on $J_\lambda$, namely $g'(\lambda)$. We can consider the ordinal sum $E' = \sum F_\lambda$. It is defined by $(R,F,G)$ where $F$ and $G$ are functions with domain $L$, $G(\lambda)$ is the ordinal sum $(r_\lambda, f'_\lambda, g'_\lambda)$, $F(\lambda)$ is its substrate, and $R$ is the ordering on the index set, hence $r'$. An element of the substrate has the form $(x, \lambda)$, where $\lambda \in L$, and $x \in F(\lambda)$. This means that $x$ has the form $(y, i)$ where $i \in J_\lambda$ and $y \in f'_\lambda(i)$. Thus, an element in the substrate of $E'$ has the form $((y, i), \lambda) \lambda \in L, i \in f''(\lambda)$. Compare this with (*). This gives a natural bijection between $E$ and $E'$. It is an order isomorphism since $(x, i, \lambda) \leq (x', i', \lambda')$ if and only if either $\lambda < \lambda'$ or $\lambda = \lambda'$ and either $i < i'$ or $(i = i'$ and $x \leq x'$).

Section Ordinal_assoc.

Variables $r \hspace{1mm} f \hspace{1mm} g \hspace{1mm} r' \hspace{1mm} f' \hspace{1mm} g'$: Set.
Hypothesis oa_axiom : ordinal_sum_axioms $r \hspace{1mm} f \hspace{1mm} g$.
Hypothesis oa_axiom' : ordinal_sum_axioms $r' \hspace{1mm} f' \hspace{1mm} g'$.
Hypothesis oa_link : $r = \text{ordinal_sum} \hspace{1mm} r' \hspace{1mm} f' \hspace{1mm} g'$.

Definition ordinal_sum_assoc_aux $l$:=
\text{ordinal_sum} \hspace{1mm} (V \hspace{1mm} 1 \hspace{1mm} g') \hspace{1mm} (L \hspace{1mm} (V \hspace{1mm} 1 \hspace{1mm} f') \hspace{1mm} (\text{fun} \hspace{1mm} i => V \hspace{1mm}(J \hspace{1mm} i \hspace{1mm} l) \hspace{1mm} f))
\hspace{1mm} (L \hspace{1mm} (V \hspace{1mm} 1 \hspace{1mm} f') \hspace{1mm} (\text{fun} \hspace{1mm} i => V \hspace{1mm}(J \hspace{1mm} i \hspace{1mm} l) \hspace{1mm} g)).

Definition ordinal_sum_assoc :=
\text{ordinal_sum} \hspace{1mm} r'
\hspace{1mm} (L \hspace{1mm} (\text{domain} \hspace{1mm} f') \hspace{1mm} (\text{fun} \hspace{1mm} l \hspace{1mm} => \text{disjoint_union} \hspace{1mm} (L \hspace{1mm} (V \hspace{1mm} 1 \hspace{1mm} f') \hspace{1mm} (\text{fun} \hspace{1mm} i => V \hspace{1mm}(J \hspace{1mm} i \hspace{1mm} l) \hspace{1mm} f))))
\hspace{1mm} (L \hspace{1mm} (\text{domain} \hspace{1mm} f') \hspace{1mm} (\text{fun} \hspace{1mm} l \hspace{1mm} => \text{ordinal_sum_assoc_aux} \hspace{1mm} 1))).

Lemma ordinal_sum_assoc_aux1 :forall $l$,
\text{inc} \hspace{1mm} $l$ \hspace{1mm} (\text{substrate} \hspace{1mm} $r'$) ->
\text{ordinal_sum_axioms} \hspace{1mm} (V \hspace{1mm} 1 \hspace{1mm} g') \hspace{1mm} (L \hspace{1mm} (V \hspace{1mm} 1 \hspace{1mm} f') \hspace{1mm} (\text{fun} \hspace{1mm} i => V \hspace{1mm}(J \hspace{1mm} i \hspace{1mm} l) \hspace{1mm} f))
\hspace{1mm} (L \hspace{1mm} (V \hspace{1mm} 1 \hspace{1mm} f') \hspace{1mm} (\text{fun} \hspace{1mm} i => V \hspace{1mm}(J \hspace{1mm} i \hspace{1mm} l) \hspace{1mm} g)).

Lemma ordinal_sum_assoc_aux2 :forall $l$,
\text{inc} \hspace{1mm} $l$ \hspace{1mm} (\text{domain} \hspace{1mm} $f'$) -> \text{order} \hspace{1mm} (\text{ordinal_sum_assoc_aux} \hspace{1mm} 1).

Lemma ordinal_sum_assoc_aux3 : ordinal_sum_axioms $r'$
\hspace{1mm} (L \hspace{1mm} (\text{domain} \hspace{1mm} $f'$) \hspace{1mm} (\text{fun} \hspace{1mm} $l$ \hspace{1mm} => \text{disjoint_union} \hspace{1mm} (L \hspace{1mm} (V \hspace{1mm} 1 \hspace{1mm} $f'$) \hspace{1mm} (\text{fun} \hspace{1mm} $i$ => V \hspace{1mm}(J \hspace{1mm} $i$ \hspace{1mm} $l$) \hspace{1mm} $f$))))
\hspace{1mm} (L \hspace{1mm} (\text{domain} \hspace{1mm} $f'$) \hspace{1mm} (\text{fun} \hspace{1mm} $l$ \hspace{1mm} => \text{ordinal_sum_assoc_aux} \hspace{1mm} 1))).

Lemma ordinal_sum_assoc1: \text{order} \hspace{1mm} \text{ordinal_sum_assoc}. (* 70 *)

Lemma ordinal_sum_assoc_iso:
\text{order_isomorphism} \hspace{1mm} (BL \hspace{1mm} (\text{fun} \hspace{1mm} $x$ => J \hspace{1mm} (J \hspace{1mm} (P \hspace{1mm} $x$) \hspace{1mm} (P \hspace{1mm} (Q \hspace{1mm} $x$))) \hspace{1mm} (Q \hspace{1mm} (Q \hspace{1mm} $x$)))
\hspace{1mm} (\text{disjoint_union} \hspace{1mm} f) \hspace{1mm} (\text{substrate} \hspace{1mm} (\text{ordinal_sum_assoc})))
\hspace{1mm} (\text{ordinal_sum} \hspace{1mm} $r$ \hspace{1mm} $f$ \hspace{1mm} $g$) \hspace{1mm} (\text{ordinal_sum_assoc}). (* 70 *)

End Ordinal_assoc.
Chapter 4

Equipotent Sets. Cardinals

Bourbaki denotes by Eq(X, Y) the property that there is a bijection between X and Y and denotes by Card(X) the set \( \tau_2(\text{Eq}(X, Z)) \). He calls this the cardinal of X, or the power of X. It is interesting to notice that no name is given to the notation \( a^b \) when this means the cardinal of the set of mappings from one set into another (the operation is nevertheless called “exponentiation of cardinals”). The term “power” is used only in the phrase “power of the continuum”, where it means the cardinal of the set of real numbers (to be defined elsewhere), or, equivalently, the cardinal of \( \mathcal{P}(\mathbb{N}) \) (where \( \mathbb{N} \) is the set of natural integers, defined in Chapter 6). For us, the term “power” will only be used to denote \( a^b \).

Bourbaki does not define “a cardinal”. The only possible interpretation of “\( \tau \) is a cardinal” is “the object \( \tau \) is of the form \( \text{Card}(E) \) for some set \( E \)”. Using a specific font for cardinals suggests that a cardinal is some special object, and that we should perhaps introduce a type for these cardinals. If \( A = \{ \emptyset \} \) and \( a \) denotes the cardinal of \( A \), it is impossible to prove \( a = A \) or \( a \neq A \) (non-uniqueness of \( \tau \)). This means that giving a different type to these objects invalidates no theorem of Bourbaki (with the exception of \( 0 = \emptyset \)).

One can multiply cardinals. For instance \( a \cdot a = \text{Card}(A \times A) \) is \( a \) (if \( A \) is the set given above). This makes sense because \( \text{Card}(A \times B) \) is left unchanged when \( A \) is replaced by \( A' \) with \( \text{Card}(A) = \text{Card}(A') \). But it becomes difficult to assert associativity or commutativity of the product: we need the notion of a family of cardinals, which is a function \( f : I \to C \), where \( I \) is some index set and \( C \) is the type of the cardinals (we can also consider graphs of functions, which are subsets of \( I \times C \); this is even more problematic, because \( C \) is too big to be a set, hence \( I \times C \) cannot be identified to a set). If \( J \) is a subset of \( I \), the cardinal product of the restriction of \( f \) to \( J \) is a cardinal, and this induces a function \( \mathcal{P}(I) \to C \). Such an object is neither a function in the Bourbaki sense (with a source, a target, a graph), neither in the Coq sense.

Bourbaki solves the problem by defining the cardinal product as the cardinal of the product. This means that cardinals are ordinary sets. This also means that we can consider the cardinal product of any two sets. The relation \( a \cdot 1 = a \cdot a \) is valid for two cardinals, valid for any two sets.

Our theorems are easier to prove and use if we drop the requirements that the arguments are cardinals. The relation \( a \cdot 1 = a \) is true only if \( a \) is a cardinal. The relation \( a \leq a \cdot b \) is true if \( b \neq 0 \); in order for \( \leq \) to be antisymmetric we impose that its arguments are cardinals, so that we need \( a \) to be a cardinal. Our proof uses \( 1 \leq b \) which is valid only if \( b \) is a cardinal. Thus our theorem assumes that both arguments are cardinals. This is a case where assumptions are not minimal.
4.1 The cardinal of a set

We denote by \(\text{Eq}(X,Y)\) or \(\text{equipotent } X Y\) the property that there is a bijection between \(X\) and \(Y\). We know that this relation is reflexive, symmetric and transitive (but is not an equivalence, because it has no graph). We also know that two sets are equipotent if there is a bijective mapping of type \(X \rightarrow Y\). For instance, the mapping \(f_1\) below can be used to show that two singletons are equipotent. The mapping \(f_2\) can be used to show that two doubletons are equipotent (assuming of course \(x \neq x'\) and \(y \neq y'\)). The definition is a bit tricky: the body has the form: if \(a = x\) then \(y\) else \(y'\); here \(H_2\) is a proof that this expression is in \(\{y, y'\}\), and \(H_1\) is a proof that \(x\) is in \(\{x, x'\}\), and \(Bo\) converts \(a \in b\) into an object \(a'\) of type \(b\).

\begin{align*}
H_2 &: \forall a : \text{doubleton } x x', \text{inc } (\text{Yo } (a = \text{Bo } H_1) y y') (\text{doubleton } y y') \\
f_1 &: \text{fun } _-: \text{singleton } x \Rightarrow \text{Bo} (\text{singleton_inc } y)) \\
f_2 &: \text{fun } a : \text{doubleton } x x' \Rightarrow \text{Bo} (H_2 a))
\end{align*}

If a set \(E\) contains the \(n\) distinct elements \(x_1, x_2, \ldots, x_n\), and if a set \(F\) contains the \(n\) distinct elements \(y_1, y_2, \ldots, y_n\), then the set \(G = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}\) is the graph of a bijection between \(E\) and \(F\). We shall use this method to prove equipotency of doubletons.

\begin{align*}
\text{Lemma singletons_equipotent}: \forall x, y, \\
&\text{equipotent } (\text{singleton } x) (\text{singleton } y). \\
\text{Lemma doubleton_equipotent1}: \forall x, y, x', y', \\
&x \neq x' \Rightarrow y \neq y' \Rightarrow \text{equipotent } (\text{doubleton } x x') (\text{doubleton } y y').
\end{align*}

Products of equipotent sets are equipotent. We first consider the case of \(\text{product}\) since \(\text{ext_prod_map}\) is a bijection from \(\prod E\) to \(\prod F\) (See Part I, section 6.7). We also consider the case of the product of two sets (the bijection is \(\text{ext_to_prodC}\)).

\begin{align*}
\text{Lemma equipotent_productf}: \forall \text{In } p1, p2, \\
&(\forall i, \text{inc } i \text{ In } \Rightarrow \text{equipotent } (p1 i) (p2 i)) \Rightarrow \\
&\text{equipotent } (\text{productf In } p1)(\text{productf In } p2). \\
\text{Lemma equipotent_productb}: \forall x, y, \text{fgraph } x \Rightarrow \text{fgraph } y \Rightarrow \\
&(\forall i, \text{inc } i (\text{domain } x) \Rightarrow \text{equipotent } (V i x) (V i y)) \Rightarrow \\
&\text{equipotent } (\text{productb x}) (\text{productb y}). \\
\text{Lemma equipotent_product}: \forall a, b, a', b', \\
&a \text{ equipotent } a' \Rightarrow b \text{ equipotent } b' \Rightarrow \\
&(\text{equipotent } a b) (\text{product } a b').
\end{align*}

If \(A, B\) and \(C\) are sets, then \(A \times B\) is equipotent to \(B \times A\), and \(A \times (B \times C)\) is equipotent to \((A \times B) \times C\). We have \((A \cup B) \times C = (A \times C) \cup (B \times C)\). Finally, if \(B\) is a singleton, \(A\) and \(A \times B\) are equipotent.

\begin{align*}
\text{Lemma equipotent_product_sym}: \forall a, b, \\
&a \text{ equipotent } b \Rightarrow b \text{ equipotent } a. \\
\text{Lemma product2associative } : \forall a, b, c, \\
&a \text{ equipotent } b \Rightarrow c \Rightarrow (a \times b) \text{ equipotent } (b \times c). \\
\text{Lemma distrib_inter_prod2}: \forall a, b, c, \\
&(\text{product } (\text{union2 } a b) c) = \text{union2 } (\text{product } a c) (\text{product } b c). \\
\text{Lemma distrib_inter_prod3}: \forall a, b, c, \\
&(\text{product } (\text{union2 } a b) c) = \text{union2 } (\text{product } c a) (\text{product } c b). \\
\text{Lemma equipotent_a_times_singl}: \forall a, b, \\
&a \text{ equipotent } a \Rightarrow (a \times \text{singleton } b).
\end{align*}
Two sets $A \times B$ and $A' \times B'$ are disjoint if $B$ and $B'$ are disjoint; this is the case when $B$ and $B'$ are distinct singletons.

**Lemma disjoint_pr:** \(\forall a \ b, \) \(\forall u, \text{inc } u \ a \rightarrow \text{inc } u \ b \rightarrow \text{False} \rightarrow \text{disjoint } a \ b.\)

**Lemma disjoint_union2_pr0:** \(\forall a \ b \ x \ y,\) \(\text{disjoint } x \ y \rightarrow \text{disjoint } (\text{product } a \ x) \ (\text{product } b \ y).\)

**Lemma disjoint_union2_pr1:** \(\forall x \ y,\) \(x \neq y \rightarrow \text{disjoint } (\text{singleton } x) \ (\text{singleton } y).\)

**Lemma disjoint_union2_pr:** \(\forall a \ b \ x \ y, \) \(x \neq y \rightarrow \text{disjoint } (\text{product } a \ (\text{singleton } x)) \ (\text{product } b \ (\text{singleton } y)).\)

Two unions $\bigcup X_\iota$ and $\bigcup Y_\iota$ with the same index set are equipotent if the sets are equipotent and if each family is mutually disjoint. For if $f_\iota$ is a function from $X_\iota$ into $Y_\iota$, we can find a function $f$ such that $f(x) = f_\iota(x)$ whenever $x \in X_\iota$, provided that $x$ is in a unique $X_\iota$ (i.e., the family is mutually disjoint). If the family $\bigcup Y_\iota$ is mutually disjoint, then $f(x) = f(y)$ implies that there is $i$ such that $x \in X_i$ and $y \in X_i$, hence $f_\iota(x) = f_\iota(y)$. Thus $f$ is injective if each $f_\iota$ is injective.

Two disjoint unions of equipotent sets are equipotent. Remember that the disjoint union of a family of sets $X_\iota$ is the union of the sets $X_\iota'$ that $X_\iota \times \{\iota\}$. Two lemmas mentioned above say that each $X_\iota$ is equipotent to $X_\iota'$ and the family is disjoint.

**Lemma equipotent_disjoint_union:** \(\forall X \ Y, \) \(\forall i, \text{inc } i \ (\text{domain } X) \rightarrow \text{equipotent } (V \ i \ X) \ (V \ i \ Y) \rightarrow \text{mutually_disjoint } X \rightarrow \text{mutually_disjoint } Y \rightarrow \text{equipotent } (\text{unionb } X) \ (\text{unionb } Y).\)

**Lemma equipotent_disjoint_union1:** \(\forall X \ Y, \) \(\forall i, \text{inc } i \ (\text{domain } X) \rightarrow \text{equipotent } (V \ i \ X) \ (V \ i \ Y) \rightarrow \text{equipotent } (\text{disjoint_union } X) \ (\text{disjoint_union } Y).\)

We denote by $X_{\alpha\beta}(A, B)$, the function that maps $\alpha$ to $A$ and $\beta$ to $B$. If $\alpha$ and $\beta$ are the elements of the canonical doubleton, we omit the indices. Any function that maps $TPa$ and $TPb$ to $A$ and $B$ is $X(A, B)$ modulo a change of variables in the domain.

**Lemma two_terms_bij:** \(\forall a \ b \ x \ y \ f, \) \(x \neq y \rightarrow \text{graph } f \rightarrow \text{domain } f = \text{doubleton } x \ y \rightarrow V \ x \ f = a \rightarrow V \ y \ f = b \rightarrow \exists g, (\text{bijective } g \ & \ \text{target } g = \text{two_points} \ & \ \text{source } g = \text{doubleton } x \ y \ & \ f = \text{gcompose } (L\text{variantc } a \ b) \ (\text{graph } g)).\)

If $A$ and $B$ are two sets, the union of the family $X(A, B)$ is $A \cup B$. As a consequence, if $A$ is equipotent to $A'$ and $B$ is equipotent to $B'$ and the sets are disjoint, then $A \cup B$ and $A' \cup B'$ are equipotent. The disjoint union of the family $X_{\alpha\beta}(A, B)$ is $A \times \{\alpha\} \cup B \times \{\beta\}$. It depends on $\alpha$ and $\beta$; but two such disjoint unions are equipotent (see later). We shall therefore use the family $X(A, B)$. Its disjoint union depends only on $A$ and $B$. We shall use later on the relation $X_{\alpha\beta}(A, B) = X_{\beta\alpha}(B, A)$, which implies, after re-ordering, that the disjoint union of $A$ and $B$ (whatever the index set) is equipotent to the disjoint union of $B$ and $A$.

**Lemma union_of_twosets_aux1:** \(\forall a \ b, \) \(\text{union2 } a \ b = \text{unionb } (L\text{variantc } a \ b).\)

RR n° 7150
Lemma disjoint_union2: \( \forall a b a' b', \)
\( \text{disjoint } a b \rightarrow \text{disjoint } a' b' \rightarrow \text{equipotent } a a' \rightarrow \text{equipotent } b b' \rightarrow \)
\( \text{equipotent } (\text{union2 } a b) (\text{union2 } a' b'). \)

The representative of an equivalent class for equipotency (this is not a set) of the set \( X \), is called its \textit{cardinal}, and denoted \( \text{Card}(X) \). Bourbaki denotes by 0, 1 and 2, the cardinals of the empty set, a singleton, or a doubleton with two distinct elements.\(^1\)

Definition cardinal \( x := \text{choose } (\text{fun } z \Rightarrow \text{equipotent } x z). \)
Definition card_zero := cardinal emptyset.
Definition card_one := cardinal (singleton emptyset).
Definition card_two := cardinal (two_points).

Objects of the form \( \text{Card}(x) \) are called \textit{cardinals}. Thus 0, 1 and 2 are cardinals.

Definition is_cardinal \( x := \exists y, x = \text{cardinal } y. \)

Lemma cardinal_le0: \( \forall x, \text{is_cardinal } (\text{cardinal } x). \)
Lemma cardinal0: \( \text{is_cardinal } \text{card_zero}. \)
Lemma cardinal1: \( \text{is_cardinal } \text{card_one}. \)
Lemma cardinal2: \( \text{is_cardinal } \text{card_two}. \)

Proposition 1 [2, p. 158] states that \( X \) and \( Y \) are equipotent if and only if they have the same cardinal.

Lemma cardinal_pr: \( \forall x, \text{equipotent } (\text{cardinal } x) x. \)
Lemma cardinal_pr0: \( \forall x, \text{equipotent } x (\text{cardinal } x). \)

Theorem cardinal_equipotent: \( \forall x y, \)
\( (\text{cardinal } x = \text{cardinal } y) = (\text{equipotent } x y). \)

We study here some properties of the cardinal 0.

Lemma equipotent_to_emptyset:
\( \forall x, \text{equipotent } x \text{ emptyset } \rightarrow x = \text{emptyset}. \)
Lemma cardinal_zero: \( \text{cardinal } \text{emptyset} = \text{emptyset}. \)
Lemma zero_is_emptyset: \( \text{card_zero} = \text{emptyset}. \)
Lemma cardinal_emptyset: \( \text{cardinal } \text{emptyset} = \text{card_zero}. \)
Lemma cardinal_nonemptyset: \( \forall x, \)
\( \text{cardinal } x = \text{card_zero } \rightarrow x = \text{emptyset}. \)
Lemma cardinal_nonemptyset1: \( \forall x, \)
\( \text{nonempty } x \rightarrow \text{cardinal } x \neq \text{card_zero}. \)

We study some properties of the cardinal 1.

Lemma cardinal_singleton: \( \forall x, \text{cardinal} (\text{singleton } x) = \text{card_one}. \)
Lemma cardinal_one_is_singleton: \( \text{isSingleton} (\text{card_one}). \)

We study some properties of the cardinal 2.

---

\(^1\) Definition of 2 changed in V3
Lemma cardinal_doubleton: forall x x',
   x <> x' -> cardinal(doubleton x x') = card_two.
Lemma set_of_card_two: forall x, cardinal x = card_two ->
   exists u, exists v, u<>v & x = doubleton u v.
Lemma cardinal_two_is_doubleton: exists x, exists x',
   x <> x' & card_two = doubleton x x'.

These three cardinals are distinct.

Lemma card_one_not_zero: card_one <> card_zero.
Lemma card_two_not_zero: card_two <> card_zero.
Lemma card_one_not_two: card_one <> card_two.

4.2 Order relation between cardinals

We restate here that composition of injective functions is injective. Thus if f is a bijection
A → B and B ⊂ C, its composition g with the canonical inclusion B → C is an injection A → C.
Conversely, given a function g : A → C, its restriction to its image B is a surjective function,
so that if g is injective, its restriction is bijective. The existence of g depends only on the
cardinals of A and C, and this defines on ordering on cardinals.

Lemma inj_compose1: forall f f',
   injective f-> injective f' -> source f' = target f ->
   injective (compose f' f).
Definition restriction_to_image f :=
   restriction2 f (source f) (image_of_fun f).
Lemma restriction_to_image_axioms: forall f, is_function f ->
   restriction2_axioms f (source f) (image_of_fun f).
Lemma restriction_to_image_surjective: forall f, is_function f ->
   surjective (restriction_to_image f).
Lemma restriction_to_image_bijective: forall f, injective f ->
   bijective (restriction_to_image f).

A well-ordering relation is an order relation such that every nonempty set in which the
relation is reflexive has a least element. We restate this as follows: for every set E such that
x ∈ E implies x ≺ x, there exists a well-ordering, denoted by ≤, whose substrate is E, such that
x ≤ y is equivalent to “x ∈ E and y ∈ E and x ≺ y.”

Definition worder_r r :=
   order_r r & forall x, (forall a, inc a x -> r a a) ->
   nonempty x ->
   exists y, least_element (graph_on r x) y.
Lemma wordering_pr: forall r x, worder_r r ->
   (forall a, inc a x -> r a a) ->
   (substrate (graph_on r x) = x & worder (graph_on r x)). (* 16 *)

We say that r ≤ Card n if r and n are cardinals, and r is equipotent to a subset of n. The
notation is often simplified to r ≤ n. We also introduce the notation r < Card n. We do not
introduce specific notations for ≥Card or >Card.

Definition is_cardinal x:= exists y, x = cardinal y.
Definition equipotent_to_subset x y:= exists z, sub z y & equipotent x z.
Definition cardinal_le x y :=
is_cardinal x & is_cardinal y & equipotent_to_subset x y.
Definition cardinal_lt a b := cardinal_le a b & a <> b.

We list here some useful properties. First, for all \( x \), \( \text{Card}(x) \) is a cardinal hence \( \text{Card}(\text{Card}(x)) = \text{Card}(x) \). Since the composition of two injections is an injection, and bijections are injections, we get some interesting results. A is equipotent to a subset of B if and only if there is an injection from A into B. There is an injection from A into B if and only if there is an injection from Card(A) into Card(B). Thus A is equipotent to a subset of B if and only if Card(A) is equipotent to a subset of Card(B). If a is a cardinal, then Card(a) = a and a \( \leq a \). If A is equipotent to a subset of B and B is equipotent to C, then A is equipotent to a subset of C. If A \( \subset B \) then A is equipotent to a subset of B. If \( f : A \rightarrow B \) is injective then Card(A) \( \leq \) Card(B). Finally, if E is a set of cardinals, the support of the order induced by \( \leq \text{Card} \) on E is E.

Lemma cardinal_le0: forall x, is_cardinal (cardinal x).

Lemma cardinal_le1: forall x y, 
equipotent_to_subset x y = 
(exists f, injective f & source f = x & target f = y). (* 15 *)

Lemma cardinal_le2: forall x y, 
equipotent_to_subset x y = equipotent_to_subset (cardinal x) (cardinal y).

Lemma cardinal_le3: forall x y, 
equipotent_to_subset x y = cardinal_le (cardinal x) (cardinal y).

Lemma cardinal_le9: forall f, injective f -> cardinal_le (cardinal (source f)) (cardinal (target f)).

Lemma cardinal_le4: forall x, is_cardinal x -> cardinal x = x.

Lemma cardinal_le_reflexive: forall x, is_cardinal x -> cardinal (cardinal x) x x.

Lemma cardinal_le5: forall E, (forall x, inc x E -> is_cardinal x) -> 
substrate (graph_on cardinal_le E) = E.

Lemma cardinal_le6: forall x, cardinal (cardinal x) = cardinal x.

Lemma cardinal_le7: forall a b c, 
equipotent b c -> equipotent_to_subset a b -> equipotent_to_subset a c.

Lemma cardinal_le8: forall a b, sub a b -> equipotent_to_subset a b.

Lemma sub_smaller: forall a b, 
sub a b -> cardinal_le (cardinal a) (cardinal b).

Theorem one [2, p. 159] says that the ordering between cardinals is a well-ordering. The idea is the following. Let E be a set of cardinals, and A its union. Consider a well-ordering on A. Let \( \phi(x) \) be the smallest segment of A equipotent to x (if x \( \in E \), x is a subset of A hence isomorphic, hence equipotent, to a segment of A; hence \( \phi \) is well-defined). The relation \( a \leq \text{Card} b \) on E is equivalent to \( \phi(a) \subset \phi(b) \) (if \( a \leq \text{Card} b \) then a is isomorphic to a subset of \( \phi(b) \), hence a is isomorphic to a segment \( u \) of \( \phi(b) \); by definition \( \phi(a) \subset u \), hence \( \phi(a) \subset \phi(b) \); converse is easy). From this, one deduces that the relation \( a \leq \text{Card} b \) is an order on E. This is a well-ordering, since the set of segments is well-ordered. Assume \( a \leq \text{Card} b \) and \( b \leq \text{Card} a \). If we consider the doubleton \( \{ a, b \} \), we have \( a \leq b \) and \( b \leq a \) for the induced order, hence \( a = b \).

Theorem wordering_cardinal_le: worder_r cardinal_le. (* 101 *)

Some consequences: if a, b, and c, are cardinals, then \( a \leq \text{Card} b \) and \( b \leq \text{Card} c \) implies \( a \leq \text{Card} c \) (this is easy). Either \( a \leq \text{Card} b \) or \( b \leq \text{Card} a \); but if both relations hold, then \( a = b \). This can be restated as: if there is an injection from A into B and an injection from B into A, then there is a bijection between the two sets A and B. This is sometimes called the Cantor-Bernstein Theorem. It can be shown without the axiom of choice.

INRIA
Lemma wordering_cardinal_le_pr : forall x,
  (forall a, inc a x -> is_cardinal a) ->
  (substrate (graph_on cardinal_le x) = x &
  worder (graph_on cardinal_le x)).

Lemma cardinal_antisymmetry1: forall x y,
  cardinal_le x y -> cardinal_le y x -> x = y.

Lemma not_card_le_lt: forall a b, cardinal_le a b -> cardinal_lt b a -> False.

Lemma cardinal_antisymmetry2: forall a b,
  equipotent_to_subset a b -> equipotent_to_subset b a ->
  equipotent a b.

Lemma cardinal_le_transitive: forall a b c,
  cardinal_le a b -> cardinal_le b c -> cardinal_le a c.

Lemma cardinal_lt_le_trans: forall a b c,
  cardinal_lt a b -> cardinal_le b c -> cardinal_lt a c.

Lemma cardinal_le_lt_trans: forall a b c,
  cardinal_le a b -> cardinal_lt b c -> cardinal_lt a c.

Lemma cardinal_le_total_order: forall a b,
  equipotent_to_subset a b / equipotent_to_subset b a.

We have 0 \leq a for every cardinal a, and 1 \leq a if moreover a \neq 0. We have Card(E) \geq 1 if and
only if E is non-empty,

Lemma zero_smallest: forall x, is_cardinal x -> cardinal_le card_zero x.

We have Card(E) \geq 2 if and only if E has at least two elements.

Lemma card_le_two_prop: forall E,
  cardinal_le card_two (cardinal E) ->
  exists a, exists b, inc a E & inc b E & a <> b.

For every cardinal a, the set of objects of the form Card(b) for b \in \mathcal{P}(a) is the set of cardinals \leq a. Given a family of cardinals (a_i)_{i \in I}, we can find a cardinal b greater than all a_i (for
instance the union) and consider the set $E$ of cardinals $\leq b$. The family, being bounded in a well-ordered set, has a supremum $c$. If $d$ is another upper bound, either $d \geq b$ hence $d \geq c$, or $d \leq b$, hence is in $E$ and $d \geq c$. It is called the supremum of the family. This is Proposition 2 in [2, p. 160]. We first show the same result for a set of cardinals.

Definition set_of_cardinals_le a :=
  fun_image(powerset a)(fun x => cardinal x).

Lemma set_of_cardinals_pr: forall a b, is_cardinal a ->
  inc b (set_of_cardinals_le a) = (cardinal_le b a).

Lemma cardinal_supremum: forall x,
  (forall a, inc a x -> is_cardinal a) ->
  exists_unique (fun b => is_cardinal b &
    (forall a, inc a x -> cardinal_le a b) &
    (forall c, is_cardinal c -> (forall a, inc a x -> cardinal_le a c) ->
      cardinal_le b c)). (* 33 *)

Theorem cardinal_supremum1: forall x,
  fgraph x ->
  (forall a, inc a (domain x) -> is_cardinal (V a x)) ->
  exists_unique (fun b => is_cardinal b &
    (forall a, inc a (domain x) -> cardinal_le (V a x) b) &
    (forall c, is_cardinal c ->
      (forall a, inc a (domain x) -> cardinal_le (V a x) c) ->
      cardinal_le b c)).

Proposition 3 in [2, p. 160] says that $\text{Card}(Y) \leq \text{Card}(X)$ if there is a surjection of $X$ onto $Y$. As a consequence, the range of a function is not bigger than the source.

Theorem surjective_cardinal_le: forall x y,
  (exists z, surjective z & source z = x & target z = y) ->
  cardinal_le (cardinal y) (cardinal x).

Lemma image_smaller_cardinal: forall f, is_function f ->
  cardinal_le (cardinal (image_of_fun f))(cardinal (source f)).

4.3 Operations on cardinals

Given a family of cardinals $(a_i)_{i \in I}$, the cardinal of the sum of these sets is called the cardinal sum and denoted by $\sum_{i \in I} a_i$; the cardinal of the product is called the cardinal product and denoted $\prod_{i \in I} a_i$. The qualificative “cardinal” will be omitted if there is no risk of confusion. The associated operations are called addition and multiplication. The notation $\prod_{i \in I} a_i$ will later be used for both the normal product and the cardinal product. There is no need to introduce a specific notation for the cardinal sum (since there is no notation for the sum, aka the disjoint union).

Definition cardinal_sum x := cardinal (disjoint_union x).
Definition cardinal_prod x := cardinal (productb x).

Proposition 4 of [2, p. 160] says that the cardinal sum or cardinal product of the family $\text{Card}(E_i)$ is the cardinal of the sum or the product of the sets $E_i$. In other terms, if $a_i = \text{Card}(E_i)$ then $\text{Card}(\bigcup E_i) = \prod_{i \in I} a_i$ and $\text{Card}(\bigcap E_i) = \sum_{i \in I} a_i$. One can notice that the cardinal of a union is at most the cardinal of the disjoint union.
Theorem `cardinal_prod_pr`: forall x, fgraph x ->  
  cardinal (productb x) =  
  cardinal_prod (L (domain x) (fun a => cardinal (V a x))).

Theorem `cardinal_sum_pr`: forall x, fgraph x ->  
  cardinal (disjoint_union x) =  
  cardinal_sum (L (domain x) (fun a => cardinal (V a x))).

Lemma `cardinal_sum_pr1`: forall x, fgraph x ->  
  cardinal_le (cardinal (unionb x))  
  (cardinal_sum (L (domain x) (fun a => cardinal (V a x))))).

Lemma `mutually_disjoint_prop`: forall f,  
  (forall i j y, inc i (domain f) -> inc j (domain f) -> i<> j ->  
  inc y (V i f) -> inc y (V j f) -> False) ->  
  mutually_disjoint f.

Lemma `mutually_disjoint_prop2`: forall x f,  
  (forall i j y, inc i x -> inc j x ->  
  inc y (f i) -> inc y (f j) -> i=j) ->  
  mutually_disjoint (L x f).

Proposition 5 [2, p. 161] says that if \( f \) is a bijection from \( K \) to \( I \) and if \( a_\lambda \) is a cardinal then  
("commutativity" of the sum and product):

(4)

\[
\sum_{\kappa \in K} a_{f(\kappa)} = \sum_{i \in I} a_i, \quad \prod_{\kappa \in K} a_{f(\kappa)} = \prod_{i \in I} a_i.
\]

If the family \((I_\lambda)_{\lambda \in \Lambda}\) is a partition of \( I \), then  
("associativity" of the sum and product):

(5)

\[
\sum_{i \in I} a_i = \sum_{\lambda \in \Lambda} \big( \sum_{i \in I_\lambda} a_i \big), \quad \prod_{i \in I} a_i = \prod_{\lambda \in \Lambda} \big( \prod_{i \in I_\lambda} a_i \big).
\]

Let \((\alpha_{\lambda, i})_{i \in I_\lambda})_{\lambda \in \Lambda}\) be a family of families of cardinals. Let \( I = \prod I_\lambda \). Distributivity of product  
over sum is

(6)

\[
\prod_{\lambda \in \Lambda} \big( \sum_{i \in I_\lambda} a_{\lambda, i} \big) = \sum_{f \in F} \big( \prod_{\lambda \in \Lambda} a_{\lambda, f(\lambda)} \big).
\]

Note that we do not need \( a_\lambda \) be a cardinal in any of these theorems. The relations are  
trivial for the product, and in the case of the union, we have to check that the families are  
disjoint. These formulas are numbered (4), (5) and (6), in order to respect the original Bour-  
baki numbering.

Theorem `cardinal_sum_commutative`: forall X f,  
  fgraph X -> target f = domain X -> bijective f ->  
  cardinal_sum X = cardinal_sum (gcompose X (graph f)). (* 30 *)

Theorem `cardinal_prod_commutative`: forall X f,  
  fgraph X -> target f = domain X -> bijective f ->  
  cardinal_prod X = cardinal_prod (gcompose X (graph f)).

Theorem `cardinal_sum_assoc`: forall f g,  
  fgraph f -> partition_fam g (domain f) ->  
  cardinal_sum f = cardinal_sum (L (domain g) (fun l =>  
  cardinal_sum (restr f (V l g)))).

Theorem `cardinal_prod_assoc`: forall f g,  
  fgraph f -> partition_fam g (domain f) ->  
  cardinal_prod f = cardinal_prod (L (domain g) (fun l =>  
  cardinal_prod (restr f (V l g))))).

Theorem `cardinal_distrib_prod_sum`: forall f, (* 51 *)
\[ \text{fgraph } f \mapsto \]
\[ (\forall l, \text{inc } l \text{ (domain } f) \mapsto \text{fgraph } (V l f)) \mapsto \]
\[ \text{cardinal}_\text{prod} \left( L \text{ (domain } f) \left( \text{fun } l \mapsto \text{cardinal}_\text{sum} \left( V l f) \right) \right) \right) = \]
\[ \text{cardinal}_\text{sum} \left( L \text{ (productf } (\text{domain } f) \left( \text{fun } l \mapsto \text{(domain} \left( V l f) \right) ) \right) \right) \]
\[ \text{fun } g \mapsto \left( \text{cardinal}_\text{prod} \left( L \text{ (domain } f) \left( \text{fun } l \mapsto V \left( V l g \right) \left( V l f) \right) \right) \right) \).

Given two sets \( a \) and \( b \), we can consider a family of two elements whose range is the doubleton \( \{a, b\} \) (for instance \( X_{xy}(a, b) \), see page \[67\]). The cardinal product of this family is the cardinal of the product, it is denoted by \( ab \) or \( a \cdot b \). The cardinal sum of the family is the cardinal of the disjoint union, namely \( a \times \{x\} \cup b \times \{y\} \). We shall sometimes denote this as \( a_x \cup b_y \). The cardinal sum of this family is independent of the pair \((x, y)\) by commutativity. It will be denoted by \( a + b \). If \( a \) and \( a' \) are equipotent, if \( b \) and \( b' \) are equipotent, the products \( a \times b \) and \( a' \times b' \) are equipotent, so that the cardinal products are equal; we show that the same result is true for the cardinal sum.

Definition \( \text{TPas} := \text{singleton } \text{TPa} \).
Definition \( \text{TPbs} := \text{singleton } \text{TPb} \).
Definition \( \text{card_plus} \ a \ b := \text{cardinal}_\text{sum} \left( \text{Lvariantc } a \ b \right) \).
Definition \( \text{card_mult} \ a \ b := \text{cardinal}_\text{prod} \left( \text{Lvariantc } a \ b \right) \).
Definition \( \text{doubleton}_\text{fam} \ f \ a \ b := \exists x, \exists y, x \neq y \& \text{fgraph } f \& \text{domain } f = \text{doubleton } x \ y \& V x f = a \ & V y f = b \).

Lemma \( \text{card_plus_is_cardinal} \): \( \forall a \ b, \text{is_cardinal} \ (\text{card_plus } a \ b) \).
Lemma \( \text{card_mult_is_cardinal} \): \( \forall a \ b, \text{is_cardinal} \ (\text{card_mult } a \ b) \).

Lemma \( \text{card_mult_pr1} \): \( \forall a \ b, \text{card_mult } a \ b = \text{cardinal} \ (\text{product } a \ b) \).
Lemma \( \text{card_plus_pr} \): \( \forall a \ b \ f, \text{doubleton}_\text{fam} \ f \ a \ b \mapsto \text{card_plus } a \ b = \text{cardinal}_\text{sum } f \).
Lemma \( \text{card_mult_pr} \): \( \forall a \ b \ f, \text{doubleton}_\text{fam} \ f \ a \ b \mapsto \text{card_mult } a \ b = \text{cardinal}_\text{prod } f \).

Lemma \( \text{disjoint_union2_pr3} \): \( \forall a \ b \ x \ y, y \neq x \mapsto \text{equipotent } (\text{card_plus } a \ b) (\text{union2 } (\text{product } a \ (\text{singleton } x)) (\text{product } b \ (\text{singleton } y))) \).
Lemma \( \text{disjoint_union2_pr4} \): \( \forall a \ b, \text{equipotent } (\text{card_plus } a \ b) \ (\text{union2 } (\text{product } a \ \text{TPas}) (\text{product } b \ \text{TPbs})) \).
Lemma \( \text{card_plus_pr1} \): \( \forall a \ b \ a' \ b', \text{disjoint } a \ b \mapsto \text{equipotent } a \ a' \mapsto \text{equipotent } b \ b' \mapsto \text{cardinal} \ (\text{union2 } a \ b) = \text{card_plus } a' \ b' \).
Lemma \( \text{cardinal_sum_pr2} \): \( \forall a \ b \ a' \ b', \text{equipotent } a \ a' \mapsto \text{equipotent } b \ b' \mapsto \text{card_plus } a \ b = \text{card_plus } a' \ b' \).
Lemma \( \text{card_mult_pr2} \): \( \forall a \ b \ a' \ b', \text{cardinal } a = \text{cardinal } a' \mapsto \text{cardinal } b = \text{cardinal } b' \mapsto \text{card_mult } a \ b = \text{card_mult } a' \ b' \).

Lemma \( \text{doubleton}_\text{fam}_\text{canon} \): \( \forall f : \text{EE}, \text{doubleton}_\text{fam} \ (L \text{two_points } f) \ (f \ \text{TPas}) \ (f \ \text{TPb}) \).
Lemma \( \text{card_commutative_aux} \): \( \forall a \ b, \text{doubleton}_\text{fam} \ (L\text{variantc } a \ b) \ a \ b \).
Lemma card_plus_pr0: forall f, 
  cardinal_sum (L two_points f) = card_plus (f TPa) (f TPb).

Lemma card_mult_pr0: forall f, 
  cardinal_prod (L two_points f) = card_mult (f TPa) (f TPb).

As a corollary, if \( a \), \( b \) and \( c \) are cardinals we have

1. \( a + b = b + a \) and \( ab = ba \),
2. \( a + (b + c) = (a + b) + c \) and \( a(bc) = (ab)c \),
3. \( a(b + c) = ab + ac \).

Note that the formulas are true even if \( a \), \( b \) and \( c \) are not cardinals. In the case of (1), we use \( X_{x y}(a, b) = X_{y x}(b, a) \). Associativity of the product is a consequence of equipotency of \( A \times (B \times C) \) and \( (A \times B) \times C \). Associativity of the sum is a consequence of associativity of \( \cup \), commutativity of \( + \) and \( \cup \), and the property that \( a + (b + c) \) is equipotent \( a \cup (b \cup c) \), if the indices are distinct; the current proof is four times shorter than the original one. The same idea can be used for (3). The quantity \( a(b + c) \) is equipotent to \( a \times (b \setminus c) \) hence to \( (a \times b) \setminus (a \times c) \), and \( (a \times b) \setminus (a \times c) \), by associativity of the product. We show in fact \( (b + c)a = ba + ca \), because, basically we use equipotency of \( (A \cup B) \times C \) and \( (A \times C) \cup (B \times C) \). The same techniques as above show

\[ a \sum_{i \in I} b_i = \sum_{i \in I} ab_i. \]

Lemma card_plus_commutative: forall a b, 
  card_plus a b = card_plus b a.

Lemma card_mult_commutative: forall a b, 
  card_mult a b = card_mult b a.

Lemma card_mult_associative: forall a b c, 
  card_mult a (card_mult b c) = card_mult (card_mult a b) c.

Lemma card_plus_associative: forall a b c, (* 17 *)
  card_plus a (card_plus b c) = card_plus (card_plus a b) c.

Lemma equipotent_product1: forall a b c, 
  equipotent a b -> equipotent (product a c) (product b c).

Lemma cardinal_distrib_prod_sum3 : forall a b c, 
  card_mult a (card_plus b c) = card_plus (card_mult a b) (card_mult a c). (* 16 *)

Lemma cardinal_distrib_prod_sum2 : forall a b c, 
  card_mult (card_plus b c) a = 
  card_plus (card_mult b a) (card_mult c a).

Lemma distrib_prod2_sum: forall A f, 
  product A (unionb f) = unionb (L (domain f) (fun x => product A (V x f))).

Lemma cardinal_distrib_prod2_sum: forall a f, is_cardinal a -> fgraph f -> 
  card_mult a (cardinal_sum f) = 
  cardinal_sum (L (domain f) (fun i => (card_mult a (V i f)))).

4.4 Properties of the cardinals 0 and 1

If a family is empty, the sum is zero and the product is one. If a family has a single element that is a cardinal, this element is the sum or the product.
Lemma trivial_cardinal_sum: forall f, domain f = emptyset ->
    cardinal_sum f = card_zero.
Lemma trivial_cardinal_prod: forall f, fgraph f -> domain f = emptyset ->
    cardinal_prod f = card_one.
Lemma trivial_cardinal_sum1: forall x f, domain f = singleton x ->
    is_cardinal (V x f) -> cardinal_sum f = V x f.
Lemma trivial_cardinal_plus: forall x a, is_cardinal a ->
    cardinal_sum (cst_graph (singleton x) a) = a.
Lemma trivial_cardinal_prod1: forall x f, fgraph f -> domain f = singleton x ->
    is_cardinal (V x f) -> cardinal_prod f = V x f.

One can remove 0 in a sum and 1 in a product. This is Proposition 6 [2, p. 162]. The result is clear for the sum, because 0_0 = 0 (where 0_i means 0 \times \{i\}). In the case of a product, it is a trivial consequence of bijective_prj. If the family has two elements, this gives nice results. If a factor of a product is zero, so is the product itself.

Theorem zero_unit_sum: forall f j,
    fgraph f -> sub j (domain f) ->
    (forall i, inc i (complement (domain f) j) -> (V i f) = card_zero) ->
    cardinal_sum f = cardinal_sum (restr f j).
Theorem one_unit_prod: forall f j,
    fgraph f -> sub j (domain f) ->
    (forall i, inc i (complement (domain f) j) -> (V i f) = card_one) ->
    cardinal_prod f = cardinal_prod (restr f j).

Lemma zero_unit_sumr: forall a, is_cardinal a ->
    card_plus a card_zero = a.
Lemma zero_unit_suml: forall a, is_cardinal a ->
    card_plus card_zero a = a.
Lemma zero_unit_prodr: forall a, is_cardinal a ->
    card_mult a card_one = a.
Lemma zero_unit_prodl: forall a, is_cardinal a ->
    card_mult card_one a = a.
Lemma zero_prod_absorbing: forall a,
    card_mult a card_zero = card_zero.
Lemma zero_product_absorbing: forall f,
    fgraph f -> (exists i, inc i (domain f) & cardinal (V i f) = card_zero) ->
    cardinal_prod f = card_zero.

Let a and b be two cardinals; consider a set I equipotent to b and the two families \(a_i = a\) and \(c_i = 1\). Then

\[
ab = \sum_{i \in I} a_i; \quad b = \sum_{i \in I} c_i.
\]

The first formula is obtained from the second after multiplication by a, and using distributivity.

Lemma sum_of_ones: forall b j, is_cardinal b -> equipotent b j ->
    cardinal_sum (L j (fun _ => card_one)) = b.
Lemma sum_of_ones1: forall b,
    equipotent (cardinal_sum (cst_graph b card_one)) b.
Lemma sum_of_same: forall a b j, is_cardinal a -> is_cardinal b ->
    equipotent b j ->
    cardinal_sum (cst_graph j a) = card_mult a b.
Lemma sum_of_same1: forall a b,
    cardinal_sum (cst_graph b a) = card_mult a b.
Proposition 7 [2 p. 162] says that a cardinal product is non-zero if and only if each factor is non-zero (because a product is non-empty if and only if no factor is empty). Proposition 8 [2 p. 162] asserts injectivity of the successor function, namely that if \( a \) and \( b \) are two cardinals such that \( a + 1 = b + 1 \) then \( a = b \). In effect, there exists \( X \) equipotent to \( a \), \( Y \) equipotent to \( b \), and \( u \notin X, v \notin Y \) such that \( X \cup \{u\} = Y \cup \{v\} \). If \( u = v \), then \( X = Y \); otherwise, if \( Z = Y \cap Y \), we have \( X = Z \cup \{v\} \) and \( Y = Z \cup \{u\} \), so that if \( c = \text{card}(Z) \) we have \( a = b = c + 1 \).

Lemma disjoint_with_singleton: forall \( a, b \),
- \((\text{inc } b \ a) \rightarrow \text{disjoint } a \ (\text{singleton } b)\).

Theorem zero_cardinal_product: forall \( f \),
\((\text{fgraph } f) \rightarrow \forall i, \text{inc } i \ (\text{domain } f) \rightarrow \text{V } i \ f \neq \text{card_zero}) =
\text{cardinal_prod } f \neq \text{card_zero}.

Lemma zero_cardinal_product2: forall \( a, b \), \( a \neq \text{card_zero} \rightarrow b \neq \text{card_zero} \rightarrow
\text{card_mult } a \ b \neq \text{card_zero}.

Theorem succ_injective: forall \( a, b \), \( \text{is_cardinal } a \rightarrow \text{is_cardinal } b \rightarrow
\text{card_plus } a \ \text{card_one} = \text{card_plus } b \ \text{card_one} \rightarrow
a = b. \ (* 56 *)

4.5 Exponentiation of cardinals

If \( a \) and \( b \) are two cardinals, the cardinal of the set of functions from \( b \) to \( a \) is denoted \( a^b \), by abuse of notation.\(^2\) Proposition 9 [2 p. 163] says that we can replace \( a \) and \( b \) by equipotent sets.

Definition card_pow \( a, b := \text{cardinal } (\text{set_of_functions } b \ a)\).

Lemma card_pow_pr: forall \( a, b, a', b' \),
equipotent \( a \ a' \rightarrow \text{equipotent } b \ b' \rightarrow
\text{card_pow } a \ b = \text{card_pow } a' \ b'.

Theorem card_pow_pr1: forall \( x, y \),
\( \text{cardinal } (\text{set_of_functions } y \ x) = \text{card_pow } (\text{cardinal } x) \ (\text{cardinal } y) \).

Proposition 10 [2 p. 163] says that if \( a \) and \( b \) are two cardinals, \( I \) is a set with cardinal \( b \) and \( a \) \( \iota \) is the constant family \( a \), then \( a^b = \bigcup_{\iota \in I} a^\iota \). This is a trivial consequence of the fact that the set of functions and the set of graphs of functions are equipotent. Note: we do not need \( a \) and \( b \) to be cardinals. Note also that \( \text{Card}(I) = b \) implies that \( b \) is a cardinal, hence, we give also another version of the theorem.

A consequence is that, if \( a \) and \( b \) are cardinals, \((a_i)_{i \in I} \) and \((b_i)_{i \in I} \) are families of cardinals we have
\[
\sum_{i \in I} a_i^b_i = \prod_{i \in I} a_i^b_i, \quad \left( \prod_{i \in I} a_i \right)^b = \prod_{i \in I} a_i^b.
\]

The proof does not make use of the fact that the sets are cardinals, so we dropped the assumption. The proof of the first formula is as follows. Let \( a_i = a \). We have \( a_i \sum_{j \in J} b_j = \bigcup_{i \in I} a_i \), where \( J \) is any set whose cardinal is \( \sum_{i \in I} b_i \); we chose the disjoint union of the sets \( b_i \). We have a natural partition of \( J \) and we can apply the associativity of the product. For the second formula, let \( a_{i \beta} = a_i \) for \( i \in I \) and \( \beta \in b \). This is a family defined on the product \( I \times b \), for which we have

\(^2\)The trouble seems to be that \( 4^2 \) and \( 2^4 \) denote the set of graphs of mappings from 2 to 4 or from 4 to 2; these sets are obviously distinct, but have the same number of elements; hence \( 4^2 = 2^4 \) is true with these new notations, see page 132

RR n° 7150
have two natural partitions (all elements with the same $\tau$, or all elements with the same $\beta$); we can apply associativity of the product twice. We also have

\[(ab)^c = a^b c, \quad a^b c = a^{(b) c}.\]

Lemma card_pow_pr2: for all $a$, $b$,
\[\text{cardinal_product} (\text{cst}\_\text{graph} b \ a) = \text{card}_\text{pow} a \ b.\]

Theorem card_pow_pr3: for all $a$, $b$, $j$, cardinal $j = b$ ->
\[\text{cardinal_product} (\text{cst}\_\text{graph} j \ a) = \text{card}_\text{pow} a \ b.\]

Lemma power_of_sum: for all $a$, $f$, $f$\_\text{graph} $f$ ->
\[\text{card}_\text{pow} a (\text{card}_\text{sum} f) = \text{cardinal}\_\text{product} (L \ (\text{domain} f) \ (\text{fun} i => \text{card}_\text{pow} a (V i \ f))).\]

Lemma power_of_prod: for all $a$, $b$, $f$, $f$\_\text{graph} $f$ ->
\[\text{cardinal}_\text{product} (\text{cst}\_\text{graph} j \ a) = \text{card}_\text{pow} a \ b.\]

Lemma power_of_sum2: for all $a$, $b$, $c$,
\[\text{card}\_\text{pow} a (\text{card}_\text{plus} b \ c) = \text{card}_\text{mult} (\text{card}_\text{pow} \ a \ b) \ (\text{card}_\text{pow} \ a \ c).\]

Lemma power_of_prod2: for all $a$, $b$, $c$,
\[\text{card}_\text{pow} (\text{card}_\text{mult} \ a \ b) \ c = \text{card}_\text{mult} (\text{card}_\text{pow} \ a \ c) \ (\text{card}_\text{pow} \ b \ c).\]

The Bourbaki proof is the following. We want to compute the number of functions from $F$ to $E$ is some cases. If $F$ is empty, there is only the empty function; if $F$ is a singleton then $E^F$ are $E$ equinumerous (the bijection is product\_canon), if $E$ has a single element, there is only one function, a constant; finally if the source is non-empty and the target is empty, there is no function. We use different properties. In the first two cases, we replace the power by a product whose index set has 0 or 1 element, and simplify the result. In the third case we rewrite 1 as a product whose index set is empty, and use distributivity (9b).

Lemma power_x_0: for all $a$,
\[\text{card}_\text{pow} a \ \text{card}_\text{zero} = \text{card}_\text{one}.\]

Lemma power_0_0: \[\text{card}_\text{pow} \ \text{card}_\text{zero} \ \text{card}_\text{zero} = \text{card}_\text{one}.\]

Lemma power_x_1: for all $a$,
\[\text{is}_\text{cardinal} a \rightarrow \text{card}_\text{pow} a \ \text{card}_\text{one} = a.\]

Lemma power_1_x: for all $a$,
\[\text{card}_\text{pow} \ \text{card}_\text{one} \ a = \text{card}_\text{one}.\]

Lemma power_0_x: for all $a$,
\[\text{a <> card}_\text{zero} \rightarrow \text{card}_\text{pow} \ \text{card}_\text{zero} \ a = \text{card}_\text{zero}.\]

We have $1 + 1 = 2$, our proof uses formula (8.b), where $I$ is the canonical doubleton. A consequence is $a^2 = a \ a$.

Lemma card_two_pr: \[\text{card}_\text{two} = \text{card}_\text{plus} \ \text{card}_\text{one} \ \text{card}_\text{one}.\]

Lemma power_x_2: for all $a$,
\[\text{is}_\text{cardinal} a \rightarrow \text{card}_\text{pow} a \ \text{card}_\text{two} = \text{card}_\text{mult} a \ a.\]

The final result in this section is Proposition 12 [2, p. 164], it states that the cardinal of the power set of $X$ is $2^X$ (for each subset $Y$ of $X$, we can consider the characteristic function, whose value is 0 on $Y$ and 1 elsewhere).

Lemma card_powerset: for all $X$,
\[\text{cardinal} (\text{powerset} \ X) = \text{card}_\text{pow} \ \text{card}_\text{two} \ X.\]

INRIA
4.6 Order relation and operations on cardinals

Proposition 13 [2, p. 164] states that \( a \geq b \) if and only if there exists \( c \) such that \( a = b + c \) (for simplicity, we assume all three quantities to be cardinals, although \( c \) could be any set, and both relations \( a \geq b \) and \( a = b + c \) imply that \( a \) is a cardinal).

Proof. Assume \( B \) equipotent to a subset \( X \) of \( A \) and let \( C \) be the complement. Then \( B + C \) is equipotent to \( B_1 \cup C_2 \) (where \( B_1 = B \times \{1\} \)). We can replace \( B \) by \( X \), then omit the indices, so that \( B + C \) is equipotent to \( A \). Conversely, if \( A \) is equipotent \( B_1 \cup C_2 \), there is a bijection \( B_1 \cup C_2 \rightarrow A \), and by restriction, an injection \( B_1 \rightarrow A \), and by composition, an injection \( B \rightarrow A \).

Theorem cardinal_le_when_complement: forall a b, (* 36 *)
\[
\text{is_cardinal } a \rightarrow \text{is_cardinal } b \rightarrow
(\text{cardinal_le } b a) = (\exists c, \text{is_cardinal } c \land \text{card_plus } b c = a).
\]

Proposition 14 [2, p. 165] says that if \( a_i \geq b_i \) (for two families of cardinals) we have
\[
(\sum_{i \in I} a_i \geq \sum_{i \in I} b_i), \quad \left( \prod_{i \in I} a_i \geq \prod_{i \in I} b_i \right)
\]
The first formula is shown as follows. We have a bijection from \( b_i \) into a subset \( E_i \) of \( a_i \), hence a bijection from \( b_i \times \{i\} \) into a subset \( E_i \times \{i\} \) of \( a_i \times \{i\} \). This gives a bijection from the disjoint union \( \bigcup b_i \times \{i\} \) into a subset \( \bigcup E_i \times \{i\} \) of \( \bigcup a_i \times \{i\} \). The proof of the second formula is similar: we get a bijection from \( \prod b_i \) into a subset \( \prod E_i \) of \( \prod a_i \). As a corollary, we obtain a smaller result if we restrict the domain of the sum or the product; in the case of a product, we assume all factors distinct (proof: missing terms are replaced by zero, or one). The power is increasing with respect to both arguments.

Theorem sum_increasing: forall f g,
\[
fgraph f \rightarrow fgraph g \rightarrow \text{domain } f = \text{domain } g \rightarrow
(\forall x, \text{inc } x (\text{domain } f) \rightarrow \text{cardinal_le } (V x f) (V x g)) \rightarrow
\text{cardinal_le } (\text{cardinal_sum } f) (\text{cardinal_sum } g).
\]
Theorem product_increasing: forall f g,
\[
fgraph f \rightarrow fgraph g \rightarrow \text{domain } f = \text{domain } g \rightarrow
(\forall x, \text{inc } x (\text{domain } f) \rightarrow \text{cardinal_le } (V x f) (V x g)) \rightarrow
\text{cardinal_le } (\text{cardinal_prod } f) (\text{cardinal_prod } g).
\]
Lemma sum_increasing1: forall f j, fgraph f ->
\[
(\forall x, \text{inc } x (\text{domain } f) \rightarrow \text{is_cardinal } (V x f)) \rightarrow
\text{sub } j (\text{domain } f) \rightarrow \text{cardinal_le } (\text{cardinal_sum } (\text{restr } f j)) (\text{cardinal_sum } f).
\]
Lemma product_increasing1: forall f j, fgraph f ->
\[
(\forall x, \text{inc } x (\text{domain } f) \rightarrow \text{is_cardinal } (V x f)) \rightarrow
(\forall x, \text{inc } x (\text{domain } f) \rightarrow V x f \not< \text{card_zero}) \rightarrow
\text{sub } j (\text{domain } f) \rightarrow \text{cardinal_le } (\text{cardinal_prod } (\text{restr } f j)) (\text{cardinal_prod } f).
\]
Lemma sum_increasing2: forall a b a' b',
\[
\text{cardinal_le } a a' \rightarrow \text{cardinal_le } b b' \rightarrow
\text{cardinal_le } (\text{card_plus } a b) (\text{card_plus } a' b').
\]
Lemma product_increasing2: forall a b a' b',
\[
\text{cardinal_le } a a' \rightarrow \text{cardinal_le } b b' \rightarrow
\text{cardinal_le } (\text{card_mult } a b) (\text{card_mult } a' b').
\]
Lemma sum_increasing3: forall a b, \text{is_cardinal } a \rightarrow \text{is_cardinal } b \rightarrow
\text{cardinal_le } a (\text{card_plus } a b).
\]
Lemma product_increasing3: forall a b, \text{is_cardinal } a \rightarrow \text{is_cardinal } b \rightarrow
\text{card_zero} \rightarrow
\text{cardinal_le } a (\text{card_mult } a b).
Lemma power_increasing1 : forall a b a' b',
  a <> card_zero -> cardinal_le a a' -> cardinal_le b b' ->
  cardinal_le (card_pow a b) (card_pow a' b').

To conclude this chapter, we prove Cantor’s theorem (Theorem 2, [2, p. 165]) stating that
$2^a > a$ for every cardinal $a$, so that there is no set containing all cardinals.

Theorem cantor: forall a, is_cardinal a ->
  cardinal_lt a (card_pow card_two a).
Lemma cantor_bis: ~ (exists a, forall x, is_cardinal x -> inc x a).
Chapter 5

Natural integers. Finite sets

There are two kinds of sets and cardinals: the finite ones and the infinite ones. There is a set $N$ containing all finite cardinals, so that we have statements of the form: if $n \in N$ then $n \neq n + 1$, and no special font is required. Moreover, we think of elements of $N$ as elements, not sets: the relation $1 \neq 2$ means technically that either there is $x \in 1$ and $x \notin 2$ or there is $x \in 2$ and $x \notin 1$. One can define integers without using the axiom of choice, for instance, using pseudo-ordinals, case where $1 \subset 2$, so that there is $x \in 2$ and $x \notin 1$. All sensible definitions of integers as sets assume that 1 is a singleton and 2 a doubleton, so obviously at least one of the two elements of 2 is not an element of 1. Which one is irrelevant: integers are used to count objects. In this chapter, we give only some basic facts (addition, multiplication, subtraction and division are studied in the next chapter).

Integers are presented in [6] as follows. There is a symbol O and a symbol S, and two operations $a + b$ and $a \cdot b$ (sum and product), defined on integers, which are a finite (maybe empty) sequences of letters S followed by a single O. The five axioms are

1. Axiom 1 $\forall a, Sa \neq O.$
2. Axiom 2 $\forall a, a + O = a.$
3. Axiom 3 $\forall a \forall b, a + Sb = S(a + b).$
4. Axiom 4 $\forall a, a \cdot O = O.$
5. Axiom 5 $\forall a \forall b, a \cdot Sb = (a \cdot b) + a.$

The first axiom has an unusual form, since most axioms are of the form $a \implies b = c$. This axiom is built-in in Coq: an object of a type with $n$ constructors is defined by a single constructor: an integer is either O or Sa, but nor both. This means that if $c$ an integer, one and only one of axioms 2 and 3 apply to $a + c$. The axiom implies injectivity of S. Note that Coq defines addition an multiplication by induction on the first argument.

In the system presented above, it is impossible to prove $\forall a, a = O + a$, although the result is obvious for any $a$. Thus a new principle is needed. It says something like: "If all the strings in a pyramidal family are theorems, then so is the universally quantified string which summarizes them". (We get a pyramid if we center the statements $a = O + a$, for consecutive values of $a$). The whole pyramid has an infinite number of statements, and proving it requires an infinite proof. Assume that each line can be shown from the previous one, using exactly the same argument. Then the proof has that form P and Q and Q and Q, etc. It is infinite, but not too much, hence is accepted. The induction principle is: "Suppose $u$ is a variable, and $X(u)$ is a well-formed formula in which $u$ occurs free. If both $\forall u : X[u] \implies X[Su/u]$ and $X[0/u]$ are theorems, then $\forall u : X[u]$ is also a theorem." This is built-in in Coq, under the form

```coq
nat_ind =
fun P : nat -> Prop => nat_rect P
```

RR n° 7150
In this chapter we shall prove that the Bourbaki integers satisfy the induction principle, under the form

\[ \text{Lemma } \text{cardinal.c.induction.v: forall } r: \mathbb{E}, \]
\[ (r \text{ card_zero}) \rightarrow (\text{forall } n, \text{inc } n \text{ Bnat}\rightarrow r n \rightarrow r (\text{succ } n)) \]
\[ \rightarrow (\text{forall } n, \text{inc } n \text{ Bnat }\rightarrow r n). \]

and as a consequence, that all these definitions are essentially the same. The proof of the principle is as follows: the least element of the set (assumed non-empty) of elements not satisfying a property is either 0 or Sa. This is a consequence of the fact that \( \mathbb{N} \) is well-ordered. Note that the property shown by induction (\( X, P, r, \) in the examples) is quantified in Coq, but neither in \[6\] nor in Bourbaki.

An important property of integers is the possibility of defining a function by induction. This is a Coq example

```
Fixpoint add (n m:nat) {struct n} : nat :=
match n with
| O => m
| S p => S (add p m)
end.
```

This definition says that the source is \( \mathbb{N} \times \mathbb{N} \), induction is on \( n \), and the result is of type \( \mathbb{N} \). By induction, there is at most one function satisfying Axioms 2 and 3. In Bourbaki, one could define, for each \( m \), a function \( f_m: \mathbb{N} \rightarrow E_m \), which is the unique surjective function satisfying the two axioms, show that \( E_m \subset \mathbb{N} \), extend the function \( f'_m: \mathbb{N} \rightarrow \mathbb{N} \), then merge all these functions to get \( f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \). This function cannot be defined without first showing the existence of the set of integers (You will be have to wait until Chapter 6 for this). It is however possible to prove by induction that addition satisfies the two axioms (if one replaces “\( n \in \mathbb{N} \)” by “\( n \) is a finite cardinal” in the induction principle). Obviously, definition by induction is a particular case of definition by transfinite induction. Exercise 2.17 defines sum and product, exercise 2.18 defines exponentiation of ordinals. The situation is simpler: since there is no set containing all ordinals, what has to be defined is not a function; it is called an “ordinal functional symbol”, this is something that associates an ordinal to a pair of ordinals.

5.1 Definition of integers

A \textit{finite} cardinal is one that satisfies \( a \neq a + 1 \). This will be called an \textit{integer}. The quantity \( a + 1 \) is the \textit{successor} of \( a \).

Definition \text{succ } x := \text{card_plus } x \text{ card_one}.
Definition \text{is_finite_c } x := \text{is_cardinal } x \& x \leftrightarrow \text{succ } x.
Definition \text{is_finite_set } x := \text{is_finite_c } (\text{cardinal } x).
Definition \text{card_three } := \text{succ } \text{card_two}.
Definition \text{card_four } := \text{succ } \text{card_three}.

If \( a \) is finite, so is \( a + 1 \), by injectivity of the successor function. The converse is obvious. This is Proposition 1 [2] p. 166]. It follows that 0, 1, 2, 3 and 4 are finite.
Lemma integer_is_cardinal: forall x, is_finite_c x -> is_cardinal x.
Lemma succ_is_cardinal: forall a, is_cardinal (succ a).
Lemma cardinal_succ: forall a, cardinal (succ a) = succ a.
Lemma is_finite_succ1: forall x, is_finite_c x -> is_finite_c (succ x).

Theorem is_finite_succ: forall x, is_cardinal x ->
(is_finite_c x) = (is_finite_c (succ x)).
Lemma succ_cardinal: forall z, succ (cardinal z) = succ z.
Lemma is_finite_succ1: forall x, is_finite_c x -> is_finite_c (succ x).
Lemma is_finite_succ2: forall x, is_finite_set x -> is_finite_c (succ x).
Lemma succ_zero: succ card_zero = card_one.

Lemma is_finite0: is_finite_c card_zero.
Lemma is_finite1: is_finite_c card_one.
Lemma is_finite2: is_finite_c card_two.
Lemma is_finite3: is_finite_c card_three.
Lemma is_finite4: is_finite_c card_four.

5.2 Inequalities between integers

Proposition 2 [2, p. 166] says that if a is a cardinal and n an integer, if a \leq n then a is an integer. If n is an integer and n \neq 0, then there is a unique integer m such that n = m + 1. In this case a < n is equivalent to a \leq m. If a + b is an integer and a is a cardinal, then a is an integer. The same holds in the case of a product, if b \neq 0.

Lemma cardinal_le_when_complement1: forall a b,
  cardinal_le b a -> (exists c, is_cardinal c & card_plus b c = a).
Lemma succ_injective: forall a b, is_cardinal a -> is_cardinal b ->
succ a = succ b -> a = b.
Lemma is_less_than_succ: forall a, is_cardinal a ->
cardinal_le a (succ a).
Lemma is_finite_in_sum: forall a b, is_cardinal b ->
is_finite_c (card_plus a b) -> is_finite_c b.
Lemma cardinal_le when complement2: forall a b, is_cardinal a ->
is_finite_c (card_plus a b) -> is_finite_c a.
Theorem le_int_is_int: forall a b, is_finite_c b ->
cardinal_le a b -> is_finite_c a.
Lemma finite_in_product: forall a b, is_cardinal a -> is_cardinal b ->
b \neq card_zero -> is_finite_c (card_mult a b) -> is_finite_c a.

For each non-zero cardinal a, there is a unique cardinal b such that a = b + 1. It is called the predecessor of a (uniqueness follows from injectivity of the successor function, we show it only in the case where a is finite). We changed the definition of the predecessor in Version 2; as a consequence, whenever a and b are cardinals, the latter being non-zero, there exists c such that ab = ac + a. If this expression is finite, so is a.

Definition predc n := choose (fun m => is_cardinal m & n = succ m).

Lemma predc_pr0: forall n, is_cardinal n -> n <> card_zero ->
is_cardinal (predc n) & n = succ (predc n).
Lemma predc_pr: forall n, is_finite_c n -> n <> card_zero ->
is_finite_c (predc n) & n = succ (predc n).
Theorem exists_predc: forall n, is_finite_c n -> n <> card_zero ->
exists_unique (fun m => is_finite_c m & n = succ m).
Lemma finite_in_product: forall a b, is_cardinal a -> is_cardinal b ->
b <> card_zero -> is_finite_c (card_mult a b) -> is_finite_c a.
Theorem lt_is_le_succ: forall a n, is_finite_c n ->
cardinal_lt a (succ n) = cardinal_le a n.

Lemma lt_is_le_succ1: forall a b, is_finite_c b ->
cardinal_le a (succ b) -> a <> (succ b) -> cardinal_le a b.

Lemma lt_n_succ_le1: forall a b, is_cardinal a -> is_finite_c b ->
cardinal_le (succ a) (succ b).

Lemma succ_nonzero1: forall n, cardinal_le card_one (succ n).

Lemma succ_nonzero: forall n, succ n <> card_zero.

Lemma predc_pr1: forall n, is_cardinal n -> predc (succ n) = n.

Lemma succ_positive: forall a, cardinal_lt card_zero (succ a).

Lemma lt_n_succ_le0: forall a b, is_cardinal a -> is_finite_c b ->
cardinal_le (succ a) b = cardinal_lt a b.

As a corollary, every subset of a finite set is finite. If X ⊆ Y, X ≠ Y and Y is finite, then
Card(X) < Card(Y). Bourbaki says that the converse is true by definition. In fact, if Y is empty,
it is finite, otherwise there is x ∈ Y, and if X is the complement of {x} in Y, then Card(Y) =
Card(X) + 1. The relation Card(X) < Card(Y) implies that Card(X) is finite, hence Card(X) + 1
is also finite.

Lemma sub_finite_set: forall x y, sub x y -> is_finite_set y ->
is_finite_set x.

Lemma cardinal_succ_pr0: forall a b, equipotent a b -> succ a = succ b.

Lemma cardinal_succ_pr: forall a b, ~ (inc b a) ->
cardinal (tack_on a b) = succ a.

Lemma cardinal_succ_pr1: forall a b,
cardinal (tack_on (complement a (singleton b)) b) =
succ (cardinal (complement a (singleton b))).

Lemma strict_sub_smaller: forall x y, sub x y -> is_finite_set y ->
x<> y -> cardinal_lt (cardinal x) (cardinal y).

Lemma strict_sub_smaller1: forall y,
(forall x, sub x y -> x<> y -> cardinal_lt (cardinal x) (cardinal y)) ->
is_finite_set y.

The image of a finite set by a function is finite. We give some variants of this property.
Consider two sets E and F with the same cardinal, and a function f: E → F. Assume E finite.
If f is injective and not surjective, then f(E) is a strict subset of F equipotent to F, thus cannot
be finite. Hence we claim: if f injective, then f is bijective. Assume f surjective. It has a right
inverse, which is injective, so that f is also bijective.

Lemma finite_image: forall f, is_function f -> is_finite_set (source f) ->
is_finite_set (image_of_fun f).

Lemma finite_image_by: forall f A, is_function f -> sub A (source f) ->
is_finite_set A -> is_finite_set (image_by_fun f A).

Lemma finite_image_by: forall f A, is_function f -> sub A (source f) ->
is_finite_set A -> is_finite_set (image_by_fun f A).

Lemma finite_image: forall f, is_function f -> is_finite_set (source f) ->
is_finite_set (image_of_fun f).

Lemma finite_range: forall f, fgraph f -> is_finite_set(domain f) ->
is_finite_set (range f).

Lemma finite_graph_domain: forall f, fgraph f ->
is_finite_set f -> is_finite_set (domain f).

Lemma finite_graph_range: forall f, fgraph f ->
is_finite_set f -> is_finite_set (range f).

Lemma finite_domain_graph: forall f, fgraph f ->
is_finite_set (domain f) -> is_finite_set f.

Lemma bijective_if_same_finite_c_inj: forall f,
cardinal (source f) = cardinal (target f) -> is_finite_set (source f) ->
is_finite_set (target f).
Lemma injective f -> bijective f.

Lemma sub_image_of_fun: forall f x, is_function f -> sub x (source f) -> sub (image_by_fun f x) (image_of_fun f).

Lemma bijective_if_same_finite_c_surj: forall f, cardinal (source f) = cardinal (target f) -> isFiniteSet (source f) -> surjective f -> bijective f.

5.3 The set of natural integers

Bourbaki introduces the set $\mathbb{N}$ of natural integers in the Chapter 6; he needs an axiom that asserts the existence of an infinite set; in Coq, we know that $\mathbb{N}$ exists; it is infinite. Instead of saying “for all $x$ and $y$, if $x$ and $y$ are finite cardinals, then $x+y$ is a finite cardinal”, we will say “for all $x \in \mathbb{N}$ and $y \in \mathbb{N}$ we have $x+y \in \mathbb{N}$.

Remember that $\mathbb{N}$ is the set of all $S^kO$, i.e., the set that contains O, SO, SSO, SSSO, etc. The mapping $x \mapsto Sx$ is injective but not surjective. Let’s denote by $s$ the Bourbaki function associated to $S$. It is injective and not surjective. The previous previous theorem implies that $\mathbb{N}$ cannot be finite. We say that $\alpha$ is an infinite cardinal if it is a cardinal, but not a finite cardinal, and we set that $E$ is an infinite set if it is not finite, i.e., when its cardinal is infinite. If $\alpha$ is finite and $\beta$ is infinite, then $\alpha < \beta$ thus $\alpha \leq \beta$. As a consequence, the set of all finite cardinals $\leq \beta$ it is the set of all finite cardinals. This gives a set $\mathbb{N}$ such that $x \in \mathbb{N} \iff x$ is a finite cardinal.

Definition is_infinite_c a := is_cardinal a & ~ (is_finite_c a).
Definition infinite_set E := is_infinite_c (cardinal E).

Definition Bnat := Zo(set_of_cardinals_le (cardinal nat)) (fun z => is_finite_c z).

Lemma finite_lt_infinite: forall a b, is_finite_c a -> is_infinite_c b -> cardinal_lt a b.

Lemma finite_le_infinite: forall a b, is_finite_c a -> is_infinite_c b -> cardinal_le a b.

Lemma S_inj_not_bij: injective (acreate S) & (~ surjective (acreate S)).
Lemma nat_infinite_set: is_infinite_c (cardinal nat).
Lemma finite_smaller_infinite: forall a b, is_finite_c a -> is_infinite_c b -> cardinal_lt a b.

Lemma inc_Bnat: forall a, inc a Bnat = is_finite_c a.
Opaque Bnat.

Lemma Bnat_is_cardinal: forall x, inc x Bnat -> is_cardinal x.

We define $x \leq_N y$ to be “$x \in \mathbb{N}$ and $y \in \mathbb{N}$ and $x \leq_{\text{Card}} y$”. This is a well-ordering on $\mathbb{N}$.

Definition Bnat_order := graph_on cardinal_le Bnat.
Definition Bnat_le x y := inc x Bnat & inc y Bnat & cardinal_le x y.
Definition Bnat_lt x y := Bnat_le x y & x<>y.

Lemma substrate_Bnat_order: substrate Bnat_order = Bnat.
Lemma worder_Bnat_order: worder Bnat_order.
Lemma related_Bnat_order: forall x y, gle Bnat_order x y = Bnat_le x y.
We now restate some theorems of the form "\(x\) is finite" as \(x \in \mathbb{N}\).

- Lemma inc0_Bnat: inc card_zero Bnat.
- Lemma inc1_Bnat: inc card_one Bnat.
- Lemma inc2_Bnat: inc card_two Bnat.
- Lemma inc_succ_Bnat: forall x, inc x Bnat -> inc (succ x) Bnat.
- Lemma le_int_in_Bnat: forall a b, cardinal_le a b -> inc b Bnat -> inc a Bnat.

### 5.4 The principle of induction

If a property \(p\) is true for 0 and if \(p(n) \implies p(n+1)\) for all integers \(n\), then \(p\) is true for all integers \(n\) (let \(X\) be the set of cardinals \(\leq n\) that do not satisfy \(p\). If \(n \notin X\) then \(p(n)\) is true, otherwise \(X\) is non-empty and well-ordered; its least element is an integer \(m\); we know that \(m\) cannot be 0, hence is of the form \(n+1\) and \(p(n)\) is false, hence \(n \in X\), absurd).

We give four variants of the principle. Let \(S(n)\) be the relation: \(n\) is an integer and \(R\) is true for all integers \(p < n\). If \(S\) implies \(R\), then \(R\) is true for all integers.

If \(R(a)\) is true, and if \(R(n)\) together with \(a \leq n < b\) implies \(R(n+1)\), then for all \(n\) such that \(a \leq n \leq b\), the relation \(R\) is true. In both cases \(n\) must be an integer (in the second case, we assume \(b\) integer, so that \(n < b\) or \(n \leq b\) implies that \(n\) is an integer). Bourbaki uses induction on \(a \leq n < b \implies R(n)\), but it is simpler to use \(a \leq n \leq b \implies R(n)\).

The last variant is: if \(a \leq n < b\) and \(R(n+1)\) implies \(R(n)\), if moreover \(R(b)\) is true, then \(a \leq n \leq b\) implies \(R(n)\). The proof is by induction on \(P = \neg R\). If \(R\) is false for some \(n\) with \(a \leq n \leq b\) then \(P\) is true for some \(c\) with \(a \leq c < b\). On the other hand, if \(a \leq n < b\) then \(P(n)\) implies \(P(n+1)\).

- Lemma cardinal_c_induction: forall r:EP, 
  (r card_zero) -> (forall n, is_finite_c n -> r n -> r (succ n))
  -> (forall n, is_finite_c n -> r n).
- Lemma cardinal_c_induction1: forall r:EP,
  let s:= fun n => forall p, is_finite_c n -> is_finite_c p -> cardinal_le p n -> r p in
  (forall n, is_finite_c n -> s n -> r n) ->
  (forall n, is_finite_c n -> r n).
- Lemma cardinal_c_induction2: forall (r:EP) k,
  is_finite_c k -> r k ->
  (forall n, is_finite_c n -> cardinal_le k n -> r n -> r (succ n))
  -> (forall n, is_finite_c n -> cardinal_le k n -> r n).
- Lemma cardinal_c_induction3: forall (r:EP) a b,
  is_finite_c a -> is_finite_c b -> r a ->
  (forall n, cardinal_le a n -> cardinal_le b n -> r n -> r (succ n))
  -> (forall n, cardinal_le a n -> cardinal_le b n -> r n).
- Lemma cardinal_c_induction4: forall (r:EP) a b,
  is_finite_c a -> is_finite_c b -> r b ->
  (forall n, cardinal_le a n -> cardinal_le b n -> r (succ n) -> r n)
  -> (forall n, cardinal_le a n -> cardinal_le b n -> r n).

We rewrite our induction principle with \(x \in \mathbb{N}\) instead of "\(x\) is a finite cardinal". We rewrite variants 3 and 4, replacing \(a \leq n \leq b\) by \(n \in [a, b]\). We first rewrite \(n \in [a, b]\) as \(a \leq n \leq b\). We then as \(a \leq \text{Card } n \leq b\). The trick is that \(n \leq \text{Card } b\) implies \(n \in \mathbb{N}\).
Lemma Bnat_interval_cc_pr:forall a b x,inc a Bnat->inc b Bnat->
inc x (interval cc Bnat_order a b) = (Bnat_le a x & Bnat_le x b).
Lemma Bnat_interval_co_pr:forall a b x,inc a Bnat->inc b Bnat->
inc x (interval co Bnat_order a b) = (Bnat_le a x & Bnat_lt x b).
Lemma Bnat_interval_cc_pr1:forall a b x,inc a Bnat->inc b Bnat->
inc x (interval cc Bnat_order a b) = (cardinal_le a x & cardinal_le x b).
Lemma Bnat_interval_co_pr1:forall a b x,inc a Bnat->inc b Bnat->
inc x (interval co Bnat_order a b) = (cardinal_le a x & cardinal_lt x b).

The empty set is finite, and if X is finite then \( X \cup \{x\} \) is finite. We then show a partial converse, that will be useful for induction on finite sets. If X has cardinal zero, it is the empty set, and if X has cardinal \( n + 1 \), it is of the form \( X' \cup \{x\} \), where \( X' \) has cardinal \( n \).

Lemma predc_pr2:forall n,inc n Bnat->predc (succ n) = n.
Lemma emptyset_finite:is_finite_set (emptyset).
Lemma tack_on_finite:forall X x, is_finite_set X -> is_finite_set(tack_on X x).
Lemma singleton_finite:forall x, is_finite_set(singleton x).
Lemma doubleton_finite:forall x y, is_finite_set(doubleton x y).
Lemma card_one_not_zero:card_one <> card_zero.
Lemma tack_if_succ_card:forall x n, is_cardinal n -> cardinal x = succ n ->
exists u, exists v, x = tack_on u v & ~(inc v u) & cardinal u = n.

The induction principle on finite sets is now: If a property P is true for the empty set, if P(a) implies P(a \cup \{b\}), then P is true for every finite set. In general P has the form: if A then B. Note: if \( b \in a \), then \( a \cup \{b\} = a \), and we have a version where we add the condition \( b \notin a \).

Lemma finite_set_induction0:forall s:EP,
s emptyset -> (forall a b, s (a) -> ~(inc b a) -> s (tack_on a b)) ->
forall x, is_finite_set x -> s x.
Lemma finite_set_induction:forall s:EP,
s emptyset -> (forall a b, s (a) -> s (tack_on a b)) ->
forall x, is_finite_set x -> s x.
Lemma finite_set_induction1:forall (A B:EP) x,
(A emptyset -> B emptyset)
-> (forall a b, (A a -> B a) -> A(tack_on a b) -> B(tack_on a b))
-> is_finite_set x -> A x -> B x.

In some cases P is false for the empty set. If P is true for all singletons, then P is true for every non-empty finite set.

Lemma finite_set_induction2:forall (A B:EP) x,
\[\begin{align*}
&\text{(forall } a, A (\text{singleton } a) \rightarrow B (\text{singleton } a)) \\
&\quad \rightarrow (\text{forall } a b, (A a \rightarrow \text{nonempty } a \rightarrow B a) \rightarrow \\
&\qquad \text{nonempty } a \rightarrow A (\text{tack_on } a b) \rightarrow B (\text{tack_on } a b)) \\
&\quad \rightarrow \text{is_finite_set } x \rightarrow A x \rightarrow \text{nonempty } x \rightarrow B x.
\end{align*}\]

The next lemmas correspond to Exercise 4.1. If we denote by \(\mathcal{F}(E)\) the set of finite subsets of \(E\), and by \(P(E, \emptyset)\) the property: (i) \(\emptyset \in \mathcal{F}\); (ii) the relation \(X \in \mathcal{F}\) and \(x \in E\) imply \(X \cup \{x\} \in \mathcal{F}\), then \(P(E, \emptyset)\) is true; by induction, \(P(E, \emptyset)\) implies \(\mathcal{F} \subseteq \emptyset\). As a consequence, the union of two finite sets is finite. The powerset of a finite set is finite (proof by induction: \(\mathcal{P}(X \cup \{x\})\) is the union of \(\mathcal{P}(X)\) and the image of \(\mathcal{P}(X)\) by the mapping \(Y \mapsto (Y \cup \{x\})\); if \(x \notin X\), the union is disjoint, and the cardinal is twice the cardinal of \(\mathcal{P}(X)\).)

Definition set_of_finite_subsets \(E := \text{Zo(powerset } E)(\text{fun } X \Rightarrow \text{is_finite_set } X)\).

Definition set_of_finite_subsets_prop \(E F := \text{inc emptyset } F \& \text{forall } x X, \text{inc } x E \rightarrow \text{inc } X F \rightarrow \text{inc } (\text{tack_on } X x) F\).

Lemma set_of_finite_subsets_pr: \(\text{forall } E,\)
\(\text{set_of_finite_subsets_prop } E (\text{set_of_finite_subsets } E) \&\)
\(\text{(forall } F, \text{set_of_finite_subsets_prop } E F \rightarrow \text{sub } (\text{set_of_finite_subsets } E) F)\).

Lemma finite_union2: \(\text{forall } x y, \text{is_finite_set } x \rightarrow \text{is_finite_set } y \rightarrow \)
\(\text{is_finite_set } (\text{union2 } x y)\).

Lemma finite_powerset: \(\text{forall } x, \text{is_finite_set } x \rightarrow \text{is_finite_set } (\text{powerset } x)\). (* 36 *)

### 5.5 Finite subsets of ordered sets

Let \(\leq\) be an order relation on a set \(E\) that makes it a directed set, a lattice, or a totally ordered set; and let \(X\) be a finite non-empty subset of \(E\). Then \(X\) has an upper bound, or has a least upper bound and a greatest lower bound, or has a least and greatest element respectively (Proposition 3, [2, p. 170]). We have to show that there is an \(x\) such that \(P(x, X)\). By assumption, this is true if \(X\) is a doubleton (therefore, if \(X\) is a singleton). If \(X = Y \cup \{b\}\) and \(P(a, X)\) we have to show the property for the doubleton \(\{a, b\}\).

Lemma finite_set_induction3: \(\text{forall } (p:EEP) E X,\)
\(\text{(forall } a b, \text{inc } a E \rightarrow \text{inc } b E \rightarrow \exists y, p \text{ (doubleton } a b) y \rightarrow \)
\(\text{(forall } a b x y, \text{sub } a E \rightarrow \text{inc } b E \rightarrow \exists p \text{ a x } \rightarrow p \text{ (doubleton } x b) y \rightarrow \)
\(p \text{ (tack_on } a b) y \rightarrow \)
\(\text{(forall } X x, \text{sub } X E \rightarrow \text{nonempty } X \rightarrow \exists p \text{ x } \rightarrow \text{inc } x E \rightarrow \)
\(\text{nonempty } X \rightarrow \text{is_finite_set } X \rightarrow \text{sub } X E \rightarrow \exists x, p X x)\).

Lemma finite_subset_directed_bounded: \(\text{forall } r X,\)
\(\text{right_directed } r \rightarrow \text{is_finite_set } X \rightarrow \text{sub } X \text{ (substrate } r) \rightarrow \text{nonempty } X \)
\(\rightarrow \text{bounded_above } r X\).

Lemma finite_subset_lattice_inf: \(\text{forall } r X,\)
\(\text{lattice } r \rightarrow \text{is_finite_set } X \rightarrow \text{sub } X \text{ (substrate } r) \rightarrow \text{nonempty } X \)
\(\rightarrow \exists x, \text{greatest_lower_bound } r X x\).

Lemma finite_subset_lattice_sup: \(\text{forall } r X,\)
\(\text{lattice } r \rightarrow \text{is_finite_set } X \rightarrow \text{sub } X \text{ (substrate } r) \rightarrow \text{nonempty } X \)
\(\rightarrow \exists x, \text{least_upper_bound } r X x\).

Lemma finite_subset_torder_greatest: \(\text{forall } r X,\)

INRIA
Some consequences. A nonempty finite set (the word “nonempty” is missing in Bourbaki) has a maximal element, and if totally ordered, has a greatest element. A finite totally ordered set is well-ordered.

\[
\text{Lemma finite_set_torder_greatest: } \forall r, \text{total_order } r \rightarrow \text{is_finite_set } (\text{substrate } r) \rightarrow \text{nonempty } (\text{substrate } r) \rightarrow \exists x, \text{greatest_element } (\text{induced_order } r \ X) \ x. \\
\text{Lemma finite_set_torder_worder: } \forall r, \text{total_order } r \rightarrow \text{is_finite_set } (\text{substrate } r) \rightarrow \text{worder } r. \\
\text{Lemma finite_set_maximal: } \forall r, \text{order } r \rightarrow \text{is_finite_set } (\text{substrate } r) \rightarrow \text{nonempty } (\text{substrate } r) \rightarrow \exists x, \text{maximal_element } r \ x.
\]

5.6 Properties of finite character

If \( E \) is a set, a property \( P \) of \( X \) (where \( X \) is a subset of \( E \)) is said to be of finite character if the set \( \mathcal{S} \) of all \( X \) satisfying \( P \) is of finite character; this means \( X \in \mathcal{S} \) if and only if every finite subset \( Y \) of \( X \) satisfies \( Y \in \mathcal{S} \). Example: the set of totally ordered subsets of an ordered set. Theorem 1 [2, p. 171] states: Every set \( \mathcal{S} \) of subsets of a set \( E \) which is of finite character has a maximal element (when ordered by inclusion). The word “nonempty” is missing: if \( X \in \mathcal{S} \), then \( \emptyset \) is a finite subset of \( X \); hence \( \emptyset \in \mathcal{S} \). But the empty set is of finite character.

Definition of finite_character \( s := \forall x, \text{(inc } x \ s) = (\forall y, (\text{sub } y \ x \ \& \ \text{is_finite_set } y) \rightarrow \text{inc } y \ s). \)

Lemma of_finite_character_example: \( \forall r, \text{order } r \rightarrow \text{of_finite_character } (\text{Zo } (\text{powerset } (\text{substrate } r))) \ (\text{fun } z \Rightarrow \text{total_order } (\text{induced_order } r \ z))). \)

Lemma maximal_inclusion: \( \forall s, \text{of_finite_character } s \rightarrow \text{nonempty } s \rightarrow \exists x, \text{maximal_element } (\text{inclusion_suborder } s) \ x. \)

5.7 Finite cardinals and the type nat

5.7.1 Pseudo-ordinals

This section is an answer to Exercise 20 of section 2 of Bourbaki. In an early edition of the book, a pseudo-ordinal was defined as a set \( E \) satisfying the three following properties: (1) \( \emptyset \in E \), (2) if \( y \in E \) and \( x \in y \) then \( x \in E \), (3) the relation \( "x \in E \text{ and } y \in E \text{ and } (x = y \text{ or } x \in y)" \) is a well-order in \( E \). If \( F \) is a well-ordered set, the ordinal of \( F \) is a well-ordered set (defined via the axiom of choice) isomorphic to \( F \); the purpose of the exercise was to show that every well-ordered set is isomorphic to a unique pseudo-ordinal, so that one could define the ordinal of a set as this unique pseudo-ordinal.

In fact, ordinals are defined in this way in [7], before introducing the axiom of choice. However, condition (1) has been replaced by: there are no \( x \) and \( y \) in \( E \) such that \( x \in y \) and
José Grimm

If \( y \in x \). If \( y \) is the smallest element of \( E \), then \( x \in y \) implies \( x \in E \), hence \( y = x \) or \( y \in x \), which are absurd; thus, if \( E \) is not empty, \( \emptyset \in E \). On the other hand, if \( E = \{ \emptyset, E \} \), then \( E \) is a pseudo-ordinal according to (1), (2) and (3) (whether such a set exists is undecidable). The new definition of pseudo-ordinals given below is completely different.

We denote here by \( T(x) \) the quantity \( x \cup \{ x \} \). A set \( X \) is transitive if \( x \in X \) implies \( x \subseteq X \). A set \( S \) is called decent if \( x \in S \) implies \( x \notin x \). A pseudo-ordinal is a set \( X \) such that, if \( Y \) is a transitive subset of \( X \), distinct from \( X \), then \( Y \) is an element of \( X \).

**Definition**

\[
\text{transitive} \ X := \forall x, \text{inc} \ x \ X \rightarrow \text{sub} \ x \ X.
\]

**Definition**

\[
\text{pseudo} \text{-} \text{ordinal} \ X := \forall Y, \text{sub} \ Y \ X \rightarrow \text{transitive} \ Y \rightarrow
\]

\[
Y \not\in X \rightarrow \text{inc} \ Y \ X.
\]

**Definition**

\[
\text{decent} \ X := \forall y, \text{inc} \ y \ x \rightarrow \neg \ (\text{inc} \ y \ y).
\]

If \( X \) is transitive so is \( T(X) \). Unions and intersections of transitive sets are transitive. A pseudo-ordinal is transitive and decent. If \( X \) is a pseudo-ordinal, so is \( T(X) \). The empty set is a pseudo-ordinal.

**Lemma**

\[
\text{transitive} \text{-} \text{tack} \text{-} \text{on} \text{-} \text{itself} : \forall y,
\]

\[
\text{transitive} \ Y \rightarrow \text{transitive} \ (\text{tack} \_ \text{on} \ y \ y).
\]

**Lemma**

\[
\text{transitive} \text{-} \text{union} : \forall x, (\forall y, \text{inc} \ y \ x \rightarrow \text{transitive} \ y)
\]

\[
\rightarrow \text{transitive} \ (\text{union} \ x).
\]

**Lemma**

\[
\text{transitive} \text{-} \text{intersection} : \forall x, (\forall y, \text{inc} \ y \ x \rightarrow \text{transitive} \ y)
\]

\[
\rightarrow \text{nonempty} \ x \rightarrow \text{transitive} \ (\text{intersection} \ x).
\]

**Lemma**

\[
\text{pseudo} \text{-} \text{ordinal} \text{-} \text{transitive} \text{-} \text{1} : \forall x,
\]

\[
\text{pseudo} \text{-} \text{ordinal} \ x \rightarrow (\text{transitive} \ x \ & \ \text{decent} \ x). (** 17**) \]

**Lemma**

\[
\text{pseudo} \text{-} \text{ordinal} \text{-} \text{transitive} : \forall x,
\]

\[
\text{pseudo} \text{-} \text{ordinal} \ x \rightarrow \text{transitive} \ x.
\]

**Lemma**

\[
\text{pseudo} \text{-} \text{ordinal} \text{-} \text{tack} \text{-} \text{on} : \forall x,
\]

\[
\text{pseudo} \text{-} \text{ordinal} \ x \rightarrow \text{pseudo} \text{-} \text{ordinal} \ (\text{tack} \_ \text{on} \ x \ x).
\]

**Lemma**

\[
\text{pseudo} \text{-} \text{ordinal} \text{-} \text{empty} \text{-} \text{set} : \text{pseudo} \text{-} \text{ordinal} \ \text{empty} \text{-} \text{set}.
\]

**Lemma**

\[
\text{pseudo} \not\text{-} \text{inc} \text{-} \text{itself} : \forall x, \text{pseudo} \text{-} \text{ordinal} \ x \rightarrow \neg (\text{inc} \ x \ x).
\]

If \( X \) and \( Y \) are two pseudo-ordinals, we have \( X \in Y \) or \( Y \in X \) or \( X = Y \). A transitive set is a pseudo ordinal whenever all elements are pseudo-ordinals. As a consequence all elements of a pseudo-ordinal are pseudo-ordinals. The intersection of a family of pseudo-ordinals is the smallest element for the inclusion order (i.e., is an element of the family). Thus, a pseudo-ordinal is well-ordered for the inclusion order.

**Lemma**

\[
\text{pseudo} \text{-} \text{ordinal} \text{-} \text{dichotomy} : \forall x, y,
\]

\[
(\text{inc} \ x \ y \ \vee \ \text{inc} \ y \ x \ \vee \ x = y).
\]

**Lemma**

\[
\text{pseudo} \text{-} \text{ordinal} \text{-} \text{pr} : \forall x, \text{transitive} \ x \rightarrow
\]

\[
(\forall y, \text{inc} \ y \ x \rightarrow \text{pseudo} \text{-} \text{ordinal} \ y) \rightarrow
\]

\[
\text{pseudo} \text{-} \text{ordinal} \ x.
\]

**Lemma**

\[
\text{pseudo} \text{-} \text{ordinal} \text{-} \text{empty} : \text{pseudo} \text{-} \text{ordinal} \ \text{empty} \text{-} \text{set}.
\]

**Lemma**

\[
\text{inc} \text{-} \text{pseudo} \text{-} \text{pseudo} : \forall x, y, \text{pseudo} \text{-} \text{ordinal} \ x \rightarrow \text{inc} \ y \ x \rightarrow
\]

\[
\text{pseudo} \text{-} \text{ordinal} \ y.
\]

**Lemma**

\[
\text{intersection} \text{-} \text{of} \text{-} \text{pseudo} \text{-} \text{ordinals} : \forall x, \text{nonempty} \ x \rightarrow
\]

\[
(\forall a, \text{inc} \ a \ x \rightarrow \text{pseudo} \text{-} \text{ordinal} \ a) \rightarrow \text{inc} \ (\text{intersection} \ x) \ x.
\]

**Lemma**

\[
\text{worder} \text{-} \text{sub} \text{-} \text{ordinal} : \forall x, \text{pseudo} \text{-} \text{ordinal} \ x \rightarrow
\]

\[
\text{worder} \ (\text{inclusion} \text{-} \text{suborder} \ x).
\]

The conclusion of Exercise 20 is: for every ordinal \( \alpha \) there exists a unique pseudo-ordinal \( E_\alpha \) such that \( \text{Ord}(E_\alpha) = \alpha \). Exercise 2.13 defines \( \text{Is}(\Gamma, \Gamma') \) as the property that \( \Gamma \) and \( \Gamma' \) are two
orderings and there is an isomorphism between the two orderings (compare with Eq(E,E′), that says that there a bijection between the two set), and Ord(Γ) to be ℏ(Γ,Δ) (compare with Card(E)). This is called the order-type of Γ. The order type of a well-ordered set is called an ordinal in Exercise 14.

We show here that, for every well-ordered set E, there exists a unique pseudo-ordinal X and an order isomorphism between E and X. Uniqueness is proved as follows. Let X and Y be two pseudo-ordinals, and f an isomorphism. This means that if a ∈ X and b ∈ X then a < b is equivalent to f(a) < f(b). Since a, b, f(a) and f(b) are pseudo ordinals, a ∈ E is equivalent to f(a) ∈ f(b). Let A be the subset of X formed of all a such that f(a) ≠ a. If A is not empty, it has a smallest element b (because X is well-ordered). If c ∈ b, then c < b and c ≠ b, hence c /∈ A and f(c) = c. On the other hand, if u ∈ f(b), then u ∈ Y by transitivity of Y, so that u = f(v) for some v ∈ X. From f(v) ∈ f(b) we deduce v ∈ b, hence v = f(v) = u thus f(b) ⊂ b. Since f(b) is a pseudo-ordinal distinct from b we deduce f(b) ∈ b, hence f f(b) = f(b) hence f(b) = b by injectivity, absurd. Thus A is empty, and f(a) = a for all a ∈ X. This implies X ⊂ Y; by surjectivity we have X = Y.

Let p(f, x) be the set f(x), namely the set of all f(y) for y ∈ x. Assume that ≤ is a well-ordering on a set E and define a function f by transfinite induction on E via p. This means that for every x ∈ E, we have f(x) = f(|→, x|), where |→, x| is the set of all b such that b < x. From the definition we get f(a) ∈ f(b) if a < b and f(a) ⊂ f(b) if a ≤ b. Assume f(a) ∈ f(a); every w ∈ f(a) is of the form f(v) for v < a; if w = f(a), we find v < a such that f(v) ∈ f(v). The set of all a such that f(a) ∈ f(a) has no smallest element hence is empty. This implies injectivity of f; so that f is an order isomorphism (where the target of f is ordered by inclusion). If x ∈ f(a), then x = f(b) for some b < a, thus f(b) ⊂ f(a) and f(a) is transitive. If a is the smallest element such that f(a) is not a pseudo-ordinal, then all its elements are pseudo-ordinals; contradiction. Since the image of f is transitive and contains only pseudo-ordinals, it is a pseudo-ordinal.

Lemma pseudo_ordinal_isomorphism_unique: forall x y f, pseudo_ordinal x -> pseudo_ordinal y -> order_isomorphism f (inclusion_suborder x)(inclusion_suborder y) -> x = y. (* 53 *)

Lemma pseudo_ordinal_isomorphism_exists: forall r, worder r -> exists y, exists f, (pseudo_ordinal y & order_isomorphism f r (inclusion_suborder y)). (* 71 *)

One can define the cardinal of a set E as the smallest pseudo-ordinal equipotent to it. This avoids using the axiom of choice. Of course, in order to show that a set is equipotent to a pseudo-ordinal, we use Zermelo's theorem, put a well-ordering on the set, and use the previous result. Let X be such a pseudo-ordinal. Let Y be the smallest pseudo-ordinal equipotent to E (in the well-ordered set X). Let Z be a pseudo-ordinal equipotent to E. If Z ⊂ Y, then Z ⊂ X by transitivity of X; by definition of Y we have Y ⊂ Z, absurd. Thus Y ⊂ Z. This property shows that Y does not depend on X.

Lemma pseudo_ordinal_pr1: forall x, exists y, pseudo_ordinal y & equipotent x y & (forall z, pseudo_ordinal z -> equipotent x z -> sub y z).

5.7.2 Pseudo-ordinals and the type nat

Our implementation of Bourbaki in Coq relies on the fact that a set is a type, and if a is a set, a ∈ B means a = Rb for some b of type B (where R denotes Ro). This is an abstract
construction. If we define a type \( A \) with two constructors \( B \) and \( C \), then \( AB \in A \) and \( AC \in A \). We assume \( R \) injective; since \( B \neq C \) by construction, the set \( A \) has two distinct elements \( AB \) and \( AC \). The only property of \( AB \) is that it is one of the two elements of \( A \). A property of the form \( AB = \emptyset \) is undecidable.

Let's now define a more complicated type, \( nat \), denoted \( \mathbb{N} \); it has a constant constructor \( O \), and another constructor \( S \) that is a function on \( \mathbb{N} \). This means that, whenever \( x \) is of type \( \mathbb{N} \), then \( Sx \) is also of type \( \mathbb{N} \). This set satisfies the principle of induction (that says under which condition a property is true for the elements of this set), and we can define a function by induction. Later on, Bourbaki introduces \( \mathbb{N} \), the set of finite cardinals. It satisfies the principle of induction (see section 5.4), and functions can be defined by induction (Chapter six, section 7.2), as a variant of definition by transfinite induction of the well-ordered set \( \mathbb{N} \).

In the next section, we shall show that \( \mathbb{N} \) and \( \mathbb{N} \) are isomorphic; in this section we compare \( \mathbb{N} \) and the collection of finite pseudo-ordinals (this is in fact a set, but it will not be used).

Since \( Sn \) is of type \( \mathbb{N} \) whenever \( n \) is of type \( \mathbb{N} \), we can define a function \( s \) such that \( s(a) \in \mathbb{N} \) whenever \( a \in \mathbb{N} \): if \( a \in \mathbb{N} \) and \( a = R(b) \) then \( s(a) = R(S(b)) \). As noted above, a property of the form \( RO = \emptyset \) is undecidable. Although the exact value of \( s(RO) \) is unknown, we can show some properties of \( s \): for instance, \( s \) is injective and not surjective (there is a unique way to construct an object of type \( \mathbb{N} \); so that \( Sx \) is never \( O \) and \( Sx = Sy \) implies \( x = y \)). The Coq parser and pretty printer identify \( O \) and \( 0 \), \( SO \) and \( 1 \), \( SSO \) and \( 2 \). In order to avoid confusion, we shall write \( 0 \), \( 1 \) and \( 2 \) for the cardinals (note that \( 0 = \emptyset \)).

Let's define by induction a function \( f \) by \( f(0) = RO \) and \( f(n + 1) = R(S(R(f(n)))) \) where \( a = R(f(n)) \) is defined by \( Ra = f(n) \). For instance \( f(1) = R(1) \). The property “\( f \) is the identity function” (more precisely \( f = R \)) is undecidable (it cannot be proved; we hope that adding it as an axiom does not make the theory contradictory).

The type \( \mathbb{N} \) is called \( nat \) in Coq; it has an order relation, noted \( \leq \), and two operations + and \( * \), that correspond, via the bijection \( f \), to comparison, sum and product of finite cardinals. We shall import all theorems about natural integers from the Coq library by identification of \( \mathbb{N} \) and \( \mathbb{N} \). Given that \( \emptyset = f(0) = RO = RO \), we may assume \( RO = \emptyset \). The relation \( f(1) = R(1) \) suggest that \( R(1) \) should be \( 1 \), but this is a set defined via the axiom of choice, as a set with one element; it could be \( \{ \emptyset \} \), it could also be any other set. We will add the relation \( R(SO) = \{ \emptyset \} \) as axiom. As a consequence \( R(SO) \) is unlikely to be a cardinal, but it will allow us to construct a function card, such that \( \text{card}(x) = 1 \) whenever \( x \) is a singleton, i.e., whenever \( \text{Card}(x) = 1 \). The two axioms relating \( R \) and \( 0 \) have been introduced by Carlos Simpson in the following way:

\[
\begin{align*}
(*) & \quad \text{Axiom nat_realization_0 : } \forall x : \text{Set}, \neg x \in (\text{Ro } 0). \\
& \quad \text{Axiom nat_realization_S :} \\
& \quad \quad \forall (n : \text{nat}) (x : \text{Set}), \\
& \quad \quad \quad (\text{inc } (\text{Ro } (S n)) - (\text{inc } (\text{Ro } n)) \lor x = \text{Ro } n).
\end{align*}
\]

\[
\text{Lemma nat_zero_emptyset : } \text{Ro } 0 = \emptyset.
\]

These axioms are useless, hence have been withdrawn. On the other hand, we can define a function that shares exactly the same properties. The first axioms defines a set \( RO \) that contains no element, hence is the emptyset. The second axioms defines \( R(Sn) \), that is equal (by extensionality) to \( T(Rn) \). Thus, we define \( natR \) denoted by \( R_N \), via \( R_N 0 = \emptyset \) and \( R_N(Sn) = T(R_N n) \).

\[
\text{Fixpoint natR } (n: \text{nat}) :=
\]
The conclusion of Exercise 20 is: In particular the pseudo-ordinals whose order-type are 0, 1, 2 = 1 + 1, and 3 = 2 + 1 are respectively
\[ \emptyset, \{\emptyset\}, \{\emptyset,\{\emptyset\}\}, \{\emptyset,\{\emptyset\},\{\emptyset\}\}. \]

Lemma value_R_0: natR 0 = emptyset.
Lemma value_R_1: natR 1 = singleton emptyset.
Lemma value_R_2: natR 2 = doubleton (singleton emptyset) emptyset.
Lemma value_R_3: let tripleton a b c := tack_on (doubleton a b) c in
\[ \text{natR 3} = \text{tripleton (doubleton (singleton emptyset) emptyset)} \]
\[ \text{singleton emptyset) emptyset}. \]

If \(a\) is a pseudo-ordinal, then so is \(T(a)\). By induction, we deduce that if \(n\) is of type \(\text{nat}\), \(\mathcal{R}_\text{N} n\) is a finite pseudo-ordinal.

Lemma pseudo_ordinal_Rnat: forall i, pseudo_ordinal (natR i).
Lemma finite_Rnat: forall i, is_finite_set (natR i).

Define a relation \(\leq\) on \(\text{nat}\) by the properties:
\[ \forall x, x \leq x \text{ and } \forall x y, x \leq y \implies x \leq S(y). \]
This is reflexive and transitive. Showing that it is an order is not completely trivial (see the Coq library). One can show that the relation \(x < y\), defined by \(Sx \leq y\), is equivalent to \(x \leq y\) and \(x \neq y\).

It is clear by induction that if \(x \leq y\) then \(\mathcal{R}_\text{N} x \subset \mathcal{R}_\text{N} y\). If \(x < y\) then \(\mathcal{R}_\text{N} (Sx) \subset \mathcal{R}_\text{N} y\), hence \(\mathcal{R}_\text{N} x \in \mathcal{R}_\text{N} y\). If \(\mathcal{R}_\text{N} x \subset \mathcal{R}_\text{N} y\), then \(x \leq y\), for otherwise we would have \(y < x\), hence \(\mathcal{R}_\text{N} y \in \mathcal{R}_\text{N} x\), absurd. In the same fashion, \(x < y\) is equivalent to \(\mathcal{R}_\text{N} (Sx) \subset \mathcal{R}_\text{N} y\).

Note that, if \(\mathcal{R}_\text{N} i = \mathcal{R}_\text{N} j\), then \(\mathcal{R}_\text{N} i \subset \mathcal{R}_\text{N} j\) and \(\mathcal{R}_\text{N} j \subset \mathcal{R}_\text{N} i\), this \(i \leq j\) and \(j \leq i\); hence \(i = j\). This shows injectivity of \(\mathcal{R}_\text{N}\).

Lemma Rnat_le_implies_sub : forall i j, i <= j -> sub (natR i) (natR j).
Lemma Rnat_lt_implies_inc : forall i j, i < j -> inc (natR i) (natR j).
Lemma Rnat_lt_implies_strict_sub : forall i j, i < j -> strict_sub (natR i) (natR j).
Lemma Rnot_inc_itself: forall i, ~ (inc (natR i)(natR i)).
Lemma Rnat_inc_lt : forall i j, inc (natR i) (natR j) = (i < j).

As a consequence, if \(i < j\) then \(\text{Card}(\mathcal{R}_\text{N} i) < \text{Card}(\mathcal{R}_\text{N} j)\), and if \(\text{Card}(\mathcal{R}_\text{N} i) = \text{Card}(\mathcal{R}_\text{N} j)\), then \(i = j\). From this, we deduce that each finite cardinal is of the form \(\text{Card}(\mathcal{R}_\text{N}(i))\) for a unique \(i\).

Lemma cardinal_Rnat_lt: forall i j, i< j -> cardinal_lt (cardinal (natR i)) (cardinal (natR j)).
Lemma cardinal_Rnat_inj: forall i j, cardinal (natR i) = cardinal (natR j) -> i = j.
Lemma exists_nat_cardinal: forall a, is_finite_c a -> exists_unique(fun i:nat => cardinal (natR i)=a).
We can now introduce a function $\text{card}(n)$ making the following diagram commutative

(Finite cardinals)

\[
\begin{array}{ccc}
\text{Set} & \xrightarrow{\text{Card}} & \mathbb{N} \\
\text{card} & \downarrow & \\
\mathbb{N} & \xrightarrow{\text{Card}} & \text{Set}
\end{array}
\]

In this diagram, $\mathbb{N}$, Set and $\mathbb{N}$ are types; $\mathbb{N}$ is the set of natural numbers (as a Coq type), and $\mathbb{N}$ is the collection of cardinals (the objects $x$ such that $x$ is a cardinal do not form a set, neither a type, we call it a collection). We use the notation $\mathbb{N}$ to emphasize that if $x$ is a finite set, then its cardinal is a member of the set of finite cardinals. If $x$ is not finite, we define $\text{card}(x)$ to be 0, in this case the diagram does not commute. If however $n$ is finite we have $\text{Card}(\mathbb{N}(\text{card}(n))) = \text{Card}(n)$. By uniqueness, we have $\text{card}(\mathbb{N}(i)) = i$ for every nat $i$. If $A$ is a finite set, then $\text{Card}A = \text{Card}B$ implies $\text{card}A = \text{card}B$. The converse is true if both sets are finite.

Definition cardinal_nat $x :=$ choosenat(fun $i => \text{cardinal} (\text{natR } i) = x$).

Lemma cardinal_nat_cardinal: forall $x$, $\text{cardinal} (\text{cardinal} x) = \text{cardinal} x$.

Lemma cardinal_nat_pr: forall $x$, is_finite_set $x$ -> $\text{cardinal} (\text{natR} (\text{cardinal} x)) = \text{cardinal} x$.

Lemma cardinal_nat_pr1: forall $i$, $\text{cardinal} (\text{natR} i) = i$.

Lemma cardinal_nat_finite_eq: forall $a b$, is_finite_set $a$ -> cardinal $a = \text{cardinal} b$ -> cardinal $a = \text{cardinal} b$.

Lemma cardinal_nat_finite_eq1: forall $a b$, is_finite_set $a$ -> is_finite_set $b$ -> cardinal $a = \text{cardinal} b$ -> cardinal $a = \text{cardinal} b$.

5.7.3 Bijection between nat and the integers

Denote by $s(n)$ the successor of $n$. We have $s(0) = 1$, and $a + s(n) = s(a + n)$ (associativity of the sum). We have $a.s(b) = ab + a$ and $a.0 = 0$. By induction we deduced that the sum and product of two integers are integers.

Lemma plus_via_succ: forall $a n$, $\text{card_plus a} (\text{succ n}) = \text{succ} (\text{card_plus a n})$.

Lemma Bnat_stable_plus: forall $a b$, inc a Bnat -> inc b Bnat -> inc (card_plus a b) Bnat.

Lemma mult_via_plus: forall $a b$, is_cardinal a ->
We define now by induction a function $\mathcal{N}$ that associates a cardinal to each $\text{nat}$; by construction $\mathcal{N}(0) = 0$ and $\mathcal{N}(S(n)) = s_0(\mathcal{N}(n))$. This function converts addition and multiplication on $\text{nat}$ to cardinal sum and cardinal product (induction on $\mathbb{N}$). This function is injective (because $\text{succ}$ is injective). By induction on $\mathbb{N}$, this function is surjective. More precisely, every finite cardinal has the form $\mathcal{N}(n)$. Assume $a \leq b$; then $\mathcal{N}(a) \leq_\text{Card} \mathcal{N}(b)$; conversely, if this relation holds then $\mathcal{N}(a) + x = \mathcal{N}(b)$ for some $x$. By surjectivity $x = \mathcal{N}(c)$, by injectivity $a + c = b$ which implies $a \leq b$. By injectivity of $\mathcal{N}$ we deduce that $a < b$ and $\mathcal{N}(a) <_\text{Card} \mathcal{N}(b)$ are equivalent.

Let $g$ be the inverse of $\mathcal{N}$; such a function exists using the axiom of choice. By uniqueness this function is card, hence $\text{card}(\mathcal{N}(x)) = x$ and $\mathcal{N}(\text{card}(x)) = x$.

We finish with the definition of the power function on $\mathbb{N}$.

Fixpoint pow (n m:nat) {struct m} : nat :=
match m with 0 => 1 | S p => (pow n p) * n end
where "n ^ m" := (pow n m) : nat_scope.
Chapter 6

Properties of integers

Bourbaki introduces the set of integers in the next chapter, while we have done so in the previous one. As a consequence, in all theorems, the phrase "x is an integer" will be replaced by $x \in \mathbb{N}$. Sometimes, we shall use $x \in \mathbb{N}$ or $x : \mathbb{N}$, where $\mathbb{N}$ is the set of finite cardinals and $\mathbb{N}$ is the type $\text{nat}$. The function $\mathcal{N}$ is the natural bijection between $\mathbb{N}$ and $\mathbb{N}$.

6.1 Operations on integers and finite sets

Consider a finite family $x_i$. This means that we have a functional graph $G$, with domain $I$, and an associated mapping $i \mapsto x_i$. Induction can be performed on the domain, the range or the graph: for instance, we can show by induction on the range of the family that the union of finite sets is finite, or that the supremum is finite. In these two cases, $\sup x_i$ or $\bigcup x_i$, the result depends only on the range (and one can consider the supremum of union of a set of sets, instead of a family). This is false in the case of a sum (we know that if $x_i = 1$, the sum is the cardinal of the index set, so that the range can be a singleton and the sum infinite).

In all these cases, we have a function $F$ (union, supremum, sum) and a function $g$ such that $F(x_1, x_2, \ldots, x_n) = g(x_1, F(x_2, \ldots, x_n))$. This formula allows us to prove properties by induction on the length $n$ of the sequence (for $n \geq 2$). We may have $F(x) = x$, in which case we can handle the case $n = 1$. In the case of the sum or union, the case $n = 0$ is trivial, in the case of the intersection or supremum, the function is not defined if the sequence is empty. Finite sequences (i.e. sequences where indices are 1, 2, 3, etc.) will be studied later. If $g$ is not commutative, we can define $F$ only in the case where the index set is ordered; if $g$ is commutative (as in the examples above), any ordering can be used, and there is no need to convert the finite family into a finite sequence. We know that union, sum, supremum are associative. In some cases, we want to prove an associativity formula for a function $F$ defined as above, for a non-commutative function $g$ (this is basic algebra). We shall explain how this can be done, in section 6.4.

We show that a finite sum $\sum_{i \in I} x_i$ of integers is an integer, by considering $f(I) = \sum_{i \in I} x_i$. The proof is by induction on the cardinal of $I$. If $I = I' \cup \{j\}$, and $j \notin I'$, we have a partition of $I$, with index set $K = \{1, 2\}$, and we can apply the associativity formula. It says $f(I) = \sum_{k \in K} y_k$. Since $K$ has two elements this is $y_1 + y_2$, and we know that the sum of two integers is an integer. We have $y_1 = f(I')$ and $y_2 = x_j$ (in both cases, a double restriction is involved). A trivial consequence of these considerations will be that $x_i \leq \sum x_j$. We start with some ancillary lemmas.
Lemma domain_restr_empty: forall f, fgraph f ->
    domain (restr f emptyset) = emptyset.
Lemma double_restr: forall f a b, fgraph f ->
    sub a b -> sub b (domain f) ->
    (restr (restr f b) a) = (restr f a).
Lemma trivial_cardinal_sum3: forall f a, fgraph f ->
    inc a (domain f) -> is_cardinal (V a f) ->
    cardinal_sum (restr f (singleton a)) = V a f.
Lemma trivial_cardinal_prod3: forall f a, fgraph f ->
    inc a (domain f) -> is_cardinal (V a f) ->
    cardinal_prod (restr f (singleton a)) = V a f.
Lemma partition_tack_on: forall a b, ~ inc b a ->
    partition_fam (Lvariantc a (singleton b)) (tack_on a b).
Lemma partition_complement: forall a b, inc b a ->
    partition_fam (Lvariantc (complement a (singleton b)) (singleton b)) a.

Given a family of cardinals $a_i$ with sum $S$ and product $P$ we have $a_i \leq S$ and $a_i \leq P$, whenever all factors are non-zero.

Lemma sum_increasing6: forall f j, fgraph f ->
    (forall x, inc x (domain f) -> is_cardinal (V x f)) ->
    inc j (domain f) -> cardinal_le (V j f) (cardinal_sum f).
Lemma prod_increasing6: forall f j, fgraph f ->
    (forall x, inc x (domain f) -> is_cardinal (V x f)) ->
    (forall x, inc x (domain f) -> V x f <> card_zero) ->
    inc j (domain f) -> cardinal_le (V j f) (cardinal_prod f).

A finite family of integers is a functional graph $i \in I \mapsto x_i$ where $I$ is finite and each $x_i$ is finite. We may rewrite this as $x_i \in \mathbb{N}$.

Definition finite_int_fam f:= fgraph f &
    (forall i, inc i (domain f) -> inc (V i f) Bnat) &
    is_finite_set (domain f).

Proposition 1 [2, p. 171] says that if $(a_i)_{i \in I}$ is a finite family of integers, then $\sum_{i \in I} a_i$ and
$\prod_{i \in I} a_i$ are integers. As a consequence, if $J \subset I$ then $\sum_{i \in J} a_i$ and $\prod_{i \in J} a_i$ are integers. As explained above, we first show the result for all $J$, by induction on the cardinal, then consider the special case $J = I$.

Lemma finite_sum_finite_aux: forall f x, finite_int_fam f ->
    sub x (domain f) -> inc (cardinal_sum (restr f x)) Bnat.
Lemma finite_product_finite_aux: forall f x, finite_int_fam f ->
    sub x (domain f) -> inc (cardinal_prod (restr f x)) Bnat.
Theorem finite_sum_finite: forall f, finite_int_fam f ->
    inc (cardinal_sum f) Bnat.
Theorem finite_product_finite: forall f, finite_int_fam f ->
    inc (cardinal_prod f) Bnat.

We have obvious consequences. For instance, a finite union of finite sets is finite. As explained above, this is easy by induction. Bourbaki says that, if $E$ is the union and $S$ is the sum, then $S$ is finite, and, since there is a surjection from $S$ onto $E$, we have $\text{Card}(E) \leq S$, so that $\text{card}(E)$ is finite. However $\text{Card}(E) \leq S$ has already been stated (as corollary to Proposition 4).
A finite product of finite sets is a finite set (since the cardinal of the product is the product of the cardinals). Since \( a^b \) is a product, it is finite if \( a \) and \( b \) is finite. Thus, the powerset of a finite set is finite.

**Lemma finite_union_finite:** For all \( f \), fgraph \( f \) -
(forall \( i \), inc \( i \) (domain \( f \)) -> is_finite_set (V \( i \) \( f \)))
-> is_finite_set (domain \( f \)) -> is_finite_set (unionb \( f \)).

**Lemma finite_product_finite_set:** For all \( f \), fgraph \( f \) -
(forall \( i \), inc \( i \) (domain \( f \)) -> is_finite_set (V \( i \) \( f \)))
-> is_finite_set (domain \( f \)) -> is_finite_set (productb \( f \)).

**Lemma finite_c_set:** For all \( b \), is_finite_c \( b \) -> is_finite_set \( b \).

**Lemma Bnat_stable_pow:** For all \( a \) and \( b \), inc \( a \) Bnat -> inc \( b \) Bnat ->
inc (card_pow \( a \) \( b \)) Bnat.

**Lemma finite_powerset:** For all \( a \), is_finite_set \( a \) -> is_finite_set (powerset \( a \)).

### 6.2 Strict inequalities between integers

We start this section with a list of some definitions and theorems, extracted from the Coq library. Consider for instance \( \text{zerop} \). We show its type, not its value which is irrelevant for the use we shall make of it; this value is a proof that for every \( n \) (of type \( \text{nat} \)), one of \( A \) or \( B \) is true. This is summarized by the notation \([A] + [B]\) (certified disjoint union). The \textit{heavyside} function is not part of the library, it is an example of how this construction can be used. The underscores in the definition represent the two proofs. The Coq parser and pretty-printer interpret this in the same fashion as \( \text{if} \ zerop \ n \ \text{then} \ 0 \ \text{else} \ 1 \). A property is decidable if it can be shown true of false. For us, all properties are decidable since we have an axiom that says so. It is however useful to know that equality and inequality are decidable. We state also some theorems such as if \( n \leq m \) is false then \( n > m \) is true. In this case, the result is a consequence of the fact that one of the properties is true.

\[
\begin{align*}
\text{Definition zerop} \ n & : \ {n = 0} + \ {0 < n}.
\text{Definition lt_eq_lt_dec} \ n \ m & : \ {n < m} + \ {n = m} + \ {m < n}.
\text{Definition gt_eq_gt_dec} \ n \ m & : \ {m > n} + \ {n = m} + \ {n > m}.
\text{Definition le_lt_dec} \ n \ m & : \ {n \leq m} + \ {m < n}.
\text{Definition le_le_S_dec} \ n \ m & : \ {n \leq m} + \ {S m \leq n}.
\text{Definition le_ge_dec} \ n \ m & : \ {n \leq m} + \ {n = m}.
\text{Definition le_gt_dec} \ n \ m & : \ {n \leq m} + \ {n > m}.
\text{Definition le_lt_eq_dec} \ n \ m & : \ n \leq m \Rightarrow \ {n < m} + \ {n = m}.
\text{Definition heavyside} \ n & := \text{match} \ (\text{zerop} \ n) \ \text{with} \ \text{left} \ _ \Rightarrow \ 0 \ | \ \text{right} \ _ \Rightarrow \ 1 \ \text{end}.
\end{align*}
\]

**Theorem dec_le:** For all \( n \) and \( m \), decidable \( (n \leq m) \).
**Theorem dec_lt:** For all \( n \) and \( m \), decidable \( (n < m) \).

**Theorem dec_ge:** For all \( n \) and \( m \), decidable \( (n \geq m) \).

**Theorem not_eq:** For all \( n \) and \( m \), \( n \neq m \Rightarrow n < m \lor m < n \).

**Theorem not_le:** For all \( n \) and \( m \), \( \neg n \leq m \Rightarrow n > m \).

**Theorem not_gt:** For all \( n \) and \( m \), \( \neg n > m \Rightarrow n \leq m \).

**Theorem not_ge:** For all \( n \) and \( m \), \( \neg n \geq m \Rightarrow n < m \).

**Theorem not_lt:** For all \( n \) and \( m \), \( \neg n < m \Rightarrow n \geq m \).

*)
Proposition 2 [2, p. 173] says that \( a < b \) if and only if there is \( c \) such that \( 0 < c \) and \( b = c + a \).

Proof. From \( a < b \) we deduce \( b \neq 0 \), hence \( b = Sb' \) and \( a \leq b' \). As a consequence \( b' = a + c' \), and \( b = Sb' = S(a + c') = a + Sc' \). The first relation says that \( c' \) is an integer, so that \( Sc' \) is an integer; it is obviously \( > 0 \). Conversely, from \( a \leq a \) we get \( a < Sa \), i.e. \( a < a + 1 \), and from \( 0 < c \) we get \( 1 \leq c \). Since addition is increasing we have \( a + 1 \leq a + c \) and we conclude by transitivity.

In our implementation, we first prove the result for the type \( \text{nat} \).

Theorem \( \text{lt_to_plus} \): for all \( a: \text{nat} \), \( a < b \) exists \( c: \text{nat} \), \( 0 < c \) \& \( c + a = b \).

Theorem \( \text{cardinal_lt_pr} \): for all \( a \) \& \( b \), \( \text{inc} a \) \& \( \text{inc} b \) \& \( \text{Bnat} \rightarrow \text{inc} b \) \& \( \text{Bnat} \rightarrow \)
\( \text{exists} c: \text{nat} \), \( \text{is_finite_c} c \) \& \( \text{cardinal_lt} \) \& \( \text{card_zero} c \) \& \( b = \text{card_plus} a c \).

We give here a list of theorems of the standard Coq library, that relate addition, multiplication and order. We add a theorem that says that if \( a < b \) and \( c \leq d \) then \( ac < bd \) (whenever \( d \neq 0 \)).

(* These are in the Coq library

\[
\begin{align*}
\text{Lemma plus_reg_l : } & \text{forall} n m p, \ p + n = p + m \rightarrow n = m. \\
\text{Lemma plus_le_reg_l : } & \text{forall} n m p, \ p + n \leq p + m \rightarrow n \leq m. \\
\text{Lemma plus_lt_reg_l : } & \text{forall} n m p, \ p + n < p + m \rightarrow n < m. \\
\text{Lemma plus_le_compat_l : } & \text{forall} n m p, \ n \leq m \rightarrow p + n \leq p + m. \\
\text{Lemma plus_le_compat_r : } & \text{forall} n m p, \ n \leq m \rightarrow n + p \leq m + p. \\
\text{Lemma le_plus_l : } & \text{forall} n m, \ n \leq n + m. \\
\text{Lemma le_plus_r : } & \text{forall} n m, \ m \leq n + m. \\
\text{Theorem le_plus_trans : } & \text{forall} n m p, \ n \leq m \rightarrow n \leq m + p. \\
\text{Theorem lt_plus_trans : } & \text{forall} n m p, \ n < m \rightarrow n < m + p. \\
\text{Lemma plus_lt_compat_l : } & \text{forall} n m p, \ n < m \rightarrow p + n < p + m. \\
\text{Lemma plus_lt_compat_r : } & \text{forall} n m p, \ n < m \rightarrow n + p < m + p. \\
\text{Lemma plus_le_compat : } & \text{forall} n m p q, \ n \leq m \rightarrow p + q \leq p + q. \\
\text{Lemma plus_le_lt_compat : } & \text{forall} n m p q, \ n \leq m \rightarrow p + q \leq m + q. \\
\text{Lemma plus_lt_le_compat : } & \text{forall} n m p q, \ n < m \rightarrow p + q < m + q. \\
\text{Lemma plus_lt_compat : } & \text{forall} n m p q, \ n < m \rightarrow p + q < m + q. \\
\text{Lemma mult_0_le : } & \text{forall} n m, \ m = 0 \rightarrow n \leq n * m. \\
\text{Lemma mult_le_reg : } & \text{forall} n m p, \ n \leq m \rightarrow p * n \leq p * m. \\
\text{Lemma mult_le_compat_l : } & \text{forall} n m p, \ n \leq m \rightarrow n * p \leq m * p. \\
\text{Lemma mult_le_compat_r : } & \text{forall} n m p, \ n \leq m \rightarrow p * n \leq p * m. \\
\text{Lemma mult_le_compat : } \\
& \text{forall} n m p q, \ n \leq m \rightarrow p + q \rightarrow n * p \leq m * q. \\
\text{Lemma mult_S_le_reg_l : } & \text{forall} n m p q, \ n < m \rightarrow S n + m \leq S n + p. \\
\text{Lemma mult_S_lt_compat_l : } & \text{forall} n m p q, \ n < m \rightarrow S n + m \leq S n + q. \\
\text{Lemma mult_S_reg_l : } & \text{forall} n m p q, \ n \leq m \rightarrow S n + m \leq S n + p. 
\end{align*}
\)

(*}

\[
\begin{align*}
\text{Lemma mult_S_le_reg_l : } & \text{forall} n m p q, \ n \leq m \rightarrow p + q \rightarrow n * p \leq m * q. \\
\text{Lemma mult_S_le_reg_r : } & \text{forall} n m p q, \ n \leq m \rightarrow p + q \rightarrow n * p \leq m * q. \\
\text{Lemma zero_lt_one : } & \text{cardinal_lt} \text{card_zero} \text{card_one}. \\
\text{Lemma zero_lt_oneN : } & 0 < 1. \\
\end{align*}
\]

Proposition 3 [2, p. 173] says that \( \sum a_i < \sum b_i \) and \( \prod a_i < \prod b_i \) for two families of integers with the same index set, if \( a_i \leq b_i \) for each \( i \) and \( a_j < b_j \) for some \( j \). In the case of a product,
$b_i > 0$ is required. The case where the family has two elements is a consequence of the statements given above. In the general case, assume $a_j < b_j$, and consider the partition $J \cup \{j\}$ of $I$. We have $\sum_{i \in J} a_i = A + a_j$, where $A = \sum_{i \in J} a_i$ (we use the same argument as when showing that the sum is finite). In the same way, $\sum_{i \in J} b_i = B + b_j$, and $A \leq B$. The proof in the case of the product is similar. Note that $A$ is finite since it is the sum of a restriction.

Consequences: if $a < a'$ then $a + b < a' + b$. This implies $a + 1 < a' + 1$, thus $a + 1 \leq a'$.

Lemma finite_sum2_lt: forall a b a' b',
  inc a Bnat -> inc b Bnat -> inc a' Bnat -> inc b' Bnat->
  cardinal_le a a' -> cardinal_lt b b' ->
  cardinal_le (card_plus a b) (card_plus a' b').

Lemma finite_sum3_lt: forall a a' b,
  inc a Bnat -> inc b Bnat -> inc a' Bnat ->
  cardinal_le a a' -> cardinal_gt b b' ->
  cardinal_le (card_plus a b) (card_plus a' b).

Lemma lt_n_succ_le: forall a b, inc a Bnat -> inc b Bnat ->
  cardinal_le (succ a) b= cardinal_lt a b .

Lemma lt_n_succ_leN: forall a b, a < b -> S a <= b.

Lemma finite_prod2_lt: forall a b a' b',
  inc a Bnat -> inc b Bnat -> inc a' Bnat -> inc b' Bnat->
  cardinal_le a a' -> cardinal_lt b b' -> a' <> card_zero ->
  cardinal_lt (card_mult a b) (card_mult a' b').

Theorem finite_sum_lt: forall f g,
  finite_int_fam f -> finite_int_fam g -> domain f = domain g ->
  (forall i, inc i (domain f) -> cardinal_le (V i f) (V i g)) ->
  (exists i, inc i (domain f) & cardinal_lt (V i f) (V i g)) ->
  cardinal_lt (cardinal_sum f) (cardinal_sum g).

Theorem finite_product_lt: forall f g,
  finite_int_fam f -> finite_int_fam g -> domain f = domain g ->
  (forall i, inc i (domain f) -> cardinal_le (V i f) (V i g)) ->
  (exists i, inc i (domain f) & cardinal_gt (V i f) (V i g)) ->
  cardinal_gt (cardinal_prod f) (cardinal_prod g).

Consequences: $a < a'$ implies $0 < a'$. If $0 < a$ and $1 < b$ then $a < ab$. If $a > 0$ and $b \geq 1$ then $a^b \geq a$ (this holds also for infinite cardinals). We have $a^b < a^{b'}$ if $a < a'$ and $b > 0$ (the first condition implies $a' > 0$). We have $a^b < a^{b'}$ if $a > 1$ and $b < b'$ (the case $a = 0$ is special, if $a = 1$, both terms are 1). Writing $b' = b + x$ we must show $a^b < a^{b+1}$. If $b > 1$ we get $a < b^{b'}$.

Lemma special_cardinal_positive: forall a a',
  cardinal lt a a' -> cardinal lt card_zero a'.

Lemma finite_lt_a_ab: forall a b, inc a Bnat -> inc b Bnat ->
  cardinal lt card_zero a -> cardinal lt card_one b ->
  cardinal lt a (card_mult a b).

Lemma cardinal_le_a_apowb: forall a b,
  cardinal lt card_zero a -> cardinal le card_one b ->
  cardinal le a (card_pow a b).

Lemma le_one_not_zero: forall a, cardinal le card_one a ->
  cardinal lt card_zero a.

Lemma non_zero_apowb: forall a b,
  cardinal lt card_zero a -> is_cardinal b ->
  cardinal lt card_zero (card_pow a b).

Lemma finite_power_lt1: forall a a' b,
  inc a Bnat -> inc a' Bnat -> inc b Bnat->
  cardinal lt a a' -> cardinal lt card_zero b ->
  cardinal lt (card_pow a b) (card_pow a' b).
Lemma finite_power_lt2: forall a b b',
    inc a Bnat -> inc b Bnat -> inc b' Bnat ->
    cardinal_lt b b' -> cardinal_lt card_one a ->
    cardinal_lt (card_pow a b) (card_pow a b').

Lemma lt_a_power_b_a: forall a b, inc a Bnat -> inc b Bnat ->
    cardinal_lt card_one b -> cardinal_lt a (card_pow b a).

We study here the function \( \text{pow} \) on the type \( \text{nat} \).

Lemma power_of_sumN: forall a b c, a ^ (b+c) = (a ^ b) *(a ^ c).

Lemma power_x_0N: forall a, a ^ 0 = 1.

Lemma power_0_xN: forall a, a ^ 1 = a.

Lemma pow_succ: forall a b, inc a Bnat -> inc b Bnat ->
    card_pow a (succ b) = card_mult(card_pow a b) a.

Lemma nat_B_pow: forall n m, nat_to_B (n ^ m) = card_pow (nat_to_B n)(nat_to_B m).

Lemma power_of_prodN: forall a b c, (a * b) ^ c = (a ^ c) * (b ^ c).

Lemma pow_0_x: forall a, a <> 0 -> 0 ^ a = 0.

Lemma nat_not_zero_pr: forall a, a <> 0 -> nat_to_B a <> card_zero.

Lemma power_0_x: forall a, a <> 0 -> 0 ^ a = 0.

Lemma non_zero_apowbN: forall a b, 0 < a -> 0 < a ^ b.

Lemma finite_power_lt1N: forall a a' b, a < a' -> 0 < b -> a ^ b < a' ^ b.

Lemma power_of_sum: forall a b c, a ^ (b+c) = (a ^ b) *(a ^ c).

Lemma power_x_0: forall a, a ^ 0 = 1.

Lemma power_0_x: forall a, a ^ 1 = a.

Lemma pow_succ: forall a b, inc a Bnat -> inc b Bnat ->
    card_pow a (succ b) = card_mult(card_pow a b) a.

Lemma nat_B_pow: forall n m, nat_to_B (n ^ m) = card_pow (nat_to_B n)(nat_to_B m).

Lemma power_of_prod: forall a b c, (a * b) ^ c = (a ^ c) * (b ^ c).

Lemma pow_0_x: forall a, a <> 0 -> 0 ^ a = 0.

Lemma nat_not_zero_pr: forall a, a <> 0 -> nat_to_B a <> card_zero.

Lemma power_0_x: forall a, a <> 0 -> 0 ^ a = 0.

Lemma non_zero_apowb: forall a b, 0 < a -> 0 < a ^ b.

Lemma finite_power_lt1: forall a a' b, a < a' -> 0 < b -> a ^ b < a' ^ b.

Lemma power_of_sum: forall a b c, a ^ (b+c) = (a ^ b) *(a ^ c).

Lemma power_x_0: forall a, a ^ 0 = 1.

Lemma power_0_x: forall a, a ^ 1 = a.

Lemma pow_succ: forall a b, inc a Bnat -> inc b Bnat ->
    card_pow a (succ b) = card_mult(card_pow a b) a.

Lemma nat_B_pow: forall n m, nat_to_B (n ^ m) = card_pow (nat_to_B n)(nat_to_B m).

Lemma power_of_prod: forall a b c, (a * b) ^ c = (a ^ c) * (b ^ c).

Lemma pow_0_x: forall a, a <> 0 -> 0 ^ a = 0.

Lemma nat_not_zero_pr: forall a, a <> 0 -> nat_to_B a <> card_zero.

Lemma power_0_x: forall a, a <> 0 -> 0 ^ a = 0.

Lemma non_zero_apowb: forall a b, 0 < a -> 0 < a ^ b.

Lemma finite_power_lt1: forall a a' b, a < a' -> 0 < b -> a ^ b < a' ^ b.

Lemma power_of_sum: forall a b c, a ^ (b+c) = (a ^ b) *(a ^ c).

Lemma power_x_0: forall a, a ^ 0 = 1.

Lemma power_0_x: forall a, a ^ 1 = a.

Lemma pow_succ: forall a b, inc a Bnat -> inc b Bnat ->
    card_pow a (succ b) = card_mult(card_pow a b) a.

Lemma nat_B_pow: forall n m, nat_to_B (n ^ m) = card_pow (nat_to_B n)(nat_to_B m).

Lemma power_of_prod: forall a b c, (a * b) ^ c = (a ^ c) * (b ^ c).

Lemma pow_0_x: forall a, a <> 0 -> 0 ^ a = 0.

Lemma nat_not_zero_pr: forall a, a <> 0 -> nat_to_B a <> card_zero.

Lemma power_0_x: forall a, a <> 0 -> 0 ^ a = 0.

Lemma non_zero_apowb: forall a b, 0 < a -> 0 < a ^ b.

Lemma finite_power_lt1: forall a a' b, a < a' -> 0 < b -> a ^ b < a' ^ b.
function, denoted by \( \text{sub} \), defined for all integers, whose value is zero for \( a > b \); we extend our function so that they share the same behavior.

Definition card_sub0 a b :=
choose (fun c => inc c Bnat & card_plus b c = a).
Definition card_sub a b := Yo(cardinal_le b a) (card_sub0 a b) card_zero.

Lemma card_sub_pr0: forall a b, inc a Bnat-> inc b Bnat ->
cardinal_le b a ->
(inc (card_sub a b) Bnat & card_plus b (card_sub a b) = a).
Lemma Bnat_stable_sub: forall a b, inc a Bnat -> inc b Bnat ->
inc (card_sub a b) Bnat.
Lemma cardinal_sub_wrong: forall a b, inc a Bnat -> inc b Bnat ->
~ (cardinal_le b a) -> card_sub a b = card_zero.
Lemma card_sub_pr: forall a b, inc a Bnat-> inc b Bnat ->
cardinal_le b a -> card_plus b (card_sub a b) = a.

We have \((a+b)−b=a\) for all integers. Uniqueness means that if \(a+b = c\) then \(a = c−b\) and \(b = c−a\).

Lemma card_sub_pr1: forall a b, inc a Bnat-> inc b Bnat ->
card_sub (card_plus a b) b = a.
Lemma card_sub_pr2: forall a b c, inc a Bnat-> inc b Bnat ->
card_plus a b = c -> a = card_sub c b.
Lemma plus_minusC: forall n m p , inc m Bnat-> inc p Bnat ->
n = card_plus m p -> p = card_sub n m.
Lemma nat_B_sub: forall a b,
nat_to_B (a−b) = card_sub (nat_to_B a) (nat_to_B b).

Once we have shown that we have the same subtraction on \(\mathbb{N}\) and on \(\mathbb{N}\), we can deduce some properties from the Coq Library.

We have \((b−a)+(b′−a′) = (b+b′)−(a+a′)\) if the first two differences are defined. We have the trivial formulas: \(a−a = 0\) and \(a−0 = a\). If \(a > 0\), then \(a−1\) is the predecessor of \(a\). We have \((a−b)−c = a−(b+c)\) if \(a \geq b+c\). Taking \(c = 1\), and denoting by \(P\) and \(S\) the predecessor and successor, we have \(P(a−b) = a−Sb\). If \(b \leq a\), then \(a−b \leq a\); and if \(b < a\), the \((a−b)−1 < a\). If \(b+1 \leq a\) then \(b < a\).

(* These are in the Coq library

Lemma minus_n_n : forall n, 0 = n - n.
Lemma minus_n_O : forall n, n = n - 0.
Lemma le_plus_minus : forall n m, n <= m -> m = n + (m - n).
Lemma plus_minus : forall n m p, n = m + p -> p = n - m.
Lemma minus_plus : forall n m, n + m - n = m.
Theorem le_minus : forall n m, n - m <= n.
Lemma minus_plus_simpl_l_reverse : forall n m p, n - m = p + n - (p + m).
Lemma minus_Sn_m : forall n m, n <= m -> S (n - m) = S n - m.
Lemma le_plus_minus_r : forall n m, n <= m -> n + (m - n) = m.
Lemma lt_minus : forall n m, m <= n -> 0 < m -> n - m < n.
Theorem not_le_minus_0 : forall n m, ~ m <= n -> n - m = 0.*

Lemma minus_wrong: forall n m, n<=m -> n-m = 0.
Lemma pred_minus: forall n m, m<n -> n-m = S(n - S m).

RR n° 7150
Lemma minus_n_nC: forall a, inc a Bnat -> card_sub a a = card_zero.
Lemma minus_n_0C: forall a, inc a Bnat -> card_sub a card_zero = a.

Lemma card_sub_pr4: forall a b a' b', inc a Bnat-> inc b Bnat ->
inc a' Bnat-> inc b' Bnat ->
cardinal_le a b-> cardinal_le a' b' ->
card_plus (card_sub b a) (card_sub b' a') =
card_sub (card_plus b b') (card_plus a a').
Lemma card_sub_pr4N: forall a b a' b',
a<b -> a' <= b' -> (b-a) + (b'-a') = (b+b')- (a+a').

Lemma Sn_is_1plus: forall n, S n = 1 + n.
Lemma Sn_is_plus1: forall n, S n = n +1.
Lemma lt_i_n : forall i n, i< n -> 1 <= n-i.

Lemma card_sub_associative: forall a b c,
inc a Bnat -> inc b Bnat -> inc c Bnat ->
cardinal_le (card_plus b c) a ->
card_sub (card_sub a b) c = card_sub a (card_plus b c).
Lemma card_sub_associativeN: forall a b c,
(b+c) <= a -> (a-b) -c = a - (b+c).
Lemma prec_pr1: forall a, inc a Bnat -> a <> card_zero
-> predc a = card_sub a card_one.
Lemma nat_B_pred: forall a, 0 <> a -> nat_to_B (pred a) = predc (nat_to_B a).
Lemma prec_is_cardinal_prec: forall a, inc a Bnat ->
a <> card_zero -> cardinal_nat (prec a) = pred (cardinal_nat a).
Lemma card_sub_non_zero: forall a b, inc a Bnat -> inc b Bnat ->
cardinal_le (succ b) a -> card_sub a b <> card_zero.
Lemma card_sub_associative1: forall a b, inc a Bnat -> inc b Bnat ->
cardinal_le (succ b) a -> predc (card_sub a b) = card_sub a (succ b).
Lemma sub_le_symmetry: forall a b, inc a Bnat -> inc b Bnat ->
cardinal_le b a -> cardinal_le (card_sub a b). 
Lemma sub_lt_symmetry: forall n p,
icc p Bnat -> cardinal_lt n p ->
cardinal_lt (prec (card_sub p n)) p.
Lemma double_sub: forall n p, Bnat_le p n ->
cardinal_le p (card_sub n p). 
Lemma double_subN: forall n p, p <= n -> n - (n- p) = p.

We state here some properties of the ordering on N.

Lemma Bnat_le_reflexive: forall a, inc a Bnat -> Bnat_le a a.
Lemma sum_increasing5: forall a b, inc a Bnat -> inc b Bnat ->
Bnat_le a (card_plus a b).
Lemma Bnat_le_reflexive: forall a, inc a Bnat -> Bnat_le a a.
Lemma Bnat_le_transitive: forall a b c, Bnat_le a b -> Bnat_le b c ->
Bnat_le a c.
Lemma Bnat_le_antisymmetric: forall a b, Bnat_le a b -> Bnat_le b a -> a = b.
Lemma Bnat_total_order: forall a b, inc a Bnat -> inc b Bnat ->
Bnat_le a b \/ Bnat_lt b a.
Lemma Bnat_zero_smallest: forall a, inc a Bnat -> Bnat_le card_zero a.
Lemma Bnat_zero_smallest1: forall a, Bnat_le a card_zero -> a = card_zero.

We show here that if $a+b \leq a+b'$, $a+b < a+b'$, $ab \leq ab'$ or $ab < ab'$ then $b \leq b'$ or $b < b'$ if inequality is strict in the assumption; in the case of a product, $a$ must be non-zero. Thus, if $ab$ is an integer and $b \neq 0$ then $a$ is finite. By, contradiction, we would have $a = a+1$, hence if
Lemma Bnat_plus_le_simplifiable: forall a b c,  
inc a Bnat -> inc b Bnat -> inc c Bnat->
cardinal_le (card_plus a b) (card_plus a c) -> cardinal_le b c.

Lemma Bnat_plus_lt_simplifiable: forall a b c,  
inc a Bnat -> inc b Bnat -> inc c Bnat->
cardinal_lt (card_plus a b) (card_plus a c) -> cardinal_lt b c.

Lemma Bnat_mult_le_simplifiable: forall a b c,  
inc a Bnat -> inc b Bnat -> inc c Bnat->
cardinal_le (card_mult a b) (card_mult a c) -> cardinal_le b c.

Lemma Bnat_mult_lt_simplifiable: forall a b c,  
inc a Bnat -> inc b Bnat -> inc c Bnat->
cardinal_le (card_mult a b) (card_mult a c) -> cardinal_le b c.

Lemma is_finite_in_product: forall a b, is_cardinal a -> is_cardinal b ->
b <> card_zero -> is_finite_c (card_mult a b) -> is_finite_c a.

(*

Lemma plus_le_reg_l : forall n m p, p + n <= p + m -> n <= m.

Lemma plus_lt_reg_l : forall n m p, p + n < p + m -> n < m.

Lemma mult_S_le_reg_l : forall n m p, S n * m <= S n * p -> m <= p.

Lemma nonzero_suc: forall n, 0<>n -> exists m, n = S m.

Lemma mult_S_lt_reg_l : forall n m p, S n * m < S n * p -> m < p.

Lemma mult_lt_reg_l : forall n m p, 0<>n -> n * m < n * p -> m < p.

Lemma mult_lt_reg_r : forall n m p, 0<>n -> m * n < p * n -> m < p.

*)

6.3 Intervals in sets of integers

Bourbaki says that, for every integer a, there is a set containing all integers \( \leq a \); he denotes this as \([0, a]\). The set \([a, b]\) is used without definition, in a context where this denotes the set of all integers \(x\) such that \(a \leq x \leq b\). He says that \(x \mapsto x + a\) is a strictly increasing isomorphism of \([0, b]\) onto \([a, a+b]\). In fact, these sets contain only cardinals, hence are well-ordered by \(\leq_{\text{Card}}\). As a consequence, all isomorphisms are strictly increasing.

We use here a different approach. If \(a \in \mathbb{N}\) and \(b \in \mathbb{N}\), we can consider \([a, b]\) as an interval for the ordering \(\leq_{\mathbb{N}}\) on \(\mathbb{N}\) (ordered by \(\leq_{\mathbb{N}}\)). This set is the same as the previous one, and has the same ordering.

Definition interval_Bnat a b := interval_cc Bnat_order a b.
Definition interval_co_0a a:= interval_co Bnat_order card_zero a.
Definition interval_Bnatb a b :=
graph_on cardinal_le (interval_cc Bnat_order a b).

We give here some properties of intervals. We have \(x \in [a, b]\) if and only if \(a \leq x \leq b\). Note that \(a \leq b\) implies \(x \in \mathbb{N}\). Thus we state: \(x \in [0, a]\) if and only if \(x \in \mathbb{N}\) and \(x \leq b\). Note that \(x \leq b\) implies \(x \in \mathbb{N}\). These two intervals are subsets of \(\mathbb{N}\). We have \([0, a + 1] = [0, a]\).

Lemma interval_Bnat_pr: forall a b x, inc a Bnat -> inc b Bnat ->
inc x (interval_Bnat a b) = (Bnat_le a x & Bnat_le x b).
Lemma sub_interval_Bnat: forall a b,
Lemma interval_Bnat_pr0: forall b x, inc b Bnat ->
  inc x (interval_Bnat card_zero b) = cardinal_le x b.

Lemma sub_interval_co_0a_Bnat: forall a, sub (interval_co_0a a) Bnat.

Lemma interval_co_0a_pr2: forall a x, inc a Bnat ->
  inc x (interval_co_0a a) = cardinal_lt x a.

Lemma interval_co_0a_pr3: forall a x, inc a Bnat ->
  inc x (interval_co_0a (succ a)) = cardinal_le x a.

Lemma interval_co_cc: forall p, inc p Bnat ->
  interval_Bnat card_zero p = interval_co_0a (succ p).

Lemma interval_cc_0a_increasing: forall a b, inc b Bnat ->
  cardinal_le a b ->
  sub (interval_Bnat card_zero a) (interval_Bnat card_zero b).

Lemma interval_cc_0a_increasing1: forall a, inc a Bnat ->
  sub (interval_Bnat card_zero a) (interval_Bnat card_zero (succ a)).

Lemma inc_a_interval_co_succ: forall a, inc a Bnat ->
  inc a (interval_co_0a (succ a)).

Lemma interval_co_0a_increasing: forall a, inc a Bnat ->
  sub (interval_co_0a a) (interval_co_0a (succ a)).

Lemma interval_co_0a_increasing1: forall a b, inc a Bnat -> inc b Bnat ->
  cardinal_le a b -> sub (interval_co_0a a) (interval_co_0a b).

Lemma interval_co_pr4: forall n, inc n Bnat ->
  ( (tack_on (interval_co_0a n) n = (interval_co_0a (succ n))
    & ~(inc n (interval_co_0a n))).

Lemma cardinal_c_induction5_v: forall (r:EP) a,
  inc a Bnat -> r card_zero ->
  (forall n, cardinal_lt n a -> r n -> r (succ n))
  -> (forall n, cardinal_le n a -> r n).

Note that $x \leq_{[a,b]} y$ is equivalent to $a \leq x \leq y \leq b$, where $\leq$ is the ordering on cardinals, 
since this relation implies that $x$ and $y$ are finite.

Lemma worder_interval_Bnato: forall a b, inc a Bnat -> inc b Bnat ->
  worder (interval_Bnato a b).

Lemma substrate_interval_Bnato: forall a b, inc a Bnat -> inc b Bnat ->
  substrate (interval_Bnato a b) = interval_Bnat a b.

Lemma related_interval_Bnato: forall a b x y, inc a Bnat -> inc b Bnat ->
  gle (interval_Bnato a b) x y = (inc x (interval_Bnato a b) &
  inc y (interval_Bnato a b) & cardinal_le x y).

Lemma related_interval_Bnato1: forall a b x y, inc a Bnat -> inc b Bnat ->
  gle (interval_Bnato a b) x y = (cardinal_le a x &
  cardinal_le a y & cardinal_le x b & cardinal_le y b & cardinal_le x y).

Lemma related_interval_Bnato2: forall a b x y, inc a Bnat -> inc b Bnat ->
  gle (interval_Bnato a b) x y = (cardinal_le a x &
  cardinal_le y b & cardinal_le x y).

We define here the ordered interval $[0, a]$. This is a well-ordered set (in fact, it is a segment 
of $\mathbb{N}$). We have $x \leq_{[0,a]} y$ if and only if $x \leq y$ and $y < a$, since these two relations imply $x \in [0, a]$ 
and $y \in [0, a]$.

Definition interval_Bnatco a :=
  graph_on cardinal_le (interval_co_0a a).

Lemma worder_interval_Bnatco: forall a, inc a Bnat ->
  worder (interval_Bnatco a).

INRIA
Lemma substrate_interval_Bnatco: forall a, inc a Bnat ->
substrate (interval_Bnatco a) = interval_co_0a a.

Lemma related_interval_Bnatco: forall a x y, inc a Bnat ->
gle (interval_Bnatco a) x y = (cardinal_le x y & cardinal_lt y a).

Lemma sum_increasing4: forall a b a' b',
Bnat_le a a' -> Bnat_le b b' ->
Bnat_le (card_plus a b) (card_plus a' b').

Lemma sub_increasing2: forall a b c, inc a Bnat -> inc b Bnat -> inc c Bnat->
cardinal_le c (card_plus a b) -> cardinal_le b c ->
cardinal_le (card_sub c b) a.

We consider now the function $z \rightarrow z + b$, ($z \in [0,a], z + b \in [a, a+b]$), that has $z \rightarrow z - b$ as inverse, and hence is a bijection. Proposition 4 [2, p. 174] says these these functions are
order isomorphisms.

Definition rest_plus_interval a b :=
BL(fun z => card_plus z b)(interval_Bnat card_zero a)
(interval_Bnat b (card_plus a b)).

Definition rest_minus_interval a b :=
BL(fun z => card_sub z b) (interval_Bnat b (card_plus a b))
(interval_Bnat card_zero a)

Lemma rest_plus_interval_axioms: forall a b, inc a Bnat -> inc b Bnat ->
transf_axioms (fun z => card_plus z b)(interval_Bnat card_zero a)
(interval_Bnat b (card_plus a b)).

Lemma rest_minus_interval_axioms: forall a b, inc a Bnat -> inc b Bnat ->
transf_axioms (fun z => card_sub z b) (interval_Bnat b (card_plus a b))
(interval_Bnat card_zero a).

Lemma restr_plus_minus_bij: forall a b, inc a Bnat -> inc b Bnat ->
(bijection (rest_plus_interval a b) & bijective (rest_minus_interval a b) &
(rest_minus_interval a b) = inverse_fun (rest_plus_interval a b)).

Theorem restr_plus_interval_isomorphism: forall a b, inc a Bnat -> inc b Bnat->
order_isomorphism (rest_plus_interval a b)
(interval_Bnato card_zero a)
(interval_Bnato b (card_plus a b)).

If $a \leq b$, then $[a, b+1] = [a, b] \cup (b+1)$ and the union is disjoint. Thus $[a, b+1]$ has one more
element than $[a, b]$. By induction, it has $b+1$ elements when $a = 0$, and by application of
the isomorphism shown above, it has $(b - a) + 1$ elements. This is Proposition 5 [2 p. 174].
As a consequence, the set of integers is infinite (since $[0,n]$ is subset of $\mathbb{N}$ we have
$n + 1 \leq \text{Card}(\mathbb{N})$, so that Card($\mathbb{N}$) cannot be of the form $n$). This argument is used at the start of Chapter 6:
the axiom that asserts the existence of an infinite set is equivalent to the assertion that there
exists a set containing all finite cardinals.

Lemma cardinal_interval0a: forall a, inc a Bnat ->
cardinal (interval_Bnat card_zero a) = succ a.

Theorem cardinal_interval: forall a b, Bnat_le a b->
cardinal (interval_Bnat a b) = succ (card_sub b a).

Lemma finite_set_interval_Bnat: forall a b, Bnat_le a b ->
is_finite_set (interval_Bnat a b).
Lemma finite_set_interval_co: forall a, inc a Bnat ->
  is_finite_set (interval_co Bnat_order card_zero a).

Lemma Bnat_infinite: ~(is_finite_set Bnat).

Proposition 6 [2] p. 175] asserts that every finite totally ordered set is isomorphic to a
unique interval [1, n], where n is the number of elements. Bourbaki adds the condition n ≥ 1,
this is not needed. We start with a lemma that says that [1, n] has n elements (note that
this is also true for n = 0). Then we pretend that if E and F are two finite equipotent totally
ordered sets, there is a unique order isomorphism between them. This is because the sets
are well-ordered, so that there exists a unique order morphism from E onto a segment of F;
whatever the image, the function is bijective hence is an order isomorphism. The general
theorem says that there is another possibility, namely that there exists an isomorphism from
F onto a segment of E; it is bijective, so that its inverse is an isomorphism from E onto F.
Bourbaki uses Corollary 2 to Proposition 2 of § 2, no. 2 (it says: if X is a subset of a finite set
E, and X ≠ E, then Card(X) < Card(E). Maybe Corollary 4 was intended, since it says that
an injection is bijective).

Lemma cardinal_interval1a: forall a, inc a Bnat ->
  cardinal (interval_Bnat card_one a) = a.

Lemma isomorphism_worder_finite: forall r r', (* 27 *)
  total_order r -> total_order r' ->
  is_finite_set (substrate r) -> equipotent (substrate r) (substrate r') ->
  exists_unique (fun f => order_isomorphism f r r').

Theorem finite_ordered_interval: forall r, total_order r ->
  is_finite_set (substrate r) ->
  exists_unique (fun f => order_isomorphism f r
  (interval_Bnato card_one (cardinal (substrate r)))).

We consider here properties of [0, b − 1]. If we denote it by I_b, it is the interval [0, b]. Note
that [0, b] exists even when b = 0. We can rewrite Proposition 6 as: every finite totally ordered
set is isomorphic to a unique interval [0, n], where n is the number of elements.

Lemma cardinal_interval_co_0a: forall a, inc a Bnat -> a <> card_zero ->
  cardinal (interval_Bnat card_zero (predc a)) = a.

Lemma interval_co_0a_pr: forall a x, inc a Bnat -> a <> card_zero ->
  inc x (interval_Bnat card_zero (predc a)) = (inc x Bnat & cardinal_lt x a).

Lemma interval_co_0a_pr1: forall a, inc a Bnat -> a <> card_zero ->
  interval_Bnat card_zero (predc a) = interval_co_0a a.

Lemma cardinal_interval_co_0a1: forall a, inc a Bnat ->
  cardinal (interval_co_0a a) = a.

Lemma emptyset_interval_00: interval_co_0a card_zero = emptyset.

Theorem finite_ordered_interval1: interval_co_0a card_zero = emptyset.

6.4 Finite sequences

A finite sequence is a family (x_i)_{i∈I} whose index set is a finite subset of N (Bourbaki says:
a finite set of integers). Let f be the unique isomorphism f of the interval [1, n] onto I (with
the natural ordering on I). Then x_{f(k)} is defined for k ∈ [1, n]. It is called the kth term of the
sequence. If k = 1 or k = n, it is called the first or last term.
If $P \in I$ is equivalent to $i \in I$, where $I$ is a finite set of integers, then $(x_i)_{i \in I}$ may be written as $(x_i)_{P \in I}$. In fact, such a notation can be used whatever $I$. As an example one can see $(t_i)_{a \leq i \leq b}$.

The sum of such a family may be denoted by $\sum_{i=a}^{b} t_i$.

Lists are defined in Coq by

```
Inductive list (A : Type) : Type :=
  nil : list A
| cons : A -> list A -> list A
```

A list can be either empty (this is $nil$), or of the form $cons A a b$ where $a$ is of type $A$ and $b$ is a list of type $A$. The parameter $A$ is often implicit. The expression $cons A a b$ is denoted by $a::b$. There are many functions in the standard library that deal with lists. For instance, $seq$ can produce the list containing 1, 2, 3. Given a list containing $x_1, x_2$ and $x_3$ (of type $A$) it is possible to create the list containing $(1, x_1), (2, x_2)$, and $(3, x_3)$ (of type $\mathbb{N} \times A$) then the set of all these values. This is a finite sequence (i.e., a functional graph, with domain $\{1, 2, 3\}$) In this section, we explain how to convert operations defined by Bourbaki for finite sequences (like sum and product) into operations on Coq lists.

Additional theorems about integers.

```
Lemma plus_n_Sm_subSn: forall n m, n + S m - n - 1 = m.
Lemma plus_n_Sm_subSm: forall n m, n + S m - m - 1 = n.
Lemma minus_SnSi: forall i n, i < S n -> S n - i - 1 = n - i.
Lemma double_compl_nat:forall i n, i< n ->
  i = n - (n - i - 1) -1.
Lemma double_compl_ex:forall i n, i< n ->
  (n - i - 1) < n.
```

### 6.4.1 Lists as functions

Given a function $g$, we define here the list $L$ containing $g(0), g(1), g(2)$ up to $g(n-1)$. The list has length $n$; it is stored in natural order. On the diagram below, the mapping $g \rightarrow L$ is denoted by $fl$. Conversely given a $L$ of length $n$, we define a function $g$ that returns the $k$-th element of the list, and 0 if $k \geq n$. It will be denoted by $lf$ on the diagram below.

We consider a variant of $lf$ where $L$ is a list of sets (the default value is then $\emptyset$) and, later on, a variant of $fl$, where $g$ is a function in the Bourbaki sense.

```
Fixpoint fct_to_list_rev (A:Type) (f: nat->A)(n:nat): list A :=
  match n with O => nil
  | S m => (f m) ::(fct_to_list_rev f m) end.

Definition fct_to_list A f n := rev (fct_to_list_rev (A:=A) f n).

Definition list_to_fct (a: list nat) :=
  fun n => nth n a 0.

Definition list_to_fctB (a: list Set) :=
  fun n => nth n a emptyset.
```

```
Lemma card_interval_c0_pr: forall n,
1In the previous version, we used the other order: $g(n-1)$ was the head of the list
```
José Grimm

...cardinal_nat (interval_co_0a (nat_to_B n)) = n.
Lemma list_extens: forall (A:Type) (l1 l2 : list A) (u:A),
length l1 = length l2 ->
(forall i, i< length l1 -> nth i l1 u = nth i l2 u) -> l1 = l2.

Lemma fct_to_list_length : forall A (f:nat->A) n,
length (fct_to_list f n) = n.

...Note that if \( g \) and \( g' \) agree on \([0,n-1]\) then \( fl(g) = fl(g') \). On the other hand, if \( L \) is a list
of size \( n \) and \( L' = a::L \), if the associated functions are \( g \) and \( g' \), then \( g'(n) = a \), and \( g \) and \( g' \)
agree on \([0,n-1]\).

...Given a list \( L \) of elements of \( \mathbb{N} \), of length \( n \), if \( g = \lfloor L \rfloor \), we construct a function \( G: [0,n] \rightarrow \mathbb{N} \via g(\text{card}(i)) = \text{card}(G(i)) \). The mapping \( L \rightarrow G \) will be denoted by \( LF \) on the diagram
below. Similarly, given a list \( L \) of sets, we construct \( G: [0,n] \rightarrow E \via g(\text{card}(i)) = G(i) \). This is
well-defined if all elements of the list belong to the set \( E \), see later.

Definition list_to_f (l: list nat):=
  BL (fun n => nat_to_B (list_to_fct l (cardinal_nat n)))
  (interval_co_0a (nat_to_B (length l))) Bnat.
Definition list_to_fB (l: list Set) E:=
  BL (fun n => list_to_fctB l (cardinal_nat n))
  (interval_co_0a (nat_to_B (length l))) E.
Lemma source_list_to_f: forall (l: list nat),
   source (list_to_f l) = (interval_co_0a (nat_to_B (length l))).

Lemma target_list_to_f: forall (l: list nat),
   target (list_to_f l) = Bnat.

Lemma W_list_to_f: forall (l: list nat) n,
   inc n (interval_co_0a (nat_to_B (length l))) ->
   W n (list_to_f l) = nat_to_B (list_to_fct l (cardinal_nat n)).

Lemma W_list_to_f1: forall (l: list nat) n,
   n < length l ->
   W (nat_to_B n) (list_to_f l) = nat_to_B (list_to_fct l n).

Lemma W_list_to_f2: forall (l: list nat) n,
   n < length l ->
   cardinal_nat(W (nat_to_B n) (list_to_f l)) = list_to_fct l n.

(Finite Lists)
match L with nil => True
  | a :: b => single_list_prop b (q a) \ double_list_prop b q
end.
*)

These definitions changed in Version 2. The two-arguments case was unused, and removed; the single-argument case has been replaced by an inductive object.

Inductive list_prop (A:Type) (q:A->Prop) : list A -> Prop :=
  | list_prop_nil: list_prop q nil
  | list_prop_cons: forall (a:A)(l:list A),
    q a -> list_prop q l -> list_prop q (a::l).

Lemma list_prop1: forall A (q:A->Prop), list_prop q nil.
Lemma list_prop2: forall A a b (q:A->Prop),
  q a -> (list_prop q b) = (list_prop q (a::b)).
Lemma list_prop3: forall A a b (q:A->Prop),
  (list_prop q a) -> (list_prop q b)
  -> (list_prop q (a++b)).
Lemma list_prop_refine: forall A L (p q:A->Prop),
  (forall a, p a -> q a) -> list_prop p L -> list_prop q L.
Lemma list_prop_nth: forall A (q:A->Prop) L u n,
  list_prop q L -> n < length L ->
  q (nth n L u).

The contraction \( C_{f,v}(L) \) of a list \( L \) is inductively defined by \( C_{f,v}(a::L) = f(a,C_{f,v}(L)) \), the value of the empty list being \( v \). If \( f(a,b) = b \cup \{a\} \), we call this the range of the list and denote it by \( r(L) \). We write \( L \subset E \) if \( P_E(L) \) holds, where \( P_E(x) \) is \( x \in E \); this means that every element of the list belongs to \( E \).

Fixpoint contraction (A B: Type) (L: list A) (f: A->B->B) (v: B):B :=
  match L with | nil => v
  | a :: b => f a (contraction b f v) end.

Definition list_range l := contraction l (fun a b => tack_on b a) emptyset.
Definition list_subset L E := list_prop (fun x => inc x E) L.

The range of a list is the smallest set \( E \) such that \( L \subset E \). We show \( L \subset r(L) \) by induction. We have \( r(L) \subset r(a::L) \). We then use the fact that if \( P \) implies \( Q \), then \( P(L) \) implies \( Q(L) \), where \( P \) is \( x \in r(L) \) and \( Q \) is \( x \in r(a::L) \). We can now state: if \( L \subset E \) is a list of length \( n \), there is an associated function \( [0,n[ \rightarrow E \).

Lemma list_range_pr: forall L, list_subset L (list_range L).
Lemma list_range_pr1: forall L E, list_subset L E -> sub (list_range L) E.

Lemma axioms_list_to_fB: forall l E, list_subset l E ->
  transf_axioms (fun n => (list_to_fctB l (cardinal_nat n)))
  (interval_co_0a (nat_to_B (length l))) E.
Lemma function_list_to_fB: forall l E, list_subset l E ->
  is_function (list_to_fB l E).
Lemma W_list_to_fB: forall l E n, list_subset l E ->
  inc n (interval_co_0a (nat_to_B (length l))) ->

INRIA
Lemma W list_to_fB1: forall l E n, list_subset l E ->
n < length l ->
W (nat_to_B n) (list_to_fB l E) = list_to_fctB l n.
Lemma fct_to_rev: forall (A:Type) (f:nat->A) n,
   rev (fct_to_list f n) = fct_to_list(fun i=> f(n-i-1)) n.

More properties of intervals.

Lemma partition_tack_on_intco: forall a, inc a Bnat ->
   partition_fam (Lvariantc (interval_co_0a a)
     (singleton a)) (interval_co_0a (succ a)).
Lemma interval_co_0a_restr: forall a f, inc a Bnat ->
   (L (interval_co Bnat_order card_zero a) f
    = (restr (L (interval_co Bnat_order card_zero (succ a)) f)
      (interval_co_0a a))).

Let L₁ and L₂ be two lists, L = L₁ ++ a::L₂, Let G₁ and G be the functions associated to L₁ and L. If L₁ is a list of size n, then G(n) = a, and G and G₁ agree on [0, n−1]. In fact, G₁ is the restriction of G to the interval [0, n[, and if L₂ is empty, then G is the function obtained from G₁ by adding the relation G(n) = a.

Lemma length_app1: forall (A:Type) (a:A) l l’,
   length l < length (l ++ a :: l’).
Lemma length_app2: forall (A:Type) (a:A) l ,
   nat_to_B (length (l++a::nil)) = succ (nat_to_B (length l)).
Lemma list_to_f_cons0: forall a l l’,
   W (nat_to_B (length l)) (list_to_f (l++ a:: l’)) = nat_to_B a.
Lemma list_to_f_cons1: forall a l l’ n, n < length l ->
   W (nat_to_B n) (list_to_f (l ++ a :: l’)) = W (nat_to_B n) (list_to_f l).
Lemma list_to_f_cons2: forall a l l’,
   list_to_f l = restriction_function (list_to_f (1++ a :: l’))
     (interval_co_0a (nat_to_B (length l))).
Lemma list_to_f_cons3: forall a l,
   list_to_f (1+a::nil) = tack_on_f (list_to_f l)
     (nat_to_B (length l)) (nat_to_B a).

Lemma list_subset_cons: forall a l l’ E,
   list_subset l E -> inc a E -> list_subset l’ E ->
   list_subset (l’++a::l) E.
Lemma list_to_f_consB0: forall a l l’ E,
   list_subset l E -> inc a E -> list_subset l’ E ->
   W (nat_to_B (length l)) (list_to_fB (l++ a :: l’) E) = a.
Lemma list_to_f_consB1: forall a l l’ n E, n< length l ->
   list_subset l E -> inc a E -> list_subset l’ E ->
   W (nat_to_B n) (list_to_fB (1++ a :: l’) E) = W (nat_to_B n) (list_to_fB l E).
Lemma list_to_f_consB0: forall a l E, list_subset l E -> inc a E ->
   W (nat_to_B (length l)) (list_to_fB (a :: l) E) = a.
Lemma list_to_f_consB1: forall a l n E, n< length l ->
   list_subset l E -> inc a E ->
   W (nat_to_B n) (list_to_fB (a :: l) E) = W (nat_to_B n) (list_to_fB l E).
Lemma list_to_f_consB2: forall a l l’ E,
   list_subset l E -> inc a E -> list_subset l’ E ->

RR n° 7150
list_to_fB l E = restriction_function \( \text{list_to_fB} (l++ a :: l') E \)
\( \text{(interval_co_0a (nat_to_B (length l)))} \).

**Lemma list_to_f_consB3:** for all \( a \) \( l \) \( E \),
list_subset l E \( \rightarrow \) inc a E \( \rightarrow \)
list_to_fB \((l++a::nil) E =\) tack_on_f \( \text{list_to_fB} l E \) \( \text{(nat_to_B (length l))} a \).

We denote by \( LFB \) the variant of \( lf \) that converts a list \( L \subset E \) into a function \( I \rightarrow E \). The source of this function is an interval \([0, n]\); we shall call this an iid function. We denote by \( FLB \) the variant of \( fl \) which is the inverse of \( LFB \), i.e. \( LFB(FLB(f)) = f \) and \( FLB(LFB(E)) = E \), whenever \( f \) is a function whose source is \([0, n]\) and is target is \( E \), and whenever \( L \subset E \).

**Definition fct_to_listB1 f n:=**
\( \text{fct_to_list} (\text{fun} \ n \Rightarrow \text{W} \ (\text{nat_to_B} n) f) n \).

**Definition fct_to_listB f :=** fct_to_listB1 f \( \text{(cardinal_nat (source f))} \).

**Definition iid_function f :=** is_function f \& exists n, source f = interval_co_0a \( \text{(nat_to_B n)} \).

**Lemma list_to_fB_pr:** for all \( l \) \( E \), list_subset l E \( \rightarrow \)
iid_function \( \text{list_to_fB} l E \).

**Lemma fct_to_list_lengthB :** for all f, iid_function f \( \rightarrow \)
nat_to_B \( \) (length (fct_to_listB f)) = cardinal (source f).

**Lemma fct_to_listB_pr0:** for all \( f \) \( i \),
iid_function f \( \rightarrow \) i< cardinal_nat (source f) \( \rightarrow \)
list_to_fctB \((\text{fct_to_listB} f) i = \text{W} \ (\text{nat_to_B} i) f \).

**Lemma fct_to_listB_pr1:** for all \( l \) \( E \), list_subset l E \( \rightarrow \)
fct_to_listB \((\text{list_to_fB} l E) = l \).

**Lemma fct_to_listB_pr2:** for all f, iid_function f \( \rightarrow \)
list_subset \((\text{fct_to_listB} f) \) \( \) (target f).

**Lemma fct_to_listB_pr3:** for all f, iid_function f \( \rightarrow \)
list_to_fB \((\text{fct_to_listB} f) \) \( \) (target f) = f.

### 6.4.2 Contracting lists

We show here the following. Assume that \( f(n) \) is a cardinal for all \( n \). Let \( F(n) \) be the cardinal sum of the family \( i \rightarrow f(i) \) on \([0, n-1]\). Then \( F(n+1) = f(n) + F(n) \), and there is a similar relation for the product. The same formula holds if \( F(n+1) \) is the cardinal sum of the graph of the function \( f \) and \( F(n) \) is cardinal sum of the graph of the restriction of \( f \) to \([0, n-1]\).

We apply this to the case where \( f \) is \( LF(L++a::nil) \); its restriction is \( LF(L) \), and \( f(n) = a \).

**Lemma induction_on_sum:** for all a f, inc a Bnat \( \rightarrow \)
\( \text{(forall a, inc a Bnat \rightarrow is_cardinal (f a)) \rightarrow \}
let iter := fun n=> cardinal_sum (L (interval_co_0a n)f)
in card_plus (iter a) (f a) = (iter (succ a)).

**Lemma induction_on_prod:** for all a f, inc a Bnat \( \rightarrow \)
\( \text{(forall a, inc a Bnat \rightarrow is_cardinal (f a)) \rightarrow \}
let iter := fun n=> cardinal_prod (L (interval_co_0a n ) f)
in card_mult (iter a) (f a) = (iter (succ a)).

**Lemma induction_on_sum1:** for all f n,
is_function f \( \rightarrow \) source f = interval_co_0a (succ n) \( \rightarrow \) inc n Bnat \( \rightarrow \)
\( \text{(forall a, inc a (source f) \rightarrow is_cardinal (W a f)) \rightarrow \}
card_plus (cardinal_sum (graph (restriction_function f (interval_co_0a n)))) (W n f = cardinal_sum (graph f).
Lemma induction_on_prod1: forall f n,
is_function f -> source f = interval_co_0a (succ n) -> inc n Bnat ->
(forall a, inc a (source f) -> is_cardinal (W a f)) ->
card_mult (cardinal_prod (graph (restriction_function f (interval_co_0a n))))
(W n f) = cardinal_prod (graph f).

Denote by S(L) the cardinal sum of the family LF(L). The induction principle says S(L++
a::nil) = S(L) + a. By associativity we get S(L' ++ +L) = S(L') + S(L). We have S(nil) = 0 and
S(a::nil) = a. If we take L' = a::nil, the associativity formula gives S(a::L) = a + S(L). Note: in
version 2, we changed the ordering of the elements of the list. This changes the properties of
S; we proved the previous formula by using commutativity (rather than associativity).

Lemma induction_on_sum2: forall a l,
card_plus (cardinal_sum (graph (list_to_f l))) (nat_to_B a)
= cardinal_sum (graph (list_to_f (l++a::nil))).

Lemma induction_on_prod2: forall a l,
card_mult (cardinal_prod (graph (list_to_f l))) (nat_to_B a)
= cardinal_prod (graph (list_to_f (l++a::nil))).

Lemma induction_on_sum0:
cardinal_sum (graph (list_to_f nil)) = card_zero.

Lemma induction_on_sum5: forall a,
cardinal_sum (graph (list_to_f (a::nil))) = nat_to_B a.

Lemma induction_on_prod0:
cardinal_prod (graph (list_to_f nil)) = card_one.

Lemma induction_on_prod5: forall a,
cardinal_prod (graph (list_to_f (a::nil))) = nat_to_B a.

Lemma induction_on_sum4: forall l l',
card_plus (cardinal_sum (graph (list_to_f l))) (cardinal_sum (graph (list_to_f l')))
= cardinal_sum (graph (list_to_f (l++l'))).

Lemma induction_on_prod4: forall l l',
card_mult (cardinal_prod (graph (list_to_f l))) (cardinal_prod (graph (list_to_f l')))
= cardinal_prod (graph (list_to_f (l++l'))).

We define here the sum and product of a list of integers as a contraction. We shall denote
this by Σ(L) and Π(L). This operation is related to the previous one by 
\[ N(\Sigma(L)) = \sum LF(L) \] and 
\[ N(\Pi(L)) = \prod LF(L). \]

Definition list_sum l := contraction (rev l) plus 0.
Definition list_prod l := contraction (rev l) mult 1.

Lemma list_sum_pr: forall l,
nat_to_B (list_sum l) = cardinal_sum (graph (list_to_f l)).

Lemma list_prod_pr: forall l,
nat_to_B (list_prod l) = cardinal_prod (graph (list_to_f l)).

If we denote by a++b the concatenation of two lists, then 
\[ C_{f_\nu}(a++b) = f(C_{f_\nu}(a), C_{f_\nu}(b)) \]
provided that the result is true for the empty list, i.e., \( f(v, b) = b \) for all \( b \), and if \( f \) is associative.
As a consequence \( \Sigma(a++b) = \Sigma(a) + \Sigma(b) \) and \( \Pi(a++b) = \Pi(a) \cdot \Pi(b) \). This is a general
property of contractions of an associative function \( f \).

Denote by \( \Sigma'_n(f) \) the expression \( \Sigma(fl(f, n)) \). This is the sum of the list of the values \( f(i) \) for
\( i < n \). If we denote by \( f_1 + f_2 \) the function \( i \mapsto f_1(i) + f_2(i) \) then we have 
\[ \Sigma'_n f + \Sigma'_n g = \Sigma'_n (f + g). \]
There are similar formulas for the product. We have two induction formulas; the trivial one is \( \sum_{n+1}(f) = f(n) + \sum_n(f) \); the non-trivial one is \( \sum_{n+1}(f) = f(0) + \sum_n(f \circ S) \), where \( (f \circ S)(i) = f(i+1) \).

**Lemma** contraction_assoc: forall (A : Type) (L1 L2: list A) (f: A \rightarrow A) (v: A),
(f a b c, f a (f b c) = f (f a b) c) ->
(f v a = a) ->
(contraction (L1++L2) f v) = f (contraction L1 f v)(contraction L2 f v).

**Lemma** list_sum_single: forall a, list_sum (a::nil) = a.
**Lemma** list_prod_single: forall a, list_prod (a::nil) = a.
**Lemma** list_sum_app: forall a b, list_sum (a++b) = (list_sum a)+ (list_sum b).
**Lemma** list_sum_cons: forall a b, list_sum (a::b) = a + (list_sum b).
**Lemma** list_sum_consr: forall a b, list_sum (a++(b::nil)) = (list_sum a)+ b.
**Lemma** list_prod_app: forall a b,
list_prod (a++b) = (list_prod a)* (list_prod b).
**Lemma** list_prod_cons: forall a b, list_prod (a::b) = a*(list_prod b).
**Lemma** list_prod_consr: forall a b, list_prod (a++(b::nil)) = (list_prod a)* b.

Definition fct_sum f n:= list_sum (fct_to_list f n).
Definition fct_prod f n:= list_prod(fct_to_list f n).

**Lemma** fct_sum0: forall f, fct_sum f 0 = 0.
**Lemma** fct_prod0: forall f, fct_prod f 0 = 1.
**Lemma** fct_sum_rec: forall f n, fct_sum f (S n) = (fct_sum f n) + (f n).
**Lemma** fct_prod_rec: forall f n, fct_prod f (S n) = (fct_prod f n) * (f n).
**Lemma** fct_sum_rec1: forall f n,
fct_sum f (S n) = (f 0) + (fct_sum (fun i=> f (S i)) n).
**Lemma** fct_prod_rec1: forall f n,
fct_prod f (S n) = (f 0) * (fct_prod (fun i=> f (S i)) n).
**Lemma** fct_sum_plus: forall f g n,
(fct_sum f n) + (fct_sum g n) = fct_sum (fun i=> (f i) + (g i)) n.
**Lemma** fct_prod_mult: forall f g n,
(fct_prod f n) * (fct_prod g n) =fct_prod (fun i=> (f i) * (g i)) n.

We show here some trivial results. The sum of a constant function is the product, and the sum is unchanged if we replace the list by its reverse. A bit more complicated: the reverse of the list associated to a function \( f \) is the list associated to \( i \rightarrow f(n-i-1) \).

**Lemma** fct_sum_const: forall n m, fct_sum (fun _ => m) n = n *m.
**Lemma** fct_prod_const: forall n m, fct_prod (fun _ => m) n = pow m n.
**Lemma** list_sum_rev: forall l, list_sum l = list_sum (rev l).
**Lemma** list_prod_rev: forall l, list_prod l = list_prod (rev l).
**Lemma** fct_sum_rev: forall f n,
fct_sum f n = fct_sum (fun i=> f(n-i-1)) n.
**Lemma** fct_prod_rev: forall f n,
fct_prod f n = fct_prod (fun i=> f(n-i-1)) n.
**Lemma** fct_to_rev: forall (A:Type) (f:nat\rightarrow A) n,
rev (fct_to_list f n) = fct_to_list(fun i=> f(n-i-1)) n.

We consider here the inverse of \( BN \): if \( f \) is a function of type \( nat \rightarrow nat \), we construct a function \([0, n[\rightarrow N \). It is the composition of \( fl \) and \( LF \). We shall denote it by \( NB \). The first
Theorem is a statement about \( NB \), the two others are statements about the graph of \( NB \). The third theorem is deduced from the second by applying \([0, n + 1] = [0, n]\).

\[ \text{Lemma } l_{to\_fct}: \forall f, n, \]
\[ \quad \text{BL} \left( \lambda p \rightarrow \text{nat\_to\_B}(f(\text{cardinal\_nat}(p))) \right) \left( \text{interval\_co\_0a} \left( \text{nat\_to\_B}(n) \right) \right) \]
\[ \quad \text{BNat} = \text{list\_to\_f} \left( \text{fct\_to\_list} f n \right). \]

\[ \text{Lemma } l_{to\_fct1}: \forall f, n, \]
\[ \quad \text{L} \left( \text{interval\_co\_0a} \left( \text{nat\_to\_B}(n) \right) \right) \left( \lambda p \rightarrow \text{nat\_to\_B}(f(\text{cardinal\_nat}(p))) \right) \]
\[ \quad = \text{graph} \left( \text{list\_to\_f} \left( \text{fct\_to\_list} f n \right) \right). \]

\[ \text{Lemma } l_{to\_fct2}: \forall f, n, \]
\[ \quad \text{L} \left( \text{interval\_Bnat} \text{card\_zero} \left( \text{nat\_to\_B}(n) \right) \right) \]
\[ \quad \left( \lambda p \rightarrow \text{nat\_to\_B}(f(\text{cardinal\_nat}(p))) \right) \]
\[ \quad = \text{graph} \left( \text{list\_to\_f} \left( \text{fct\_to\_list} f (\text{S} n) \right) \right). \]

### 6.5 Characteristic functions on sets

We define \( \phi_A(x) \) to be 1 if \( x \in A \) and 0 otherwise. This induces a function on every set \( B \), the characteristic function of \( B \).

\[ \text{Definition } \text{char\_fun} A B := \text{BL} \left( \lambda z \rightarrow \text{Yo}(\text{inc}(z A) \text{ card\_one} \text{ card\_zero}) \right) \]
\[ \quad \left( \text{doubleton card\_one card\_zero} \right). \]

\[ \text{Lemma } \text{char\_fun\_axioms}: \forall A B, \]
\[ \quad \text{transf\_axioms} \left( \lambda z \rightarrow \text{Yo}(\text{inc}(z A) \text{ card\_one} \text{ card\_zero}) \right) \]
\[ \quad \left( \text{doubleton card\_one card\_zero} \right). \]

\[ \text{Lemma } \text{function\_char\_fun}: \forall A B, \text{is\_function} \left( \text{char\_fun} A B \right). \]

\[ \text{Lemma } \text{W\_char\_fun}: \forall A B x, \]
\[ \quad \text{inc} x B \rightarrow \text{W} x \left( \text{char\_fun} A B \right) = \text{Yo}(\text{inc} x A) \text{ card\_one} \text{ card\_zero}. \]

\[ \text{Lemma } \text{cardinal\_W\_char\_fun}: \forall A B x, \]
\[ \quad \text{inc} x B \rightarrow \text{is\_cardinal} \left( \text{W} x \left( \text{char\_fun} A B \right) \right). \]

\[ \text{Lemma } \text{W\_char\_fun\_a}: \forall A B x, \text{sub} A B \rightarrow \text{inc} x A \rightarrow \]
\[ \quad \text{W} x \left( \text{char\_fun} A B \right) = \text{card\_one}. \]

\[ \text{Lemma } \text{W\_char\_fun\_b}: \forall A B x, \text{sub} A B \rightarrow \text{inc} x (\text{complement} B A) \rightarrow \]
\[ \quad \text{W} x \left( \text{char\_fun} A B \right) = \text{card\_zero}. \]

Now some properties. We have \( \phi_A = \phi_B \) if and only if \( A = B \). The function \( \phi_A \) (for \( A \subset E \)) is constant if and only if \( A = E \) or \( A = \emptyset \). Proposition 7 [2, p. 176] lists additional properties.

\[ \phi_{E-A}(x) = 1 - \phi_A(x) \]
\[ \phi_{A\cap B}(x) = \phi_A(x)\phi_B(x) \]
\[ \phi_{A\cup B}(x) + \phi_{A\cap B}(x) = \phi_A(x) + \phi_B(x) \]

\[ \text{Lemma } \text{chart\_fun\_injective}: \forall A A' B, \text{sub} A B \rightarrow \text{sub} A' B \rightarrow \]
\[ \quad (A=A') = \left( \text{char\_fun} A B = \text{char\_fun} A' B \right). \]

\[ \text{Lemma } \text{W\_char\_fun\_aa}: \forall A x, \text{inc} x A \rightarrow \]
\[ \quad \text{W} x \left( \text{char\_fun} A A \right) = \text{card\_one}. \]

\[ \text{Lemma } \text{W\_char\_fun\_bb}: \forall A x, \text{inc} x A \rightarrow \]
\[ \quad \text{W} x \left( \text{char\_fun} \emptyset A \right) = \text{card\_zero}. \]

\[ \text{Lemma } \text{constant\_char\_fun}: \forall A B, \text{sub} A B \rightarrow \]
\[ \quad (\forall x y, \text{inc} x B \rightarrow \text{inc} y B \rightarrow \text{W} x \left( \text{char\_fun} A B \right) = \text{W} y \left( \text{char\_fun} A B \right)) \]

RR n° 7150
Lemma char_fun_complement: forall A B x, sub A B -> inc x B ->
W x (char_fun (complement B A) B)
= card_sub card_one (W x (char_fun A B)).

Lemma char_fun_inter: forall A A’ B x, sub A B -> sub A’ B -> inc x B ->
W x (char_fun (intersection2 A A’) B)
= card_mult (W x (char_fun A B))(W x (char_fun A’ B)).

Lemma char_fun_union: forall A A’ B x, sub A B -> sub A’ B -> inc x B ->
card_plus (W x (char_fun (intersection2 A A’) B))
(W x (char_fun (union2 A A’) B ))
= card_plus (W x (char_fun A B))(W x (char_fun A’ B)).

6.6 Euclidean Division

Assume that $P \{ x \}$ is a property of integers, satisfied by at least one element. Since the set of integers is well-ordered, there is a smallest such element, hence $x$ such that $P(x)$ is false and $P(x+1)$ is true, unless $P(0)$ is true. We give two variants of this fact.

We also give a proof on the type $nat$. We show that if $p(0)$ is false and $p(Sn)$ is true for some $n$, negating the existence of $x$ such that $p(Sx)$ true and $p(x)$ false is absurd. The double negation axiom then shows that such an $x$ must exist.

Lemma least_int_prop: forall prop:EP,
(prop x -> inc x Bnat) -> (exists x, prop x) ->
prop card_zero / (exists x, inc x Bnat & prop(succ x) & ~ prop x).

Lemma least_int_prop1: forall prop:EP,
(prop x -> inc x Bnat) -> ~(prop card_zero) ->
(exists x, prop x) -> (exists x, inc x Bnat &prop (succ x) & ~ prop x).

Lemma least_int_prop0: forall p:nat->Prop,
~(p 0) -> (exists x, p x) -> (exists x, p (S x) & ~ p x).

Theorem 1 [2, p. 176] says that, if $b > 0$, $a$ and $b$ are integers, there exist unique integers $q$ (called quotient) and $r$ (called remainder) such that $a = bq + r$ and $r < b$. We show that the conditions are equivalent to $bq \leq a < b(1 + q)$ and $r = a - bq$. Thus $q$ is the smallest integer such that $a < b(q + 1)$. This inequality is satisfied for $q = a$, this shows existence and uniqueness of $q$.

Lemma division_prop_nat: forall a b q r, 0 <>b ->
(a=b*q+r & r<b) = (b*q <= a & a < b* (S q) & r = a - (b*q)).

Lemma Ndivision_unique: forall a b q r q’ r’, 0 <> b ->
a = b* q + r -> r < b -> a = b* q’ + r’ -> r’< b ->
(q = q’ & r = r’).

Lemma Ndivision_existence: forall a b, 0 <> b ->
exists q, exists r, (a = b* q + r & r < b).

In order to define the quotient and remainder, we must use the axiom of choice. We start
with the definition of the quotient and remainder for finite cardinals. If the remainder of the
division of $a$ by $b$ is zero we say that $b$ divides $a$.

Definition division_prop a b q r :=
a = card_plus (card_mult b q) r & cardinal_lt r b.
Definition card_rem a b :=
choose (fun r => inc r Bnat & exists q, inc q Bnat & division_prop a b q r).
Definition card_quo a b :=
   choose (fun q => inc q Bnat & exists r, inc q Bnat & division_prop a b q r).
Definition Bnat_divides b a := card_rem a b = card_zero.

We prove again existence and uniqueness of the division; this shows that our definitions make sense.

Lemma division_result_integer: forall a b q r, inc a Bnat-> inc b Bnat ->
   b <> card_zero -> division_prop a b q r -> is_cardinal q ->
   (inc q Bnat & inc r Bnat).

Lemma division_prop_alt: forall a b q r, inc a Bnat-> inc b Bnat ->
   inc q Bnat-> inc r Bnat -> division_prop a b q r = (cardinal_le (card_mult b q) a &
   cardinal_lt a (card_mult b (succ q)) &
   r = card_sub a (card_mult b q)).

Lemma division_unique:forall a b q r q', r', inc a Bnat-> inc b Bnat ->
   inc q Bnat-> inc r Bnat -> inc q' Bnat-> inc r' Bnat -> b <> card_zero ->
   division_prop a b q r -> division_prop a b q' r' ->
   (q = q' & r = r').

Lemma division_exists:forall a b, inc a Bnat-> inc b Bnat ->
   b <> card_zero -> exists q, exists r,
   (inc q Bnat & inc r Bnat & division_prop a b q r).
Lemma Bnat_division: forall a b, inc a Bnat-> inc b Bnat -> b <> card_zero ->
   (inc (card_rem a b) Bnat & (inc (card_quo a b) Bnat) &
   (division_prop a b (card_quo a b) (card_rem a b))).

Note. Bourbaki says: the number \( q \) introduced above is \textit{the integral part of the quotient of} \( a \) \textit{by} \( b \), since in the set of rational numbers \( \mathbb{Q} \), there exists \( c \) such that \( a = bc \), and \( q \) is the integral part of \( c \). He reserves the term \textit{quotient} only to the case where the remainder is zero. Moreover he says “writing \( a \div b \) or \( \frac{a}{b} \) will imply that \( b \) divides \( a \).” This is an abuse of notations. (It is all right to say that \( a < b \) implies that \( a \) and \( b \) are integers, because we can consider as a short-hand for “\( a < b \) and \( a \in \mathbb{N} \) and \( b \in \mathbb{N} \)” but, if \( d(a, b) \) is the property that \( b \) divides \( a \), and \( q(a, b) \) is the quotient, then \( a/b \) cannot be a short-hand for “\( q(a, b) \) and \( d(a, b) \)” because this expression makes no sense (it is neither a term nor a relation). Moreover, the convention is not always respected since Bourbaki proves

\[
\sum_{i=1}^{n} i = \frac{1}{2} n(n + 1).
\]

Euclidean division is curiously defined in Coq. The following two lemmas say that if \( b > 0 \), then for every \( a \) we have \( \{x : \mathbb{N} | \exists y : \mathbb{N}, \ Z\} \) where \( Z \) is the division property \( a = bq + r \) and \( r < b \), and \( (x, y) \) is \((q, r)\) or \((r, q)\). This expression is a type; from it one can extract \( q \) and the associated property (namely that there is \( r \) such that \( Z \)).

(*
Lemma quotient :
   forall n,
   n > 0 ->
   forall m:nat, {q : nat | exists r : nat, m = q * n + r /\ n > r}.
Lemma modulo :
   forall n,

RR n° 7150
José Grimm

\[ n > 0 \rightarrow \\
\forall m : \text{nat}, \{ r : \text{nat} \mid \exists q : \text{nat}, m = q \cdot n + r \land n > r \}. \]

Hence we provide the following definition. For simplicity, in the case \( b = 0 \), we shall use \( b = 1 \) instead (quotient one, remainder zero). However, we say that \( b \) divides \( a \) only when \( b \) is non-zero.

Definition \( \text{Nquo} \ a \ b := \)
\[
\text{cardinal_nat} (\text{card_quo} (\text{Ro} (\text{nat_to_B} a))
\quad (\text{Yo} (b = 0) \text{card_one} (\text{Ro} (\text{nat_to_B} b))))).
\]

Definition \( \text{Nrem} \ a \ b := \)
\[
\text{cardinal_nat} (\text{card_rem} (\text{Ro} (\text{nat_to_B} a))
\quad (\text{Yo} (b = 0) \text{card_one} (\text{Ro} (\text{nat_to_B} b)))).
\]

Definition \( \text{Ndivides} \ b \ a := 0 \leftrightarrow b \land \text{Nrem} \ a \ b = 0. \)

Lemma \( \text{Ndivision\_exists} : \forall a \ b, 0 \leftrightarrow b \rightarrow \\
(a = b \cdot (\text{Nquo} \ a \ b) + (\text{Nrem} \ a \ b) \land (\text{Nrem} \ a \ b < b)). \)

Lemma \( \text{Ndivision\_pr} : \forall a \ b \ q \ r, 0 \leftrightarrow b \rightarrow \\
a = b \cdot q + r \rightarrow r < b \rightarrow q = \text{Nquo} \ a \ b \land r = \text{Nrem} \ a \ b. \)

Lemma \( \text{Ndivision\_pr\_q} : \forall a \ b \ q \ r, 0 \leftrightarrow b \rightarrow \\
a = b \cdot q + r \rightarrow r < b \rightarrow q = \text{Nrem} \ a \ b. \)

Lemma \( \text{Ndivision\_pr\_r} : \forall a \ b \ q \ r, 0 \leftrightarrow b \rightarrow \\
a = b \cdot q + r \rightarrow r < b \rightarrow r = \text{Nrem} \ a \ b. \)

All properties true for \( \text{Nquo} \) and \( \text{Nrem} \) are true for \( \text{card\_quo} \) and \( \text{card\_rem} \). For this reason, we shall only prove our theorems for the case of type \( \text{nat} \).

Lemma \( \text{nat\_B\_division} : \forall a \ b, 0 \leftrightarrow b \rightarrow \\
(\text{nat\_to_B} (\text{Nquo} \ a \ b) = \text{card\_quo} (\text{nat\_to_B} a) (\text{nat\_to_B} b) \land \\
\text{nat\_to_B} (\text{Nrem} \ a \ b) = \text{card\_rem} (\text{nat\_to_B} a) (\text{nat\_to_B} b)). \)

Lemma \( \text{nat\_B\_quo} : \forall a \ b, 0 \leftrightarrow b \rightarrow \\
\text{nat\_to_B} (\text{Nquo} \ a \ b) = \text{card\_quo} (\text{nat\_to_B} a) (\text{nat\_to_B} b). \)

Lemma \( \text{nat\_B\_rem} : \forall a \ b, 0 \leftrightarrow b \rightarrow \\
\text{nat\_to_B} (\text{Nrem} \ a \ b) = \text{card\_rem} (\text{nat\_to_B} a) (\text{nat\_to_B} b). \)

Now some consequences when division is exact. Bourbaki says: every multiple \( a' \) of a multiple \( a \) of \( b \) is a multiple of \( b \). One can restate this as: if \( b \) divides \( a \), then \( b \) divides \( ac \).

Lemma \( \text{inc\_quotient\_bnat} : \forall a \ b, \text{inc} a \ \text{Bnat} \rightarrow \text{inc} b \ \text{Bnat} \rightarrow b \leftrightarrow \text{card\_zero} \rightarrow \\
\text{inc} (\text{card\_quo} a b) \ \text{Bnat}. \)

Lemma \( \text{inc\_remainder\_bnat} : \forall a \ b, \\
\text{inc} a \ \text{Bnat} \rightarrow \text{inc} b \ \text{Bnat} \rightarrow b \leftrightarrow \text{card\_zero} \rightarrow \\
\text{inc} (\text{card\_rem} a b) \ \text{Bnat}. \)

Lemma \( \text{Ndivides\_pr} : \forall a \ b, \\
\text{Ndivides} \ b \ a \rightarrow a = b \cdot (\text{Nquo} \ a \ b). \)

Lemma \( \text{Ndivides\_pr1} : \forall a \ b, 0 \leftrightarrow b \rightarrow \text{Ndivides} \ b \ (b \ast a). \)

Lemma \( \text{Ndivides\_pr2} : \forall a \ b \ q, 0 \leftrightarrow b \rightarrow \\
a = b \ast q \rightarrow q = \text{Nquo} \ a \ b. \)

Lemma \( \text{one\_divides\_all} : \forall a, \text{Ndivides} \ 1 \ a. \)

Lemma \( \text{Ndivides\_pr3} : \forall a \ b \ q, \\
\text{Ndivides} \ b \ a \rightarrow q = \text{Nquo} \ a \ b \rightarrow a = b \ast q. \)

Lemma \( \text{Ndivides\_pr4} : \forall a \ b \ q, 0 \leftrightarrow b \rightarrow \\
\text{INRIA} \)

\[\text{Nquo } (b \ast q) b = q.\]

Lemma \text{Ndivision\_itself}: for all \(a, 0 <> a \rightarrow (\text{Ndivides } a a \& \text{Nquo } a a = 1).\)

Lemma \text{Ndivides\_itself}: for all \(a, 0 <> a \rightarrow \text{Ndivides } a a.\)

Lemma \text{Nquo}: for all \(a, 0 <> a \rightarrow \text{Nquo } a a = 1.\)

Lemma \text{Ndivision\_of\_zero}: for all \(a, 0 <> a \rightarrow (\text{Ndivides } a 0 \& \text{Nquo } 0 a = 0).\)

Lemma \text{Ndivides\_trans}: for all \(a, b, a', \text{Ndivides } a a' \rightarrow \text{Ndivides } b a \rightarrow \text{Ndivides } b a'.\)

Lemma \text{Ndivides\_trans1}: for all \(a, b, a', \text{Ndivides } a a' \rightarrow \text{Ndivides } b a \rightarrow \text{Nquo } a' b = (\text{Nquo } a' a) \ast (\text{Nquo } a b).\)

Lemma \text{Ndivides\_trans2}: for all \(a, b, c, \text{Ndivides } b a \rightarrow \text{Ndivides } b (a \ast c).\)

Lemma \text{non\_zero\_mult}: for all \(a, b, 0 <> a \rightarrow 0 <> b \rightarrow 0 <> (a \ast b).\)

Lemma \text{Nquo\_simplify}: for all \(a, b, c, 0 <> b \rightarrow 0 <> c \rightarrow \text{Nquo } (a \ast c) (b \ast c) = \text{Nquo } a b.\)

If \(b\) divides \(a\) and \(a'\), it divides the sum and the difference.

Lemma \text{card\_quo\_simplify}: for all \(a, b, c,\)
\[\text{inc } a \text{ Bnat } \rightarrow \text{inc } b \text{ Bnat } \rightarrow \text{inc } c \text{ Bnat } \rightarrow b <> \text{card\_zero } \rightarrow c <> \text{card\_zero} \rightarrow \text{card\_quo } \left(\text{card\_mult } a c \right) \left(\text{card\_mult } b c \right) = \text{card\_quo } a b.\]

Lemma \text{divides\_and\_sum}: for all \(a, a', b, \text{Ndivides } a a' \rightarrow \text{Ndivides } b a' \rightarrow (\text{Ndivides } b (a + a') \& \text{Nquo } (a + a') b = (\text{Nquo } a b) + (\text{Nquo } a' b)).\)

Lemma \text{distrib\_prod2\_sub}: for all \(a, b, c, \text{inc } a \text{ Bnat } \rightarrow \text{inc } b \text{ Bnat } \rightarrow \text{inc } c \text{ Bnat} \rightarrow \text{card\_le } c b \rightarrow \text{card\_mult } a \left(\text{card\_sub } b c \right) = \text{card\_sub } \left(\text{card\_mult } a b \right) \left(\text{card\_mult } a c\right).\)

Lemma \text{distrib\_prod2\_subN}: for all \(a, b, c, c <= b \rightarrow a \ast (b - c) = (a \ast b) - (a \ast c).\)

Lemma \text{divides\_and\_difference}: for all \(a, a', b, \text{inc } a \text{ Bnat } \rightarrow \text{inc } a' \text{ Bnat} \rightarrow \text{inc } b \text{ Bnat } \rightarrow \text{card\_zero} \rightarrow \text{card\_le } a' a \rightarrow \text{Bnat\_divides } b a \rightarrow \text{Bnat\_divides } b b' \rightarrow \text{card\_le } (\text{card\_quo } a' b) \left(\text{card\_quo } a b \right) \& \text{card\_quo } (\text{card\_sub } a a') b = \text{card\_sub } (\text{card\_quo } a b) \left(\text{card\_quo } a' b\right)).\)

6.7 Expansion to base \(b\)

Proposition 8 [2, p. 177] is Let \(b\) be an integer > 1. For each integer \(k > 0\) let \(E_k\) be the lexicographic product of the family \(\{J_h\}_{0 \leq h \leq k-1}\) of intervals all identical with \([0, b-1]\); For each \(r = (r_0, r_1, \ldots, r_{k-1}) \in E_k\), let \(f_k(r) = \sum_{h=0}^{k-1} r_h b^{k-h-1};\) then the mapping \(f_k\) is an isomorphism of the ordered set \(E_k\) onto the interval \([0, b^k - 1]\). Bourbaki notes that (if \(a > 0\)) there is a least integer \(k\) such that \(a < b^k\) hence a unique sequence \(r_h\) such that

\[
a = \sum_{h=0}^{k-1} r_h b^{k-h-1}
\]

subject to the conditions \(0 \leq r_h \leq b - 1\) for \(0 \leq h \leq k - 1\) and \(r_0 > 0.\)

Discussion. We say that (1) is a BE-expansion, and it is a normalized expansion if either \(k = 0\) (the sum is empty) or \(r_0 > 0.\) The quantity \(r_h\) is the digit of index \(k,\) and \(r_0\) is the leading
digit. We can restate the theorem as: every integer has an expansion to base \( b \) for some \( k \), and a unique normalized expansion. Two numbers expressed in base \( b \) with \( k \) digits can be compared using only the value of the digits, starting with the leading digits. We can complete the theorem as follows: one can add or remove zero leading digits in the expansion, hence given two numbers with \( k \) and \( k' \) digits, one can add leading zeroes to smallest sequence, then apply the theorem, or else remove leading zeroes in order to get normalized expansions, and then the number that has the smallest number of digits is the smallest number.

Note that the conditions \( 0 \leq r_h \) and \( 0 \leq h \) are redundant, since negative integers have not yet been introduced. The conditions can be restated as \( r_h < b \) for \( h < k \), and the interval \([0, b - 1]\) is the interval \([0, b] \), this is the set of all integers \( < b \). The condition \( 0 \leq h \leq k - 1 \) is equivalent to \( 0 \leq k - h - 1 \leq k - 1 \), and the sum can be rewritten as \( \sum_{h=0}^{k-1} r_{k-h-1} b^h \). If \( s_k = r_{k-h-1} \), we get

\[
a = \sum_{h=0}^{k-1} s_h b^h
\]

subject to the conditions \( 0 \leq s_h \leq b - 1 \) for \( 0 \leq h \leq k - 1 \) and \( s_{k-1} \neq 0 \) is the normalization condition. We call this the LE-expansion. Associated to \( f_k(r) \) is the function \( g_k(s) \).

If \( \psi(s) \) is the sequence \( (s_1, \ldots, s_k) \), then

\[
g_{k+1} = s_0 + b \cdot g_k(\psi(s))
\]

(Bourbaki has a similar formula with \( f \) and \( \phi \)). This is a recursive definition; one can convert it into an iterative one: as long as there are digits, multiply by \( b \) and add the next digit. We start with \( s_{k-1} \) and terminate with \( s_0 \). This means that we consider digits from left to right, \( r_0 \) then \( r_1 \), then \( r_2 \), etc. This is called the Horner scheme for the formula (1), and is used by every computer program to read numbers. If \( s \) is represented as a list, then \( s_0 \) is the head of the list and \( \psi(s) \) is its tail, and (3) is the natural way to associate a value to the list.

A consequence of (3) is that \( s_0 \) and \( g_k(\psi(s)) \) are the remainder and quotient of the Euclidean division of \( a \) by \( b \), and this shows uniqueness by induction. Computers use this method for printing numbers, i.e., finding the sequence \( s_h \) given \( a \); the number \( k \) is not known a priori. In practice, one has either fixed-size numbers, say \( < 2^{32} \), case where an apriori bound can be found; or else \( a = \sum_0^{k-1} s_h b^h \), for some \( B \), case where \( k \leq nK \) for some \( n \), which is the size of the expansion of \( B \) in base \( b \). The digits are computed one after the other, stored in a buffer. After that, the number is normalized (useless zeroes are removed).

Assume \( s_0 < b \), \( s_0' < b \); then \( s_0 + bg \leq s_0 + bg' \) if and only if either \( g = g' \) and \( s_0 \leq s_0' \) or \( g < g' \). This condition is equivalent to \( (g, s_0) \leq (g', s_0') \), where \((g, s_0)\) is in the substrate of some lexicographic product \( F_k \times J \) of two sets. By induction, we can identify \( F_k \) with the set of sequences \( (s_1, \ldots, s_k) \). Because \( s_0 \) comes after \( g \), this set is the lexicographic product in reverse order of the sets \( J_h \). Thus, the ordering of the sequence \( r_h \) is the lexicographic product of the sets \( J_h \).

Consider now the sequence \( \Psi(s) = (s_0, \ldots, s_{k-1}) \), then

\[
g_{k+1} = g_k(\Psi(s)) + s_k \cdot b^k.
\]

It happens that \( s_k \) and \( g_k(\Psi(s)) \) are the quotient and remainder of the Euclidean division of \( g_{k+1} \) by \( b^k \). This is an alternate way to show uniqueness of the expansion (one could use it to

\[\text{According to Wikipedia, little-endian storage means: increasing numeric significance with increasing memory addresses; big-endian is its opposite, most-significant byte first.}\]
print a number in a computer program, the drawback being that one has to compute all \( b^k \) in decreasing order). Note that \( s_k b^k \leq g_{k+1} < (s_k + 1)b^k \). This shows that two numbers with distinct leading digits compare as their leading digits, and shows the theorem. We shall use this approach since \( \Psi \) is just the restriction.

We define an expansion to be a family of \( k \) terms, all less than \( b \), where \( k \) and \( b \) are integers, \( b \geq 2 \). The domain of the family is the interval \([0,k]\), it is the set of integers \( i \) with \( i < k \). The associated value is \( \sum f_i b^i \). It is an integer. If we have an expansion of length \( k+1 \), the restriction to \([0,k]\) is an expansion. The values are the same, up to the quantity \( f_k b^k \). Similarly, we can extend an expansion from size \( k \) to size \( k+1 \).

\begin{align*}
\text{Lemma } b\text{\textunderscore power\textunderscore k\textunderscore large: } & \forall a, b, \text{inc } a, \text{inc } b \\
& \quad \text{card\textunderscore lt } a \land \text{card\textunderscore le } b \\
& \quad \text{inc } k, \text{card\textunderscore lt } k \\
& \quad \exists k, \text{inc } k, \text{card\textunderscore le } k \\
& \quad \text{card\textunderscore le } (\text{card\textunderscore pow } b^k). \\
\text{Definition } \text{is\textunderscore expansion } f, b, k := \\
& \quad \text{inc } b, \text{inc } k, \text{card\textunderscore one } b \\
& \quad \text{f\textunderscore graph } f \\
& \quad \text{domain } f = \text{interval\textunderscore co\textunderscore 0a } k \\
& \quad \forall i, \text{inc } i (\text{domain } f) \\
& \quad \text{card\textunderscore lt } i, k \\
& \quad \text{inc } (V i f). \\
\text{Definition } \text{expansion\textunderscore value } f, b := \\
& \quad \text{card\textunderscore sum } (L (\text{domain } f) (\text{fun } i \rightarrow \text{card\textunderscore mult } (V i f) (\text{card\textunderscore pow } b i))). \\
\text{Lemma } \text{is\textunderscore expansion\textunderscore prop0: } & \forall f, b, k, i, \\
& \quad \text{is\textunderscore expansion } f, b, k \\
& \quad \text{inc } i (\text{domain } f) = \text{card\textunderscore lt } i, k. \\
\text{Lemma } \text{is\textunderscore expansion\textunderscore prop1: } & \forall f, b, k, i, \\
& \quad \text{is\textunderscore expansion } f, b, k \\
& \quad \text{card\textunderscore lt } i, k \\
& \quad \text{inc } (V i f) B\text{nat}. \\
\text{Lemma } \text{is\textunderscore expansion\textunderscore prop2: } & \forall f, b, k, \\
& \quad \text{is\textunderscore expansion } f, b, k \\
& \quad \text{finite\textunderscore int\textunderscore fam } (L (\text{domain } f) (\text{fun } i \rightarrow \text{card\textunderscore mult } (V i f) (\text{card\textunderscore pow } b i))). \\
\text{Lemma } \text{is\textunderscore expansion\textunderscore prop3: } & \forall f, b, k, \\
& \quad \text{is\textunderscore expansion } f, b, k \\
& \quad \text{inc } (\text{expansion\textunderscore value } f, b) B\text{nat}. \\
\text{Lemma } \text{is\textunderscore expansion\textunderscore prop4: } & \forall f, b, k, \\
& \quad \text{is\textunderscore expansion } f, b, k \\
& \quad \text{is\textunderscore cardinal } k \\
& \quad \text{inc } k B\text{nat}. \\
\text{Lemma } \text{is\textunderscore expansion\textunderscore prop5: } & \forall f, b, k, \\
& \quad \text{is\textunderscore expansion } f, b, k \\
& \quad \text{is\textunderscore expansion } (\text{restr } f (\text{interval\textunderscore co\textunderscore 0a } k)) b, k. \\
\text{Lemma } \text{is\textunderscore expansion\textunderscore prop6: } & \forall f, b, k, \\
& \quad \text{is\textunderscore cardinal } k \\
& \quad \text{is\textunderscore expansion } f, b (\text{succ } k) \\
& \quad \text{inc } (V k f) B\text{nat}. \\
\text{Lemma } \text{is\textunderscore expansion\textunderscore prop7: } & \forall f, b, k, \\
& \quad \text{is\textunderscore expansion } f, b (\text{succ } k) \\
& \quad \text{is\textunderscore cardinal } k \\
& \quad \text{expansion\textunderscore value } f, b (\text{succ } k) \\
& \quad \text{inc } (\text{expansion\textunderscore value } f, b) B\text{nat}. \\
& \quad \text{expansion\textunderscore value } f, b. \\
\text{Lemma } \text{is\textunderscore expansion\textunderscore prop8: } & \forall f, b, k, \\
& \quad \text{let } g := L (\text{interval\textunderscore co\textunderscore 0a } k) (\text{fun } i \rightarrow \text{Yo } i = k) x (V i f) \\
& \quad \text{is\textunderscore expansion } f, b, k \\
& \quad \text{inc } x B\text{nat} \\
& \quad \text{inc } (\text{expansion\textunderscore value } g, b) \\
& \quad \text{expansion\textunderscore value } g, b = \text{card\textunderscore plus } (\text{expansion\textunderscore value } f, b) \\
& \quad \text{card\textunderscore mult } (\text{card\textunderscore pow } b k, x). \\
\end{align*}

We have \( \sum_{i < k} f_i b^i < b^k \). As a consequence the quotient and remainder of the division of \( \sum_{i < k+1} f_i b^i \) by \( b^k \) are \( f_k \) and \( \sum_{i < k} f_i b^i \). This shows uniqueness of the expansion. If \( a < b^k \)
there is an extension of length \( k \) (proof by induction, the highest term is the quotient of the division by \( b^{k-1} \)). Since \( a < b^k \), there is at least one extension.

Lemma is_expansion_prop9: \( \forall f \ b \ k, \ is\_expansion f b k \rightarrow \)
\( \text{cardinal}_{\lt}(\expansion\_value f b) (\text{card}_{\lt} b k).(*)^{22} \)

Lemma is_expansion_prop10: \( \forall f \ b \ k, \ is\_cardinal k \rightarrow \)
\( \text{is}\_expansion f b (\text{succ} k) \rightarrow \)
\( \text{division\_prop}(\expansion\_value f b) (\text{card}_{\lt} b k) (V k f) \)
\( (\expansion\_value (\text{restr f} (\text{interval\_co_0a} k)) b). \)

Lemma is_expansion_unique: \( \forall f \ g \ b \ k, \)
\( \text{is}\_expansion f b k \rightarrow \text{is}\_expansion g b k \rightarrow \)
\( \expansion\_value f b = \expansion\_value g b \rightarrow f = g.(*)^{32} \)

Lemma is_expansion_exists1: \( \forall a \ b \ k, \ inc \ a B\text{nat} \rightarrow \text{inc b B\text{nat} \rightarrow} \)
\( \text{cardinal}_{\lt} a (\text{card}_{\lt} b k) \rightarrow \)
\( \exists f, \ (\text{is}\_expansion f b k \& \expansion\_value f b = a). \)

Lemma is_expansion_exists: \( \forall a \ b, \ inc \ a B\text{nat} \rightarrow \text{inc b B\text{nat} \rightarrow} \)
\( \exists k, \exists f, \)
\( \text{is}\_expansion f b k \rightarrow \exists k, \exists f, \)
\( (\text{is}\_expansion f b k \& \expansion\_value f b = a). \)

As a consequence \( \sum_{i<k+1} f^i b^i \) and \( \sum_{i<k+1} g^i b^i \) are in the same order as \( f_k \) and \( g_k \) if these are different. **Todo**: state and prove a theorem that compares two arbitrary expansions.

Lemma is_expansion_prop11: \( \forall f \ g \ b \ k, \ is\_cardinal k \rightarrow \)
\( \text{is}\_expansion f b (\text{succ} k) \rightarrow \text{is}\_expansion g b (\text{succ} k) \rightarrow \)
\( \text{cardinal}_{\lt} (V k f) (V k g) \rightarrow \)
\( \text{cardinal}_{\lt} (\expansion\_value f b) (\expansion\_value g b). \)

### 6.8 Combinatorial analysis

The next result is Proposition 9 [2, p. 179], known in French as the shepherd’s principle. If \( f \) is a function from a set with cardinal \( a \) onto a set with cardinal \( b \), and if all set \( f^{-1}(\{x\}) \) have the same cardinal \( c \), then \( a = bc \). Bourbaki assumes \( f \) surjective; in fact if \( x \) is in the target but not in the range, then \( c = 0, \) and the source is empty.

Theorem shepherd_principle: \( \forall f \ c, \ is\_function f \rightarrow \)
\( (\forall x, \text{inc} x (\text{target} f) \rightarrow \text{cardinal} (\text{inv\_image\_by\_fun f} (\text{singleton} x))=c) \)
\( \rightarrow \text{cardinal} (\text{source} f) = \text{card}_{\mult} (\text{cardinal} (\text{target} f)) c. (*)^{27} \)

### 6.8.1 Iterated functions

Note: all useful results of this section have been moved to section 6.4.2. The remaining trivial results are given without comment.

Definition function_on_nat f :=
\( \text{fun} \ m \rightarrow \text{nat}\_\text{to}\_B (f (\text{cardinal}\_\text{nat} m)). \)

Lemma inc_function_on_nat_Bnat : \( \forall f \ n, \)
\( \text{inc} (\text{function\_on\_nat} f n) \text{\_B\text{nat}.} \)

Lemma function_on_nat_pr : \( \forall f n, \)
\( \text{cardinal}\_\text{nat}(\text{function\_on\_nat} f n) = f (\text{cardinal}\_\text{nat} n). \)

Lemma function_on_nat_pr1 : \( \forall f n, \)
\( \text{function\_on\_nat} f (\text{nat}\_\text{to}\_B n) = \text{nat}\_\text{to}\_B (f n). \)

INRIA
6.8.2 Factorial

Bourbaki defines the factorial of \( n \), denoted by \( n! \), as \( \prod_{i < n} (i + 1) \). If \( S \) is the successor function, this is \( \Pi' \langle S \rangle \), with the notations of page 116; it satisfies \( 0! = 1 \) and \( (n + 1)! = n! (n + 1) \). These two conditions characterize the function. We define the factorial function by induction, something that Bourbaki cannot do yet (defining a function by induction is introduced in the next chapter).

```coq
Fixpoint factorial (n:nat) : nat :=
  match n with
  | 0 => 1
  | S p => (factorial p) * S p
  end.

Lemma factorial0: factorial 0 = 1.
Lemma factorial1: factorial 1 = 1.
Lemma factorial2: factorial 2 = 2.
Lemma factorial_succ: forall n, factorial (S n) = (factorial n) * (S n).
Lemma factorial_nonzero: forall n, 0 <> factorial n.
Lemma factorial_prop: forall f, f 0 = 1 ->
  (forall n, f (S n) = (f n) * (S n)) ->
  forall x, f x = factorial x.
Lemma factorial_prop1: forall n, factorial n = fct_prod S n.
```

6.8.3 Number of injections

Proposition 10 \([2, p. 170]\) says that the number of injections from a set with \( m \) elements to a set with \( n \) elements is \( A_{nm} = n!/ (n - m)! \). Note that, if such an injection exists, we have \( m \leq n \); otherwise the number is zero. We first prove that the quantity is well-defined, since if \( J \subset I \), the product \( \prod f_i \) restricted to \( J \) divides the product \( \prod f_i \) restricted to \( J \). In fact, in order to show this, we have to prove some auxiliary facts (\( f_i \) must be a non-zero integer, so that the products are non-zero, etc). This requires 44 lines of proof, but proving by induction on \( c \) that \( b! \) divides \( (b + c)! \) requires only 3 lines.

Thus, if \( m \leq n \), then \( m! \) and \( (n - m)! \) divide \( n! \); it happens that the product of these two numbers divides \( n! \), but such a result is generally false.

```coq
(*
  Lemma divides_restriction_product: forall f x, fgraph f ->
  (forall i, inc i (domain f) -> is_finite_c (V i f)) ->
  (forall i, inc i (domain f) -> (V i f) <> card_zero) ->
  is_finite_set (domain f) -> sub x (domain f) ->
  Bnat_divides (cardinal_prod (restr f x)) (cardinal_prod f).
  Lemma quotient_of_factorials: forall a b, inc a Bnat -> inc b Bnat ->
  cardinal_le b a -> Bnat_divides (factorial b) (factorial a).
*)

Lemma quotient_of_factorials: forall a b, b <= a ->
  Ndivides (factorial b) (factorial a).
Lemma quotient_of_factorials1: forall a b, b <= a ->
  Ndivides (factorial (a - b)) (factorial a).
```
Consider an injective function \( f \) from \( A \) into \( B \), which are sets with cardinals \( a \) and \( b \), we know \( a \leq b \); since \( a \) is the cardinal of the image, the quantity \( b - a \) is the cardinal of the complement of \( f(A) \) in \( B \).

**Lemma tack_on_nat:** \( \forall \, a, b, \; \text{is_finite_c} \left( \text{cardinal} \left( \text{tack_on} \, a \, b \right) \right) \rightarrow \\
\quad \neg \, \left( \text{inc} \, b \, a \right) \rightarrow \text{cardinal_nat} \left( \text{tack_on} \, a \, b \right) = S \left( \text{cardinal_nat} \, a \right). \)

**Lemma cardinal_complement_image:** \( \forall \, f, \; \text{injective} \, f \rightarrow \\
\quad \text{is_finite_set} \left( \text{target} \, f \right) \rightarrow \\
\quad \left( \text{cardinal} \, \left( \text{source} \, f \right) \right) \land \\
\quad \text{cardinal} \left( \text{complement} \left( \text{target} \, f \right) \left( \text{image_of_fun} \, f \right) \right) = \\
\quad \text{card_sub} \left( \text{cardinal} \, \left( \text{target} \, f \right) \right) \left( \text{cardinal} \, \left( \text{source} \, f \right) \right). \) (* 21 *)

We have \( A_{nm}(n-m)! = n! \). From this we deduce \( A_{nm}(n-m) = A_{n,m+1} \).

**Definition number_of_injections** \( b \, a := \\
\quad \text{Nquo} \left( \text{factorial} \, a \right) \left( \text{factorial} \left( a - b \right) \right). \)

**Lemma number_of_injections_pr:** \( \forall \, a, b, \; b \leq a \rightarrow \\
\quad \left( \text{number_of_injections} \, b \, a \right) \ast \left( \text{factorial} \left( a - b \right) \right) = \text{factorial} \, a. \)

**Lemma number_of_injections_rec:** \( \forall \, a, b, \; b < a \rightarrow \\
\quad \left( \text{number_of_injections} \, b \, a \right) \ast \left( a - b \right) = \text{number_of_injections} \left( S \, b \right) \, a. \)

**Lemma number_of_injections_base:** \( \forall \, a, \; \text{number_of_injections} \, 0 \, a = 1. \)

The proof of the proposition is as follows. If \( m = 0 \), then \( A_{nm} = 1 \); and there is a unique function from the empty set into \( E \), this function is injective. Consider now \( A = A' \cup \{ a \} \), where \( A' \) has \( m \) elements. Let \( G_1 \) and \( G_2 \) be the sets of injective functions from \( A \) and \( A' \) to \( F \), and \( H_1 \) and \( H_2 \) their cardinals. By induction, using the recurrence formula for \( A_{nm} \) we must show \( H_1 = H_2(n-m) \). Given \( f \in G_1 \), its restriction \( R(f) \) to \( A' \) is obviously injective, hence is in \( G_2 \). Given \( f' \in G_2 \), and \( b \in F \), there is a unique \( f \) with \( f' = R(f) \) and \( f(a) = b \). This function is an injection if and only if \( b \) is not in the range of \( f' \). In other terms, \( f \rightarrow f(a) \) is a bijection from \( R^{-1}(\{f'\}) \) onto the complementary of the range of \( f' \) that has \( n-m \) elements. Hence \( R^{-1}(\{f'\}) \) has \( n-m \) elements; the conclusion follows from the shepherd's principle.

**Definition set_of_injections** \( E \, F := \\
\quad \text{Zo} \left( \text{set_of_functions} \, E \, F \right) \left( \text{fun} \, z=> \text{injective} \left( \text{inv_corr_value} \, z \right) \right). \)

**Lemma number_of_injections_prop:** \( \forall \, E \, F \, n \, m, \; \left( \ast \, 128 \, \ast \right) \\
\quad \text{cardinal} \, E = \text{nat_to_B} \left( n \rightarrow \text{cardinal} \, F \right) \rightarrow \text{nat_to_B} \, m \rightarrow \, n \leq m \rightarrow \\
\quad \text{cardinal} \left( \text{set_of_injections} \, E \, F \right) = \text{nat_to_B} \left( \text{number_of_injections} \, n \, m \right). \)

An injection from \( E \) into itself is a bijection when \( E \) is finite. Since \( A_{nn} = n! \), we deduce that \( n! \) is the number of *permutations* of \( E \).

**Definition set_of_permutations** \( E := \\
\quad \left( \text{Zo} \left( \text{set_of_functions} \, E \, E \right) \left( \text{fun} \, z=> \text{bijective} \left( \text{inv_corr_value} \, z \right) \right) \right). \)

**Lemma number_of_permutations:** \( \forall \, E \, n, \; \text{cardinal} \, E = \text{nat_to_B} \left( n \rightarrow \text{cardinal} \left( \text{set_of_permutations} \, E \right) \right) = \text{nat_to_B} \left( \text{factorial} \, n \right). \)

INRIA
6.8.4 Number of coverings

Proposition 11 [2, p. 180] says that if $E$ is a set with $n$ elements, $n = \sum p_i$, the number of coverings by mutually disjoint sets $(X_i)_{i \in I}$ of $E$ such that $\text{Card}(X_i) = p_i$ is $n!/(\prod p_i!)$. By abuse of language, we shall call this a partition of $E$ (the abuse is that $X_i$ is required to be non-empty for a partition, and also that, in the first Chapter, we defined the set of partitions of $E$ as a subset of $\mathcal{P}(\mathcal{P}(E))$). Here we consider functions, i.e., a subset of $\mathcal{F}(I, \mathcal{P}(E))$. For Bourbaki, the index set $I$ is the interval $[1, h]$ but any finite set could be used instead. The "number of objects such that $Q$" is the cardinal of the set of objects such that $Q$, and we first exhibit this set. The proof of the proposition will show that $B(p_1) = n!/\prod p_i$ is well defined. The quantity $B(p_1, p_2)$ is called the binomial coefficient; it satisfies $B(p_1+1, q) + B(p_1, q+1) = B(p_1+1, q+1)$ hence is an integer (this is Proposition 13), so that $B(p_1)$ is an integer, by induction on the number of $p_i$ (for instance $B(p_1, p_2, p_3) = B(p_1+p_2, p_3)B(p_1, p_2)$). The proof given here is not by induction. It is a rather long (over 500 lines).

In the definition that follows, $p$ is the sequence of integers $p_i$, $E$ is the base set, $f$ is the function $i \mapsto X_i$ and $z$ is the value of the function (as a set). Assume that $\text{Card}(E) = \sum p_i$. This means that we have a bijection $f$ from the disjoint union of $p_i$ to $E$. Let $F_i = p_i \times \{i\}$; the source of $f$ is the union of these $F_i$ whose cardinal is the same as the cardinal of $p_i$ which is $p_i$. We pretend that $f(F_i)$ and $F_i$ have the same cardinal. Thus, if $P$ denotes the set of partitions of $E$ with $p_i$ elements, $P$ is non-empty since $i \mapsto f(F_i)$ belongs to $P$.

Definition partition_with_pi_elements $p E f :=$
   is_function $f$ & source $f = \text{domain } p$ &
   (forall $i$, inc $i$ (domain $p$) -> cardinal ($W i f$) = $V i p$) &
   partition_fam (graph $f$) $E$.

Definition set_of_partitions $p E :=$
   Zo(set_of_functions (domain $p$) (powerset $E$))
   (fun $z$=> partition_with_pi_elements $p E$ (inv_corr_value $z$)).

Lemma equipotent_restriction: forall $f x$,
   sub $x$ (source $f$) -> bijective $f$ ->
   equipotent $x$ (image_by_fun $f x$).

Lemma mutually_disjoint_prop1: forall $f$, is_function $f$ ->
   (forall $i j y$, inc $i$ (source $f$) -> inc $j$ (source $f$) ->
    inc $y$ ($W i f$) -> inc $y$ ($W j f$) -> $i=j$) ->
   mutually_disjoint (graph $f$).

Lemma number_of_partitions1: forall $p E$,
   finite_int_fam $p$ -> cardinal_sum $p$ = cardinal $E$ ->
   nonempty(set_of_partitions $p E$). (* 28 *)

Define $Q(E)$ to be the set of permutations of $E$. Assume $g \in Q(E)$. Denote by $\psi(p, E, f, g)$ the mapping $i \mapsto g(E_i)$; it belongs to $P$ (same argumentation as before). Thus we have a function $\phi : g \mapsto \psi(p, E, f, g)$, from $Q$ to $P$. We pretend this is surjective (lemma 4) (if $X_i$ is a partition with $p_i$ elements, then $F_i$ is equipotent to $X_i$; this gives a bijection $h_i$ from $F_i$ to $X_i$, hence a function $g_i$ that extends $h_i$, with target $E$, and a function $g$ that coincides with $g_i$ on $F_i$).

Definition set_of_partitions_aux $p E f g :=$
   BL (fun $i$ => image_by_fun (inv_corr_value $g$) ($W i f$))

RR n° 7150
Lemma number_of_partitions2: \( \forall E \, p \, f \, g, \)
\( \text{inc } g \, (\text{set_of_permutations } E) \rightarrow \)
\( \text{transf_axioms } (\text{fun } i \Rightarrow \text{image_by_fun} \, (\text{inv_corr_value } g) \, (W \, i \, f)) \)
\( (\text{domain } p) \, (\text{powerset } E) \).

Lemma number_of_partitions3: \( \forall E \, p \, f \, g, \) (* 29 *)
\( \text{finite_int_fam } p \rightarrow \text{cardinal_sum } p = \text{cardinal } E \rightarrow \)
\( \text{partition_with_pi_elements } p \, E \, f \rightarrow \text{inc } g \, (\text{set_of_partitions } E) \rightarrow \)
\( \text{inc } (\text{corr_value } (\text{set_of_partitions_aux } p \, E \, f \, g)) \, (\text{set_of_partitions } p \, E) \).

Lemma number_of_partitions4: \( \forall E \, p \, f, \) (* 78 *)
\( \text{finite_int_fam } p \rightarrow \text{cardinal_sum } p = \text{cardinal } E \rightarrow \)
\( \text{partition_with_pi_elements } p \, E \, f \rightarrow \)
\( \text{surjective } (\text{BL } (\text{fun } g \Rightarrow \text{corr_value } (\text{set_of_partitions_aux } p \, E \, f \, g)) \)
\( (\text{set_of_partitions } E) \, (\text{set_of_partitions } p \, E)) \).

This function \( \phi \) is not injective: lemma 5 says \( \phi(g) = \phi(h) \) if and only if \( h^{-1} \circ g \) is a bijection that leaves each \( f(i) \) invariant. Fix \( h \); for each \( g \) and \( i \), the restriction \( \psi_i \) of \( h^{-1} \circ g \) to \( f(i) \) can be considered as a function from \( f(i) \) to itself; it is in fact a bijection, hence the family \( (\psi_i)_i \) is an element of the product of the sets \( Q(f(i)) \) (this is lemma 6).

Consider now the function \( \Phi \) that associates to each permutation \( k \) of \( E \) the family of restrictions to \( A_i = f(i) \). If \( k \) leaves \( A_i \) invariant, the restriction of \( k \) to \( A_i \) is a bijection, so that, if we consider as target of \( \Phi \) the product of the permutations of \( A_i \), \( \Phi \) is well-defined for \( h^{-1} \circ g \), for each \( g \in \phi^{-1}(\langle h \rangle) \). This is a bijection (lemma 7). The main result follows: the target of \( \Phi \) has cardinal \( \prod p_i ! \); the source of \( \Phi \) is \( \phi^{-1}(\langle h \rangle) \) if we take \( k = h^{-1} \circ g \); it then suffices to apply the shepherd’s principle.

Lemma number_of_partitions5: \( \forall E \, p \, f \, g \, h, \) (* 43 *)
\( \text{finite_int_fam } p \rightarrow \text{cardinal_sum } p = \text{cardinal } E \rightarrow \)
\( \text{partition_with_pi_elements } p \, E \, f \rightarrow \)
\( \text{inc } h \, (\text{set_of_permutations } E) \rightarrow \text{inc } g \, (\text{set_of_permutations } E) \rightarrow \)
\( (\text{set_of_partitions_aux } p \, E \, f \, g = \text{set_of_partitions_aux } p \, E \, f \, h) = \)
\( (\forall i, \text{inc } i \, (\text{domain } p) \rightarrow \text{image_by_fun } (\text{compose} \, (\text{inverse_fun} \, (\text{inv_corr_value } h))) \, (W \, i \, f) = (W \, i \, f)) \).

Lemma number_of_partitions6: \( \forall E \, p \, f \, h, \) (* 33 *)
\( \text{finite_int_fam } p \rightarrow \text{cardinal_sum } p = \text{cardinal } E \rightarrow \)
\( \text{partition_with_pi_elements } p \, E \, f \rightarrow \)
\( \text{inc } h \, (\text{set_of_permutations } E) \rightarrow \)
\( \text{transf_axioms } (\text{fun } g \Rightarrow \text{L } (\text{domain } p)(\text{fun } i \Rightarrow \text{corr_value } (\text{restriction2} \)
\( (\text{compose} \, (\text{inverse_fun} \, (\text{inv_corr_value } h))) \, (\text{inv_corr_value } g))) \)
\( (W \, i \, f) \, (W \, i \, f))) \)
\( (\text{Zo } (\text{set_of_permutations } E) \)
\( (\text{fun } g \Rightarrow (\text{set_of_partitions_aux } p \, E \, f \, g = \text{set_of_partitions_aux } p \, E \, f \, h))) \)
\( (\text{productb } (\text{L } (\text{domain } p)(\text{fun } i \Rightarrow (\text{set_of_permutations } (W \, i \, f)))))) \).

Lemma number_of_partitions7: \( \forall E \, p \, f \, h, \) (* 148 *)
\( \text{finite_int_fam } p \rightarrow \text{cardinal_sum } p = \text{cardinal } E \rightarrow \)
\( \text{partition_with_pi_elements } p \, E \, f \rightarrow \)
\( \text{inc } h \, (\text{set_of_permutations } E) \rightarrow \)
\( \text{bijective } (\text{BL } (\text{fun } g \Rightarrow \text{L } (\text{domain } p)(\text{fun } i \Rightarrow \text{corr_value } (\text{restriction2} \)
\( (\text{compose} \, (\text{inverse_fun} \, (\text{inv_corr_value } h))) \, (\text{inv_corr_value } g))) \)
\( (W \, i \, f) \, (W \, i \, f))) \)
\( (\text{Zo } (\text{set_of_permutations } E) \)
\( (\text{fun } g \Rightarrow (\text{set_of_partitions_aux } p \, E \, f \, g = \text{set_of_partitions_aux } p \, E \, f \, h))) \)

INRIA
We give here the long and the short version of the theorem.

**Definition** factorialC n := nat_to_B (factorial (cardinal_nat n)).

**Theorem** number_of_partitions: forall p E, finite_int_fam p -> cardinal_sum p = cardinal E ->
let num:= factorialC (cardinal E) in
let den := cardinal_prod (L (domain p) (fun z => factorial (V z p)))
in (num = card_mult (cardinal (set_of_partitions p E)) den &
is_finite_c num & is_finite_c den & den <> card_zero &
is_finite_set (set_of_partitions p E)). (* 55 *)

**Theorem** number_of_partitions_bis: forall p E, finite_int_fam p -> cardinal_sum p = cardinal E ->
cardinal (set_of_partitions p E) =
card_quo (factorialC (cardinal E))
  (cardinal_prod (L (domain p) (fun z => factorialC (V z p)))).

**Todo:** restate this theorem using lists instead of families. The idea would be the following. Consider a list L of sets with elements L_i, and a list of integers p with elements p_i. It makes sense to define the property Q(E,L,p): L and p have the same length, L_i is of cardinal p_i, L_i ⊂ E. One can define by induction the sum n of the list p and the union U of the list L, and add the conditions U = E and n = card(E). This condition is equivalent to say that the sets L_i are mutually disjoint.

### 6.8.5 The binomial coefficient

We define here by induction a function, called the *binomial coefficient*, satisfying

\[
\begin{align*}
\binom{n}{0} &= 1, \\
\binom{0}{p+1} &= 0, \\
\binom{n+1}{p+1} &= \binom{n}{p} + \binom{n}{p+1}.
\end{align*}
\]

We show here

\[
\begin{align*}
\binom{n}{0} &= 1, \\
\binom{n}{1} &= n, \\
\binom{n+1}{2} &= \frac{n(n+1)}{2}.
\end{align*}
\]

**Fixpoint** binom (n p:nat) {struct n} : nat :=
match n, p with
| 0, 0 => 1
| 0, S m => 0
| S q, 0 => 1
| S q, S m => (binom q (S m)) + (binom q m)
end.

**Lemma** binom0: forall n, binom n 0 = 1.
**Lemma** binom1: forall n, binom n 1 = n.
**Lemma** binom2a: forall n, 2*(binom (S n) 2) = n * S n.
**Lemma** binom2: forall n, binom (S n) 2 = Nquo (n * S n) 2.

Let f(n,p) be the product of the binomial coefficient by p!(n−p)!. Note that if p > n, n − p is zero by convention and (n−p)! is one. We have then (n−p)! = if(p < n, n−p, 1).(n−(p+1))!. This gives us an induction property for f, from which we deduce f(n,p) = if(p ≤ n, n!, 0).
Lemma binom_alt_pr: forall n m, (binom n m) * (factorial m) * (factorial (n-m)) = if(le_lt_dec m n) then (factorial n) else 0.

Eliminating if gives now the following
\[
\binom{n}{p} = \binom{n}{n-p} = \frac{n!}{p!(n-p)!}
\]
when \( p \leq n \) \( \binom{n}{p} = 0 \) when \( p > n \).

Moreover division is exact. Proposition 13 \cite[p. 181]{2} is the following relation, which is true by definition:
\[
\binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}.
\]

If \( p \leq n \), the binomial coefficient is non-zero; if \( p = n \) it is one, and if \( p \leq n + 1 \) it is a strictly increasing function of \( n \).

Lemma binom_pr: forall n p, p <= n -> Ndivides ((factorial p) * (factorial (n-p))) (factorial n).

Lemma binom_pr0: forall n p, p > n -> binom n p = 0.

Lemma binom_pr1: forall n p, p <= n -> binom n p = Nquo (factorial n) ( (factorial p) * (factorial (n-p))).

Lemma binom_pr2: forall n p, (binom n (p+1)) = (binom n (p+1)) + (binom n p).

Lemma binom_symmetric:forall n p, p <= n -> binom n p = binom n (n - p).

Lemma binom_nn : forall n, binom n n = 1.

Lemma binom_pr3: forall n p, p <= n -> 0<> binom n p.

Lemma binom_monotone1: forall k n m, 0<k<= S n -> n < m -> binom n k < binom m k.

Consider a set \( E \) with \( n \) elements, and the set of all subsets \( A \) of \( E \) with \( p \) elements; we shall denote this by \( Q_p(E) \), or simply \( Q_p \). If \( p > n \) this set is empty. We assume here \( p \leq n \). If \( A \) is a subset of \( E \) with \( p \) elements, then \( E - A \) has \( n - p \) elements; these two sets form a partition of \( E \) with \( (p_i) \) elements, where the family \( (p_i) \) is formed of \( p \) and \( n - p \). We restate this as: \((X_i)_i \rightarrow X_1\) is a bijection from the set of partitions of \( E \) with \( (p_i) \) elements onto \( Q_p \). Thus, these sets have the same cardinal, the quotient of \( n! \) and the product of the \( (p_i)! \), which is \( p!(n-p)! \). Note that \( A \rightarrow E - A \) is a bijection from \( Q_p \) to \( Q_{n-p} \).

The last theorem given here has the following form: if \( n \) and \( p \) are two natural numbers with \( p \leq n \), if \( Card(E) = \mathcal{N}(n) \) and if \( d \) is \( p!(n-p)! \), then \( Q_{\mathcal{N}(p)}(E) \) is finite, \( d \neq 0 \) and \( n! = d \cdot card(Q_{\mathcal{N}(p)}(E)) \).

Definition subsets_with_p_elements p E:= Zo (powerset E)(fun z=> cardinal z = p).

Lemma binomial1: forall n p, inc n Bnat -> inc p Bnat ->
  cardinal_le p n -> finite_int_fam (Lvariantc p (card_sub n p)).

Lemma binomial2: forall n p, inc n Bnat -> inc p Bnat ->
  cardinal_le p n -> cardinal_sum (Lvariantc p (card_sub n p)) = n.

Lemma cardinal_complement: forall A E, sub A E ->

\[\text{INRIA}\]
Lemma cardinal_complement1: forall n p E A, inc n Bnat -> inc p Bnat ->
  cardinal E = n -> cardinal A = p -> sub A E ->
  cardinal (complement E A) = card_sub n p.

Lemma cardinal_complement2: forall n p E A, inc n Bnat -> inc p Bnat ->
  cardinal le p n -> let pp:=Lvariantc p (card_sub n p) in
  cardinal Prod (L (domain pp) (fun z => factorialC (V z pp))) =
  card_mult (factorialC p) (factorialC (card_sub n p)).

Lemma subsets_with_p_elements_pr: forall n p E, inc n Bnat -> inc p Bnat ->
  cardinal E = n ->
  cardinal (set_of_partitions (Lvariantc p (card_sub n p)) E) =
  cardinal (subsets_with_p_elements p E). (* 58 *)

Lemma subsets_with_p_elements: forall n p E, inc n Bnat -> inc p Bnat ->
  cardinal E = n ->
  cardinal (subsets_with_p_elements p E) =
  cardinal (set_of_partitions (Lvariantc p (card_sub n p)) E).

We restate the previous result as: if $Q_p(E)$ is the set of subsets $A$ of $E$ with $\text{Card } A = N(p)$, then $\text{Card}(Q_p(E)) = N\left(\binom{n}{p}\right)$.

Theorem binomial7: forall n p E, cardinal E = nat_to_B n ->
  cardinal (subsets_with_p_elements (nat_to_B p) E) = nat_to_B(binom n p).

We have $\sum_{p \leq n} \binom{n}{p} = 2^n$ (this is Proposition 12 [2, p. 181]). The sum is over all $p$ with $p \leq n$; implicitly, in Bourbaki the sum is over all integers, with the convention that the coefficients of the binomial with $p > n$ are zero. We give two proofs for the same theorem. We first consider the relation $\sum \text{Card}(Q_p(E)) = N\left(\sum \binom{n}{p}\right)$. The sets $Q_p(E)$ are mutually disjoint and the union is the powerset of $E$ whose cardinal is $2^n$ (every subset of $E$ has a cardinal $p$ with $p \leq n$). The second proof is by induction on $n$. Let $B_n$ be the function $p \mapsto \binom{n}{p}$. We have

\begin{equation}
\sum_{p < n+1} B_{n+1}(p) = B_{n+1}(0) + \sum_{p < n} B_{n+1}(p+1).
\end{equation}

We have $\sum B_{n+1}(p+1) = \sum B_{n}(p+1) + \sum B_{n}(p)$ since the relation is true (without the $\sum$) by definition. By induction, the second sum is $2^n$; applying (*) with $n$ instead of $n+1$ shows that the first sum is $2^n$ (modulo the additional term, the conclusion follows because $B_{n+1}(0) = B_{n}(0)$).

Lemma sum_of_binomial: forall n, inc n Bnat ->
  cardinal_sum (L (interval Bnat card_zero n)
  (fun p => nat_to_B(binom (cardinal_nat n) (cardinal_nat p)))) =

RR n° 7150
Lemma sum_of_binomial1: forall n,
  fct_sum (fun p => binom n p) (S n) = pow 2 n.
Lemma sum_of_binomial2: forall n,
  fct_sum (binom n) (S n) = pow 2 n.

We show here that \(2^n = n + n\), hence \(2 + 2 = 4\) and \(2^4 = 4^2\).

Lemma two_plus_two: card_plus card_two card_two = card_four.
Lemma two_times_n: forall n, card_mult card_two n = card_plus n n.
Lemma two_times_two: card_mult card_two card_two = card_four.
Lemma power_2_4: card_pow card_two card_four = card_pow card_four card_two.

6.8.6 Number of increasing functions

Consider two finite totally ordered sets \(E\) and \(F\). Denote by \(\mathcal{S}(E,F)\) the set of strictly increasing mappings from \(E\) into \(F\). We pretend that

\[
\text{Card}(\mathcal{S}(E,F)) = \binom{n}{p} \quad \text{if Card}(E) = p \text{ and Card}(F) = n.
\]

The idea is that the mapping \(f \mapsto R(f)\) is a bijection from \(\mathcal{S}(E,F)\) onto the set of subsets with \(p\) elements of \(F\), where \(R(f)\) denotes the range of \(f\). We consider Theorem 3 (§ 2, no. 5), or its variant that says that if \(E\) and \(X\) are two finite equipotent totally ordered sets, there is a unique order isomorphism from \(E\) onto \(X\). We can extend this isomorphism into a strictly increasing function \(E \to F\). Conversely, if \(f\) and \(f'\) are two strictly increasing mappings, with the same range, if \(f = i \circ g\) and \(f' = i \circ g'\) are the canonical decompositions of the functions, where \(i\) is the canonical injection from the common range to \(F\), then \(g\) and \(g'\) are bijections, and equal by uniqueness.

Lemma cardinal_set_of_increasing_functions1: forall r r' f, total_order r -> strict_increasing_fun f r r' ->
  (order_morphism f r r' & cardinal (substrate r) = cardinal (image_of_fun f)).
Lemma cardinal_set_of_increasing_functions2: forall r r',
  total_order r -> total_order r' ->
  is_finite_set (substrate r) -> is_finite_set (substrate r') ->
  bijective(BL (fun z => range (graph (inv_corr_value z))))
  (Zo (set_of_functions (substrate r) (substrate r'))
  (fun z=> strict_increasing_fun (inv_corr_value z) r r'))
  (subsets_with_p_elements (cardinal (substrate r)) (substrate r')).

We give here a characterisation of increasing (and strictly increasing) functions whose source is a segment of \(N\). Let \(E\) be an ordered set, assume \(f(x) \in E\) for \(x \leq p\). Assume \(f(x) \leq_E f(y)\) for \(x, y \leq p\).
\[ f(x+1) \text{ for } x < p. \] Then \( f(x) \leq f(y) \) whenever \( x \leq y \leq p \) (we write \( y = x+c \) and use induction on \( c \)). Thus, if \( g \) is a mapping \([0, p] \rightarrow E\), then \( g \) is increasing (resp. strictly increasing and injective) if \( g(x) \leq g(x+1) \) (resp. \( g(x) < g(x+1) \)) for \( x < p \).

**Lemma increasing_prop1**: forall \( p \) \( f \) \( r \), inc \( p \) Bnat -> order \( r \) ->
\( \begin{align*}
\forall i, &\text{ cardinal_le } i \text{ p } \rightarrow \text{ inc } (f \ i) \text{ (subrate } r)) \rightarrow \\
\forall n, &\text{ cardinal_lt } n \text{ p } \rightarrow \text{ gle } r \ (f \ n) \ (f \ (\text{succ } n)) \rightarrow \\
\forall i, &\text{ cardinal_le } i \ j \rightarrow \text{ cardinal_le } j \ p \rightarrow \\
&\text{ gle } r \ (f \ i) \ (f \ j).
\end{align*} \)

**Lemma strict_increasing_prop1**: forall \( p \) \( f \) \( r \), inc \( p \) Bnat -> is_function \( f \) ->
\( \begin{align*}
\forall i, &\text{ cardinal_le } i \text{ p } \rightarrow \text{ inc } (f \ i) \text{ Bnat} \\
\forall i, &\text{ cardinal_le } i \ j \rightarrow \text{ cardinal_le } j \ p \rightarrow \\
&\text{ gle } r \ (f \ i) \ (f \ j)).
\end{align*} \)

**Lemma increasing_prop**: forall \( p \) \( f \) \( r \), inc \( p \) Bnat -> is_function \( f \) ->
\( \begin{align*}
\forall i, &\text{ cardinal_le } i \text{ p } \rightarrow \text{ inc } (f \ i) \text{ Bnat} \\
\forall i, &\text{ cardinal_le } i \ j \rightarrow \text{ cardinal_le } j \ p \rightarrow \\
&\text{ gle } r \ (f \ i) \ (f \ j)).
\end{align*} \)

Assume now \( f(x) \) is an integer, \( f(x) < f(y) \) for \( x < y \leq p \). Then \( x \leq f(x) \) for \( x < p \), by induction on \( x \). The function \( i \rightarrow f(i) - i \) is decreasing, according to the previous result. Denote by \( I_p \) the interval \([0, p]\). Assume \( f \) maps \( I_p \) into \( I_{n+p} \). When \( i < p \) we have \( f(i) - i \leq f(p-1) - (p-1) < n + p - p + 1 \), hence \( f(i) - i \in I_{n+1} \).

**Lemma strict_increasing_prop2**: forall \( f \) \( p \), inc \( p \) Bnat -> is_function \( f \) ->
\( \begin{align*}
\forall i, &\text{ cardinal_le } i \text{ p } \rightarrow \text{ inc } (f \ i) \text{ Bnat} \\
\forall i, &\text{ cardinal_le } i \ j \rightarrow \text{ cardinal_le } j \ p \rightarrow \\
&\text{ gle } r \ (f \ i) \ (f \ j)).
\end{align*} \)

**Denote by \( \mathcal{A}(E, F) \) the set of increasing mappings from \( E \) into \( F \). If \( f \) is a mapping, denote by \( s(f) \) the mapping \( i \rightarrow f(i) - i \). We have show that \( s \) is a mapping from \( \mathcal{I}(I_p, I_{n+p}) \) into \( \mathcal{A}(I_p, I_{n+p}) \). We pretend that it is a bijection. In fact, it is rather easy to show that the inverse mapping is \( a(f) : i \rightarrow f(i) + i \). If \( f \) is increasing, then \( a(f) \) is strictly increasing, and if \( f(i) \leq n \) for \( i < p \), then \( f(i) + i < n + p \). The two sets being equipotent, we get
\[
\text{Card}(\mathcal{A}(I_p, I_{n+p})) = \text{Card}(\mathcal{I}(I_p, I_{n+p})) = \binom{n+p}{n}.
\]
Consider now two finite totally ordered set $E$ and $F$. We pretend

$$\text{Card}(\mathcal{A}(E, F)) = \binom{n+p-1}{p} \text{ if Card}(E) = p \text{ and Card}(F) = n.$$ 

If $n = p = 0$, it is understood that $n + p - 1 = 0$, the binomial coefficient is one, and we have only one function, namely the empty function from $E$ into $F$. If $n = 0$ and $p > 0$ the binomial coefficient is zero, $F$ is empty, and there is no function $E \to F$. Consider now $n > 0$. There is a unique order isomorphism $f$ between between $E$ and $[0, p]$, and $g$ between $F$ and $[0, n - 1]$. Assume $h : E \to F$ increasing. Then $g \circ h \circ f^{-1} : [0, p] \to [0, n]$. We state a first result that says that the composition of two increasing functions is increasing, then a result that says that the composition of three functions is increasing if two of them (say $g$ and $f^{-1}$) are strictly increasing and the middle one (say $h$) is increasing. Now, if $k = g \circ h \circ f^{-1}$ we have $h = g^{-1} \circ k \circ f$, so that $h$ is increasing if and only if $k$ is increasing. This gives an isomorphism between $\mathcal{A}(E, F)$ and $\mathcal{A}([p], [n])$.

**Lemma increasing_compose:** forall $f\ g\ r\ r'\ r''$, 
increasing_fun $f$ $r$ $r'$ -> increasing_fun $g$ $r'$ $r''$ -> 
(composable $g$ $f$ & 
(forall $x$, inc $x$ (source $f$) -> W $x$ (compose $g$ $f$) = W (W $x$ $f$) $g$) & 
increasing_fun (compose $g$ $f$) $r$ $r''$).

**Lemma increasing_compose3:** forall $f\ g\ h\ r\ r'\ r''\ r'''$, 
strict_increasing_fun $f$ $r$ $r'$ -> increasing_fun $g$ $r'$ $r''$ -> 
strict_increasing_fun $h$ $r''$ $r'''$ -> 
let res:= compose (compose $h$ $g$) $f$ in 
(increasing_fun (corr_value res) (set_of_functions (source $f$) (target $h$)) $k$
(forall $x$, inc $x$ (source $f$) -> W $x$ res = W (W $x$ $f$) $g$) & 
increasing_fun res $r'''$).

**Lemma cardinal_set_of_increasing_functions4:** forall $n\ p\ r\ r'$, 
total_order $r$ -> total_order $r'$-> cardinal (substrate $r$) = nat_to_B $p$ -> 
cardinal (substrate $r'$) = nat_to_B $n$ -> 
cardinal (Zo (set_of_functions (substrate $r$) (substrate $r'$))) 
(fun $z$ => increasing_fun (inv_corr_value $z$) $r$ $r'$)) = 
nat_to_B(binom (n+p-1) $p$). (* 105*)

We compute now the number $a_n$ of pairs $(i, j)$ such that $1 \leq i \leq j \leq n$, and the number $b_n$ of pairs satisfying $1 \leq i < j \leq n$. This is the number of increasing (resp. strictly increasing) mappings of a set with two elements into the interval $[1, n]$, which has $n$ elements. Our previous results show

$$a_n = \frac{n(n+1)}{2} = \binom{n+1}{2}, \quad b_n = \frac{n(n-1)}{2} = \binom{n}{2}.$$ 

The Bourbaki proof of these relations (Proposition 14 [2, p. 181]) is different. He notices that $a_n = b_n + n$ since $i \leq j$ is equivalent to $i < j$ or $i = j$. A subset of $[1, n]$ is of cardinal two if and
only if it is a doubleton \( \{i, j\} \) with \( i \neq j \), and we may assume \( i < j \); hence \( b_n \) is the number of subsets of cardinal two of \([1, n]\). The link between \( a_n \) and \( b_n \) is given by the following trivial relation:

\[
\binom{n+1}{2} = \frac{n(n+1)}{2} = \binom{n}{2} + n.
\]

Lemma binom_2plus: forall n, binom (S n) 2 = Nquo(n *(S n)) 2.
Lemma binom_2plus0: forall n, binom (S n) 2 = (binom n 2) +n.

Lemma cardinal_pairs_lt: forall n, \( \text{cardinal}(\mathbb{Z}_0 (\text{product} \mathbb{B}_{\text{nat}} \mathbb{B}_{\text{nat}})(\text{fun } z \text{=> cardinal}_{\leq} \text{card}_1 \text{(P z) \& cardinal}_{\leq} \text{(P z)} \text{(Q z) \& cardinal}_{\leq} \text{(Q z)} \text{(nat}_2 \text{B n)})) = \text{nat}_2 \text{B (binom (S n) 2)} \). (* 56 *)
Lemma cardinal_pairs_le: forall n, \( \text{cardinal}(\mathbb{Z}_0 (\text{product} \mathbb{B}_{\text{nat}} \mathbb{B}_{\text{nat}})(\text{fun } z \text{=> cardinal}_{\leq} \text{card}_1 \text{(P z) \& cardinal}_{\leq} \text{(P z)} \text{(Q z) \& cardinal}_{\leq} \text{(Q z)} \text{(nat}_2 \text{B n)})) = \text{nat}_2 \text{B (binom (S n) 2)} \). (* 38 *)

A corollary is the following formula

\[
\sum_{i=1}^{n} i = \frac{n(n+1)}{2} = \binom{n+1}{2}.
\]

We shall give different variants. Denote this by \( s_n \). We have consider \( s_{n-1} = \Sigma_{n}^I (I) \) where \( I \) is the identity function; remember that \( \Sigma_{n}^I \) is the sum for \( 0 \leq i < n \); adding \( i = 0 \) does not change the sum. The proof by induction fits on a line. We consider then \( \Sigma_{n}^I \) which is the sum in reverse order. This is \( \Sigma_{n}^I (n - i - 1) \). Thus \( 2s_{n-1} = \Sigma_{n}^I (n - 1) = n(n-1) \). The proof needs 8 lines. Finally, we shall give the proof of Bourbaki: we have \( s_n = a_n \), where \( a_n \) is the cardinal of the set \( E \) of all pairs \((i, j)\) with \( 1 \leq i \leq j \leq n \), since \( E \) is the union of the sets \([1, j] \times \{j\}\), i.e., the disjoint union of the intervals \([1, j]\), which are of cardinal \( j \).

Lemma fct_sum_const1: forall f n m, (forall i, i<n -> f i = m) -> fct_sum f n = n *m.
Lemma sum_of_i: forall n, fct_sum (fun i=> i) n = binom n 2.
Lemma sum_of_i2: forall n, \( \text{cardinal}_{\sum} \text{(L (interval} \mathbb{B}_{\text{nat}} \text{card}_1 \text{(nat}_2 \text{B n)} \text{(fun } i \text{=>i)})) = \text{nat}_2 \text{B (binom (S n) 2)} \). (* 26 *)

6.8.7 Number of monomials

Consider a set \( E \), a law of composition of \( E \), and elements \( x, y, z \), etc, of \( E \). Consider a combination of these variables, where \( x \) appears 3 times, \( z \) appears twice and \( y \) appears once. If the law is associative and commutative, the combination is equal to \( x \cdot (x \cdot (x \cdot (y \cdot (z \cdot z))) \)). This is called a monomial, and denoted by \( x^3 y z^2 \). The total number of terms (here six) is called the degree. Assume that we have a second law of composition \( a + b \), and that the usual rules apply. This means that \( (a + b)^n \) can be expanded as sum monomials: \( (a + b)^n = \sum \gamma_{ij} a^i b^j \). It happens that \( \gamma_{ij} = \binom{n}{i+j} \) if \( i + j = n \) (this is the explanation of the term “binomial coefficient”). More generally, \( \sum x_i^n = \sum x_i^n \Gamma_i x^i \), where \( I \) is a mapping \( i \rightarrow n_i \), \( x^i \) denotes the monomial \( x_1^{n_1} x_2^{n_2} \cdots x_p^{n_p} \). The total degree of the monomial is \( \sum n_i = n \). Taking \( a = b = 1 \),

RR n° 7150
José Grimm

\[
gives \sum p \binom{n}{p} = 2^n. \text{ Taking } a = -1 \text{ and } b = 1 \text{ gives } \sum (-1)^p \binom{n}{p} = 0 \text{ (The first result has already been proved, the second is the object of Exercise 5.2). We have also } \sum_{i \in \mathbb{S}_n} \Gamma_i = p^n \text{ (it can be shown, by induction of the number of variables, that } \Gamma_i \text{ is the number of coverings of a set with } n \text{ elements by subsets with } n_i \text{ elements). The cardinal of the set } S_n \text{ is the object of the next theorem. We compute it by induction on both } n \text{ and } p. \]

Let } E \text{ be a set with } h \text{ elements, } \bar{A}_n \text{ and } \bar{B}_n \text{ be the sets of functions } u \text{ with } \sum_{i \in E} u(i) \leq n \text{ and } \sum_{i \in E} u(i) = n \text{ respectively. Let } A_{nh} \text{ and } B_{nh} \text{ the cardinals of these sets. Proposition 15 [2, p. 182]) says}

\[
A_{nh} = \binom{n + h}{h} \quad B_{nh} = \binom{n + h - 1}{h - 1}.
\]

We have } A_{nh} = B_{nh} + A_{n-1,h} \text{ since } \bar{A}_n \text{ is the disjoint union of } \bar{B}_n \text{ and } \bar{A}_{n-1} \text{ (one difficulty of the proof is that Bourbaki has not yet defined the set of integers; as a consequence, he adds the condition that the target of } u \text{ is the interval } [0, n], \text{ hence } \bar{A}_{n-1} \text{ is not a subset of } \bar{A}_n; \text{ it is nevertheless isomorphic to the complement of } \bar{B}_n \text{ in } \bar{A}_n). \text{ If } x \notin E, \text{ every function } u \text{ such that } \sum u(i) \leq n \text{ can be uniquely extended to } E \cup \{x\} \text{ in such a way as } \sum_{i \in E \cup \{x\}} u(i) = n. \text{ This gives } B_{n,h+1} = A_{nh}. \text{ The formulas follows by induction (they are trivial for } h = 0 \text{ and } n = 0). \]

Definition set_of_functions_sum_le E n:=
Zo (set_of_functions E (interval_Bnat card_zero n))
(fun z=> cardinal_le(cardinal_sum (P z)) n).

Definition set_of_functions_sum_eq E n:=
Zo (set_of_functions E (interval_Bnat card_zero n))
(fun z=> (cardinal_sum (P z)) = n).

Lemma set_of_functions_sum0: forall f,
(forall a b, inc (f a b) Bnat) ->
(forall a, f 0 a = card_one) ->
(forall a , f a 0 = card_one) ->
(forall a b, f (S a) (S b) = card_plus (f (S a) b) (f a (S b))) ->
forall a b, f a b = nat_to_B(binom (a+b) a).

Lemma set_of_functions_sum1: forall E x n,
inc n Bnat -> is_finite_set E -> ~ (inc x E) ->
equipotent (set_of_functions_sum_le E n)
(set_of_functions_sum_eq (tack_on E x) n). (* 102 * )

Lemma set_of_functions_sum2: forall E n,
inc n Bnat -> is_finite_set E ->
equipotent (complement (set_of_functions_sum_le E (succ n))
(set_of_functions_sum_eq E (succ n)))
(set_of_functions_sum_le E n). (* 106 * )

Lemma set_of_functions_sum3: forall E,
cardinal (set_of_functions_sum_le E card_zero) = card_one. (* 32 * )

Lemma set_of_functions_sum4: forall n, is_cardinal n->
cardinal (set_of_functions_sum_le emptyset n) = card_one.

Lemma set_of_functions_sum_pr: forall n h,
le intv:= fun h => (interval_co_0a (nat_to_B h)) in
let slu:= fun n h => set_of_functions_sum_le (intv h) (nat_to_B n) in
let seq := fun n h => set_of_functions_sum_eq (intv h) (nat_to_B n) in
let a:= fun n h => cardinal (slu n h) in
let b:= fun n h => cardinal (seq n h) in
(A n h = B n (S h) & A n h = nat_to_B(binom (n+h) n)). (* 118 *)
We give now a variant of the theorem\footnote{Suggested by Jean-Baptiste Pomet}. We pretend that the number of functions \( y \) defined on \([0, p]\) with values in \([0, n] \) and such that \( \sum y_i \leq n \) is \( \Lambda_{n, p+1} = \binom{n+p+1}{p+1} \). This is the previous result for \( h = p + 1 \) (if \( h = 0 \), there is a unique function defined on a set with \( h \) elements, the empty function, and the sum is zero). The quantity \( \Lambda_{n, p+1} \) is the number of subsets of \([0, n + p]\) with \( p + 1 \) elements. Consider the sequence \( x_i \), defined by induction (see next chapter) via \( x_0 = y_0 \) and \( x_{i+1} = y_{i+1} + x_i + 1 \). All we have to do is prove that the mapping \( y \mapsto \{x_0, x_1, \ldots, x_p\} \) is bijective (as a function with values in the subset of \( \mathcal{P}([0, n+p]) \) formed of sets with \( p+1 \) elements). The idea is that the function \( y \) is strictly increasing, and uniquely defined by its range. Since \( \Lambda_{n, p+1} \) is the number of strictly increasing functions \([0, p] \to [0, n + p]\); all we have to do is to prove that the mapping \( y \mapsto x \) is a bijection (as a function into \( \mathcal{P}([0, p], [0, n+p]) \)).

The inverse mapping of \( y \mapsto x \) is defined by \( y_{i+1} = x_{i+1} - (x_i + 1) \). It is easier to consider \( y_{i+1} = z_{i+1} - z_i \), where \( z_i = x_i - i \). It happens that \( z_i \) is the sum of the restriction of \( y \) to the interval \([0, i] \) (there is no need to define it by induction) and is obviously increasing. Since \( \Lambda_{n, p+1} \) is the cardinal of \( \mathcal{A}([0, p], [0, n]) \), the set of increasing functions \([0, p] \to [0, n] \), all we have to do is show that \( y \mapsto z \) is a bijection \( C_{pn} \to C'_{pn} \) where \( C_{pn} \) is the set of functions \( y : [0, p] \to [0, n] \) such that \( \sum y_i \leq n \) and \( C'_{pn} = \mathcal{A}([0, p], [0, n]) \). We first show that \( \Lambda_{n, p+1} \) is the cardinal of \( C'_{pn} \).

Definition set_of_functions_sum_le_int p n :=
    set_of_functions_sum_le (interval_Bnat card_zero p) n.

Definition set_of_increasing_functions_int p n :=
    (Zo (set_of_functions (interval_Bnat card_zero p) (interval_Bnat card_zero n))
     (fun z => increasing_fun (inv_corr_value z)
      (interval_Bnato card_zero p)
      (interval_Bnato card_zero n))).

Lemma card_set_of_increasing_functions_int : forall p n,
    cardinal (set_of_increasing_functions_int (nat_to_B p)(nat_to_B n)) =
    nat_to_B(binom (n+p+1) (p+1)).

If \( R(f, i) \) denoted the restriction of the function \( f \) to the interval \([0, i] \) we have \( R(R(f, i), j) = R(f, j) \) if \( j \leq i \). If \( S(f, i) \) is the sum of the restriction of \( R(f, i) \) we have \( S(f, 0) = f(0) \) and \( S(f, i+1) = f(i+1) + S(f, i) \).

Lemma double_restrc: forall f n p, fgraph f -> inc p Bnat ->
    cardinal_lt n p ->
    domain f = interval_Bnat card_zero p ->
    restr (restr f (interval_Bnat card_zero (succ n)))
     (interval_Bnat card_zero n) =
    restr f (interval_Bnat card_zero n).

Lemma induction_on_sum3: forall f m,
    is_function f -> inc m Bnat ->
    source f = interval_Bnat card_zero m ->
    (forall a, inc a (source f) -> is_cardinal (W a f)) ->
    (cardinal_sum (restr (graph f) (interval_Bnat card_zero card_zero))
     = (W card_zero f)
    & (forall n, cardinal_le n m ->
     card_plus (cardinal_sum (restr (graph f) (interval_co_0a n))) (W n f)
     = cardinal_sum (restr (graph f) (interval_co_0a (succ n)))).
Given a function $y$, we consider $z$ such that $z_i = S(y, i)$. We first show that $z$ maps $[0, p]$ into $[0, n]$, and then that $z \in C'_{p,n}$ if $y \in C_{p,n}$ (more that $i \rightarrow S(y, i)$ is increasing). We then show that $y \rightarrow z$ is injective and surjective. The key relation is $z_0 = y_0$ and $z_{i+1} = y_{i+1} + z_i$ (trivial consequence of induction_on_sum3); it says that $y$ is uniquely defined from $z$. Moreover, given an increasing function $z'$, if $y_0 = z'_0$ and $y_{i+1} = z'_{i+1} - z'_i$, the same formula is satisfied by $z'$, hence $z = z'$, thus proving surjectivity.

\begin{verbatim}
Definition sum_to_increasing_fun y :=
  fun i => cardinal_sum (restr (graph y) (interval_Bnat card_zero i)).

Definition sum_to_increasing_fct y n p :=
  BL (sum_to_increasing_fun (inv_corr_value y))
  (interval_Bnat card_zero p) (interval_Bnat card_zero n).

Lemma sum_to_increasing1: forall y n p,
  inc n Bnat -> inc p Bnat ->
  inc y (set_of_functions_sum_le_int p n) ->
  transf_axioms (sum_to_increasing_fun (inv_corr_value y))
  (interval_Bnat card_zero p) (interval_Bnat card_zero n).

Lemma sum_to_increasing2: forall n p,
  inc n Bnat -> inc p Bnat ->
  transf_axioms (fun y=> corr_value (sum_to_increasing_fct y n p))
  (set_of_functions_sum_le_int p n) (set_of_increasing_functions_int p n). (* 50 *)

Lemma sum_to_increasing4: forall n p,
  inc n Bnat -> inc p Bnat ->
  injective (BL (fun y=> corr_value (sum_to_increasing_fct y n p))
  (set_of_functions_sum_le_int p n) (set_of_increasing_functions_int p n)). (* 46 *)

Lemma sum_to_increasing5: forall n p,
  inc n Bnat -> inc p Bnat ->
  surjective (BL (fun y=> corr_value (sum_to_increasing_fct y n p))
  (set_of_functions_sum_le_int p n) (set_of_increasing_functions_int p n)). (* 79 *)

Lemma sum_to_increasing6: forall n p,
  cardinal (set_of_functions_sum_le_int (nat_to_B p) (nat_to_B n)) =
  nat_to_B(binom (n+p+1) (p+1)).
\end{verbatim}
Chapter 7

Infinite sets

7.1 The set of natural integers

Bourbaki defines an infinite set as a set that is not finite. If such a set exists and \( a \) is its cardinal, then all integers \( n \) satisfy \( n < a \), since otherwise we would have \( a \leq n \), which implies \( a \) finite. This means that the set \( N \) of cardinals \( n \) such that \( n \) is finite contains all integers. By extensionality, it does not depend on \( a \). Bourbaki has an axiom that asserts the existence of an infinite set, and deduces (Theorem 1, [2, p. 184]) that the set \( N \) of integers exists. Its cardinal is denoted by \( \aleph_0 \).

We have shown that \( nat \) is infinite because \( S \) is injective and not surjective. We have shown that \( N \) and \( \mathbb{N} \) are isomorphic. In fact, we have defined a function \( \mathfrak{N} \) from the type \( nat \) to the set \( N \) that is compatible with successor, addition, multiplication and order. We have shown that it is injective and surjective. This means that \( \mathbb{N} \) and \( N \) are equipotent, so that \( N \) is infinite. We have already shown this fact, using the same argument as Bourbaki: assume \( N \) finite, with cardinal \( n \); then the interval \([0, n]\) is a subset of \( N \) hence \( s(n) \leq n \), where \( s(n) \) is the cardinal of the interval. But we know that \( s(n) = n + 1 \) and \( n < s(n) \).

\[
\text{Lemma equipotent\_nat\_Bnat: equipotent Bnat nat.}
\]
\[
\text{Lemma infinite\_Bnat: is\_infinite\_c (cardinal Bnat).}
\]

Bourbaki defines a sequence as a family whose index set \( I \) is a subset of \( N \). It is called an infinite sequence if \( I \) is infinite. Remember that a finite sequence is a family where \( I \) is finite and contains only integers; this means that \( I \) is a finite subset of \( N \).

Let’s quote Bourbaki [2, p. 184] “Let \( P \mid n \) be a relation and let \( I \) denote the set of integers \( n \) such that \( P \mid n \) is true. \( I \) is then a subset of \( N \). A sequence \((x_n)_{n \in I}\) is then sometimes written \((x_n)_{P \mid n}\), and \( x_n \) is called then \( n \text{th term} \) in the sequence.” Example. Assume that \( P \mid n \) is the relation \( n \in \mathbb{Z} \) where \( \mathbb{Z} \) denotes the set of rational integers as a subset of \( N \). According to the quote, \((x_n)_{n \in N}\) and \((x_n)_{n \in \mathbb{Z}}\) are the same sequences. This may be confusing since they are obviously different families. In section 6.4 Bourbaki assumes that \( P \mid n \) implies that \( n \) is an integer; this is missing here. Other example: we consider the property “\( n \) even and \( n < 10 \). This is a finite sequence and the 4th term is 6; in the French version, we can read “\( x_4 \) est le terme d’indice 4” and “\( x_6 \) est le 4ème terme”. In English this is translated as “\( x_4 \) is the 4th term” and “\( x_6 \) is the 4th term”. This may be confusing.
According to Bourbaki, if the property is \( n \geq k \), the sequence is written as \((x_n)_{n \geq k}\) or even \((x_n)\) if \( k = 0 \) or \( k = 1 \). This last notation is obviously ambiguous. The sum of such a family may be denoted a \( \sum_{n=k}^{\infty} x_n \).

Two sequences \((x_n)_{n \in \mathbb{N}}\) and \((y_n)_{n \in \mathbb{N}}\) with the same index set are said to differ only in the order of their terms if there exists a permutation \( f \) of the index set \( I \) such that \( x_{f(n)} = y_n \) for all \( n \in I \). This makes sense even if \( I \) is not a subset of the integers. By commutativity, two sequences that differ only in the order of their terms have same sum and product.

A multiple sequence is a family whose index set is a subset of a product \( \mathbb{N}^p \) \( (p \) is a integer). Let \( f \) be a bijection of \( \mathbb{N} \) onto a set \( I \). For each family \((x_i)_{i \in I}\), the sequence \( n \mapsto X_{f(n)} \) is said to be obtained by arranging the family \((x_i)_{i \in I}\) in the order defined by \( f \).

### 7.2 Definition of mappings by induction

If we instantiate Criterion C60 (see page 13) to the well-ordered set \( \mathbb{N} \) we get another criterion\(^1\) it assert that, for any term \( T \), there exists a unique surjective function \( f \) such that

\[
\forall n, n \in \mathbb{N} \implies f(n) = T| f(n) |
\]

where \( u^{(x)} \) denotes the restriction of \( u \) to the segment \( ]-\), \( x[\). Recall that \( ]-\), \( x[\) is the set of all elements \( y \) such that \( y < x \); this is just the interval \([0, x[\).

In Bourbaki, the operator \( T| u | \) is defined for any set \( u \). In the proof, it is used only when \( u \) is of the form \( u_n = f^{(n)} \), this is the restriction of some unknown function to a segment of our well-ordered set. If we denote by \( M(u) \) the cardinal of the source of \( u \), then \( M(u_n) = n \), and \( M(u_{n+1}) - 1 = n \). By definition of \( u_n \), we have \( u_{n+1}(y) = f(y) \) for \( y \leq n \), thus \( f(n) = u_{n+1}(n) = u_{n+1}(M(u_{n+1}) - 1) \). Write this as \( f(n) = R| u_{n+1} | \).

In the case of general transfinite induction on a set \( E \), we have to change the definition of \( M \), since cardinals are unlikely to be elements of \( E \); we let \( M'(u) \) be the greatest element of the source of \( u \). If we denote by \( n + 1 \) the successor of \( n \) \( (this is the least element of the complementary of \( ]-\), \( n[\), it exists unless \( n \) is the greatest element of \( E \)), then the source of \( u_{n+1} \) is \( ]-\), \( n+1[\), and has \( n \) as greatest element; thus \( M'(u_{n+1}) = n \) and we still have \( f(n) = R| u_{n+1} | \) for some \( R \).

If our term \( T \) satisfies \( T| u | = s( R| u |) \) whenever \( u \) is of the form \( u_{n+1} \), then \( f(n+1) = s(f(n)) \) for all \( n \). The function \( f \) is well-defined if we specify the values \( f(m) \) when \( m \) is not a successor. In the case of general induction, there can be many such values. In the case of integers, there is only one, and it suffices to specify the value \( f(0) \).

Consider the following definitions

\[
\begin{align*}
M & \colon= \text{fun } u \mapsto \text{cardinal (source } u) \\
T & \colon= \text{fun } u \mapsto Yo (M u = \text{card_zero} a \ (s (\prec (M u) u))) \\
T' & \colon= \text{fun } u \mapsto Yo (M u = \text{card_zero} a \ (h (\prec (M u)) (W (\prec (M u) u))) )
\end{align*}
\]

Remember that \( Yo a b c \) evaluates to \( b \) if \( a \) is true and to \( c \) otherwise. The previous discussion shows that for all \( a \) and \( s \), there exists a unique surjective function \( f \) defined on \( \mathbb{N} \) such that

\[
\text{(IND)} \quad f(0) = a \quad \text{and} \quad f(n+1) = s(f(n)).
\]

\(^1\)This section has been completely rewritten in Version 2
It is easy to show by induction on \( n \), that if \( E \) is any set, \( a \in E \) and \( s(E) \subset E \), then \( f(n) \in E \) for all \( n \).

If we use \( T' \) instead of \( T \), we see that there exists a unique surjective function \( f \) defined on \( N \) such that

\[
\text{IND0} \quad f(0) = a \quad \text{and} \quad f(n + 1) = h(n, f(n)).
\]

As previously, if \( a \in E \) and if \( h(n, x) \in E \) whenever \( n \in N \) and \( x \in E \), then \( f(n) \in E \) for all \( n \). It is trivial to deduce (IND) from (IND0) (consider the function \( h(n, x) = s(x) \)).

Bourbaki first shows (IND), then deduces a variant of (IND0) as follows. He considers a function \( h : N \times E \rightarrow E \), where \( E \) is some fixed set. Denote by \( F \) the set \( \{ h(a) : a \in N \} \). Define \( a_n = \text{pr}_1(g(n)) \) and \( b_n = \text{pr}_2(g(n)) \). From \( g(n) \in F \), one deduces \( a_n \in N \), \( b_n \in E \) and \( g(n) = (a_n, b_n) \), hence the two recurrence relations \( a_{n+1} = a_n + 1 \) and \( b_{n+1} = h(a_n, b_n) \). Obviously \( a_n = n \), thus \( b_{n+1} = h(n, b_n) \), and the function associated to \( b_n \) satisfies (IND0).

Consider the following example. Given a sequence of cardinals \((x_i)\), we consider \( h(n, y) = x_{n+1} + y \) or \( h(n, y) = x_{n+1}^y \). Using (IND0), there exists two sequences satisfying \( y_0 = x_0 \) and \( y_{n+1} = x_{n+1} + y_n \) or \( z_0 = x_0 \) and \( z_{n+1} = x_{n+1}^z \). Let's try to apply the Bourbaki method. There is a set \( E \) stable by cardinal sum that contains the range \( E_0 \) of the sequence \((x_i)\). If \( E_0 \) is a subset of \( N \), just take \( N \), otherwise let \( \alpha \) be the supremum of \( E_0 \) (see page 72). This is an infinite cardinal, and we shall see in the next section that the set of all cardinals \( \leq \alpha \) is stable by cardinal sum. As a consequence, we can use the Bourbaki construction and \( y_\alpha \in E \). Doing the same for \( z_\alpha \) is tricky. For any set \( E \) we define \( p(E) \) to be the set of all \( x^y \) for \( x \in E \) and \( y \in E \), and for any cardinal \( \alpha \), we define \( E_\alpha \) to be the set of all cardinals \( \leq \alpha \) and \( s(\alpha) \) to be the supremum of \( p(E_\alpha) \). Let \( f \) be the function defined by induction via \( s \) (where \( f(0) \) is any cardinal such that \( E_{f(0)} \) contains the range of the sequence \((x_i)\)). Finally, let \( E \) be the union of the sets \( E_{f(i)} \). Since \( f \) is increasing, if \( x \) and \( y \) are two elements of \( E \), there is an \( i \) such that \( x \in E_{f(i)} \) and \( y \in E_{f(i)} \) hence \( x^y \in E_{f(i+1)} \). This is a very large set (we could reduce a bit its size by defining \( p(E) \) to be the set of all \( x^y \) for \( x \in E_0 \) and \( y \in E \)).

In the first version of the Software we had

\[
\begin{align*}
M & := \text{fun } u \Rightarrow \text{supremum } \text{Nat_order} \text{ (source } u) \\
T & := \text{fun } u \Rightarrow \text{Yo } (u = \text{empty_function} \ a \ (s \ (\text{w } (M \ u) \ u)))
\end{align*}
\]

We recognise here the quantity \( M' \); it is defined whenever \( u \) has nonempty source, which is equivalent to say that \( u \) is not the empty function.

The Bourbaki definition is much more complicated. He starts with

\[
D(u) = \{ x \in N \text{ and } (\exists y)((x, y) \in \text{pr}_1(\text{pr}_1(u))) \}.
\]

He says that, if \( u \) is a function defined on a subset of \( N \), then \( D(u) \) is the domain. In fact, \( D(u) \) is by definition the intersection of the domain of the graph of \( u \) and \( N \). If \( u \) is a function, \( D(u) \) is the intersection of its source and \( N \). As mentioned above, in the proof we need only to the consider the case where the source is a subset of \( N \), and \( D(u) \) could be replaced by the source of \( u \). Bourbaki defines \( M(u) \) as being the least upper bound of \( D(u) \), and in a footnote says that one could change the definition of the least upper bound, in order to give a meaning to this term even when \( D(u) \) is unbounded. Another idea would be to consider \( \text{Card}(D(u)) - 1 \); a possible definition of \( x - 1 \) could be \( x \) when \( x = 0 \) or is an infinite cardinal, the usual definition otherwise. Let \( \phi \) be the empty function, and consider the relation

\[
\forall y, u : (u = \phi \text{ and } y = a) \text{ or } (u \neq \phi \text{ and } y = \text{S} \text{ u}(M(u)))
\].
Let $T \lambda u$ be the term $\tau_y (R \lambda y, u \lambda u)$. If $u = \emptyset$ then $T \lambda u$ is $a$, otherwise it is $S \lambda (M(u))$. Our equivalent of the if-then-else construct is $Y a$. The argument $u$ of the term $T$ will always be (this is obvious by induction) the restriction of $f$ to the interval $[0, n - 1]$. If $n = 0$, the restriction is $\emptyset$ hence $f(0) = a$, and if $n = m + 1$, the restriction has source $[0, m]$, whose supremum is $m$, so that $f(m + 1) = S f(m)$.

We start with two useful lemmas. The first says that $\vdash x \in [0, x]$. The second says that two surjective functions with the same source and taking the same values are equal.

Lemma segment_Bnat_order: forall x, inc x Bnat ->
  segment Bnat_order x = interval_co Bnat_order card_zero x.

Lemma funct_extensionality1: forall f g, source f = source g ->
  surjective f -> surjective g ->
  (forall x, inc x (source f) -> W x f = W x g) -> f = g.

We give here six definitions. In the the first cases, the function $f$ is assumed to be surjective, and in the other cases, the target will be a given set $E$. The function will satisfy one of (IND) or (IND0) or

(IND1') $f(0) = a$ and $f(n + 1) = g(n, f(n))$ if $n < m$.

We call this partial induction. In order to get uniqueness, we either have to restrict the source of $f$ to the interval $[0, m]$ or specify a value $f(n)$ for $n > m$. We consider

(IND1) $f(0) = a$ and $f(n + 1) = g(n, f(n))$ if $n < m$ and $f(n) = a$ otherwise.

Definition induction_defined s a := choosef(fun f=>
  source f = Bnat & surjective f & W card_zero f = a &
  forall n, inc n Bnat -> W (succ n) f = s (W n f)).

Definition induction_defined0 h a := choosef(fun f=>
  source f = Bnat & surjective f & W card_zero f = a &
  forall n, inc n Bnat -> W (succ n) f = h n (W n f)).

Definition induction_defined1 h a p := choosef(fun f=>
  source f = Bnat & surjective f & W card_zero f = a &
  (forall n, cardinal_lt n p -> W (succ n) f = h n (W n f)) &
  (forall n, inc n Bnat -> ~ (cardinal_le n p) -> W n f = a)).

Definition induction_defined_set s a E := choosef(fun f=>
  is_function f &source f = Bnat & target f = E & W card_zero f = a &
  forall n, inc n Bnat -> W (succ n) f = s (W n f)).

Definition induction_defined0_set h a E := choosef(fun f=>
  is_function f & source f = Bnat & target f = E & W card_zero f = a &
  forall n, inc n Bnat -> W (succ n) f = h n (W n f)).

Definition induction_defined1_set h a p E := choosef(fun f=>
  is_function f & source f = Bnat & target f = E & W card_zero f = a &
  (forall n, cardinal_lt n p -> W (succ n) f = h n (W n f)) &
  (forall n, inc n Bnat -> ~ (cardinal_le n p) -> W n f = a)).

We state some theorems that say that such a function exists and is unique, and we use the axiom of choice in order to show that the chosen function satisfies the property.
Lemma integer_induction0: forall h a,
    exists_unique (fun f=> source f = Bnat & surjective f &
                      W card_zero f = a
                      & forall n, inc n Bnat -> W (succ n) f = h n (W n f)).

Lemma integer_induction: forall s a, exists_unique (fun f =
                      source f = Bnat & surjective f & W card_zero f = a &
                      forall n, inc n Bnat -> W (succ n) f = s (W n f)).

Lemma integer_induction1: forall h a p, inc p Bnat ->
    exists_unique (fun f =
                      source f = Bnat & surjective f &
                      W card_zero f = a &
                      (forall n, cardinal_lt n p -> W (succ n) f = h n (W n f)) &
                      (forall n, inc n Bnat -> ~ (cardinal_le n p) -> W n f = a)).

Lemma induction_defined_pr: forall s a,
    let f := induction_defined s a in
    source f = Bnat & surjective f & W card_zero f = a &
    forall n, inc n Bnat -> W (succ n) f = s (W n f).

Lemma induction_defined_pr0: forall h a,
    let f := induction_defined0 h a in
    source f = Bnat & surjective f & W card_zero f = a &
    forall n, inc n Bnat -> W (succ n) f = h n (W n f).

Lemma induction_defined_pr1: forall h a p,
    let f := induction_defined1 h a p in
    inc p Bnat ->
    ( source f = Bnat & surjective f &
      W card_zero f = a &
      (forall n, cardinal_lt n p -> W (succ n) f = h n (W n f)) &
      (forall n, inc n Bnat -> ~ (cardinal_le n p) -> W n f = a)).

We now show that the target of the function defined by induction is a subset of E under some conditions. It follows that there is a variant where the target is E. We shall not prove uniqueness, it is obvious.

Lemma integer_induction_stable: forall E g a,
    inc a E -> (forall x, inc x E -> inc (g x) E) ->
    sub (target (induction_defined g a)) E.

Lemma integer_induction_stable0: forall E h a,
    inc a E -> (forall n x, inc x E -> inc n Bnat -> inc (h n x) E) ->
    sub (target (induction_defined0 h a)) E.

Lemma integer_induction_stable1: forall E h a p,
    inc p Bnat ->
    inc a E -> (forall n x, inc x E -> cardinal_lt n p -> inc (h n x) E) ->
    sub (target (induction_defined1 h a p)) E.

Lemma induction_defined_pr_set: forall E g a,
    let f := induction_defined_set g a E in
    inc a E -> (forall x, inc x E -> inc (g x) E) ->
    (is_function f & source f = Bnat & target f = E & W card_zero f = a &
     forall n, inc n Bnat -> W (succ n) f = g (W n f)).

Lemma induction_defined_pr_set0: forall E h a,
    let f := induction_defined0_set h a E in
    inc a E -> (forall n x, inc x E -> inc n Bnat -> inc (h n x) E) ->
    (is_function f & source f = Bnat & target f = E & W card_zero f = a &
     forall n, inc n Bnat -> W (succ n) f = h n (W n f)).

Lemma induction_defined_pr_set1: forall E h a p,
    let f := induction_defined1_set h a p E in
inc p Bnat ->
inc a E -> (forall n x, inc x E -> cardinal_lt n p -> inc (h n x) E) ->
(is_function f & source f = Bnat & target f = E & W card_zero f = a &
(foreall n, cardinal_lt n p -> W (succ n) f = h n (W n f)) &
(foreall n, inc n Bnat -> ~ (cardinal_le n p) -> W n f = a)).

In Version 1 we had the following two definitions (compare with induction_defined0_set and induction_defined1_set). They are of the form choose IND0 and choose IND1’. We have two theorems saying that these objects satisfy (IND0) and (IND1’) respectively, and two others stating existence and uniqueness of (IND0), and existence of (IND1’).

(*
Definition induction_defined1 E h a:= choosef(fun f=>
is_function f & source f = Bnat & target f = E & W card_zero f = a &
forall n, inc n Bnat -> W (succ n) f = h n (W n f)).
Definition induction_defined2 E h a p:= choosef(fun f=>
is_function f & source f = Bnat & target f = E & W card_zero f = a &
forall n, cardinal_lt n p -> W (succ n) f = h n (W n f)).
*)

Together with these for theorems, we show a variant of integer_induction_stable and the Bourbaki variant of (IND0).

(*
Lemma integer_induction_stable: forall E g a,
icc a E -> is_function g -> source g = E -> target g = E ->
sub (target (induction_defined g a)) E.
Lemma induction_with_var: forall E h a,
is_function h -> source h = product Bnat E -> target h = E -> inc a E ->
extists_unique (fun f=> is_function f & source f = Bnat & target f= E &
W card_zero f a &
forall n, inc n Bnat -> W (succ n) f = h n (W n f)).
Lemma induction_with_var1: forall E h a,
(foreall n x, inc n Bnat -> inc x E -> inc (h n x) E) -> inc a E ->
extists_unique (fun f=> is_function f & source f = Bnat & target f= E &
W card_zero f = a &
forall n, inc n Bnat -> W (succ n) f = h n (W n f)).
Lemma induction_with_var2: forall E h a p,
(foreall n x, inc n Bnat -> inc x E -> cardinalLt n p -> inc (h n x) E)
-> inc a E -> inc p Bnat ->
extists f, is_function f & source f = Bnat & target f= E &
W card_zero f = a &
forall n, cardinalLt n p -> W (succ n) f = h n (W n f).
Lemma induction_defined_pr2: forall E h a p,
(foreall n x, inc n Bnat -> inc x E -> cardinalLt n p -> inc (h n x) E)
-> inc a E -> inc p Bnat ->
let f := induction_defined2 E h a p in is_function f &
sourse f = Bnat & target f = E & W card_zero f = a &
forall n, cardinalLt n p -> W (succ n) f = h n (W n f).
Lemma induction_defined_pr1: forall E h a,
(foreall n x, inc n Bnat -> inc x E -> inc (h n x) E)
7.3 Properties of infinite cardinals

Bourbaki claims (Lemma 1, [2, p. 186]) that every infinite set $E$ has a subset $F$ equinumerous to $\mathbb{N}$; the argument being that there exists a well-ordering on $E$. If $E$ is isomorphic to a segment of $\mathbb{N}$, then $E$ is equinumerous to $\mathbb{N}$ since all other segments are of the form $[0, x[i$, hence $[0, x[i$, thus are finite. Otherwise, $\mathbb{N}$ is isomorphic to segment of $E$, hence equinumerous to a subset of $E$.

Lemma equipotent_range: forall $f$, injective $f$ ->
equipotent (source $f$) (range (graph $f$)).
Lemma morphism_range: forall $f$ a b,
order_morphism f a b -> equipotent (substrate a) (range (graph $f$)).
Lemma morphism_range1: forall $f$ a b,
order_morphism f a b -> cardinal (substrate a) = cardinal (range (graph $f$)).
Lemma infinite_greater_countable: forall E,
infinite_set E -> exists F, sub F E & cardinal F = cardinal $\mathbb{N}$.
Bourbaki claims that $\mathbb{N} \times \mathbb{N}$ is equinumerous to $\mathbb{N}$: the relation Card($\mathbb{N}$) ≤ Card($\mathbb{N} \times \mathbb{N}$) is a consequence of $\{0\} \times \mathbb{N} \subset \mathbb{N} \times \mathbb{N}$; moreover there is an injection from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{N}$. He uses expansion to base 2. Assume $x = \sum x[i 2^i$ and $y = \sum y[i 2^i$, then $\sum (2x[i + y[i]4^i$ is an injective function of $x$ and $y$. We use here a different function: consider

$$f(n, m) = n + \binom{n + m + 1}{2} = n + g(n + m).$$

The function $g$ is the binomial coefficient with indices $a + 1$ and 2, it is also $g(a) = a(a + 1)/2$; it satisfies $g(a + 1) = g(a) + a + 1$, hence $g(n + m) \leq f(n, m) < g(n + m + 1)$. This relation shows that $n + m$ is uniquely defined by $f(n, m)$, from which injectivity follows. Consider $x$ and the least $a$ such that $x < g(a)$. Then $x = f(n, m)$, where $n$ and $m$ are the unique integers satisfying $n + m + 1 = a$ and $x = n + g(a - 1)$. This shows that $f$ is bijective.

Lemma equipotent_N2_N: equipotent (product $\mathbb{N} \times \mathbb{N}$) $\mathbb{N}$. (* 41 *)

We show here Theorem 2 ([2, p. 186]): for every infinite cardinal $a$, we have $a = a^2$. The proof is by induction (in reality, Zorn's lemma, since there is no induction for infinite cardinals).

We consider an infinite set $E$, and study bijections of the form $\psi: A \to A \times A$, where $A \subset E$. This is the same as studying the set $\mathfrak{M}$ of functions defined on a subset $A$ of $E$ that are injective, whose target is $E \times E$, and whose range is $A \times A$. Bourbaki says "It is immediately seen that $\mathfrak{M}$ is inductive". (The example in section 3.4 is the set of functions without these conditions). The proof is similar to the one that states that there exists an isomorphism between well-ordered sets. The proof is tedious but straightforward.

Since $E$ is infinite there exists a subset $D$ equinumerous to $\mathbb{N}$, hence (previous theorem) a bijection between $D$ and $D \times D$. This gives us an element $\psi_0$ of $\mathfrak{M}$. Let $\mathfrak{M}_0$ be the set of elements
of \( \mathfrak{M} \) that extend \( \psi_0 \). This set is inductive as well. We consider a maximal element with source \( F \) and cardinal \( b \). We have \( \text{Card}(F) \geq \text{Card}(D) \), so that \( b \) is infinite. We have \( b = b^2 \). If \( c \leq b \) then \( b \leq c + b \leq 2b \leq b^2 = b \), hence \( c + b = b \). In particular \( b = 2b = 3b \).

Our theorem is true if \( b = \text{Card}(E) \). Assume otherwise \( b < a \). The cardinal \( c \) of the complementary of \( F \) in \( E \) is \( \geq b \) (a consequence of the theorem will be \( c = a \)). Hence, there exists a subset \( Y \) of \( E \) disjoint from \( F \) with cardinal \( b \). Let \( Z = Y \cup F \). The relation \( b = 3b^2 \) implies that \( Y \) is equipotent to \( (Z \times Z) - (F \times F) \) hence \( Z \) is equipotent to \( Z \times Z \). This contradicts maximality.

Definition \( \text{set}\_\text{for}\_\text{equipotent}\_\text{inf2}\_\text{inf} \ E \psi := \)
\[
\text{Zo (set_of_sub_functions} E (\text{product} E E)) (\text{fun} z = > \text{injective} (\text{inv_corr_value} z) ~ & \text{range} (P z) = \text{product} (P (Q z)) (P (Q z)) ~ & \text{sub} (P psi) (P z)).
\]

Lemma \( \text{inductive}\_\text{set}\_\text{for}\_\text{equipotent}\_\text{inf2}\_\text{inf} : \forall E \psi, \)
\[
\text{inc psi (set_for_equipotent_inf2_inf E psi)} -> \text{inductive_set} (\text{induced_order} (\text{opposite_order} (\text{extension_order} E (\text{product} E E)))) (\text{set_for_equipotent_inf2_inf E psi}) \].  (* 106 *)

Theorem \( \text{equipotent}\_\text{inf2}\_\text{inf} : \forall a, \text{is_infinite_c} a -> \text{card_pow} a (\text{card_two}) = a. \)  (* 187 *)

By induction, \( a^n = a \) if \( a \) is an infinite cardinal and \( n \geq 1 \) is an integer. As a consequence, if \( (a_i)_{i \in I} \) is a finite family of non-zero cardinals, if the largest one is an infinite cardinal \( a \), then the product is \( a \). If \( a_i \leq a \) then \( \sum a_i \leq a \) and we have equality if one of the cardinals is \( a \). The cardinals can be zero, and the index set can be infinite, provided that \( \text{Card}(I) \leq a \). Finally, if \( a \) and \( b \) are two non-zero cardinals, one of them being infinite, then the sum and the product is the greatest of them.

Note. Bourbaki writes “sup\((a, b)\)” instead of “the greatest of them”; our function \( \text{sup} \) takes three arguments, one of them being the order; in this case, there is no order (because there is no set containing all cardinals). We know that the supremum of any family of cardinals exists, so that the supremum of two cardinals is well-defined, but we have no notation for this operation. Note also that using a lemma of the form: if \( a \) is infinite or \( b \) is infinite, then \( a + b = \text{sup}(a, b) \) is uneasy, since this means that \( a + b \) is at least \( a \), at least \( b \), and at most any \( c \) that is at least \( a \) and at least \( b \). It is much easier to say: if \( a \) is infinite and \( b \leq a \) then \( a + b = a \), and use commutativity of addition when needed. Note that \( b \) infinite implies \( a \) infinite, and \( b \) can be zero (since \( a \) is infinite, it is clearly non-zero). In the case of a product, we need the condition \( b \neq 0 \).

Lemma \( \text{power_of_infinite} : \forall a n, \text{is_infinite_c} a -> \text{inc} n \text{ Bnat} -> \)
\[
n \neq \text{card_zero} -> \text{card_pow} a n = a.
\]

Lemma \( \text{finite_family_product} : \forall a f, \text{fgraph} f -> \)
\[
\text{is_finite_set} (\text{domain} f) -> \text{is_infinite_c} a -> \)
\[
(\forall i, \text{inc} i (\text{domain} f) -> \text{cardinal_le} (V i f) a) -> \)
\[
(\forall i, \text{inc} i (\text{domain} f) -> V i f <> \text{card_zero}) -> \)
\[
(\exists j, \text{inc} j (\text{domain} f) & (V j f) = a) -> \)
\[
\text{cardinal_prod} f = a.
\]

Lemma \( \text{product2_infinite} : \forall a b, \text{cardinal_le} b a -> \)
\[
\text{is_infinite_c} a -> b <> \text{card_zero} -> \text{card_mult} a b = a.
\]

Lemma \( \text{notbig_family_sum} : \forall a f, \text{fgraph} f -> \)
\[
\text{is_infinite_c} a -> \text{cardinal_le} (\text{cardinal} (\text{domain} f)) a -> \)
\[
(\forall i, \text{inc} i (\text{domain} f) -> \text{cardinal_le} (V i f) a) ->
\]
cardinal_le (cardinal_sum f) a.

Lemma notbig_family_sum1: forall a f, fgraph f ->
  is_infinite_c a -> cardinal_le (cardinal (domain f)) a ->
  (forall i, inc i (domain f) -> cardinal_le (V i f) a) ->
  (exists j, inc j (domain f) & (V j f) = a) ->
  (cardinal_sum f) = a.

Lemma sum2_infinite: forall a b, cardinal_le b a ->
  is_infinite_c a -> card_plus a b = a.

7.4 Countable sets

A countable set is one that is equipotent to a subset of \(\mathbb{N}\). Proposition 2 [2, p. 188] says that an infinite countable set is equipotent to \(\mathbb{N}\). We rewrite this as: a countable set is finite or equipotent to \(\mathbb{N}\).

Proposition 1 [2, p. 188] says that a subset of a countable set is countable; the product of a finite family of countable sets is countable; the union of a countable family of countable sets is countable.

Proposition 3 [2, p. 189] says that an infinite set \(E\) has a partition \((X_i)_{i \in I}\) where \(X_i\) is infinite countable and \(I\) is equipotent to \(E\). Proposition 4 [2, p. 189] says that if \(f\) is a function from \(E\) onto \(F\), such that \(f\) is a function from \(E\) onto \(F\), such that \(f^{-1}(\{x\})\) is countable for any \(x \in F\), then \(F\) is equipotent to \(E\).

Definition is_countable_set E := equipotent_to_subset E Bnat.
Lemma countable_prop: forall E,
  is_countable_set E = cardinal_le (cardinal E) (cardinal Bnat).

Lemma infinite_greater_countable1: forall E,
  infinite_set E -> cardinal_le (cardinal Bnat) (cardinal E).

Lemma countable_finite_or_N: forall E, is_countable_set E ->
  is_finite_c (cardinal E) / cardinal E = cardinal Bnat.

Lemma countable_finite_or_N_b: forall E, is_countable_set E ->
  infinite_set E -> equipotent E Bnat.

Theorem countable_subset: forall E F, sub E F -> is_countable_set F ->
  is_countable_set E.

Theorem countable_product: forall f, fgraph f ->
  is_finite_set (domain f) ->
  (forall i, inc i (domain f) -> is_countable_set (V i f)) ->
  is_countable_set (productb f).

Theorem countable_union: forall f, fgraph f ->
  is_finite_set (domain f) ->
  (forall i, inc i (domain f) -> is_countable_set (V i f)) ->
  is_countable_set (unionb f).

Theorem infinite_partition: forall E, infinite_set E ->
  exists f, partition_fam f E & equipotent (domain f) E &
  (forall i, inc i (domain f) -> (infinite_set (V i f) &
  is_countable_set (V i f))). (* 33 *)

Theorem countable_inv_image: forall f, surjective f ->
  (forall y, inc y (target f) ->
  is_countable_set (inv_image_by_fun f (singleton y))) ->
  infinite_set (target f) ->
  equipotent (source f) (target f). (* 41 *)
Proposition 5 [2, p. 189] says that the set $\mathfrak{F}$ of finite subsets of an infinite set $E$ is equipotent to $E$. The proof of Bourbaki is not clear. He defines $F_n$ as the set of all subsets with $n$ elements of $E$ and claims $\text{Card}(F_n) \leq \text{Card}(E)$. Thus, the cardinal of the union of these sets is at most $\sum_{n \in \mathbb{N}} \text{Card}(E) = \text{Card}(E)$. Thus $\text{Card}(\mathfrak{F}) \leq \text{Card}(E)$; equality holds because the set of singletons is equipotent to $E$ and is a subset of $\mathfrak{F}$.

The Bourbaki claim is: for every $X \in F_n$ there is a bijection from $[1, n]$ onto $X$, so that the cardinal of $F_n$ is at most the cardinal of the set of functions from $[1, n]$ into $X$ which is $\text{Card}(E^n) = \text{Card}(E)$. Our proof is as follows.

For every $X \in F_n$ there is a bijection $[1, n] \to X$, hence an injective function from $[1, n]$ into $E$ with range $X$, but it is not unique. Let $K$ be the set of injections from $[1, n]$ into $E$. Let $f$ be the function that associates to each element of $K$ its range. The target of this function is clearly $\mathfrak{F}_n$. Let $Q$ be the set of permutations of $[1, n]$, and $c$ it cardinal. This is a non-zero integer. We pretend that the cardinal of $f^{-1}(\{x\})$ is $c$. We take an element $g$ in this set (it exists, by the remark above). For every permutation $h$ of $[1, n]$, we consider $g \circ h$. This operation is a bijection from $Q$ onto $f^{-1}(\{x\})$. Surjectivity of this operation uses the fact that for any $k$ there exists $g$ such that $k = g \circ h$, if the ranges are the same (since $h$ is injective) and this function is surjective. It is bijective since it is an endomorphism of a finite set. We can now apply the shepherd's principle. The product of the cardinal $a$ of $\mathfrak{F}_n$ and $c$ is the cardinal $b$ of the set of injections, that is smaller than the cardinal $d$ of the set of functions from $[1, n]$ into $E$. If $n = 0$, we clearly have $a \leq \text{Card}(E)$; otherwise $d = \text{Card}(E)$. Hence $ac = b \leq \text{Card}(E)$. If $a$ is finite, we have $a \leq \text{Card}(E)$; but if $a$ is infinite, we have $a = ac$ (since $c$ is non-zero finite). This implies $a \leq \text{Card}(E)$.

As a corollary, the set of finite sequences with value into $E$ is equipotent to $E$; in fact, this set is the union of the sets of functions from $I$ into $E$ (that has the same cardinal as $E^I$) for all finite subsets $I$ of $\mathbb{N}$. Since $E^I$ and $I$ are equipotent and since the set of finite subsets of $\mathbb{N}$ is countable, the result is immediate.

Theorem infinite_finite_subsets: forall E, infinite_set E ->
   equipotent (Zo (powerset E) (fun z => is_finite_set z)) E. (* 141 *)

Lemma infinite_finite_sequence: forall E, infinite_set E ->
   equipotent (Zo(set_of_sub_functions Bnat E) (fun z=> is_finite_set (P (Q z))))
   E. (* 66 *)

A set is said to have the power of the continuum if it is equipotent to $\mathcal{P}(\mathbb{N})$. In this case, its cardinal is $2^{\aleph_0}$, and the set is not countable.

### 7.5 Stationary sequences

A sequence $(x_n)_{n \in \mathbb{N}}$ is stationary if there exists an integer $m$ such that $x_n = x_m$ for $n \geq m$. We define here the notion of increasing and decreasing sequences. It is the graph of an increasing function where the source is $\mathbb{N}$ with its natural order. Note that a decreasing sequence is increasing for the opposite order.

Definition stationary_sequence f :=
   fgraph f & domain f = Bnat &
   exists m, inc m Bnat & forall n, inc n Bnat -> cardinal_le m n ->
   V n f = V m f.

Definition increasing_sequence f r :=

INRIA
Proposition 6 \([2, p. 190]\) says that, if \(E\) is an ordered set, each non-empty set has a maximal element if and only if each increasing sequence is stationary. We start with a lemma: a function \(f\) such that \(f(n) \leq f(n+1)\) is increasing (by induction on \(m\), we have \(f(n) \leq f(n+m)\)). By definition \(\text{increasing}_\text{fun} f r r'\) says that the target of \(f\) is the substrate of \(r\); in our case, it is merely a subset, so that the definition will not be used: we show that the graph of \(f\) is an increasing sequence.

The Proposition is shown as follows. Given an increasing sequence, its range is non-empty. If it has a maximal element \(x_n\) and \(m \geq n\) then \(x_n \leq x_m\) implies \(x_m = x_n\). Conversely, assume that we have a set \(A\) that has no maximal element. For each \(x\), the subset \(T_x\) of elements of \(A\) greater than \(x\) is non-empty. This means that the product \(\prod T_x\) is non-empty, hence there is a function \(f: A \rightarrow A\) such that \(f(x) > x\) and a sequence \(x_n+1 = f(x_n)\). This sequence is strictly increasing, absurd.

As a consequence a totally ordered set \(E\) is well-ordered if and only if each decreasing sequence is stationary (to show that it is well-ordered, we consider the opposite order; thus every non-empty set has a minimal element, this element is the least element, since all subsets of \(E\) are directed). Moreover, an increasing sequence in a finite ordered set has a maximal element.

**Lemma increasing_prop:** \(\forall f \, r, \text{order} \ r \rightarrow \text{is\_function} \ f \rightarrow \text{source} \ f = \text{Bnat} \rightarrow \text{sub} \ (\text{target} \ f) \ (\text{substrate} \ r) \rightarrow (\forall n, \text{inc} \ n \ \text{Bnat} \rightarrow \text{gle} \ r \ (W n f) \ (W (\text{succ} n) f)) \rightarrow \text{increasing\_sequence} (\text{graph} \ f) \ r.\)

**Lemma decreasing_prop:** \(\forall f \, r, \text{order} \ r \rightarrow \text{is\_function} \ f \rightarrow \text{source} \ f = \text{Bnat} \rightarrow \text{sub} \ (\text{target} \ f) \ (\text{substrate} \ r) \rightarrow (\forall n, \text{inc} \ n \ \text{Bnat} \rightarrow \text{gge} \ r \ (W n f) \ (W (\text{succ} n) f)) \rightarrow \text{decreasing\_sequence} (\text{graph} \ f) \ r.\)

**Theorem increasing_stationary:** \(\forall r, \text{order} \ r \rightarrow (\forall X, \text{sub} \ X \ (\text{substrate} \ r) \rightarrow \text{nonempty} \ X \rightarrow \exists a, \text{maximal\_element} (\text{induced\_order} \ r X) a) \rightarrow (\forall f, \text{increasing\_sequence} f \ r \rightarrow \text{stationary\_sequence} f).\) (* 43 *)

**Theorem decreasing_stationary:** \(\forall r, \text{total\_order} \ r \rightarrow (\forall X, \text{sub} \ X \ (\text{substrate} \ r) \rightarrow \text{nonempty} \ X \rightarrow \exists a, \text{maximal\_element} (\text{induced\_order} \ r X) a) \rightarrow (\forall f, \text{decreasing\_sequence} f \ r \rightarrow \text{stationary\_sequence} f).\) (* 38 *)

**Theorem finite_increasing_stationary:** \(\forall r, \text{order} \ r \rightarrow \text{is\_finite\_set} (\text{substrate} \ r) \rightarrow (\forall f, \text{increasing\_sequence} f \ r \rightarrow \text{stationary\_sequence} f).\)

Proposition 7 \([2, p. 190]\) says that if \(E\) is noetherian (every non-empty set has maximal element) and if \(F\) is a subset of \(E\) such that for \(a \in E\), if \(\forall x, x > a \implies x \in F\) then \(a \in F\); then \(F = E\).
sub F (substrate r) ->
(forall a, inc a (substrate r) -> (forall x, glt r a x -> inc x F)
  -> inc a F)
-> F = substrate r.
Chapter 8

The size of one

When I was young, I was intrigued by the following quote of Bourbaki:

Bien entendu il ne faut pas confondre le terme mathématique désigné (chap. I, § 1, n° 1) par le symbole « 1 » et le mot « un » du langage ordinaire. Le terme désigné par « 1 » est égal, en vertu de la définition donnée ci-dessus, au terme désigné par le symbole

\[ \tau_Z((\exists u)(\exists U)(u = (U, \{\emptyset\}, Z) \text{ and } U \subset \{\emptyset\} \times Z \text{ and } (\forall x)((x \in \{\emptyset\}) \implies (\exists y)((x, y) \in U)) \text{ and } (\forall x)(\forall y)(((x, y) \in U \text{ and } (x, y') \in U) \implies (y = y'))) \text{ and } (\forall y)((y \in Z) \implies (\exists x)((x, y) \in U))). \]

A rough estimate shows that the term so denoted is an assembly of several tens of thousands of signs (each of which is one of \(\tau, \Box, \lor, \neg, =, \in, \supset\)).

The same expression appears in the English version and in the French one (except that “and” is replaced by “et” in French). By definition, 1 is \(\text{Card}(\{\emptyset\}) = \tau_Z(\text{Eq}(\{\emptyset\}, Z))\).

If 1 is a big object, then how big is 2? or the set \(\mathbb{N}\) of integers, or the set \(\mathbb{R}\) of real numbers? If \(P(X, n)\) is: \(X = (x, y, z)\) and \(x^n + y^n = z^n\) and \(x \neq 0\) and \(y \neq 0\) and \(z \neq 0\), what is the size of the formula \((\forall n)(n \in \mathbb{N} \implies (\exists X)(X \in \mathbb{R}^3 \text{ and } P(X, n)))\)? If this is an assembly with millions of signs, how big will be a proof of it? If billions of signs are needed, how can one check the proof? I am convinced that it is a bad idea to try to reduce the object under consideration to its basic components (a kind of normal form) and apply low-level theorems to it; Fermat’s theorem cannot be proved by exhibiting an assembly that is a proof in the sense of Bourbaki.

On the other hand, the estimation of Bourbaki shows that it should be possible to print the whole assembly denoting 1 on an A0-size poster. Alas, the estimation is wrong.
First comments. For simplicity, we shall write \( Y \) instead of \( \emptyset \). The formula is hence

\[
\tau_Z(\exists u)(\exists U)(\quad u = (U, Y, Z) \\
\text{and } U \subset Y \times Z \\
\text{and } (\forall x)((x \in Y) \implies (\exists y)((x, y) \in U)) \\
\text{and } (\forall x)(\forall y)(\forall y')(((x, y) \in U \text{ and } (x, y') \in U) \implies (y = y')) \\
\text{and } (\forall y)((y \in Z) \implies (\exists x)((x, y) \in U)) \\
\text{and } (\forall x)(\forall x')((\forall y)(((x, y) \in U \text{ and } (x', y) \in U) \implies (x = x'))).
\]

(\text{**})

This is of the form \( \tau_Z(W_Z) \) where \( W_Z \) is \( (\exists u)(\exists U) W \), and where \( W \) is of the form \( P_1 \) and \( P_2 \) and \( P_3 \) and \( P_4 \) and \( P_5 \) and \( P_6 \). Properties \( P_1 \) and \( P_2 \) say that \( u \) is a correspondence with source \( Y \), target \( Z \) and graph \( U \), properties \( P_3 \) and \( P_4 \) say that \( u \) is a function, property \( P_5 \) that \( u \) is injective, and \( P_6 \) that \( u \) is injective. In other words, \( W \) says that \( u \) is the graph of a bijection with source \( Y \) and target \( Z \). Our formula is thus \( \tau_Z(\text{Eq}(Y, Z)) \), as it should be. Note that \( P_6 \) is missing in \( (\ast) \). In fact, if \( (x, y) \in U \), then \( x \in Y \), hence \( x = \emptyset \), so that \( P_6 \) is a consequence of other relations. Hence, the term designed by \( (\ast) \) is \textit{equal} but not \textit{identical} to 1. In what follows, we shall discuss the size of \( (\text{**}) \).

The case of Coq. The expression \( W \) has the form

\[
\exists u : \text{Set}, \\
\exists U : \text{Set}, \\
u = J(JU \text{ emptyset})Z \& \\
(\forall x : \text{Set}, \text{inc} x U \rightarrow \text{inc} x (\text{record} Y (\text{fun} _ : \text{Set} \rightarrow Z))) \& \\
(\forall x : \text{Set}, \text{inc} x Y \rightarrow \exists y : \text{Set}, \text{inc} (J x y) U \& \\
(\forall x y y' : \text{Set}, \text{inc} (J x y) U \rightarrow \text{inc} (J x y') U \rightarrow y = y') \& \\
(\forall x y Z \rightarrow \exists x : \text{Set}, \text{inc} (J x y) U \& \\
(\forall x x' y : \text{Set}, \text{inc} (J x y) U \rightarrow \text{inc} (J x' y) U \rightarrow x = x')
\]

Expanding everything but \( J \) gives:

\[
\exists u : \text{Set}, \\
\exists U : \text{Set}, \\
u = J(JU \text{ emptyset})Z \& \\
(\forall x : \text{Set}, \\
(\exists a : U, \text{Ro} a = x) \rightarrow \\
\exists a : \text{record} (\text{IM} (\text{fun} _ : \text{one_point} \rightarrow \text{emptyset})) \\
(\text{fun} _ : \text{Set} \rightarrow Z), \text{Ro} a = x) \& \\
(\forall x : \text{Set}, \\
(\exists a : \text{IM} (\text{fun} _ : \text{one_point} \rightarrow \text{emptyset}), \text{Ro} a = x) \rightarrow \\
\exists x y y' : \text{Set}, \exists x : \text{Set}, \text{exists} a : U, \text{Ro} a = J x y \& \\
(\exists a : U, \text{Ro} a = J x y \rightarrow (\exists a : U, \text{Ro} a = J x y') \rightarrow y = y') \& \\
(\forall y : \text{Set}, (\exists a : Z, \text{Ro} a = y) \rightarrow \\
\exists x : \text{Set}, \exists x : \text{Set}, \exists x : \text{Set}, \text{exists} a : U, \text{Ro} a = J x y) \& \\
(\forall x x' y : \text{Set}, (\exists a : U, \text{Ro} a = J x y) \rightarrow \\
(\exists a : U, \text{Ro} a = J x' y) \rightarrow x = x')
\]

Because of our implementation of \( \tau \) in Coq, the full expansion of 1 is three times as big as this quantity. This gives a total of 500 tokens (we count \textit{forall}, \textit{exists}, \textit{Set}, etc, as a single token).

In \cite{INRIA}, the symbol that looks like \( \supset \) has been withdrawn, and a pair is no more a primitive. As explained in the first part of this document, we do not use the same implementation as
Bourbaki. In particular, we use a primitive object `two_points` which is a set with two distinct elements. The expansion of the last line of the previous code is then:

\[
\begin{align*}
&\exists a : U, \quad \text{Ro} \ a = \text{IM} \ (\text{fun} \ t : \text{two_points} \Rightarrow \\
&\quad \begin{cases}
| \text{two_points}_a \Rightarrow \text{IM} \ (\text{fun} \ _ : \text{one_point} \Rightarrow x') \\
| \text{two_points}_b \Rightarrow \text{IM} \ (\text{fun} \ t : \text{two_points} \Rightarrow \\
\quad \begin{cases}
| \text{two_points}_a \Rightarrow \text{emptyset} \\
| \text{two_points}_b \Rightarrow \text{IM} \ (\text{fun} \ _ : \text{one_point} \Rightarrow y)
\end{cases}
\end{cases}
\end{cases}
\end{align*}
\]

If we estimate this as 50 tokens, this gives a total size of one that is less than 2000 tokens.

For Bourbaki, a correspondence is an object that satisfies P1 and P2 (namely \( u = (U, Y, Z) \) and \( U \subset Y \times Z \)), and for us, a correspondence is a data structure, that has three fields (source, target and graph) and some properties; denoting by \( u \) the triple formed of these three objects, by \( U, Y \) and \( Y \) the components of the triples, then \( U \) is a graph, whose domain is a subset of \( Y \) and whose range is a subset of \( Z \). This is equivalent to \( U \subset Y \times Z \). This is also equivalent to say that the graph of the correspondence is a subset of the product of the source and the range, but becomes much larger if we expand everything that can be expanded. We estimate that the number of tokens, after full expansion, is roughly 16000.

**Premiminary computations.** Let’s try to count exactly the numbers of signs of one in Bourbaki. Remember that the empty set is the following list of signs:

\[
\tau \neg\neg\neg \in \tau \neg\neg \in \Box \Box \Box
\]

It is easy to count them: there are 12 signs. The definition of the empty set is \( \tau \neg\neg\neg \in \tau \neg\neg \in \Box \Box \Box \). If \( P \) is a formula we denote by \( L[P] \) its length; assume that \( P \) depends on \( z \) and has \( \alpha \) signs and \( \beta \) other signs. Remember that \( \exists z P(z) \) is \( (\tau_z P) \), this is the formula obtained by replacing all \( z \) by \( \tau_z P \). Thus we have

\[
L[(\exists z P(z))] = (\alpha + 1)(\alpha + \beta).
\]

Since \( \forall z P(z) \) is \( \neg(\exists z)(\neg(Pz)) \), we get

\[
L[(\forall z P(z))] = 1 + (\alpha + 1)(\alpha + \beta + 1).
\]

In the case of \( (\forall y)(y \notin x) \), we have \( \alpha = 1 \) and \( \beta = 4 \), the length is 11, hence \( L[\varnothing] = 12 \). The following formulas are obvious:

\[
\begin{align*}
L[A \text{ or } B] &= 1 + L[A] + L[B] \\
L[A \text{ and } B] &= 4 + L[A] + L[B] \\
L[A \implies B] &= 2 + L[A] + L[B] \\
L[A \iff B] &= 8 + 2L[A] + 2L[B]
\end{align*}
\]

The set of all \( x \) such that \( P(z) \) is \( \tau_y((\forall z)(z \in y) \iff P) \) hence

\[
L[\{z, P(z)\}] = 4\alpha^2 + 36\alpha + 47 + (4\alpha + 6)\beta.
\]

RR n° 7150
The length of $z = x$ or $z = y$ is $3 + x + y + 2z$, and since $\{x, y\}$ is the set of all $z$ such that $z = x$ or $z = y$ we get

$$L[(x, y)] = 177 + 14x + 14y.$$ 

Since $\emptyset = \emptyset$, we get

$$L[\emptyset] = 513.$$ 

Assume that $W$ has length $\alpha + \beta U + \gamma Z + u$. The size of $(\exists U)W$ is

$$(\beta + 1)(\alpha + \beta + \gamma Z + u);$$

the size of $(\exists u)(\exists U)W$ is

$$(\beta + 1)(\beta + 2)(\alpha + \beta + \gamma Z + 1);$$

hence the size of one is

$$1 + (\beta + 1)(\beta + 2)(\alpha + \beta + \gamma + 1).$$

Size of a triple. We estimate here the length of the expression $u = (U, Y, Z)$, assuming that the triple is the pair of pairs $((U, Y), Z)$. Since the pair $(x, y)$ is $\{(x), (x, y)\}$ we have

$$L[(x, y)] = 5133 + 588x + 196y.$$ 

$$L[((x, y), z)] = 3023337 + 345744x + 115248y + 196z$$

$$L[u = (U, Y, Z)] = 62145562 + 345744U + 196Z + u$$

Let $\alpha$ be the constant that appears here, and $\beta$ the coefficient of $U$. Since the size of one is at least $\alpha \beta^2$, this formula shows that the size is a bit larger than what Bourbaki claims. Instead of "several tens of thousands", it is at least $10^{18}$.

The English version of Bourbaki (as well as the 1956 French edition) has the special symbol that looks like $\supset$ and creates a pair. We use here the notation $L'$, when we count the size of the English one; we have

$$L'[u = (U, Y, Z)] = u + U + Z + 516.$$ 

Size of a graph. We try to find the size of expression $P_2$, namely $U \subset Y \times Z$. If $B$ is $Y \times Z$, this expression is $\forall (z)(z \in A \implies z \in B)$, its size is $22 + 3A + 3B$. The size of "$z = (x, y)$ and $x \in Y$ and $y \in Z$" is $z + 2x + 2y + Y + Z + 12$. If this is $P$, then $Y \times Z$ is the set of all $z$ so that there exists $x$ such that there exists $y$ such that $P$. Quantifying $\exists y$ gives $42 + 6x + 3Y + 3Z + 3z$, quantifying $\exists x$ gives $336 + 21(Y + Z + z)$. Taking the set of all $z$ gives $32807 + 1890(Y + Z)$.

$$L'[U \subset Y \times Z] = 98443 + 3U + 5670(Y + Z);$$

$$L'[P_2] = 3007153 + 3U + 5670Z.$$ 

For the French version, the length of $P$ is

$$589x + 5144 + 197y + z + Y + Z.$$ 

Quantifying over $y$ gives

$$1057518 + 198Y + 198Z + 116622x + 198z.$$
Quantifying over $x$ gives

$$136931729220 + 23091354(Y + Z + z).$$

Taking the set of all $z$ gives

$$L[Y \times Z] = 1264988979794532895 + 2132842656761388(Y + Z);$$
$$L[U \subset Y \times Z] = 37949669383598707 + 3U + 6398527970284164(Y + Z);$$
$$L[P2] = 41232114242589374839 + 3U + 6398527970284164Z.$$This number is so big that it is impossible to put in a computer the full expansion of $U \subset \{\varnothing\} \times Z$.

**Size of a bijection.** Let's try to find the size of the expressions $P2$, $P3$, $P4$, $P5$ and $P6$. They are similar. We start with $(x, y) \in U$, the size is

$$5134 + 588x196y + U; \text{ or } 2 + x + y + U.$$The size is $(\exists y)((x, y) \in U)$ is

$$1050010 + 197U + 115836x or 6 + 2U + 2x.$$The size of $x \in Y \implies (\exists y)((x, y) \in U)$ is

$$1050013 + 197U + 115837x + Y or 9 + 2U + 3x + Y.$$The size of $(\forall x)(x \in Y \implies (\exists y)((x, y) \in U))$ is

$$135049848139 + 22820086U + 115838Y or 53 + 8U + 4Y.$$The size of $P3$ is

$$135109273033 + 22820086U or 2105 + 8U.$$The size of $(x, y) \in U \text{ and } (x, y') \in U$ is

$$10272 + 1176x + 196y + 196y' + 2U or 8 + 2x + y + y' + 2U;$$The size of $(x, y) \in U \text{ and } (x, y') \in U \implies y = y'$ is

$$10275 + 1176x + 197y + 197y' + 2U or 11 + 2x + 2y + 2y' + 2U;$$The size of $(\forall y')(\exists y)((x, y) \in U \text{ and } (x, y') \in U \implies y = y')$ is

$$2073655 + 396U + 34848x + 39006y or 43 + 6U + 6x + 6y.$$The size of $(\forall y)(\forall y')(\exists y)((x, y) \in U \text{ and } (x, y') \in U \implies y = y')$ is

$$82408606635 + 15446772U + 9082701936x or 351 + 42U + 42x.$$Finally the size of $P4$ is

$$83098828553569103965 + 140298425964797364U or 16943 + 1806U.$$
The size of $(\exists x)((x, y) \in U)$ is
\[3370258 + 589U + 115444y + 6 + 2U + 2y.\]

The size of $y \in Z \implies (\exists x)((x, y) \in U)$ is
\[3370261 + 589U + 115445y + Z + 9 + 2U + 3y + Z.\]

Hence the size of $P_5$ is
\[402410930323 + 67997694U + 115446Z + 53 + 8U + 4Z.\]

The size of $(x, y) \in U$ and $(x', y) \in U \implies x = x'$ is
\[10275 + 589x + 589x' + 392y + 2U + 11 + 2x + 2x' + 2y + 2U.\]

The size of $(\forall y)((x, y) \in U$ and $(x', y) \in U \implies x = x')$ is
\[4192525 + 786U + 231477(x + x') + 43 + 6U + 6x + 6x'.\]

The size of $(\forall x')((\forall y)((x, y) \in U and (x', y) \in U \implies x = x'))$ is
\[1024059366435 + 181941708U + 5358183306x or 351 + 42U + 42x.\]

Hence the size of $P_6$ is
\[57741990789964425582095 + 9748770215064355956U + 16943 + 1806U.\]

The size of the expressions $P_3$ to $P_6$ is hence
\[58572979076087514889416 + 9889068641119971100U + 115446Z + 36044 + 3628U + 4Z.\]

This gives, for the French version $\alpha = 5861421119033016409837 \beta = 9889068641120316847 \gamma = 6398527970399806$, and for the English version: This gives $\alpha = 3033733$, $\beta = 36732$ and $\gamma = 5675$.

**Conclusion.** The statement, at the start of the chapter, quoted from the 1956 edition of Bourbaki, translated in English in 1968, is grossly wrong since the size is not several thousands, but in fact
\[4150763939024663.\]

Moreover, the 1970 decision to remove the axiom of the ordered pair had a dramatic effect on the size of one, that increases to
\[573306704017980337582376403672241161543539419681476659296689.\]
Chapter 9

Exercises

There are 111 exercises for this chapter (plus 9 concerning direct and inverse limits). We
give here the number of lines of the code of all these.

Section 1. 1 (12), 2 (350), 3 (671), 4 (149), 5 (114), 6 (977), 7 (128), 8 (29), 9 (145), 10 (17),
11 (364), 12 (29), 13 (78), 14 (76), 16 (294),

Section 6. 1 (147), 2 (59), 3 (64), 4 (63).

This is example 1 page 148: Let \( E = \{\alpha, \beta\} \) be a set whose elements are distinct. It is easily
verified that the subset \( \{ (\alpha, \alpha), (\beta, \beta), (\alpha, \beta) \} \) of \( E \times E \) is the graph of a well-ordering on \( E \).

Definition example_worder :=
union2(doubleton (J TPa TPa) (J TPb TPb)) (singleton (J TPa TPb)).

We first show that we have an ordering.

Lemma example_is_worder: worder example_worder.
Proof. set (g:= example_worder).
assert (forall z, inc z g =\( (z = J TPa TPa \lor z = J TPb TPb \lor z = J TPa TPb) \)).
uf g. uf example_worder.
ir. app iff_eq. ir. ufi g H. nin (union2_or H). left. am. right. left. am. right. right. app singleton_eq. ir. uf g. nin H.
rw H. fprops. app union2_first. fprops. nin H; rw H. app union2_first. fprops.
app union2_second. fprops.
assert (is_graph g). red. ir. rwi H H0. nin H0. rw H0. fprops. nin H0.
rw H0. fprops. rw H0. fprops.
assert (H a: related g TPa TPa). red. rw H. left. tv.
assert (H b: related g TPb TPb). red. rw H. right. left. tv.
assert (H c: related g TPa TPb). red. rw H. right. right. tv.
assert (substrate g = two_points). set_extens. rwi (inc_substrate_rw x H0) H1.
nin H1. nin H1. rwi H H1. nin H1. rw (pr1_injective H1). fprops.
nin H1. rw (pr1_injective H1); fprops.
nin H1. rwi H H1. nin H1. rw (pr2_injective H1). fprops.
nin H1; rw (pr2_injective H1); fprops. rwi two_points_pr H1. nin H1; rw H1.
app (inc_arg1_substrate Ha). app (inc_arg1_substrate Hb).
assert (order g). red. ee. am. red. split. am. ir. rwi H1 H2.
rwi two_points_pr H2. nin H2; rw H2; am.
red. split. am. ir. red in H2. red in H3. rwi H H2. rwi H H3.
assert (related g TPa z). nin H3. rww (pr2_injective H3).
nin H3; rww (pr2_injective H3). nin H2. rww (pr1_injective H2).
nin H2; rww (pr1_injective H2). nin H3. rw (pr2_injective H3).
If $X$ is a subset of $E$, it contains only $\alpha$ or $\beta$. If it is a singleton, it has clearly a least element. Otherwise, if it is not empty, it must be $E$ and the smallest element is $\alpha$. All in all, we have to show four relations of the type $x \leq y$. Note that in the case of a totally ordered set with three elements, checking transitivity consists in considering 36 pairs of the form $x \leq y$ and $y \leq z$, and checking that it is well-ordered consists in finding a smallest element for 7 sets, thus checking 12 relations.

The set $\Phi$ of mappings of subsets of $E$ into subsets of $F$ is inductive, with respect to the order "$\nu$ extends $\mu$" between $\mu$ and $\nu$ (i.e., the opposite of the extension ordering), because there is a common extension on a totally ordered subset.

The set $\Phi(E,F)$ of mappings of subsets of $E$ into subsets of $F$ is inductive, with respect to the order "$\nu$ extends $\mu$" between $\mu$ and $\nu$ (i.e., the opposite of the extension ordering), because there is a common extension on a totally ordered subset.

Lemma inductive_graphs: forall a b, inductive_set (opposite_order (extension_order a b)).
Proof. ir. cp (extension_is_order a b). red. ir. red in H1. ee. awi H2;try am.
awi H0.
assert (Ha:forall i, inc i X -> is_function (inv_corr_value i)).
ir. cp (H0 _ H3). rwi set_of_sub_functions_pr1 H4. ee; am.
assert (Hb:forall i, inc i X -> target (inv_corr_value i) = b).
ir. cp (H0 _ H3). rwi set_of_sub_functions_pr1 H4. ee; am.
set (f:= fun z => P (Q z)).
assert (Hc:forall i, inc i X -> source (inv_corr_value i) = f i).
ir. cp (H0 _ H3). rwi set_of_sub_functions_pr1 H4. ee; uf f.
set (k:= inv_corr_value i). fold k in H7. wr H7. uf corr_value. aw.
assert (Hd: forall i j, inc i X -> inc j X ->
agrees_on (intersection2 (f i) (f j)) (inv_corr_value i) (inv_corr_value j)).
ir. cp (H0 _ H3). cp (H0 _ H4).
set (f:= fun z => P (Q z)).
assert (H0:forall i X, source (inv_corr_value i) = f i).
Qed.

Consider two injections \( f : E \rightarrow F \) and \( g : F \rightarrow E \). For \( X \subset E \), consider \( h(X) = E - g(F - f(X)) \). Since taking the complementary of a set by a function is decreasing and the composition of two decreasing functions is increasing, this function is increasing. If it has a fixed point \( M \). We have \( E - M = g(F - f(M)) \).

Lemma Cantor_Bernstein: forall \( f \) \( g \),
injective \( f \) \rightarrow injective \( g \) \rightarrow source \( f \) = target \( g \) \rightarrow source \( g \) = target \( f \) \rightarrow
equipotent (source \( f \))(source \( g \)).
Proof. ir. set (E:= source \( f \)) in *.
set (F:=source \( g \)) in *.
set \( h \) (fun \( x \) => complement E (image_by_fun g (complement F (image_by_fun f x))))).
assert (Ha:is_function \( f \)). nin H; am.
assert (forall \( x \), sub \( x \) E \rightarrow sub (h \( x \)) E). ir. uf h. app sub_complement.
assert (forall \( x \) \( y \), sub \( x \) \( y \) \rightarrow sub \( y \) E \rightarrow sub (h \( x \))(h \( y \))). ir. uf h.
red. ir. srwi H6. nin H6. srw. split. am. red. ir. elim H7. avi H8. nin H8.
srwi H8. ee. aw. exists x1. srw. ee. am. red. ir. elim H10.
awi H11. nin H11. aw. exists x2. ee. app H4. am. am.
apply sub_trans with \( y \). am. am. am. nin H0; am. app sub_complement.
nin H0; am. app sub_complement.
nin (Cantor_Bernstein_aux _ H3 H4). nin H5. ufi h H6.
set \( T := \text{image_by_fun g (complement F (image_by_fun f x))} \) in *.
assert (sub \( T \) E). uf T. red. ir. avi H7. nin H7. nin H7. wr H8. wr H8. wr H1.
app inc_W_target. nin H0; am. srwi H7. nin H7. am. nin H0; am.
app sub_complement. cp (double_complement H7). wrw H6 H8.

Let \( T = g(F - f(M)) \). This is the complementary of \( M \). Every element in \( T \) is of the form \( g(\( y \)) \) for some \( y \) not of the form \( f(\( x \)) \) for \( x \in T \). We use the choice function in order to get a function \( f_2 \). Note that the choice is limited, this \( y \) is unique by injectivity of \( g \). We consider the function \( f_1 \) whose value is \( f \) on \( M \) and \( f_2 \) on \( T \).

set (f1:= fun \( a \)= choose(fun \( y \)= inc \( y \) F \& ~ inc \( y \) (image_by_fun f x) \&
\( a = W y g \))).
assert (forall \( a \), inc \( a \) T \rightarrow (inc (f1 \( a \) ) F \& ~ inc (f1 \( a \)) (image_by_fun f x) \&
\( a = W (f1 \( a \)) \)).
ir. uf f1. app choose_pr. app H9.
set (f2:= fun \( a \)= Yo (inc \( a \) T) (f1 \( a \) ) (W a f)).

This function is injective. Assume \( f_1(\( x \)) = f_1(\( y \)) \). If one of \( x \), \( y \) is in \( M \) and the other one is in \( T \), one image is in \( f(M) \), and the other is in the complement, absurd. If both elements are in \( M \), we use injectivity of \( f \). Otherwise \( f_1(\( x \)) = x' \) where \( x = g(x') \) and \( f_1(\( y \)) = y' \) where \( y = g(y') \). We use injectivity of \( g \). This function is clearly surjective, thus is a bijection \( E \rightarrow F \).

assert (transf_axioms f2 E F). red. ir. uf f2. nin (inc_or_not c T).
ir. rw Y_if_rw. cp (H10 _ H12). ee. am. am. ir. rww Y_if_not_rw. wr H2.
app inc_W_target.
exists (BL f2 E F). ee. split. app injective_af_function. ir.
ufi f2 H14. nin (inc_or_not u T); [ rww Y_if_rw H14 ]
nin (inc_or_not v T). cp (H10 _ H15). cp (H10 _ H16). ee. rwi Y_if_rw H14.
wr H22; wr H20; wr H14. cp (H10 _ H15). ee. rwi Y_if_not_rw H14.
elim H18. aw. exists v. wr H14. split. wr H6. srw. split; am. tv.
wr H6. srw. split. am. am. sy; am. rwi Y_if_not_rw H14.
nin H. app H17.
app (surjective_af_function). ir. nin (inc_or_not y (image_by_fun f x)).
awi H12. nin H12. nin H13. exists x0. split. app H5. uf f2.
rew Y_if_not_rw. am. wri H6 H13. srwi H13. nin H13; am. am. am.
exists (W y g). split. rw H1. app inc_W_target. nin H0; am.
uf f2. assert (inc (W y g) T). uf T. aw. exists y. split. srw. split.
am. am. tv. nin H0; am. app sub_complement. rew Y_if_rw. cp (H10 _ H14).
ee. nin H0. app H18. tv. tv.
Qed.

We give now a variant of the theorem. In fact, we show that if \( \nu \) an injection \( A \rightarrow B \) and \( B \subset A \), then \( A \) and \( B \) are equipotent. Consider two functions \( f \) and \( g \), let \( A \) be the source of \( f \) and \( B \) the image of \( g \). We have the canonical decomposition of \( g \) as a function \( \bar{g} : F \to B \), the canonical injection \( i \) of \( B \) into \( A \). By assumption \( \bar{g} \) is bijective. The compositio of \( \bar{g} \circ f \) is an injection \( A \rightarrow B \), hence there is a bijection \( \nu : A \rightarrow B \), and \( \bar{g}^{-1} \circ \nu \) is a bijection \( E \rightarrow F \). We leave the details to the reader.

We consider the set \( A \) of subsets of \( E \) invariant by \( F \), the set \( B \) which is the complementary of \( F \) in \( E \), the set \( C \) of all elements of \( A \) that contain \( B \), and the intersection \( D \) of \( C \). This intersection is well-defined, since \( E \in C \). It is the smallest element of \( C \).

Lemma Cantor_Bernstein_aux2: forall (E F: Set) (f:Set -> Set),
sub F E ->
(foreall x, inc x E -> inc (f x) F) ->
(foreall x y, inc x E -> inc y E -> f x = f y -> x = y) ->
equipotent E F.
Proof. ir.
set (A := Zo (powerset E)(fun x=> forall y, inc y x -> inc (f y) x)).
set (B:= complement E F).
set (C:= Zo A (fun x=> sub B x)).
set (D:= intersection C).
assert (sub A (powerset E)). uf A. app Z_sub.
assert (inc E C). uf C. Ztac. uf A.
Ztac. app powerset_inc. fprops. uf B. app sub_complement.
assert (forall x, inc x C -> sub D x). ir. red. ir. ufi D H5.
ap (intersection_forall F H4).
assert (inc D A). uf A. Ztac. app powerset_inc. red. uf D. ir.
cp (intersection_forall H4 H3). am. ir. uf D. app intersection_inc.
exists E. am. ir. assert (inc y y0). ufi D H4.
assert (inc D C). uf C. Ztac. uf D. red. ir. app intersection_inc. exists E.
assert (complement E B=F). uf B. app double_complement.

We consider the function \( g \) whose value is \( f \) on \( D \), the identity elsewhere. The relation \( B \subset D \) implies \( E - D \subset F \), so that \( g \) has value in \( F \). Since \( f(D) \subset D \) and \( f \) is injective, the function \( g \) is clearly injective.

set (g:=fun y => Yo (inc y D) (f y) y).
assert (transf_axioms g E F). red. ir. uf g. nin (inc_or_not c D).
rew Y_if_rw. app H0. rew Y_if_not_rw. wr H8. srw. split. am.
red. ir. elim H10. app H7.
exists (BL g E F). ee. red. split. app injective_af_function. ir.

RR n° 7150
Let's show surjectivity. We must show that if $y \in F$ and $y \in D$, then $y = f(x)$ for some $x$ in $D$. Let $T = D - \{y\}$. This contains $B$ (since $B \subset D$ and $y \not\in B$). It is not in $A$ (otherwise, it would be in $C$, hence contain $D$, which is impossible since $y \in D$ and $y \not\in T$). This means that $T$ is not invariant by $f$. Consider $x \in T$ such that $f(x) \not\in T$. We have $f(x) = y$.

9.1 Section 1

1. Let $E$ be an ordered set in which there exists at least one pair of distinct comparable elements. Show that if $RÄ\ x, yÄ$ denotes the relation “$x \in E$ and $y \in E$ and $x < y$”, then $R$ satisfies the first two conditions of no. 1 but not the third.
2. (a) Let $E$ be a preordered set and let $S \triangle x, y \triangle$ be an equivalence relation on $E$. Let $R_{X, Y}$ denote the relation "$x \in E/S$ and $y \in E/S$ and for each each $x \in X$ there exists $y \in Y$ such that $x \leq y". Show that $R$ is a preorder relation on $E/S$, called the quotient by $S$ of the relation $x \leq y$. The quotient $E/S$, endowed with this preorder relation, is called (by abuse of language; cf Chapter IV, § 2, no. 6) the quotient by $S$ of the preordered set $E$.

In what follows, we shall denote by $\leq_E$ the given preorder, and by $x \leq_E y$ the associated preordered relation; in the same way, $\leq_Q$ is the quotient preorder and $x \leq_Q y$ its associated relation. In other words, $x \leq_Q y$ is the relation $R_{x, y}$ defined in the text and $\leq_Q$ is the graph of this relation on $E/S$.

Definition quotient_order_r r s X Y :=
  inc X (quotient s) & inc Y (quotient s) &
  forall x, inc x X -> exists y, inc y Y & gle r x y.
Definition quotient_order r s :=
  graph_on (quotient_order_r r s) (quotient s).

First part: we show that $x \leq_Q y$ is a preorder relation.

Lemma Exercise1_2a: forall r s, is_equivalence s -> preorder r -> substrate s = substrate r ->
  preorder_r (quotient_order_r r s).
Proof. ir. red. split. uf quotient_order_r. red. ir. ee. am. am.
  ir. cp (H7 _ H8). destruct H9 as [ a [ H9 H10]]. cp (H5 _ H9). nin H11.
  nin H11. exists x1. split. am. red in H0; ee. nin H14.
  app (H15 _ _ _ H10 H12). red. uf quotient_order_r. red in H0. ee.
  nin H2. ir. ee. am. ir. exists x0. split. am. app H4. wr H1.
  app (inc_in_quotient_substrate H H8 H5). am. am.
  ir. exists x0. split. am. app H4. wr H1.
  app (inc_in_quotient_substrate H H8 H6).
Qed.

We now show that $\leq_Q$ is a preorder on $E/S$, associated to the relation $x \leq_Q y$.

Lemma quotient_order_pr: forall r s x y, related (quotient_order r s) x y = quotient_order_r r s x y.
Proof. ir. uf quotient_order. uf graph_on. uf related. ap iff_eq. ir. Ztac.
  awi H1. am. ir. Ztac. red in H. ee. fprops. aw.
Qed.

Lemma quotient_is_preorder: forall r s, is_equivalence s -> preorder r -> substrate s = substrate r ->
  preorder (quotient_order r s).
Proof. ir. uf quotient_order. app preorder_from_rel. app Exercise2_2a.
Qed.

Lemma substrate_quotient_order: forall r s, is_equivalence s -> preorder r -> substrate s = substrate r ->
  substrate (quotient_order r s) = quotient s.
Proof. ir. cp (quotient_is_preorder H H0 H1). set_extens.
  rwi preorder_reflexivity H3. rwi quotient_order_pr H3. red in H3. nin H3. am.
  am. rw preorder_reflexivity. rv quotient_order_pr. red. split. am. split. am.
  ir. exists x0. split. am. wr preorder_reflexivity. wr H1.
  app (inc_in_quotient_substrate H H4 H3). am. am.
Qed.

RR n° 7150
(b) Let $\phi$ be the canonical mapping of $E$ onto $E/S$. Show that if $g$ is a mapping of the preordered quotient set $E/S$ into a preordered set $F$ such that $g \circ \phi$ is an increasing mapping, then $g$ is an increasing mapping. The mapping $\phi$ is increasing if and only if $S$ satisfies the following condition

(C) the relations $x \leq y$ and $x \equiv x'$ (mod $S$) in $E$ imply that there exists $y' \in E$ such that $y \equiv y'$ (mod $S$) and $x' \leq y'$.

Every equivalence relation $S$ which is compatible (in $x$) with the preorder relation $x \leq y$ (Chapter II, § 6, no. 3) is a fortiori weakly compatible (in $x$ and $y$) with this relation.

We consider now a function $g$ such that $g \circ \phi$ is an increasing mapping, and show that $g$ is increasing. Assume $X \leq Q Y$, and that we want to show $g(X) \leq F g(Y)$. Since $X$ is a class, there is $x \in X$ hence there is $y \in Y$ such that $x \leq E y$. Thus $g(\phi(x)) \leq F g(\phi(y))$. It remains to show that $X = \phi(x)$ and $Y = \phi(y)$.

Definition increasing_pre $f$ $r$ $r'$ :=
is_function $f$ & preorder $r$ & preorder $r'$ & substrate $r$ = source $f$
& substrate $r'$ = target $f$ & increasing_map (fun w => $W$ w $f$) (source $f$) $r$ $r'$.

Lemma Exercise1_2b1: forall $r$ $s$ $g$ $r'$,
is_equivalence $s$ -> preorder $r$ -> substrate $s$ = substrate $r$ ->
is_function $g$ -> preorder $r'$ -> quotient $s$ = source $g$ ->
increasing_pre (compose $g$ (canon_proj $s$)) $r$ $r'$ ->
increasing_pre $g$ (quotient_order $r$ $s$) $r'$.
Proof. ir. red. ee. am. app quotient_is_preorder. am.
  rww substrate_quotient_order. red in H5. ee. am.
  assert (composable $g$ (canon_proj $s$)). red. ir. ee. am.
  app function_canon_proj. sy; tv. red. ir.
  cp (inc_rep_itself H H9). nin (H16 _ H18). nin H19.
  assert (inc (rep $x$) (substrate $r$)). app (inc_arg1_substrate H20).
  assert (inc $x$0 (substrate $r$)). app (inc_arg2_substrate H20).
  cp (H14 _ _ H21 H22 H20). rwi H17 H21; rwi H17 H22.
  rwi $W$ compose H23. rwi $W$ compose H23. avi H23; try am.
  assert (class $s$ (rep $x$) = $x$). app class_rep. rwi H24 H23.
  assert ($y = class$ $s$ $x$0). assert (class $s$ (rep $y$) = $y$). app class_rep.
  am. rww H25.
Qed.

The converse is true if $\phi$ is increasing, this is equivalent to the following condition.

Definition weak_order_compatibility $r$ $s$ :=
preorder $r$ & is_equivalence $s$ & substrate $s$ = substrate $r$ &
forall $x$ $y$ $x'$, gle $r$ $x$ $y$ -> related $s$ $x$ $x'$ -> exists $y'$,
  (related $s$ $y$ $y'$ & gle $r$ $x'$ $y'$).

We show that strong compatibility implies weak compatibility (assume $x \leq y$ and $x \equiv x'$ (mod $S$) in $E$, we can take $y' = y$ in $y \equiv y'$ (mod $S$) and $x' \leq y'$ since $y$ is in the substrate of $S$).

Lemma strong_order_compatibility: forall $r$ $s$,
  preorder $r$ -> is_equivalence $s$ -> substrate $s$ = substrate $r$ ->
  (forall $x$ $x'$ $y$, gle $r$ $x$ $y$ -> related $s$ $x$ $x'$ -> gle $r$ $x'$ $y'$) ->
weak_order_compatibility r s.
Proof. ir. red. ee. am. am. am. ir. exists y. split. app reflexivity_e.
   rw H1. app (inc_arg2_substrate H3). ap (H2 _ _ H3 H4).
Qed.

Let's show that the canonical projection is increasing.

Lemma compatibility_proj_increasing: forall r s,
   is_equivalence s -> preorder r -> substrate s = substrate r ->
   weak_order_compatibility r s =
   increasing_pre (canon_proj s) r (quotient_order r s).
Proof. ir. cp (quotient_is_preorder H H0 H1). uf increasing_pre. simpl.
   wr H1. uf increasing_map. rww substrate_quotient_order.
   assert (Ha: is_graph s). nin H; am.
   ap iff_eq; ir; ee; try tv. app function_canon_proj.
   ir. rw quotient_order_pr. uf quotient_order_r. aw.
   ee. gprops. gprops.
   ir. red in H3. ee. bwi H7.
   nin (H10 _ _ H6 H7). exists x1. bw. am.
   red. ee;try am. ir.
   assert (inc x (substrate s)). rw H1. app (inc_arg1_substrate H9).
   assert (inc y (substrate s)). rw H1. app (inc_arg2_substrate H9).
   cp (H8 _ _ H11 H12 H9). rwi quotient_order_pr H13. awi H1.
   uf quotient_order_r H13.
   ee. wri inc_class H10. awi H15; try am. nin (H15 _ H10). nin H16. bwi H16.
   exists x0. auto. am. am.

(c) Let \( E_1 \) and \( E_2 \) be two preordered sets. Show that if \( S_1 \) is the equivalence relation \( \text{pr}_1 z = \text{pr}_1 z' \) on \( E_1 \times E_2 \), then \( S_1 \) is weakly compatible in \( z \) and \( t \) with the product preorder relation \( z \leq t \) on \( E_1 \times E_2 \) (but is not usually compatible with this relation in \( z \) or \( t \) separately); moreover if \( \phi_1 \) is the canonical mapping of \( E_1 \times E_2 \) onto \( (E_1 \times E_2)/S_1 \), and if \( \text{pr}_1 = f_1 \circ \phi_1 \) is the canonical decomposition of \( \text{pr}_1 \) with respect to the equivalence relation \( S_1 \), then \( f_1 \) is an isomorphism of \( (E_1 \times E_2)/S_1 \) into \( E_1 \).

We show here weak compatibility of the product of two preorder relations on \( E_1 \) and \( E_2 \) and the equivalence \( S_1 \) in \( E_1 \times E_2 \) defined by \( \text{pr}_1 z = \text{pr}_1 z' \).

Lemma exercise1_2c1: forall r1 r2,
   preorder r1 -> preorder r2 ->
   weak_order_compatibility (product2_order r1 r2)
   (first_proj_equivalence (substrate r1) (substrate r2)).
Proof. ir. red. ee. app preorder_product2_order.
   ap equivalence_first_proj. rw substrate_first_proj_equivalence.
   rw substrate_preorder_product2_order. ir.
   rwi product2_order_pr H1. red in H1. rwi first_proj_equivalence_related H2.
   ee. exists (J (P y) (Q x')).
   rw product2_order_pr. rw first_proj_equivalence_related. uf product2_order_r.
   aw. awi H5. awi H3. ee; fprops; try am. wr H4. wrr preorder_reflexivity.
Qed.

If \( S_1 \) is compatible with \( \leq \), then if \( x \leq x \) and if \( x \) and \( y \) are related by \( S_1 \), we have \( x \leq y \) or \( y \leq x \) (depending on whether \( S_1 \) is compatible with the first or second argument). Consider the case of the product order and the first projection. If we take \( x = (a, b) \) and \( y = (a, c) \), then \( x \leq y \) or \( y \leq x \), hence \( b \leq c \) or \( c \leq b \). This means that all elements in \( E_2 \) are related. Note that if \( E_1 \) is empty, the product is empty and the condition is vacuous.
Lemma exercise1_2c2: forall r1 r2,
let compatibility r s :=
  (forall x y, gle r x y -> related s x y -> gle r x y) in
preorder r1 -> preorder r2 -> nonempty (substrate r1) ->
compatibility (product2_order r1 r2)
(first Proj_equivalence (substrate r1) (substrate r2)) ->
r2 = coarse (substrate r2).
Proof. ir. assert (preorder (product2_order r1 r2)).
appl preorder_product2_order. set_extens. uf coarse.
assert (is_pair x). red in H0. ee. app H0. app product_inc.
appl inc_pr1_substrate. appl inc_pr2_substrate. uf x1 coarse H4.
rwi inc_product. red in H4. ee. ufi x1 H14. awi H14.
set (x1:= J y (Q x)). set (x2:= J y (P x)).
appl inc x (product (substrate r1) (substrate r2)). uf x1. fprops.
appl inc x2 (product (substrate r1) (substrate r2)). uf x2. fprops.
appl gle (product2_order r1 r2) x1 x1. wrr preorder_reflexivity.
rwi substrate_preorder_product2_order.
s what (s:=first Proj_equivalence (substrate r1) (substrate r2)).
appl related s x1 x2. uf s. rw first Proj_equivalence_related.
split. am. split. am. uf x1. uf x2. aw.
fold s in H2. cp (H2 __ __ H9 H10).
rwi product2_order_pr H11. red in H11. ee. ufi x1 H14; ufi x2 H14. awi H14.
red in H14. assert (J (P x) (Q x) = x). app pair_recov. wrr H15.
Qed.

Same proof, with definitions of x1 and x2 exchanged.

Lemma exercise1_2c3: forall r1 r2,
let compatibility r s :=
  (forall x y, gle r x y -> related s x y' -> gle r x y') in
preorder r1 -> preorder r2 -> nonempty (substrate r1) ->
compatibility (product2_order r1 r2)
(first Proj_equivalence (substrate r1) (substrate r2)) ->
r2 = coarse (substrate r2).
Proof. ... Qed.

We show that pr1 = f1 ◦ φ1 implies that f1 is an isomorphism; we first introduce the defi-
nition of a pre-order isomorphism. If E2 is empty, then pr1 is in general not surjective, thus
f1 is not surjective; this explains why we add the condition E2 ≠ ∅. If f1(x) = f1(y), where x
and y are the classes of x′ and y′, then pr1 x′ = pr1 y′, hence x′ ≡ y′ and x = y, so that f1 is
injective. With the same notations, f1(x) ≤ f1(y) if and only if pr1 x′ ≤ pr1 y′.

Definition preorder_isomorphism f r r' :=
(order r) & (order r') &
(bijective f) & (substrate r = source f) & (substrate r' = target f) &
(forall x y, inc x (source f) -> inc y (source f) ->
gle r x y = gle r' (W x f) (W y f)).

Lemma exercise1_2c4: forall r1 r2 f,
let s := (first Proj_equivalence (substrate r1) (substrate r2)) in
let r := product2_order r1 r2 in
is_function f -> source f = quotient s -> target f = (substrate r1) ->
preorder r1 -> preorder r2 -> nonempty (substrate r2) ->
compose f (canon_proj s) = (first Proj (product (substrate r1) (substrate r2)))
-> preorder_isomorphism f (quotient_order r s) r1.
Proof. ir. set (E1 := substrate r1) in *. set (E2 := substrate r2) in *.
assert (Ha: substrate r = product E1 E2). uf r.
rf substrate preorder product2 order.
assert (Hb: substrate s = product E1 E2). uf s.
rf substrate first proj equivalence.
assert (Hc: is equivalence s). uf s; app equivalence first proj.
assert (composable f (canon proj s)). red. ee. am. app function canon proj.
rr.
assert (Hd: preorder r). uf r. app preorder product2 order.
assert (source (canon proj s) = product E1 E2). rr.
red. ee. app quotient is preorder. rrw Ha. am. red. ee. red. ee. am. ir.
assert (inc x (quotient s)). wrr H0. cp (canon proj show surjective Hc H11).
assert (inc y (quotient s)). wrr H0. cp (canon proj show surjective Hc H13).
wr (related rep rep Hc H11 H13). uf s.
wr first proj equivalence related. ee. wr Hb. app inc rep substrate.
wr Hb. app inc rep substrate.
wri H12 H10. wri H14 H10. assert (inc (rep x) (source (canon proj s))).
assert (inc (rep y) (source (canon proj s))). rrw H7. wr Hb.
surjective proj6. rw H1. ir. nin H4. exists (W (J y y0) (canon proj s)).
assert (inc (J y y0) (source (canon proj s))). rrw H7. fprops.
ee. assert (source f = target (canon proj s)). rrw H10. app inc W target. app function canon proj. wr (W compose H6 H9).
rrw H5. wr W first proj. aw. fprops. fprops. sy; rrw substrate quotient order.
rrw Ha. sy. am. ir. set (u := W x f). set (v := W y f).
assert (inc x (quotient s)). wrr H0. cp (canon proj show surjective Hc H10).
assert (inc y (quotient s)). wrr H0. cp (canon proj show surjective Hc H12).
assert (inc (rep x) (source (canon proj s))).
assert (inc (rep y) (source (canon proj s))). rrw H7. wr Hb.
rrwi W first proj H14. rrwi W first proj H15. hr H14; hr H15.
rrw quotient order pr. uf quotient order r. app iff eq. ir. ee.
assert (inc (rep x) x). app (inc rep itself Hc H10). nin (H20 _ H21).
nin H22. ufi r H23. rr product2 order pr H23. ufi product2 order r H23. ee.
cc (is class pr Hc H22 H19). assert (inc x0 (substrate s)).
app (inc in quotient substrate Hc H22 H19). cp (related rep class Hc H28).
ir. ee. am. am. ir.
assert (inc (J v (Q x0)) (product (substrate r1) (substrate r2))). aw. ee.
fprops. rwi H7 H17. awi H17. ee. rwi H15.
cp (inc in quotient substrate Hc H19 H10). rwi Hb H20; awi H20. ee. am.
assert (inc x0 (product (substrate r1) (substrate r2))).
cp (inc in quotient substrate Hc H19 H10). rwi Hb H21. am.
exists (J v (Q x0)). ee. wr (class rep Hc H12). rrw inc class. uf s.
rw first proj equivalence related. ee. wr H7. am. am. sy. aw. nin Hc; am.
uf r. rr product2 order pr. red. ee. am. am. aw. rw H15.
assert (inc (rep x) x). app (inc rep itself Hc H10). cc (is class pr Hc H19 H10). assert (inc x0 (substrate s)).
app (inc in quotient substrate Hc H19 H10). cp (related rep class Hc H24).
av. red in H3. ee. red in H22. ee. aw. aw H24. awi H21; ee; am. fprops. wr H7.
fprops. wr H7.

RR n° 7150
(d) With the hypothesis of (a), suppose that \( E \) is an ordered set and that the following condition is satisfied:

\[ (C') \text{ The relations } x \leq y \leq z \text{ and } x \equiv z \pmod{S} \text{ in } E \text{ imply } x \equiv y \pmod{S}. \]

Show that \( R \mid x, y \) is then an order relation between \( X \) and \( Y \) in \( E/S \).

Definition quotient_order_axiom \( r s := \)

\[ \forall x y z, \text{gle} r x y \to \text{gle} r y z \to \text{related} s x z \to \text{related} s x y. \]

Lemma Exercise1_2d: \( \forall r s, \text{is_equivalence} s \to \text{order} r \to \text{substrate} s = \text{substrate} r \to \text{order} \left( \text{quotient_order} r s \right). \)

Proof. ir. assert (preorder \( r \)). red in \( H0 \). red. intuition.

\[ \text{cp \ (quotient_is_preorder} H H3 H1) \ . \ \text{red in} \ H4. \ \text{ee. red. ee. am. am. am. red. ee. am. ir. rwi quotient_order_pr} H7. \ \text{rwi quotient_order_pr} H8. \]

\[ \text{red in} \ H7. \ \text{red in} \ H8. \ \text{ee. set_extens. nin \ (H12 _ H13). ee.} \]

\[ \text{nin \ (H10 _ H14). ee. assert (related} s x0 x2). \ \text{rw in_class_related.} \]

\[ \text{exists} x. \ \text{ee. wr inc_quotient. am. am. am. red in} \ H2. \]

\[ \text{cp \ (H2 _ _ H15 H17 H18). cp \ (is_class_pr} H H14 H11). \ \text{rw H20.} \]

\[ \text{bw. app symmetryicty. nin} H; \ \text{am.} \]

\[ \text{nin \ (H10 _ H13). ee. nin \ (H12 _ H14). ee. assert (related} s x0 x2). \]

\[ \text{rw in_class_related. exists} y. \ \text{ee. wr inc_quotient. am. am. am. red in} \ H2. \]

\[ \text{cp \ (H2 _ _ H15 H17 H18). cp \ (is_class_pr} H H14 H7). \ \text{rw H20.} \]

\[ \text{bw. app symmetryicty. nin} H; \ \text{am.} \]

Qed.

(e) Give an example of a totally ordered set \( E \) with four elements and an equivalence relation \( S \) and \( E \) such that neither of the conditions \( (C) \) and \( (C') \) is satisfied, but such that \( E/S \) is an ordered set.

Assume that \( E \) is a totally ordered finite set, and consider two classes \( X \) and \( Y \); they have a greatest element \( x \) and \( y \). The condition \( x \leq y \) is equivalent to \( X \leq Y \), so that the quotient is totally ordered. Assume \( a < b < c \), \( S \) is such that \( a \) and \( c \) are related by \( S \), but no other pair of distinct pairs are related. Then \( (C') \) is false. In \( (C) \), take \( a \), \( b \) and \( c \) for \( x \), \( y \) and \( y' \). Since \( y \equiv y' \) implies \( y = y' \), condition \( (C) \) is false. This gives an example with three elements. But one can add a fourth one.

(f) Let \( E \) be an ordered set, let \( f \) be an increasing mapping of \( E \) into an ordered set \( F \), and let \( S \mid x, y \) be the equivalence relation \( f(x) = f(y) \) on \( E \). Then the condition \( (C') \) is satisfied.

Moreover the condition \( (C) \) is satisfied if and only if the relations \( x \leq y \) and \( f(x) = f(x') \) imply that there exists \( y' \in E \) such that \( x' \leq y' \) and \( f(y) = f(y') \). Let \( g = g \circ \phi \) be the canonical decomposition of \( f \). Then \( g \) is an isomorphism of \( E/S \) onto \( f(E) \) if and only if this condition is satisfied and, in addition, the relation \( f(x) \leq f(y) \) implies that there exists \( x', y' \) such that \( f(x) = f(x') \), \( f(y) = f(y') \), and \( x' \leq y' \).

Lemma Exercise1_2f1: \( \forall r r', f, \text{increasing_fun} f r r' \to \text{quotient_order_axiom} r \left( \text{eq_rel_associated} f \right). \)

Proof. ir. red. ir. red in \( H \). ee. cp (inc_arg1_substrate H1). rwi \( H5 H8. \)

\[ \text{rw related_ea. rwi related_ea} H2. \ \text{ee. am. am. cp \ (H7 _ _ H2 H8 H0).} \]

\[ \text{cp \ (H7 _ _ H8 H9 H1). simpl in H11. simpl in H12. rwi H10 H12.} \]

\[ \text{app \ (order_antisymmetry} H4 H11 H12). \ am. am. \]

Qed.
Lemma Exercise1_2f2: forall r r' f, increasing_fun f r r' ->
weak_order_compatibility r (eq_rel_associated f) =
(forall x y x', gle r x y -> inc x' (source f) -> \ W x f = \ W x' f ->
exists y', inc y' (source f) \& gle r x' y' \& \ W y f = \ W y' f).
Proof. ir. uf weak_order_compatibility. red in H. ee. ap iff_eq. ir. ee.
assert (related (eq_rel_associated f) x'). rw related_ea. ee.
wr H2. app (inc_arg1_substrate H6). am. am. am. nin (H11 _ _ _ H6 H12).
wri related_ea H13. ee. exists x0. intuition. am. ir. ee.
red in H0; red; ee;am. app equivalence_graph_ea. rw substrate_graph_ea.
sy; am. ir. wri related_ea H7. ee. nin (H5 _ _ _ H6 H8 H9). exists x0.
rw related_ea. intuition. wr H2. app (inc_arg2_substrate H6). am. am.
Qed.

The next point is straightforward, but a bit longish. The idea is the following. If X is in the
quotient, and if x stands for rep X, then g(X) = f(x). The equivalence relation is defined by
a \in X if and only if f(x) = f(a).

Lemma Exercise1_2f3: forall r r' f g,
let CC:= forall x y x', gle r x y -> inc x' (source f) -> \ W x f = \ W x' f ->
exists y', inc y' (source f) \& gle r x' y' \& \ W y f = \ W y' f in
let DD:= forall x y, inc x (source f) -> inc y (source f) ->
gle r' (W x f) (W y f) -> exists x', exists y',
\ W x f = \ W x' f \& \ W y f = \ W y' f \& gle r x' y' in
increasing_fun f r r' ->
composable g (canon_proj (eq_rel_associated f)) ->
f = compose g (canon_proj (eq_rel_associated f)) ->
order_morphism g (quotient_order r (eq_rel_associated f)) r' = (CC & DD).
Proof. ir. cp (Exercise1_2f1 H). rename H2 into Hc.
red in H. ee. set (s:= eq_rel_associated f) in *.
assert (Ha:is_equivalence s). uf s. app equivalence_graph_ea.
assert (Hb: substrate s = substrate r). uf s. sy; rww substrate_graph_ea.
assert (Hd:preorder r). red in H2; red; intuition.
assert (He: forall x, inc x (quotient s) ->( inc (rep x) (source f) \&
\ W (rep x) f = W x g)). ir. cp (inc_rep_substrate Ha H7). split. wr H4.
wrr Hb. cp (W (canon_proj Ha H8)). rrvi class_rep H9.
assert (W (W (rep x) (canon_proj s)) g = W x g). rrw H9. wri W-compose H10.
wri H1 H10. am. am.
assert (Hf:forall x a, inc x (quotient s) ->
inc a x = (inc (rep x)(source f) \& inc a(source f) \& W (rep x) f = W a f)).
ir. ap iff_eq. ir. cp (related_rep_in_class Ha H7 H8). ufi s H9.
wri related_ea H9. am. am. ir. wr (class_rep Ha H7). bw.
uf s. rw related_ea. am. am. red in Ha; ee; am.

Assume that g(a) \leq g(b) implies a \leq b. We have: if x and y in E, X and Y are their equiva-
lence classes, then f(x) \leq f(y) implies X \leq Y. Expanding the last relation, we get: if x' is in
the class of x, there exists y' such that f(y) = f(y') and x' \leq y'.

app iff_eq. ir.
assert (forall x y x', inc x (source f) -> inc y (source f) ->
gle r' (W x f) (W y f) -> inc x' (class s x) ->
exists y', inc y' (source f) \& gle r x' y' \& \ W y f = \ W y' f).
ir. assert(inc x (substrate s)). rrw Hb. rrw H4.
assert (inc x (class s x)). app inc_itself_class.
assert (inc x (class s x) (quotient s)). gpops.
It is now easy to show that if $g$ is a morphism, then the two conditions are true.

We now show the converse.

Let $I$ be an ordered set and let $(E_\iota)_{\iota \in I}$ be a family of non-empty ordered sets indexed by $I$.

(a) Let $F$ be the sum (Chapter II, § 4, no. 8) of the family $(E_\iota)_{\iota \in I}$; for each $x \in F$, let $\lambda(x)$ be the index $\iota$ such that $x \in E_\iota$; and let $G$ be the graph consisting of all the pairs $(x, y) \in F \times F$ such that either $\lambda(x) < \lambda(y)$ or else $\lambda(x) = \lambda(y)$ and $x \leq y$ in $E_{\lambda(x)}$. Show that $G$ is the graph of an
ordering on F. The set F endowed with this ordering is called the ordinal sum of the family 
\((E_i)_{i \in I}\) relative to the ordering on I and is denoted \(\sum_{i \in I} E_i\). Show that the equivalence relation 
corresponding to the partition \((E_i)_{i \in I}\) of F satisfies conditions (C) and (C’) of Exercise 2, and 
that the quotient ordered set (Exercise 2) is canonically isomorphic to I.

We have defined the ordinal sum in section 3.7 and shown that is an ordered set. We show here the claim of the last sentence.

Let’s consider three variables, \(r, f\) and \(g\). We define some quantities associated to them, 
prefixed by \(E13\). Assumption H1 says that \(f\) is a family of sets (the family \(E_i\)), \(r\) is an ordering 
on the index set, \(g\) is a family of orderings on \(E_i\). We shall denote the ordinal sum by \(F\) and its 
support (the disjoint union) by \(sF\) or \(\bar{F}\). The quantity \(\lambda\) will be the function \(\lambda\), i.e., the 
surjective function on \(\bar{F}\) defined by \(\lambda(x) = pr_2 x\). Finally \(S\) the equivalence associated to \(\lambda\). 
Assumption H2 says that the sets \(E_i\) are non-empty.

Section Exercise1_3a.
Variables \(r f g\): Set.
Definition \(E13_{\text{lam}} := \text{second_proj} (\text{disjoint_union} f)\).
Definition \(E13_S := \text{eq_rel_associated} (\text{second_proj} (\text{disjoint_union} f))\).
Definition \(E13_F := \text{ordinal_sum} r f g\).
Definition \(E13_{\text{sF}} := \text{disjoint_union} f\).
Definition \(E13_{\text{H1}} := \text{ordinal_sum_axioms} r f g\).
Definition \(E13_{\text{H2}} := \text{is_graph} f \& \) 
(forrall i, inc i (domain f) -> nonempty (V i f)).

We show, successively, that \(\bar{F}\) is a graph, that \(pr_2\) can be considered as a surjective function 
on \(F\), that its target is I if \(H2\) is true, and that it is an increasing function.

Lemma Exercise1_3a1: is_graph E13_{sF}.
Proof. ir. uf disjoint_union. uf disjoint_union_fam. red. ir. rwi unionb_rw H.
   nin H. nin H. bwi H0. awi H0. nin H0; am. bwi H. am.
Qed.

Lemma Exercise1_3a0: is_function E13_{lam}.
Proof. ir. uf E13_{lam}. app function_second_proj. ap Exercise1_3a1.
Qed.

Lemma Exercise1_3a2: surjective E13_{lam}.
Proof. ap surjective_pr6. ap Exercise1_3a0. cp Exercise1_3a1. uf E13_{lam}.
   simpl.
   uf disjoint_union. uf disjoint_union_fam. ir. awi H0. nin H0.
   exists (J x y). split. am. rw W_second_proj. aw. am. am. am.
Qed.

Lemma Exercise1_3a3: E13_{H2} -> domain f = target E13_{lam}.
Proof. ir. nin H. uf E13_{lam}. simpl.
   set_extens. nin (H0 _ H1). aw. exists y. uf disjoint_union.
   uf disjoint_union_fam.
   rw unionb_rw. exists x. bw. split. am. fprops. ap Exercise1_3a1.
   awi H1. nin H1. ufi disjoint_union H1. ufi disjoint_union_fam H1.
   rwi unionb_rw H1. nin H1. bwi H1. nin H1. awi H2. nin H2. nin H3.
   rww H4. nin H1. am. ap Exercise1_3a1.
Qed.

Lemma Exercise1_3a4: E13_{H1} -> E13_{H2} -> increasing_fun E13_{lam} E13_F r.
Proof. ir. red in H. cp H; red in H. red. ee. ap Exercise1_3a0.
uf E13_F. fprops. am. uf E13_F; uf E13_lam.
simpl. rw substrate_ordinal_sum. rw H2. app Exercise1_3a3.
red. uf E13_lam. simpl. ir. cp Exercise1_3a1.
nin H13; am. nin H13. rw H13. wrr order_reflexivity. rw H2.
cp (du_index_pr H9); ee; am. am.
Qed.

Consider now the “equivalence relation corresponding to the partition \((E_i)_i\) of \(F\).” The set \(\overline{F}\) is the union of \(f'\), the graph of \(i \rightarrow E_i \times \{i\}\), where \(f\) is the graph of \(i \rightarrow E_i\). Consider now a function \(f''\) whose graph is \(f'\). This function defines a partition. By abuse of notations, \(F\) is identified with \(\overline{F}, E_i \times \{i\}\) with \(E_i\), and \(f''\) with \(f'\). Let \(S'\) be the equivalence associated to \(f''\). We show here that \(x\) and \(y\) are related by \(S'\) (resp. \(S\)) if and only if \(x\) and \(y\) are in the disjoint union and \(\text{pr}_2 x = \text{pr}_2 y\). This shows \(S' = S\).

Definition disjoint_union_function f :=
corresp (domain f)(range (disjoint_union_fam f))(disjoint_union_fam f).

Lemma disjoint_union_function_pr:
is_function (disjoint_union_function f) &
graph (disjoint_union_function f) = (disjoint_union_fam f).
Proof. ir. uf disjoint_union_function. uf is_function. uf is_correspondence.
uf corr_axiom. simpl. assert (fgraph (disjoint_union_fam f)).
uf disjoint_union_fam. gprops. wri is_functional H. ee. am.
uf disjoint_union_fam. bw. fprops. fprops. am. uf disjoint_union_fam. bw. tv.
Qed.

Lemma Exercise1_3a5: forall x y, fgraph f ->
related (partition_relation (disjoint_union_function f) (disjoint_union f))
x y = (inc x E13_sF & inc y E13_sF & Q x = Q y).
Proof. ir. uf E13_sF. rename H into Ha. cp disjoint_union_function_pr. ee.
rw partition_relation_pr. uf in_same_coset. uf W. uf disjoint_union.
uf disjoint_union_function. simpl. uf disjoint_union_fam. ap iff_eq.
ir. nin H1. ee. rw unionb_rw. exists x0. split. bw. am. rw unionb_rw.
exists x0. split. bw. am. bwi H2. bwi H3. awi H2; awi H3. ee.
rw H7; rw H5; tv. am. am.
ir. ee. rwi unionb_rw H1. rwi unionb_rw H2. nin H1; nin H2. ee. bwi H1. bwi H2.
exists x0. split. am. split. am. assert (x0 = x1). bwi H5; bwi H4.
avi H5; avi H4. ee. rwi H9 H3. rwi H7 H3. am.
am. am. am. rww H6. am. rw H0. app partion_union_disjoint.
Qed.

Lemma Exercise1_3a6: forall x y,
related E13_S x y = (inc x E13_sF & inc y E13_sF & Q x = Q y).
Proof. ir. cp Exercise1_3a1. assert (is_function E13_lam). ap Exercise1_3a0.
uf E13_S. rw related_eq. simpl.
app iff_eq. ir. nin H1; nin H2. rwi W_second_proj H3.
rwi W_second_proj H3. intuition. ir. ee; try am.
rww W_second_proj. rww W_second_proj. am.
Qed.

We show that the classes of \(S\) are the sets \(E_i \times \{i\}\). If \(\phi\) is the canonical projection of \(\overline{F}\) on \(\overline{F}/S\), there exists a function \(g\) defined by \(\lambda = g \circ \phi\) (canonical decomposition) because of the surjectivity of \(\lambda\), it is unique. It is the function induced by \(\lambda\) by passing on the quotient. We
can restate it as: an element X of the quotient is of the form \( \iota \rightarrow E \times \{ \iota \} \), and \( g(\mathbf{X}) = \iota \). We show that \( g \) is a function, that \( g \circ \phi \) exists and that \( g \) is bijective.

**Lemma Exercise1_3a7:** is_equivalence E13_S.

**Proof.** uf E13_S. app equivalence_graph_ea. ap Exercise1_3a0. Qed.

**Lemma Exercise1_3a8:** forall a, E13_H2 ->
inc a (quotient E13_S) = exists i,
inc i (domain f) & a = product (V i f) (singleton i).

**Proof.** ir. cp Exercise1_3a7. rw inc_quotient. rww is_class_rw.
tv. app function_second_proj. ap Exercise1_3a1.
ap iff_eq. ir. ee. nin H2. assert (inc y (disjoint_union f)). wr H1. app H3.
cp (du_index_pr H5). ee. exists (Q y). ee. am. set_extens.

**Lemma Exercise1_3a9:** is_function(fun_on_quotient E13_S E13_lam).

**Proof.** ir. cp Exercise1_3a0. app function_foqc. ap Exercise1_3a7.
uf E13_S. rww substrate_graph_ea.
Qed.

**Lemma Exercise1_3a10:**
composable (fun_on_quotient E13_S E13_lam) (canon_proj E13_S).

**Proof.** red. ee. ap Exercise1_3a9. ap function_canon_proj. ap Exercise1_3a7.
tv.
Qed.

**Lemma Exercise1_3a11:**

**Proof.** ap (canonical_decomposition_surj2 Exercise1_3a2).
Qed.

**Lemma Exercise1_3a12:** forall x, E13_H2 ->
inc x (quotient E13_S) -> exists i,
inc i (domain f) & x = product (V i f) (singleton i) &
W x (fun_on_quotient E13_S E13_lam) = i.

**Proof.** ir. cp Exercise1_3a0. cp Exercise1_3a7.
assert (source E13_lam = substrate E13_S).
uf E13_S. sy; app substrate_graph_ea.
ap Exercise1_3a1. ufi E13_lam H3. simpl in H3. rw H3.
app inc_rep_substrate. rww W_foqc. wr H4.

RR n° 7150
Lemma Exercise1_3a13: E13_H2 -> bijective (fun_on_quotient E13_S E13_lam).
Proof. ir. cp Exercise1_3a9. red. split. split. am. simpl.
ir. nin (Exercise1_3a12 H H1). nin (Exercise1_3a12 H H2). ee.
rv H8; rw H6; wr H9; rv H3;rw H7. tv.
app surjective_pr6. impl. cp (Exercise1_3a3 H). simpl in H1.
wr H1; clear H1.
ir. set (a:=product (V y f) (singleton y)).
assert (inc a (quotient E13_S)). rw Exercise1_3a8. exists y. ee. am. tv. am.
exists a. split. am. cp (Exercise1_3a12 H H2). nin H3. ee. rw H5.
wr H8; wr H9; red; split; am.
app Exercise1_3a4. app Exercise1_3a10. app Exercise1_3a11.
cp Exercise1_3a13. red in H3. red. intuition.
Qed.

We apply Exercise 2f; the two conditions are easily satisfied. We deduced that \( g \) is an isomorphism on its image. Since we know that \( g \) is bijective, it is an order isomorphism between \( F/S \) and \( I \).

Lemma Exercise1_3a14: E13_H1 -> quotient_order_axiom E13_F E13_S.
Proof. ir. red. uf E13_F. uf E13_S. ir. assert (order (ordinal_sum r f g)).
red in H; fprops. rw Exercise1_3a6. rwi Exercise1_3a6 H2. awi H0. awi H1.
ee. am. am. nin H. nin H9. nin H7. cp (lt_lt_trans H H9 H7). nin H11.
Qed.

Lemma Exercise1_3a15: E13_H1 -> E13_H2 ->
order_isomorphism (fun_on_quotient E13_S E13_lam)
(quotient_order E13_F E13_S) r.
Proof. ir. cp Exercise1_3a1. assert (order (ordinal_sum r f g)). fprops.
assert (order_morphism (fun_on_quotient E13_S E13_lam)
(quotient_order E13_F (eq_rel_associated E13_lam)) r). rw Exercise1_2f3.
assert (source E13_lam = disjoint_union f). uf E13_lam. tv.
wr H3. uf E13_F. split. ir. awi H4. ee.
assert (W x E13_lam = Q x). uf E13_lam. rwi W_second_proj.
assert (W x' E13_lam = Q x'). uf E13_lam. rwi W_second_proj.
assert (W y E13_lam = Q y). uf E13_lam. rwi W_second_proj.
exists x'. ee. am. wr order_reflexivity. rwi substrate_ordinal_sum. am.
ir. awi H6. ee. exists x. nin (equal_or_not (W x E13_lam) (W y E13_lam)).
exists x. split. tv. split. sy. am. wr order_reflexivity.
wr substrate_ordinal_sum. am. exists y. ee. tv. tv. av. ee. am. am. left.
assert (W x E13_lam = Q x). uf E13_lam. rwi W_second_proj.
assert (W y E13_lam = Q y). uf E13_lam. rwi W_second_proj.
wr H8; wr H9; red; split; am.
app Exercise1_3a4. app Exercise1_3a10. app Exercise1_3a11.
cp Exercise1_3a13. red in H3. red. intuition.
Qed.
End Exercise1_3a.
(b) If the set \( I \) is the ordinal sum of a family \((I_\lambda)_{\lambda \in L}\) of ordered sets, where \( L \) is an ordered set, show that the ordered set \( \sum_{\iota \in I} E_\iota \) is canonically isomorphic to the ordinal sum \( \sum_{\lambda \in L} F_\lambda \) where \( F_\lambda = \sum_{\iota \in I_\lambda} E_\iota \) ("associativity of the ordinal sum"). If \( I \) is the linearly ordered set \([1,2]\), we write \( E_1 + E_2 \) for the ordinal sum of \( E_1 \) and \( E_2 \). Show that \( E_2 + E_1 \) and \( E_1 + E_2 \) are not necessarily isomorphic.

The associativity formula has been shown in the main text. Consider two ordered sets \( E_1 \) and \( E_2 \) that we identify as subsets of the sum \( E_1 + E_2 \). Let \( x \) be the greatest element of the sum \( E_1 + E_2 \). Assume \( E_2 \) not empty; thus \( y \in E_2 \). Since \( y \leq x \), we deduce \( x \in E_2 \). Obviously, for all \( z \in E_2 \) we have \( z \leq x \). Thus, we have shown: if the sum \( E_1 + E_2 \) has a greatest element, then \( E_2 \) has a greatest element. This shows that \( E_1 + E_2 \) is not always isomorphic to \( E_2 + E_1 \).

Lemma ordinal_sum2_order_greatest: forall r r' x, order r -> order r' -> nonempty (substrate r') -> greatest_element (ordinal_sum2 r r') x -> greatest_element r' (P x).
Proof. ir. nin H1. red in H2. nin H2.
assert (inc (J y (singleton emptyset)) (substrate (ordinal_sum2 r r'))).
 rw substrate_ordinal_sum2. rw canonical_du2_pr. split. fprops. right.
av. split. am. tv. am. am. cp (H3 _ H4).
 rwi substrate_ordinal_sum2 H2. rwi canonical_du2_pr H2. nin H2. nin H6.
nin H6. cp (related_ordinal_sum2_order_spec H H0 H6 H1).
 assert (x = J (P x) emptyset). app pair_extensionality. fprops. aw. aw.
wri H9 H8. elim (not_le_gt (order_ordinal_sum2 H H0) H5 H8).
ee. red. ee. am. ir.
 assert (inc (J x0 (singleton emptyset)) (substrate (ordinal_sum2 r r'))).
 rw substrate_ordinal_sum2. rw canonical_du2_pr. split. fprops. right.
av. split. am. tv. am. am. cp (H3 _ H9). rwi related_ordinal_sum2_order H10.
ee. nin H12. nin H12. awi H12. elim one_not_zero. am. nin H12. nin H12.
nin H13. awi H14. am. nin H12. awi H12. elim one_not_zero. am. am. am.
 am. am.
Qed.

(c) An ordinal sum \( \sum_{\iota \in I} E_\iota \) is right directed if and only if \( I \) is right directed and \( E_\omega \) is right directed for each \( \omega \) of \( I \).

(d) An ordinal sum \( \sum_{\iota \in I} E_\iota \) is totally ordered if and only if \( I \) and each \( E_\iota \) is totally ordered.

(e) An ordinal sum \( \sum_{\iota \in I} E_\iota \) is a lattice if and only if the following conditions are satisfied:

(I) The set \( I \) is a lattice, and for each pair \((\lambda, \mu)\) of non-comparable indices in \( I \), \( E_{\sup(\lambda, \mu)} \) (resp. \( E_{\inf(\lambda, \mu)} \)) has a least (resp. greatest) element.

(II) For each \( \alpha \in I \) and each pair \((x, y)\) of elements of \( E_\alpha \) such that the set \( \{x, y\} \) is bounded above (resp. bounded below) in \( E_\alpha \), the set \( \{x, y\} \) has a least upper bound (resp. greatest lower bound) in \( E_\alpha \).

(III) For each \( \alpha \in I \) such that \( E_\alpha \) contains a set of two elements which has no upper bound (resp. no lower bound) in \( E_\alpha \), the set of indices \( \lambda \in I \) such that \( \lambda > \alpha \) (resp. \( \lambda < \alpha \)) has a least element (resp. a greatest element) \( \beta \), and \( E_\beta \) has a least element (resp. greatest element).

The French edition corrects point (c) as: “il faut et il suffit que \( I \) soit filtrant à droite et que, pour tout élément maximal \( \omega \) de \( E \), \( E_\omega \) soit filtrant à droite.” This can be translated as:

RR n° 7150
An ordinal sum $\sum_{i \in I} E_i$ is right directed if and only if $I$ is right directed and $E_\omega$ is right directed for each maximal element $\omega$ of $I$.

The proof is as follows. We identify $E_k$ with a subset of the disjoint union. Assume the sum directed. For every pair of indices $i$ and $j$, there is $x \in E_i$ and $y \in E_j$, and if $z \in E_k$ is an upper bound for $x$ and $y$, then $k$ is an upper bound for $i$ and $j$. Let $k$ be a maximal index, $x$ and $y$ in $E_k$. Every upper bound of $x$ and $y$ in the sum must be in $E_k$. Conversely, let $x \in E_i$ and $y \in E_j$ be in the disjoint union; assume $I$ right directed, so that there is $k \in I$ with $i \leq k$ and $j \leq k$. If $k$ is one of $i$ and $j$, but not both, then $x < y$ or $y < x$. If $i < k$ and $j < k$, there is $z \in E_k$ with $x < z$ and $y < z$. If $k$ is not maximal, there is $k'$ with $k < k'$, and the same conclusion holds. Finally, if $i = j = k$ and $k$ is maximal, we have an upper bound since $E_k$ is right directed.

Lemma directed_ordinal_sum_order: forall r f g, ordinal_sum_axioms1 r f g -> right_directed (ordinal_sum r f g) = (right_directed r & forall i, maximal_element r i -> right_directed (V i g)).
Proof. ir. red in H. ee. cp H. red in H1. ee. ap iff_eq. ir. rwi right_directed_pr H8. awi H8. ee. rw right_directed_pr. ee. am. ir. rwi H2 H10; rwi H2 H11. nin (H0 _ H10). nin (H0 _ H11). cp (inc_disjoint_union H10 H12). cp (inc_disjoint_union H11 H13). nin (H9 _ H14 H15). ee. exists (Q x0). cp (du_index_pr H16). ee. rw H2. am. cp (related_ordinal_sum_order_id H H17). avi H22. am. cp (related_ordinal_sum_order_id H H18). avi H22. am. ee. ir. rw right_directed_pr. red in H10. ee. app H6. wrr H2. ir. rwi H2 H10. rwi (H7 _ H10) H12. cp (inc_disjoint_union H10 H12). rwi (H7 _ H10) H13. cp (inc_disjoint_union H10 H13). nin (H9 _ H14 H15). ee. cp (related_ordinal_sum_order_id H H17). avi H19. cp (du_index_pr H16). ee. rwi H2 H11. cp (H11 _ H20 H19). avi H17; avi H18. ee. exists (P x0). ee. rww H7. wrr H23. nin H27. nin H27. elim H28. sy; am. ee. am. nin H25. nin H25. elim H28. sy; am. ee; am. am. am. am. am. ir. ee. rwi right_directed_pr H8. ee. rw right_directed_pr. ee. fprops. aw. ir. cp (du_index_pr H11). cp (du_index_pr H12). ee. rwi H2 H10. nin (H10 _ H13 H14). ee. nin (equal_or_not (Q x) x0). nin (equal_or_not (Q y) x0). nin (p_or_not_p (maximal_element r x0)). cp (H9 _ H24). rwi right_directed_pr H25. ee. rwi H7 H26. rwi H22 H17; rwi H23 H15. nin (H26 _ H17 H15). ee. exists (J x1 x0). ee. app inc_disjoint_union. aw. ee. am. app inc_disjoint_union. right. ee. am. rww H22. aw. ee. am. app inc_disjoint_union. right. ee. am. rww H23. am. ufi maximal_element H24. assert (exists x1, inc x1 (substrate r) & glt r x0 x1). app exists_proof. red. ir. elim H24. ee. rww H2. ir. nin (equal_or_not x0 x1). sy; am. elim (H25 x1). ee. am. red; ee; am. nin H25. ee. rwi H2 H25. nin (H0 _ H25). cp (inc_disjoint_union H25 H27). exists (J y0 x1). ee. am. aw. ee. am. am. left. app (leq_lt_trans H8 H20 H26). aw. ee. am. am. left. app (leq_lt_trans H8 H21 H26). exists x. ee. am. wrr order_reflexivity. aw. fprops. aw. ee. am. am. left. rw H22. red. ee. am. am. nin (equal_or_not (Q y) x0). exists y. ee. am. aw. fprops. aw. ee. am. am. left. rw H23. red. ee. am. am. wrr order_reflexivity. aw. fprops. nin (H0 _ H19). cp (inc_disjoint_union H19 H24). exists (J y0 x0). ee. am. aw. ee. am. am. left. red; ee; am. aw. ee. am. am. left. red. ee; am. Qed.
We show that if an ordinal sum is a lattice, so is the index set $I$. The idea is the following.

Consider two indices $a$ and $b$. If they are comparable, there is a supremum. Otherwise, let $x \in E_a$, $y \in E_b$, and $z = \sup(x, y)$. We have $z \in E_c$, and $c$ is an upper bound of $a$ and $b$. Let $d$ be another upper bound. Since $a$ and $b$ are incomparable, we have $a < d$ and $b < d$. For every $t \in E_d$ we have $x < t$ and $y < t$ hence $z \leq t$ hence $c \leq d$.

Lemma ordinal_sum_pr1: forall $r f g$,
\[
\text{ordinal_sum_axioms1} \ r f g \quad\Rightarrow\quad
\forall i, \text{inc} i (\text{domain} f) \rightarrow \exists y, \text{inc} y (V i f) \&
\text{inc} (J y i) (\text{substrate} (\text{ordinal_sum} r f g)).
\]

Proof. ir. red in H. ee. nin (H1 _ H0). exists y. ee. am.
\text{cp (inc_disjoint_union H0 H2)}. aw.
Qed.

Lemma ordinal_sum_lattice1: forall $r f g$,
\[
\text{ordinal_sum_axioms1} \ r f g \rightarrow
\text{lattice} (\text{ordinal_sum} r f g) \rightarrow (\text{lattice} r).
\]

Proof. ir. set (F:= ordinal_sum r f g) in H0.
assert (Ha:forall i, \text{inc} i (\text{domain} f) \rightarrow \exists y, \text{inc} y (V i f) \&
\text{inc} (J y i) (\text{substrate} F)). ir. uf F. app ordinal_sum_pr1. nin H.
assert (Hb:substrate F = disjoint_union f). uf F. av.
red. ee. am. ir. rwi H4 H10; rwi H4 H11. nin (Ha _ H10). nin (Ha _ H11).
ee. cp (lattice_sup_pr H0 H15 H14). fold F in H16. ee. red.
nin (p_or_not_p (gle r x y)). exists y. app sup_comparable. ir.
nin (p_or_not_p (gle r y x)). exists x. rw doubleton_symm.
app sup_comparable. ir.
set (z:= (sup F (J x0 x) (J x1 y))) in *. cp (inc_arg2_substrate H16).
rwi Hb H21. cp (du_index_pr H21). ee. exists (Q z).
app least_upper_bound_doubleton. ufi F H16.

Qed.
With the same notations as before, assume that \( a \) and \( b \) cannot be compared, let \( x \in A_a \), \( y \in E_b \) and \( z \in E_c = \text{sup}(x, y) \). Then \( c = \text{sup}(a, b) \). Every \( z' \) in \( E_c \) is an upper bound of \( x \) and \( y \). Hence \( \text{sup}(x, y) \) is the smallest element of \( E_c \).

**Lemma ordinal_sum_lattice2:** forall \( r \ f \ g \),  
\[
\text{ordinal_sum_axioms1} \ r \ f \ g \rightarrow \\
\text{lattice (ordinal_sum r f g)} \rightarrow \\
(\text{forall i j, inc i (domain f) \rightarrow inc j (domain f) \rightarrow} \\
\text{gle r i j \lor gle r j i \lor (exists u, exists v,} \\
\text{least_element (V (sup r i j) g) u \&} \\
\text{greatest_element (V (inf r i j) g) v)))
\]

**Proof.** ir. cp (ordinal_sum_lattice1 H H0). set \((F := \text{ordinal_sum r f g})\) in H0. assert \((\text{Ha :forall i, inc i (domain f) \rightarrow exists y, inc y (V i f) \&} \\
\text{inc (J y i) (substrate F))})\). ir. uf F. app ordinal_sum_pr1. nin H.
assert (order F). uf. fprops. cp H; red in H;ee.
nin (p_or_not_p (gle r i j)). ir. left. am. ir.
nin (p_or_not_p (gle r j i)). ir. right. left. am. ir. right. right.
nin (Ha _ H1). nin (Ha _ H2). ee.
cp (lattice_sup_pr H0 H18 H17). cp (lattice_inf_pr H0 H18 H17).
set \( (A := \text{inf F (J x i) (J x0 j)}) \) in H20. set \( (a := \text{sup r i j}) \).
set \( (B := \text{sup F (J x i) (J x0 j)}) \) in H19. set \( (b := \text{sup r i j}) \).
lee.
wri H7 H1. wri H7 H2. cp (lattice_inf_pr H3 H1 H2). fold a in H25. ee.
cp (lattice_sup_pr H3 H1 H2). fold b in H28. ee.
assert (Hc:Q A = a).
assert (gle r (Q A) a). ufi F H20. cp (related_ordinal_sum_order_id H6 H20).
app H27. cp (inc_arg1_substrate H25). wri H7 H32. nin (Ha _ H32). ee.
assert (gle F (J x1 a) (J x i)). uf F. aw. ee. wrr Hb. wrr Hb. left.
red. ee. am. red. ir. wri H35 H26. elim H13. am.
assert (gle F (J x i) (J x0 j)). uf F. aw. ee. wrr Hb. wrr Hb. left.
red. ee. am. red. ir. wri H36 H25. elim H14. am.
cp (H22 _ H35 H36). uf F. cp (related_ordinal_sum_order_id H6 H37).
awei H38. ap (order_antisymmetry H H31 H38).
assert (Hd:Q B = b).
assert (gle r b (Q B)). ufi F H19. cp (related_ordinal_sum_order_id H6 H19).
ufi F H23. cp (related_ordinal_sum_order_id H6 H23). awi H31. awi H32.
app H30. cp (inc_arg2_substrate H28). wri H7 H32. nin (Ha _ H32). ee.
assert (gle F (J x i) (J x1 b)). uf F. aw. ee. wrr Hb. wrr Hb. left.
red. ee. am. red. ir. wri H35 H29. elim H14. am.
assert (gle F (J x0 j) (J x1 b)). uf F. av. ee. wrr Hb. wrr Hb. left.
red. ee. am. red. ir. wri H36 H28. elim H13. am.
cp (H24 _ H35 H36). uf F. cp (related_ordinal_sum_order_id H6 H37).
awei H38. ap (order_antisymmetry H H31 H38).
assert (Hc:Q B = b).
awei (H12 _ H32) H33. wri Hb H33.
cp (inc_arg1_substrate H21). wri Hb H35. cp (du_index_pr H35). ee.
red. ee. am. ir. wrii H12 H39.
assert (inc (J x1 b) (disjoint_union f)). app inc_disjoint_union. wrr Hd.
assert (gle F (J x i) (J x1 b)). uf F. aw. ee. wrr Hb. am. left.
red. ee. am. red. ir. wri H41 H29. elim H14. am.
assert (gle F (J x0 j) (J x1 b)). uf F. av. ee. wrr Hb. am. left.
red. ee. am. red. ir. wri H42 H28. elim H13. am.
cp (H24 _ H41 H42). ufi F H43. awi H43. ee. nin H45. red in H45. ee.
Assume $a = b$ and $t$ is an upper bound for $x$ and $y$ in $E_a$. Then $z \leq t$, thus $c \leq a$, hence $a = c$. This means $z \in E_a$, so that $x$ and $y$ have a least upper bound in $E_a$.

Lemma ordinal_sum_lattice3: forall $r \ f \ g \ i \ x \ y \ t$,
ordinal_sum_axioms1 $r \ f \ g$ -> lattice (ordinal_sum $r \ f \ g$) ->
inc $i$ (domain $f$) -> gle ($V \ i \ g$) $x \ t$ -> gle ($V \ i \ g$) $y \ t$ ->
has_supremum ($V \ i \ g$) (doubleton $x \ y$).
Proof. ir. set (F:= ordinal_sum $r \ f \ g$) in H0.
assert (Ha:forall $i$, inc $i$ (domain $f$) -> exists $y$, inc $y$ ($V \ i \ f$) &
inc ($J \ y \ i$) (substrate F)). ir. uf F. app ordinal_sum_pr1. nin H.
assert (order F). uf F. fprops. cp H; red in H;ee.
assert (Hb: substrate F = disjoint_union $f$). uf F. av.
cp (inc_arg1_substrate H2). cp (inc_arg2_substrate H2).
cp (inc_arg1_substrate H3).
assert (inc ($J \ x \ i$) (substrate F)). uf F. av. app inc_disjoint_union. wrr H12.
assert (inc ($J \ y \ i$) (substrate F)). uf F. av. app inc_disjoint_union. wrr H12.
assert (inc ($J \ t \ i$) (substrate F)). uf F. av. app inc_disjoint_union. wrr H12.
cp (lattice_sup_pr H0 H17 H16). ee.
assert (gle F ($J \ y \ i$) ($J \ t \ i$)). uf F. av. ee. wrr Hb. wrr Hb. right. ee. tv.
am. assert (gle F ($J \ x \ i$) ($J \ t \ i$)). uf F. av. ee. wrr Hb. wrr Hb. right.
ee. tv. am. cp (H21 _ H22 H23). set (z:= sup F ($J \ y \ i$) ($J \ x \ i$)) in *.
cp (related_ordinal_sum_order_id H6 H19). awi H25.
cp (order_antisymmetry H H25 H26).
exists (P z). ap least_upper_bound_doubleton. app H11.
ufi F H20. awi H20. ee. nin H29. red in H29. nin H29. elim H30. am. ee;am.
am. ufi F H19. awi H19. ee. nin H29. red in H29. nin H29. elim H30. am. ee;am. am. ir.
assert (inc ($J \ t0 \ i$) (substrate F)). uf F. av. app inc_disjoint_union.
wrr H12. cp (inc_arg2_substrate H28). am.
assert (gle F ($J \ y \ i$) ($J \ t0 \ i$)). uf F. av. ee. wrr Hb. wrr Hb. right. ee. tv.
am. assert (gle F ($J \ x \ i$) ($J \ t0 \ i$)). uf F. av. ee. wrr Hb. wrr Hb. right.
ee. tv. am. cp (H21 _ H31 H32). ufi F H33. awi H33. ee. nin H35.
red in H35. ee. elim H36. sy; am. ee. rwi H35 H36. am. am.
Qed.

Lemma ordinal_sum_lattice4: forall $r \ f \ g \ i \ x \ y \ t$,
ordinal_sum_axioms1 $r \ f \ g$ -> lattice (ordinal_sum $r \ f \ g$) ->
inc $i$ (domain $f$) -> gle ($V \ i \ g$) $t \ x$ -> gle ($V \ i \ g$) $t \ y$ ->
has_infimum ($V \ i \ g$) (doubleton $x \ y$).
Proof. ir. set (F:= ordinal_sum $r \ f \ g$) in H0.
assert (Ha:forall $i$, inc $i$ (domain $f$) -> exists $y$, inc $y$ ($V \ i \ f$) &
inc ($J \ y \ i$) (substrate F)). ir. uf F. app ordinal_sum_pr1. nin H.
assert (order F). uf F. fprops. cp H; red in H;ee.
assert (Hb: substrate F = disjoint_union $f$). uf F. av.

José Grimm

Lemma ordinal_sum_lattice5: forall r f g i x y,
ordinal_sum_axioms1 r f g -> lattice (ordinal_sum r f g) ->
inc i (domain f) -> inc x (V i f) -> inc y (V i f) ->
(exists j, inc j (domain f) & least_element (induced_order r (Zo (domain f) (fun k=> glt r i k))) j &
exists z, least_element (V j g) z).
Proof. ir. set (F:= ordinal_sum r f g) in H0.
assert (Ha:forall i, inc i (domain f) -> exists y, inc y (V i f) &
inc (J y i) (substrate F)). ir. uf F. app ordinal_sum_pr1. nin H.
assert (order F). uf F. fprops. cp H; red in H;ee.
assert (Hb: substrate F = disjoint_union f). uf F. aw.
assert (inc (J y i) (substrate F)). uf F. aw. app inc_disjoint_union.
assert (inc (J y i) (substrate F)). uf F. aw. app inc_disjoint_union.
cp (lattice_sup_pr H0 H14 H15). ee. set (Z:=sup F (J x i) (J y i)) in *.
ufi F H16. ufi F H17. awi H16; awi H17. ee.
assert (inc (Q Z) (domain f)). cp (du_index_pr H21). ee. am.
assert (glt r i (Q Z)). nin H22. am. nin H20. am. ee.
cp (du_index_pr H21). ee. wri H20 H27. elim (H4 _ H27). ee; am.
assert (sub (Zo (domain f) (fun k => glt r i k)) (substrate r)).
red. ir. Ztac. red in H27. ee. app (inc_arg2_substrate H27).
clear H26. aw. nin (Ha _ H27). ee.
assert (glt F (J x i) (J x1 x0)). uf F. aw. ee. am. wrr Hb. left. am.
assert (gle F (J y i) (J x1 x0)). uf F. aw. ee. am. wrr Hb. left. am.
cp (H18 _ H30 H31). cp (relatedOrdinal_sum_order_id H7 H32). awi H33. am.
cp (du_index_pr H19). ee. am. ir. rwi H13 H26.

Assume again $a = b$, but now, suppose no upper bound for $x$ and $y$ exists in $E_a$. Then the interval $[a,c[$ is empty and $z$ is the least element of $E_c$. The first condition can be restated as: $c$ is the least element of $[a, a[$.

Lemma ordinal_sum_lattice5: forall r f g i x y,
ordinal_sum_axioms1 r f g -> lattice (ordinal_sum r f g) ->
inc i (domain f) -> inc x (V i f) -> inc y (V i f) ->
(exists j, inc j (domain f) &
least_element (induced_order r (Zo (domain f) (fun k=> glt r i k))) j &
exists z, least_element (V j g) z).
Proof. ir. set (F:= ordinal_sum r f g) in H0.
assert (Ha:forall i, inc i (domain f) -> exists y, inc y (V i f) &
inc (J y i) (substrate F)). ir. uf F. app ordinal_sum_pr1. nin H.
assert (order F). uf F. fprops. cp H; red in H;ee.
assert (Hb: substrate F = disjoint_union f). uf F. aw.
assert (inc (J y i) (substrate F)). uf F. aw. app inc_disjoint_union.
assert (inc (J y i) (substrate F)). uf F. aw. app inc_disjoint_union.
cp (lattice_sup_pr H0 H14 H15). ee. set (Z:=sup F (J x i) (J y i)) in *.
ufi F H16. ufi F H17. awi H16; awi H17. ee.
assert (inc (Q Z) (domain f)). cp (du_index_pr H21). ee. am.
assert (glt r i (Q Z)). nin H22. am. nin H20. am. ee.
cp (du_index_pr H21). ee. wri H20 H27. elim (H4 _ H27). ee; am.
assert (sub (Zo (domain f) (fun k => glt r i k)) (substrate r)).
red. ir. Ztac. red in H27. ee. app (inc_arg2_substrate H27).
clear H26. aw. nin (Ha _ H27). ee.
assert (glt F (J x i) (J x1 x0)). uf F. aw. ee. am. wrr Hb. left. am.
assert (gle F (J y i) (J x1 x0)). uf F. aw. ee. am. wrr Hb. left. am.
cp (H18 _ H30 H31). cp (relatedOrdinal_sum_order_id H7 H32). awi H33. am.
cp (du_index_pr H19). ee. am. ir. rwi H13 H26.
assert (inc (J x0 (Q Z)) (disjoint_union f)). app inc_disjoint_union.
assert (gle F (J x i) (J x0 (Q Z))). uf F. aw. ee. am. am. left. am.
assert (gle F (J y i) (J x0 (Q Z))). uf F. aw. ee. am. am. left. am.
cp (H18 _ H28 H29). ufi F H30. avi H30. ee. nin H32. red in H32. ee.
elim H33. tv. ee. am. am. am. am. am. am.
Qed.

Lemma ordinal_sum_lattice6: forall r f g i x y,
  ordinal_sum_axioms1 r f g ->
  lattice (ordinal_sum r f g) ->
  inc i (domain f) ->
  inc x (V i f) ->
  inc y (V i f) ->
  (forall t, inc t (V i f) ->
   ~ (gle (V i g) t x & gle (V i g) t y)) ->
  exists j, inc j (domain f) &
  greatest_element (induced_order r (Zo (domain f) (fun k=> glt r k i))) j &
  exists z, greatest_element (V j g) z.
Proof. ir. set (F:= ordinal_sum r f g) in H0.
assert (Ha:forall i, inc i (domain f) ->
  exists y, inc y (V i f) &
  inc (J y i) (substrate F)). ir. uf F. app ordinal_sum_pr1. nin H.
assert (order F). uf F. fprops. cp H; red in H; ee.
assert (Hb: substrate F = disjoint_union f). uf F. av.
assert (inc (J x i) (substrate F)). uf F. av. app inc_disjoint_union.
assert (inc (J y i) (substrate F)). uf F. av. app inc_disjoint_union.
cp (lattice_inf_pr H0 H14 H15). ee. set (Z:=inf F (J x i) (J y i)) in *.
ufi F H16. ufi F H17. avi H16; avi H17. ee.
assert (inc (Q Z) (domain f)). cp (du_index_pr H16). ee. am.
assert (gle r (Q Z) i). nin H22. am. nin H20. am. ee.
cp (du_index_pr H16). ee. wri H20 H27. elim (H4 _ H27). wr H22. ee; am.
assert (sub (Zo (domain f) (fun k => glt r k i)) (substrate r)).
red. ir. Ztac. red in H27. ee. app (inc_arg1_substrate H27).
clear H26. aw. nin (Ha _ H27). ee.
assert (gle F (J x1 x0) (J x i)). uf F. av. ee. wr Hb. am. left. am.
assert (gle F (J x1 x0) (J y i)). uf F. av. ee. wr Hb. am. left. am.
cp (H18 _ H30 H31). cp (related_ordinal_sum_order_id H7 H32). avi H33. am.
assert (inc (J x0 (Q Z)) (disjoint_union f)). app inc_disjoint_union.
assert (gle F (J x0 (Q Z))) (J x i)). uf F. av. ee. am. am. left. am.
assert (gle F (J x0 (Q Z))) (J y i)). uf F. av. ee. am. am. left. am.
cp (H18 _ H28 H29). ufi F H30. avi H30. ee. nin H32. red in H32. ee.
elim H33. tv. ee. am. am. am. am. am.
Qed.

We are now ready for the main result.

Lemma ordinal_sum_lattice: forall r f g,
  ordinal_sum_axioms r f g ->
  lattice (ordinal_sum r f g) =
  ((lattice r) k
  (forall i j, inc i (domain f) -> inc j (domain f) ->
   (gle r i j /
    gle r j i /
    (exists u, exists v,
     least_element (V (sup r i j) g) u &
     greatest_element (V (inf r i j) g) v)) k
   (forall i x y t, inc i (domain f) ->
    gle (V i g) x t -> gle (V i g) y t ->
    has_supremum (V i g) (doubleton x y)) &
   (forall i x y t, inc i (domain f) ->
    gle (V i g) t x -> gle (V i g) t y ->
    has_inifimum (V i g) (doubleton x y)) &

RR n° 7150
(forall i x y,
  inc i (domain f) -> inc x (V i f) -> inc y (V i f) ->
  (forall t, inc t (V i f) -> ~ (gle (V i g) x t & gle (V i g) y t)) ->
  exists j, inc j (domain f) &
  least_element (induced_order r (Zo (domain f) (fun k => glt r i k))) j &
  exists z, least_element (V j g) z &
  (forall i x y, inc i (domain f) -> inc x (V i f) -> inc y (V i f) ->
  (forall t, inc t (V i f) -> ~ (gle (V i g) t x & gle (V i g) t y)) ->
  exists j, inc j (domain f) &
  greatest_element (induced_order r (Zo (domain f) (fun k => glt r i k))) j &
  exists z, greatest_element (V j g) z).

We start with some preliminary assertions. One half of the proof is obvious; it suffices to
collect the previous results.

Proof. ir. assert (Ht:=H). nin H. set (F:= ordinal_sum r f g).
  assert (order F). uf F. fprops. cp H; red in H; ee.
  assert (Hb: substrate F = disjoint_union f). uf F. aw.
  assert (Ha:forall i, inc i (domain f) -> exists y, inc y (V i f) &
     inc (J y i) (substrate F)). ir. nin (H0 _ H9).
     exists y. ee. am. cp (inc_disjoint_union H9 H10). rw Hb.
     app iff_eq. ir. cp (ordinal_sum_lattice1 Ht H9). ee. am.
     ir. app (ordinal_sum_lattice2 Ht).
     ir. app (ordinal_sum_lattice3 Ht H9 H11 H12 H13).
     ir. app (ordinal_sum_lattice4 Ht H9 H11 H12 H13).
     ir. app (ordinal_sum_lattice5 Ht H9 H11 H12 H13 H14).
     ir. app (ordinal_sum_lattice6 Ht H9 H11 H12 H13 H14).

Let' s show the existence of a supremum.

ir. ee. red. ee. ir. am. ir. ee. red. rwi Hb H15. rwi Hb H16.
  cp (lattice_sup_pr H9 H17 H18). ee. set (a:= sup r (Q x) (Q y)) in *. assert (forall z, gle F x z -> gle F y z -> gle r a (Q z)).
  ir. ufi F H26. cp (related_ordinal_sum_order_id H2 H27).
  wri H3 H17. rwi H3 H18.

nin (equal_or_not (Q x) (Q y)). wri H27 H19.
nin (p_or_not_p (exists t, gle (V (Q x) g) (P x) t &gle (V (Q x) g) (P y) t)).
nin H28. nin H28. cp (H11 _ _ _ _ H17 H28 H29).

wri H8 H21; wri H8 H19. cp (sup_pr (H7 _ H17) H21 H19 H30).

ee. set (z:= sup (V (Q x) g) (P x) (P y)) in *.

assert (inc (J z (Q x)) (substrate F)). rw Hb. app inc_disjoint_union. wr H8.

app (inc_arg2_substrate H31). am. exists (J z (Q x)).

ap least_upper_bound_doubleton. am. uf F. aw. ee. am. wrr Hb. right.

ee. tv. am. uf F. aw. ee. am. wrr Hb. right. ee. sy; am. wr H27. am. ir.

ufi F H35; ufi F H36; awi H35; awi H36. ee. uf F. aw. ee. wrr Hb. am.
nin H40. left. am. nin H38. left. rw H27. right. ee. am. app H33. rw H27.

am. am. am. am. am.

assert (forall t, inc t (V (Q x) f) -> ~ (gle (V (Q x) g) (P x) t &
   gle (V (Q x) g) (P y) t)). ir. red. ir. elim H28. exists t. am.
nin (H13 _ _ _ _ _ _ _ _ H17 H21 H19 H29). ee. nin H32. nin H32. ee.

assert (inc (J x1 x0) (disjoint_union f)). app inc_disjoint_union. wrr H8.

assert(Hc:sub (Zo (domain f) (fun k => glt r (Q x) k)) (substrate r)). rw H3. app Z_sub. red in H31. ee. awi H35. awi H31. Ztac. clear H31.
exists \((J \, x1 \, x0)\). ap least_upper_bound_doubleton. am. uf F. aw. ee. am. am. left. am. uf F. aw. ee. am. am. left. wr H27. ir.
ufi F H31; ufi F H38; avi H31; avi H38. ee. uf F. aw. ee. am. am.
nin (equal_or_not x0 \((Q \, t)\)). right. ee. am. app H33. cp (du_index_pr H39).
ee. rw H43. rw H8. left. nin (p_or_not_p (gle r \((Q \, x)\) \((Q \, t))\)). ir.
assert (inc \((Q \, t)\)). (Zo (domain f) (fun k => gle r \((Q \, x)\) k)). Ztac.
wr H3. app (inc_arg1_substrate H44). cp (H35 \_ H45). avi H46.
red. ee. am. am. cp (inc_arg1_substrate H46). avi H47. am. am. am. am.
ir. nin H42. elim H44. am. nin H40. elim H44. rw H27. ee.
am. am. am. am. am. am. am.

Let's show the existence of an infimum.

ee. red. rwi Hb H15. rwi Hb H16.
cp (lattice_inf_pr H9 H17 H18). ee. set (a:= inf r \((Q \, x)\) \((Q \, y)\)).
assert (forall z, gle F z x-> gle F z y -> gle r \((Q \, z)\) a).
ir. ufi F H26. cp (related_ordinal_sum_order_id H2 H26).
am. wri H8. am. wri H3. am. am. am. am. am. am. am. am.

nin (equal_or_not a \((Q \, t)\)). (Q y)). wr order_reflexivity. rw H3. am.
cp (order_antisymmetry H H24 (H25 \_ H28 H31)). elim H29; am.
assert (inc \((J \, x0 \, a)\) \(\text{(disjoint_union f)}\)). app inc_disjoint_union. wr H3.
exists \((J \, x0 \, a)\). ap least_upper_bound_doubleton. am. uf F. aw. ee. am. am.
left. red. ee. am. am. uf F. aw. ee. am. am. left. red. ee. am. am. ir.
cp (H26 \_ H34 H35).
ufi F H34. avi H34. ufi F H35. avi H35. uf F. aw. ee. am. am.
nin (equal_or_not a \((Q \, t)\)). right. ee. am. app H32. rw H8. rw H41.
cp (du_index_pr H37). ee; am. wr H3. app (inc_arg2_substrate H23).
left. red. ee. am. am. am. am.

nin (equal_or_not \((Q \, x)\) \((Q \, y)\) \((Q \, x)\)). wri H27 H19.
nin (p_or_not_p (exists t, gle \((V \, (Q \, x) \, g)\) \((P \, x)\) \& gle \((V \, (Q \, x) \, g)\) \((P \, y)\))).
nin H28. nin H28. cp (H12 \_ \_ \_ H17 H28 H29).

left. am. nin H38. left. rw H27. right. ee. am. am. am. am. am. am.
assert (forall t, inc t \((V \, (Q \, x) \, f)\) \(-\) \((gle \((V \, (Q \, x) \, g)\) \((P \, x)\) \&
\- gle \((V \, (Q \, x) \, g)\) \((P \, y)\))\)). ir. red. ir. elim H28. exists t. am.
nin (H14 \_ \_ H17 H21 H19 H29). ee. nin H32. nin H32. ee.
assert (inc \((J \, x1 \, x0)\) \(\text{(disjoint_union f)}\)). app inc_disjoint_union. wr H8.
assert(Hc:sub \((Zo \, (\text{domain f})\) \((\text{fun} \, k \Rightarrow \text{gle r} \, k \, (Q \, x))\) \(\text{(subscript r)}\)).
Let $E$ be an ordered set, and let $(E_i)_{i \in I}$ be the partition of $E$ formed by the connected components of $E$ (Chapter II, § 6, Exercise 10) with respect to the reflexive and symmetric relation "either $x = y$ or $x$ and $y$ are not comparable".

(a) Show that if $i \neq k$ and if $x \in E_i$ and $y \in E_k$, then $x, y$ are comparable; and that if, for example, $x \leq y, y' \in E_k$, and if $y' \neq y$, then also $x \leq y'$ (use the fact that there exists no partition of $E_k$ into two sets $A$ and $B$ such that every element of $A$ is comparable with every element of $B$).

(b) Deduce from (a) that the equivalence relation $S$ corresponding to the partition $(E_i)$ of $E$ is compatible (in $x$ and $y$) with the order relation $x \leq y$ on $E$, and that the quotient ordered set $E/S$ (Exercise 2) is totally ordered.

(c) What are the connected components of an ordered set $E = F \times G$ which is the product of two totally ordered sets?

We first recall some facts about connected components. We shall denote by $R$ the relation “either $x = y$ or $x$ and $y$ are not comparable”, and by $S$ the equivalence relation associated; the sets $E_i$ are the equivalence classes of $S$. 

INRIA
Definition not_comp_rel r := fun x y => inc x (substrate r) & inc y (substrate r) & x = y / ~ ((gle r x y) / (gle r y x)).

Definition ncr_equiv r := Exercice1.Sgraph (not_comp_rel r) (substrate r).
Definition ncr_component r := Exercice1.connected_comp (not_comp_rel r) (substrate r).

Lemma ncr_properties: forall r, order r ->
(is_equivalence (ncr_equiv r) &
substrate (ncr_equiv r) = substrate r &
(forall x, inc x (substrate r) -> class (ncr_equiv r) x = ncr_component r x)&
(forall x y, not_comp_rel r x y -> related (ncr_equiv r) x y)).
Proof. ir. uf ncr_equiv. uf ncr_component.
assert (reflexive_r (not_comp_rel r) (substrate r)).
red. uf not_comp_rel. ir. ee. am. am. left. tv.
ir. ee. am.
assert (symmetric_r (not_comp_rel r)). red. uf not_comp_rel. ir. ee.
am. am. nin H3. left. sy; am. right. red. ir. elim H3. intuition.
uf not_comp_rel.
assert (forall x y, not_comp_rel r x y -> inc x (substrate r)).
ir. red in H2. ee; am.
ee. app Exercice1.equivalence_Sgraph. app Exercice1.substrate_Sgraph.
ir. app Exercice1.connected_comp_class.
av. exists (Exercice1.chain_pair x y). ee. simpl. intuition. simpl. tv.
simpl. tv.
Qed.

We restate "ι ≠ κ and if x ∈ Eι and y ∈ Eκ, then x, y are comparable" as: either the classes (mod S) of x and y are equal, or x, y are comparable. This can also be restated as R x, y implies S x, y.

Lemma Exercice1_4a1: forall r x y, order r ->
inc x (substrate r) -> inc y (substrate r) ->
gle r x y / gle r y x / class (ncr_equiv r) x = class (ncr_equiv r) y.
Proof. ir. nin (p_or_not_p ((gle r x y) / (gle r y x))). nin H2. left. am.
right. left. am. right. right. assert (not_comp_rel r x y). red. ee. am.
am. right. am. cp (ncr_properties H). ee. wr r related_class_eq. app H7.
app reflexivity_e. rww H5.
Qed.

Consider the hint of the second claim. Consider a class C modulo S that is the union of two sets A and B such that each element of A is comparable with each element of B. Assume neither set empty, let a ∈ A and b ∈ B. Then a and b are related by S. This means that there is a chain (x_i)_i, relating a and b, thus a chain (x_i)_i with head in A and tail in B; by induction, there exist elements a' ∈ A and b' ∈ B related by R (if a chain is non-trivial, its head a' is related to another chain with head b'; these elements are in the same equivalence class (namely C) because they are related by R; if b' ∈ A, the result follows by induction, otherwise b' ∈ B and we have a solution). Since a' and b' are comparable, and related by R, they are equal. Thus the intersection of A and B is nonempty.

Lemma Exercice1_4a2: forall r y, order r ->
inc y (substrate r) ->
forall a b, union2 a b = class (ncr_equiv r) y ->
\[(\forall u \ v, \text{inc} \ u \ a \to \text{inc} \ v \ b \to \text{gle} \ r \ u \ v \ \lor \text{gle} \ r \ v \ u) \to\]
\[a = \text{emptyset} \lor b = \text{emptyset} \lor \text{nonempty} \ (\text{intersection2} \ a \ b).\]


assert (exists u, exists v, inc u a & inc v b & (\text{not_comp_rel} r) u v).
nin (inc_or_not (Exercice1.chain_head x) a). ir. app IHx.
rw H4. assert (inc v (substrate r)). app (inc_arg2_substrate H2).
nin H6. exists x0. app intersection2_inc. rw H18. elim H18. app H2.

Qed.

Let C be a class for S, x \in E \setminus C, A the set of all y \in C such that x \leq y, B the set of y' \in C such that y' \leq x. We have shown C = A \cup B. Obviously, if y \in A and y' \in B then y' \leq y, and y \neq y' (this would imply y = x hence x \in C). As a consequence one of A and B is empty.

Lemma Exercice1_4a3: \(\forall r x y y', \text{order} \ r \to \text{inc} x (\text{substrate} r) \to \text{related} (\text{ncr_equiv} r) y y' \to \text{gle} r x y \to \text{related} (\text{ncr_equiv} r) x y \lor \text{gle} r x y'.\)

Proof. ir. cp (ncr_properties H). ee. set (C:= \text{class} (\text{ncr_equiv} r) y).
set (A:= Zo C (fun z => \text{gle} r x z)). set (B:= Zo C (fun z => \text{gle} r z x)). assert (forall u v, inc u A \to inc v B \to \text{gle} r u v \lor \text{gle} r v u).
app (\text{order_transitivity} H H11 H10).
nin (p_or_not_p (related (\text{ncr_equiv} r) x y)). left. am. right.
assert (inc y (substrate r)). app (inc_arg2_substrate H2).
assert (\text{union2} A B = \text{class} (\text{ncr_equiv} r) y). set_extens. nin (\text{union2} or H10).
assert (inc x0 (substrate r)). wr H4. app (\text{sub_class_substrate} H3 H10).
nin (Exercice1_4a1 H H0 H11). app union2_first. uf A. Ztac.
nin H12. app union2_second. uf B. Ztac. elim H8.
apply transitivity_e with x0. am. rw related_class_eq.
appl reflexivity_e._rw H4. app symmetricity. wr inc_class. am.
red in H3; ee; am. cp (Exercice1_4a2 H H9 H10 H7). nin H11.
assert (inc y emptyset).wr H11. uf A. Ztac. uf C. rw inc_class.
appl reflexivity_e. rw H4. red in H3; ee; am. elim (emptyset_pr H12).
nin H11. assert (inc y' C). uf C. bw. am. red in H3; ee; am.
rv (\text{order_antisymmetry} H H14 H16). app symmetricity. wr inc_class. am.
red in H3; ee; am.

Qed.
Let's show the compatibility of the equivalence and the order. We must show that if \( x \) and \( x' \) are in the same class, if \( y \) and \( y' \) are in the same class, then \( x \leq y \) is the same as \( x' \leq y' \). The assumption is that the classes are distinct. We know that \( x' \leq y', y' \leq x' \) or \( R(x', y') \). The first possibility is the desired result, the last one says that the classes are the same. We have shown that \( y' \leq x' \) implies \( y' \leq x \) and \( x \leq y \) implies \( x \leq y' \). Thus, the second possibility says \( x = y', \) absurd.

**Lemma Exercice1_4b1:** forall \( r \) \( x \) \( y \) \( x' \) \( y' \), order \( r \) -> related (ncr_equiv r) \( x \) \( x' \) -> related (ncr_equiv r) \( y \) \( y' \) -> class (ncr_equiv r) \( x \) <> class (ncr_equiv r) \( y \) -> gle r \( x \) \( y \) -> gle r \( x' \) \( y' \).

**Proof.** ir. cp (ncr_properties H). ee.
- assert (inc \( x' \) (substrate r)). wr H5. app (inc_arg2_substrate H0).
- assert (inc \( y' \) (substrate r)). wr H5. app (inc_arg2_substrate H1).
- assert (inc \( x \) (substrate r)). wr H5. app (inc_arg1_substrate H0).
- assert (inc \( y \) (substrate r)). wr H5. app (inc_arg1_substrate H1).
- nin (Exercice1_4a1 H H8 H9). am. nin H12.
- assert (Ha:related (ncr_equiv r) \( x \) \( x \)). app reflexivity_e. rww H5.
- nin (Exercice1_4a3 H H10 H1 H3). elim H2. wr related_class_eq.
- assert (related (ncr_equiv r) \( x' \) \( x \)). app symmetricity.
- nin (Exercice1_4a3 H H9 H14 H12). elim H2.
- wr related_class_eq. apply transitivity_e with \( x' \). am. am.
- app symmetricity. apply transitivity_e with \( y' \). am. am. am.
- wri (order_antisymmetry H H13 H15) H1. elim H2. wr related_class_eq.
- app symmetricity. elim H2. wr related_class_eq.
- apply transitivity_e with \( x' \). am. am. apply transitivity_e with \( y' \). am.
- rw related_class_eq. app reflexivity_e. rw H5. app symmetricity.
- app reflexivity_e. rw H5.
Qed.

The quotient order is an order, according to condition C'. To show it, assume \( x \leq y \leq z \), \( x \) and \( z \) in the same class. If \( x \) and \( y \) are not in the same class, then \( x \leq y \) implies \( z \leq y \). This says \( y = z \), absurd. The quotient order is total, since, given two distinct classes, the representatives are comparable. Now, if \( x \in X \) and \( y \in Y \), the compatibility condition says \( X \leq Y \) in the quotient if and only if \( x \leq y \) in the substrate.

**Lemma Exercice1_4b:** forall \( r \), order \( r \) ->

**total_order(quotient_order r (ncr_equiv r)).**

**Proof.** ir. cp (ncr_properties H). ee.
- assert (order (quotient_order r (ncr_equiv r))). app Exercise1_2d. red. ir. nin (p_or_not_p (related (ncr_equiv r) \( x \) \( y \))). am. assert (related (ncr_equiv r) \( y \) \( y \)). app reflexivity_e. rw H1.
- app (inc_arg1_substrate H5).
- assert (class (ncr_equiv r) \( x \) <> class (ncr_equiv r) \( y \)). red. ir.
- elim H7. app symmetricity. rw related_class_eq. sy; am.
- cp (Exercise1_4b1 H H6 H8 H9 H4). cp (order_antisymmetry H H5 H10).
- rw H11. red. ee. am. rw substrate_quotient_order. ir. uf gge.
- nin (equal_or_not x y). left. rw H7. wr order_reflexivity.
- rw substrate_quotient_order. am. am. red; red in H; ee; am. am. am.
- ir. uf gge. rw quotient_order_pr. rw quotient_order_pr. uf quotient_order_r.
- cp (inc_rep_itself H0 H5). cp (inc_rep_itself H0 H6).
- assert (inc (rep \( x \)) (substrate r)). wr H1. app inc_rep_substrate.
- assert (inc (rep \( y \)) (substrate r)). wr H1. app inc_rep_substrate.
- assert (Ha:class (ncr_equiv r) (rep \( x \)) <> class (ncr_equiv r) (rep \( y \))).
red. ir. wri (inc_quotient x H0) H5. wri (inc_quotient y H0) H6. elim H7. red in H5; red in H6. ee. rw H16; rw H14. am. cp (Exercice1_4a1 H H10 H11). nin H12. left. ee. am. am. ir. exists (rep y). ee. am. assert (related (ncr_equiv r) (rep x) x0).
app related_rep_in_class. assert (related (ncr_equiv r) (rep y)(rep y)). app related_rep_in_class. ap (Exercice1_4b1 H H14 H15 Ha H12). nin H12. right. ee. am. am. ir. exists (rep x). ee. am. assert (related (ncr_equiv r) (rep y) x0).
app related_rep_in_class. assert (related (ncr_equiv r) (rep x)(rep x)). app related_rep_in_class. assert (class (ncr_equiv r) (rep x) <> class (ncr_equiv r) (rep y)). intuition. ap (Exercice1_4b1 H H14 H15 Ha H12). elim Ha. am. am. ir. exists (rep x). ee. am. app related_rep_in_class. ap (Exercice1_4b1 H H14 H15 H16 H12). elim Ha. am. am. red in H;red; ee;am. am. Qed.

Consider a product of two totally ordered sets $E = F \times G$. Let’s determine the set of components. We have $x \leq y$ if and only if $\text{pr}_1 x \leq \text{pr}_1 y$ and $\text{pr}_2 x \leq \text{pr}_2 y$. We exclude the case where the sets are empty. If $G$ is a singleton, then $\text{pr}_2 x \leq \text{pr}_2 y$ is always true, and the product is totally ordered. The set of components is then isomorphic to $E$. If $a$ and $a'$ are the least elements of $F$ and $G$, $l = (a, a')$, then $l$ is the least element of $E$, and $|l|$ is a component. In the same fashion, if $g$ is the greatest element of $E$ then $|g|$ is a component.

We assume now that $E$ has at least two elements $b$ and $c$, $F$ has at least two elements $b'$ and $c'$. We pretend that the class $C$ of $(b, c')$, contains all elements of $E$, with the possible exception of $l$ and $g$. It contains obviously $(c, b')$. 2 or 3 components. Let $y = (b, b')$, and assume that $y \neq l$. Then $y \in C$. In fact, if $a < b$, then $\text{R}[l(a, c'), (b, b')]$ and $\text{R}[l(a, c'), (c, b')]$, so that $(b, b')$ and $(c, b')$ are in the same class. On the other hand, if $a' < b'$, then $\text{R}[l(c, a'), (b, b')]$ and $\text{R}[l(c, a'), (b, c')]$, so that $(b, b')$ and $(c, c')$ are in the same class. In the same way, $(c, c')$ is the class if it is not the greatest element. Assume $c < d$. Then $(c, b')$ and $(d, b')$ are related to $(b, c')$, Then $(c, b')$ and $(d, b')$ are related to $(b, c')$, and $(b, c')$ and $(c, c')$ are related to $(d, b')$. This shows that the six elements of the product $\{b, c, d\} \times \{b', c', d'\}$, minus the greatest and least elements are in the same class. By symmetry, if $d' \in F$, the six elements of the product $\{b, c, d\} \times \{b', c', d'\}$, minus the greatest and least elements are in the same class.

It follows (the Coq code is still missing), that $x \in E$ and $y \in E$ are related if neither of them is the last of greatest element of $E$. 

5. Let $E$ be an ordered set. A subset $X$ of $E$ is said to be free if no two distinct elements of $X$ are comparable. Let $\mathcal{I}$ be the set of free subsets of $E$. Show that, on $\mathcal{I}$, the relation “given any $x \in X$, there exists $y \in Y$ such that $x \leq y$” is an order relation between $X$ and $Y$, written $X \leq Y$. The mapping $x \rightarrow \{x\}$ is an isomorphism of $E$ onto a subset of the ordered set $\mathcal{I}$. If $X \subseteq Y$ where $X \in \mathcal{I}$ and $Y \in \mathcal{I}$, show that $X \leq Y$. The ordered set $\mathcal{I}$ is totally ordered if and only if $E$ is totally ordered, and then $\mathcal{I}$ is canonically isomorphic to $E$.

We restate the definition as: if $x \in X$ and $y \in X$ and $x \leq y$ then $x = y$.

Definition free_subset r X := forall x y, inc x X -> inc y X -> gle r x y -> x = y.
Definition set_of_free_subsets r :=
  Zoo powerset (substrate r) (fun X=> free_subset r X).
Definition free_subset_compare r X Y :=
inc X (set_of_free_subsets r) & inc Y (set_of_free_subsets r) &
forall x, inc x X -> exists y, inc y Y & gle r x y.

Definition free_subset_order r :=
graph_on (free_subset_compare r) (set_of_free_subsets r).

The relation \( \forall x \in X, \exists y \in Y, x \leq y \) is clearly a preorder relation. Antisymmetry follows from the fact that if \( x \in X, y \in Y, x \leq y \) and \( x' \in X, y \leq x' \) then \( x = x' \) by transitivity, when \( X \) is free, and \( x = y \) by antisymmetry.

Lemma Exercise1_5a: forall r, order r ->
order_r (free_subset_compare r).
Proof. ir. red. uf free_subset_compare. split. red. ir. ee. am. am.
ir. nin (H5 _ H6). nin H7. nin (H3 _ H7). nin H9. exists x2. split. am.
ap (order_transitivity H H8 H10). split. red. ir. ee.
set_extens. nin (H5 _ H6). nin H7. nin (H3 _ H7). nin H9.
cp (order_transitivity H H8 H10). ufi set_of_free_subsets H0. Ztac.
red in H13. wri (H13 _ _ H6 H9 H11) H10. rww (order_antisymmetry H H8 H10).
nin (H3 _ H6). nin H7. nin (H5 _ H7). nin H9.
red in H13. wri (H13 _ _ H6 H9 H11) H10. rww (order_antisymmetry H H8 H10).
red. ir. ee. am. am. ir. exists x0. split. am. wr order_reflexivity.
ufi set_of_free_subsets H0. Ztac. rwi powerset_inc_rw H4. app H4. am. am.
ir. exists x0. split. am. wr order_reflexivity.
Qed.

Lemma fs_order_pr: forall r x y,
related (free_subset_order r) x y = free_subset_compare r x y.
Proof. ir. uf free_subset_order. uf graph_on. uf related. ap iff_eq. ir. Ztac.
avi H1. am. ir. Ztac. red in H. ee. app product_pair_inc. aw.
Qed.

Lemma fs_is_order: forall r,
order r -> order (free_subset_order r).
Proof. ir. uf free_subset_order. app order_from_rel. app Exercise1_5a.
Qed.

Lemma substrate_fs_order: forall r,
order r -> substrate (free_subset_order r) = set_of_free_subsets r.
Proof. ir. cp (fs_is_order H). set_extens. rwi order_reflexivity H1.
  rwi fs_order_pr H1. red in H1. nin H1. am.
am. rw order_reflexivity. rw fs_order_pr. red. split. am. split. am.
ir. exists x0. split. am. wr order_reflexivity. ufi set_of_free_subsets H1.
Ztac. rwi powerset_inc_rw H3. app H3. am. am.
Qed.

A singleton is free; the mapping \( x \mapsto \{x\} \) is an isomorphism onto its range. If \( E \) is a totally ordered set, then the only nonempty-free subsets are the singletons, so that the range is \( \mathcal{J} - \{\emptyset\} \).

Lemma Exercise1_5b: forall r x, order r ->
inc x (substrate r) -> inc (singleton x) (set_of_free_subsets r).
rw (singleton_eq H1). am. red. ir. rw (singleton_eq H1).
rww (singleton_eq H2).
Qed.
Lemma Exercise1_5c: forall r x y, order r ->
  inc x (substrate r) -> inc y (substrate r) ->
  gle r x y = gle (free_subset_order r) (singleton x) (singleton y).
Proof. ir. rw fs_order_pr. app iff_eq. ir. red. ee. app Exercise1_5b.
  app Exercise1_5b. ir. rw (singleton_eq H3). exists y. split. fprops. am.
  ir. red in H2. ee. assert (inc x (singleton x)). fprops. cp (H4 _ H5). nin H6.
  nin H6. wrr (singleton_eq H6).
Qed.

Lemma Exercise1_5d: forall r, order r ->
  order_morphism (BL singleton (substrate r) (set_of_free_subsets r))
  r (free_subset_order r).
Proof. ir.
  assert (transf_axioms singleton (substrate r) (set_of_free_subsets r)).
  red. ir. app Exercise1_5b.
  assert (is_function (BL singleton (substrate r) (set_of_free_subsets r))).
  app af_function. red. simpl. ee. am. app fs_is_order.
  app injective_af_function. ir. app singleton_inj. tv. rww substrate_fs_order.
  ir. rww W_af_function. rww W_af_function. app Exercise1_5c.
Qed.

Lemma Exercise1_5e: forall r X, total_order r ->
  inc X (set_of_free_subsets r) -> small_set X.
Proof. ir. red. ir. red in H. ee. ufi set_of_free_subsets H0. Ztac.
  rwi powerset_inc_rw H4. red in H5. nin (H3 _ _ (H4 _ H1) (H4 _ H2)).
  app H5. red in H6. sy. app H5.
Qed.

If X ⊂ Y then X ≤ Y (this is trivial). If E is totally ordered so is J. In fact, the empty set is the
least element of J; two non-empty sets are singletons, and singletons are compared accord-
ing to there elements. The converse is trivial. Bourbaki says that J is canonically isomorphic
to E in this case. This is obviously wrong: as noted above x → {x} is an isomorphism between
E and J − {∅}.

Lemma Exercise1_5f: forall r X Y, order r ->
  inc X (set_of_free_subsets r) -> inc Y (set_of_free_subsets r) ->
  sub X Y -> gle (free_subset_order r) X Y.
Proof. ir. rw fs_order_pr. red. ee. am. ir. exists x. split. app H2.
  wr order_reflexivity. ufi set_of_free_subsets H0. Ztac.
  rwi powerset_inc_rw H4. app H4. am.
Qed.

Lemma Exercise1_5g: forall r, total_order r ->
  total_order (free_subset_order r).
Proof. ir. cp H. nin H. red. split. app fs_is_order. rwi substrate_fs_order.
  assert (inc emptyset (set_of_free_subsets r)). uf set_of_free_subsets.
  Ztac. app powerset_inc. app sub_emptyset_any. red. ir. elim (emptyset_pr H2).
  ir. cp (Exercise1_5e H0 H3). cp (Exercise1_5e H0 H4).
  nin (emptyset_dichot x). rw H7. left. app Exercise1_5f. app sub_emptyset_any.
  nin (emptyset_dichot y). rw H8. right. red. app Exercise1_5f.
  app sub_emptyset_any. nin H7. nin H8.
  ufi set_of_free_subsets H4; Ztac. rwi powerset_inc_rw H3.
  cp (H9 _ H7). cp (H3 _ H8).
  assert (x = singleton y0). set_extens. red in H5. rw (H5 _ _ H7 H14). fprops.
  rw (singleton_eq H14). am.
in (H1 _ _ H12 H13). left. wrr Exercise1_5c. right. red. wrr Exercise1_5c. Qed.

Lemma Exercise1_5h: forall r, order r -> 
total_order (free_subset_order r) -> total_order r. 
Proof. ir. red. split. am. nin H0. ir. rwi substrate_fs_order H1. 

nin (H1 _ _ (Exercise1_5b H H2) (Exercise1_5b H H3)). left. 
rww Exercise1_5c. right. red. red in H4. rww Exercise1_5c. am. Qed.

6. Let E and F be two ordered sets and let $\mathcal{A}(E, F)$ be the subset of the product ordered set $F^E$ consisting of the increasing mappings of E into F.

We change the definition of $\mathcal{A}(E, F)$: it will be a subset of $\mathcal{F}(E; F)$, the set of mappings from E to F, that is canonically isomorphic to $F^E$. It will be ordered by the ordering on functions.

Definition set_of_increasing_mappings r r' := 
Zo (set_of_functions (substrate r) (substrate r')) 
(fun z=> increasing_fun (inv_corr_value z) r r').

Definition increasing_mappings_order r r' := 
induced_order (function_order (substrate r) (substrate r') r') 
(set_of_increasing_mappings r r').

We give here some trivial lemmas expliciting the definitions.

Lemma set_of_increasing_mappings_pr: forall r r' f, order r -> order r' -> 
inc f (set_of_increasing_mappings r r') = exists g, 
is_function g & source g = (substrate r) & target g = substrate r' 
& increasing_fun g r r' & corr_value g = f. 
Proof. ir. uf set_of_increasing_mappings. app iff_eq. ir. Ztac. 
nin (set_of_functions_inc H2). ee. exists x. intuition. wri H7 H3. 
rwi inv_corr_value_pr H3. am. ir. nin H1. ee. Ztac. wr H2; wr H3; wr H5. 
app inc_set_of_functions. wr H5. rww inv_corr_value_pr. Qed.

Lemma imo_order: forall r r', order r -> order r' -> 
order (increasing_mappings_order r r'). 
Proof. ir. uf increasing_mappings_order. app order_induced_order. 
rw substrate_function_order. uf set_of_increasing_mappings. app Z_sub. am. 
tv. app order_function_order. Qed.

Lemma imo_substrate: forall r r', order r -> order r' -> 
substrate (increasing_mappings_order r r') = set_of_increasing_mappings r r'. 
Proof. ir. uf increasing_mappings_order. rw substrate_induced_order. tv. 
app order_function_order. uf set_of_increasing_mappings. 
rw substrate_function_order. app Z_sub. am. tv. 
Qed.
Lemma imo_pr: forall r r' f g, order r -> order r' ->
  gle (increasing_mappings_order r r') f g =
  (inc f (set_of_increasing_mappings r r') &
  inc g (set_of_increasing_mappings r r') &
  function_order_r (substrate r) (substrate r') r' (inv_corr_value f)
  (inv_corr_value g)).
Proof. ir. app iff_eq. ir. cp (imo_order H H0).
cp (inc_arg1_substrate H1). cp (inc_arg2_substrate H1). rwi imo_substrate H3.
ri imo_substrate H4. ufi increasing_mappings_order H1. awi H1.
ufi function_order H1. ufi graph_on H1. ee. am. am. red in H1. Ztac. clear H1.
awi H5. ee. nin (set_of_functions_inc H5). ee.
wr H15. wr H11. rw inv_corr_value_pr. rw inv_corr_value_pr. awi H6.
wr (corr_propc x). wr (corr_propc x0). rw H9; rw H10; rw H13; rw H14; am.
am. am. am. am. am.
ir. ee. uf increasing_mappings_order. aw.
uf function_order. red. uf graph_on. Ztac. av. ee. fprops. am. am.
cp (sof_value_pr H4). cp (sof_value_pr H1). ee. wri H13 H3. wri H10 H3.
ri inv_corr_value_pr H3. rwi inv_corr_value_pr H3. aw.
Qed.

(a) Show that if E, F, G are three ordered sets, then the ordered set \( A(E, F \times G) \) is isomorphic to the product ordered set \( A(E, F) \times A(E, G) \).

Given a function \( f : E \rightarrow F \times G \), we can consider the two projections \( f_1 : E \rightarrow F \) and \( f_2 : E \rightarrow G \). We first show that \( f \mapsto (f_1, f_2) \) is a bijection \( \mathcal{F}(E; F \times G) \) onto \( \mathcal{F}(E; F) \times \mathcal{F}(E; G) \).

Definition first_projection f a b := BL (fun z => P (W z f)) a b.
Definition secnd_projection f a c := BL (fun z => Q (W z f)) a c.
Definition two_projections a b c :=
  BL (fun z => (J (corr_value (first_projection (inv_corr_value z) a b))
  (corr_value (secnd_projection (inv_corr_value z) a c))))
  (set_of_functions a (product b c))
  (product (set_of_functions a b) (set_of_functions a c)).
Lemma Exercice1_6a: forall f a b c, is_function f -> source f =a ->
target f = product b c ->
  (transf_axioms (fun z => P (W z f)) a b &
  transf_axioms (fun z => Q (W z f)) a c &
  is_function (first_projection f a b) &
  is_function (secnd_projection f a c) &
  (forall x, inc x a -> W x (first_projection f a b) = P (W x f)) &
  (forall x, inc x a -> W x (secnd_projection f a c) = Q (W x f))).
Proof. ir. assert (transf_axioms (fun z => P (W z f)) a b). red. ir. wri H0 H2.
cp (inc_W_target H H2). rri H1 H3. av H3; ee;am.
assert (transf_axioms (fun z => Q (W z f)) a c). red. ir. wri H0 H3.
cp (inc_W_target H H3). rri H1 H4. av H4; ee;am. uf first_projection.
uf secnd_projection. ee. am. am. app af_function. app af_function.
ir. aw. ir. aw.
Qed.

Lemma Exercice1_6b: forall a b c,
  (transf_axioms
    (fun z => (J (corr_value (first_projection (inv_corr_value z) a b))))
(corr_value (secnd_projection (inv_corr_value z) a c)))
(set_of_functions a (product b c))
(product (set_of_functions a b) (set_of_functions a c)).
Proof. ir. red. ir. nin (set_of_functions_inc H). ee.
 cp (Exercice1_6a H0 H1 H2). ee. aw. wr H3. rw inv_corr_value_pr. ee. fprops.
 set (g := first_projection x a b). assert (a = source g). uf g. tv. rw H10.
 assert (b = target g). uf g. tv. rw H11. app inc_set_of_functions.
 set (g := secnd_projection x a c). assert (a = source g). uf g. tv. rw H10.
 assert (c = target g). uf g. tv. rw H11. app inc_set_of_functions.
Qed.

Lemma Exercice1_6c: forall a b c, bijective (two_projections a b c).
Proof. ir. cp (Exercice1_6b (a:=a) (b:=b)(c:=c)).
 assert (is_function (two_projections a b c)). uf two_projections.
 app af_function. uf two_projections. red. split.
(* injectivity *) app injective_af_function.
 wr H11; wr H8; wri H11 H3; wri H8 H3; repeat rwi inv_corr_value_pr H3.
 cp (pr1_injective H3). cp (pr2_injective H3).
 rewrite correspondence_extensionality1 in H12, H13 |- *.
 app funct_extensionality. rww H6. rww H7. rww H9. ir.
 cp (Exercice1_6a H4 H5 H6 H7). ee.
 app pair_extensionality. assert (inc (W x1 x) (product b c)). wr H10.
 app inc_W_target. rw H9. awi H27; ee; am.
 assert (inc (W x1 x0) (product b c)). wr H7. app inc_W_target. rww H6.
 awi H27; ee; am. wr H25. wr H20. rww H12. am. am.
(* surjectivity *) app surjective_af_function. ir. awi H1. ee.
 set (f := BL (fun z=> J (W z x) (W z x0)) a (product b c)).
 assert (transf_axioms (fun z=> J (W z x) (W z x0)) a (product b c)).
 red. ir. av. ee. fprops. wr H10. app inc_W_target. rw H9.
 wr H7. app inc_W_target. rww H6.
 assert (is_function f). uf f. app af_function.
 assert (source f = a). uf f; tv. assert (target f = product b c). uf f; tv.
 assert (inc (corr_value f) (set_of_functions a (product b c))).
 wr H14; wr H15. app inc_set_of_functions.
 cp (Exercice1_6a H3 H4 H5). ee.
 exists (corr_value f). split. am. rw inv_corr_value_pr.
 app pair_extensionality. fprops. wr H11. aw.
 rewrite correspondence_extensionality1. app funct_extensionality. ir.
 rewrite correspondence_extensionality1. app funct_extensionality. ir.
Qed.

Now we show that this operation is compatible with the order: if f is increasing, both
projections are increasing; the converse is equally true. This means that f → (f_1, f_2)
induces a bijection S(E,F×G) onto S(E,F)×S(E,G). Finally, we show that it is an order isomorphism.

Hint Rewrite substrate_order_product2_order: bw.

Lemma Exercice1_6d: forall f r r' r'', order r -> order r' -> order r'' ->
increasing_fun f r (product2_order r' r'') ->
(increasing_fun (first_projection f (substrate r) (substrate r')) r r' &
increasing_fun (secnd_projection f (substrate r) (substrate r')) r r'').

RR n° 7150
Proof. ir. red in H2. nin H2; nin H3; nin H4; nin H5; nin H6.
cp (Exercice1_6a H2 H5 H6). ee. red. ee. am. am. tv. tv. red. simpl.
ir. rw H12. rw H12. red in H7. ee. rwi H5 H7. cp (H7_ _ H14 H15 H16).
ren product2_order_pr H17. red in H17. ee. am. am.
red. ee. am. am. tv. tv. red. simpl.
ir. rw H13. rw H13. red in H7. ee. rwi H5 H7. cp (H7_ _ H14 H15 H16).
ren product2_order_pr H17. red in H17. ee. am. am. am. am.
Qed.

Definition two_projections_increasing r r' r'' :=
restriction2 (two_projections (substrate r) (substrate r')(substrate r''))
(set_of_increasing_mappings r (product2_order r' r''))
(product (set_of_increasing_mappings r r')
(set_of_increasing_mappings r r'')).

Lemma Exercice1_6e: forall r r' r'', order r -> order r' -> order r'' ->
(restriction2_axioms
(two_projections (substrate r) (substrate r')(substrate r''))
(set_of_increasing_mappings r (product2_order r' r''))
(product (set_of_increasing_mappings r r')
(set_of_increasing_mappings r r''))).
Proof. ir.
cp (Exercice1_6c (substrate r) (substrate r') (substrate r'')).
red. ee. app bij_is_function. simpl. uf set_of_increasing_mappings.
bw. app Z_sub. simpl.
app product_monotone. uf set_of_increasing_mappings. app Z_sub.
uf set_of_increasing_mappings. app Z_sub.
uf image_by_fun. red. ir. cp (bij_is_function H2). awi H4. nin H4. nin H4.
red in H6. rw (W_pr H5 H6). uf two_projections. rww W_af_function.
ren set_of_increasing_mappings_pr H4. nin H4. ee.
cp (Exercice1_6d H H0 H1 H9). ee. bwi H8.
cp (Exercice1_6a H4 H7 H8). ee. wr H10. rw inv_corr_value_pr. aw. ee. fprops.
ren set_of_increasing_mappings_pr.
exists (first_projection x1 (substrate r) (substrate r')).
ee. am. tv. tv. am. tv. am. am. rw set_of_increasing_mappings_pr.
exists (second_projection x1 (substrate r) (substrate r'')).
ee. am. tv. tv. am. am. am. am. am. app order_product2_order.
Qed.

Lemma Exercice1_6f: forall r r' r'', order r -> order r' -> order r'' ->
bijection (two_projections_increasing r r' r'').
Proof. ir. cp (Exercice1_6e H H0 H1).
red. split. uf two_projections_increasing. app injective_restriction2.
uf two_projections_increasing. app surjective_pr6. ir.
assert (inc y (target (two_projections (substrate r) (substrate r')(substrate r'')))). simpl. awi H6. ee. uf set_of_increasing_mappings H7.
Ztac. am. nin (surjective_pr2 H4 H7). nin H8.
assert (inc x (set_of_increasing_mappings r (product2_order r' r''))).
Bourbaki: Theory of sets in Coq. II (v2)

195

ufi two_projections H8. simpl in H8.
cp (Exercice1_6a H10 H11 H12). wri H13 H9; rwi inv_corr_value_pr H9.
exists x0. ee. am. am. bw. am. am. am.
red. ee. am. am. app order_product2_order. sy; am. sy; bw. red. ir.
set (f1 := first_projection x0 (substrate r) (substrate r')) in *.
set (f2 := second_projection x0 (substrate r) (substrate r'')) in *.
rw product2_order_pr. red. split. wr H12. app inc_W_target. split.
rt set_of_increasing_mappings_pr H23. nin H23. ee.
rwi correspondence_extensionality1 H28. wr H28. red in H27. ee. app H33.
wr H31. wri H31. am. am.
rwi correspondence_extensionality1 H28. wr H28. red in H27. ee. app H33.
wr H31. wr H31. am. am. am. am. am. am. am. am. am. am. am. am. am. am. am. am. am. am. am. am.
app Exercice1_6b. exists x. ee. am. rw W_restriction2.
Qed.

Lemma Exercice1_6g: forall r r' r'', order r -> order r' -> order r'' ->
(order_isomorphism (two_projections_increasing r r' r''))
(increasing_mappings_order r (product2_order r' r''))
(product2_order (increasing_mappings_order r r')
(increasing_mappings_order r r'')).
Proof. ir. assert (order (product2_order r' r'')). app order_product2_order.
red. ee. app imo_order. app order_product2_order. app imo_order.
app imo_order. app Exercice1_6f. simpl. rw imo_substrate. tv.
am. app order_product2_order. bw.
uf two_projections_increasing. simpl. rw imo_substrate. rw imo_substrate.
app imo_order. app two_projections_increasing. simpl. ir.
uf two_projections_increasing.
cp (Exercice1_6b (a := substrate r) (b := substrate r') (c := substrate r'')).
cp (Exercice1_6e H H0 H1). rw W_restriction2. rw W_restriction2. clear H6.
assert (Ha := H3). assert (Hb := H4).
nin H3; nin H4. ee. assert (Hc := H11). assert (Hd := H7).
bwi H11. cp (Exercice1_6a H3 H10 H11).
bwi H7. cp (Exercice1_6a H4 H6 H7). ee.
uf two_projections. rw W_af_function. rw W_af_function.
clear H5. wr H9; wr H13; rw inv_corr_value_pr; rw inv_corr_value_pr.
rw product2_order_pr. uf product2_order_r. aw. rw imo_pr. rw imo_pr.
rt imo_pr. repeat rw imo_substrate. repeat rw inv_corr_value_pr.
cp (Exercice1_6d H H0 H1 H12). cp (Exercice1_6d H H0 H1 H8). ee. app iff_eq. (* direct *) ir.
assert (inc (corr_value (first_projection x0 (substrate r) (substrate r'))).
(set_of_increasing_mappings r r')). rw set_of_increasing_mappings_pr.
exists (first_projection x0 (substrate r) (substrate r')). ee. am.
tv. tv. am. tv. am.
assert (inc (corr_value (second_projection x0 (substrate r) (substrate r''))).
(set_of_increasing_mappings r r'')). rw set_of_increasing_mappings_pr.
exists (second_projection x0 (substrate r) (substrate r'')). ee. am.
tv. tv. am. tv. am.
assert (inc (corr_value (first_projection x1 (substrate r) (substrate r'))).
(set_of_increasing_mappings r r')). rw set_of_increasing_mappings_pr.
exists (first_projection x1 (substrate r) (substrate r')). ee. am.

RR n° 7150
(b) Show that if $E$, $F$, $G$ are three ordered sets, then the ordered set $\mathcal{A}(E \times F, G)$ is isomorphic to the ordered set $\mathcal{A}(E, \mathcal{A}(F, G))$.

Let's show that $S = \mathcal{A}(E \times F, G)$ is isomorphic to the ordered set $T = \mathcal{A}(E, \mathcal{A}(F, G))$. We shall assume $E$ and $F$ non-empty. For otherwise, the product $E \times F$ is empty, case where there is a single element in $S$. If $F$ is empty, $\mathcal{A}(F, G)$ has a single element (the empty function) and $\mathcal{A}(E, \mathcal{A}(F, G))$ has a single element (that maps everything to the empty function). Assume $E$ empty. Then $\mathcal{A}(E, \mathcal{A}(F, G))$ contains only the empty function. Whatever the orderings on the sets $S$ and $T$, since the sets are singletons, the orders are trivial and any function between $S$ and $T$ is an isomorphism.

In all our lemmas we consider orderings $r$, $r'$ and $r''$, with substrate $E$, $F$ and $G$. An increasing function $f : r \times r' \rightarrow r''$ if a function with source $E \times F$ and target $G$; the first lemma says, that if $r$ and $r'$ are orders, the substrate of $r \times r'$ is indeed the product of the substrates, namely $E \times F$, and if these two sets are non-empty, one can recover the sets from the product. The second lemma says that $f_x$ is increasing for all $x \in E$. The third lemma says that the range of $x \mapsto f_x$ is a subset of the set of increasing functions.

Lemma Exercice1_6h: $\forall f \ r \ r' \ r'', \ order \ r \rightarrow \ order \ r' \rightarrow$
\nonempty (substrate r) $\rightarrow$ \nonempty (substrate r') $\rightarrow$
increasing_fun f (product2_order r r') r'' $\rightarrow$
\((\text{domain } (\text{source } f)) = \text{substrate } r \& (\text{range } (\text{source } f)) = \text{substrate } r').$
Proof. ir. red in H3. ee. wr H6. bw. rv domain_product. tv. am.
wr H6. bw. rv range_product. tv. am.
Qed.

Lemma Exercice1_6i: $\forall f \ x \ r \ r' \ r'', \ order \ r \rightarrow \ order \ r' \rightarrow$
\nonempty (substrate r) $\rightarrow$ \nonempty (substrate r') $\rightarrow$
\increasing_fun f (product2_order r r') r'' $\rightarrow$
inc x (substrate r) $\rightarrow$ increasing_fun (second_partial_fun f x) r' r''.
Proof. ir. nin (Exercice1_6h H H0 H1 H2 H3).
red in H3. ee. assert (partial_fun_axioms f). red. ee. am.
wr H9. bw. exists (substrate r). exists (substrate r'). tv.
wr i H5 H4. cp (function_spf H12 H4). red. ee. am. am. am. simpl.
sy; am. am. red. simpl. ir. rw W_spf. rw W_spf.
assert (inc (J x0) (source f)). wr H9. bw. aw. ee. fprops. wr H5. wr H6.

Lemma Exercice1_6j: forall f r r' r'', order r -> order r' -> nonempty (substrate r) -> nonempty (substrate r') -> increasing_fun f (product2_order r r') r'' -> (restriction2_axioms (second_partial_function f) (substrate r) (set_of_increasing_mappings r' r'')).

We consider now \( \Phi = \text{second_partial_map} \) (this is the bijection from \( \mathcal{F}(E \times F; G) \) onto \( \mathcal{F}(E, \mathcal{F}(F; G)) \)). For each \( a \in E \), \( \Phi(f)(a) \) is in \( \mathcal{F}(F; G) \); if \( f \) is increasing this is in \( \mathcal{A}(F, G) \). Thus we can restrict \( \Phi(f) \) as a function \( \Phi(f) \) from \( E \) into \( \mathcal{A}(F, G) \). The mapping \( f \mapsto \Phi(f) \) will be our isomorphism. It is clearly injective; proving surjectivity is a bit longer.

If \( f_a \) and \( a \mapsto f_a \) are increasing, then \( a \leq a' \) and \( b \leq b' \) implies \( f_a(b) \leq f_{a'}(b') \), so that \( f \) is increasing. Conversely, if \( f \) is increasing, then \( f_a \) is increasing since if \( b \leq b' \) then \( f_a(b) \leq f_a(b') \), using \( a \leq a' \); and \( a \mapsto f_a \) is increasing since if \( a \leq a' \) then \( f_a(b) \leq f_{a'}(b) \), using \( b \leq b' \). These are the only properties of the order that are used here.

Definition second_partial_map2 r r' r'':=
BL (fun f=> corr_value(restriction2 (second_partial_function (sof_value (product (substrate r)(substrate r')) (substrate r'')) f)) (substrate r) (set_of_increasing_mappings r' r'')) (set_of_increasing_mappings (product2_order r r') r'') (set_of_increasing_mappings r (increasing_mappings_order r' r'')).

Lemma Exercice1_6k: forall r r' r'', order r -> order r' -> order r'' -> nonempty (substrate r) -> nonempty (substrate r') -> transf_axioms (fun f=> corr_value(restriction2 (second_partial_function (sof_value (product (substrate r)(substrate r')) (substrate r'')) f)) (substrate r) (set_of_increasing_mappings r' r'')) (set_of_increasing_mappings (product2_order r r') r'') (set_of_increasing_mappings r (increasing_mappings_order r' r'')).
Proof. ir. red. ir. rwi set_of_increasing_mappings_pr H4. nin H4. ee. set (f:= sof_value (product (substrate r) (substrate r')) (substrate r'')) c). assert (f=x). uf f. bwi H5. wr H5. wr H6. wr H8. uf sof_value. uf corr_value. aw. app corr_procp. am. am. rw H9. clear H9. clear f. cp (Exercice1_6j H H0 H2 H3 H7). nin (Exercice1_6h H H0 H2 H3 H7).

RR n° 7150
assert (Ha: partial_fun_axioms x). red. split. am.
rv H5. exists (substrate r). exists (substrate r'). tv. bw.
set (g:= restriction2 (second_partial_function x) (substrate r)
(set_of_increasing_mappings r' r'')).
assert (is_function g). uf g. app function_restriction2.
rv set_of_increasing_mappings_pr. exists g. ee. am. uf g.
tv. uf g. simpl. rw imo_substrate.
red. ee. am. am. app imo_order. uf g. tv.
rv imo_substrate. tv. am. am. red. uf g.
simpl. ir. rw W_restriction2. rv W_restriction2.
rw W_spfa. rw W_spfa. rv wo_pr. rv wo_pr2.value_pr. rv wo_pr2.value_pr.
uf function_order_r.
cp (Exercice1_6i H H0 H2 H3 H7 H13). cp (Exercice1_6i H H0 H2 H3 H7 H14).
rw set_of_increasing_mappings_pr. exists (second_partial_fun x x0).
ee. am. sy; am. sy; am. am. tv. am. am.
rw set_of_increasing_mappings_pr. exists (second_partial_fun x y).
ee. am. sy; am. sy; am. am. tv. am. sy; am. sy; am. sy; am. ir. rv W_spf. rv W_spf. assert (inc (J x0 i) (source x)).
rw H5. bw. aw. ee. fprops. am. am. assert (inc (J y i) (source x)).
rw H5. bw. aw. ee. fprops. am. am. red in H7. ee. app H37.
rw product2_order_pr. red. ee. ee. fprops. am. am. ee. ee. fprops.
am. am. av. wrr order_reflexivity. am. rw H10. rw H11. am.
rw H10. rw H11. am. am. rw H10. am. rw H10. am. am. am. tv.
am. am. app imo_order. app order_product2_order. am.
Qed.

Lemma Exercice1_6l: forall r r' r'', order r -> order r' -> order r'' ->
nonempty (substrate r) -> nonempty (substrate r') ->
let f:= second_partial_map2 r r' r'' in
(is_function f &
  source f = (set_of_increasing_mappings (product2_order r r') r'') &
target f = (set_of_increasing_mappings r
  (increasing_mappings_order r' r'')) &
bijective f).
Proof. ir. uf f. uf second_partial_map2. simpl. ee.
app af_function. app Exercice1_6k. tv. tv. red. split.
(* injectivity *) app injective_af_function. app Exercice1_6k. ir.
rv correspondence_extensionality1 H6.
rw correspondence_extensionality1.
set (f1:= sof_value (product (substrate r) (substrate r'))(substrate r''))
(corr_value x)).
assert (f1=x). uf f1. bwi H7. wr H7. wr H8. uf sof_value.
uf corr_value. av. app corr_propc. am. am. fold f1 in H6. wri H15 H6.
clear H15. clear f1.
set (f1:= sof_value (product (substrate r) (substrate r'))(substrate r''))
(corr_value x0)).
assert (f1=x0). uf f1. bwi H11. wr H11. wr H12. uf sof_value.
uf corr_value. av. app corr_propc. am. am. fold f1 in H6. wri H15 H6.
clear H15. clear f1.
assert (Ha: partial_fun_axioms x). red. split. am.
rw H7. exists (substrate r). exists (substrate r'). tv. bw.
assert (Hb: partial_fun_axioms x0). red. split. am.
rw H11. exists (substrate r). exists (substrate r'). tv. bw.
cp (Exercice1_6h H H0 H2 H3 H9). cp (Exercice1_6h H H0 H2 H3 H13). ee.
assert (second_partial_function x = second_partial_function x0).
app funct_extensionality. app function_spfa. app function_spfa.
simpl. rw H7; rw H11; tv.
simpl. rw H8; rw H12; rw H7; rw H11; tv.
simpl. ir. rwi H15 H19.
transitivity (W x1 (restriction2 (second_partial_function x) (substrate r)
(set_of_increasing_mappings r' r''))) .
rww W_restriction2. app Exercice1_6j. rw H6. rww W_restriction2.
app Exercice1_6j. clear H6.
assert (inc (P x1) (domain (source x))). rww H15. cp (W_spfa Ha H22).
assert (inc (P x1) (domain (source x))). rww H16. cp (W_spfa Hb H24).
assert (x1 = J (P x1) (Q x1)). sy. app pair_recov. rw H25.
assert (inc (Q x1) (range (source x))). rww H18. wr (W_spfa Ha H22 H26).
assert (inc (Q x1) (range (source x))). rww H17. wr (W_spfa Hb H24 H27).
rww H23. am. am. app order_product2_order. am. app order_product2_order. am.

(* surjectivity *) app surjective_af_function. app Exercice1_6k. ir.
rs set_of_increasing_mappings_pr H4. nin H4. ee.
assert (substrate (product2_order r r') =
product (substrate r) (substrate r')). bw.
assert (trans_axioms (fun z => W (Q z) (sof_value (substrate r')
(substrate r'')) (W (P z) x))
(substrate r') (W (P z) x))}
red. ir. set (f1:= sof_value (substrate r')(substrate r'') (W (P c) x)).
ee. assert (f1= x0). uf f1. uf sof_value. wr H14. wr H15.
wr H17. uf corr_value. aw. app corr_propc. rw H18. wr H15. app inc_W_target.
rww H14. am. am. am. am.
set (g:= BL (fun z => W (Q z) (sof_value (substrate r')
(substrate r'')) (W (P z) x))
(substrate r'') (W (P z) x))}
assert (is_function g). uf g. app af_function.
assert (increasing_fun g (product2_order r r' r'')).
red. ee. am. app order_product2_order. am. bw. tv. red. ir. simpl in H12.
simpl in H13. uf g. rww W_af_function. rww W.af_function.
set (f1:= sof_value (substrate r')(substrate r'') (W (P x0) x)).
set (f2:= sof_value (substrate r')(substrate r'') (W (P y0) x)).
aw H12; awi H13. ee. rwi H5 H17. rwi H5 H15. cp (inc_W_target H4 H17).
rsimo_substrate H20. rs set_of_increasing_mappings_pr H20. nin H20.
ee. assert (f1= x1). uf f1. uf sof_value. wr H25. wr H26.
wr H28. uf corr_value. aw. app corr_propc. rw H29.
assert (f2= x2). uf f2. uf sof_value. wr H21. wr H22.
wr H24. uf corr_value. aw. app corr_propc. rw H30.
cp (H35 _ _ H17 H15 H37). rwi imo_pr H39. ee. wr H28 H41; rwi H24 H41.
rs invo corr_value_pr H41. rwi inv_corr_value_pr H41. red in H41. ee.
assert (gle r'' (W (Q x0) x1) (W (Q x0) x2)). app H47.
assert (gle r'' (W (Q x0) x2) (W (Q y0) x2)). red in H23. ee.
appr53. wr H45. am. rww H45.
Lemma Exercice1_6m: forall r r' r'', order r -> order r' -> order r'' ->
nonempty (substrate r) -> nonempty (substrate r') ->
order_isomorphism (second_partial_map2 r r' r'')
(increasing_mappings_order (product2_order r r') r'')
(increasing_mappings_order r (increasing_mappings_order r' r'')).

Proof. ir. cp (Exercice1_6l H H0 H2 H3). cbv zeta in H4. ee.
assert (Ha: order (product2_order r r'')). app order_product2_order. 
red. ee. app imo_order. app imo_order. app imo_order. am. rw imo_substrate. 
sy; am. am. am. rw imo_substrate. sy; am. am. app imo_order. rw H5. ir. 
rrw imo_pr. rw H6. 
set (u1:= inc (W x (second_partial_map2 r r' r''))
(target (second_partial_map2 r r' r''))). assert u1. uf u1. 
app inc_W_target. set (u2:= inc (W y (second_partial_map2 r r' r''))
(target (second_partial_map2 r r' r''))). assert u2. uf u2. 
app inc_W_target. 
app iff_eq. ir. ee. am. am. ufi u1 H10; ufi u2 H11. 
cp (Exercice1_6k H H0 H1 H2 H3). unfold second_partial_map2 in H10, H11 |-*. 
rrw W_af_function H11. clear H15. 
nin H8. nin H9. ee. simpl in H10. simpl in H11. 
assert (sof_value (product (substrate r) (substrate r')) (substrate r'')
 x = x0). uf sof_value. wr H20. wr H22. uf corr_value. av. bwi H19. 
wr H19. nin x0. tv. am. am. rw H23; rwi H23 H10; clear H23. 
assert (sof_value (product (substrate r) (substrate r')) (substrate r'')
y = x1). uf sof_value. wr H18. uf corr_value. av. wr H16. bwi H15. 
wr H15. nin x1. tv. am. am. rw H23; rwi H23 H11; clear H23. 
wr inv_corr_value_pr. rw inv_corr_value_pr. rw imo_substrate. 
red. simpl. 
cp (Exercice1_6j H H0 H2 H3 H21). cp (Exercice1_6j H H0 H2 H3 H17). 
e. ee. app function_restriction2. app function_restriction2. tv. tv. tv.
assert (Hu: partial_fun_axioms x1). red. split. am. rw H15. bw.
exists (substrate r). exists (substrate r'). tv.
assert (Hv: partial_fun_axioms x0). red. split. am. rw H19. bw.
exists (substrate r). exists (substrate r'). tv.
assert (inc i (domain (source x0))). rw H19. bw. rww domain_product.
assert (inc i (domain (source x1))). rw H15. bw. rww domain_product.
assert (range (source x0) = substrate r'). rw H19. bw. rww range_product.
assert (range (source x1) = substrate r'). rw H15. bw. rww range_product.
rww W_spfa. rww W_spfa.
rw imo_pr. rw inv_corr_value_pr. rw inv_corr_value_pr.
rw set_of_increasing_mappings_pr. ee. exists (second_partial_fun x0 i).
e. app function_spf. tv. tv.
app (Exercice1_6i H H0 H2 H3 H21 H25). tv.
rw set_of_increasing_mappings_pr. ee. exists (second_partial_fun x1 i).
e. app function_spf. tv. tv.
app (Exercice1_6i H H0 H2 H3 H17 H25). tv. am. am.
red. ee. app function_spf. app function_spf. tv. tv. tv. tv.
ir. rw W_spf. rw W_spf.
nin H14. ee. wri H22 H36; wri H18 H36. rwi inv_corr_value_pr H36.
rrw inv_corr_value_pr H36. app H36. bw. fprops. am. am. rww H29. am. am.
rww H28. am. am. am. am. am.
(* converse *) ir. ee. am. am. red in H14.
set (f1: W x (second_partial_map2 r r' r'')) in *.
set (f2: W y (second_partial_map2 r r' r'')) in *.
e. cp (Exercice1_6k H H0 H1 H2 H3).
assert (f1= W x (second_partial_map2 r r' r'')). tv.
assert (f2= W y (second_partial_map2 r r' r'')). tv.
ufi second_partial_map2 H22. rwi W_af_function H22.
ufi second_partial_map2 H23. rwi W_af_function H23.
rrw set_of_increasing_mappings_pr H8; rwi set_of_increasing_mappings_pr H9.
nin H8; nin H9. ee. wr H31. wr H27. rw inv_corr_value_pr.
rrw inv_corr_value_pr. red. ee. am. am. am. am. am. ir.
assert (sof_value (product (substrate r)(substrate r')) (substrate r'')x=x0).
bwi H28. wr H28. wr H29. wr H31. uf corr_value. uf sof_value. av. nin x0. tv.
am. am. rwi H33 H22. clear H33.
assert (sof_value (product (substrate r)(substrate r')) (substrate r'')y=x1).
bwi H24. wr H24. wr H25. wr H27. uf corr_value. uf sof_value. av. nin x1. tv.
am. am. rwi H33 H23. clear H33.
bwi H32. avi H32. ee.
assert (Hu: partial_fun_axioms x1). red. split. am. rw H24. bw.
exists (substrate r). exists (substrate r'). tv.
assert (Hv: partial_fun_axioms x0). red. split. am. rw H28. bw.
exists (substrate r). exists (substrate r'). tv.
assert (inc (P i) (domain (source x1))). rw H24. bw. rww domain_product.
assert (inc (P i) (domain (source x0))). rw H28. wrr H24.
assert (inc (Q i) (range (source x1))). rw H24. bw. rww range_product.
assert (inc (Q i) (range (source x0))). rw H28. wrr H24.
assert (i \in J (P i) (Q i)). sy; app pair_recov. rw H39. cp (H20 _ H33).
rrw H22 H40. rwi H23 H40. rwi inv_corr_value_pr H40.
rwi inv_corr_value_pr H40. clear H22; clear H23; clear H21.
cp (Exercice1_6j H H0 H2 H3 H30). cp (Exercice1_6j H H0 H2 H3 H26).
rwi W_restriction2 H40. rwi W_restriction2 H40. clear H21; clear H22.
rrw W_spfa H40. rwi W_spfa H40. rwi W_spfa H40. rwi imo_pr H40. ee.
rwi inv_corr_value_pr H23. rwi inv_corr_value_pr H23. red in H23. ee.
cp (H45 _ H34). rwi W_spf H46. rwi W_spf H46. am. am. am. am. am.
(c) If \( E \neq \emptyset \), then \( \mathcal{A}(E, F) \) is a lattice if and only if \( F \) is a lattice.

We pretend that constant functions are increasing, and if \( E \neq \emptyset \), the constants \( \cdot \rightarrow x \) and \( \cdot \rightarrow x' \) compare as \( x \) and \( x' \).

Lemma constant_increasing: forall \( r \ r' \), order \( r \rightarrow order \ r' \) ->
forall \( y \) (\( Hy:inc \ y \ (substrate \ r') \)),
\((inc \ (corr_value \ (constant_function \ (substrate \ r) \ (substrate \ r') \ y \ Hy)) \)
(\(\text{set_of_increasing_mappings} \ r \ r' \)).
Proof. ir. rw set_of_increasing_mappings_pr.
exists (constant_function \ (substrate \ r) \ (substrate \ r') \ y \ Hy). ee.
app function_constant_fun. tv. tv. red. ee.
app function_constant_fun. am. am. tv. tv. tv. red. simpl. ir.
rw W_constant. rw W_constant. wrr order_reflexivity. am. am. tv. am. am.
Qed.

Lemma constant_increasing1: forall \( r \ r' \), order \( r \rightarrow order \ r' \) ->
nonempty (substrate \ r) ->
forall \( y \) (\( Hy:inc \ y \ (substrate \ r') \)) \( y' \) (\( Hy':inc \ y' \ (substrate \ r') \)),
\( (gle \ r' \ y \ y' = \)
\((gle \ (\text{increasing_mappings_order} \ r \ r') \)
\( (corr_value \ (constant_function \ (substrate \ r) \ (substrate \ r') \ y \ Hy)) \)
\( (corr_value \ (constant_function \ (substrate \ r) \ (substrate \ r') \ y' \ Hy')). \)
Proof. ir. rw imo_pr. app iff_eq. ir. ee. app constant_increasing.
app constant_increasing. aw. red. ee. app function_constant_fun.
rw W_constant. rw W_constant. am. am. am. ir. ee. awi H4. nin H1. red in H4. ee. cp (H10 _ H1).
rwi W_constant H11. rwi W_constant H11. am. am. am. am. am.
Qed.

Assume that \( F \) is a lattice; given two functions \( f \) and \( g \) we can consider \( x \mapsto \sup(f(x), g(x)) \) and \( x \mapsto \inf(f(x), g(x)) \). Since \( F \) is a lattice, if \( f \) and \( g \) are functions with target \( F \), these are functions with target \( F \).

Lemma Exercice1_6n: forall \( r \ r' \), order \( r \rightarrow order \ r' \) ->
nonempty (substrate \ r) ->
lattice \( r' = lattice \ (\text{increasing_mappings_order} \ r \ r') \).
Proof. ir. app iff_eq. clear H1. ir. uf lattice. split. app imo_order.
rwi imo_substrate. ir. assert (Hx:=H2). assert (Hy:=H3).
rwi set_of_increasing_mappings_pr H2.
rwi set_of_increasing_mappings_pr H3. nin H2; nin H3.
set (E:=substrate \ r) in *; set (E':=substrate \ r') in *.
assert (transf_axioms \ (fun i=> sup \ r' \ (W i x0) \ (W i x1)) \ E \ E')). red. ir.
ee. assert (inc \ (W c x0) \ E'). wr H10. app inc_W_target. rww H9.
assert (inc \ (W c x1) \ E'). wr H6. app inc_W_target. rww H5.
cp (lattice_sup_pr H1 H13 H14). nin H15. app (inc_arg2_substrate H15).
assert (transf_axioms \ (fun i=> inf \ r' \ (W i x0) \ (W i x1)) \ E \ E')). red. ir.
ee. assert (inc \ (W c x0) \ E')). wr H11. app inc_W_target. rww H10.
assert (inc \ (W c x1) \ E')). wr H7. app inc_W_target. rww H6.
cp (lattice_inf_pr H1 H14 H15). nin H16. app (inc_arg1_substrate H16).
set (f1:= BL \ (fun i=> sup \ r' \ (W i x0) \ (W i x1)) \ E \ E')).
sf (f2:= BL \ (fun i=> inf \ r' \ (W i x0) \ (W i x1)) \ E \ E')).
assert (is_function f1). uf f1. app af_function.
assert (is_function f2). uf f2. app af_function.
The mappings $x \mapsto \sup(f(x), g(x))$ and $x \mapsto \inf(f(x), g(x))$ are increasing, hence in $\mathcal{A}(E, F)$.

The mapping $x \mapsto \sup(f(x), g(x))$ is the supremum.
The mapping \( x \mapsto \inf(f(x), g(x)) \) is the infimum.

Conversely. Given two values \( a \) and \( b \) in \( F \), we can consider the two constant functions 

\[ x \mapsto a \quad \text{and} \quad x \mapsto b. \]

They are increasing.

Constant functions are in the same order as their value on a fixed point in \( E \). The value \( c \) of the supremum of the two functions at the point is an upper bound for \( a \) and \( b \). Given an upper bound \( c' \), we construct the constant function \( x \mapsto c' \), and compare it, and get \( c \leq c' \).
set (x3 := W y x0). assert (inc x3 E'). uf x3. uf E’. wr H14.
app inc_W_target. rww H13. exists x3. rw least_upper_bound_pr. split.
red. ee. am. ir. nin (doubleton_or H18); rw H19.
 wri H16 H28. avi H28. ufi f1 H28. rwi W_constant H28. am. am. am. am.
 ir. nin H18. set (f4:= constant_function E E’ z H18).
 assert (inc (corr_value f4) (set_of_increasing_mappings r r’)).
 uf f4. uf E. uf E’. app constant_increasing.
 assert (gle (increasing_mappings_order r r’)(corr_value f1) (corr_value f4)).
 uf f1. uf f4. uf E. uf E’. wr constant_increasing1. app H19. fprops. am.
 am. am.
 assert (gle (increasing_mappings_order r r’)(corr_value f2) (corr_value f4)).
 uf f2. uf f4. uf E. uf E’. wr constant_increasing1. app H19. fprops. am.
 am. am. cp (H11 _ H21 H22). rwi imo_pr H23. ee. red in H25. ee.
 cp (H31 _ H1). wri H16 H32. awi H32. ufi f4 H32. rwi W_constant H32. am.
 am. am. am. am. red. ir. nin (doubleton_or H18); rw H19; am. am. am. am. am.

Idem for the infimum.

cp (lattice_inf_pr H2 H7 H8).
 set (f3:= (inf (increasing_mappings_order r r’) (corr_value f1)
 (corr_value f2))) in *.
 ee. assert (inc f3 (increasing_mappings_order r r’))).
 app (inc_arg1_substrate H9). rwi imo_substrate H12.
 set (x3 := W y x0). assert (inc x3 E’). uf x3. uf E’. wr H14.
 app inc_W_target. rww H13. exists x3. rw greatest_lower_bound_pr. split.
 red. ee. am. ir. nin (doubleton_or H18); rw H19.
 wri H16 H28. avi H28. ufi f1 H28. rwi W_constant H28. am. am. am. am.
 ir. nin H18. set (f4:= constant_function E E’ z H18).
 assert (inc (corr_value f4) (set_of_increasing_mappings r r’)).
 uf f4. uf E. uf E’. app constant_increasing.
 assert (gle (increasing_mappings_order r r’)(corr_value f4) (corr_value f1)).
 uf f1. uf f4. uf E. uf E’. wr constant_increasing1. app H19. fprops. am.
 am. am.
 assert (gle (increasing_mappings_order r r’)(corr_value f4) (corr_value f2)).
 uf f2. uf f4. uf E. uf E’. wr constant_increasing1. app H19. fprops. am.
 am. am. cp (H11 _ H21 H22). rwi imo_pr H23. ee. red in H25. ee.
 cp (H31 _ H1). wri H16 H32. awi H32. ufi f4 H32. rwi W_constant H32. am.
 am. am. am. am. red. ir. nin (doubleton_or H18); rw H19; am. am. am. am. am.
Qed.

(d) Suppose that E and F are both non-empty. Then \(\mathcal{A}(E, F)\) is totally ordered if and only if one of the following conditions is satisfied:
(a) F consists in a single element;
(b) E consists in a single element and F is totally ordered;
(c) E and F are both totally ordered and F has two elements.

We first show that if \(\mathcal{A}(E, F)\) is totally ordered and E non-empty, then F is totally ordered, using constant functions as above.

RR n° 7150
Lemma Exercice1_6o: forall r r', order r -> order r'-> nonempty (substrate r)->
total_order (increasing_mappings_order r r') ->
total_order r'.

Proof. ir. nin H2. red. ee. am. ir.
  set (E:=substrate r) in *; set (E':=substrate r') in *. nin H1.
  set (f1:= constant_function E E' x H4).
  set (f2:= constant_function E E' y H5).
  assert (inc (corr_value f1) (set_of_increasing_mappings r r')).
  rw set_of_increasing_mappings_pr. exists f1. ee. uf f1.
  app function_constant_fun. tv. tv. red. ee. uf f1.
  app function_constant_fun. am. am. tv. tv. red. simpl. ir. uf f1.
  rw W_constant. rw W_constant. wrr order_reflexivity. am. am. tv. am. am.
  assert (inc (corr_value f2) (set_of_increasing_mappings r r')).
  rw set_of_increasing_mappings_pr. exists f2. ee. uf f2.
  app function_constant_fun. tv. tv. red. ee. uf f2.
  app function_constant_fun. am. am. tv. tv. red. simpl. ir. uf f2.
  rw W_constant. rw W_constant. wrr order_reflexivity. am. am. tv. am. am.
  rwi imo_substrate H3. ufi gge H3. nin (H3 _ _ H6 H7); rwi imo_pr H8; ee.
  avi H10. red in H10. ee. cp (H16 _ H1). ufi f1 H17; ufi f2 H17.
  rwi W_constant H17. rwi W_constant H17. left. am. am. am. am. am.
  avi H10. red in H10. ee. cp (H16 _ H1). ufi f1 H17; ufi f2 H17.
  rwi W_constant H17. rwi W_constant H17. right. am. am. am. am. am. am.
Qed.

If F is a singleton, then \(A(E,F)\) has a single element, hence is totally ordered. If E is a
singleton, all functions are constant and \(A(E,F)\) is isomorphic to F.

Lemma Exercice1_6p: forall r r', order r -> order r'->
is_singleton (substrate r') ->
total_order (increasing_mappings_order r r').

Proof. ir. red. ee. app imo_order. rw imo_substrate. ir. left.
  rw imo_pr. ee. am. am. red. rwi set_of_increasing_mappings_pr H2.
  rwi set_of_increasing_mappings_pr H3. nin H2. nin H3. ee.
  wr H11. aw. wr H7. aw. wr H11. aw. wr H7; aw. wr H7. aw.
  wr H7. wr H11. ir. aw. assert (inc (W i x0) (substrate r')). wr H9.
  app inc_W_target. rw H8. assert (inc (W i x1) (substrate r')). wr H5.
  app inc_W_target. rw H4. nin H1. rwi H1 H13; rwi H1 H14.
  rw (singleton_eq H13). rw (singleton_eq H14). wrr order_reflexivity.
  rw H1. fprops. am. am. am. am. am.
Qed.

Lemma Exercice1_6q: forall r r', order r -> order r'->
is_singleton (substrate r) -> total_order r' ->
total_order (increasing_mappings_order r r').

Proof. ir. red. ee. app imo_order. rw imo_substrate. nin H1.
  ir. uf gge. rw imo_pr. rw imo_pr. cp H3; cp H4.
  rwi set_of_increasing_mappings_pr H3. nin H3.
  rwi set_of_increasing_mappings_pr H4. nin H4. ee.
  set (a:= W x x1). set (b:= W x x2).
  assert (inc a (substrate r')). wr H12. uf a. app inc_W_target. rw H11.
  rw H1. fprops.
  assert (inc b (substrate r')). wr H8. uf b. app inc_W_target. rw H7.
  rw H1. fprops.
  assert (forall u, inc u (substrate r) -> W u x1 = a). ir.
  rwi H1 H17. rw (singleton_eq H17). tv.
  assert (forall u, inc u (substrate r) -> W u x2 = b). ir.
  rwi H1 H18. rw (singleton_eq H18). tv.

INRIA
Assume that $E$ and $F$ are two totally ordered sets, and $F$ has two elements. We may assume that these elements are distinct and satisfy $a < b$. Assume $f(u) < g(u)$. Then $f(u) = a$ and $g(u) = b$. If no such $u$ exists, then $f \geq g$. Otherwise, consider $v$; if $f(v) > g(v)$ we get $f(v) = b$ and $g(v) = a$. Since $u$ and $v$ can be compared, this implies that one of $f$ and $g$ is non-increasing.

Lemma Exercice1_6r: forall $r \ r'$, order $r$ -> order $r'$ ->
  total_order $r$ -> total_order $r'$ ->
  (exists $a$, exists $b$, substrate $r' = doubleton a b$) ->
  total_order (increasing_mappings_order $r \ r'$).
Proof. ir. nin H3; nin H3. nin (equal_or_not x x0).
  app Exercice1_6p. rw H3. rw H4. rw doubleton_singleton. exists x0. tv.
  assert (exists $u$, exists $v$, substrate $r' = doubleton u v \& glt r' u v$).
  red in H2. ee. assert (inc $x$ (substrate $r'$)). rw H3. fprops.
  assert (inc $x0$ (substrate $r'$)). rw H3. fprops.
  nin (H5 _ _ H6 H7). exists x. exists x0. split. am. red. ee. am. am.
  exists x0. exists x. split. rw doubleton_symm. am. red. ee. am. intuition.
  clear H3. clear H4. nin H5. nin H6. nin H3.
  red. ee. app imo_order. rwi set_of_increasing_mappings. ir. cp H5; cp H6.
  rwi set_of_increasing_mappings. ir. cp H5; cp H6.
  assert (forall $u$, inc $u$ (substrate $r$) -> glt $r'$ (W $u$ x4) (W $u$ x5) ->
  (W $u$ x4 = x1 & W $u$ x5=x2)). ir.
  cp (inc_lt1_substrate H18). cp (inc_lt2_substrate H18). rwi H3 H19.
  rwi H3 H20.
  nin (doubleton_or H19); nin (doubleton_or H20);rwi H21 H18; rwi H22 H18.
  nin H18. elim H23. tv. split;am. nin H18. nin H4.
  cp (order_antisymmetry H0 H4 H18). elim H23. sy; am. nin H18. elim H23. tv.
  nin (p_or_not_p (exists $u$, inc $u$ (substrate $r$)& glt $r'$ (W $u$ x4) (W $u$ x5)))
  aw. assert (inc (W $i$ x4) (substrate $r'$)). wr H14. app inc_W_target.
  rwi H13. assert (inc (W $i$ x5) (substrate $r'$)). wr H10. app inc_W_target.
  rwi H9. nin H2. rwi H3 H21. rwi H3 H22. nin (doubleton_or H21).
  rwi H24. nin (doubleton_or H22); rwi H25. wrr order_reflexivity.
  rw H3. fprops. nin H4. am. rw H24. nin (doubleton_or H22); rwi H25.
  cp (H17 _ H18 H19). nin H1. assert (inc x6 (source x5)). rw H9.
  assert (inc i (source x5)). rw H9. nin (H27 _ H18 H20).
  red in H11. ee. cp (H36 _ H28 H29 H30). simpl in H37.
  rwi H31 H37. rwi H25 H37. am. red in H30. red in H15. ee.
  rwi H9 H28; rwi H9 H29; wri H13 H28; wri H13 H29.
  cp (H36 _ H29 H28 H30). simpl in H37.
  rwi H24 H37. rwi H26 H37. am. wrr order_reflexivity. rw H3. fprops.
  am. am. ir. right. red. rw imo_pr. ee. am. am. red. ee. wr H12. aw. wr H16.
  aw. assert (inc (W $i$ x4) (substrate $r'$)). wr H14. app inc_W_target.
  rwi H13. assert (inc (W $i$ x5) (substrate $r'$)). wr H10. app inc_W_target.
Converse. Assume \( \mathcal{A}(E,F) \) totally ordered, both sets \( E \) and \( F \) non-empty. We may assume that \( F \) is totally ordered and that both sets have at least two elements. We may assume that \( b < b' \) in \( F \).

Lemma Exercice1_6s: for all \( r, r' \), order \( r \rightarrow \) order \( r' \rightarrow 
\) nonempty \( \text{substrate}(r) \rightarrow \) nonempty \( \text{substrate}(r') \rightarrow 
\) total_order \( \text{increasing_mappings_order}(r, r') \rightarrow 
\) \((\text{is_singleton}(r') \lor \text{is_singleton}(r) \land \text{total_order}(r') \lor \text{total_order}(r) \land \exists u, \exists v, \text{substrate}(r') = \text{doubleton}(u, v)) \).

Proof. ir. \( cp \) (Exercice1_6o H H0 H1 H3). nin H2.
\( \text{nin} \) \( (\text{equal_or_not}(\text{substrate}(r'), \text{singleton}(y))) \). ir. left.
exists \( y \). tv. ir. right. \( \text{nin} \) H1.
\( \text{nin} \) \( (\text{equal_or_not}(\text{substrate}(r), \text{singleton}(y0))) \). ir. left. split.
exists \( y0 \). tv. am. ir. \( \text{right. split. am.} \)
assert \( (\exists y1, \text{inc}(y1, \text{substrate}(r') \land y1 \neq y)) \). app exists-proof. red.
ir. \( \text{elim} \) H5. set_extens. \( \text{nin} \) \( (\text{equal_or_not}(x, y)) \). rw H9. fprops.
elim \( (H7 x) \). intuition. \( \text{rw} \) \( (\text{singleton_eq}(H8)) \). am. \( \text{nin} \) H7.
assert \( (\exists u, \exists v, \text{inc}(u, \text{substrate}(r') \land \text{inc}(v, \text{substrate}(r') \land \text{gle}(r, u, x0) \land y \lor \text{gle}(r, v, x0) \land y0)) \). app exists-proof. red.
ir. \( \text{elim} \) H6. set_extens. \( \text{nin} \) \( (\text{equal_or_not}(x, y0)) \). rw H8. fprops.
elim \( (H5 x2) \). intuition. \( \text{rw} \) \( (\text{singleton_eq}(H7)) \). am. \( \text{nin} \) H5.
rename \( y0 \) into \( a \); rename \( x2 \) into \( a' \); rename \( x0 \) into \( b \); rename \( x1 \) into \( b' \).

Consider the mapping \( f_u \) that associates \( b \) if \( x \leq u \) and \( b' \) otherwise. Assume \( x \leq x' \); the relation \( f(x) \leq f(x') \) is true if one of the values is \( f(x') \) is \( b' \). Otherwise we have \( x' \leq u \), thus \( x \leq u \) and \( f(x) = b \). Thus \( f_u \) is increasing. Consider similarly \( f_v \). Since \( \mathcal{A}(E,F) \) is totally ordered, we may compare the functions. If \( f_u \leq f_v \) we have \( f_u(v) \leq f_v(v) = b \). We cannot have \( f_u(v) = b' \), hence \( v \leq u \). Similarly if \( f_v \leq f_u \) we have \( u \leq v \).

assert (total_order r). red. ee. am. ir.
set \( \text{(f1:= fun u=> Yo (gle r u x0) b b')}. \)
assert (transf_axioms f1 (substrate r) (substrate r')). red. ir. uf f1. \( \text{nin} \) (equal_or_not (gle r c x0)). ir.
rw Y_if_rw. ir. \( \text{rw} \) Y_if_not_rw.
assert (inc (corr_value (BL f1 (substrate r) (substrate r')))).
(\( \text{set_of_increasing_mappings}(r, r') \)). \( \text{rw} \) \( \text{set_of_increasing_mappings_pr} \).
exists (BL f1 (substrate r) (substrate r')). ee. app af_function. tv. tv.
red. ee. app af_function. am. am. tv. tv. red. ir. simpl in H14.
simpl in H15. \( \text{rw} \) W_af_function. \( \text{rw} \) W_af_function. uf f1.
\( \text{nin} \) (p_or_not_p (gle r x1 x0)). ir. \( \text{rw} \) Y_if_rw.
\( \text{nin} \) (p_or_not_p (gle r y1 x0)). ir. \( \text{rw} \) Y_if_rw.
\( \text{wrr} \) order_reflexivity. ir. \( \text{rw} \) Y_if_not_rw. \( \text{nin} \) H9. am. ir.
rw Y_if_not_rw. \( \text{nin} \) (p_or_not_p (gle r y1 x0)). ir.
rw Y_if_rw. elim H16. app (order_transitivity H H15 H17). ir.
We pretend now that $F$ has at most two elements. We use contradiction. We are reduced to analyze the case where $F$ has three elements satisfying $x_0 < x_1 < x_2$.

The set $E$ has two elements $c < c'$; we could use the same argument as above, but we use here inf($a, a'$) < sup($a, a'$). We consider two functions. First the constant function $f: x \mapsto x_1$; then the function $g$ that associates $x_0$ if $x \leq c$ and $x_2$ otherwise. The same arguments as above show that they are increasing. Since $\mathcal{A}(E, F)$ is totally ordered, we may compare them. We have $f(u) < g(v)$ and $f(u) > g(u)$.

set (f:=corr_value(constant_function (substrate r) (substrate r') x1 H8)).
assert (inc f (set_of_increasing_mappings r r')).

7. In order that every mapping of an ordered set \( E \) into an ordered set \( F \) with at least two elements, which is both an increasing and a decreasing mapping, should be constant on \( E \), it is necessary and sufficient that \( E \) should be connected with respect to the reflexive and symmetric relation “\( x \) and \( y \) are comparable” (Chapter II, § 6, Exercise 10). This condition is satisfied if \( E \) is either left or right directed.

If \( F \) is empty or has a single element, the all functions with values in \( F \) are constant. This explains why \( F \) is assume to have at least two elements. Denote the relation by \( x \sim y \). We start, as in Exercise 4, with some properties of the connected components of this relation.

Definition comp_rel \( r := \text{fun } x y \Rightarrow (\text{gle } r x y \lor \text{gle } r y x) \).
Definition cr_equiv r :=
  Exercice1.Sgraph (comp_rel r) (substrate r).

Definition cr_component r :=
  Exercice1.connected_comp (comp_rel r) (substrate r).

Lemma cr_properties: forall r, order r ->
  (is_equivalence (cr_equiv r) &
   (forall x y, comp_rel r x y -> (inc x (substrate r) & inc y (substrate r))) &
   substrate (cr_equiv r) = substrate r &
   (forall x, inc x (substrate r) -> class (cr_equiv r) x = cr_component r x) &
   (forall x y, comp_rel r x y -> related (cr_equiv r) x y)).

Proof. ir. uf cr_equiv. uf cr_component.

assert (forall x y : Set, comp_rel r x y -> (inc x (substrate r) & inc y (substrate r))). ir. nin H0.

split. app (inc_arg1substrate H0). app (inc_arg2substrate H0).

split. app (inc_arg2substrate H0). app (inc_arg1substrate H0).

assert (reflexive_r (comp_rel r) (substrate r)).

red. ir. app iff_eq. uf comp_rel. ir. intuition. uw. wrr order_reflexivity. left. am.

ir. nin (H0 _ _ H1). am.

assert (symmetric_r (comp_rel r)). red. uf comp_rel. ir. intuition.

assert (forall x y, comp_rel r x y -> inc x (substrate r)).

ir. nin (H0 _ _ H3). am.

ee. app Exercice1.equivalence_Sgraph. am. app Exercice1.substrate_Sgraph.

ir. app Exercice1.connected_comp_class.

ir. red. uf Exercice1.Sgraph. uf graph_on. ee. Ztac. nin (H0 _ _ H4).

fprops. red. aw. exists (Exercice1.chain_pair x y). ee. simpl. am.

tv. tv.

Qed.

Given two elements of $E$, if they have an upper bound or lower bound, this bound is related to both elements. Thus $E$ is directed, it has a single component.

Lemma Exercice1_7a: forall r x, right_directed r ->
  inc x (substrate r) -> cr_component r x = substrate r.

Proof. ir. rwi right_directed_pr H. nin H. cp (cr_properties H). ee. wr H5.

app extensionality. wr H4. app sub_class_substrate. red. ir. bw.

nin (H1 _ _ H0 H7). nin H8. nin H9. assert (related (cr_equiv r) x x1).

app H6. red. left. am. assert (related (cr_equiv r) x1 x0).

app H6. red. right. am. apply transitivity_e with x1. am. am.

nin H2. am. nin H2; am. am.

Qed.

Lemma Exercice1_7b: forall r x, left_directed r ->
  inc x (substrate r) -> cr_component r x = substrate r.

Proof. ir. rwi left_directed_pr H. nin H. cp (cr_properties H). ee. wr H5.

app extensionality. wr H4. app sub_class_substrate. red. ir. bw.

nin (H1 _ _ H0 H7). nin H8. nin H9. assert (related (cr_equiv r) x x1).

app H6. red. right. am. assert (related (cr_equiv r) x1 x0).

app H6. red. left. am. apply transitivity_e with x1. am. am.

nin H2. am. nin H2; am. am.

Qed.

If $f$ is increasing and decreasing, $x$ and $y$ are related, then $f(x) = f(y)$.

Lemma Exercice1_7c: forall r r' f x y, increasing_fun f r r' ->
decreasing_fun f r r' -> comp_rel r x y ->
W x f = W y f.
Proof. ir. assert (order r). nin H; ee; am.
assert (inc x (substrate r) & inc y (substrate r)).
destruct (cr_properties H2) as [._ [H3_.]]. app H3. nin H3. nin H. ee.
nin H1. cp (H9 _ _ H3 H4 H1). cp (H14 _ _ H3 H4 H1). red in H16.
ap (order_antisymmetry H11 H15 H16). cp (H9 _ _ H4 H3 H1).
Qed.

If \( f \) is increasing and decreasing, then \( f \) is constant on chains. If \( E \) is the class of \( x \), every element \( u \in E \) is chained to \( x \), \( f(u) = f(x) \) hence \( f \) is constant.

Lemma Exercice1_7d: \( \forall r \ r', \, \text{increasing_fun}\ f\ r\ r' \rightarrow \text{decreasing_fun}\ f\ r\ r' \rightarrow\)
\( \exists x, \text{inc} x (\text{substrate} r) \land \text{cr_component} r x = \text{substrate} r \)
\( \rightarrow \text{(is_constant_function} f) \).
Proof. ir. assert (order r). nin H; ee; am. cp (cr_properties H2). ee.
nin H1. ee.
assert (forall x y, \text{comp_rel} r x y \rightarrow W x f = W y f). ir.
app (Exercice1_7c H H0 H9). assert (is_function f). nin H; ee; am.
red. ee. am. ir. assert (source f = substrate r). sy; red in H; ee; am.
assert (forall u, inc u (source f) -> W u f = W x f). ir. rwi H13 H14.
assert (related (cr_equiv r) u x). apply symmetricity. am. am.
Qed.

Converse. We assume that \( F \) is a set with at least two elements \( a \) and \( b \), and that \( E \) contains \( c \) such that the component \( C \) of \( c \) is not \( E \) (if \( c' \) is another element of \( E \), the components of \( c \) and \( c' \) are equal of disjoint, so that the component of \( c' \) cannot be \( E \)). We consider the function \( g \) that maps \( x \) to \( a \) if \( x \in C \), and to be otherwise. This is a non-constant function since since is a nonempty strict subset of \( C \).

Lemma Exercice1_7e: \( \forall r \ r', \, \text{order} r \rightarrow \text{order} r' \rightarrow\)
\( \exists u, \text{exists} v, \text{inc} u (\text{substrate} r') \land \text{inc} v (\text{substrate} r') \land u <> v)\)
\( \rightarrow \exists x, \text{inc} x (\text{substrate} r) \land \text{cr_component} r x <> \text{substrate} r \)
\( \rightarrow \exists f, \text{increasing_fun} f r r' \land \text{decreasing_fun} f r r' \land\)
\( \neg(\text{is_constant_function} f) \).
Proof. ir. nin H1. nin H1. nin H2. ee. cp (cr_properties H). ee.
set (f := (fun u => Yo (inc u (cr_component r x1)) x x0)).
assert (transf_axioms f (substrate r) (substrate r')). red. ir.
uf f. nin (p_or_not_p (inc c (cr_component r x1))). ir. rww Y_if_rw.
ir. rww Y_if_not_rw.
set (g := BL f (substrate r) (substrate r')).
assert (is_function g). uf g. app af_function.
We pretend that if \( x \leq y \) then either both or none of \( x \) and \( y \) are in \( C \). This is equivalent to say that if \( x \sim y \) then either both or none of \( x \) and \( y \) is related to \( c \), and is a consequence of the transitivity of \( \sim \). It follows \( g(x) = g(y) \), thus \( g(x) \leq g(y) \), and \( g(x) \geq g(y) \). This means that \( g \) is increasing and decreasing.

8. Let \( E \) and \( F \) be two ordered sets, let \( f \) be an increasing mapping of \( E \) into \( F \), and \( g \) an increasing mapping of \( F \) into \( E \). Let \( A \) (resp. \( B \)) be the set of all \( x \in E \) (resp. \( y \in F \)) such that \( g(f(x)) = x \) (resp. \( f(g(y)) = y \)). Show that the two ordered sets \( A \) and \( B \) are canonically isomorphic.

The restriction of the function \( f \) is a bijection from \( A \) onto \( B \). It is clearly increasing.

Lemma Exercice1_8: forall r r' f g,
let A := Zo (substrate r) (fun z => W (W z f) g = z) in
let B := Zo (substrate r') (fun z => W (W z g) f = z) in
increasing_fun f r r' -> increasing_fun g r' r ->
exists h, order_isomorphism h (induced_order r A)(induced_order r' B).
Proof. ir. assert (forall x, inc x A -> inc (W x f) B). ir. ufi A H1. Ztac.
rw H3. assert (forall x, inc x B -> inc (W x g) A). ir. ufi B H2. Ztac.
clear H2. uf A. Ztac. red in H0. ee. rw H7. app inc_W_target. wr H6. rww H4.
set (h:=restriction2 f A B). assert (restriction2_axioms f A B).
red. red in H. ee. am. uf A. wr H5. app Z_sub. wr H6. uf B. app Z_sub.

RR n° 7150
9. *If $E$ is a lattice, prove that
$$\sup \left( \inf \left( x_{ij} \right) \right) \leq \inf \left( \sup \left( x_{ij} \right) \right)$$
for every finite “double” family $(x_{ij})$. *

In a lattice, if a set has a supremum or an infimum, the same is true if we add an element.

Lemma lattice_finite_sup1: forall r X x a, lattice r ->
sub X (substrate r) -> least_upper_bound r X x -> inc a (substrate r) ->
least_upper_bound r (tack_on X a) (sup r x a).
Proof. ir. assert (order r). red in H; ee; am.
assert (sub (tack_on X a) (substrate r)). app tack_on_sub.
rwi (least_upper_bound_pr x H3 H0) H1. ee.
assert (inc x (substrate r)). red in H1. ee. am.
cp (lattice_sup_pr H H6 H2). ee.
rw (least_upper_bound_pr (sup r x a) H3 H4). ee. red. ee.
app (inc_arg2_substrate H7). ir. rwi tack_on_inc H10. nin H10. red in H1.
ee. cp (H11 _ H10). apply order_transitivity with x. am. am. am. rw H10.
ir. red in H10. app H9. ee. app H5. red. ee. am. ir. app H11. fprops. ee.
app H11. fprops.
Qed.

Lemma lattice_finite_inf1: forall r X x a, lattice r ->
sub X (substrate r) -> greatest_lower_bound r X x -> inc a (substrate r) ->
greatest_lower_bound r (tack_on X a) (inf r x a).
Proof. ir. assert (order r). red in H; ee; am.
assert (sub (tack_on X a) (substrate r)). app tack_on_sub.
rwi (greatest_lower_bound_pr x H3 H0) H1. ee.
assert (inc x (substrate r)). red in H1. ee. am.
cp (lattice_inf_pr H H6 H2). ee.
rw (greatest_lower_bound_pr (inf r x a) H3 H4). ee. red. ee.
app (inc_arg1_substrate H7). ir. rwi tack_on_inc H10. nin H10. red in H1.
A proof by induction shows that a finite set has a supremum and an infimum.

Lemma lattice_finite_sup2: forall r x, lattice r ->
  is_finite_set x -> nonempty x -> sub x (substrate r) ->
  has_supremum r x.
Proof. ir. app (finite_set_induction2 (fun x => (sub x (substrate r)))
  (fun x => has_supremum r x)). ir.
  assert (inc a (substrate r)). app H3. fprops. wr (doubleton_singleton a).
  red in H. ee. nin (H5 _ _ H4 H4). am. ir.
  assert (inc b (substrate r)). app H5. fprops.
  assert (sub a (substrate r)). apply sub_trans with (tack_on a b). fprops.
  am. cp (H3 H7 H4). red in H8. nin H8. exists (sup r x0 b).
  ap (lattice_finite_sup1 H H7 H8 H6).
Qed.

Lemma lattice_finite_inf2: forall r x, lattice r ->
  is_finite_set x -> nonempty x -> sub x (substrate r) ->
  has_infimum r x.
Proof. ir. app (finite_set_induction2 (fun x => (sub x (substrate r)))
  (fun x => has_infimum r x)). ir.
  assert (inc a (substrate r)). app H3. fprops. wr (doubleton_singleton a).
  red in H. ee. nin (H5 _ _ H4 H4). am. ir.
  assert (inc b (substrate r)). app H5. fprops.
  assert (sub a (substrate r)). apply sub_trans with (tack_on a b). fprops.
  am. cp (H3 H7 H4). red in H8. nin H8. exists (inf r x0 b).
  ap (lattice_finite_inf1 H H7 H8 H6).
Qed.

If $F$ is a finite subset of $E$, then $x \leq \inf F$ if and only if $x \leq y$ for all $y \in F$.

Lemma lattice_finite_sup3: forall r x y, lattice r ->
  is_finite_set x -> nonempty x -> sub x (substrate r) ->
  gle r (supremum r x) y = (forall z, inc z x -> gle r z y).
Proof. ir. cp (lattice_finite_sup2 H H0 H1 H2).
  assert (order r). red in H; ee; am.
  cp (supremum_pr H4 H2 H3). ee. app iff_eq. ir. red in H5. ee.
  cp (H9 _ H8). apply order_transitivity with (supremum r x). am. am. am.
  ir. app H6. red. ee. nin H1. cp (H7 _ H1). app (inc_arg2_substrate H8). am.
Qed.

Lemma lattice_finite_inf3: forall r x y, lattice r ->
  is_finite_set x -> nonempty x -> sub x (substrate r) ->
  gle r y (infimum r x) = (forall z, inc z x -> gle r y z).
Proof. ir. cp (lattice_finite_inf2 H H0 H1 H2).
  assert (order r). red in H; ee; am.
  cp (infimum_pr H4 H2 H3). ee. app iff_eq. ir. red in H5. ee.
  cp (H9 _ H8). apply order_transitivity with (infimum r x). am. am. am.
  ir. app H6. red. ee. nin H1. cp (H7 _ H1). app (inc_arg1_substrate H8). am.
Qed.

If $f$ is a family, with source $I$ and target $E$, if $I$ is finite, then $x \leq \inf_{i \in I} f(i)$ if and only if $x \leq f(i)$ for all $i \in E$. 

RR n° 7150
Lemma lattice_finite_sup4: forall r f y, lattice r ->
  fgraph f -> is_finite_set (domain f) -> nonempty (domain f) ->
  sub (range f) (substrate r) ->
  gle r (sup_graph r f) y = (forall z, inc z (domain f) -> gle r (V z f) y).
Proof. ir. uf sup_graph. rw lattice_finite_sup3.
  app iff_eq. ir. app H4. app inc_V_range. ir. rwi frange_inc_rw H5.
  nin H5. ee. rw H6. app H4. am. am. app finite_range. nin H2.
  exists (V y0 f). app inc_V_range. am.
Qed.

Lemma lattice_finite_inf4: forall r f y, lattice r ->
  fgraph f -> is_finite_set (domain f) -> nonempty (domain f) ->
  sub (range f) (substrate r) ->
  gle r y (inf_graph r f) = (forall z, inc z (domain f) -> gle r y (V z f)).
Proof. ir. uf inf_graph. rw lattice_finite_inf3.
  app iff_eq. ir. app H4. app inc_V_range. ir. rwi frange_inc_rw H5.
  nin H5. ee. rw H6. app H4. am. am. app finite_range. nin H2.
  exists (V y0 f). app inc_V_range. am.
Qed.

Lemma lattice_finite_sup5: forall r f, lattice r ->
  fgraph f -> is_finite_set (domain f) -> nonempty (domain f) ->
  sub (range f) (substrate r) ->
  inc (sup_graph r f) (substrate r).
Proof. ir. assert (has_sup_graph r f). uf has_sup_graph.
  app lattice_finite_sup2. app finite_range. nin H2. exists (V y f).
  app inc_V_range. red in H. ee. cp (is_sup_graph_pr1 H H3 H4).
  rwi least_upper_bound_pr H6. ee. red in H6. ee. am. am. am.
Qed.

Lemma lattice_finite_inf5: forall r f, lattice r ->
  fgraph f -> is_finite_set (domain f) -> nonempty (domain f) ->
  sub (range f) (substrate r) ->
  inc (inf_graph r f) (substrate r).
Proof. ir. assert (has_inf_graph r f). uf has_inf_graph.
  app lattice_finite_inf2. app finite_range. nin H2. exists (V y f).
  app inc_V_range. red in H. ee. cp (is_inf_graph_pr1 H H3 H4).
  rwi greatest_lower_bound_pr H6. ee. red in H6. ee. am. am. am.
Qed.

Applying the previous lemmas in one direction gives inf_i x_i_j \leq x_i_j \leq sup_j x_i_j; apply it in
the other direction gives the result.

Lemma Exercice1_9: forall I1 I2 r f,
  lattice r -> fgraph f -> domain f = product I1 I2 ->
  is_finite_set I1 -> is_finite_set I2 -> nonempty I1 -> nonempty I2 ->
  sub (range f) (substrate r) ->
  gle r (sup_graph r (L I2 (fun j => inf_graph r (L I1 (fun i => V (J i j) f))))))
  (inf_graph r (L I1 (fun i => sup_graph r(L I2 (fun j => V (J i j) f))))))).
Proof. ir. assert (Ha: order r). red in H; ee; am.
  assert (Hb: forall i j, inc i I1 -> inc j I2 ->
    inc (V (J i j) f) (substrate r)). ir. app H6. app inc_V_range. rw H1.
  fprops.
  rw lattice_finite_sup4. ir. bwi H7. rw lattice_finite_inf4. ir.
  bwi H8. bw.
  apply order_transitivity with (V (J z0 z) f). am.
  set (fa:= (L I1 (fun i : Set => V (J i z) f)))).
assert (fgraph fa). uf fa. gprops. assert (is_finite_set (domain fa)).
uf fa. bw. assert (nonempty (domain fa)). uf fa. bw.
assert (sub (range fa) (substrate r)). uf fa. red. ir. rwi fringe_inc_rw H12.
cp (lattice_finite_inf4 (inf_graph r fa) H H9 H10 H11 H12).
assert (gle r (inf_graph r fa) (inf_graph r fa)). wr order_reflexivity.
app lattice_finite_inf5. am. rwi H13 H14.
assert (V (J z0 z) f = V z0 fa). uf fa. bw. tv. rw H15. app H14. uf fa. bw.
set (fb:= L I2 (fun j : Set => V (J z0 j) f)).
assert (fgraph fb). uf fb. gprops. assert (is_finite_set (domain fb)).
uf fb. bw. assert (nonempty (domain fb)). uf fb. bw.
assert (sub (range fb) (substrate r)). uf fb. red. ir. rwi fringe_inc_rw H12.
cp (lattice_finite_sup4 (sup_graph r fb) H H9 H10 H11 H12).
assert (gle r (sup_graph r fb) (sup_graph r fb)). wr order_reflexivity.
app lattice_finite_sup5. am. rwi H13 H14.
assert (V (J z0 z) f = V z fb). uf fb. bw. tv. rv H15. app H14. uf fb. bw.
am. gprops. bw. bw. red. ir. rwi fringe_inc_rw H8. nin H8. bwi H8. ee.
rv H9. app lattice_finite_sup5. gprops. bw. bw.
red. ir. rwi fringe_inc_rw H10. nin H10. bwi H10. bwi H11.
rvw H11. app Hb. am. gprops. ee;am. gprops. am. gprops. bw. bw.
red. ir. rwi fringe_inc_rw H7. nin H7. bwi H7. bwi H8. rw H8.
app lattice_finite_inf5. gprops. bw. bw. red. ir.
am. gprops. ee;am. gprops.
Qed.

10. Let \(E\) and \(F\) be two lattices. Then a mapping \(f\) of \(E\) into \(F\) is increasing if and only if

\[ f(\inf(x,y)) \leq \inf(f(x),f(y)) \]

for all \(x \in E\) and \(y \in E\).

* Give an example of an increasing mapping \(f\) of the product ordered set \(\mathbb{N} \times \mathbb{N}\) into the orders set \(\mathbb{N}\) such that the relation

\[ f(\inf(x,y)) = \inf(f(x),f(y)) \]

is false for at least one pair \((x,y) \in \mathbb{N} \times \mathbb{N}\).

If \(a, b, c,\) and \(d\) are integers we have \((a,b) \leq (c,d)\) if and only if \(a \leq c\) and \(b \leq d\). The infimum of these two quantities is \((\inf(a,c),\inf(b,d))\). The function \(f : (x,y) \mapsto x + y\) is increasing. If we take \(x = (1,0)\) and \(y = (0,1)\), then \(f(x) = f(y) = 1\), the infimum is \((0,0)\) and the value is 0; this is the counter example. The main result is straightforward.

Lemma exercise1_10: forall r r' f,

\[
\text{lattice } r \rightarrow \text{lattice } r' \rightarrow \text{is_function } f \rightarrow \text{substrate } r = \text{source } f \rightarrow \\
\text{substrate } r' = \text{target } f \rightarrow \\
(\text{increasing_fun } f \text{ } r \text{ } r') = \\
(\forall x y, \text{inc } x \text{ } \text{substrate } r) \rightarrow \text{inc } y \text{ } \text{substrate } r \rightarrow \\
\text{gle } r' \left( \text{W } f \text{ } f \text{ } f \right) \left( \text{W } f \text{ } f \right)).
\]

Proof. ir. ap iff_eq. ir. red in H4; ee.

destruct (lattice_inf_pr H H5 H6) as [Ha [Hb _]].
assert (inc (inf r x y) (source f)). wr H2. app (inc_arg1_substrate Ha).
  rwi H2 H5; rwi H2 H6. cp (H11 _ _ H12 H5 Ha). cp (H11 _ _ H12 H6 Hb).
  simpl in H13; simpl in H14. cp (inc_W_target H4 H5). cp (inc_W_target H4 H6).
  ir. cp H; nin H. red. ee; try am. nin H0; am. red. ir.
  rwi H2 H4. cp (H4 _ _ H7 H8). rwi (inf_comparable1 H H9) H10.
  cp (inc_W_target H1 H7). cp (inc_W_target H1 H8). wri H3 H11; wri H3 H12.
  destruct (lattice_inf_pr H0 H11 H12) as [_ [Hb _]].
  nin H0. ap (order_transitivity H0 H10 Hb).

11. A lattice \( E \) is said to be complete if every subset of \( E \) has a least upper bound and a
greatest lower bound in \( E \); this means in particular that \( E \) has a greatest and a least element.

(a) Show that if an ordered set \( E \) is such that every subset of \( E \) has a least upper bound in
\( E \), then \( E \) is a complete lattice.

The first claim is obvious: it suffices to take the supremum of infimum of the emptyset.
The second claim is easy: Let \( X \) be a set and \( X' \) be the set of lower bounds. If \( X' \) has a suprema-
mum, this is the infimum of \( X \).

Definition complete_lattice r := order r &
  forall X, sub X (substrate r) -> (has_supremum r X & has_infimum r X).

Lemma exercise1_11a: forall r, complete_lattice r ->
  ((exists a, greatest_element r a) & (exists b, least_element r b)).
Proof. ir. nin H. assert (sub emptyset (substrate r)). ap sub_emptyset_any.
  nin (H0 _ H1). nin H2. nin H3. rwi (least_upper_bound_emptyset x H) H2.
  rwi (greatest_lower_bound_emptyset x0 H) H3.
  split. exists x0; am. exists x; am.
Qed.

Lemma exercise1_11b: forall r, order r ->
  (forall X, sub X (substrate r) -> has_supremum r X) ->
  complete_lattice r.
Proof. ir. red. split. am. ir. split. nin (H0 _ H1). exists x. am. red.
  set (Z := (Zo (substrate r) (fun z => lower_bound r x z))).
  assert (sub Z (substrate r)). uf Z; app Z_sub. nin (H0 _ H2).
  exists x. rwi (least_upper_bound_pr x H H2) H3. nin H3.
  rw (greatest_lower_bound_pr x H H1). split. red. split.
Qed.

(b) A product of ordered sets is a complete lattice if only if each of the factors is a complete
lattice.

Let \( X \) be a subset of \( \prod E_i \) and \( X_i = \text{pr}_i X \). If each \( E_i \) is a complete lattice, then \( \sup X_i \) is the
supremum of the set \( X_i \), and \( i \mapsto \sup X_i \) is the supremum of \( X \). Conversely, if the product is a
complete lattice, it is non-empty since it has a smallest element. If \( X_i \subset E_i \) we can find a set
\( X \) with \( X_i = \text{pr}_i X \). If \( x \) is the supremum of \( X \) then \( x_i \) is the supremum of \( X_i \).

Lemma exercise1_11c: forall f g, axioms_product_order f g ->
(forall i, inc i (domain f) -> complete_lattice (V i g)) ->
complete_lattice (product_order f g).

Proof. ir. app exercise1_11b. fprops.
assert (Ha:substrate (product_order f g) = productb f).
app substrate_product_order. assert (Hb:=H). red in H; ee. ir.
set (Xi := fun i => (image_by_fun (pr_i f i) X)).
assert (forall i, inc i (domain f) -> sub (Xi i) (substrate (V i g))).
ir. rw H4. uf Xi. assert (target (pr_i f i) = (V i f)). tv. wr H7.
uf image_by_fun.
assert (is_function (pr_i f i)). app function_pri.
apply sub_trans with (range (graph (pr_i f i)))). app sub_image_by_graph.
fprops. app range_correspondence. nin H8; am. am.
set (v:= L (domain f) (fun i => supremum (V i g)(Xi i))).
assert (forall i, inc i (domain f) -> least_upper_bound (V i g) (Xi i)(V i v)).
ir. nin (H0 _ H7). cp (H6 _ H7). nin (H9 _ H10). uf v. bw. app supremum_pr1.
assert (inc v (substrate (product_order f g))). rw Ha.
rw productb_pr. ee. uf v. gprops. uf v. bw. ir. ufi v H8. bwi H8.
exists v. rw least_upper_bound_pr. split. red. split. am.
ir. rw related_product_order. rwi Ha H5; rwi Ha H8. ee. app H5. am.
ir. cp (H7 _ H10). rwi least_upper_bound_pr H11. nin H11. red in H11. nin H11.
app H13. uf Xi. uf image_by_fun. assert (is_function (pr_i f i)).
app function_pri. aw. exists y. split. am. red.
assert (inc y (productb f)). app H5. wr (W_pri H H10 H15). app defined_leq.
wrr Ha. wr Ha. ir. cp (H7 _ H11). rwi least_upper_bound_pr H12. nin H12.
assert (y = V i x). awi H15. red in H15. wr (W_pri (f:=f)). app W_pr.
assert (y = V i x). rw H15. rwi (W_pri (f:=f)). rwi H19. app H18. am.
app function_pri. simpl. wr H4.
assert (is_function (pr_i f i)). app function_pri. app H3. app H6.
appr order_product_order. am.
Qed.

Lemma exercise1_11d: forall f g, axioms_product_order f g ->
complete_lattice (product_order f g) ->
complete_lattice (V i g)).

Proof. ir. cp (exercise1_11a H0). nin H2. clear H3. nin H2. nin H2. clear H3.
awi H2; try am. assert (Ha:=H).nin H. ee. app exercise1_11b. app H5. ir.
wi productb_pr H2. ee.
set (Y:= L(domain f) (fun j => Yo(j=i) X (singleton (V j x)))).
assert (sub (productb Y) (substrate (product_order f g))). aw.
bw. nin (equal_or_not i0 i). rw Y_if_rw. wr H6. rwi H6. am.
rw Y_if_not_rw. red. ir. rw (singleton Eq H12). app H9. rwi H8. am.
nin H0. cp (H11 _ H10). nin H12. nin H12.
assert (Xo (pr_i f i) = V i x0). rwi W_pri.
ei. exists (Xo (pr_i f i)). rw least_upper_bound_pr. split. red. ee.
ir. assert (inc (L(domain f) (fun j => Yo (j = i) y (V j x)))(productb Y)).
app productb_pr. bw. ee. gprops. uf Y. bw. ir. bw.
nin (equal_or_not i0 i). rw H19. rw Y_if_rw. uf Y. bw. rw Y_if_rw. am. tv.
tv. uf Y. bw. rw Y_if_not_rw. rw Y_if_not_rw. fprops. am. am. uf Y. gprops.
cp (H15 _ H18). rwi related_product_order H19. ee. cp (H21 _ H1).
bwi H22. rwi Y_if_rw H22. tv. rw H16. am. tv. am. am.
ir. set (w:= (L(domain f)(fun j=> (Yo (j = i) z (V j x)))).
assert (inc w (productb f)). uf w. rw productb_pr. bw. ee. gprops. tv. ir.
bw. nin (equal_or_not i0 i). rw H19. rw Y_if_rw. red in H17. nin H17. wr H8. tv.
wr H16. am. tv. am. tv. am. am. ir. set (w:= (L(domain f)(fun j=> (Yo (j = i) z (V j x))))).
assert (inc w (productb f)). uf w. rw productb_pr. bw. ee. gprops. tv. ir.
assert (upper_bound (product_order f g) (productb Y) w). red. split.
aw. ir. rw related_product_order. ee. awi H10. app H10. am. am. ir.
cp (H22 _ H20). bwi H23. nin (equal_or_not i0 i). rw Y_if_rw.
rw Y_if_not_rw. rwi Y_if_not_rw H23. rw (singleton_eq H23).
wr order_reflexivity. rww H6. app H9. rw H8. app H5. am. am. am.
uf Y; gprops. am. cp (H14 _ H19). rwi related_product_order H20. ee.
rw H16. cp (H22 _ H1). ufi w H23. bwi H23. rwi Y_if_rw H23. am. tv. am.
app H5. am. am. am. am.
Qed.

(c) An ordinal sum (Exercise 3) \( \sum_{i \in I} E_i \) is a complete lattice if and only if the following conditions are satisfied:

(I) \( I \) is a complete lattice

(II) If \( J \) is a subset of \( I \) which has no greatest element, and if \( \sigma = \sup J \), then \( E_\sigma \) has a least element.

(III) For each \( i \in I \) every subset of \( E_i \) which has an upper bound in \( E_i \) has a least upper bound in \( E_i \).

(IV) For each \( i \in I \) such that \( E_i \) has no greatest element, the set of all \( \kappa > i \) has a least element \( \alpha \) and \( E_\alpha \) has a least element.

Condition III has to be replaced by: “every non-empty subset of \( E_i \) which has an upper bound has a supremum” Example. Consider the sum of two sets, a singleton and the reverse order of \( N \). The empty set is bounded in \( N \) but has no greatest lower bound. This is now the theorem we try to show.

Definition greatest_induced r X x := greatest_element (induced_order r X) x.
Definition least_induced r X x := least_element (induced_order r X) x.

Lemma exercise1_11e: forall r f g, ordinal_sum_axioms1 r f g->
complete_lattice (ordinal_sum r f g) =
(complete_lattice r
& (forall j, sub j (substrate r) ->
  (exists u, greatest_induced r j u) ->
  exists v, least_element (V (supremum r j) g) v)
& (forall i x, inc i (substrate r) -> sub x (substrate (V i g)) ->
  (exists u, upper_bound (V i g) x u) ->
  (exists u, least_upper_bound (V i g) x u))
& (forall i, inc i (substrate r) ->
  (exists u, greatest_element (V i g) u ) ->
  exists v, least_induced r (Zo (substrate r) (fun j =>
    glt r i j)) v
& exists w, least_element (V v g) w).

We recall that the ordinal sum is the set of all \((i, x_i)\) where \(i \in I\) and \(x_i \in E_i\), and \((i, x_i) < (j, x_j)\) if either \(i < j\) (in \( I \)) or \(i = j\) and \(x_i < x_j\) (in the ordered set \( E_i \)). We assume \( E_i \) non-empty. In particular, this allows us to define a function \( k \) such that \( k(i) \in E_i \), hence consider \( I \) is a subset of the sum.
Proof. ir. set (E:= substrate r). set (F:= disjoint_union f).
nin H. rename H0 into Hb.
asert (Hc:order (ordinal_sum r f g)). app order_ordinal_sum.
asert (Ha: substrate (ordinal_sum r f g) = F). rww substrate_ordinal_sum.
app iff.eq. ir. cp H.
asert (Hd:forall i, inc i (domain f) -> exists y, inc y (V i f) &
inc (J y i) (substrate (ordinal_sum r f g))). ir. nin (Hb _ H2).
exists y. split. am. cp (inc_disjoint_union H2 H3). aw.
set (k:= fun i => choose(fun y => inc y (V i f) &
inc (J y i) (substrate (ordinal_sum r f g)))).
asert (forall i, inc i (domain f) -> (inc (k i) (V i f)&inc (J (k i) i)F)).
ir. wr Ha. uf k. app choose_pr. app Hd. nin H1. nin H0.

Let J be a subset of I, and consider the least upper bound $x_J$ of $k(J)$. Then $j$ is the supremum of J.

assert (forall j, sub j E -> exists x,
least_upper_bound (ordinal_sum r f g) (fun_image j (fun i => J (k i) i)) x
& inc x F & least_upper_bound r j (Q x)).
ir. ee. set (Y:= fun_image j (fun i=> J (k i) i)).
asert (sub Y F). uf Y. red. ir. avi H11. nin H11. nin H11.
asert (inc x0 (domain f)). wr H3. app H5. nin (H2 _ H13). wr H12.
wr Ha H4. nin (H4 _ H11). nin H12. exists x. split. am. avi H12. nin H12.
asert (inc x F). red in H12. ee. wr Ha. split. am.
asert (inc (J (k y) y) Y). uf Y. aw. exists y. auto.
cp (H20 _ H21). cp (related_ordinal_sum_order_id H H22). avi H23. am.
ir. red in H19. ee. assert (inc (J (k z) z) F). rwi H3 H19. nin (H2 _ H19).
am. assert (upper_bound (ordinal_sum r f g) Y (J (k z) z)).
red. rw Ha. split. ir. am. ir. aw. split. app H11. split. am.
nin (equal_or_not x0 z). rw H25. right. split. tv. wr order_reflexivity.
cp (H14 _ H22). cp (related_ordinal_sum_order_id H H23). avi H24. am.
am. rww Ha.

Consider a subset J of I and the least upper bound $x_J$ of $k(J)$. Then $j$ is the least upper bound of J. This shows (I), namely that I is a complete lattice. The quantity $j$ is the supremum of J. Assume that J has no greatest element, so that $j \not\in J$. Every element in E_J is an upper bound of k(J). Thus $x_J$ must be the least element of E_J. This shows (II).
Consider now a non-empty bounded subset $X_i$ of $E_i$. We can consider this as a subset $X$ of the sum. It has a least upper bound $x_k$. Since $X_i$ is non-empty, there is $x_i \in X \cap E_i$ hence $i \leq k$. Since $X_i$ has an upper bound, $X$ has an upper bound in $E_i$ hence $k \leq i$. Thus $k = i$. It follows that $x_k$ can be considered as an element of $X_i$ and is hence the supremum. This is point (III).

Consider finally point (IV). Let $i \in E$. Consider $J$, the subset of $I$ formed of indiced $j > i$; consider $E_i$ as a subset $X$ of the sum. Let $x_k$ be its supremum. Since $E_i$ is nonempty, there is $y_i \leq x_k$, hence $i \leq k$. If $i = k$, then $y_k$ is the greatest element of $E_i$. Let's assume that $E_i$ has no greatest element. This implies $k \in J$. For every $j \in J$, any element of $E_j$ is an upper bound of $X$, this $k \leq j$. This means that $k$ is the least element of $J$. Take $j = k$. Then $x_k$ is the least element of $E_k$. This proves (IV).

ee. ir. set (X:= product (substrate (V i g)) (singleton i)).
assert (J (P x) (Q x)= x). app pair_recov.
assert (inc (J z i) F). uf F. app inc_disjoint_union.
red in H16. ee. app H22.
assert (Q x i = i). cp (H20 _ H21). cp (related_ordinal_sum_order_id H H22).
awi H23. nin H14. assert (inc (J y i) X). uf X. aw. ee. fprops. am. fprops.
red in H18. ee. cp (H25 _ H24). cp (related_ordinal_sum_order_id H H26).
awi H27. app (order_antisymmetry H1 H23 H27). exists (P x1).
wr H22. ir. assert (inc (J y i) X). uf X. aw. ee. fprops. am. fprops.
cp (H23 _ H28). awi H29. ee. nin H31. red in H31. ee. elim H32. sy. am.
nin H31. am. am. ir. red in H27. ee. rwi H10 H27.
assert (inc (J z i) F). uf F. app inc_disjoint_union.
assert (upper_bound (ordinal_sum r f g) X (J z i)).
red. ee. rwi Ha. ir. aw. ee. app H17. am. ufi X H30. awi H30. ee.
rw H32. right. split. tv. app H28. cp (H20 _ H30). awi H31.
e. rwi H22 H33. nin H33. nin H33. elim H34. tv. nin H33. am. am. am.
app H9. rwi H10. am. rw Ha. am. am.

INRIA
assert (inc (J x0 i) X). uf X. aw. ee. fprops. am. fprops.

\begin{verbatim}
assert (upper_bound (ordinal_sum r f g) X (J (k x0) x0)). red. rw Ha. split. am. ir. aw. ee. app H13. am. left. ufi X H26. awi H26. ee. rww H28. cp (H16 _ H26).
\end{verbatim}

\begin{verbatim}
assert (inc (J x0 (Q x)) F). uf F. app inc_disjoint_union. ufi Ii H20. Ztac. wr H3. am.
\end{verbatim}

Assume the four assumptions true. Take a subset X. We have to show that it has a least upper bound. Let J be the set of indices i of all (xi) ∈ X. It has a least upper bound i, by assumption (I).

\begin{verbatim}
ir. ee. app exercise1_11b. ir.
rwi Ha H4. cp H. red in H. ee.
set (j:= Zo E (fun i=> exists x, inc x X & i = Q x)).
assert (sub j E). uf j. app Z_sub.
nin H0. nin (H13 _ H12). clear H15. cp (supremum_pr1 H H12 H14).
\end{verbatim}

Assume that J has a greatest element j. Each upper bound xk of X satisfies k ≥ j. Let Xj be the set of all elements xk of X such that k = j.

\begin{verbatim}
nin (p_or_not_p (exists u, greatest_induced r j u)).
nin H16. rename x into k. red in H16. red in H16. awi H16; try am. ee.
assert (Hd:forall z, upper_bound (ordinal_sum r f g) X z -> gle r k (Q z)).
cp (H19 _ H21). rw H22. app (related_ordinal_sum_order_id H H23).
assert (He: inc k (domain f)). wr H6. app H12.
set (Xj:= Zo (substrate (V k g))
(fun y=> exists x, inc x X & y = P x & k = Q x)).
\end{verbatim}

The set Xj is non-empty. Assume that it has an upper bound. We apply assumption (III). It says that Xj has a least upper bound x. Consider this as xj in the sum. If yk ∈ X, then k ∈ J hence k ≤ j. If k < j then yk < xj, and if k = j we have yk ≤ xj in Xj. Conversely, consider an upper bound of yk of X. If k > j then xj < yk. Otherwise, yk ∈ Xj and is an upper bound of Xj hence xj ≤ yk.

\begin{verbatim}
exists (P x). uf Xj. Ztac. ee. cp (du_index_pr (H4 _ H16)). ee.
rwi H11. rwi H19. rwi H19. exists x. ee. am. tv. am.
nin (p_or_not_p (exists u, upper_bound (V k g) X j u)).
ir. assert (sub Xj (substrate (V k g))). uf Xj. app Z_sub.
nin (H2 _ _ (H12 _ H16) H19 H18). rwi least_upper_bound_pr H20. ee.
assert (inc (J x k) F). uf F. app inc_disjoint_union. nin H20. wr H11.
exists (J x k). rr least_upper_bound_pr.
split. red. aw. split. am. ir. aw. ee. app H4. am.
\end{verbatim}
Assume that $X_j$ has no upper bound in $E_j$. Then $E_j$ has no greatest element, and we can use (IV). It asserts existence of an index $k$, the least index such that $k > i$ and a least element $x$ in $E_k$. This is obviously an upper bound of $X$. If we consider another upper bound $z_t$, we must have $t > j$, thus $t \geq k$. If $t = k$, we use $x \leq z_t$.

Assume finally that $J$ has no greatest element. By assumption (II), the set $E_i$ has a least element $x$. Consider the pair $(x, x)$. It is a strict upper bound of $X$ since it is a strict upper bound of $J$. Consider another upper bound, say $(z, z)$. We have $x \leq z$ in $E_k$ hence $x' \leq z'$. If $i = j$, we have $x \leq z$ in $E_i$ hence $x' \leq z'$.

\[ \text{nin} (H1 _ H12 H16). \]

Assume finally that $J$ has no greatest element. By assumption (II), the set $E_i$ has a least element $x$. Consider the pair $(i, x)$. It is a strict upper bound of $X$ since $i$ is a strict upper bound of $J$. Consider another upper bound, say $(j, z)$. We have $i \leq j$. If $i < j$ it follows $x' < z'$. If $i = j$, we have $x \leq z$ in $E_i$ hence $x' \leq z'$.
app H23. am. am. aw. ir. nin H20. ee. rwi Ha H20. cp (du_index_pr H20).
 rwi least_upper_bound_pr H15. ee. assert (upper_bound r j (Q z)). red.
ap (related_ordinal_sum_order_id H5 H30). cp (H25 _ H26). aw. ee. am. am.
nin (equal_or_not (Q b) (Q z)). right. split. am. uf b. aw. nin H17.
ap H29. rw H11. wri H28 H23. ufi b H23. awi H23. am. left. split.
uf b. av. am. am. am. am. rww Ha.
Qed.

(d) The ordered set $\mathcal{A}(E,F)$ of increasing maps of an ordered set $E$ into an ordered set $F$
(Exercise 6) is a complete lattice if and only if $F$ is a complete lattice.

Assume that $\mathcal{A}(E,F)$ is a complete lattice. If $E$ is non-empty, then $F$ is a complete lattice,
see Exercise 6 (c).

Lemma exercise1_11f: forall r r', order r -> order r' ->
nonempty (substrate r) ->
complete_lattice (increasing_mappings_order r r') -> complete_lattice r'.
Proof. ir. app exercise1_11b. ir. red.
set (E:= substrate r). set (E':=substrate r').
set (Y:= Zo (substrate (increasing_mappings_order r r'))
(fun f => exists y, exists Hy: inc y X,
f = corr_value(constant_function E E' y (H3 y Hy)))
assert (sub Y (substrate (increasing_mappings_order r r')))). uf Y. app Z_sub.
nin H6. rwi imo_substrate H6. cp H1. nin H1.
set (u:= W y x0). assert (inc u E'). uf u. uf E'. wr H12. app inc_W_target.
rww H11. exists u. aw. split. red. ee. am. ir.
set (f:=corr_value (constant_function E E' y0 (H3 y0 H16))).
assert (inc f Y). uf Y. Ztac. rw imo_substrate.
f u. uf E; uf E'. app constant_increasing. am. am. exists y0. exists H16.
tv. cp (H9 _ H17). rwi imo_pr H18. ee. red in H20. ee.
set (f:=corr_value (constant_function (substrate r) (substrate r') z H16)).
assert (inc f (set_of_increasing_mappings r r')). uf f.
app constant_increasing.
assert (upper_bound (increasing_mappings_order r r') Y f)). red. ee.
uf f. uf E. uf E'. wrr constant_increasing1. app H17. cp (H8 _ H19).
rwi imo_pr H20. ee. red in H22. ee. cp (H28 _ H1). ufi f H29. awi H29.
rwi W_constant H29. wri H14 H27. awi H27. am. am. am. am. am.
app imo_order. uf Y. app Z_sub.
Qed.

Let’s show the converse. We consider a subset $X$ of $\mathcal{A}(E,F)$, and for each $x \in E$ the set $G_X$
of all $f(x)$ for $f \in X$. If $F$ is a complete lattice, this set has a least upper bound, say $f_x$. This
gives us a function $f : x \mapsto f_x$.

Lemma exercise1_11g: forall r r', order r -> order r' ->
complete_lattice r' -> complete_lattice (increasing_mappings_order r r').
Proof. ir. app exercise1_11b. ir. app imo_order. rww imo_substrate. ir.
set (E:=substrate r). set (E':=substrate r').
set (img:= fun x=> fun_image X (fun f => (inv_corr_value f))).
This function $f$ is increasing. Assume $a \leq b$. We have $g(b) \leq \sup_{h \in X} h(b)$ if the supremum is over $X$ and $g \in X$. Thus $g(a) \leq g(b) \leq f(b)$. Taking the supremum over $g$ gives $f(a) \leq f(b)$.

It is easy to show that the function $f$ is the supremum.

12. Let $\Phi$ be a mapping of a set $A$ into itself. Let $\mathcal{F}$ be the subset of $\mathcal{P}(A)$ consisting of all $X \subset A$ such that $f(X) \subset X$ for each $f \in \Phi$. Show that $\mathcal{F}$ is a complete lattice with respect to the relation of inclusion.

Let $X \in \mathcal{F}$. We show that $\bigcup X \in \mathcal{F}$ and $\bigcap X \in \mathcal{F}$ (if $X$ is empty, the intersection is replaced by $E$).
target f = E ->
complete_lattice (inclusion_suborder (Zo (powerset E) (fun X =>
sub (image_by_fun f X) X))).
Proof. ir. set (F:=Zo (powerset E) (fun X : Set => sub (image_by_fun f X) X)).
avert (order (inclusion_suborder F)). ap subinclusion_is_order. red. split.
am. ir. rwi substrate_subinclusion_order H3.
avert (sub F (powerset E)). uf F. ap Z_sub. assert (sub X (powerset E)).
apply sub_trans with F. am. am.
avert (Ha:sub (union X) E). E. ir. nin (union_exists H6). nin H7. cp (H5 _ H8).
set (v:= Yo (nonempty X) (intersection X) E).
avert (Hb: sub v E). uf v. nin (p_or_not_p (nonempty X)).
rww Y_if_rw. nin H6. cp (intersection_sub H6). apply sub_trans with y. am.
app powerset_sub. app H5. rww Y_if_not_rw. fprops.
avert (inc v F). uf F. Ztac. app powerset_inc.
uf v. nin (p_or_not_p (nonempty X)). rww Y_if_rw. cp H6. nin H6.
red. ir. awi H8. nin H8. nin H8. app intersection_inc.ir.
cp (H3 _ H10). ufi F H11. Ztac. app H13. aw. exists x0. split.
avert (intersection_forall H8 H10). am. rw H0. app powerset_sub. am. rw H0.
avert (v = intersection X). uf v. rww Y_if_rw. wr H9.
rww Y_if_not_rw. red. ir. awi H7. nin H7. ee. rw H8. wri H0 H7. wr H1.
fprops. am. rw H0. fprops.
avert (inc (union X) F). uf F. Ztac. app powerset_inc. red. ir.
avi H7. nin H7. nin H7. nin (union_exists H7). nin H9. cp (H3 _ H10).
ufi F H11. Ztac. apply union_inc with x1. app H13. aw. exists x0. split.
am. am. rw H0. app powerset_sub. am. am. rw H0.
split. red. exists (union X). app (union_is_sup1 H4 H3 H7).
red. exists v. app (intersection_is_inf1 H4 H3 H6).
Qed.

13. Let E be an ordered set. A mapping f of E into itself is said to be a closure if it satisfies the following conditions: (1) f is increasing, (2) for each x ∈ E, f(x) ≥ x, (3) for each x ∈ E, f(f(x)) = f(x). Let F be the set of elements of E which are invariant under f.

(a) Show that for each x ∈ E the set Fx of elements y ∈ F such that x ≤ y is not empty and has a least element, namely f(x). Conversely, if G is a subset of E such that, for each x ∈ E, the set of all y ∈ G such that x ≤ y has a least element g(x), then g is a closure and G is the set of elements of E that are invariant under g.

(b) Suppose that E is a complete lattice. Show that the greatest lower bound in E of any non-empty subset of F belongs to F.

(c) Show that if E is a lattice, then f(sup(x, y)) = f(sup(f(x), f(y))) for each pair of elements x, y of E.

We start with some definitions.

Definition is_closure f r :=
ingcreasing_fun f r &
(forall x, inc x (substrate r) -> gle r x (W x f)) &
(forall x, inc x (substrate r) -> W (W x f) f = W x f).

Definition set_of_invariants f := Zo (source f) (fun x => W x f = x).
Definition set_of_upper_bounds F r x := Zo F (fun y => gle x y).
First part of (a) is trivial.

Lemma Exercise1_13a: forall f r x, is_closure f r ->
let F := set_of_invariants f in
least_element (induced_order r (set_of_upper_bounds F r x)) (W x f).
Proof. ir. red in H. ee. red in H. ee. assert (inc (W x f) F). uf F.
assert (sub (set_of_upper_bounds F r x) (substrate r)).
uf set_of_upper_bounds. apply sub_trans with F. app Z_sub.
uf F. uf set_of_invariants. wr H5. app Z_sub.
uf least_element. aw.
Ztac. app H1. rww H5. split. am. ir. aw. ufi set_of_upper_bounds H11.
ap (H7 _ _ H0 H14 H13).
Qed.

Second part is a bit more complicated. Consider a set G. Let G_x be the set of upper bounds of x that are in G. Let P_G(x,y) be the property that y is the least upper bound G_x. We have an assumption that for each x there is an y satisfying P(x,y). We use the axiom of choice and define a function y = g_G(x). This assumption says that g_G(x) \in G_x and is the smallest element of this set (assertions Hb and Hc). The first assumption says that, if y = g_G(x), then y belongs to E (so that there is a function g : E \rightarrow E), it belongs to G and x \leq y. If x \in G, then x \in G_x, assumption Hc says y \leq x, hence y = x. Conversely, if x = y then x \in G (since y \in G) Assume now a \leq b. Since b \leq g(b) we have g(b) \in G_a, hence g(a) \leq g(b). This shows that the function is increasing, thus is a closure.

Lemma Exercise1_13b: forall r G, order r -> sub G (substrate r) ->
let g:= fun x => choose (fun y => least_element (induced_order r
(set_of_upper_bounds G r x)) y) in
(forall x, inc x (substrate r) -> exists y,
least_element (induced_order r (set_of_upper_bounds G r x)) y) ->
(is_closure (BL g (substrate r) (substrate r)) r &
(G = set_of_invariants (BL g (substrate r) (substrate r)))).
Proof. ir. assert (forall x, inc x (substrate r) ->
least_element (induced_order r (set_of_upper_bounds G r x)) (g x)).
ir. uf g. app choose_pr. app H1. clear H1.
set (E:= substrate r) in *.
assert (Ha:forall x, inc x E -> sub (set_of_upper_bounds G r x) E).
ir. uf set_of_upper_bounds. apply sub_trans with G. app Z_sub. am.
assert (Hb:forall x, inc x E -> (inc (g x) (set_of_upper_bounds G r x)))).
ir. cp (H2 _ H1). red in H3. ee. avi H3. am. am. app Ha.
assert (Hc:forall x y, inc x E -> inc y (set_of_upper_bounds G r x) ->
gle r (g x) y).
ir. cp (H2 _ H1). red in H4. ee. avi H5. cp (H5 _ H3). avi H6. am.
avi H4. am. am. app Ha. am. am. app Ha.
assert (Hd:forall x, inc x E -> (inc (g x) E \& inc (g x) G \& gle r x (g x))).
ir. cp (Hb _ H1). uf set_of_upper_bounds H3. Ztac. app H0. am. am.
assert(He:forall x, inc x G -> (g x) = x). ir.
assert (gle r (g x) x). app Hc. app H0. uf set_of_upper_bounds. Ztac.
wr order_reflexivity. app H0. assert (inc x E). app H0. cp (Hd _ H4).
ee. app (order_antisymmetry H3 H7).
assert (transf_axioms g E E). red. ir. nin (Hd _ H1). am.
assert (forall x, inc x E -> W x (BL g E E) = g x). ir. app W_af_function.
Converse. Assume that \( x \) is a lower bound of \( E \subset F \). Then \( x \leq y \) forall \( y \in E \), hence \( f(x) \leq f(y) \). But \( f(y) = y \) so that \( f(x) \) is also a lower bound. If \( y \) is the least upper bound, we get \( f(y) \leq y \); since \( y \leq f(y) \) we get \( f(y) = y \), hence \( y \in F \).

Lemma Exercise1_13c: forall \( f \in B \), is_closure \( r \) -> complete_lattice \( r \) ->
let \( F := \text{set_of_invariants} f \) in
sub \( E \) F -> nonempty \( E \) -> inc (infimum \( r \) \( E \)) \( F \).
Proof. ir. nin H0. nin H. ee. nin H. ee.
assert (\( \text{sub} F \) \( \text{substrate} \) \( r \)). uf F. uf set_of_invariants. rw H8. app Z_sub.
assert (\( \text{sub} E \) \( \text{substrate} \) \( r \)). apply sub_trans with \( F \). am. am.
nin (H3 _ H12). cp \( \text{infimum} \) pr1 \( H0 \) H12 H14). rwi greatest_lower_bound_pr \( H15 \).
ee. set \( y:= \text{infimum} \) \( r \) \( E \) in *. assert (inc \( \) \( y \) \( \text{substrate} \) \( r \)). nin \( H15 \). am.
assert (inc \( \( W \) \( y \) \( f \) \) \( \text{substrate} \) \( r \)) \( \text{rwi} \) greatest_upper_bound_pr \( H16 \).
ee. set \( y:= \text{infimum} \) \( r \) \( E \) in *. assert (inc \( \) \( y \) \( \text{substrate} \) \( r \)). nin \( H15 \). am.
assert (inc \( \) \( W \) \( y \) \( f \) \) \( \text{substrate} \) \( r \)) \( \text{rwi} \) greatest_upper_bound_pr \( H16 \).
ee. set \( y:= \text{infimum} \) \( r \) \( E \) in *. assert (inc \( \) \( y \) \( \text{substrate} \) \( r \)). nin \( H15 \). am.
assert (inc \( \) \( W \) \( y \) \( f \) \) \( \text{substrate} \) \( r \)) \( \text{rwi} \) greatest_upper_bound_pr \( H16 \).
ee. set \( y:= \text{infimum} \) \( r \) \( E \) in *. assert (inc \( \) \( y \) \( \text{substrate} \) \( r \)). nin \( H15 \). am.
Qed.

Consider a set with the following elements eight elements \( t', x, y, z, x', y', z', T \) and \( z' \).

Look at the following table.

<table>
<thead>
<tr>
<th>( t' )</th>
<th>( x )</th>
<th>( y )</th>
<th>( z )</th>
<th>( x' )</th>
<th>( y' )</th>
<th>( T )</th>
<th>( z' )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
</tr>
<tr>
<td>( &gt; )</td>
<td>.</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
</tr>
<tr>
<td>( &gt; )</td>
<td>.</td>
<td>( &gt; )</td>
<td>.</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
<td>( &lt; )</td>
</tr>
<tr>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
</tr>
<tr>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
<td>( &gt; )</td>
</tr>
</tbody>
</table>

The diagonal contains dots, and if there is \( < \) at position \( (a, b) \) we have \( > \) at position \( (b, a) \).

Let's ignore for a moment the little bars.

Define the relation \( a < b \) if \( a = b \) or \( (a, b) \) contains \( < \). This is a reflexive and antiymmetric relation. It is transitive. Proof. Assume \( a < b \) and \( b < c \). Let's show \( a < c \). The result is true if \( a = t \) or \( c = z' \) the smallest element is \( t' \), the greatest is \( z' \). Let's ignore these elements. Then the result is true if \( c = T \) (since \( T \) is the second greatest element in the list). There are four remaining pairs, \( (x, z), (x, x'), (y, y'), (y, z) \). Notice that it is not possible to find \( a, b \) such that one pair is \( (a, b) \) and another one is \( (b, c) \).
Let $A$ and $B$ be two sets, and let $R$ be any subset of $A \times B$. For each subset $X$ of $A$ (resp. each subset $Y$ of $B$) let $\rho(X)$ (resp. $\sigma(Y)$) denote the set of all $y \in B$ (resp. $x \in A$) such that $(x, y) \in R$ for all $x \in A$ (resp. $(x, y) \in R$ for all $y \in B$). Show that $\rho$ and $\sigma$ are decreasing mappings and that the mapping $X \mapsto \sigma(\rho(X))$ and $Y \mapsto \rho(\sigma(Y))$ are closures (Exercise 13) in $\mathbb{P}(A)$ and $\mathbb{P}(B)$ respectively (ordered by inclusion).

The definition has to be corrected as: “For each subset $X$ of $A$ (resp. each subset $Y$ of $B$) let $\rho(X)$ (resp. $\sigma(Y)$) denote the set of all $y \in B$ (resp. $x \in A$) such that $(x, y) \in R$ for all $x \in X$ (resp. $(x, y) \in R$ for all $y \in Y$).”

Lemma Exercice1_14: forall $A$ $B$ $R$,
let rho := fun $X$ => Zo $B$ (fun $y$ => forall $x$, inc $x$ $X$ -> inc $(J \times y)$ $R$) in
let sigma := fun $Y$ => Zo $A$ (fun $x$ => forall $y$, inc $y$ $Y$ -> inc $(J \times x)$ $R$) in
let fr:=BL rho (powerset $A$) (powerset $B$) in
let fs:=BL sigma (powerset $B$) (powerset $A$) in
let iA := inclusion_order $A$ in
let iB := inclusion_order $B$ in
sub $R$ (product $A$ $B$) ->
(decreasing_fun fr iA iB & decreasing_fun fs iB iA &
is_closure (compose fs fr) iA & is_closure (compose fr fs) iB).

We start by showing that $\sigma$, $\rho$, $\sigma \circ \rho$ and $\rho \circ \sigma$ are functions.

Proof. ir. assert (transf_axioms rho (powerset $A$) (powerset $B$)).
red. ir. uf rho. app powerset_inc. app Z_sub.
assert (transf_axioms sigma (powerset $B$) (powerset $A$)).
red. ir. uf sigma. app powerset_inc. app Z_sub.
assert (is_function fr). uf fr. app af_function.
assert (is_function fs). uf fs. app af_function.
assert (composable fs fr). red. auto.
assert (composable fr fs). red. auto.
assert (is_function (compose fs fr)). app is_function_compose.
assert (is_function (compose fr fs)). app is_function_compose.
We show these four functions are monotone.

assert (forall u v, sub u v -> sub (rho v) (rho u)).
assert (forall u v, sub u v -> sub (sigma v) (sigma u)).
assert (forall u v, sub u v -> sub (sigma (rho u)) (sigma (rho v))).
ir. app H9. app H8.
assert (forall u v, sub u v -> sub (rho (sigma u)) (rho (sigma v))).
ir. app H8. app H9.
assert (order iA). uf iA. app inclusion_is_order.
assert (order iB). uf iB. app inclusion_is_order.
assert (substrate iA = powerset A). uf iA. rww substrate_inclusion_order.
assert (substrate iB = powerset B). uf iB. rww substrate_inclusion_order.
split. red. ee; try am. red. ir. uf fr. rww W_af_function. rww W_af_function.
red. uf iB. aw. ufi iA H18. awi H18. ee. app powerset_sub. app H0.
apppowerset_sub. app H0. app H8.
split. red. ee; try am. red. ir. uf fs. rww W_af_function. rww W_af_function.
red. uf iA. aw. ufi iB H18. awi H18. ee. app powerset_sub. app H1.
apppowerset_sub. app H1. app H9.
assert (Ha: forall x, sub x A -> sub x (sigma (rho x))).
assert (Hb: forall x, sub x B -> sub x (rho (sigma x))).
assert (increasing_fun (compose fs fr) iA iA). red. ee. am. am. am.
rww source_compose. rww target_compose. red. ir. rww W_compose.
rww W_compose. uf fr. aw. assert (inc (rho y) (powerset B)). app H0.
assert (inc (rho x) (powerset B)). app H0. uf fs. aw. uf iA. aw.
e. app powerset_sub. app H1. app powerset_sub. app H1. app H0.
ufi iA H18. awi H18. ee; am.
assert (increasing_fun (compose fr fs) iB iB). red. ee. am. am. am.
rww source_compose. rww target_compose. red. ir. rww W_compose.
rww W_compose. uf fs. aw. assert (inc (sigma y) (powerset A)). app H1.
assert (inc (sigma x) (powerset A)). app H1. uf fr. aw. uf iB. aw.
e. app powerset_sub. app H0. app powerset_sub. app H0. app H11.
ufi iB H19. awi H19. ee; am.

We have $x \subset \sigma(\rho(x))$ and $y \subset \rho(\sigma(y))$. This implies $\rho \sigma = \rho$ and $\sigma \rho = \sigma$ (cf. Proposition 2 of §1, no. 5). The conclusion follows.
15. (a) Let $E$ be an ordered set, and for each subset $X$ of $E$ let $\rho(X)$ (resp. $\sigma(X)$) denote the set of upper (resp. lower) bounds of $X$ in $E$. Show that, in $\mathcal{P}(E)$, the set $\tilde{E}$ of subsets $X$ such that $X = \sigma(\rho(X))$ is a complete lattice, and that the mapping $i : x \rightarrow \sigma(\{x\})$ is an isomorphism (called canonical) of $E$ onto an ordered subset $E'$ of $\tilde{E}$ such that, if a family $(x_i)$ of elements of $E$ has a least upper bound (resp. greatest lower bound) in $E$, the image of this least upper bound (resp. greatest lower bound) is the least upper bound (resp. greatest lower bound) in $\tilde{E}$ of the family of images of the $x_i$. $\tilde{E}$ is called the completion of the ordered set $E$.

(b) Show that, for every subset $X$ of $E$, $\sigma(\rho(X))$ is the least upper bound in $\tilde{E}$ of the subset $i(X)$ of $\tilde{E}$. If $f$ is any increasing mapping of $E$ into a complete lattice $F$, there exists a unique increasing mapping $\bar{f}$ of $\tilde{E}$ into $F$ such that $f = \bar{f} \circ i$ and $\bar{f}(\sup Z) = \sup(\bar{f}(Z))$ for every subset $Z$ of $\tilde{E}$.

(c) If $E$ is totally ordered, show that $\tilde{E}$ is totally ordered.

¶ 16. A lattice $E$ is said to be distributive if it satisfies the following two conditions

(D') \[ \sup(x, \inf(y, z)) = \inf(\sup(x, y), \sup(x, z)) \]

(D'') \[ \inf(x, \sup(y, z)) = \sup(\inf(x, y), \inf(x, z)) \]

for all $x, y, z$ in $E$. A totally ordered set is a distributive lattice.

(a) Show that each of the conditions (D'), (D'') separately implies the condition

(D) \[ \sup(\inf(x, y), \inf(y, z), \inf(z, x)) = \inf(\sup(x, y), \sup(y, z), \sup(z, x)) \]

for all $x, y, z$ in $E$.

(b) Show that the condition (D) implies the condition

(M) \[ \text{If } x \geq z, \text{ then } \sup(z, \inf(x, y)) = \inf(x, \sup(y, z)). \]

Deduce that (D) implies each of (D') and (D''), and hence that the three axioms (D), (D') and (D'') are equivalent (to show, for example, that D implies D', take the least upper bound of $x$ and each side of (D) and use (M)).

(c) Show that each of the two conditions

(T') \[ \inf(z, \sup(x, y)) \leq \sup(x, \inf(y, z)), \]

(T'') \[ \inf(\sup(x, y), \sup(z, \inf(x, y))) = \sup(\inf(x, y), \inf(y, z), \inf(z, x)), \]

for all $x, y, z$ in $E$ is necessary and sufficient for $E$ to be distributive. (To show that (T') implies (D''), consider the element \[ \inf(z, \sup(x, \inf(y, z))). \]

Let’s introduce the following definitions.
Definition distributive_lattice1 r :=
  forall x y z, inc x (substrate r) -> inc y (substrate r) ->
  inc z (substrate r) ->
  sup r (inf r y z) = inf r (sup r x y) (sup r x z).

Definition distributive_lattice2 r :=
  forall x y z, inc x (substrate r) -> inc y (substrate r) ->
  inc z (substrate r) ->
  inf r x (sup r y z) = sup r (inf r x y) (inf r x z).

Definition distributive_lattice3 r :=
  forall x y z, inc x (substrate r) -> inc y (substrate r) ->
  inc z (substrate r) ->
  sup r (inf r x y) (sup r (inf r y z) (inf r z x)) =
  inf r (sup r x y) (sup r (inf r y z) (sup r z x)).

Definition distributive_lattice4 r :=
  forall x y z, inc x (substrate r) -> inc y (substrate r) ->
  inc z (substrate r) ->
  gle r z x -> sup r z (inf r x y) = inf r x (sup r y z).

Definition distributive_lattice5 r :=
  forall x y z, inc x (substrate r) -> inc y (substrate r) ->
  inc z (substrate r) ->
  gle r (inf r z (sup r x y)) (sup r x (inf r y z)).

Definition distributive_lattice6 r :=
  forall x y z, inc x (substrate r) -> inc y (substrate r) ->
  inc z (substrate r) ->
  inf r (sup r x y) (sup r z (inf r x y))
  = sup r (inf r x y) (sup r (inf r y z) (inf r z x)).

Let's show the following trivial facts. In particular, we state associativity of sup and inf,
which are implicit in the formulation (D).

Lemma lattice_props: forall r, lattice r ->
  let E := substrate r in
  (forall x y, inc x E -> inc y E -> inc (sup r x y) E)
  & (forall x y, inc x E -> inc y E -> inc (inf r x y) E)
  & (forall x y, inc x E -> inc y E -> sup r x y = sup r y x)
  & (forall x y, inc x E -> inc y E -> inf r x y = inf r y x)
  & (forall x y z, inc x E -> inc y E -> inf r y z = sup r (inf r x y) y = y)
  & (forall x y z, inc x E -> inc y E -> sup r (inf r x y) y = y)
  & (forall x y z, inc x E -> inc y E -> inf r (sup r x y) y = y)
  & (forall x y z, inc x E -> inc y E -> sup r (inf r x y) z = sup r (sup r x y) z)
  & (forall x y z, inc x E -> inc y E -> inf r x (inf r y z) = inf r (inf r x y) z).

Proof. ir. uf E. ee.
  ir. cp (lattice_sup_pr H H0 H1). ee. app (inc_arg2_substrate H2).
  ir. cp (lattice_inf_pr H H0 H1). ee. app (inc_arg1_substrate H2).

ir. cp (lattice_sup_pr H H0 H1). ee.
  cp (lattice_sup_pr H H1 H0). ee. nin H.
  assert (gle r (sup r x y) (sup r y x)). app H4.
  assert (gle r (sup r x y) (sup r x y)). app H7.
  app (order_antisymmetry H H9 H10).
  uf E. ir. cp (lattice_inf_pr H H0 H1). ee.
  cp (lattice_inf_pr H H1 H0). ee. nin H.
  assert (gle r (inf r x y) (inf r y x)). app H7.
  assert (gle r (inf r x y) (inf r x y)). app H4.
  app (order_antisymmetry H H9 H10).
  ir. app sup_comparable1. nin H. am. cp (lattice_inf_pr H H0 H1). ee. am.
ir. cp (lattice_sup_pr H H0 H1). ee.
assert (inc (sup r x y) (substrate r)). app (inc_arg2_substrate H2).
cp (lattice_inf_pr H H5 H1). ee.
assert (gle r y (inf r (sup r x y))) app H8. wrr order_reflexivity.
nin H. am. nin H. app (order_antisymmetry H H7 H9).

Associativity of sup.

ir. cp (lattice_sup_pr H H0 H1). cp (lattice_sup_pr H H1 H2). ee.
assert (inc (sup r y z) (substrate r)). app (inc_arg2_substrate H5).
assert (inc (sup r x y) (substrate r)). app (inc_arg2_substrate H3).
cp (lattice_sup_pr H H0 H9). cp (lattice_sup_pr H H10 H2). ee. nin H.
assert (gle r (sup r x (sup r y z))(sup r (sup r x y) z)). ap H16.
apply order_transitivity with(sup r x y). am. ap H3. ap H12. ap H6.
apply order_transitivity with(sup r x y). am. ap H7. ap H12. ap H13.
assert (gle r (sup r (sup r x y) z) (sup r x (sup r y z))). ap H14.
ap H8. ap H11. apply order_transitivity with(sup r x y). am. ap H4. ap H15.
aply order_transitivity with(sup r x y). am. ap H5. ap H15.
ap (order_antisymmetry H H18 H19).

Associativity of inf.

ir. cp (lattice_inf_pr H H0 H1). cp (lattice_inf_pr H H1 H2). ee.
assert (inc (inf r y z) (substrate r)). app (inc_arg1_substrate H5).
assert (inc (inf r x y) (substrate r)). app (inc_arg1_substrate H3).
cp (lattice_inf_pr H H0 H9). cp (lattice_inf_pr H H10 H2). ee. nin H.
assert (gle r (inf r x (inf r y z))(inf r (inf r x y) z)). ap H14.
ap H8. ap H11. apply order_transitivity with(inf r x y). am. ap H15. ap H4.
aply order_transitivity with(inf r x y). am. ap H12. ap H3. ap H6.
apply order_transitivity with(inf r x y). am. ap H12. ap H7. ap H13.
ap (order_antisymmetry H H18 H19).
Qed.

Let's show that D' implies D. We just expand and simplify, ad libitum.

Lemma Exercise1_16a: forall r, lattice r ->
(distributive_lattice1 r -> distributive_lattice3 r) &
(distributive_lattice2 r -> distributive_lattice3 r).
Proof. ir. set (E:= substrate r).
cp (lattice_props H). simpl in H0. fold E in H0. ee.
rename H6 into sup_assoc. rename H7 into inf_assoc.
ir. red in H6. red. fold E. fold E in H6. ir.
set (sxy:=sup r x y). set (syz:=sup r y z). set (szx:= sup r z x).
cp (H1 _ _ H8 H9). rw (H6 _ _ _ H10 H9 H7). rw (H2 _ _ _ H10 H7).

t (sxy _ _ _ H7 H8 H9). rw (H2 _ _ _ H10 H7). fold szx. fold sxy.

rw (H4 _ _ _ H8 H9).
assert (inf r z (inf r sxy szx) = inf r z sxy). cp (H0 _ _ _ H7 H8).
cp (H0 _ _ _ H8 H9). uf sxy. uf szx. rw (H3 _ _ H11 H12).
rw (inf_assoc _ _ _ _ H9 H12 H11). rw (H3 _ _ _ H9 H12). rw (H2 _ _ _ H9 H7).
rw (H5 _ _ _ H7 H9). tv. rw H11. cp (H0 _ _ _ H7 H8). fold sxy in H12.
rw (H6 _ _ _ _ H8 H8 H9 H12). rw (H2 _ _ _ H1 _ _ H7 H8 H9).
rw (H6 _ _ _ _ H9 H7 H8). fold szx. rw (H2 _ _ _ _ H9 H8). fold sxy.
rw (H2 _ _ _ (H1 _ _ _ _ H7 H8 H8 H12). rw (H6 _ _ _ _ H1 H7 H8).
assert (inf r (sup r sxy x) (sup r sxy y) = sxy).
Let's show that \((D')\) implies \((D)\). Same as above, exchanging sup and inf.

**Lemma Exercise1_16b**: \(\forall r, \text{lattice } r \rightarrow \) 
\((\text{distributive}_3 r \rightarrow \text{distributive}_4 r) \land \) 
\((\text{distributive}_3 r \rightarrow \text{distributive}_1 r) \land \) 
\((\text{distributive}_3 r \rightarrow \text{distributive}_2 r)\).

**Proof.** \(\text{ir. set } (E:= \text{substrate } r)\). 
\(\text{cp (lattice_props H). simpl in H0. fold E in H0.}\) 
\(\text{assert (distributive}_3 r \rightarrow \text{distributive}_4 r).\) \(\text{ee.}\) 
\(\text{rename H6 into sup_assoc. rename H7 into inf_assoc. ir. red in H6. red. fold E in H6. ir.}\) 
\(\text{set (sxy:=inf r x y). set (syz:=inf r y z). set (szx:= inf r z x).}\) 
\(\text{cp (H0 _ _ H8 H9). rw (H6 _ _ _ H10 H9 H7). rw (H3 _ _ H10 H7).}\) 
\(\text{rw (H6 _ _ _ H7 H8 H9). rw (H3 _ _ H7 H9). fold szx. fold sxy.}\) 
\(\text{rw (H5 _ _ H8 H9).}\) 
\(\text{assert (sup r z (sup r sxy szx) = sup r z sxy). cp (H1 _ _ H7 H8).}\) 
\(\text{cp (H1 _ _ H9 H7). uf sxy. uf szx. rw (H2 _ _ H11 H12).}\) 
\(\text{rw (sup_assoc _ _ _ H9 H12 H11). rw (H2 _ _ _ H9 H12). rw (H3 _ _ H9 H7).}\) 
\(\text{rw (H4 _ _ _ H7 H9). tv. rw H11. cp (H1 _ _ H7 H8). fold sxy in H12.}\) 
\(\text{rw (H6 _ _ _ H0 _ _ H7 H8 H9 H12). rw (H3 _ _ _ H0 _ _ H7 H8 H9).}\) 
\(\text{rw (H6 _ _ _ H0 _ _ H7 H8). fold szx. rw (H3 _ _ _ H9 H8). fold szx.}\) 
\(\text{rw (H3 _ _ _ H0 _ _ H7 H8). rw (H6 _ _ _ H12 H7 H8).}\) 
\(\text{assert (sup r (inf r sxy x) (inf r sxy y) = sxy).}\) 
\(\text{uf sxy. cp (lattice_inf_pr H H7 H8). ee. uf i sxy H12.}\) 
\(\text{assert (inf r (inf r x y) x = (inf r x y)).}\) 
\(\text{app inf_comparable1. nin H;am. rw H16.}\) 
\(\text{assert (inf r (inf r x y) y = (inf r x y)).}\) 
\(\text{app inf_comparable1. nin H;am. rw H17. app sup_comparable1. nin H. am.}\) 
\(\text{wrr order_reflexivity. nin H; am. rw H13.}\) 
\(\text{assert (sup r syz szx= sup r szx syz). rw H2. app refl_equal.}\) 
\(\text{uf syz. app H1. uf szx. app H1. rw H14. rw H2. app refl_equal. am.}\) 
\(\text{ap H0. uf szx. app H1. uf syz. app H1.}\) 
\(\text{Qed.}\)
Let's show that that (D) implies (D'). Write (D) as \( \alpha = \beta \). Set \( a = \sup(x, \alpha) \). This the supremum of four terms, two of them being smaller than \( x \). After simplification, we see that \( a \) is the LHS of (D')

\[
\text{ir. cp (H1 H9). rename H10 into HM. ufi distributive_lattice3 H9. ufi distributive_lattice4 HM. uf distributive_lattice1; fold E.}
\]

\[
\text{set (a:= sup r x (sup r (inf r x y) (sup r (inf r y z) (inf r z x)))).}
\]

\[
\text{set (b:= sup r x (inf r (sup r x y) (inf r (sup r y z) (sup r z x)))).}
\]

\[
\text{assert (a = b). uf a; uf b. rw H9.}
\]

\[
\text{set (c:= sup r (inf r y z) (inf r z x))).}
\]

\[
\text{assert (a = sup r x (sup r (inf r x y) c))}. \text{ uf a. fold c. app refl_equal.}
\]

\[
\text{rwi H7 H14. assert (sup r x (inf r x y) = x). rw H3. app sup_comparable1.}
\]

\[
\text{nin H; am. cp (lattice_inf_pr H H10 H11). ee. am. app H2. rwi H15 H14.}
\]

\[
\text{ufi c H14. clear H15. clear c.}
\]

\[
\text{assert (sup r (inf r y z) (inf r z x)) = sup r (inf r x y) (inf r y z)).}
\]

\[
\text{app H3. app H2. rwi H15 H14. rwi H7 H14.}
\]

\[
\text{assert (sup r x (inf r z x) = x). rw H3. app sup_comparable1. nin H; am.}
\]

\[
\text{cp (lattice_inf_pr H H12 H10). ee. am. app H2. rwi H16 H14. wr H14.}
\]

\[
\text{clear H15. clear H16. clear H14. wr H13. clear H13. clear a.}
\]

We must show that \( \sup(x, \beta) = \inf(\sup(x, y), \sup(x, z)) \), where \( \beta \) is a infimum. We can apply (M). We get \( \sup(x, \beta) = \inf(\sup(x, y), d) \) where \( d = \sup(\inf(\sup(y, z), \sup(z, x)), x) \). We can apply (M) again. We get \( d = \inf(\sup(z, x), (\sup(x, y), \sup(x, z))) \). This simplifies to the first term.

\[
\text{set (c:= inf r (sup r y z) (sup r z x)) in * .}
\]

\[
\text{assert (inc (sup r x y) E). app H0. assert (gle r x (sup r x y)).}
\]

\[
\text{cp (lattice_sup_pr H H10 H11). ee. am. assert (inc c E). uf c. app H2.}
\]

\[
\text{app H0. uf b. rw (HM _ _ H13 H15 H10 H14). uf c.}
\]

\[
\text{set (d:= sup r (inf r y z) (sup r z x))) x).}
\]

\[
\text{assert (d= sup r x (inf r (sup r x y) (sup r y z)) (sup r z x))).}
\]

\[
\text{rw H3.}
\]

\[
\text{assert (d= sup r x (inf r x y) (sup r y z))).}
\]

\[
\text{rw H16. wr H4.}
\]

\[
\text{app refl_equal. app H0. app H0. assert (inc (sup r x) E). app H0.}
\]

\[
\text{assert (inc (sup r y z) E). app H0. assert (gle r x (sup r x y))).}
\]

\[
\text{cp (lattice_sup_pr H H12 H10). ee. am.}
\]

\[
\text{rwi (HM _ _ _ H18 H19 H10 H20) H17.}
\]

\[
\text{assert(d= sup r z x). rw H17. ap inf_comparable1. nin H; am. wr H7.}
\]

\[
\text{set (e:= sup r z x). assert (inc e E). uf e. app H0.}
\]

\[
\text{cp (lattice_sup_pr H H11 H21). ee. am. am. am. am. rw H21.}
\]

\[
\text{rw (H3 _ _ H12 H10). app refl_equal. am. app H2. app H2. am. app H2.}
\]

\[
\text{uf c. app H0. app H2. app H2.}
\]

The same argument show that (D) implies (D''). Step one. We simplify \( \inf(x, \beta) \) to the RHS of (D'').

\[
\text{ir. cp (H1 H9). rename H10 into HM. ufi distributive_lattice3 H9. ufi distributive_lattice4 HM. uf distributive_lattice1; fold E.}
\]

\[
\text{fold E in H9. fold E in HM. ir.}
\]

\[
\text{set (a:= inf r x (sup r (inf r x y) (sup r (inf r y z) (inf r z x)))).}
\]

\[
\text{set (b:= inf r x (inf r (sup r x y) (inf r (sup r y z) (sup r z x)))).}
\]

\[
\text{assert (a = b). uf a; uf b. rw H9.}
\]

\[
\text{set (c:= inf r (sup r y z) (sup r z x)).}
\]

\[
\text{assert (b = inf r x (inf r (sup r x y) c))}. \text{ uf b. fold c. app refl_equal.}
\]

\[
\text{rwi H8 H14. assert (inf r x (sup r x y) = x). rw H4.}
\]

\[
\text{rw H4. app inf_comparable1. nin H; am. cp (lattice_sup_pr H H10 H11). ee. am.}
\]

\[
\text{app H0. app H0. rwi H15 H14. ufi c H14. clear H15. clear c.}
\]

INRIA
assert (inf r (sup r y z) (sup r z x) = inf r (sup r z x) (sup r y z)).
app H4. app H0. app H0. rwi H15 H14. rwi H8 H14.
assert (inf r x (sup r z x))=x). ap inf_comparable1. nin H; am.

Step two. We use (M) (in reverse order).

set (c:= sup r (inf r y z) (inf r z x)) in *.
assert (inc (inf r x y) E). app H2. assert (gle r (inf r x y) x).
cp (lattice_inf_pr H H10 H11). ee. am. assert (inc c E). uf c. app H0.
assert (inc r y z E). app H2. assert (gle r (inf r z x) x).
cp (lattice_inf_pr H H10 H12). ee. am. assert (inc (inf r x z) E). app H2.
wr (HM _ _ H10 H16 H18 H17).
assert (sup r (inf r x z) (inf r x y)) = inf r x z).
rw (H4 _ _ H10 H12). rw (H4 _ _ H11 H12). rw H8. rw (H4 _ _ H10 H12).
rw H3. ap sup_comparable1. nin H; am. cp (lattice_inf_pr H H18 H11). ee. am.
app H2. rw H19. app refl_equal. am. am. am. app H0. app H0. am. app H0.
uf c. app H2. app H0. app H0.
Qed.

Let’s show that (D′) implies (T′) and conversely.

Lemma Exercise1_16c: forall r, lattice r ->
(distributive_lattice3 r = distributive_lattice5 r).
Proof. ir. app iff_eq. ir. red. ir. cp (Exercise1_16b H). ee. cp (H6 H0).
red in H7. rw H7. cp (lattice_props H). simpl in H8.
set (E:= substrate r) in *. ee. rw (H11 _ _ H3 H2).
set (b:=inf r y z) in *. assert (inc b E). uf b; app H9.
ap H20. assert (order r). nin H; am. assert (gle r (inf r z x) x).
cp (lattice_inf_pr H H3 H1). ee. am. assert (gle r x (sup r x b)).
cp (lattice_sup_pr H H1 H16). ee. am. ap (order_transitivity H21 H22 H23).
cp (lattice_sup_pr H H1 H16). ee. am.

We show that (T′) implies (D′). We first notice that the sup is smaller than the inf.

ir. cut (distributive_lattice1 r). ir. cp (Exercise1_16a H). ee. ap H2. am.
red. red in H0. cp (lattice_props H). simpl in H1. ee.
set (E:= substrate r) in *. ir. set (b:= sup r x (inf r y z)).
assert (inc b E). uf b. app H1. ap H2.
assert (gle r b (inf r (sup r x y) (sup r x z))).
assert (inc (sup r x y) E). app H1. assert (inc (sup r x z) E). app H1.
cp (lattice_inf_pr H H13 H14). ee. ap H17. uf b.
assert (inc r y z E). app H2. cp (lattice_sup_pr H H9 H18). ee.
ap H21. cp (lattice_sup_pr H H9 H10). ee; am.
assert (gle r (inf r y z) y). cp (lattice_inf_pr H H10 H11). ee; am.
assert (gle r y (sup r x y)). cp (lattice_sup_pr H H9 H10). ee; am.
in H. app (order_transitivity H22 H23). uf b.
assert (inc r y z E). app H2. cp (lattice_sup_pr H H9 H18). ee.
ap H21. cp (lattice_sup_pr H H9 H11). ee; am.
assert (gle r (inf r y z) z). cp (lattice_inf_pr H H10 H11). ee; am.
assert (gle r z (sup r x z)). cp (lattice_sup_pr H H9 H11). ee; am.
in H. app (order_transitivity H22 H23).
Write \((D')\) as \(a = b\). We apply \((T')\) to \(b\) and get \(b \leq \sup(x, \inf(z, \sup(x, y)))\). According to \((T')\), the second term is \(\leq \sup(x, \inf(y, z))\). This is \(a\). Since \(\sup\) is increasing, we get \(b \leq \sup(x, a)\); but \(a \geq x\), thus \(b \leq a\).

\[
\text{cp } (H_0 \_ \_ H_9 H_{10} H_{11}). \\
\text{cp } (H_0 \_ \_ H_9 H_{11} (H_1 \_ \_ H_9 H_{10})). \\
\text{set } (a := \inf r (\sup r x y) (\sup r x z)) \text{ in } *. \\
\text{set } (c := \inf r z (\sup r x y)) \text{ in } *.
\]

\[
\text{assert } (\sup r x b = b). \text{ ap sup_comparable1. nin } H; \text{ am. uf } b. \\
\text{cp } (\text{lattice_sup_pr } H H_9 (H_2 \_ \_ H_{10} H_{11})). \text{ ee; am.} \\
\text{assert } (\text{gle } r (\sup r x c) b). \text{ wr } H_{16}. \text{ assert } (\text{inc } c E). \text{ uf } c. \text{ app } H_2. \text{ app } H_1. \\
\text{cp } (\text{lattice_sup_pr } H H_9 H_{12}). \text{ cp } (\text{lattice_sup_pr } H H_9 H_{17}). \text{ ee.} \\
\text{ap } H_{21}. \text{ ap } H_{18}. \text{ nin } H. \text{ ap } (\text{order_transitivity } H H_{14} H_{22}). \\
\text{nin } H. \text{ cp } (\text{order_transitivity } H H_{15} H_{17}). \\
\text{ap } (\text{order_antisymmetry } H H_{13} H_{19}). \\
\text{Qed.}
\]

Let's show that \((D'')\) is equivalent to \((T'')\). One implication is easy.

**Lemma Exercise1_16d:** forall \(r\), lattice \(-\rightarrow\)
\(\text{(distributive_lattice3 } r = \text{ distributive_lattice6 } r)\).
**Proof.** ir. \(\text{cp } (\text{lattice_props } H). \text{ ap iff_eq. ir.} \\
\text{assert } (\text{distributive_lattice2 } r). \text{ cp } (\text{Exercise1_16b } H). \text{ ee. app } H_4. \\
\text{red in } H_2. \text{ red. simpl in } H_0. \text{ ir. ee. set } (E := \text{ substrate } r) \text{ in } *. \\
\text{cp } (H_0 \_ \_ H_3 H_4). \text{ cp } (H_6 \_ \_ H_3 H_4). \text{ rw } (H_2 \_ \_ H_5 H_6 H_{14}). \\
\text{rw } (H_8 \_ \_ H_{13} H_5). \text{ rw } (H_2 \_ \_ H_3 H_4). \text{ rw } (H_8 \_ \_ H_4 H_5). \\
\text{assert } (\text{inf } r (\sup r x y) (\inf r x y) = \text{ inf } r x y). \text{ rww } H_8. \\
\text{ap inf_comparable1. nin } H; \text{ am.} \\
\text{cp } (\text{lattice_sup_pr } H H_3 H_4). \text{ cp } (\text{lattice_inf_pr } H H_3 H_4). \text{ ee.} \\
\text{nin } H. \text{ ap } (\text{order_transitivity } H H_{16} H_{15}). \text{ rw } H_{15}. \\
\text{set } (\text{xy} := \text{inf } r x y). \text{ set } (\text{zx} := \text{inf } r z x). \text{ set } (\text{zy} := \text{inf } r z y). \\
\text{rw } H_7. \text{ ap uneq. rw } H_7. \text{ ap uneq. tv. uf } zx. \text{ app } H_6. \text{ uf } zy. \text{ app } H_6. \\
\text{app } H_0. \text{ uf } zx. \text{ app } H_6. \text{ uf } zy. \text{ app } H_6. \text{ app } H_4.
\]

Conversely \((T'')\) (if the form \(a = b\) implies \((T')\) (of the form \(a' \leq b'\)), since \(a' \leq a\) and \(b' \leq b\) are clear. is easy too. The LHS of \((T')\)

\[
\text{ir. rww Exercise1_16c. red in } H_1. \text{ red. ir.} \\
\text{simp in } H_0. \text{ ir. ee. set } (E := \text{ substrate } r) \text{ in } *. \\
\text{set } (a := \text{inf } r z (\text{sup } r x y)). \text{ assert } (a = \text{inf } r (\text{sup } r x y) z). \text{ rw } H_7. \text{ tv.} \\
\text{app } H_0. \text{ am. assert } (\text{gle } r a (\text{inf } r (\text{sup } r x y) (\text{sup } r z (\text{inf } r x y)))). \\
\text{rw } H_{12}. \text{ set } (\text{xy} := \text{sup } r x y). \text{ assert } (\text{inc } xy E). \text{ uf } xy. \text{ app } H_0. \\
\text{set } (b := \text{inf } r x y). \text{ assert } (\text{inc } b E). \text{ uf } b. \text{ app } H_5. \\
\text{assert } (\text{gle } r z (\text{sup } r x b)). \text{ cp } (\text{lattice_sup_pr } H H_4 H_14). \text{ ee. am.} \\
\text{cp } (\text{lattice_inf_pr } H H_{13} (H_0 \_ \_ H_4 H_{14})). \text{ ee.} \\
\text{cp } (\text{lattice_inf_pr } H H_{13} H_4). \text{ ee.} \text{ ap } H_{18}. \text{ am. nin } H. \\
\text{ap } (\text{order_transitivity } H H_{20} H_{15}). \text{ rwi } H_1 H_{13}. \\
\text{set } (c := \text{sup } r (\text{inf } r x y) (\text{sup } r (\text{inf } r y z) (\text{inf } r x z)) \text{ in } *. \\
\text{assert } (\text{gle } r c (\text{sup } r x (\text{inf } r y z))). \text{ uf } c. \\
\text{set } (\text{xy} := \text{inf } r x y). \text{ assert } (\text{inc } xy E). \text{ uf } xy. \text{ app } H_5. \\
\text{set } (\text{yz} := \text{inf } r y z). \text{ assert } (\text{inc } yz E). \text{ uf } yz. \text{ app } H_5. \\
\text{set } (\text{zx} := \text{inf } r z x). \text{ assert } (\text{inc } zx E). \text{ uf } zx. \text{ app } H_5. \\
\text{assert } (\text{inc } (\text{sup } r y z x) E). \text{ app } H_0. \\
\text{cp } (\text{lattice_inf_pr } H H_2 H_3). \text{ fold } xy \text{ in } H_{18}. \text{ ee.} \\
\text{cp } (\text{lattice_inf_pr } H H_4 H_2). \text{ fold } zx \text{ in } H_{21}. \text{ ee.}
\]

INRIA
A lattice $E$ which has a least element $\alpha$ is said to be relatively complemented if, for each pair of elements $x, y$ of $E$ such that $x \leq y$, there exists an element $x'$ such that $\sup(x, x') = y$ and $\inf(x, x') = \alpha$. Such an element $x'$ is called a relative complement of $x$ with respect to $y$.

We define now a relatively complemented set, a Boolean lattice, the complement, and show that in a relatively complemented set, a complement does exists.

Definition relatively_complemented $r$ :=

lattice $r$ & (exists $u$, least_element $r$ $u$) &
(forall $x$ $y$, gle $r$ $x$ $y$ -> exists $x'$,
   (inc $x'$ $($substrate $r)$ & sup $r$ $x$ $x'$ = $y$ & inf $r$ $x$ $x'$ = the_least_element $r$)).

Definition boolean_lattice $r$ :=
relatively_complemented $r$ & (exists $u$, greatest_element $r$ $u$) &
distributive_lattice3 $r$.

Definition the_complement $r$ $x$ $y$ :=
choose (fun $x'$ => (inc $x'$ $($substrate $r)$ &
   sup $r$ $x$ $x'$ = $y$ & inf $r$ $x$ $x'$ = the_least_element $r$)).

Lemma the_complement_pr: forall $r$ $x$ $y$,
relatively_complemented $r$ -> gle $r$ $x$ $y$ ->
let $x'$ := the_complement $r$ $x$ $y$ in
   (inc $x'$ $($substrate $r)$ & sup $r$ $x$ $x'$ = $y$ & inf $r$ $x$ $x'$ = the_least_element $r$).
Proof. ir. uf $x'$. uf the_complement. app choose_pr. red in H. ee. ir. app H2.
Qed.

Let's state a theorem that says what happens when we take the supremum or infimum of two elements, one of them being the least or greatest element.

Lemma least_greatest_pr: forall $r$, order $r$ ->
((forall $a$, inc $a$ $($substrate $r)$ -> (exists $u$, least_element $r$ $u$) ->
   sup $r$ $($the_least_element $r$ $r$) $a$ = $a$) &
   (forall $a$, inc $a$ $($substrate $r)$ -> (exists $u$, greatest_element $r$ $u$) ->
     inf $r$ $a$ $($the_greatest_element $r$ $r$) = $a$) &
   (forall $a$, inc $a$ $($substrate $r)$ -> (exists $u$, least_element $r$ $u$) ->
     inf $r$ $($the_least_element $r$ $r$) $a$ = $($the_least_element $r$ $r$)) &
   (forall $a$, inc $a$ $($substrate $r)$ -> (exists $u$, greatest_element $r$ $u$) ->
     sup $r$ $a$ $($the_greatest_element $r$ $r$) = $($the_greatest_element $r$ $r$)).
Proof. ir. ee.
   ir. app sup_comparable1. cp (the_least_element_pr $H$ $H1$). nin $H2$. app $H3$.
   ir. app inf_comparable1. cp (the_greatest_element_pr $H$ $H1$). nin $H2$. app $H3$.
   ir. app inf_comparable1. cp (the_least_element_pr $H$ $H1$). nin $H2$. app $H3$.
   ir. app sup_comparable1. cp (the_greatest_element_pr $H$ $H1$). nin $H2$. app $H3$.
Qed.
*(a)* Show that the set \( E \) of vector subspaces of a vector space of dimension \( \geq 2 \), ordered by inclusion, is a relatively complemented lattice, but that if \( x, y \) are two elements of \( E \) such that \( x \leq y \), there exists in general several distinct complements of \( x \) with respect to \( y \).

Assume that \( x \) is a subspace of \( y \); consider a basis \((x_i)_{i \in I}\) of \( y \), such that for some \( J \subset I \), \((x_i)_{i \in J}\) is a basis of \( x \). Let \( x' \) be the space spanned by \((x_i)_{i \in I \setminus J}\). This is a relative complement. Fix \( i \in I \setminus J \). We may replace \( x_i \) by any element of \( y \) not in \( x \cup x' \); this changes \( x' \), but it will remain a relative complement. An example of such an element is \( x_i + x_j \) where \( j \in J \). It exists if \( x \) is neither of dimension 0 nor equal to \( y \).

(b) If \( E \) is distributive and relatively complemented, show that if \( x \leq y \) in \( E \), there exists a unique relative complement of \( x \) with respect to \( y \). \( E \) is said to be a Boolean lattice if it is distributive and relatively complemented and if, moreover, it has a greatest element \( \omega \). For each \( x \in E \), let \( x^* \) be the complement of \( x \) with respect to \( \omega \). The the mapping \( x \mapsto x^* \) is an isomorphism of \( E \) onto the ordered set obtained by endowing \( E \) with the opposite ordering, and we have \( (x^*)^* = x \). If \( A \) is any set, then the set \( \mathcal{P}(A) \) of all subsets \( A \), ordered by inclusion, is a Boolean lattice.

Let’s show that in a distributive and relatively complemented set, there exists a unique complement. Consider \( x \), complemented by \( x' \) and \( x'' \), and apply relation (D) to these three quantities. On the LHS, we have a supremum of infimums of three terms; two of them being the least element of \( E \), the result is \( \text{sup}(x', x'') \). A similar argument says that the RHS is \( \text{inf}(x', x'') \), thus equality.

**Lemma Exercice1_17a**: For all \( r \), \( x \), \( y \), relatively_complemented \( r \) ->

- distributive_lattice3 \( r \) -> gle \( r \) \( x \) \( y \) -> exists_unique \((\text{fun} x' \Rightarrow (\text{inc} x' \ (\text{substrate} r) \ & \text{sup} r \ x \ x' = y \ & \text{inf} r \ x \ x' = \text{the_least_element} r))\).

**Proof.** ir. red. ee. exists (the_complement \( r \) \( x \) \( y \)). app the_complement_pr.

ir. red in H. ee. cp (lattice_props H). simpl in H0. red in H0.

- cp (inc_arg1_substrate H1). cp (inc_arg2_substrate H1).
- set (E:= substrate r) in *. ee.
- cp (H0 _ _ _ H3 H11 H2). rwi H6 H20. rwi H14 H4. rwi H4 H20. rwi H7 H20.
- rwi H15 H5. rwi H5 H20. assert (order r). nin H; am.
- cp (least_greatest_pr H21). ee.
- assert (sup r (the_least_element r) (inf r x0 y0) = (inf r x0 y0)).
- set (axy:=sup r x0 y0). assert (inc axy E). uf axy. app H10.
- assert (inf r y (sup r x0 y0) = (sup r x0 y0)). rw H15. app inf_comparable1.
- cp (lattice_sup_pr H2 H3). ee. app H29.
- cp (lattice_sup_pr H H11 H2). ee. wr H6. am.
- cp (lattice_sup_pr H H3 H11). ee. wr H4. am. am. ufi axy H26. am.
- cp (lattice_sup_pr H H2 H3). cp (lattice_inf_pr H H2 H3). ee.
- nin H. rwi H20 H29. rwi H20 H30.
- cp (order_transitivity H H28 H30). cp (order_transitivity H H32 H29).
- ap (order_antisymmetry H H35 H36). am. am. am. am.

Qed.

Let’s call “standard completion” and denote by \( x^* \) the completion with the greatest element of \( E \). By uniquess of completion and commutativity of supremum and infinum, we have \( (x^*)^* = x \).

**Definition standard_completion r x :=**

- the_complement r x (the_greatest_element r).
Lemma standard_completion_pr: forall r x, 
let y := standard_completion r x in 
  boolean_lattice r -> inc x (substrate r) -> 
  (inc y (substrate r) & sup r x y = the_greatest_element r & 
  inf r y x = the_least_element r).
Proof. ir. uf y. uf standard_completion. app the_complement_pr. 
  red in H; ee; am. red in H. ee. red in H. ee. red in H. ee. 
  cp (the_greatest_element_pr H H1). red in H6. ee. app H7. 
Qed.

Lemma standard_completion_involutive: forall r x, 
  boolean_lattice r -> inc x (substrate r) -> 
  standard_completion r (standard_completion r x) = x. 
Proof. ir. cp (standard_completion_pr H H0). ee. 
  set (y:= standard_completion r x) in *. 
  cp (standard_completion_pr H H1). ee. 
  set (z:= standard_completion r y) in *. red in H; ee. 
  assert (lattice r). red in H. ee. am. 
  assert (gle r y (the_greatest_element r)). 
  cp (lattice_sup_pr H9 H0 H1). ee. wr H2. am. 
  nin (Exercice1_17a H H8 H10). app H12. ee. am. am. ee. am. 
  cp (lattice_props H9). simpl in H13. ee. rw H15. app H2. am. 
Qed.

Consider two elements \(x\) and \(y\), their standard completion \(a\) and \(b\). Let \(c = \inf(a, b)\). We have \(\inf(y, c) = \alpha\). We have \(\sup(y, c) = \sup(y, a)\) (we use \((D')\)). Assume \(x \leq y\) so that \(\sup(x, a) \leq \sup(y, a)\). Since \(\sup(x, a) = \omega\) we deduce \(\sup(y, c) = \omega\). As a consequence, \(c\) is the standard completion of \(y\), hence \(b = c = \inf(a, b)\). This shows \(b \leq a\).

Lemma standard_completion_monotone: forall r x y, 
  boolean_lattice r -> gle r x y -> 
  gle r (standard_completion r y) (standard_completion r x). 
Proof. ir. cp (inc_arg1_substrate H0). cp (inc_arg2_substrate H0). 
  cp (standard_completion_pr H H1). cp (standard_completion_pr H H2). ee. 
  set (a:= standard_completion r x) in *. 
  set (b:= standard_completion r y) in *. 
  set (c := inf r a b). red in H; ee. 
  assert (lattice r). red in H; ee. am. nin (lattice_props H11). ee. 
  assert (inf r y c = the_least_element r). uf c. rw (H15 _ _ H3 H4). 
  rw H19. rw H6. ap inf_comparable1. nin H11; am. nin H. ee. nin H. 
  cp (the_least_element_pr H H20). red in H23. ee. app H24. am. am. am. 
  assert (sup r y c = sup r y a). uf c. assert (distributive_lattice1 r). 
  assert (gle r (sup r x a) (sup r y a)). 
  cp (lattice_sup_pr H11 H1 H3). cp (lattice_sup_pr H11 H2 H3). ee. 
  ap H27. nin H11. app (order_transitivity H11 H0 H23). am. rwi H7 H22. 
  assert (sup r y c = the_greatest_element r). rw H21. nin H11. 
  nin (the_greatest_element_pr H11 H9). 
  assert (inc (sup r y a) (substrate r)). app H12. cp (H25 _ H26). 
  ap (order_antisymmetry H11 H27 H22). 
  cp (lattice_sup_pr H11 H2 H4). ee. rwi H5 H24. 
We show that \( x \rightarrow x^* \) is an isomorphism. This is obvious since it is increasing (for the order on \( E \) and its reverse) and involutive.

Lemma Exercise1_17b: \( \forall r, boolean_lattice r \rightarrow\)
\( \text{order_isomorphism} (BL (\text{standard_completion} r) (\text{substrate} r)(\text{substrate} r)) \)
\( r (\text{opposite_order} r) \).
Proof. ir.
assert (\( \text{transf_axioms} (\text{standard_completion} r) (\text{substrate} r) (\text{substrate} r) \)).
red. ir. nin (\( \text{standard_completion_pr} H H0 \)). am.
assert (\( \text{is_function} (BL (\text{standard_completion} r) (\text{substrate} r) (\text{substrate} r)) \)).
app af_function. assert (order r). red in H. ee. red in H; ee. nin H. am.
red. ee. am. fprops. red. split. app injective_af_function. ir.
wr (\( \text{standard_completion_involutive} H H3 \)).
wr (\( \text{standard_completion_involutive} H H4 \)). rw H5.
app surjective_af_function. ir. cp (\( \text{standard_completion_involutive} H H3 \)).
exists (\( \text{standard_completion} r y \)). split. app H0. sy; am. tv. aw.
simpl. ir. rw W_af_function. rw W_af_function. aw.
app iff_eq. ir. app standard_completion_monotone. ir.
wr (\( \text{standard_completion_involutive} H H3 \)).
wr (\( \text{standard_completion_involutive} H H4 \)). app standard_completion_monotone.
Qed.

Let’s show that \( \mathcal{P}(A) \) is a Boolean lattice. We also pretend that \( x^* \) is the complement of \( x \) in \( A \). First step. We show that we have a least and a greatest element.

Lemma Exercise1_17c: \( \forall a, \)
\( (boolean_lattice (\text{inclusion_order} a) \& \)
\( (\forall x, \text{inc} x (\text{powerset} a) \rightarrow\)
\( \text{standard_completion} (\text{inclusion_order} a) x = \text{complement} a x) \)).
Proof. ir. set (\( r:=\text{inclusion_order} a \)). uf standard_completion.
assert (\( \text{substrate} r = \text{powerset} a \)). uf r. rww substrate_inclusion_order.
assert (order r). uf r. fprops.
assert (\( \text{least_element} r \text{ emptyset} \)). red. split. rw H. app powerset_inc.
app sub_emptyset_any. ir. uf r. aw. rwi H H1. ee. app sub_emptyset_any.
app powerset_sub. sub emptyset any.
assert (\( \exists u, \text{least_element} r u \)). exists emptyset. am.
assert (\( \text{the_least_element} r = \text{emptyset} \)). cp (\( \text{the_least_element_pr} H0 H2 \)).
app (unique_least H0 H3 H1).
assert (\( \text{greatest_element} r a \)). red. split. rw H. app powerset_inc.
fprops. ir. uf r. aw. rwi H H4. rwi powerset_inc rw H4. ee. am. fprops. am.
assert (\( \exists u, \text{greatest_element} r u \)). exists a. am.
assert (\( \text{the_greatest_element} r = a \)). cp (\( \text{the_greatest_element_pr} H0 H5 \)).
app (unique_greatest H0 H6 H4). rw H6.

Let’s show that the powerset is a lattice, where sup and inf are union and intersection (note that we know that the powerset is a complete lattice).

assert (\( \forall x y, \text{inc} x (\text{powerset} a) \rightarrow \text{inc} y (\text{powerset} a) \rightarrow\)
\( \text{least_upper_bound} r (\text{doubleton} x y) (\text{union2} x y) \)).
ir. assert (\( \text{sub} x a \)). app powerset_sub. assert (\( \text{sub} y a \)). app powerset_sub.
assert (\( \text{sub} (\text{union2} x y) a \)). red. ir. nin (\( \text{union2_or} H1 \)). app H9. app H10.
app least_upper_bound_doubleton. uf r. aw. ee. am. am.
We show that the set is relatively complemented.

assert (Hd: forall x y, sub x y -> sub y a -> 
          (inc (complement y x) (substrate r) & sup r x (complement y x) = y & 
           inf r x (complement y x) = the_least_element r)).
ir. assert (sub x a). apply sub_trans with y. am. am.
assert (inc (complement y x) (powerset a)). app powerset_inc. red. ir.
app union2_complement. app powerset_inc. am. rw H11.
app intersection2_complement. app powerset_inc.
assert (Hb: relatively_complemented r). red. ee. am. am. ir.
ufi r H12. awi H12. exists (complement y x). app Hd. ee; am. ee; am.

We show distributivity via (T’).

assert (Hc: distributive_lattice3 r).
rrw Exercise1_16c. red. ir. rwi H H12; rwi H H13; rwi H H14.
rw (H10 _ _ H12 H13). assert (inc (union2 x y) (powerset a)).
app powerset_inc. red. ir. nin (union2_or H15).
assert (sub x a). app powerset_sub. app H17.
assert (sub y a). app powerset_sub. app H17.
rw (H11 _ _ H14 H15).
rw (H11 _ _ H13 H14). assert (inc (intersection2 y z) (powerset a)).
app powerset_inc. red. ir. assert (sub y a). app powerset_sub. app H17.
ap (intersection2_first H16). rw (H10 _ _ H12 H16). uf r. aw. ee.
assert (sub z a). app powerset_sub. red. ir. app H17.
ap (intersection2_first H18). red. ir. nin (union2_or H17).
assert (sub x a). app powerset_sub. app H19.
assert (sub (intersection2 y z) a). app powerset_sub. app H19.
red. ir. nin (intersection2_both H17). nin (union2_or H19).
ap union2_first. app union2_second. app intersection2_inc.

The conclusion is now obvious.

split. red. ee. am. am. am. am.
ir. assert (gle r x a). uf r. av. rwi powerset_inc_rw H12. ee. am. fprops. am.
in (Exercice1_17a Hb Hc H13). ee. cp (the_complement_pr Hb H13).
assert (sub x a). app powerset_sub. assert (sub a a). fprops.
ap (Hd _ _ H18 H19).
Qed.

(c) If $E$ is a complete Boolean lattice (Exercise 11), show that for each family $(x_\lambda)$ of elements of $E$ and each $y \in E$ we have

$$\inf\left(y, \sup_{\lambda} (x_\lambda)\right) = \sup\inf\left(y, x_\lambda\right).$$

(Reduce to the case $y = \alpha$, and use the fact that if $\inf(z, x_\lambda) = \alpha$ for every index $\lambda$, then $z^* \geq x_\lambda$ for every $\lambda$).

I do not understand the sentence “Reduce to the case $y = \alpha$”, since if $y = \alpha$ the result is trivial. We start with four formulas of the type $\inf(y, \sup(y^*, x) = \inf(y, x)$.

Lemma: Exercise1_17d: forall r x y, boolean_lattice r ->
inc x (substrate r) -> inc y (substrate r) ->
let ys := (standard_completion r y) in
(inf r y (sup r ys x) = inf r y x &
sup r y (inf r ys x) = sup r y x &
in r ys (sup r y x) = inf r ys x &
sup r ys (inf r y x) = sup r ys x).
Proof. ir. cp H. nin H. nin H3. assert (order r). nin H. nin H. am.
assert (lattice r). nin H; am. cp (lattice_props H6). simpl in H7.
assert (forall x y, inc x (substrate r) -> inc y (substrate r) ->
inf r y (sup r (standard_completion r y) x) = inf r y x). ee. ir.
cp (standard_completion_pr H2 H16). ee.
set (z:=standard_completion r y0) in *. red in H. ee. cp (Exercise1_16b H).
cp (least_greatest_pr H5). ee. rww H26. app H8.
d (forall x y, inc x (substrate r) -> inc y (substrate r) ->
sup r y (inf r (standard_completion r y) x) = sup r y x). ee. ir.
cp (standard_completion_pr H2 H17). ee.
set (z:=standard_completion r y0) in *. red in H. ee. cp (Exercise1_16b H).
cp (the_greatest_element_pr H5 H3). red in H31. ee. am. app H7.
ee. uf ys. app H8. uf ys. app H9. cp (standard_completion_involutive H2 H1).
fold ys in H17. wr H17. app H8. cp (standard_completion_pr H2 H1). ee. am.
cp (standard_completion_involutive H2 H1).
fold ys in H17. wr H17. app H9. cp (standard_completion_pr H2 H1). ee. am.
Qed.

INRIA
Let \( u = \sup_{\lambda} (\inf(y, x_\lambda)) \) and \( v = \inf(y, \sup_{\lambda} (x_\lambda)) \). We consider two functional graphs \( f \) and \( g \) associated to \( x_\lambda \) and \( \inf(y, x_\lambda) \), and state the properties of the sup and inf.

Lemma Exercise1_17e: for all \( r f y \), boolean_lattice \( r \rightarrow \) complete_lattice \( r \rightarrow \)
  \( \text{inc} y \) (substrate \( r \)) \( \rightarrow \) fgraph \( f \rightarrow \) sub (range \( f \)) (substrate \( r \)) \( \rightarrow \)
  \( \text{inf} r y \) (sup_graph \( r f \)) = sup_graph \( r (L (\text{domain} f) (\text{fun} x \mapsto \text{inf} r y (V f x))) \).

Proof. ir. set \( (v := \text{inf} r y \) (sup_graph \( r f ))) \).
  set \( (g := L (\text{domain} f) (\text{fun} x : \text{Set} \mapsto \text{inf} r y (V f x))) \).
  set \( (u := \text{sup} r g ) \).
  red \( \text{in H0. ee. assert (has_sup_graph r f). red. \text{nin (H4 _ H3). am.}
  assert (fgraph g ). uf g. gpprops.}
  assert (\text{sub (range} g \)) (substrate \( r \)). \text{red. \text{uf g. ir. rwi create_range H7.}
  avi H7. nin H7. ee. \text{wr H8. nin H. nin \( \)). \text{cp (lattice}\_\text{props \( H \)). simpl in H11.}
  ee. \text{app H12. app H3. \text{aw. exists x0. app fdefined_lem. nin H2. am.}
  assert (has_sup_graph r g). \text{nin (H4 _ H7). am.}
  \text{cp (is_sup_graph_pr1 H0 H3 H5).}
  \text{cp (is_sup_graph_pr (sup_graph r f) H0 H3 H2). ufi is_sup_graph H10.}
  \text{rwi H10. clear H10.}
  \text{cp (is_sup_graph_pr1 H0 H7 H8).}
  \text{cp (is_sup_graph_pr (sup_graph r g) H0 H7 H6). ufi is_sup_graph H11.}
  \text{rwi H11. H10. clear H11. fold u in H10. ee.}
  assert (lattice \( r \).) \text{nin H. nin \( \). am.}
  \text{cp (lattice_inf_pr H15 H1 H9). fold v in H16. ee.}

We show here \( u \leq v \leq y \). This is rather obvious.

assert (gle r u v). app H18. app H12. ir. uf g. ufi g H19. bwi H19.
  \text{rw create_V_rewrite. assert (inc (V a f) (substrate} r \)). \text{app H3. aw. \text{exists a. ap fdefined_lem. am. am. nin H2;\text{am. cp (lattice_inf_pr H15 H1 H20).}
  ee. am. am. app H12. ir. uf g. ufi g H19. bwi H19. \text{rw create_V_rewrite.}
  assert (inc (V a f) (substrate} r \)). \text{app H3. aw. \text{exists a. ap fdefined_lem.}
  am. am. nin H2;\text{am. cp (lattice_inf_pr H15 H1 H20). ee.}
  assert (gle r (V a f) (sup_graph} r f)). \text{app H13.}
  \text{ap (order_transitivity} H0 H22 H24). am.

Define \( z = \sup (y^*, u) \). We have \( \inf(y, \sup(y^*, u)) = \inf(y, u) = u \).

set \( (z := \text{sup} r (\text{standard_completion} r y) u) \).
  assert (\text{inf} r y z = u). uf z. cp (Exercise1_17d H H10 H1). \text{simpl in H20.}
  ee. \text{wr H20. cp (lattice_props H15). \text{simpl in H24. ee. \text{wr H27.}
  app inf_comparable1. \text{app (order_transitivity} H0 H19 H16). am. am.}

Let \( z' = \sup (y^*, \sup_{\lambda} (x_\lambda)) \). We have \( z = \sup (y^*, \sup_{\lambda} (\inf(y, x_\lambda))) \). We have \( z' \geq z \); we have also \( z \geq z' \); this is because \( z = \sup_{\lambda} (\text{sup} y^*, \inf(y, x_\lambda)) \), and we can simplify the expression.

assert (\( z = \text{sup} r (\text{standard_completion} r y) \) (sup_graph \( r f \)).
  uf z. set \( (ys := \text{standard_completion} r y)\) \text{in *}. uf u.
 \text{assert (inc ys (substrate} r \)). \text{cp (standard_completion_pr H H1). ee. am.}
  \text{cp (lattice_sup_pr H15 H21 H10). \text{cp (lattice_sup_pr H15 H21 H9). ee.}
  assert (gle r (sup r ys \text{sup_graph} r g)) (sup r ys \text{sup_graph} r f)).
  \text{ap H27. ap H23. ap H12. cp (lattice_props H15). \text{simpl in H28. ee. \text{app H28.}
  ir. assert (gle r (V a g) \text{sup_graph} r f)).
  \text{assert (gle r (V a g) (V a f))}. uf g. ufi g H28. bwi H28. bw.
  \text{assert (inc (V a f) (range} f)). \text{app inc_V_range. cp (H3 _ H29).}

RR n° 7150
cp (lattice_inf_pr H15 H1 H30). ee. am. ufi g H28. bwi H28. cp (H13 _ H28).
ap (order_transitivity H0 H29 H30). ap (order_transitivity H0 H29 H24).
assert (gle r (sup r ys (sup_graph r f)) (sup r ys (sup_graph r g))). ap H25. ap H22. ap H14. cp (lattice_props H15). simpl in H29. ee. app H29.
ir. assert (gle r (inf r y (V a f)) (sup_graph r g)).
assert (inf r y (V a f) = V a g). uf g. bw. rw H30. app H11. uf g. bw.
assert (gle r (sup r ys (inf r y (V a f))) (sup_graph r g)).
assert (gle r (sup r ys (sup_graph r f)) (sup r ys (sup_graph r g))).
app (order_transitivity H0 H28 H29).
app (order_antisymmetry H0 H28 H29).
We have inf(y, z') = inf(y, sup(y^*, sup(x_H))).
Since x_H = z, the conclusion is obvious.

¶ 18. *Let A be a set with at least three elements, let P be the set of all partitions of A, ordered by the relation "\( \omega \)' is finer than \( \omega \)" between \( \omega \) and \( \omega \)' (no 1, Example 4). Show that P is a complete lattice (Exercise 11), is not distributive (Exercise 17), but is relatively complemented (To prove the last assertion, well-order the sets belonging to a partition.)*

19. An ordered set E is said to be without gaps if it contains two distinct comparable elements and if, for each pair of elements x, y such that x < y, the open interval \( \langle x, y \rangle \) is not empty. Show that the ordinal sum \( \sum_{i \in I} E_i \) (Exercise 3) is without gaps if and only if the following conditions are satisfied:

(I) Either I contains two distinct comparable elements, or else there exists \( i \in I \) such that \( E_i \) contains two distinct comparable elements.

(II) Each \( E_i \) which contains at least two distinct comparable elements is without gaps.

(III) If \( \alpha, \beta \) are two elements of I such that \( \alpha < \beta \) and if the interval \( \langle \alpha, \beta \rangle \) in I is empty, then either \( E_{\alpha} \) has no maximal element or else \( E_{\beta} \) has no minimal element.

In particular, every ordinal sum \( \sum_{i \in I} E_i \) of sets without gaps is itself without gaps, provided that no \( E_i \) has a maximal element (or provided that no \( E_i \) has a minimal element). If I is without gaps, and if each \( E_i \) is either without gaps or contains no two distinct comparable elements, then \( \sum_{i \in I} E_i \) is without gaps.

¶ 20. An ordered set E is said to be scattered of no ordered subset of E is without gaps (Exercise 19). Every subset of a scattered set is scattered. *Every well-ordered set of more than one element is scattered.*

(a) Suppose that E is scattered. Then if x, y are two elements of E such that x < y, there exists two elements \( x', y' \) of E such that \( x \leq x' < y \leq y' \), and such that the interval \( \langle x', y' \rangle \) is empty. *Give an example of a totally ordered set which satisfies this condition and is not scattered (consider Cantor's triadic set).*
(b) An ordinal sum $\sum_{\iota \in I} E_\iota$ (where neither $I$ nor any $E_\iota$ is empty) is scattered if and only if $I$ and each $E_\iota$ is scattered. (Note that $E$ contains a subset isomorphic to $I$ and that every subset $F$ of $E$ is the ordinal sum of those sets $F \cap E_\iota$ which are non-empty: finally use Exercise 19.)

21. Let $E$ be a non-empty totally ordered set, and let $S \{x, y\}$ be the relation “the closed interval with endpoints $x$, $y$ is scattered” (Exercise 20). Show that $S$ is an equivalence relation which is weakly compatible (Exercise 2) in $x$ and $y$ with the order relation on $E$, that the equivalence classes with respect to $S$ are scattered sets, and that the quotient ordered set $E/S$ is either without gaps or else consists of a single element. Deduce that $E$ is isomorphic to an ordinal sum of scattered sets whose index set is either without gaps or else consists of a single element.

¶ 22. (a) Let $E$ be an ordered set; A subset $U$ of $E$ is said to be open if for each $x \in U$, $U$ contains the interval $[x, \rightarrow]$. An open set $U$ is said to be regular if there exists no open set $V \supset U$, distinct from $U$ such that $U$ is cofinal in $V$. Show that every open set $U$ is cofinal in exactly one regular open set $\bar{U}$. The mapping $U \rightarrow \bar{U}$ is increasing. If $U$, $V$ are two open sets such that $U \cap V = \emptyset$, then also $\bar{U} \cap \bar{V} = \emptyset$.

(b) Show that the set $\mathcal{R}(E)$ of regular open sets of $E$, ordered by inclusion, is a complete Boolean lattice (Exercise 17). For $\mathcal{R}(E)$ to consist of two elements, it is necessary and sufficient that $E$ should be non-empty and right directed.

(c) If $F$ is a cofinal subset of $E$, show that the mapping $U \rightarrow U \cap F$ is an isomorphism of $\mathcal{R}(E)$ onto $\mathcal{R}(F)$.

(d) If $E_1$, $E_2$ are two ordered sets, then every open set in $E_1 \times E_2$ is of the form $U_1 \times U_2$, where $U_i$ is open in $E_i$ ($i = 1, 2$). The set $\mathcal{R}(E_1 \times E_2)$ is isomorphic to $\mathcal{R}(E_1) \times \mathcal{R}(E_2)$.

¶ 23. Let $E$ be an ordered set and let $R_0(E) = \mathcal{R}(E) - \emptyset$ (Exercise 22). For each $x \in E$, let $r(x)$ denote the unique regular open set in which the interval $[x, \rightarrow]$ (which is an open set) is cofinal. The mapping $r$ so defined is called the canonical mapping of $E$ into $R_0(E)$. Endow $R_0(E)$ with the order relation opposite to the relation of inclusion.

(a) Show that the mapping $r$ is increasing and that $r(E)$ is cofinal in $R_0(E)$.

(b) An ordered set $E$ is said to be antidirected if the canonical mapping $r : E \rightarrow R_0(E)$ is injective. For this to be so it is necessary and sufficient that the following two conditions should be satisfied.

(I) If $x$ and $y$ are two elements of $E$ such that $x < y$, there exists $z \in E$ such that $x < z$ and such that the intervals $[y, \rightarrow]$ and $[z, \rightarrow]$ do not intersect.

(II) If $x$ and $y$ are two non-comparable elements of $E$ then either there exists $x' \geq x$ such that the intervals $[x', \rightarrow]$ and $[y, \rightarrow]$ do not intersect, or else there exists $y' \geq y$ such that the intervals $[x, \rightarrow]$ and $[y', \rightarrow]$ do not intersect.

(c) Show that, for every ordered set $E$, $R_0(E)$ is antidirected and that the canonical mapping of $R_0(E)$ into $R_0(R_0(E))$ is bijective (use Exercise 22(a)).

24. * (a) An ordered set $E$ is said to be branched (on the right) if for each $x \in E$ there exist $y$, $z$ in $E$ such that $x \leq y$, $x \leq z$ and the intervals $[y, \rightarrow]$ and $[z, \rightarrow]$ do not intersect. An antidirected set with no maximal element (Exercise 23) is branched.
(b) Let \( E \) be the set of intervals in \( \mathbb{R} \) of the form \([k.2^{-n}, (k+1).2^{-n}]\) \((0 \leq k < n)\), ordered by the relation \( \supset \). Show that \( E \) is antidirected and has no maximal elements.

(c) Give an example of a branched set in which there exists no antidirected cofinal subset (Take the product of the set \( E \) defined in (b) with a well-ordered set which contains no countable cofinal subset, and use Exercise 22.)

(d) Give an example of an ordered set \( E \) which is not antidirected, but which has an antidirected cofinal subset (Note that an ordinal sum \( \sum_{\xi \in E} F_\xi \) contains a cofinal subset isomorphic to \( E \)).

### 9.2 Section 2

1. Show that, in the set of orderings on a set \( E \), the minimal elements (with respect to the ordered relation “\( \Gamma \) is coarser than \( \Gamma' \)” between \( \Gamma \) and \( \Gamma' \)) are the total orderings on \( E \) and that if \( \Gamma \) is any ordering on \( E \), the graph of \( \Gamma \) is the intersection of the graphs of the total orderings on \( E \) which are coarser than \( \Gamma \) (apply Theorem 2 of no. 4). Deduce that every ordered set is isomorphic to a subset of a product of totally ordered sets.

2. Let \( E \) be an ordered set and let \( \mathcal{B} \) be the set of subsets of \( E \) which are well-ordered by the inducing ordering. Show that the relation “\( X \) is a segment of \( Y \)” on \( \mathcal{B} \) is an order relation between \( X \) and \( Y \) and that \( \mathcal{B} \) is inductive with respect to this order relation. Deduce that there exist well-ordered subsets of \( E \) which have no strict upper bound in \( E \).

3. Let \( E \) be an ordered set. Show that there exist two subsets \( A, B \), of \( E \) such that \( A \cup B = E \) and \( A \cap B = \emptyset \) and such that \( A \) is well-ordered and \( B \) has no least element (for example, take \( B \) to be the union of those subsets of \( E \) which have no least element). *Give an example in which there are several partitions of \( E \) into two subsets having these properties.*

¶ 4. An ordered set \( F \) is said to be **partially well-ordered** if every totally ordered subset of \( F \) is well-ordered. Show that in every ordered set \( E \) there exists a partially well-ordered subset which is cofinal in \( E \) (Consider the set \( \mathfrak{F} \) of partially well-ordered subsets of \( E \), and the order relation “\( X \subset Y \) and no element of \( Y \) is bounded above by any element of \( X \)” between \( X \) and \( Y \) of \( \mathfrak{F} \). Show that \( \mathfrak{F} \) is inductive with respect to this order relation).

5. Let \( E \) be an ordered set and let \( \mathfrak{I} \) be the set of free subsets of \( E \), ordered by the relation defined in § 1, Exercise 5. Show that, if \( E \) is inductive, then \( \mathfrak{I} \) has a greatest element.

¶ 6. Let \( E \) be an ordered set and let \( f \) be a mapping from \( E \) into \( E \) such that \( f(x) \geq x \) for all \( x \geq E \).

(a) Let \( \mathfrak{M} \) be the set of subsets \( M \) of \( E \) with the following properties: (1) the relation \( x \in M \) implies \( f(x) \in M \); (2) if a non-empty subset of \( M \) has a least upper bound in \( E \), then this least upper bound belongs to \( M \). For each \( a \in E \), show that the intersection \( C_a \) of the sets of \( \mathfrak{M} \) which contain \( a \) also belongs to \( \mathfrak{M} \); that \( C_a \) is well-ordered; and that if \( C_a \) has an upper bound \( b \) in \( E \), then \( b \in C_a \) and \( f(b) = b \). \( C_a \) is said to be the **chain** of \( a \) (with respect to the function \( f \)). (Consider the set \( \mathfrak{M} \) whose elements are the empty set and the subsets \( X \) of \( E \) which contain
(a) Show that \( u \leq v \) in \( F \) if and only if \( I(v) \subset I(u) \).

(b) If \( E \) is branched (§ 1, Exercise 24), show that every maximal element of \( \mathcal{R}_a \) is completely ramified.

(c) Given an example of a branched set which is not ramified. The branched set defined in § 1, Exercise 24 (c) is completely ramified.

(d) Let \( E \) be a set in which each interval \( ]-\), x[ \) is totally ordered. Show that \( E \) has an antidirected cofinal subset (§ 1, Exercise 22) (use (b)).

9. An ordinal sum \( \sum_{\alpha \in I} E_\alpha \) (§ 1, Exercise 3) is well-ordered if and only if \( I \) and each \( E_\alpha \) is well-ordered.

10. Let \( I \) be an ordered set and let \( (E_\alpha)_{\alpha \in I} \) be a family of ordered sets, all equal to the same ordered set \( E \). Show that the ordinal sum \( \sum_{\alpha \in I} E_\alpha \) (§ 1, Exercise 3) is isomorphic to the lexicographic product of the sequence \( (F_\lambda)_{\lambda \in \{\alpha, \beta\}} \), where the set \( \{\alpha, \beta\} \) of two distinct elements is well-ordered by the relation whose graph is \( \{(\alpha, \alpha), (\alpha, \beta), (\beta, \beta)\} \), and where \( F_\alpha = I \) and \( F_\beta = E \). This product is called the lexicographic product of \( E \) by \( I \) and is written \( E \cdot I \).

\( \mathfrak{11} \). Let \( E \) be a well-ordered set and let \( (E_\alpha)_{\alpha \in I} \) be a family of ordered sets, each of which contains at least two distinct comparable elements. Then the lexicographic product of the \( E_\alpha \) is well-ordered if and only if each of the \( E_\alpha \) is well-ordered and \( I \) is finite (if \( I \) is infinite, construct a strictly decreasing infinite sequence in the lexicographic product if the \( E_\alpha \) ).
§ 12. Let $I$ be a totally ordered set and let $(E_i)_{i \in I}$ be a family of ordered sets indexed by $I$. Let $R^I x, y I$ denote the following relation on $E = \prod_{i \in I} E_i$: “the set of indices $i \in I$ such that $p_i x \neq p_i y$ is well-ordered, and if $\kappa$ is the least element of this subset of $I$, we have $p_\kappa x < p_\kappa y$”. Show that $R^I x, y I$ is an order relation between $x$ and $y$ on $E$. If the $E_i$ are totally ordered, show that the connected components of $E$ with respect to the relation “$x$ and $y$ are comparable” (Chapter II, § 6, Exercise 10) are totally ordered sets. Suppose that each $E_i$ has at least two elements. Then $E$ is totally ordered if and only if if $I$ is well-ordered and each $E_i$ is totally ordered (use Exercise 3); and $E$ is then the lexicographic product of the $E_i$.

13. (a) Let $\text{Is}(\Gamma, \Gamma')$ be the relation “$\Gamma$ is an ordering (on $E$) and $\Gamma'$ is an ordering (on $E'$), and there exists an isomorphism of $E$, ordered by $\Gamma$, onto $E'$, ordered by $\Gamma'$”. Show that $\text{Is}(\Gamma, \Gamma')$ is an equivalence relation on every set whose elements are orderings. The term $\tau \Delta (\text{Is}(\Gamma, \Delta))$ is an ordering called the order-type of $\Gamma$ and denoted by $\text{Ord}(\Gamma)$, or $\text{Ord}(E)$ by abuse of notations.

Two ordered sets are isomorphic if and only if their order-types are equal.

(b) Let $R^I \lambda, \mu I$ be the relation: “$\lambda$ is an order-type, and $\mu$ is an order-type and there exists an isomorphism of the set ordered by $\lambda$ onto a subset of the set ordered by $\mu$”. Show that $R^I \lambda, \mu I$ is a preorder relation between $\lambda$ and $\mu$. It will be denoted by $\lambda < \mu$.

(c) Let $I$ be an ordered set and let $(\lambda_i)_{i \in I}$ be a family of order-types indexed by $I$. The order-type of the ordinal sum (§ 1, Exercise 3) of the family of sets ordered by the $\lambda_i$ (i.e., $i \in I$) is called the ordinal sum of the order-types $\lambda_i$ (i.e., $i \in I$) and is denoted by $\sum_{i \in I} \lambda_i$. If $(E_i)_{i \in I}$ is a family of ordered sets, the order type of $\sum_{i \in I} E_i$ is $\sum_{i \in I} \text{Ord}(E_i)$. If $I$ is the ordinal sum of a family $(J_k)_{k \in K}$, show that

$$\sum_{k \in K} \left( \sum_{i \in J_k} \lambda_i \right) = \sum_{i \in I} \lambda_i.$$

(d) Let $I$ be a well-ordered set and $(\lambda_i)_{i \in I}$ be a family of order-types indexed by $I$. The order-type of the lexicographic product of the family of sets indexed by $\lambda_i$ (i.e., $i \in I$) is called the ordinal product of the order-types $\lambda_i$ (i.e., $i \in I$) and is denoted by $\prod_{i \in I} \lambda_i$. If $(E_i)_{i \in I}$ is a family of ordered sets, the order type of the lexicographic product of the family of sets $(E_i)_{i \in I}$ is $\prod_{i \in I} \text{Ord}(E_i)$. If $I$ is the ordinal sum of a family of well-ordered sets $(J_k)_{k \in K}$, indexed by a well-ordered set $K$, show that

$$\prod_{k \in K} \left( \prod_{i \in J_k} \lambda_i \right) = \prod_{i \in I} \lambda_i.$$

(e) We denote by $\lambda + \mu$ (resp. $\mu \lambda$) the ordinal sum (resp. ordinal product) of the family $(\xi_i)_{i \in I}$ where $I = [\alpha, \beta]$ is a set with two distinct elements, ordered by the relation whose graph is $\{[\alpha, \alpha], (\alpha, \beta), (\beta, \beta)\}$, and where $\xi_{\alpha} = \lambda$ and $\xi_{\beta} = \mu$. Show that if $I$ is a well-ordered set of order-type $\lambda$ and if $(\mu_i)_{i \in I}$ is a family of order-types such that $\mu_i = \mu$ for each $i \in I$ then $\sum_{i \in I} \mu_i = \mu \lambda$. We have $(\lambda + \mu) + \nu = \lambda + (\mu + \nu)$, $(\lambda \mu) \nu = \lambda (\mu \nu)$, and $\lambda (\mu + \nu) = \lambda \mu + \lambda \nu$ (but in general $\lambda + \mu \neq \mu + \lambda$, $\lambda \mu \neq \mu \lambda$ and $(\lambda + \mu) \nu \neq \lambda \nu + \mu \nu)$.

(f) Let $(\lambda_i)_{i \in I}$ and $(\mu_i)_{i \in I}$ be two families of order-types indexed by the same ordered set $I$. Show that if $\lambda_i < \mu_i$ for each $i \in I$, then $\sum_{i \in I} \lambda_i < \sum_{i \in I} \mu_i$ and (if $I$ is well-ordered) $\prod_{i \in I} \lambda_i < \prod_{i \in I} \mu_i$. If $J$ is a subset of $I$, show that $\sum_{i \in J} \lambda_i < \sum_{i \in J} \lambda_i$ and (if $I$ is well-ordered and the $\lambda_i$ are non-empty) $\prod_{i \in J} \lambda_i < \prod_{i \in J} \lambda_i$. 

INRIA
(g) Let \( \lambda^* \) denote the order-type of the set ordered by the opposite of the ordering \( \lambda \). Then we have
\[
(\lambda^*)^* = \lambda \quad \text{and} \quad (\sum_{i \in I} \lambda_i)^* = \sum_{i \in I^*} \lambda_i^*
\]
where \( I^* \) denotes the set \( I \) endowed with the opposite of the ordering given in \( I \).

§ 14. An ordinal is the order-type of a well-ordered set (Exercise 13).

(a) Show that, if \( (\lambda_i)_{i \in I} \) is a family of ordinals indexed by a well-ordered set \( I \), then the ordinal sum \( \sum_{i \in I} \lambda_i \) is an ordinal; “and that, if moreover, \( I \) is finite, then the ordinal product \( \prod_{i \in I} \lambda_i \) is an ordinal (Exercise 11).” The order-type of the empty set is denoted by 0, and that of a set with one element by 1 (by abuse of language, cf § 3). Show that
\[
\alpha + 0 = 0 + \alpha = \alpha \quad \text{and} \quad \alpha.1 = 1.\alpha = \alpha
\]
for every ordinal \( \alpha \).

(b) Show that the relation “\( \lambda \) is an ordinal and \( \mu \) is an ordinal and \( \lambda < \mu \)” is a well-ordering relation, denoted by \( \lambda \leq \mu \) (Note that, if \( \lambda \) are ordinals, the relation \( \lambda < \mu \) is equivalent to “\( \lambda \) is equal to the order-type of a segment of \( \mu \)” (no. 5, Theorem 3, Corollary 3): given a family \( (\lambda_i)_{i \in I} \) of ordinals, consider a well-ordering in \( I \) and take the ordinal sum of the family of sets ordered by the \( \lambda_i \); finally use Proposition 2 of no 1.).

(c) Let \( \alpha \) be an ordinal. Show that the relation “\( \xi \) is an ordinal and \( \xi \leq \alpha \)” is collectivizing in \( \xi \), and that the set \( O_\alpha \) of ordinals \( < \alpha \) is a well-ordered set such that \( \text{Ord}(O_\alpha) = \alpha \). We shall often identify \( O_\alpha \) with \( \alpha \).

(d) Show that for every family \( (\xi_i)_{i \in I} \) there exists a unique ordinal \( \alpha \) such that the relation “\( \lambda \) is an ordinal and \( \xi_i \leq \lambda \) for all \( i \in I \)” is equivalent to \( \alpha \leq \lambda \). By abuse of language, \( \alpha \) is called the least upper bound of the family of ordinals \( (\xi_i)_{i \in I} \), and we write \( \alpha = \sup_{i \in I} \xi_i \) (it is the greatest element of the union of \( (\alpha) \) and the set of the \( \xi_i \)). The least upper bound of the set of ordinals \( \xi < \alpha \) is either \( \alpha \) or an ordinal \( \beta \) such that \( \alpha = \beta + 1 \). In the latter case \( \beta \) is said to be the predecessor of \( \alpha \).

15. (a) Let \( \alpha \) and \( \beta \) be two ordinals. Show that the inequality \( \alpha < \beta \) is equivalent to \( \alpha + 1 \leq \beta \), and that it implies the inequalities \( \xi + \alpha < \xi + \beta \), \( \alpha + \xi \leq \beta + \xi \), \( \alpha \xi \leq \beta \xi \) for all ordinals \( \xi \) and \( \xi \alpha < \xi \beta \) if \( \xi > 0 \).

(b) Deduce from (a) that there exists no set to which every ordinal belongs (use Exercise 14 (d)).

(c) Let \( \alpha, \beta, \mu \) be three ordinals. Show that each of the relations \( \mu + \alpha < \mu + \beta \), \( \alpha + \mu < \beta + \mu \) implies \( \alpha < \beta \); and that each of the relations \( \mu \alpha < \mu \beta \), \( \alpha \mu < \beta \mu \) implies \( \alpha < \beta \) provided that \( \mu > 0 \).

(d) Show that the relation \( \mu + \alpha = \mu + \beta \), implies \( \alpha = \beta \), and that \( \mu \alpha = \mu \beta \), implies \( \alpha = \beta \) provided that \( \mu > 0 \).

(e) Two ordinals \( \alpha \) and \( \beta \) are such that \( \alpha \leq \beta \) if and only if there exists and ordinal \( \xi \) such that \( \beta = \alpha + \xi \). This ordinal is then unique and is such that \( \xi \leq \beta \); it is written \( (-\alpha) + \beta \).

(f) Let \( \alpha, \beta, \xi \) be three ordinals such that \( \xi < \alpha \beta \). Show that there exists two ordinals \( \xi, \eta \) such that \( \xi = \alpha \eta + \xi \) and \( \xi < \alpha, \eta < \beta \) (cf. No. 5, Theorem 3, Corollary 3). Moreover, \( \xi \) and \( \eta \) are uniquely determined by these conditions.
\textbf{§ 16.} An ordinal \(\rho > 0\) is said to be \textit{indecomposable} if there exists no pair of ordinals \(\xi, \eta\) such that \(\xi < \rho, \eta < \rho\) and \(\xi + \eta = \rho\).

(a) An ordinal \(\rho\) is indecomposable if and only if \(\xi + \rho = \rho\) for every ordinal \(\xi\) such that \(\xi < \rho\).

(b) If \(\rho > 1\) is an indecomposable ordinal and if \(\alpha\) is any ordinal \(> 0\), then \(\alpha \rho\) is indecomposable, and conversely \((\text{use Exercise 15(f)})\).

(c) If \(\rho\) is indecomposable and if \(0 < \alpha < \rho\), then \(\rho = \alpha \zeta\), where \(\zeta\) is an indecomposable ordinal \((\text{use Exercise 15(f)})\).

(d) Let \(\alpha\) be an ordinal \(> 0\). Show that there exists a greatest indecomposable ordinal among the indecomposable ordinals \(< \alpha\) \((\text{consider the decomposition } \alpha = \rho + \xi, \text{ where } \rho \text{ is indecomposable})\).

(e) If \(\mathcal{E}\) is a set of indecomposable ordinals, deduced from \(\text{(d)}\) that the least upper bound of \(\mathcal{E}\) \((\text{Exercise 14(d)})\) is an indecomposable ordinal.

\textbf{§ 17.} Given an ordinal \(\alpha_0\), a term \(f(\xi)\) is said to be an \textit{ordinal functional symbol (with respect to } \xi) \textit{defined for } \xi \geq \alpha_0 \textit{if the relation } "\xi\textit{ is an ordinal and } \xi \geq \alpha_0" \textit{implies the relation } "f(\xi)\textit{ is an ordinal}"; \(f(\xi)\) is said to be \textit{normal} if the relation \(\alpha_0 \leq \xi < \eta\) implies \(f(\xi) < f(\eta)\) and if for each family \((\xi_i)_{i \in I}\) of ordinals \(\geq \alpha_0\) we have \(\sup_{i \in I} f(\xi_i) = f(\sup_{i \in I} \xi_i)\) \((\text{cf. Exercise 14(d)})\).

(a) Show that for each ordinal \(\alpha > 0, \alpha + \xi\) and \(\alpha \xi\) are ordinal functional symbols defined for \(\xi \geq 0\) \((\text{use Exercise 15(f)})\).

(b) Let \(w(\xi)\) be an ordinal functional symbols defined for \(\xi \geq \alpha_0\) such that \(w(\xi) \geq \xi\) and such that \(\alpha_0 \leq \xi < \eta\) implies \(w(\xi) < w(\eta)\). Also let \(g(\xi, \eta)\) be a term such that the relation "\(\xi\) and \(\eta\) are ordinals such that \(g(\xi, \eta) \geq \xi'\). Define a term \(f(\xi, \eta)\) with the following properties:

(1) for each ordinal \(\xi \geq \alpha_0\), \(f(\xi, 1) = w(\xi)\); for each ordinal \(\xi \geq \alpha_0\) and each ordinal \(\eta > 1\), \(f(\xi, \eta) = \sup_{0 < \xi < \eta} g(f(\xi, \xi), \xi)\) \((\text{use Criterion C60 of no. } 2)\). Show that if \(f_1(\xi, \eta)\) is another term with these properties then \(f(\xi, \eta) = f_1(\xi, \eta)\) for all \(\xi \geq \alpha_0\) and all \(\eta \geq 1\). Prove that, for each ordinal \(\xi \geq \alpha_0, f(\xi, \eta)\) is a normal functional symbol with respect to \(\eta\) \((\text{defined for } \eta \geq 1)\). Show that \(f(\xi, \eta) \geq \xi\) for all \(\eta \geq 1\) and \(\xi \geq \alpha_0\) and that \(f(\xi, \eta) \geq \eta\) for all \(\xi \geq \sup(\alpha_0, 1)\) and \(\eta \geq 1\). Furthermore, for each pair \((\alpha, \beta)\) of ordinals such that \(\alpha > 0, \alpha \geq \alpha_0\) and \(\beta \geq w(\alpha)\) there exists a unique ordinal \(\xi\) such that

\[ f(\alpha, \xi) \leq \beta < f(\alpha, \xi + 1), \]

and we have \(\xi \leq \beta\).

(c) If we take \(\alpha_0 = 0, w(\xi) = \xi + 1, g(\xi, \eta) = \xi + 1\) then \(f(\xi, \eta) = \xi + \eta\). If we take \(\alpha_0 = 1, w(\xi) = \xi, g(\xi, \eta) = \xi + \eta\) then \(f(\xi, \eta) = \xi\).

(d) Show that if the relations \(\alpha_0 \leq \xi \leq \xi', \alpha_0 \leq \eta \leq \eta'\) imply \(g(\xi, \eta) \leq g(\xi', \eta')\), then the relations \(\alpha_0 \leq \xi \leq \xi', 1 \leq \eta \leq \eta'\) imply \(f(\xi, \eta) \leq f(\xi', \eta')\). If the relations \(\alpha_0 \leq \xi \leq \xi', \alpha_0 \leq \eta \leq \eta'\) imply \(g(\xi, \eta) < g(\xi, \eta')\) and \(g(\xi, \eta) \leq g(\xi', \eta')\), then the relations \(\alpha_0 \leq \xi \leq \xi'\) and \(\eta \geq 0\) imply \(f(\xi, \eta + 1) \leq f(\xi', \eta + 1)\).

(e) Suppose that \(w(\xi) = \xi\) and that the relations \(\alpha_0 \leq \xi \leq \xi', \alpha_0 \leq \eta \leq \eta'\) imply \(g(\xi, \eta) < g(\xi, \eta')\) and \(g(\xi, \eta') \leq g(\xi', \eta')\). Suppose moreover, that for each \(\xi \geq \alpha_0, g(\xi, \eta)\) is a normal functional symbol with respect to \(\eta\) \((\text{defined for } \eta \geq \alpha_0)\), and that, whenever \(\xi \geq \alpha_0, \eta \geq \alpha_0, \) and \(\xi \geq \alpha_0\), we have the associativity relation

\[ g(\xi, \eta) \cdot g(\xi', \eta') = g(\xi', \eta) \cdot g(\xi, \eta') \]
Show that, if \( \xi \geq \alpha_0, \eta \geq 1, \) and \( \zeta \geq 1, \) we have then
\[
g(f(\xi, \eta), f(\xi, \zeta)) = f(\xi, \eta + \zeta)
\]
("distributivity" of \( g \) with respect to \( f \)) and
\[
f(f(\xi, \eta), \zeta) = f(\xi, \eta \zeta)
\]
("associativity" of \( f \)).

\section*{§ 18.} In the definition procedure defined in Exercise 17 (b), take \( \alpha_0 = 1 + 1 \) (denoted by 2 by abuse of language),
\[
w(\xi) = \xi, \quad g(\xi, \eta) = \xi \eta.
\]
Denote \( f(\xi, \eta) \) by \( \xi^n \) and define \( \alpha^0 \) to be 1 for all ordinals \( \alpha \). Also define \( \alpha^0 \) to be 0 and \( 1^0 \) to be 1 for all ordinals \( \beta \geq 1 \).

(a) Show that if \( \alpha > 1 \) and \( \beta < \beta' \), we have \( \alpha^0 < \alpha^0 \beta' \), and that, for each ordinal \( \alpha > 1 \), \( \alpha^\xi \) is a normal functional symbol with respect to \( \xi \). Moreover, if \( 0 < \alpha \leq \alpha' \), we have \( \alpha^0 \leq \alpha'^0 \).

(b) Show that \( \alpha^\xi, \alpha^n = \alpha^{\xi+n} \) and \( (\alpha^\xi)^n = \alpha^{\xi n} \).

(c) Show that if \( \alpha \geq 2 \) and \( \beta \geq 1, \alpha^0 \leq \alpha^0 \).

(d) For each pair of ordinals \( \beta \geq 1 \) and \( \alpha \geq 2 \), there exists three ordinals \( \xi, \gamma, \delta \) such that \( \beta = \alpha^\xi \gamma + \delta \) where \( 0 < \gamma \alpha \) and \( \delta < \alpha^\xi \), and these ordinals are uniquely defined by these conditions.

\section*{§ 19.} Let \( \alpha \) and \( \beta \) be two ordinals and let \( E \) and \( F \) be two well-ordered sets such that \( \text{Ord}(E) = \alpha \) and \( \text{Ord}(F) = \beta \). In the set \( E^F \) of mappings of \( F \) into \( E \) consider the subset \( G \) of mappings \( g \) such that \( g(y) \) is equal to the least element of \( E \) for all \( y \in F \). if \( F^* \) is the ordered set obtained by endowing \( F \) with the opposite order, show that \( G \) is a connected component with respect to the relation \( "x \) and \( y \) are comparable" (Chapter II, § 6, Exercise 10) in the product \( E^{F^*} \) endowed with the ordering defined in Exercise 12, and show that \( G \) is well-ordered. Furthermore, prove that \( \text{Ord}(G) = \alpha^0 \) (use the uniqueness property of Exercise 17 (b)).

\section*{§ 20.} A set \( X \) is said to be \emph{transitive} if the relation \( x \in X \) implies \( x \subset X \).

(a) If \( Y \) is a transitive set, then so is \( Y \cup \{y\} \). If \( (Y_i)_{i \in I} \) is a family of transitive sets, then \( \bigcup_{i \in I} Y_i \) are transitive.

(b) A set \( X \) is a \emph{pseudo-ordinal} if every transitive set \( Y \) such that \( Y \subset X \) and \( Y \neq X \) is an element of \( X \). A set \( S \) is said to be \emph{decent} if the relation \( x \in S \) implies \( x \not\in x \). Show that every pseudo-ordinal is transitive and decent (consider the union of decent transitive subsets of \( X \) and use (a)). If \( X \) is a pseudo-ordinal, so is \( X \cup \{x\} \).

(c) Let \( X \) be a transitive set and suppose that each \( x \in X \) is a pseudo-ordinal. Then \( X \) is a pseudo-ordinal (note that, for each \( x \in X, x \cup \{x\} \) is a pseudo-ordinal contained in \( X \)).

(d) Show that \( \varnothing \) is a pseudo-ordinal and that every element of a pseudo-ordinal \( X \) is a pseudo-ordinal (Consider the union of the transitive subsets of \( X \) whose elements are pseudo-ordinals).

(e) If \( (X_i)_{i \in I} \) is a family of pseudo-ordinals then \( \bigcap_{i \in I} X_i \) is the least element of this family (with respect to the relation of inclusion). (Use (b).) Deduced that, if \( E \) is a pseudo-ordinal, the relation \( x \subset y \) between elements \( x, y \) of \( E \) is a well-ordering relation.
(f) Show that for each ordinal \( \alpha \) there exists a unique pseudo-ordinal \( E_\alpha \) such that \( \text{Ord}(E_\alpha) = \alpha \) (use (e) and Criterion C60). In particular the pseudo-ordinals whose order-type are 0, 1, \( 2 = 1 + 1 \), and \( 3 = 2 + 1 \) are respectively
\[
\emptyset, \ \{\emptyset\}, \ \{\emptyset, \{\emptyset\}\}, \ \{\emptyset, \{\emptyset\}, \{\emptyset\}\}\]

Note. The French version of the exercise has one more item. It says: if \( X \) and \( Y \) are two pseudo-ordinals, then either \( X \in Y \) or \( Y \in X \) or \( X = Y \). The hint for item (c) is: note that if \( Y \neq X \) is transitive, then \( Y \subset x \).

9.3 Section 3

¶ 1. Let \( E \) and \( F \) be two sets, let \( f \) be an injection of \( E \) into \( F \) and let \( g \) be mapping of \( F \) into \( E \). Show that there exist two subsets \( A, B \) of \( E \) such that \( B = E - A \) and two subsets \( A', B' \) of \( F \) such that \( B' = F' - A' \) for which \( A' = f(A) \) and \( B = g(B') \). (Let \( R = E - g(F) \) and put \( h = g \circ f \); take \( A \) to be the intersection of the subsets \( M \) of \( E \) such that \( M \supset R \cup h(M) \).

2. If \( E \) and \( F \) are two distinct sets, show that \( E \cdot F \neq F \cdot E \). Deduce that if \( E \) and \( F \) are the cardinals \( 2 \) and \( 4 \) (\( 4 = 2 + 2 \)), then at least one of the sets \( E \cdot F \), \( F \cdot E \) is not a cardinal.

Assume \( E \cdot F = F \cdot E \). If \( E \) is non-empty and \( x \in E \), then the graph of the constant function with source \( F \) and value \( x \) is in \( E \cdot F \). The domain of this graph is \( F \); from \( E \cdot F = F \cdot E \) we deduce that it is \( E \), hence \( E = F \). The same conclusion holds, by symmetry, if \( F \) is non-empty. The remaining case is \( E = \emptyset = F \).

Denote by \( \text{pow}(E; F) \) the cardinal of \( F(E; F) \), the set of functions from \( F \) into \( E \). We have shown (lemma power_2_4) that \( \text{pow}(2; 4) = \text{pow}(4; 2) \). Thus, if \( a \) is a cardinal equipotent to \( F(2; 4) \) and \( b \) a cardinal equipotent to \( F(4; 2) \), we have \( a = b \). The sets \( 4^2 \) and \( 2^4 \) are equipotent; if they were cardinals we would deduce \( 2 = 4 \). From \( 4 = 2 + 2 \) we get \( 0 = 2 \), which is absurd.

it is (according to bijective_graph_function) the cardinal of \( F \cdot E \); it is \( F \cdot E \) if \( F \cdot E \) is a cardinal.

¶ 3. Let \( (a_t)_{t \in I} \) and \( (b_t)_{t \in I} \) be two families of cardinals such that \( b_t \geq 2 \) for each \( t \in I \).

(a) Show that, if \( a_t \leq b_t \) for each \( t \in I \), then
\[
\sum_{t \in I} a_t \leq \prod_{t \in I} b_t.
\]

(b) Show that, if \( a_t < b_t \) for each \( t \in I \), then
\[
\sum_{t \in I} a_t < \prod_{t \in I} b_t.
\]

(Note that a product \( \prod_{t \in I} E_t \) cannot be the union of a family \( (A_t)_{t \in I} \) such that \( \text{Card}(A_t) < \text{Card}(E_t) \) for all \( t \in I \), by observing that \( \text{Card}(\text{pr}_t(A_t)) < \text{Card}(E_t) \).)

4. Let \( E \) be a set and let \( f \) be a mapping of \( \mathbb{P}(E) - \emptyset \) into \( E \) such that for each non-empty subset \( X \) of \( E \) we have \( f(X) \in X \) ("Choice function").

(a) Let \( b \) be cardinal and let \( A \) be the set of all \( x \in E \) such that \( \text{Card}(f^{-1}(x)) \leq b \). Show that if \( a = \text{Card}(A) \), then \( 2^a \leq 1 + a \cdot b \) (note that if \( Y \subset A \) and \( Y \neq \emptyset \) then \( f(Y) \in A \)).
(b) Let $B$ be the set of all $x \in E$ such that, for each non-empty subset $X$ of $f^{-1}(x)$, $\text{Card}(X) \leq b$. Show that $\text{Card}(B) \leq b$.

5. Let $(\lambda_i)_{i \in I}$ be a family of order-types ($\S 2$, Exercise 13), indexed by an ordered set $I$. Show that
\[
\text{Card} \left( \sum_{i \in I} \lambda_i \right) = \sum_{i \in I} \text{Card}(\lambda_i)
\]
and that, if $I$ is well-ordered,
\[
\text{Card} \left( \bigcup_{i \in I} \lambda_i \right) = \bigcup_{i \in I} \text{Card}(\lambda_i)
\]

6. Show that for every set $E$ there exists $X \subset E$ such that $X \not\in E$ (use Theorem 2 of no. 6).

9.4 Section 4

1. (a) Let $E$ be a set and let $\mathfrak{F}(E)$ be the set of finite subsets of $E$. Show that $\mathfrak{F}(E)$ is the smallest subset $\mathfrak{G}$ of $\mathcal{P}(E)$ satisfying the following conditions: (i) $\emptyset \in \mathfrak{G}$; (ii) the relation $X \in \mathfrak{G}$ and $x \in E$ imply $X \cup \{x\} \in \mathfrak{G}$.

(b) Deduce from (a) that the union of two finite subsets $A$ and $B$ is finite (consider the set of subsets $X$ of $E$ such that $X \cup A$ is finite; cf $\S 5$; no 1 Proposition 1, Corollary 1).

(c) Deduce from (a) and (b) that for every finite set $E$ the set $\mathfrak{N}(E)$ is finite (consider the set of subsets $X$ of $E$ such that $\mathfrak{N}(X)$ is finite; cf $\S 5$; no 1 Proposition 1, Corollary 4).

2. Show that a set $E$ is finite if and only every non-empty subset of $\mathfrak{N}(E)$ has a maximal element (with respect to inclusion). (To show that the condition is sufficient, apply it to the set $\mathfrak{F}(E)$ of finite subsets of $E$).

3. Show that if a well-ordered set $E$ is such that the ordered set obtained by endowing $E$ with the opposite ordering is also well-ordered, then $E$ is finite (consider the greatest element $x$ of $E$ such that the segment $S_x$ is finite.

4. Let $E$ be a finite set with $n \geq 2$ elements, and let $C$ be a subset of $E \times E$ such that, for each pair $x, y$ of distinct elements of $E$, exactly one of the two elements $(x, y), (y, x)$ of $E \times E$ belongs to $C$. Show that there is a mapping $f$ of the interval $[1, n]$ onto $E$ such that $(f(i), f(i + 1)) \in C$ for $1 \leq i \leq n - 1$ (use induction on $n$).

§ 5. Let $E$ be an ordered set for which there exists an integer $k$ such that $k$ is the greatest number of elements in a free subset $X$ of $E$ ($\S 1$, Exercise 5). Show that $E$ can be partitioned into $k$ totally ordered subsets (with respect to the induced ordering). The proof is in two steps:

(a) If $E$ is finite and has $n$ elements, use induction on $n$; let $a$ be a minimal element of $E$ and let $E' = E - \{a\}$. If there exists a partition of $E'$ into $k$ totally ordered sets $C_i$ ($1 \leq i \leq k$), let $U_i$ be the set of all $x \in C_i$ which are $\geq a$. Show that there is at least one index $i$ for which a free subset $E' - U_i$ has at most $k - 1$ elements. The proof of this is by reduction ad absurdum. For

\footnote{This is called Dilworth’s theorem in the French edition}
each \( i \), let \( S_i \) be a free subset of \( E' - U_i \) which has \( k \) elements, let \( S \) be the union of the sets \( S_i \), and let \( s_j \) be the least element of \( S \cap C_j \) for each index \( j \leq k \); show that the \( k + 1 \) elements \( a, s_1, \ldots, s_k \) form a free subset of \( E \).

(b) If \( E \) is arbitrary, the proof is by induction on \( k \), as follows. A subset \( C \) of \( E \) is said to be strongly related in \( E \) if for each finite subset \( F \) of \( E \) there exists a partition of \( F \) into at most \( k \) totally ordered sets such that \( C \cap F \) is contained in one of them. Show that there exists a maximal strongly related subset \( C_0 \), and that every free subset of \( E - C_0 \) has at most \( k - 1 \) elements (Argue by contradiction, and suppose that there is a free subset \( \{a_1, \ldots, a_k\} \) of \( k \) elements in \( E - C_0 \); Consider each set \( C_0 \cup \{a_i\} \) \((1 \leq i \leq k)\), and express the fact that it is not strongly related, thus introducing a finite subset \( F_i \) of \( E \) for each index \( i \). Then consider the union \( F \) of these sets \( F_i \) and use the fact that \( C_0 \) is strongly related to obtain a contradiction).

\[ \frac{\text{§ 6.}}{\text{Let } A \text{ be a set and let } (X_i)_{1 \leq i \leq m}, (Y_j)_{m+1 \leq j \leq m+n} \text{ be two finite families of subsets of } A. \text{ Let } h \text{ be the least integer such that, for each integer } r \leq m - h \text{ and each subset } \{i_1, \ldots, i_{r+h}\} \text{ of } r + h \text{ elements of } [1, m], \text{ there exists a subset } \{j_1, \ldots, j_r\} \text{ of } r \text{ elements of } [m+1, m+n] \text{ for which the union of the sets } X_{i_{1}} (1 \leq \alpha \leq r + h) \text{ meets each of the sets } Y_{j_{1}} (1 \leq \beta \leq r) \text{ (which implies that } m \leq n + h). \text{ Show that there exists a finite subset } B \text{ of } A \text{ with at most } n + h \text{ elements such that every } X_i (1 \leq i \leq m) \text{ and every } Y_j (m + 1 \leq j \leq m + n) \text{ meets } B. \text{ Consider the order relation on the interval } [1, m+n] \text{ whose graph is the union of the diagonal and the set of pairs } (i, j) \text{ such that } 1 \leq i \leq m \text{ and } m + 1 \leq j \leq m + n \text{ and } X_i \cap Y_j \neq \emptyset, \text{ and apply Exercise 5 to this ordered set.)}

(b) Let \( E \) and \( F \) be two finite sets and let \( x \to A(x) \) be a mapping of \( E \) into \( \mathcal{P}(F) \). Then there exists an injection \( f \) of \( E \) into \( F \) such that \( f(x) \in A(x) \) for each \( x \in E \) if and only if for each subset \( H \) of \( E \), we have \( \text{Card} \{ \bigcup_{x \in H} A(x) \} \geq \text{Card}(H) \) (the method of proof is analogous to that of (a), with \( h = 0 \)).

(c) With the hypotheses of (b), let \( G \) be subset of \( F \). Then there exists an injection \( f \) of \( E \) into \( F \) such that \( f(x) \in A(x) \) for each \( x \in E \) and such that \( f(E) \supseteq G \) if and only if \( f \) satisfies the condition of (b) and for each subset \( L \) of \( G \) the cardinal of the set of all \( x \in E \) such that \( A(x) \cap L \neq \emptyset \) is \( \geq \text{Card}(L) \). (Let \( (a_1)_1 \leq \leq m \) be the sequence of distinct elements of \( G \), arranged in some order; let \( (b_j)_{p+1 \leq j \leq p+m} \) be the sequence of distinct elements of \( F \), arranged in some order; and let \( (c_k)_{p+m+1 \leq k \leq p+m+n} \) be the sequence of distinct elements of \( E \), arranged in some order. Consider the order relation on the set \([1, p + m + n]\) whose graph is the union of the diagonal and the set of pairs \((i, j)\) such that either

\[ 1 \leq i \leq p \text{ and } p + 1 \leq j \leq p + m + 1 \text{ and } a_i = b_j, \]

or

\[ 1 \leq i \leq p \text{ and } p + m + 1 \leq j \leq p + m + n \text{ and } a_i \in A(c_j), \]

or

\[ p + 1 \leq i \leq p + m \text{ and } p + m + 1 \leq j \leq p + m + n \text{ and } b_i \in A(c_j); \]

then apply Exercise 5.)

7. An element \( a \) of a lattice \( E \) is said to irreducible if the relation \( \sup(x, y) = a \) implies either \( x = a \) or \( y = a \).

(a) Show that in a finite lattice \( E \) every element \( a \) can be written as \( \sup(e_1, \ldots, e_k) \) where the \( e_i \) \((1 \leq i \leq n)\) are irreducible.

(b) Let \( E \) be a finite lattice and let \( J \) be the set of its irreducible elements. For each \( x \in E \) let \( S(x) \) be the set of all \( y \in J \) which are \( \leq x \). Show that the mapping \( x \to S(x) \) is an isomorphism of \( E \) onto a subset of \( \mathcal{P}(J) \), ordered by inclusion, and that \( S(\inf(x, y)) = S(x) \cap S(y) \).
§ 8. (a) Let $E$ be a distributive lattice ($\S$ 1, Exercise 16). If $a$ is irreducible in $E$ (Exercise 7), show that the relation $a \leq \sup(x, y)$ implies $a \leq x$ or $a \leq y$.

(b) Let $E$ be a finite distributive lattice and let $J$ be the set of its irreducible elements, ordered by the induced ordering. Show that the isomorphism $x \mapsto S(x)$ of $E$ onto a subset of $\mathcal{P}(J)$ defined in Exercise 7 (b) is such that $S(\sup(x, y)) = S(x) \cup S(y)$ Deduced that if $J^*$ is the ordered set obtained by endowing $J$ with the opposite ordering, then $E$ is isomorphic to the set $\mathcal{P}(J^*, I)$ of increasing mappings of $J^*$ into $I = [0, 1]$ ($\S$ 1, Exercise 6).

(c) With the hypothesis of (b), let $P$ be the set of elements of $J$ other than the least element of $E$. For each $x \in E$, let $y_1, \ldots, y_k$ be the distinct minimal elements of the interval $[x, \rightarrow]$ in $E$; for each index $i$, let $q_i$ be an element of $P$ such that $q_i \notin S(x)$ and $q \in S(y_i)$. Show that no two elements $q_1, \ldots, q_k$ are comparable.

(d) Conversely, let $q_1, \ldots, q_k$ be $k$ elements of $P$, no two of which are comparable. Let $u = \sup(q_1, \ldots, q_k)$ and let

$$v_i = \sup_{1 \leq j \leq k, j \neq i} (q_j) \quad (1 \leq i \leq k).$$

Show that $v_i < u$ for $1 \leq i \leq k$. Let $x = \inf(v_1, \ldots, v_k)$ and let

$$y_i = \inf_{1 \leq j \leq k, j \neq i} (v_j)$$

Show that $x < y_i$ for each index $i$, and deduce that the interval $[x, \rightarrow]$ has at least $k$ distinct minimal elements.

§ 9. A subset $A$ of a lattice $E$ is said to be a sublattice if for each pair $(x, y)$ of elements of $A$, $\sup_E(x, y)$ and $\inf_E(x, y)$ belong to $A$.

(a) Let $(C_i)_{1 \leq i \leq n}$ be a finite family of totally ordered sets and let $E = \prod_{i=1}^{n} C_i$ be their product. Let $A$ be a sublattice of $E$. Show that $A$ cannot have more than $n$ irreducible elements (Exercise 7) no two of which are comparable (The proof is by reductio ad absurdum. Suppose that there exist $r > n$ irreducible elements $a_1, \ldots, a_n$ in $A$, no two of which are comparable. Consider the elements $u = \sup(a_1, \ldots, a_n)$ and

$$v_j = \inf_{1 \leq s \leq r, j \neq i} (a_j)$$

of $A$. By projecting onto the factors, show that $u = v_i$ for some index $i$, and hence that two of the $a_i$ are comparable).

(b) Conversely, let $F$ be a finite distributive lattice, let $P$ be the set of irreducible elements of $F$ other than the least element of $F$, and suppose that $n$ is the greatest number of elements in a free subset of $P$ ($\S$ 1, Exercise 5). Show that $F$ is isomorphic to a sublattice of a product of $n$ totally ordered sets (Apply Exercise 5, which shows that $P$ is the union of $n$ totally ordered sets $P_i$ with no elements in common. Let $C_i$ be the totally ordered set obtained by adjoining a least element to $P_i$ ($1 \leq i \leq n$). With each $x \in F$ associate the family $(x_i)_{1 \leq i \leq n}$ where $x_i$ is the least upper bound in $C_i$ of the sets of elements of $P_i$ which are $\leq x$.)

§ 10. (a) An ordered set $E$ is isomorphic to a subset of a product of $n$ totally ordered sets if and only if the graph of the ordering on $E$ is the intersection of the graphs on $n$ total orderings on $E$. (To show that the condition is necessary, show that if $F = \prod_{i=1}^{n} F_i$ is a product of $n$ totally ordered sets, then

$$\prod_{i=1}^{n} \{x_i \in F_i \mid x_i \leq y_i \}$$

is a sublattice of $F$.) Conversely, let $A$ be a sublattice of $E$. Show that $A$ cannot have more than $n$ elements.

RR n° 7150
ordered sets, the graph of the product ordering on \( F \) is the intersection of \( n \) graphs of lexicographic orderings on \( F \).)

(b) An ordered set \( E \) is isomorphic to a subset of the product of two totally ordered sets if and only if the ordering \( \Gamma \) on \( E \) is such that there exists another ordering \( \Gamma' \) on \( E \) with the property that any two distinct elements of \( E \) are comparable with respect to exactly one of the orderings \( \Gamma \) and \( \Gamma' \).

(c) Let \( A \) be a finite set of \( n \) elements. Let \( E \) be the subset of \( \mathcal{F}(A) \) consisting of all subsets \( \{x\} \) and \( A - \{x\} \) as \( x \) runs through \( A \). Show that \( n \) is the smallest integer \( m \) such that \( E \), ordered by inclusion, is isomorphic to a subset of a product of \( m \) totally ordered sets (use (a)).

¶ 11. Let \( A \) be a set and let \( \mathcal{R} \) be a subset of the set \( \mathcal{F}(A) \) of finite subsets of \( A \). \( \mathcal{R} \) is set to be mobile if it satisfies the following condition:

(MO) If \( X, Y \) are two distinct elements of \( \mathcal{R} \) and if \( z \in X \cap Y \), then there exists \( Z \subset X \cap Y \) belonging to \( \mathcal{R} \) such that \( z \notin Z \).

A subset \( P \) of \( A \) is then said to be pure if it contains no set belonging to \( \mathcal{R} \).

(a) Show that every pure subset of \( A \) is contained in a maximal pure subset of \( A \).

(b) Let \( M \) be a maximal pure subset of \( A \). Show that for each \( x \in \complement M \) there exists a unique \( \text{finite subset } E_M(x) \text{ of } M \text{ such that } E_M(x) \cup \{x\} \in \mathcal{R} \). Moreover, if \( y \in E_M(x) \), the set \( (M \cup \{x\}) - \{y\} \) is a maximal pure subset of \( A \).

(c) Let \( M, N \) be two maximal pure subsets of \( A \), such that \( N \cap \complement M \) is finite. Show that \( \text{Card}(M) = \text{Card}(N) \). (Proof by induction on the cardinal of \( N \cap \complement M \), using (b).)

(d) Let \( M, N \) be two maximal pure subsets of \( A \), and put \( N' = N \cap \complement M \), \( M' = M \cap \complement N \). Show that \( M' \subseteq \bigcap_{x \in N'} E_M(x) \). " Deduce that \( \text{Card}(M) = \text{Card}(N) \) (by virtue of (c), we are reduced to the case where \( N' \) and \( M' \) are infinite; show then that \( \text{Card}(M') \leq \text{Card}(N') \)). "

9.5 Section 5

1. Prove the formula

\[
\sum_{k=q+1}^{n-p+q+1} \binom{n-k}{p-1} \binom{k-1}{q} = \binom{n}{p},
\]

where \( p \leq n \) and \( q < p \) (generalize the argument of no. 8, Corollary to Proposition 14).

2. If \( n \geq 1 \), prove the relation

\[
\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^n \binom{n}{n} = 0
\]

(Define a one-to-one correspondence between the set of subsets of \([1, n]\) which have an even number of elements, and the set of subsets of \([1, n]\) which have an odd number of elements. Distinguish between the cases \( n \) even and \( n \) odd.)

3. Prove the relations

\[
\binom{n}{p} + \binom{n-1}{p-1} + \binom{n-2}{p-2} + \ldots + \binom{n}{p} = 2^p \binom{n}{p},
\]
5. \( \sum_{i=1}^{k} u(x) \leq n \)

onto the set of strictly increasing mappings of \([1, h]\) into \([1, n+h]\).

4. Prove Proposition 15 of no. 8 by defining a bijection of the set of mappings \( u \) of \([1, h]\) into \([0, n]\) such that

\[
\left( \begin{array}{c} n \\ 0 \end{array} \right) \left( \begin{array}{c} n \\ p \end{array} \right) - \left( \begin{array}{c} n \\ 1 \end{array} \right) \left( \begin{array}{c} n-1 \\ p-1 \end{array} \right) + \left( \begin{array}{c} n \\ 2 \end{array} \right) \left( \begin{array}{c} n-2 \\ p-2 \end{array} \right) - \cdots + (-1)^{h} \left( \begin{array}{c} n \\ p \end{array} \right) \left( \begin{array}{c} n-p \\ 0 \end{array} \right) = 0.
\]

(Consider the subsets of \( p \) elements of \([1, n]\) which contain a given subset of \( k \) elements \((0 \leq k \leq p)\), and use Exercise 2 for the second formula.)

5. * (a) Let \( E \) be a distributive lattice and let \( f \) be a mapping of \( E \) into a commutative semi-group \( M \) (written additively) such that

\( f(x) + f(y) = f(\sup(x,y)) + f(\inf(x,y)) \)

for all \( x, y \) in \( E \). Show that for each finite subset \( I \) of \( E \), we have

\[
f(\sup(I)) + \sum_{2n \leq \text{Card}(I)} \left( \sum_{H \subseteq I, \text{Card}(H)=2n} f(\inf(H)) \right) = \sum_{2n+1 \leq \text{Card}(I)} \left( \sum_{H \subseteq I, \text{Card}(H)=2n+1} f(\inf(H)) \right)
\]

(By induction on \( \text{Card}(I) \).)

(b) In particular let \( A \) be a set, let \( (B_i)_{i \in I} \) be a finite family of finite subsets of \( A \) and let \( B \) be the union of the \( B_i \). For each subset \( H \) of \( I \), put \( B_H = \bigcap_{i \in H} B_i \). Show that

\[
\text{Card}(B) + \sum_{2n \leq \text{Card}(I)} \left( \sum_{\text{Card}(H)=2n} \text{Card}(B_H) \right) = \sum_{2n+1 \leq \text{Card}(I)} \left( \sum_{\text{Card}(H)=2n+1} \text{Card}(B_H) \right).
\]

6. Prove the formula

\[
\left( \begin{array}{c} n+h \\ h \end{array} \right) = 1 + \frac{h}{1} \left( \begin{array}{c} n+h-1 \\ h \end{array} \right) - \frac{h}{2} \left( \begin{array}{c} n+h-2 \\ h \end{array} \right) + \cdots + (-1)^{h} \left( \begin{array}{c} n \\ h \end{array} \right) \left( \begin{array}{c} n \\ h \end{array} \right).
\]

(If \( F \) denotes the set of mappings \( u \) of \([1, h]\) into \([0, n]\) such that \( \sum_{i=1}^{h} u(x) \leq n \), consider for each subset \( H \) of \([1, h]\) the set of all \( u \in F \) such that \( u(x) \geq 1 \) for each \( x \in H \), and use Exercise 5.)

7. (a) Let \( S_{n,p} \) denote the number of mappings of \([1, n]\) \textit{onto} \([1, p]\). Prove that

\( S_{n,p} = p^n - \left( \frac{p}{1} \right)^n + \left( \frac{p}{2} \right)(p-1)^n - \cdots + (-1)^{p-1} \left( \frac{p}{p-1} \right) \).

(Note that \( p^n = S_{n,p} = \left( \frac{p}{1} \right)^n + \left( \frac{p}{2} \right)^n + \cdots + \left( \frac{p}{p-1} \right) \) and use Exercise 3.)

(b) Prove that \( S_{n,p} = p(S_{n-1,p} + S_{n-1,p-1}) \) (method of no. 8, Proposition 13).

(c) Prove that

\[
S_{n+1,n} = \frac{n}{2} (n+1)! \quad \text{and} \quad S_{n+2,n} = \frac{n(3n+1)}{24} (n+2)!
\]

(consider the elements \( r \) of \([1, n]\) whose inverse image consists of more than one element).

(d) If \( P_{n,p} \) is the number of partitions into \( p \) parts of a set of \( n \) elements, show that \( S_{n,p} = p! P_{n,p} \).

RR n° 7150
8. Let \( p_n \) be the number of permutations of a set \( E \) with \( n \) elements such that \( u(x) \neq x \) for all \( x \in E \). Show that
\[
p_n = n! - \left( \begin{array}{c} n \ \\
1 \end{array} \right) (n-1)! + \left( \begin{array}{c} n \ \\
2 \end{array} \right) (n-2)! - \cdots + (-1)^n \]
* and hence that \( p_n \sim n!/e \) as \( n \to \infty \), (same method as in Exercise 7 (a)).

9. (a) Let \( E \) be a set with \( qn \) elements. Show that the number of partitions of \( E \) into \( n \) subsets each of \( q \) elements is equal to
\[
(qn)!/(n!(qn)^n).\]

(b) Suppose that \( E = [1,qn] \). Show that the number of partitions of \( E \) into \( n \) subsets each of \( q \) elements, no one of which is an interval is equal to
\[
\frac{(qn)! - (qn - q + 1)!}{n!(qn)!} + \frac{(qn - 2q + 2)!}{2!(n - 2)!(qn - 2)!} - \cdots + (-1)^n \]
(same method as in Exercises 7 and 8).

10. Let \( q_{n,k} \) be the number of strictly increasing mappings \( u \) of \([1,k]\) into \([1,n]\) such that for each even (resp. odd) \( x \), \( u(x) \) is even (resp. odd). Show that \( q_{n,k} = q_{n-1,k-1} + q_{n-2,k} \) and deduce that
\[
q_{n,k} = \binom{n+k}{2k}.\]

§11. Let \( E \) be a set with \( n \) elements and let \( S \) be a set of signs such that \( S \) is the disjoint union of \( E \) and a set consisting of a single element \( f \). Suppose that \( f \) has weight 2 and that each element of \( E \) has weight 0 (Chapter I, Appendix Exercise 3).

(a) Let \( M \) be the set of significant words in \( L_0(S) \) which contain each element of \( E \) exactly once. Show that if \( u_n \) is the number of elements in \( M \), then \( u_{n+1} = (4n-2)u_n \), and deduce that
\[
u_n = 2.6\ldots(4n-6) \quad (n \geq 2)\]
(This is the number of products of \( n \) different terms with respect to a non-associative law of composition).

(b) Let \( x_i \) be the \( i \)th of the elements of \( E \) which appear in a word of \( M \). Show that the number \( v_n \) of words of \( M \), for which the sequence \( x_i \) is given, is equal to \( \binom{2n-2}{n-1}/n \) and satisfies the relation
\[
v_{n+1} = v_1v_n + v_2v_{n-1} + \cdots + v_{n-1}v_2 + v_nv_1.\]

§12. (a) Let \( p \) and \( q \) be two integers \( \geq 1 \), let \( n = 2p + q \), let \( E \) be a set with \( n \) elements and let \( N = \binom{n}{p} = \binom{n}{p+q} \). Let \((X_i)_{1 \leq i \leq n} \) (resp \((Y_i)_{1 \leq i \leq n} \)) be the sequence of all subsets of \( E \) which have \( p \) (resp \( p+q \)) elements arranged in a certain order. Show that there exists a bijection \( \phi \) of \([1,n]\) onto itself such that \( X_{\phi(i)} \subset Y_i \) for all \( i \). (The method is analogous to that of Exercise 6 of §4: observe that for each \( r \leq N \) the number of sets \( Y_j \) which contain at least one of \( X_1, \ldots, X_r \) is \( \geq r \)).

(b) Let \( h, k \) be two integers \( \geq 1 \), let \( n \) be an integer such that \( 2h + k < n \), let \( E \) be a set with \( n \) elements and let \((X_i)_{1 \leq i \leq n} \) be a sequence of distinct subsets of \( E \), each having \( h \) elements. Show that there exists a sequence \((Y_j)_{1 \leq j \leq n} \) of distinct subsets of \( E \), each having \( h + k \) elements, such that each \( Y_j \) contains at least one \( X_i \) and each \( X_i \) is contained in at least one \( Y_j \) (by induction on \( n \), using (a)).
¶ 13. Let $E$ be set with $2m$ elements, let $q$ be an integer $< m$, and let $\mathcal{F}$ be the set of all 
subsets $\mathcal{G}$ of $\mathcal{P}(E)$ with the following property: if $X$ and $Y$ are two distinct elements of $\mathcal{G}$ such 
that $X \subseteq Y$, then $Y - X$ has at most $2q$ elements.

(a) Let $\mathcal{M} = (A_i)_{1 \leq i \leq p}$ be an element of $\mathcal{F}$ such that $p = \card(\mathcal{M})$ is as large as possible. 
Show that $m - q \leq \card(A_i) \leq m + q$ for $1 \leq i \leq p$ (Argue by contradiction. Suppose, for 
e.g., that there exists indices $i$ such that $\card(A_i) < m - q$ and consider those of the $A_i$ 
for which $\card(A_i)$ has the least possible value $m - q - s$ (where $s \geq 1$). Let $A_1, \ldots, A_r$, say, these 
sets. Let $\mathcal{G}$ be the set of subsets of $E$ each of which is the union of some $A_i$ for $1 \leq i \leq r$ and 
a subset of $2q + 1$ elements contained in $E - A_i$. Show that $\mathcal{G}$ contains at least $r + 1$ elements (cf. 
Exercise 12), and that if $B_1, \ldots, B_{r+1}$ are $r + 1$ distinct elements of $\mathcal{G}$, the set whose elements are 
$B_j$ $(1 \leq j \leq r + 1)$ and $A_i$ $(r + 1 \leq i \leq p)$ belongs to $\mathcal{F}$, contrary to the hypothesis.)

(b) Deduce from (a) that the number of elements $p$ of each $\mathcal{G} \in \mathcal{F}$ satisfies the inequality 
$$p \leq \sum_{k=0}^{2q} \left( \frac{2m}{m-q+k} \right).$$

(c) Establish results analogous to those of (a) and (b) when $2m$ or $2q$ is replaced by an 
uneven number.

¶ 14. Let $E$ be a finite set with $n$ elements, let $(a_j)_{1 \leq j \leq n}$ be the sequence of elements of $E$ 
arranged in some order, and let $(A_i)_{1 \leq i \leq m}$ be a sequence of subsets of $E$.

(a) For each index $j$, let $k_j$ be the number of indices $i$ such that $a_j \in A_i$, and let $S_i = \card(A_i)$. Show that 
$$\sum_{j=1}^{n} k_j = \sum_{i=1}^{m} S_i.$$ 

(b) Suppose that for each subset $\{x, y\}$ of two elements of $E$, there exists exactly one index 
i such that $x$ and $y$ are contained in $A_i$. Show that, if $a_j \notin A_i$, then $S_i \leq k_j$.

(c) With the hypotheses of (b), show that $m \geq n$ (Let $k_n$ be the least of the numbers $k_j$. 
Show that we may suppose that, whenever $i \leq k_n, j \leq k_n, and i \neq j$, we have $a_j \notin A_i$ and 
a_n \notin A_j for all $j \geq k_n$.)

(d) With the hypotheses of (b), show that $m = n$ if and only if one of the following two 
alternatives is true: (i) $A_1 = \{a_1, a_2, \ldots, a_{n-1}\}, A_i = \{a_{i-1}, a_i\}$ for $i = 2, \ldots, n$; (ii) $n = k(k-1) + 1$; 
each $A_i$ has $k$ elements, and each element of $E$ belongs to exactly $k$ set $A_i$.

¶ 15. Let $E$ be a finite set, let $\EuScript{L}$ and $\EuScript{C}$ be two disjoint non-empty subsets of $\mathcal{P}(E)$, and let $\lambda$, 
$h, k, l$ be four integers $\geq 1$ with the following properties: (i) for each $A \in \EuScript{L}$ and each $B \in \EuScript{C}$, 
$\card(A \cap B) \geq \lambda$; (ii) for each $A \in \EuScript{L}$, $\card(A) \geq h$; (iii) for each $B \in \EuScript{C}$, $\card(B) \leq k$; (iv) for each 
$x \in E$ the number of elements of $\EuScript{L} \cup \EuScript{C}$ which contain $x$ is exactly $l$. Show that $\card(\EuScript{E}) \leq hlk/\lambda$. 
(Let $(a_i)_{1 \leq i \leq n}$ be the sequence of distinct elements of $E$ arranged in some order, and for each 
i let $r_i$ be the number of elements of $\EuScript{L}$ to which $a_i$ belongs. Show that, if $\card(\EuScript{L}) = s$ and 
$\card(\EuScript{C}) = t$, then we have 
$$\sum_{i=1}^{n} r_i \leq sh, \quad \sum_{i=1}^{n} (l-r_i) \leq tk, \quad \sum_{i=1}^{n} r_i(l-r_i) \geq \lambda st.$$ 
For $\card(\EuScript{E})$ to be equal to $hlk/\lambda$ it is necessary and sufficient that for each $A \in \EuScript{L}$ and each 
$B \in \EuScript{C}$ we have $\card(A) = h$, $\card(B) = k$, $\card(A \cap B) = \lambda$ and that there exists an $r \leq l$ such that 
for each $x \in E$ the number of elements of $\EuScript{L}$ to which $x$ belongs is equal to $r$. 

RR n° 7150
16. Let $E$ be a finite set with $n$ elements, let $\mathcal{D}$ be a non-empty subset of $\mathcal{P}(E)$, and let $\lambda$, $k$, $l$ be three integers $\geq 1$ with the following properties: (i) if $A$ and $B$ are distinct elements of $\mathcal{D}$, then $\text{Card}(A \cap B) = \lambda$; (ii) for each $A \in \mathcal{D}$, $\text{card}(A) \leq k$; (iii) for each $x \in E$ the number of elements of $\mathcal{D}$ to which $x$ belongs is equal to $l$. Show that

$$n(\lambda - 1) \leq k(k - 1)$$

and that if $n(\lambda - 1) = k(k - 1)$ then $\lambda = k$ and $\text{Card}(\mathcal{D}) = n$. (Given $a \in E$, let $\mathcal{L}$ be the set of all $A - \{a\}$ where $A \in \mathcal{D}$ and $a \in A$, and let $\mathcal{C}$ be the set of all $A \in \mathcal{D}$ such that $a \not\in A$. Apply the results of Exercise 15 to $\mathcal{L}$ and $\mathcal{C}$.

§ 17. Let $i$, $h$, $k$ be three integers such that $i \geq 1$, $h \geq i$, $k \geq i$. Show that there exists an integer $m_1(h, k)$ with the following properties: for each finite set $E$ with at least $m_1(h, k)$ elements, and each partition $(\mathcal{X}, \mathcal{Y})$ of the set $\mathcal{P}_i(E)$ of subsets of $i$ elements of $E$, it is impossible that every subset of $h$ elements of $E$ contains a subset $X \in \mathcal{X}$ and that every subset of $k$ elements of $E$ contains a subset $Y \in \mathcal{Y}$; in other words, if every subset of $h$ elements of $E$ contains some $X \in \mathcal{X}$ there exists a subset $A$ of $k$ elements of $E$ such that every subset of $i$ elements of $A$ belongs to $\mathcal{X}$ (Proof by induction. Show that we may take $m_1(h, k) = h + k - 1$, $m_1(i, k) = k$ and $m_1(h, i) = h$ and finally $m_1(h, k) = m_{i-1}(m_1(h-1, k), m_1(h, k-1)) + 1$. If $E$ is a set with $m_1(h, k)$ elements if $a \in E$ and $E' = E - \{a\}$, show that if the proposition were false, then every subset of $m_1(h-1, k)$ elements of $E'$ would contain a subset $X'$ of $i - 1$ elements such that $X' \cup \{a\} \in \mathcal{X}$, and that every subset of $m_1(h, k-1)$ elements of $E'$ would contain a subset $Y'$ of $i - 1$ elements such that $Y' \cup \{a\} \in \mathcal{Y}$).

18. (a) Let $E$ be a finite ordered set with $p$ elements. If $m$, $n$ are two integers such that $mn < p$, show that $E$ has either a totally ordered subset of $m$ elements or else a free subset (§ 1, Exercise 5) of $n$ elements (use § 4, Exercise 5).

(b) Let $h$, $k$ be two integers $\geq 1$ and let $r(h, k) = (h - 1)(k - 1) + 1$. Let $I$ be a totally ordered set with at least $r(h, k)$ elements. Show that, for each finite sequence $(x_i)_{i \in I}$ of elements of a totally ordered set $E$, there exists either a subset $H$ of $h$ elements of $I$ such that the sequence $(x_i)_{i \in H}$ is increasing, or else a subset $K$ of $k$ elements of $I$ such that the sequence $(x_i)_{i \in K}$ is decreasing. (Use (a) applied to $I \times E$.)

9.6 Section 6.

1. A set $E$ is infinite if and only if each mapping $f$ of $E$ into $E$ there exists a non-empty set $S$ of $E$ such that $S \neq E$ and $f(S) \subset S$.

Assume $E$ non-empty, and let $f : E \rightarrow E$. Fix $x \in E$, and define by induction $g(n + 1) = f(g(n))$, with $g(0) = x$. Let $G$ be the range (or target) of $g$ and $S = f(G)$. Then $G$ and $S$ are non-empty and stable by $f$. If $x \not\in S$, then $S \neq E$. Otherwise, $x = f(g(m)) = g(m + 1)$. Let $n = m + 1$. Then $x = g(n)$ and by induction on $i$, $g(i) = g(i + n)$. By induction on $k$, we have $g(i) = g(i + kn)$. By Euclidean division, every element of $S$ has the form $g(i)$ for $i < n$. This show that $S$ is finite. If $E$ is infinite, we deduce $S \neq E$.

Lemma Exercise_6_1: forall E, infinite_set E =
  (forall f, is_function f -> source f = E -> target f = E ->
   exists F, sub F E & nonempty F & F <> E & sub (image_by_fun f F) F).
Proof. ir. app iff_eq. ir.

INRIA
nin (emptyset_dichot E). rwi H3 H. red in H. red in H. ee. elim H4.
app is_finite0. nin H3.
cp (integer_induction_stable H3 H0 H1 H2).
cp (induction_defined_pr (fun n : Set => W n f) y).
set (g:=induction_defined (fun n : Set => W n f) y) in *. simpl in H5. ee.
set (F:=target g). nin H6.
assert (inc y F). uf F. wr H7. app inc_w_target. rw H5. fprops.
assert (sub (image_by_fun f F) F). uf F. red. ir. ufi image_by_fun H11.
awi H5 H11. rw H5. wr H8. app inc_w_target. rw H5. fprops. am. fprops.

set (G:=image_by_fun f F).
exists G. ee. apply sub_trans with F. app H11. app H4. uf G.
exists (W y f). uf image_by_fun. aw. exists y. split. am. red.
app defined_lem. rww H1. fprops. red. ee. ir. wri H12 H3. ufi G H3.

set (k:=succ x0) in *. assert (inc k Bnat). uf k. rwi H5 H3. fprops.
assert (forall i, inc i Bnat -> W i g = W (card_plus i k) g).
app cardinal_c_induction_v. rw zero_unit_suml. fprops. ir. rw H8. rw H19.
assert (card_plus (succ n) k = succ (card_plus n k)). uf succ.
rw (card_plus_commutative n card_one).
wr card_plus_associative. app card_plus_commutative. rw H20. rw H8. fprops.
am. assert (forall i, inc i Bnat -> forall j, inc j Bnat ->
W i g = W (card_plus i (card_mult j k) g)). intros i H19.
ap cardinal_c_induction_v. rw card_mult_commutative. rw zero_prod_absorbing.
rw zero_unit_summr. fprops. ir. rw card_mult_commutative.
rw mult_via_plus. rw card_plus_associative. wr H18. rw (card_mult_commutative.
fprops. fprops. assert (forall z, inc z E -> exists m, cardinal_lt m k & z = W m g). ir.
assert (inc (succ x2) Bnat). rwi H5 H20. fprops. assert (inc k Bnat).
uf k. rwi H5 H3. fprops. assert (k <> card_zero). uf k.
cp (succ_positive x0). red in H25. ee. intuition.
rw H28. rw card_plus_commutative. exists x4. split. am.
rww card_mult_commutative. wr H19. tv. am. am. wr H5. fprops. fprops.
assert (sub E (image_by_fun g (interval_co_0a k)))). red. ir.
assert (inc k Bnat). uf k. rwi H5 H3. fprops. nin (H20 _ H21). ee.
ap (le_int_is_int H22 H23). uf image_by_fun. aw.
exists x2. ee. rw interval_co_0a_pr2.
red. rw H24. app defined_lem. rww H5. fprops.
cp (cardinal_le8 H21). rwi cardinal_le3 H22.
assert (is_finite_set (interval_co_0a k)). uf interval_co_0a.
app finite_set_interval_co.
assert (sub (interval_co_0a k) (source g)). rw H5. uf interval_co_0a.
uf interval_co. rw substrate_Bnat_order. ap Z_sub.
cp (finite_image_by H6 H24 H23). red in H25.
set (w:=cardinal (image_by_fun g (interval_co_0a k)))). in *.
cp (le_int_is_int H25 H22). red in H. red in H. ee. elim H27. am. wr H5.
fprops. fprops. uf image_by_fun. red. ir. awi H12. nin H12. nin H12.

RR n° 7150
Converse. We assume that for every function \( f : E \rightarrow E \) there is a non-trivial subset of \( E \) invariant by \( f \). This implies \( E \) non-empty. Assume \( E \) finite. There is a bijection \( T : [0, n] \rightarrow E \), where \( n \neq 0 \). Let \( f \) be the function \( i \mapsto i + 1 \) (modulo \( n \)). This induces a function \( g \) on \( E \), so that there is a set \( S \) such that \( g(S) \subset S \). Since this set is not empty, it contains an element \( T(i) \).

By induction it contains all \( T(i + j \mod n) \), thus all elements of \( E \).

ir. red. split. fprops. red. ir. set \( (n := \text{cardinal } E) \).
assert (inc n Bnat). rww inc_Bnat.
assert (equi potent E (interval_co_0a n)). wr cardinal_equi potent.
rw cardinal_interval_co_0a1. tv. am. red in H2. nin H2. ee.
set \( (y := \text{inverse_fun x}) \).
assert (nonempty E). set \( (f := \text{identity_fun } E) \).
assert (is_function f). uf f. app function_identity. assert (source f = E).
nin H9. exists y0. app H8. assert \((n \nmid \text{card_zero})\). red. ee. ir. ufi n H6.
elim (cardinal_nonemptyset1 H5). am.
set \( (f := \text{fun } i \mapsto \text{card_rem } (\text{succ } i) n) \).
assert (Ha: forall i, inc i Bnat \rightarrow inc (\text{card_rem } i n) (\text{interval_co_0a n}))
.ir. rw interval_co_0a_pr2. cp (Bnat_division H7 H1 H6).
ee. red in H10; ee; am. am.
assert (Hb: sub (\text{interval_co_0a n}) \text{Bnat}). uf interval_co_0a.
uw interval_co. rw subtrate_Bnat_order. app Z_sub.
assert (forall i, inc i (\text{interval_co_0a n}) \rightarrow inc (f i) (\text{interval_co_0a n})).
ir. uf f. app Ha. cp (Hb _ H7). fprops.
cp (inverse_bij_is_bij H2). cp (bij_is_function H2).
cp (bij_is_function H8).
set \( (\text{g := fun } u \mapsto W (f (W u x)) y) \).
assert (transf_axioms g E E). red. ir. uf g. uf y.
assert (E = \text{target (inverse_fun x)}) \text{. rw target_inverse. sy; am. rw H12.}
rw H3.
set \( (g1 := BL g E E) \). assert (is_function g1). uf g1. app af_function.
assert (source g1 = E). tv. assert (target g1 = E). tv.
nin (H _ H12 H13 H14). nin H15. nin H16. nin H17. nin H16.
set \( (i := W y0 x) \). assert (inc i Bnat). assert (inc i (target x)).
uf i. app inc_W_target. rww H3. app H15. app Hb. wr H4.
assert (inc (W i y) x0). uf i. uf y.
set \( (xi := W y0 x) \). assert (inc y0 (source x)). rw H3. app H15.
assert (xi = W y0 x). tv. cp (W_inverse2 H2 H20 H21). wr H22.
assert (forall j, inc j Bnat \rightarrow inc (W (\text{card_rem } (\text{card_plus } i j) n) y) x0).
app cardinal_c_induction_y. rw zero_unit_sumr.
assert (\text{card_rem } i n = i). cp (Bnat_division H19 H1 H6). ee.
assert (\text{division_prop } i \text{ in } \text{card_zero } i). red. split. rw zero_prod_absorbing.
rw zero_unit_suml. tv. fprops. assert (inc i (target x)).
uf i. app inc_W_target. rww H3. app H15. rwi H4 H24.
riw interval_co_0a_pr2 H24. ee; am. am.
nin (division_unique H19 H1 H22 H21 (inc0_Bnat) H19 H6 H23 H24). am.
rw H21. am. fprops. ir.
set \( (u := \text{card_rem } (\text{card_plus } i n0) n) \) in *.
assert (inc (W (W u y) g1) x0). app H18. uf image_by_fun. aw.
exists (W u y). split. am. red. app defined_lem. rw H13.
assert (E = \text{target y}). uf y. rw target_inverse. sy; am. rw H23.
app inc_W_target. uf y. rw source_inverse. rw H4. uf u. app Ha. fprops.
fprops. ufi g1 H23. rwi W_af_function H23. ufi g H23.

assert (W (W u y) x = u). sy. app W_inverse. rw H4. uf u. app Ha. fprops.

rwi H24 H23. ufi f H23.

assert (card_rem (succ u) n = card_rem (card_plus i (succ n0)) n).
uf u. assert (inc (card_plus i n0) Bnat). fprops.

cp (Bnat_division H25 H1 H6). ee. nin H28.

set (q0:= card_quo (card_plus i n0) n) in H28.

set (r0:= card_rem (card_plus i n0) n) in *, uf succ.

rw card_plus_associative. rw H28. wr card_plus_associative.

set (r1:= card_plus r0 card_one). set (r2:= card_plus (card_mult n q0) r1).
assert (inc r1 Bnat). uf r1. fprops. assert (inc r2 Bnat). uf r2. fprops.

cp (Bnat_division H30 H1 H6). cp (Bnat_division H31 H1 H6). ee.

nin H37.

assert (r2= card_plus (card_mult n q0) r1). tv. rwi H37 H39.

rwi card_plus_associative H39. rwi cardinal_distrib_prod_sum3 H39.

set (q2:= (card_plus q0 (card_quo r1 n)))

assert (division_prop r2 n q2 (card_rem r1 n)). red. split. am. am.

assert (inc q2 Bnat). uf q2. fprops.

nin (division_unique H31 H1 H41 H32 H34 H33 H6 H40 H35). am. wr H25. am.

am. app H15.

elim H17. app extensionality. red. ir. assert (E = target y). uf y.

rw target_inverse. sy; am. rwi H24 H22. red in H8. ee. fold y in H24.


rwi source_inverse H25. rwi H4 H25.

assert (inc i (target x)). uf i. app inc_W_target. rw H3. app H15.

rwi H4 H27. rwi interval_co_0a_pr2 H27.

set (j:= card_sub n i). nin H27. cp (card_sub_pr H1 H19 H27). fold j in H29.

assert (inc j Bnat). uf j. fprops.

set (k:= card_plus j x2). assert (inc k Bnat). uf k. fprops.

cp (H21 _ H31). assert (card_rem (card_plus i k) n = x2).

assert (division_prop (card_plus i k) n card_one x2). red.

rw one_unit_prodr. split. uf k. rw card_plus_associative. rwi H29.

rwi interval_co_0a_pr2 H25. ee; am. am. fprops.

assert (inc (card_plus i k) Bnat). fprops.

cp (Bnat_division H34 H1 H6). ee.

cp (division_unique H34 H1 (incl1_Bnat) (Hb _ H25) H36 H35 H6 H33 H37).

ee. sy; am. rwi H33 H32. am. am.

Qed.

2. Show that, if $a$, $b$, $c$ and $d$ are four cardinals such that $a < c$ and $b < d$ then $a + b < c + d$ and $ab < cd$. (cf. Exercise 21 (c)).

We first assume $c \leq d$. If $d$ is finite, all quantities are finite and the result is obvious.

Lemma exercice6_2: forall a b c d, cardinal_lt a c \rightarrow
cardinal_lt b d \rightarrow

(cardinal_lt (card_plus a b) (card_plus c d) &
cardinal_lt (card_mult a b) (card_mult c d)).

Proof. assert (forall a b c d, cardinal_le c d \rightarrow cardinal_lt a c \rightarrow
cardinal_lt b d \rightarrow

(cardinal_lt (card_plus a b) (card_plus c d) &
cardinal_lt (card_mult a b) (card_mult c d))).
We have now $c + d = cd = d$. Such a formula holds if one of $a$ or $b$ is infinite (the result is trivial if none is infinite). Note that if one of the cardinals is zero, so is the product, thus is $< 0$.

Here all cardinals are infinite. In particular, they are non-zero. We have $a + b = ab = a'$ where $a' < 0$ is the greatest of the two cardinals.
3. If $E$ is an infinite set, the subsets of $E$ which are equipotent to $E$ is equipotent to $\mathcal{P}(E)$ (use Proposition 3 of no. 4).

We know that $E$ is equipotent to $E_1 \cup E_2$, where the union is disjoint and both sets are equipotent to $E$ (this is not the hint given by Bourbaki). Let $f$ be a bijection $E_1 \cup E_2 \rightarrow E$. We may assume $E_1 = E \times \{\alpha\}$. For each subset $X$ of $E$, let $\bar{X}$ be $X$ as a subset of $E_1$ (i.e., $\bar{X} = X \times \{\alpha\}$), and $g(X) = f(\bar{X} \cup E_2)$. This a subset of $E$, and its cardinal is at least the cardinal of $f(E_2)$, which is the cardinal of $E$, so that $g(X)$ is equipotent to $E$.

Lemma Exercise6_3: forall $E$, infinite_set $E$ ->

\begin{align*}
&\text{equipotent (powerset E) (Zo (powerset E) (fun z => equipotent z E))}.
\end{align*}

Proof. ir. set (Qo:= Zo (powerset E) (fun z : Set => equipotent z E)).

assert (sub Qo (powerset E)). uf Qo. app Z_sub.

cp (cardinal_le8 H0). rwi cardinal_le3 H1.

set (n:= cardinal E). assert (card_plus n n = n).

assert (cardinal_le n n). uf n. fprops. red in H. fold n in H.

ap (sum2_infinite H2 H).

set (E1:= product E (singleton TPa)). set (E2:= product E (singleton TPb)).

assert (equipotent E1 n). eqtrans E. eqsym. uf E1. fprops. uf n. fprops.


assert (disjoint E1 E2). uf E1; uf E2. app disjoint_union2_pr. fprops.


set (f:= fun X => image_by_fun x (union2 (product X (singleton TPa)) E2)).

assert (forall X, sub X E -> sub (f X) E). red. ir. ufi f H10.

assert (is_function x). app bij_is_function.


app (inc_pr2graph_target H11 H12). fprops.

assert (forall X, sub X E -> equipotent (f X) E). ir.

cp (H9 _ H10). cp (cardinal_le8 H11). rwi cardinal_le3 H12.

set (b:= image_by_fun x E2). assert (sub E2 (source x)). rw H7.

red. ir. app union2_second. cp (equipotent_restriction H13 H6).

assert (sub (image_by_fun x E2) (f X)). uf f. uf image_by_fun.

app image_by_increasing. cp (bij_is_function H6). fprops. red. ir.

app union2_second. cp (cardinal_le8 H15). rwi cardinal_le3 H16.

wri cardinal_equipotent H14. wri H14 H16.

assert (cardinal E2 = cardinal E). aw. eqtrans n. am. uf n. fprops.

rwi H17 H16. wr cardinal_equipotent. app cardinal_antisymmetry1.

assert (transf_axioms f (powerset E) Qo). red. ir.


set (F:= BL f (powerset E) Qo).

assert (injective F). uf F. app injective_af_function. uf f. ir.

cp (bij_is_function H6).

set (T:= image_by_fun x (union2 (product u (singleton TPa)) E2)).
Let Q be the set of subsets of E equipotent to E. The mapping \( g(X) = f(\bar{X} \cup E_2) \) is injective \( \mathfrak{P}(E) \to Q \) because \( f \) is injective and the sets \( \bar{X} \) and \( E_2 \) are disjoint. Since \( Q \subset \mathfrak{P}(E) \), these two sets have the same cardinal.

4. If \( E \) is an infinite set, the set of all partitions of \( E \) is equipotent to \( \mathfrak{P}(E) \) (associate a subset of \( E \times E \) with each partition of \( E \)).

Let \( \omega \) be a partition, and \( \bar{\omega} \) be the union of all \( \Lambda \times \Lambda \) with \( \Lambda \in \omega \). We know that \( \omega \to \bar{\omega}' \) is an order (see chapter one), so that the function \( \omega \to \bar{\omega} \) is injective. Let \( Q \) be the set of partitions; this shows \( \text{Card}(Q) \leq \text{Card}(\mathfrak{P}(E \times E)) \), hence \( \text{Card}(Q) \leq \text{Card}(\mathfrak{P}(E)) \).


Proof. ir. set (q:=set_of_partition_set E). set (y := W (J x0 TPa) x).

assert (inc (J x0 TPa) (source x)). rw H7. app union2_first. uf E1. aw. ee. fprops. rwi powerset_inc_rw H12. app H12. fprops.

assert (inc y T). uf T. uf image_by_fun. aw. exists (J x0 TPa). split.

app union2_first. aw. ee. fprops. am. fprops. red. uf y. app defined_lem. fprops. ufi T H18. rwi H14 H18. ufi image_by_fun H18.


assert (inc x1 (source x)). rw H7. nin (union2_or H18). app union2_first.


awi H25. ee. wri H24 H27. awi H27. cp H27.

elim two_points_distinct. am. fprops.

set (y := W (J x0 TPa) x).

assert (inc (J x0 TPa) (source x)). rw H7. app union2_first. uf E1. av. ee.


assert (inc y T). uf T. rw H14. uf image_by_fun. aw. exists (J x0 TPa).

split. app union2_first. aw. ee. fprops. am. fprops. red. uf y.

app defined_lem. fprops. ufi T H18. ufi image_by_fun H18.


assert (inc x1 (source x)). rw H7. nin (union2_or H18). app union2_first.


awi H25. ee. wri H24 H27. awi H27. cp H27.

elim two_points_distinct. am. fprops.

assert (cardinal_le (cardinal (powerset E)) (cardinal Qo)). red. ee.

fprops. rwi cardinal_le2. rw cardinal_le1. exists F. ee. am. uf F.

tv. uf F. tv. wr cardinal_equipotent.

app cardinal_antisymmetry1.

Qed.
assert (equipotent_to_subset q (powerset (coarse E))). rw cardinal_le1. exists f. ee. am. tv. tv. rwi cardinal_le2 H1.
assert (cardinal_le (cardinal q) (cardinal (powerset (coarse E)))). uf cardinal_le. ee. fprops. fprops. fprops.
assert (cardinal (powerset (coarse E)) = cardinal (powerset E)).
rw card_powerset. rw card_powerset. uf coarse. app card_pow_pr. fprops.
wr cardinal_equi potent. wr card_mult_pr1.
transitivity (card_mult (cardinal E)(cardinal E)). app card_mult_pr2.
sy. fprops. sy. fprops. wr power_x_2. app equipotent_inf2_inf. fprops.

Conversely, consider the mapping $I \mapsto \{I, E \setminus I\}$. This mapping is not injective for $I \subseteq E$, but it is injective for $I \subseteq F$, where $F$ is strict subset of $E$. Since there is at least one element $y$ in $E$, we may consider $F = E \setminus \text{singleton}$.

$rwi H3 H2. nin (emptyset_dichot E). rwi H4 H. nin H. elim H5.$
$wr inc_Bnat. app inc0_Bnat. nin H4.$
$set (F:= complement E (singleton y)).$
$set (g:= fun u => doubleton u (complement E u)).$

assert (forall u v , sub u F -> sub v F -> g u = g v -> u = v). uf g. ir.

assert (inc y F). app H5. rw H8. rw inc_complement. split. am. red. ir.

If $I$ is a non-empty subset of $F$ then $I \mapsto \{I, E \setminus I\}$ is a partition of $E$.

assert (forall u, sub u F -> nonempty u -> inc (g u) q). ir.
assert (sub u E). assert (sub F E). uf F. app sub_complement.
app (sub_trans H6 H8).
uf g. uf q. rw set_of_partition_pr. red. ee. set_extens.
in (union_exists H9). nin H10. nin (doubleton_or H11). app H8. wrr H12.
rwi H12 H10. rwi inc_complement H10. nin H10; am.
in (p_or_not_p (inc x u)). ir.
assert (inc u (doubleton u (complement E u))). fprops. ap (union_inc H10 H11). ir.
assert (inc (complement E u) (doubleton u (complement E u))). fprops.
assert (inc x (complement E u)). rw inc_complement. intuition.
ap (union_inc H12 H11). ir. nin (doubleton_or H9). rw H10. rw H10.
ir. nin (doubleton_or H9); nin (doubleton_or H10); rw H11; rw H12.
left. tv. right. app disjoint_complement. right.
ap disjoint_symmetric. app disjoint_complement. left. tv.

All that remains to do is to show that $\text{Card}(\mathcal{P}(E \setminus \{y\}) \setminus \{\emptyset\}) = \text{Card}(\mathcal{P}(E))$.

set (T:= complement (powerset F) (singleton emptyset)).
assert (cardinal_le(cardinal T) (cardinal q)).
wr cardinal_le3. rw cardinal_le1. exists (BL g T q). ee.
ap injective_af_function. red. ir. ufi T H7. rwi inc_complement H7. ee.
am. ir. ufi T H7. rwi inc_complement H7. ufi T H8. rwi inc_complement H8.
ee. app H5. app powerset_sub. app powerset_sub. tv. tv.
cp (cardinal_comp_singl_inf y H). fold F in H8.
assert (infinite_set (powerset F)). red. red. split. fprops. red.
5. If E is an infinite set, the set of all permutations of E is equipotent to \(\mathcal{P}(E)\). (Use Proposition 3 of No. 4 to show that, for each subset A of E whose complementary does not consist of a single element, there exists a permutation \(f\) of E such that A is the set of elements of E which are invariant under \(f\).)

6. Let E, F be two infinite sets such that \(\text{Card}(E) \leq \text{Card}(F)\). Show that (i) the set of all mappings of E onto F, (ii) the set of all mappings of E into F, and (iii) the set of all mappings of subsets of E into F are all equipotent to \(\mathcal{P}(F)\).

7. Let E, F be two infinite sets such that \(\text{Card}(E) < \text{Card}(F)\). Show that the set of all subsets of F which are equipotent to E and the set of all injections of E into F are both equipotent to then set \(F^E\) of all mappings of E into F (for each mapping \(f\) of E into F, consider the injection \(x \mapsto (x, f(x))\) of E into \(E \times F\)).

8. Show that the set of well-orderings on an infinite set E (and a fortiori the set of orderings on E) is equipotent to \(\mathcal{P}(E)\) (Use Exercise 5).

9. Let E be a non-empty well-ordered set in which every element other than the least element of E has a predecessor (the greatest element of \(\leftarrow_x\)). Show that E is isomorphic to either N or an interval \([0, n]\) of N (remark that every segment \(\neq E\) is finite by using Proposition 6 of No. 5; then use Theorem 3 of § 2, no. 5).

10. Let \(\omega\) or \(\omega_0\) denote the ordinal \(\text{Ord}(N)\) (§ 2, Exercise 14). The set of all integers is then a well-ordered set isomorphic to the set of all ordinals \(< \omega\): For each integer \(n\) we denote again \(\omega\) (by abuse of language) the ordinal \(\text{Ord}([0, n])\).

    (a) Show that for each cardinal \(\alpha\) the relation "\(\xi\) is an ordinal and \(\text{Card}(\xi) < \alpha\) is collectivizing (use Zermelo’s theorem). Let \(W(\alpha)\) denote the set of all ordinals \(\xi\) such that \(\text{Card}(\xi) < \alpha\).

    (b) For each ordinal \(\alpha > 0\) define a function \(f_\alpha\) on the well-ordered set \(O’(\alpha)\) or ordinals \(\leq \alpha\) by transfinite induction as follows: \(f_\alpha(0) = \omega_0 = \omega\), and for each ordinal \(\xi\) such that \(0 < \xi < \alpha\), \(f_\alpha(\xi)\) is the least upper bound (§ 2, Exercise 14 (d)) of the set of ordinals \(\xi\) such that \(\text{Card}(\xi) \leq \text{Card}(f_\alpha(\eta))\) for at least one ordinal \(\eta < \xi\). Show that if \(0 \leq \eta < \xi \leq \alpha\), then \(\text{Card}(f_\alpha(\eta)) < \text{Card}(f_\alpha(\xi))\) and that, if \(\xi \leq \alpha \leq \beta\), then \(f_\alpha(\xi) = f_\beta(\xi)\). Put \(\omega_\alpha = \text{Card}(\alpha); \omega_\alpha\) is said to be the initial ordinal of index \(\alpha\). Put \(N_\alpha = \text{Card}(\omega_\alpha); N_\alpha\) is said to be the aleph of index \(\alpha\). In particular, \(N_0 = \text{Card}(N)\).
(c) Show that for each infinite cardinal $\alpha$, the least upper bound $\lambda$ of the set of ordinals $W(\alpha)$ is an initial ordinal $\omega_\alpha$, and that $\alpha = \aleph_\alpha$ (consider the least ordinal $\mu$ such that $\omega_\mu \geq \lambda$); in other words $\omega_\alpha$ is the least ordinal $\xi$ such that $\text{Card}(\xi) = \aleph_\alpha$. For each ordinal $\alpha$ the mapping $\xi \mapsto \aleph_\xi$, defined on $O'(\alpha)$, is an isomorphism of the well-ordered set of cardinals $\leq \aleph_\alpha$ onto the well-ordered set of cardinals $\leq \aleph_\alpha$; in particular $\aleph_{\alpha + 1}$ is the least cardinal $> \aleph_\alpha$. Show that if $\alpha$ has no predecessor, then for every strictly increasing mapping $\xi \mapsto \sigma_\xi$ of an ordinal $\beta$ into $\alpha$ such that $\alpha = \sup_{\xi < \beta} \sigma_\xi$, we have

$$\sum_{\xi < \beta} \aleph_\xi = \aleph_\alpha.$$  

(d) Deduce from (c) that $\omega_\xi$ is a normal ordinal functional symbol (§ 2, Exercise 17).

¶ 11. (a) Show that the ordinal $\omega_\alpha$ is the least ordinal $> 0$ which has no predecessor, that $\omega$ is indecomposable (§ 2, Exercise 16), and that for each ordinal $\alpha > 0$, $\alpha \omega$ is the least indecomposable ordinal which is $> \alpha$ (note that $n \omega = \omega$ for each integer $n$). Deduced that

$$(\alpha + 1) \omega = \alpha \omega \text{ for each } \alpha > 0.$$ 

(b) Deduce from (a) that an ordinal is indecomposable if an only if it is of the form $\omega^\beta$ (use Exercise 18 (d) of § 2).

¶ 12. (a) Show that for each ordinal $\alpha$ and each ordinal $\gamma > 1$, there exists two finite sequences of ordinals $(\lambda_i)$ and $(\mu_i)$ $(1 \leq i \leq k)$ such that

$$\alpha = \gamma^{\lambda_1} \mu_1 + \gamma^{\lambda_2} \mu_2 + \ldots + \gamma^{\lambda_k} \mu_k,$$

where $0 < \mu_i < \gamma$ for each $i$, and $\lambda_i > \lambda_{i+1}$ for $1 \leq i \leq k - 1$ (use Exercise 18 (d) of § 2 and Exercise 3 of § 4). Moreover the sequences $(\lambda_i)$, $(\mu_i)$ are uniquely determined by these conditions. In particular there exists a unique finite deceasing sequence $(\beta_j)_{1 \leq j \leq m}$ such that

$$\alpha = \omega \beta_1 + \omega \beta_2 + \cdots + \omega \beta_m.$$ 

Let $\phi(\alpha)$ denote the greatest ordinal $\omega \beta_1$ in this sequence.

(b) For each integer $n$ let $f(n) \leq n!$ be the greatest number of elements in the set of ordinals of the form $\alpha_{\sigma(1)} + \alpha_{\sigma(2)} + \cdots + \alpha_{\sigma(n)}$, where $(\alpha_i)_{1 \leq i \leq n}$ is an arbitrary sequence of $n$ ordinals and $\sigma$ runs through the set of permutations of the interval $[1, n]$. Show that

$$f(n) = \sup_{1 \leq k \leq n-1} (k.2^{k-1} + 1)f(n - k).$$

(consider first the case where all the $\phi(\alpha_i)$ are equal and show that the largest possible number of distinct ordinals of the desired form is equal to $n$, by using Exercise 16 (a) of § 2. Then use induction on the number of ordinals $\alpha_j$ for which $\phi(\alpha_j)$ takes the least possible value among the set of ordinals $\phi(\alpha_j)$ $(1 \leq j \leq n)$.) Deduce from (1) that for $n \geq 20$ we have $f(n) = 81f(n - 5)$.

(c) Show that the $n!$ ordinals $(\omega + \sigma(1))(\omega + \sigma(2)) \ldots (\omega + \sigma(n))$ where $\sigma$ runs through the set of permutations of the interval $[1, n]$, are all distinct.
¶ 13. (a) Let $w(\xi)$ be a, ordinal functional symbol (§2, Exercise 17), defined for $\xi \geq \alpha_0$ and such that the relation $\alpha_0 \leq \xi < \xi'$ implies $w(\xi) < w(\xi')$. Show that, if $\xi \geq \alpha_0$, then $w(\xi + \eta) \geq \xi(\xi) + \eta$ for every ordinal $\eta$ (argue by contradiction). Deduce that there exists $\alpha$ such that $w(\xi) \geq \xi$ for all $\xi \geq \alpha$ (take $\alpha$ to be the least indecomposable ordinal $\geq \alpha_0$; cf Exercise 11 (a)).

(b) Let $f(\xi, \eta)$ be the ordinal functional symbol defined in § 2, Exercise 17(b). Suppose that the relations $\alpha_0 \leq \xi \leq \xi'$ and $\alpha_0 \leq \eta \leq \eta'$ imply $g(\xi, \eta) \leq g(\xi', \eta')$ so that the relations $\alpha_0 \leq \xi \leq \xi'$ and $1 \leq \eta \leq \eta'$ imply $f(\xi, \eta) \leq f(\xi', \eta')$ (§ 2, Exercise 17(d)). Show that for each ordinal $\beta$ there exist at most a finite number of ordinals $\eta$ for which the equation $f(\xi, \eta) = \beta$ has at least one solution (Note that if $\xi_1$ is the least solution of $f(\xi, \eta_1) = \beta$ and if $\xi_2$ is the least solution of $f(\xi, \eta_2) = \beta$ then the relation $\eta_1 \leq \eta_2$ implies $\xi_1 > \xi_2$.)

(c) A critical ordinal with respect to $f$ is any infinite ordinal $\gamma > \alpha_0$ such that $f(\xi, \gamma) = \gamma$ for all $\xi$ such that $\alpha_0 \leq \xi < \gamma$. Show that a critical ordinal (with respect to $f$) has no predecessor. If there exists a set $A$ or ordinals such that $f(\xi, \gamma) = \gamma$ for all $\xi \in A$, and if $\gamma$ is the least upper bound of $A$, show that $\gamma$ is a critical ordinal.

(d) let $h(\xi) = f(\xi, \xi)$ (defined for $\xi \geq \alpha_0$); Defined inductively $\alpha_1 = \alpha_0 + 2 \alpha_{n+1} = h(\alpha_n)$ for $n \geq 1$. Show that the least upper bound of the sequence $(\alpha_n)$ is a critical ordinal with respect to $f$.

(e) Show that the least upper bound of every set of critical ordinals with respect to $f$ is again a critical ordinal, and that every critical ordinal is indecomposable (note that $f(\xi, \eta + 1) \geq \omega(\xi) + \eta \geq \xi + \eta$ for all $\xi \geq \alpha_0$).

¶ 14. (a) Show that if $\alpha \geq 2$ and if $\beta$ has no predecessor, then $\alpha^\beta$ is an indecomposable ordinal (cf § 2, Exercise 16 (a)); if $\alpha$ is finite and if $\beta = \omega \gamma$, then $\alpha^\beta = \omega^\gamma$; if $\alpha$ is infinite and if $\pi$ is the greatest indecomposable ordinal $\leq \alpha$, then $\alpha^\pi = \pi^\pi$ (use Exercise 11).

(b) An ordinal $\delta$ is critical with respect to the functional symbol $f(\xi, \eta) = \xi \eta$ if and only if, for each $\alpha$ such that $1 < \alpha \leq \delta$, the equation $\delta = \alpha^\xi$ has a solution; the unique solution $\xi$ if this equation is then indecomposable (Use Exercise 13 (e), together with Exercise 18 (d) of § 2). Conversely, for each $\alpha > 1$ and each indecomposable ordinal $\pi$, $\alpha^\pi$ is a critical ordinal with respect to $\xi \eta$ (use Exercise 13 (c)). Deduced that $\delta$ is a critical ordinal with respect to $\xi \eta$ if and only if $\delta$ is of the form $\omega^\omega$ (cf. Exercise 11 (b)).

(c) For an ordinal $\epsilon$ to be critical with respect to the functional symbol $f(\xi, \eta) = \xi$, i.e. such that $\gamma^\epsilon = \epsilon$ for each $\gamma$ satisfying $2 \leq \gamma \leq \epsilon$, it is sufficient that $2^\epsilon = \epsilon$. Show that the least critical ordinal $\epsilon_0$ with respect to $\xi^\eta$ is countable (cf. Exercise 13 (d)).

¶ 15. Let $\gamma$ be an ordinal $> 1$, and for each ordinal $\alpha$ let $L(\alpha)$ denote the set of exponents $\lambda_i$ in the expression for $\alpha$ given in Exercise 12 (a).

(a) Show that $\lambda_i \leq \alpha$ for each $\lambda_i \in L(\alpha)$ and that $\lambda_i = \alpha$ for one of these ordinal only if $\alpha = 0$ or if $\alpha$ is a critical ordinal with respect to $\xi^\eta$ (Exercise 14 (c)).

(b) Define $L_n(\alpha)$ by induction on $n$ as follows: $L_1(\alpha) = L(\alpha)$ and $L_n(\alpha)$ is the union of the sets $L(\beta)$ as $\beta$ runs through $L_{n-1}(\alpha)$. Show that there exists an integer $n_0$ such that $L_{n+1}(\alpha) = L_n(\alpha)$ whenever $n \geq n_0$, and that the elements of $L_n(\alpha)$ are then either $0$ or critical ordinals with respect to $\xi^\eta$ (Argue by contradiction: for each $n$, consider the set $M_n(\alpha)$ of elements $\beta \in L_n(\alpha)$ such that $\beta \notin L(\beta)$, and assume that $L_n(\alpha)$ if not empty for any $n$; use (a) to obtain a contradiction.)
16. Every totally ordered set has a well-ordered cofinal subset (§ 2, Exercise 2). The least of the ordinals $\text{Ord}(M)$ of the well-ordered cofinal subsets $M$ of $E$ is said the final character of $E$.

(a) An ordinal $\xi$ is said to be regular if it is equal to its final character, and singular otherwise. Show that every infinite regular ordinal is an initial ordinal $\omega_\alpha$ (Exercise 10). Conversely, every initial ordinal $\omega_\alpha$, whose index $\alpha$ is either 0 or has a predecessor, is a regular ordinal. An initial ordinal $\omega_\alpha$ whose index $\alpha$ has no predecessor is singular if $0 < \alpha < \omega_\alpha$; in particular, $\omega_\omega$ is the least infinite singular initial ordinal.

(b) An initial ordinal $\omega_\alpha$ is said to be inaccessible if it is regular and its index $\alpha$ has no predecessor. Show that if $\alpha = 0$, then $\omega_\alpha = \alpha$; in other words, $\alpha$ is a critical ordinal with respect to the normal functional symbol $\omega_\eta$ (Exercise 10 (d) and 13 (c)). Let $\kappa$ be the least critical ordinal with respect to this functional symbol. Show that $\omega_\kappa$ is singular, with final character $\omega$ (cf Exercise 13(d)). In other words, there exists no inaccessible ordinal $\omega_\alpha$ such that $0 < \alpha \leq \kappa$ (At present, it is not known whether or not there exist inaccessible ordinals other than $\omega$).

(c) Show that there exists only one regular ordinal which is cofinal in a given totally ordered set $E$; this ordinal is equal to the final character of $E$, and if $E$ is not empty and has no greatest element, it is an initial ordinal. If $\omega_\alpha$ is the final character of $\omega_\alpha$, then $\alpha \leq \kappa$; and $\omega_\alpha$ is regular if and only if $\alpha = \kappa$.

(d) Let $\omega_\alpha$ be a regular ordinal and let $I$ be a well-ordered set such that $\text{Ord}(I) < \omega_\alpha$. Show that, for each family $(\xi_i)_{i \in I}$ of ordinals such that $\xi_i < \omega_\alpha$ for all $i \in I$, we have $\sum_{i \in I} \xi_i < \omega_\alpha$.

17. A cardinal $\kappa_\alpha$ is said to be regular (resp. singular) if the initial ordinal $\omega_\alpha$ is regular (resp. singular). For $\kappa_\alpha$ to be regular it is necessary and sufficient that for every family $(\alpha_i)_{i \in I}$ of cardinals such that $\text{Card}(I) < \kappa_\alpha$ and $\alpha_i < \kappa_\alpha$ for all $i \in I$, we have

$$\sum_{i \in I} \alpha_i < \kappa_\alpha.$$ 

$\kappa_\alpha$ is the least singular cardinal.

¶ 18. (a) For each ordinal $\alpha$ and each cardinal $m \neq 0$ we have $\kappa_\alpha^m = \kappa_\alpha^m \cdot \kappa_{\alpha+1}$ (reduce to the case where $m < \kappa_{\alpha+1}$ and consider the mappings of the cardinal $m$ into the ordinal $\omega_{\alpha+1}$).

(b) Deduce from (a) that, for each ordinal $\gamma$ such that $\text{Card}(\gamma) \leq m$ we have $\kappa_\alpha^m = \kappa_\alpha^m \cdot \kappa_{\alpha+\gamma}$ (by transfinite induction on $\gamma$).

(c) Deduce from (b) that, for each ordinal $\alpha$ such that $\text{Card}(\alpha) \leq m$, we have $\kappa_\alpha^m = 2^m \cdot \kappa_{\alpha \text{Card}(\alpha)}$.

¶ 19. (a) Let $\alpha$ and $\beta$ be two ordinals such that $\alpha$ has no predecessor, and let $\xi \rightarrow \sigma_\xi$ be a strictly increasing mapping of the ordinal $\omega_\beta$ into the ordinal $\alpha$ such that $\sup_{\xi < \omega_\beta} \sigma_\xi = \alpha$. Show that

$$\kappa_\alpha^\beta = \prod_{\xi < \omega_\beta} \kappa_{\alpha_\xi}.$$

(With each mapping $f$ of the ordinal $\omega_\beta$ into the ordinal $\omega_\alpha$ associate an injective mapping $\tilde{f}$ of $\omega_\beta$ into the set of all $\omega_\alpha$ ($\xi < \omega_\beta$) such that $f(\xi) = \tilde{f}(\xi)$ for all $\xi < \omega_\beta$. Calculate the cardinal of the set of mappings $f$ associated with then same $\tilde{f}$ and observe that

$$m = \prod_{\xi < \omega_\beta} \kappa_{\alpha_\xi} \geq 2^{\text{card}(\omega_\beta)}$$

and $m \geq \kappa_\alpha$ (cf. § 3, Exercise 3).)

RR n° 7150
(b) Let \( \alpha \) be the ordinal such that \( \omega_\alpha \) is the final character of \( \omega_\alpha \). Show that that \( \aleph_\alpha^\alpha > \aleph_\alpha \) and that if there exists \( n \) such that \( \aleph_\alpha = n^{\omega_\alpha} \) then \( \gamma < \alpha \) (use (a) and Exercise 3 of § 3).

(c) Show that if \( \lambda < \bar{\alpha} \) then
\[
\aleph_\beta_\alpha = \sum_{\xi < \alpha} \aleph_\xi
\]
(try as in Exercise 18 (a)).

¶ 20. (a) For a cardinal \( a \) to be regular (Exercise 17) it is necessary that for every cardinal \( b \neq 0 \) we should have
\[
a^b = a \cdot \sum_{m < a} m^b.
\]
(Use Exercise 19 and consider separately the cases (i) \( b \) is finite, (ii) \( \aleph_0 \leq b < a \), (iii) \( b \geq a \); also use Exercise 3 of § 3.) The generalized continuum hypothesis implies that the above condition is also sufficient.

(b) Show that if a cardinal \( a \) is such that \( a^m = a \) for every cardinal \( m \) such that \( 0 < m < a \), then \( a \) is regular (use Exercise 3 of § 3).

(c) Show that the proposition “for every regular cardinal \( a \) and every cardinal \( m \) such that \( 0 < m < a \), we have \( a = a^m \) is equivalent to the generalized continuum hypothesis (use (a)).

¶ 21. An infinite cardinal \( a \) is said to be dominant if for each pair of cardinals \( m < a, n < a \) we have \( m^n < a \).

(a) For \( a \) to be dominant it is sufficient that \( 2^m < a \) for every cardinal \( m < a \).

(b) Define inductively a sequence \( (a_\lambda) \) of cardinals as follows: \( a_0 = \aleph_0 \), \( a_{\lambda+1} = 2^{a_\lambda} \). Show that the sum \( b \) of the sequence \( a_\lambda \) is a dominant cardinal. \( \aleph_0 \) and \( b \) are the two smallest dominant cardinals.

(c) Show that \( b^{\aleph_0} = \aleph_0^b = 2^b \) (Note that \( 2^b \leq b^{\aleph_0} \)). Deduce that \( b^{\aleph_0} = (2^b)^b \), although \( b < 2^b \) and \( \aleph_0 < b \).

¶ 22. A cardinal \( \aleph_\alpha \) is said to be inaccessible if the ordinal \( \omega_\alpha \) is inaccessible (Exercise 16 (b)). We have then \( \omega_\alpha = \alpha \) if \( \omega_\alpha \neq \omega_0 \). A cardinal \( \alpha \) is said to be strongly inaccessible if it is inaccessible and dominant.

(a) The generalized continuum hypothesis implies that every inaccessible cardinal is strongly inaccessible.

(b) For a cardinal \( \alpha \geq 3 \) to be strongly inaccessible it is necessary and sufficient that, for each family \( (a_\iota)_{\iota \in I} \) of cardinals such that
\[
\text{Card}(I) < \alpha \text{ and } a_\iota < \alpha
\]
for all \( \iota \in I \), we should have \( \prod_{\iota \in I} a_\iota < \alpha \).

(c) For an infinite cardinal \( \alpha \) to be strongly inaccessible it is necessary and sufficient that it should be dominant (Exercise 21) and that it should satisfy one of the following two conditions: (i) \( \alpha^b = a \) for every cardinal \( b \) such that \( 0 < b < \alpha \); (ii) \( \alpha^b = a \cdot 2^b \) for every cardinal \( b > 0 \) (Use Exercises 20 and 21).
23. Let $\alpha$ be an ordinal $> 0$. A mapping $f$ of the ordinal $\alpha$ into itself is said to be divergent if for each ordinal $\lambda_0 < \alpha$ there exists an ordinal $\mu_0 < \alpha$ such that the relation $\mu_0 \leq f(\xi) < \alpha$. This condition may be written as $\lim_{\xi \to \alpha, \xi < \alpha} f(\xi) = \alpha$

(a) Let $\phi$ be a strictly increasing mapping of an ordinal $\beta$ into $\alpha$ such that

$$\phi(\sup \zeta) = \sup \phi(\zeta) \text{ for all } \gamma < \beta,$$

and such that

$$\sup_{\zeta < \beta} \phi(\zeta) = \alpha.$$

(if we extend $\phi$ by defining $\phi(\beta) = \alpha$, the conditions above signify that $\phi$ is continuous.) Then there exists a divergent mapping $f$ of $\alpha$ into itself, such that $f(\xi) < \xi$ for all $\xi$ satisfying $0 < \xi < \alpha$, if and only if there exists a divergent mapping of $\beta$ into itself of the same type.

(b) Deduce from (a) that there exists a divergent mapping of $\omega_\alpha$ into itself, such that $f(\xi) < \xi$ for all $\xi$ satisfying $0 < \xi < \alpha$ if and only if the final character of $\omega_\alpha$ is $\omega_0$. (If $\omega_\alpha$ is a regular ordinal $> \omega_0$, defined inductively a strictly increasing sequence $(\eta_n)$ as follows: $\eta_1 = 1$, and $\eta_{n+1}$ is the least ordinal $\lambda$ such that $\xi < \lambda$ into itself, such that $f(\xi) = \eta_0$ for all $\xi \geq \zeta$.)

(c) Let $\omega_\alpha$ be the final character of $\omega_\alpha$ (Exercise 16). Show that, if $\alpha > 0$ and if $f$ is a mapping of $\omega_\alpha$ into itself such that $f(\xi) < \xi$ for all $\xi$ such that $0 < \xi < \omega_\alpha$, then there exists an ordinal $\lambda_0$ such that the set of solutions to the equation $f(\xi) = \lambda_0$ has a cardinal $\geq \aleph_\alpha$.

24. Let $\mathfrak{F}$ be a set of subsets of a set $E$ such that for every $A \in \mathfrak{F}$ we have $\text{Card}(A) = \text{Card}(\mathfrak{F}) = \alpha \geq \aleph_0$. Show that $E$ has a subset $P$ such that $\text{Card}(P) = \alpha$ and such that no set of $\mathfrak{F}$ is contained in $P$. (If $a = \aleph_\alpha$, define by transfinite induction two injective mappings $\xi \to f(\xi)$, $\xi \to g(\xi)$ of $\omega_\alpha$ into $E$ such that the sets $P = f(\omega_\alpha)$ and $Q = g(\omega_\alpha)$ do not intersect and such that each of them meets every subset $A \in \mathfrak{F}$.

(b) Suppose, moreover, that for each subset $\mathfrak{G}$ of $\mathfrak{F}$ such that $\text{Card}(\mathfrak{G}) < \alpha$, the complement in $E$ of the union of the sets $A \in \mathfrak{G}$ has cardinal $\geq \alpha$. Show that $E$ then has a subset $P$ such that $\text{Card}(P) = \alpha$ and such that, for each $A \in \mathfrak{G}$, $\text{card}(P \cap A) < \alpha$ (similar method).

25. (a) Let $\mathfrak{F}$ be a covering of an infinite set $E$. The degree of disjointness of $\mathfrak{F}$ is the least cardinal $c$ such that $c$ is strictly greater than the cardinals $\text{Card}(X \cap Y)$ for each pair of distinct sets $X, Y \in \mathfrak{F}$. If $\text{Card}(E) = \alpha$ and $\text{Card}(\mathfrak{F}) = \beta$, show that $\beta \leq \alpha^c$ (note that a subset of $E$ of cardinal $c$ is contained in at most one set of $\mathfrak{F}$).

(b) Let $\omega_\alpha$ be an initial ordinal and let $F$ be set such that $2 \leq \text{Card}(F) < \aleph_\alpha$. Let $E$ be the set of mappings of segments of $\omega_\alpha$, other than $\omega_\alpha$ itself, into $F$. The we have $\text{Card}(E) \leq \text{p}^{\aleph_0}$. For each mapping $f$ of $\omega_\alpha$ into $F$, let $F_f$ be the subset of $E$ consisting of the restrictions of $f$ to the segments of $\omega_\alpha$ (other than $\omega_\alpha$ itself). Show that the set $\mathfrak{F}$ of subsets of $K_f$ is a covering of $E$ such that $\text{Card}(\mathfrak{F}) = \text{p}^{\aleph_0}$ and that its degree of disjointness is equal to $\omega_\alpha$.

(c) Let $E$ be an infinite set of cardinal $\alpha$ and let $\gamma$, $\beta$ be two cardinal $> 1$ such that $\gamma < \beta$, $\text{p}^m < \alpha$ for all $m < c$ and $\alpha = \sum_{m < c} \text{p}^m$. Deduce from (b) that there exists a covering $\mathfrak{F}$ of $E$ consisting of sets of cardinal $\gamma$ with degree of disjointness equal to $\alpha$ and such that $\text{Card}(\mathfrak{F}) = \text{p}^\alpha$. In particular, if $E$ is countably infinite, there exists a covering $\mathfrak{F}$ of $E$ by infinite sets such that $\text{card}(\mathfrak{F}) = 2^{\aleph_0}$ and such that the intersection of any two sets of $\mathfrak{F}$ is finite.

26. Let $E$ be an infinite set and let $\mathfrak{F}$ be a set of subsets of $E$ such that for $A \in \mathfrak{F}$ we have $\text{card}(A) = \text{card}(\mathfrak{F}) = \text{card}(E) = \alpha \geq \aleph_0$. RR n° 7150
Show that there exists a partition \((B_i)_{i \in I}\) of \(E\) such that
\[
\text{card}(I) = \text{card}(B_i) = a
\]
for all \(i \in I\) and such that \(A \cap B_i \neq \emptyset\) for all \(A \in \mathfrak{F}\) and all \(i \in I\). (With the notation of Exercise 24 (a), consider first a surjective mapping \(f\) of \(\omega_\alpha\) into \(\mathfrak{F}\) such that for each \(A \in \mathfrak{F}\); the set of all \(\xi \in \omega_\alpha\) such that \(f(\xi) = A\) has cardinal equal to \(a\). Then, by transfinite induction, define a bijection \(g\) of \(\omega_\alpha\) onto \(E\) such that \(g(\xi) \in f(\xi)\) for every \(\xi \in \omega_\alpha\).

**§ 27.** Let \(L\) be an infinite set and let \((E_\lambda)_{\lambda \in L}\) be a family of sets indexed by \(L\). Suppose that for each integer \(n > 0\) the set of \(\lambda \in L\) such that \(\text{card}(E_\lambda) > n\) is equipotent to \(L\). Show that there exists a subset \(F\) of the product \(E = \prod_{\lambda \in L} E_\lambda\), such that \(\text{Card}(F) = 2^{\text{Card}(L)}\), and such that \(F\) has the following property: for each finite sequence \((f_k)_{1 \leq k \leq n}\) of distinct elements of \(F\) there exists \(\lambda \in L\) such that the elements \(f_k(\lambda) \in E_\lambda\) (\(1 \leq k \leq n\)) are all distinct. (Show first that there exists a partition \((L_j)_{j \in \mathbb{N}}\) of \(L\) such that \(\text{Card}(L_j) = \text{Card}(L)\) for all \(j\), and such that \(\text{Card}(E_\lambda) \geq 2^j\) for each \(\lambda \in L_j\). Hence reduce to the case where \(L\) is the sum of the countable family of sets \(X^j\) \((j \geq 1)\), where \(X\) is an infinite set, and \(E_\lambda = 2^j\) for each \(\lambda \in X^j\). With each mapping \(g \in 2^X\) of \(X\) into 2, associate the element \(f \in E\) such that \(f(\lambda) = (g(x_1), \ldots, g(x_j))\) whenever \(\lambda = (x_k)_{1 \leq k \leq j} \in X^j\); show that the set \(F\) of elements \(f \in E\) so defined has the required property.)

**§ 28.** Let \(E\) be an infinite set and let \((X_i)_{1 \leq i \leq m}\) be a finite partition of the set \(\mathfrak{F}_n(E)\) of subsets of \(E\) having \(n\) elements. Show that there exists an index \(i\) and an infinite subset \(F\) of \(E\) such that every subset of \(F\) with \(n\) elements belongs to \(X_i\). (Proof by induction on \(n\). For each \(a \in E\) show that there exists an index \(j(a)\) and an infinite subset \(M(a)\) of \(E - \{a\}\) such that, for every subset \(A\) of \(M(a)\) with \(n - 1\) elements, \(|a| \cup A\) belongs to \(X_{j(a)}\). Then define a sequence \((a_i)\) of elements of \(E\) as follows: \(a_1\) is an arbitrary element of \(E\), \(a_2\) is an arbitrary element of \(M(a_1)\), \(a_3\) is defined in terms of \(M(a_1)\) and \(a_2\) in the same way as \(a_2\) was defined in terms of \(E\) and \(a_1\), and so on. Show that the set \(F\) of elements of a suitable subsequence of the sequence \((a_i)\) satisfies the required conditions.)

29. In an ordered set \(E\), every finite union of Noetherian subsets (with respect to the induced ordering) is Noetherian.

(b) An ordered set \(E\) is Noetherian if and only if for each \(a \in E\), the interval \([a, \rightarrow]\) is Noetherian.

(c) Let \(E\) be an ordered set such that the ordered set obtained by endowing \(E\) with the opposite ordering is Noetherian. Let \(u\) be a letter and let \(T\{u\}\) be a term. Show that there exists a set \(U\) and a mapping \(f\) of \(E\) onto \(U\) such that for each \(x \in E\) we have \(f(x) = T\{x\}\), where \(T\{x\}\) denotes the mapping of \(\rightarrow, x\{\} \rightarrow, f(x)\{\}\) which coincides with \(f\) on this interval. Furthermore \(U\) and \(f\) are determined uniquely by this condition.

(d) Let \(E\) be a Noetherian ordered set such that every finite subset of \(E\) has a least upper bound in \(E\). Show that, if \(E\) has a least element, then \(E\) is a complete lattice (§ 1, Exercise 11); and that if \(E\) has no least element, the set \(E'\) obtained by adjoining a least element to \(E\) (§ 1, no. 7, Proposition 3) is a complete lattice.

30. Let \(E\) be a lattice such that the set obtained by endowing \(E\) with the opposite ordering is Noetherian. Show that every element \(a \in E\) can be written as \(\text{sup}(e_1, e_2, \ldots, e_n)\) where
$e_1, \ldots, e_n$ are irreducible (§ 4, Exercise 7; show first that there exists an irreducible element $e$ such that $a = \sup(e, b)$ if $a$ is not irreducible). Generalize Exercise 7 (b) of § 4 to $E$; also generalize Exercises 8(b) and 9(b) of § 4.

\[ \text{§ 31.} \quad \text{Let } A \text{ be an infinite set and let } E \text{ be the set of all infinite subsets of } A, \text{ ordered by inclusion. Show that } E \text{ is completely ramified (§ 2, Exercise 8) but not antidirected (§ 1, Exercise 23) and that } E \text{ has an antidirected cofinal subset } F. \text{ Consider first the set } D(A) \text{ of countable infinite subsets of } A \text{ (which is cofinal in } E) \text{ and let } Z = R_0(D(A)) \text{ (§ 1, Exercise 23). Write } Z \text{ in the form } (z_\lambda)_{\lambda \in L}, \text{ where } L \text{ is a well-ordered set, and take } F \text{ to be a set of countable subsets } X^\lambda_n, \text{ where } \lambda \text{ runs through a suitable subset of } L, n \in N, X^\lambda_m \supset X^\lambda_n \text{ whenever } m \leq n, X^\lambda_n - X^\lambda_{n+1} \text{ is infinite for all } n \geq 0 \text{ and } \cup_{n \in N} X^\lambda_n = \emptyset; \text{ the } X^\lambda_n \text{ are to be defined by transfinite induction in such a way that the images of the sets } X^\lambda_n \text{ under the canonical mapping } r : D(A) \to Z (§ 1, Exercise 23) \text{ are mutually disjoint and form a cofinal subset of } Z. \]

\[ \text{§ 32.} \quad ^* \text{ Let } (M_n), (P_n) \text{ be two sequences of mutually disjoint finite sets (not all empty), indexed by the set } Z \text{ of rational integers. Let } \alpha_n = \text{Card}(M_n), \beta_n = \text{card}(P_n). \text{ Suppose that there exists an index } k > 0 \text{ such that for each } n \in Z \text{ and each integer } l \geq 1 \text{ we have}
\]
\[
\alpha_n + \alpha_{n+1} + \cdots + \alpha_{n+l} \leq \beta_{n-k} + \beta_{n-k+1} + \cdots + \beta_{n+l+k},
\]
\[
\beta_n + \beta_{n+1} + \cdots + \beta_{n+l} \leq \alpha_{n-k} + \alpha_{n-k+1} + \cdots + \alpha_{n+l+k}.
\]

Let $M$ be the union of the family $(M_n)$ and let $P$ be the union of the family $(P_n)$. Show that there exists a bijection $\phi$ of $M$ onto $P$ such that
\[
\phi(M_n) \subseteq \bigcup_{i = n-k}^{n+k-1} P_i \text{ and } \phi(P_n) \subseteq \bigcup_{i = n-k}^{n+k-1} M_i
\]
for each $n \in Z$ (consider a total ordering on each $M_n$ (resp. $P_n$) and take $M$ (resp. $P$) to be the ordinal sum (§ 1, Exercise 3) of the family $(M_n)_{n \in Z}$ (resp. $(P_n)_{n \in Z}$). If $n_0$ is an index such that $M_{n_0} \neq \emptyset$ consider the isomorphisms of $M$ onto $P$ which transform the least element of $M_{n_0}$ into one of the elements of $\bigcup_{j = n_0-k}^{n_0+k} P_j$ and show that one of these isomorphisms satisfies the required conditions. Let $\delta$ be the least of the numbers
\[
\beta_{n-k} + \beta_{n-k+1} + \cdots + \beta_{n+l+k} - (\alpha_n + \alpha_{n+1} + \cdots + \alpha_{n+l}),
\]
\[
\alpha_{n-k} + \alpha_{n-k+1} + \cdots + \alpha_{n+l+k} - (\beta_n + \beta_{n+1} + \cdots + \beta_{n+l})
\]
for all $n \in Z$ and all $l \geq 1$. If $n \in Z$ and $l \geq 1$ are such that, for example $\beta_{n-k} + \beta_{n-k+1} + \cdots + \beta_{n+l+k} = \delta + \alpha_n + \alpha_{n+1} + \cdots + \alpha_{n+l}$ we may take $\phi$ to be such that the least element of $P_{n-k}$ is the image under $\phi$ of the least element of $M_{n-k}$. *

\[ \text{§ 33.} \quad \text{Soient } a, b \text{ deux cardinaux tels que } a \geq 2, b \geq 1, \text{ l'un au moins des deux étant infini. Soient } E \text{ un ensemble, } \mathcal{F} \text{ une partie de } \mathcal{P}(E), \text{ telle que } \text{card}(\mathcal{F}) > a^b \text{ et card}(X) \leq b \text{ pour tout } X \in \mathcal{F}. \text{ On se propose de montrer qu'il existe une partie } \mathcal{G} \subset \mathcal{F} \text{ telle que card}(\mathcal{G}) > a^b \text{ et que deux quelconques des ensembles appartenant à } \mathcal{G} \text{ aient } \text{la même intersection}. \text{ On pourra procéder de la façon suivante.}
\]

a) soit $c$ le plus petit des cardinaux > $a^b$ et soit $\Omega$ le plus petit ordinal de cardinal $c$. On considère une application injective $v \mapsto X(v)$ de $\Omega$ dans $\mathcal{F}$ et on pose $M = \bigcup_{v \in \Omega} X(v)$; on peut supposer que card($M$) = $c$, et il y a donc une bijection $v \mapsto x_v$ de $\Omega$ sur $M$, ordonnant $M$. 

RR n° 7150

Bourbaki: Theory of sets in Coq. II (v2) 277
b) Pour tout $\nu \in \Omega$ soit $\rho_\nu$ l’ordinal type d’ordre du sous-ensemble $X(\nu)$ de $M$ (on a $\text{Card}(\rho_\nu) \geq b$) et soit $\mu \mapsto y_\mu^{(\nu)}$ l’unique application bijective croissante de $\rho_\nu$ sur $X(\nu)$. On note $M_\mu$ l’ensemble des $y_\mu^{(\nu)}$ lorsque $\nu$ parcourt $\Omega$. Montrer qu’il existe au moins un ordinal $\mu$ tel que $\text{Card}(M_\mu) = c$. On désigne par $\alpha$ le plus petit de ces ordinaux; la réunion de $M_\gamma$ pour $\gamma < \alpha$ a un cardinal $\leq a^b < c$.

c) Montrer qu’il existe une partie $N_0 \subset \Omega$ telle que $\text{Card}(N_0) = c$ et que l’application $\nu \mapsto y_\nu^{(\nu)}$ de $N_0$ dans $M$ soit injective. Montrer, par récurrence sur $\beta$, qu’il existe une partie $N_\beta \subset N_0$ de cardinal $c$ telle que l’élément $y_\mu^{(\nu)} = z_\lambda$ soit indépendant de $\nu$ pour $\nu \in N_\beta$ et pour tout $\lambda \leq \beta$. Montrer que l’intersection $N$ des $N_\beta$ pour $\beta < \alpha$ a pour cardinal $c$ (considérer son complémentaire). Soit $Q$ l’ensemble des $z_\lambda$ pour $\lambda < \alpha$.

d) Pour tout $\nu \in N$, on définit par récurrence un ordinal $\lambda_\nu$ par la condition suivante : c’est le plus petit ordinal dans $N$ tel que $y_\alpha^{(\lambda_\mu)}$ soit un majorant strict, dans $M$, de la réunion des $X(\lambda_\mu)$ pour $\mu < \nu$, $\mu \in N$. Montrer que pour $\mu < \nu$ dans $N$ on a $(\lambda_\mu) \cap (\lambda_\nu) = Q$. 
Chapter 10

Theorems, Notations, Definitions

List of all theorems of Bourbaki, with their Coq equivalent.

Theorems of Chapter 1
Proposition 1 (order_cor_pr) « A correspondence Γ between E and E is an ordering on E if and only if ...», [18].
Proposition 2 (decreasing Composition) says that \( u(\nu(x)) \geq x \) and \( \nu(u(x)) \geq x \) and decreasing imply \( u \circ \nu \circ u = u \) and \( \nu \circ u \circ \nu = \nu \), [28].
Proposition 3 (adjoin_greatest) says that we can add a greatest element to an ordered set, [32].
Proposition 4 (compare_inf_sup1 and compare_inf_sup2) characterizes the supremum and infimum of a subset, [37].
Proposition 5 (sup_increasing and inf_decreasing) says that \( \sup_A \) and \( \inf_A \) are increasing functions of the set \( A \), [38].
Proposition 6 (sup_increasing2 and inf_decreasing2) says that \( \sup f \) and \( \inf f \) are increasing functions of the function \( f \), [38].
Proposition 7 (sup_distributive1 and inf_distributive2) asserts associativity of sup, [39].
Proposition 8 (sup_in_product and inf_in_product) characterizes supremum and infimum in a product, [40].
Proposition 9 (sup_induced2 and 3 variants) characterizes supremum of a subset of a subset, [40].
Proposition 10 (right_directed_maximal and left_directed_minimal) says that «in a right directed ordered set \( E \), a maximal element \( a \) is the greatest element of \( E \)», [42].
Proposition 11 (total_order_monotone_injective and total_order_increasing_morphism) characterizes increasing functions and morphism on totally ordered sets, [43].
Proposition 12 (sup_in_total_order and inf_in_total_order) characterizes supremum and infimum in a totally ordered set, [44].
Proposition 13 (intersection_interval) says that in a lattice, the intersection of two intervals is an interval, [45].

Theorems of Chapter 2
Proposition 1 (well_ordered_segment) says that «in a well-ordered set $E$, every segment of $E$ other than $E$ itself is an interval $]a, \infty[$, where $a \in E$, [49].

Proposition 2 (isomorphism_set_of_segments_iso and set_of_segments_worder) studies $x \mapsto ]-\infty, x[$ [50].

Proposition 3 (worder_merge) studies the supremum of compatible well-orderings, [51].

Lemma 1 (order_merge1 and order_merge2) is a helper for Proposition 3.

Lemma 2 (transfinite_principle1 and transfinite_principle2) is a helper for C59.

Criterion C59 (transfinite_principle) is the principle of transfinite induction, [53].

Criterion C60 (transfinite_definition and transfinite_definition_stable) (Definition of a mapping by transfinite induction), [53].

Lemma 3 (Zermelo_aux) is a helper for Theorem 1.

Theorem 1 (Zermelo) says that «every set $E$ can be well-ordered», [56].

Proposition 4 (Zorn_aux) is a generalization of Zorn’s lemma [57].

Theorem 2 (Zorn_lemma) says «every inductive ordered set has a maximal element», [57].

Corollary 1 (inductive_max_greater).

Corollary 2 (maximal_in_powerset and minimal_in_powerset).

Theorem 3 (isomorphism_worder) studies existence and uniqueness of an isomorphism between two well-ordered sets, [58].

Lemma 4 (increasing_function_segments), [58].

Corollary 1 (unique_isomorphism_onto_segment), [59].

Corollary 2 (bij_pair_isomorphism_onto_segment), [59].

Corollary 3 (isomorphic_subset_segment) [59].

Theorems of Chapter 3

Proposition 1 cardinal_equipotent «two sets $X$ and $Y$ are equipotent if and only if their cardinals are equal», [60].

Theorem 1 (wordering_cardinal_le) says that the ordering between cardinals is a well-ordering, [70].

Corollary 1 (cardinal_le_total_order).

Corollary 2 (cardinal_antisymmetry2).

Proposition 2 (cardinal_supremum) says that a family of cardinals has a supremum, [72].

Proposition 3 (surjective_cardinal_le) says «if there exists a surjection $f$ of $X$ onto $Y$, then $\text{Card}(Y) \leq \text{Card}(X)$», [72].

Proposition 4 (cardinal_prod_pr and cardinal_sum_pr) says that the cardinal sum or cardinal product of the family $\text{Card}(E_i)$ is the cardinal of the sum or the product of the sets $E_i$; [72].

Corollary (cardinal_sum_pr1).

Proposition 5 (cardinal_sum_assoc, cardinal_prod_assoc, cardinal_sum_commutative, cardinal_prod_commutative and cardinal_distrib_prod_sum) asserts commutativity, associativity and distributivity of sum and products, [73].

Corollary. Application to the case of 2 or 3 arguments.

Proposition 6 (zero_unit_sum and one_unit_prod) says that one can remove 0 in a sum and 1 in a product, [76].
Corollary 1 \((\text{zero	extunderscore unit	extunderscore sumr}, \text{zero	extunderscore unit	extunderscore suml}, \text{one	extunderscore unit	extunderscore prodr}, \text{one	extunderscore unit	extunderscore prodl})\).

Corollary 2 \((\text{sum	extunderscore of	extunderscore ones} \text{and} \text{sum	extunderscore of	extunderscore same})\).

Proposition 7 \((\text{zero	extunderscore cardinal	extunderscore product})\) says that a cardinal product is non-zero if and only if each factor is non-zero, \([77]\).

Proposition 8 \((\text{suc	extunderscore injective})\) asserts injectivity of the successor function, \([77]\).

Proposition 9 \((\text{cardinal	extunderscore pow	extunderscore pr1})\) says that \(a^b\) remains unchanged if letters are replaced by equipotent sets, \([77]\).

Proposition 10 \((\text{cardinal	extunderscore pow	extunderscore pr3})\) says that \(a^b\) is a product where all factors are the same \([77]\).

Corollary 1 \((\text{power	extunderscore of	extunderscore sum})\).

Corollary 2 \((\text{power	extunderscore of	extunderscore prod})\).

Corollary 3 \((\text{power	extunderscore of	extunderscore prod2})\).

Proposition 11 \((\text{power	extunderscore x	extunderscore 0} \text{and} \text{variants})\), states \(a^0 = 1, a^1 = a, 1^a = 1, \) and \(0^a = 0, \) \([78]\).

Proposition 12 \((\text{cardinal	extunderscore powerset})\) says \(\text{Card}(\mathcal{P}(X)) = 2^X, \) \([78]\).

Proposition 13 \((\text{cardinal	extunderscore le	extunderscore when	extunderscore complement})\) states that «\(a \geq b\) if and only if there exists a cardinal \(c\) such that \(a = b + c, \) \([79]\).

Proposition 14 \((\text{sum	extunderscore increasing} \text{and} \text{product	extunderscore increasing})\) says the sum and product are increasing functions, \([79]\).

Corollary 1 \((\text{sum	extunderscore increasing1}, \text{product	extunderscore increasing1})\).

Corollary 2 \((\text{power	extunderscore increasing1})\).

Theorem 2 \((\text{cantor})\) says \(X < 2^X, \) \([80]\).

Corollary \((\text{cantor	extunderscore bis})\).

**Theorems of Chapter 4**

Proposition 1 \((\text{is	extunderscore finite	extunderscore succ})\) says that «a cardinal \(a\) is finite if and only if \(a + 1\) is finite», \([82]\).

Proposition 2 \((\text{le	extunderscore int	extunderscore is	extunderscore int}, \text{exists	extunderscore prec})\) says that (if \(n\) is an integer), if \(a \leq n\) then \(a\) is an integer, if \(n > 0\) there is a unique \(m\) with \(m + 1 = n\) and \(a < m + 1\) is equivalent to \(a < n, \) \([83]\).

Corollary 1 \((\text{sub	extunderscore finite	extunderscore set})\).

Corollary 2 \((\text{strict	extunderscore sub	extunderscore smaller})\).

Corollary 3 \((\text{finite	extunderscore image})\).

Corollary 4 \((\text{bijective	extunderscore if	extunderscore same	extunderscore finite	extunderscore c	extunderscore inj}, \text{bijective	extunderscore if	extunderscore same	extunderscore finite	extunderscore c	extunderscore surj})\).

Criterion C61 \((\text{cardinal	extunderscore c	extunderscore induction} \text{and} \text{variants})\) (principle of induction), \([86]\).

Proposition 3 \((\text{finite	extunderscore subset	extunderscore directed	extunderscore bounded}, \text{finite	extunderscore subset	extunderscore lattice	extunderscore inf}, \text{finite	extunderscore subset	extunderscore lattice	extunderscore sup}, \text{finite	extunderscore subset	extunderscore torder	extunderscore greatest}, \text{finite	extunderscore subset	extunderscore torder	extunderscore least})\) gives some properties of a finite subset of an ordered set \([88]\).

Corollary 1 \((\text{finite	extunderscore set	extunderscore torder	extunderscore greatest}, \text{finite	extunderscore set	extunderscore torder	extunderscore worder})\).

Corollary 2 \((\text{finite	extunderscore set	extunderscore maximal})\).

Theorem 1 \((\text{maximal	extunderscore inclusion})\) says that every nonempty set which is of finite character has a maximal element, \([118]\).

**Theorems of Chapter 5**

Proposition 1 \((\text{finite	extunderscore sum	extunderscore finite} \text{and} \text{finite	extunderscore product	extunderscore finite})\) says that a finite sum or product of integers is an integer, \([98]\).
Corollary 1 (finite_union_finite).
Corollary 2 (finite_product_finite_set).
Corollary 3 (Bnat_stable_pow).
Corollary 4 (finite_powerset).

Proposition 2 (cardinal_lt_pr) says that $a < b$ if and only if there is $c$ such that $0 < c$ and $b = c + a$, [100].

Proposition 3 (finite_sum_lt and finite_product_lt) says that $\sum a_i < \sum b_i$ and $\prod a_i < \prod b_i$ if $a_i \leq b_i$ for each $i$ and $a_j < b_j$ for some $j$, [100].

Corollary 1 (finite_power_lt1).
Corollary 2 (finite_power_lt2).
Corollary 3 (plus_simplifiable_left and variants).
Corollary 4 (card_sub_pr and others).

Proposition 4 (restr_plus_interval_isomorphism) says that $x \mapsto x + a$ is a bijection (order isomorphism) $[0, b] \rightarrow [a, a + b]$, [107].

Proposition 5 (cardinal_interval) gives the cardinal of $[a, b]$, [107].

Proposition 6 (finite_ordered_interval) asserts that every finite totally ordered set is isomorphic to a unique interval $[1, n]$, [108].

Proposition 7 (char_fun_union and others) states properties of the characteristic function of a set, [117].

Theorem 1 (division_unique, division_exists) asserts existence and uniqueness of Euclidean division, [118].

Proposition 8 is expansion to base $b$ [121].

Proposition 9 (shepherd_principle) says that if $f$ is a function from a set with cardinal $a$ onto a set with cardinal $b$, and if all set $f^{-1}(\{x\})$ have the same cardinal $c$, then $a = bc$, [124].

Proposition 10 (number_of_injections_prop) gives the number of injections from a finite set into another one, [125].

Corollary (number_of_permutations).

Proposition 11 (number_of_partitions) gives the number of partitions with $p_i$ elements, [127].

Corollary 1 (binomial7).

Proposition 12 (sum_of_binomial) $\sum_{p} \binom{n}{p} = 2^n$, [130].

Proposition 13 is the binomial formula (is a definition in Coq) [130].

Proposition 14 (cardinal_pairs_lt and cardinal_pairs_le) counts the number of pairs $(i, j)$ such $1 \leq i \leq j \leq n$ or $1 \leq i < j \leq n$, [134].

Corollary (sum_of_i).

Proposition 15 counts the number of monomials, [136].

Theorems of Chapter 6

Theorem 1 «The relation ‘$x$ is an integer’ is collectivizing» (see inc_Bnat), [85].

Criterion C62 (restatement on C61, not shown in Coq).

Criterion C63 (integer_induction), [142].

Lemma 1 (infinite_greater_countable) «Every infinite set, E contains a set equipotent to N». 
Lemma 2 (\textit{equipotent\_N2\_N}) «The set $\mathbb{N} \times \mathbb{N}$ is equipotent to $\mathbb{N}$».

Theorem 2 (\textit{equipotent\_inf2\_inf}) «for every infinite cardinal $\alpha$, we have $\alpha = \alpha^2$».

Corollary 1 (\textit{power\_of\_infinite}).

Corollary 2 (\textit{finite\_family\_product}).

Corollary 3 (\textit{notbig\_family\_sum1}).

Corollary 4 (\textit{sum2\_infinite}, \textit{product2\_infinite}).

Proposition 1 (\textit{countable\_subset}, \textit{countable\_product} \textit{countable\_union}) states properties of countable sets.

Proposition 2 (\textit{countable\_finite\_or\_N}) «Every countable infinite set $E$ is equipotent to $\mathbb{N}$».

Proposition 3 (\textit{infinite\_partition}) says that every infinite set $E$ has a partition $X_i$ where $X_i$ is equipotent to $E$ and the index set to $\mathbb{N}$.

Proposition 4 (\textit{countable\_inv\_image}) says that if $f$ is a function from $E$ onto $F$, such that $F$ is infinite and $f^{-1}(\{x\})$ is countable for any $x \in F$, then $F$ is equipotent to $E$.

Proposition 5 (\textit{infinite\_finite\_subsets}) says that the set of finite subsets of an infinite set $E$ is equipotent to $E$.

Proposition 6 (\textit{increasing\_stationary}) characterizes stationary sequences.

Corollary 1 (\textit{decreasing\_stationary}).

Corollary 2 (\textit{finite\_increasing\_stationary}).

Proposition 7 (\textit{noetherian\_induction}) (Principle of Noetherian induction).

Symbols

$x \land y$ is often replaced by “and”. The Coq equivalent is $\land$.

$x \lor y$ is often replaced by “or”. The Coq equivalent is $\lor$.

$\neg x$ is often replaced by “not”. The Coq equivalent is $\neg$.

$(a|b)c$ is a Bourbaki notation, meaning the relation obtained by replacing $b$ by $a$ in $c$.

RL{x} is a Bourbaki notation, meaning that $R$ is a relation that may depend on $x$. If $R$ is a relation that depends on $y$, it is also $(x|y)R$.

$\tau_x(R)$ is a Bourbaki notation, it is the generic element satisfying RL{x}.

$x \Rightarrow y$ is represented in Coq by $x \rightarrow y$.

$x \rightarrow y$ is a Coq notation meaning the type of functions from type $a$ to type $b$.

$x = y$ is equality. We use it as synonym to $\iff$.

$x : y$ is a Coq notation meaning that $x$ is of type $y$.

$f(x)$ is the value of the function $f$ at point $x$, parentheses are sometimes omitted.

$f(x)$ is the value of $f$ on the set $x$, see \textit{fun\_image}, \textit{image\_by\_graph}, \textit{image\_by\_fun}.

$f^{-1}(x)$, see \textit{inverse\_image}.

$(\forall x)P$ and \textit{forall x}, $p$ are similar constructions.

$(\exists x)P$ and \textit{exists x}, $p$ are similar constructions.

$(\exists! x)P$ means sometimes \textit{exists\_unique}.

$x \in y$, $x \ni y$ (is element of): see $\textit{inc}$ and $\textit{elt}$.

$x \subset y$ (is subset of): see $\textit{sub}$.

$\emptyset$ (empty set): see $\textit{emptyset}$.

$\{x, R\}$ (set of $x$ such that $R$): see $\textit{Zo}$. 

RR n° 7150
\[ \{x\}, \{x, y\} : \text{see singleton or doubleton.} \]
\[ a \sim b, a \setminus b, a \cap b : \text{see complement.} \]
\[ (x, y) : \text{ordered pair: see } f. \]
\[ \bigcup_{i \in I} X_i, \text{see } \text{union.} \]
\[ a \cup b, a \cap b, \text{see } \text{union2, intersection2.} \]
\[ A \times B, u \times v, R \times R', \text{see } \text{product, ext_to_prod, prod_of_relation.} \]
\[ f \circ g, \text{see } \text{fcompose, gcompose, compose_graph, compose, composeC.} \]
\[ \Delta_A, \text{see } \text{diagonal.} \]
\[ ^{-1}G \text{ see } \text{inverse_graph, inverse_fun or inverseC.} \]
\[ x \hookrightarrow y \text{ or } x \rightarrow y \text{ is the function that maps } x \text{ to } y, \text{ for instance } x \hookrightarrow \sin x \text{ (source and target are implicit).} \]
\[ x \rightarrow T (x \in A, T \in C), \text{is the function with source } A, \text{ target } C \text{ that maps } x \text{ to } T. \]
\[ (f_x)_{x \in A} \text{ is a shorthand for } x \rightarrow f(x) (x \in A); \text{ see above, the piece } T \in C \text{ is implicit.} \]
\[ \tilde{f}, \text{ see } \text{extension_to_parts.} \]
\[ F^E, \text{ set of graphs of functions from } E \text{ to } F; \text{ see } \text{set_of_gfunctions.} \]
\[ \Phi(E, F), \text{ set of functions from } E \text{ to } F; \text{ see } \text{set_of_functions.} \]
\[ f_x, f_y \text{ sometimes denotes the mappings } y \rightarrow f((x, y)) \text{ or } x \rightarrow f((x, y)), \text{ implemented as } \text{first_partial_fun, second_partial_fun.} \]
\[ \tilde{f}, \text{ sometimes denotes the mappings } x \rightarrow f_x \text{ or } y \rightarrow f_y \text{. Implemented as } \text{first_partial_function, second_partial_function.} \]
\[ f \hookrightarrow \tilde{f}, \text{ implemented as } \text{first_partial_map, second_partial_map, is a bijection from } \Phi(B \times C; A) \text{ into } \Phi(B; \Phi(C; A) \text{ or } \Phi(C; \Phi(B; A)).} \]
\[ \prod_{i \in I} X_i, \text{ product of a family of sets, see } \text{productt.} \]
\[ \{x_i\}_{i \in I} \text{ denotes an element of a product indexed by } I. \]
\[ x \preceq y \text{ is sometimes used instead of } r(x, y), \text{ especially when } r \text{ is the graph of an equivalence relation.} \]
\[ g_E(\sim), \text{ the graph of } \sim \text{ on } E, \text{ see } \text{graph_on.} \]
\[ \sim f \text{ may denote eq_rel-associated } f. \]
\[ \check{x}, \text{ may denote the equivalence class of } x, \text{ see } \text{class.} \]
\[ \check{x} \text{ may denote a representative of the equivalence class } x. \]
\[ E/\sim, E/R (\text{quotient set of } E) \text{ see } \text{quotient.} \]
\[ R/S (\text{quotient of two equivalence relations}) \text{ see } \text{quotient_of_relations.} \]
\[ X_f \text{ sometimes means } f^{-1}(f(X)), \text{ see } \text{inverse_direct_value.} \]
\[ R_A \text{ see } \text{induced_relation.} \]
\[ x >_r y, y <_r x, \text{ notations used when } x \text{ and } y \text{ are related by a preorder relation.} \]
\[ x \preceq_r y, y \succeq_r x, \text{ notations used when } x \text{ and } y \text{ are related by an order relation.} \]
\[ x \leq y, y \geq x, x < y, x > y: \text{ notations used when } x \text{ and } y \text{ are related by an order relation, see } \text{gle, gge, glt, ggt.} \]
\[ f \mapsto G_f \text{ see } \text{graph_of_function.} \]
\[ \circ \mapsto \circ \text{ see } \text{graph_of_partition.} \]
\[ \sup(x, y), \sup_E X, \sup X, \sup f(x) \text{ see } \text{supremum, sup, sup_graph.} \]
\[ \inf(x, y), \inf_E X, \inf X, \inf f(x) \text{ see } \text{infimum, inf, sup_graph.} \]
\[ [a, b], [a, b], [a, b], [a, b], [a, b], [b, b], [b, b], [b, b], \] is an interval.

\[ \tau \leq \text{Card} n, \] order on cardinals, see \text{cardinal}\_le.

\[ g^{(x)} \] is the restriction of \( g \) to \( \rightarrow x \), see \text{restriction}\_to\_segment

\text{Card}(x) is the cardinal of \( x \), see \text{cardinal}.

\[ 0, 1, 2, 3, 4: \text{see card_zero or card_three}. \]

\[ g(x) \] is the restriction of \( g \) to \( \rightarrow x \), see \text{restriction}\_to\_segment

\text{Card}(x) is the cardinal of \( x \), see \text{cardinal}.

\[ 0, 1, 2, 3, 4: \text{see card_zero or card_three}. \]

\[ \sum_{i \in I} a_i \text{, } \prod_{i \in I} a_i: \text{cardinal sum or cardinal product of a family of cardinals, see cardinal}\_sum \]

\[ \text{and cardinal}\_prod. \]

\[ a + b, a.b, ab, \] is the cardinal sum or cardinal product of two cardinals, see \text{card_plus} \text{card}\_mult

\[ E_1 + E_2 \] denotes also the ordinal sum, see \text{ordinal}\_sum.

\[ X_{xy}(a, b) \] is the family \( x \rightarrow a \) and \( y \rightarrow b \), see \text{restriction}\_to\_segment.

\[ X(a, b) = \prod_{x \in I} X_{xy}(a, b), \] for some fixed \( \alpha \) and \( \beta \).

\[ a_x \cup b_y \] is the disjoint union of \( X_{xy}(a, b) \), i.e., \( a \times \{ x \} \cup b \times \{ y \} \).

\[ a^b \] is the cardinal power of two cardinals, see \text{card_pow}.

\[ a^b \] is the power of two integers, see \text{pow}.

\[ N, N, \] set of integers, see \text{Bnat}.

\[ a - b \] is the difference in \( N \), see \text{card_sub}: can also mean \text{minus}, the difference in \( N \).

\[ [a, b] \] is an interval on \( N \), see \text{interval}.

\[ \sum_{i=a}^b t_i \text{ is } \sum_{i \in [a,b]} t_i. \]

\[ a::b \] is \text{cons} \( a \) \( b \), it is the list obtained by putting the element \( a \) in front of the list \( b \).

\[ \phi_\mathcal{A} \] is the characteristic function on \( E \).

\[ a/b \] is the quotient of \( a \) and \( b \).

\[ n! \] is the factorial of \( n \), see \text{binom}.

\[ \binom{n}{p}, \] see \text{binom}.

\textbf{Letters}

\[ \mathcal{B} \text{ see } \\text{Bo}. \]

\[ 'C(a, b), 'C(p, q), 'C(p): \text{see by_cases a b, chooseT and choose}. \]

\[ C_{xy}a \text{ stands for constant_function x y a, it is the constant function from x to y with value a}. \]

\[ C_R x \] may denote the equivalence class of \( x \) for \( R \), see \text{class}.

\[ \text{Coll}_x R \text{ says that } R \text{ is collectivizing in } x. \]

\[ \mathcal{E}, \text{ see Set}. \]

\[ \mathcal{E}_x(R) \text{ appears in the English version where } \{ x, R \} \text{ is used in the French version; see } \text{Zo}. \]

\[ 1_A, \text{ see identity}. \]

\[ 1_{xy} \text{ see inclusionC, canonical_injection}. \]

\[ \mathcal{I}(E, T, f) \text{ says that } f \text{ is defined by transfinite induction, see transfinite_def}. \]

\[ \mathcal{L}_X f, \mathcal{L}_f, \mathcal{L}_{A,B} f \text{ (creating functions): see L,acreate, BL}. \]

\[ \mathcal{M}_f, \mathcal{M}_{A,B} f \text{ (inverse of } \mathcal{L}) \text{ see bcreate1 and bcreate}. \]

\[ N, N, \text{ set of integers, see } \text{Bnat}. \]

\[ \mathcal{N}, \text{ is the bijection from } N \text{ onto } \mathcal{N}, \text{ see } \text{nat_to_B}. \]

\[ \mathcal{P}(x), \text{ see powerset}. \]
pr₁z, pr₂z, prf, pr₁f (projections), see P, Q, pr₁i, pr₁j.

Rx see Ro.

Rab f (restriction) see restriction2.

V(x, f), Vf x (value of a function): see V.

W(x, f), see Xo.

V(P, x, y) see Yo.

Z(x, P) see Zo.

¶ is not defined. We use it as a paragraph separator.

Words

acreate f, L f, is the correspondence associated to the Coq function f.

agrees_on x f f’ is the property that for all a ∈ x, f(a) and f’(a) are defined and equal.

antisymmetric_r r says that the relation r is antisymmetric. [13].

axioms_product_order f g is the condition under which product_order f g is an order, [24].

back_to_nat fn returns the value of f (defined on a subset of N) as if f were defined on N, [111].

bcreate f A B M A;B f, is a kind of inverse of L.

bcreate1 f, M f, is a kind of inverse of L.

bijective f, bijectiveC f, means that f is a bijection.

binom n p, (n p), is the binomial coefficient, [129].

BL f a b, LA;B f, fun_function f a b, is function from A to B whose graph is LA f.

Bnat or N is the set of all integers, [85].

Bnat_divides b a says that a = bq for some q, [118].

Bnat_order, Bnat_le x y, Bnat_lt x y is the ordering on N, and the relations x ≤ y or x < y on N, [85].

Set or E is the type of sets,[1]

Bo, R, is an inverse of R.

bounded_above r X, bounded_below r X, bounded_both r X, mean that X is bounded for r (from above, below or both), [33].

by_cases a b, EC(a, b), defines an object by applying a if P is true, and b if P is false.

canonical_injection x y, I x y, is the inclusion map on x ⊂ y.

canon_proj r, is the mapping x → X from E onto E/R, where E/R is the quotient set of r.

card_mult a b, a.b or ab, is the cardinal product of a family of two elements, [74].

card_plus a b, a + b, is the cardinal sum of a family of two elements, [74].

card_quo a b and card_rem a b are the quotient and remainder in the division of a by b [118].

card_pow a b, aⁿ, is the cardinal is the set of functions (or graphs of functions) from y into x. [77].

card_sub a b, a − b is the difference of the two cardinals. [103].

¹ Changed to Set in version 2
card\_three, card\_four, or 3 and 4, are the cardinals $2 + 1$ and $3 + 1$, \[82\]
card\_zero, card\_one, card\_two, or 0, 1, 2, are the cardinals of the empty set, a singleton, or a doubleton with two distinct elements \[68\].
cardinal $x$, Card($x$) is some set equipotent to $x$, \[68\].
cardinal\_le $x\ y$, $x \leq_{\text{Card}} y$, says that $x$ and $y$ are two cardinals such that $x$ is equipotent to a subset of $y$, \[69\].
cardinal\_lt $x\ y$ is $x \leq_{\text{Card}} y$ and $x \neq y$.
cardinal\_prod $x \prod_{i \in I} a_i$, is the cardinal of the product of the family of sets, \[72\].
cardinal\_nat $x$ maps every set equipotent to the $n$\text{-th} ordinal to the natural number $n$, \[94\].
cardinal\_sum $x \sum_{i \in I} a_i$, is the cardinal of the disjoint of the family of sets, \[72\].
class $r x$ is the class of $x$ for the equivalence relation $r$.
char\_fun $A B$ is the characteristic function of $A$, as a mapping from $B$ into $\{0, 1\}$, \[117\].
choose $p$, $\mathcal{C}(p)$, is some $x$ such that $p(x)$ is true, the empty set if no $x$ satisfies $p$.
choosef $p$ is some function $f$ such that $p(f)$ is true, the identity on the empty set if no $f$ satisfies $p$.
choosenat $p$, $\mathcal{C}_n(p)$, is some integer $i$ such that $p(i)$ is true, zero if no $i$ satisfies $p$, \[94\].
choosefT $p \ q$, $\mathcal{C}_T(p, q)$, is our basic axiom of choice.
coarse $x$ is $x \times x$.
coarser $x$ is the order associated to coarser\_c, \[17\].
coarser\_c $f g$, coarser\_covering $I f J g$, two definitions that say for all $j \in J$ there is $i \in I$ such that $g_j \subset f_i$ or for all $g_j \in g$ there is $f_i \in f$ such that $g_j \subset f_i$.
coarser\_preorder is the order induced by $\subset$ on preorders, \[23\].
cofinal\_set $r A$ says that $x$ in the substrate of $r$ there is an $y \in A$ such that $x \leq_r y$, \[32\].
coinitial\_set $r A$ says that $x$ in the substrate of $r$ there is an $y \in A$ such that $x \geq_r y$, \[32\].
common\_prolongation\_order\_axiom $g$ are the conditions on $g$ for which an order can be put on the union, \[51\].
common\_prolongation\_order $g h$ says that $h$ is an order that on the union of the substrate of the $g_i$ that coincides with the restriction, \[51\].
common\_worder\_axiom $g$ are the conditions on $g$ for which an well-ordering can be put on the union of the family \[51\].
compatible\_with\_equiv\_p $p$ means that $p(x)$ and $x \sim y$ implies $p(y)$.
compatible\_with\_equiv\_f $f r$ means that $x \sim y$ is equivalent to $f(x) = f(y)$.
compatible\_with\_equiv\_f $f r r'$ means that $x \sim y$ is equivalent to $f(x) \sim f(y)$.
complement $a b$, $a \sim b$, $a \setminus b$, $\emptyset b$, is the set of element of $a$ not in $b$.
composableC $f g$, composable $f g$ is the condition on correspondences (resp. functions) $f$ and $g$ for $f \circ g$ to be a correspondence (resp. function).
compose\_graph $f g$, $f \circ g$, composition of two graphs.
compose $f g$, composeC $f g$, $f \circ g$, is the composition of two functions.
constant\_graph $s x$ is the graph of the constant function with domain $s$ and value $x$.
contraction $A B L f v$: assume $f : A \times B \to B$ is a function, $v$ an object of type $B$. If $L$ is a list of type $A C(L)$ is defined by $C(a :: b) = f(a, C(b))$ and $C(nil) = v$, \[112\].
correspondenceC is a data type with three slots, source, target and graph.
José Grimm

corr_value \( f \) associates to a correspondence \( f \) its triple \((G,A,B)\).
covering \( fX \), covering_f \( fX \), covering_s \( fX \), three variants of a family of sets (defined by \( f \) and \( I \)) whose union contains \( x \).
cut x p is the set of all \( x \) that satisfy \( p \).
cut r x is \( r \) of \( x \).
decent_set x says that no element \( y \) of \( x \) satisfies \( y \in y \), \([90]\).
decreasing_map \( f sr \) r r' is a function such that \( x \leq r y \) implies \( f(x) \geq r f(y) \), \([26]\).
decreasing_sequence \( f r \) says that \( f \) is a decreasing function with source \( N \) and target \( r \), \([148]\).
diagonal A, \( \Delta_A \), is the set of all \((x,x)\) such that \( x \in A \).
diagonal_application A is the diagonal mapping \( x \mapsto (x,x) \) of \( A \) into \( \Delta_A \).
diagonal_graphp I E is the set of graphs of constant functions from \( I \) to \( E \).
disjoint x y means \( x \cap y = \emptyset \).
disjoint_union f, disjoint_union_fam f are two variants of the disjoint union of the family of sets \( f \).
domain f is the set of \( x \) for which there is an \( y \) with \((x,y) \in f \), it is \( \text{pr}_1(f) \).
doubleton x y, \((x,y)\), is a set with elements \( x \) and \( y \).
double_list_prop A L Q says that all elements \( x \) and \( y \) of the list \( L \) of type \( A \) satisfy the predicate \( Q(x,y) \), whenever \( x \) comes before \( y \), \([111]\).
EEE is a shorthand for the type \( \text{Set} \to \text{Set} \to \text{Set} \).
EEP is a shorthand for the type \( \text{Set} \to \text{Set} \to \text{Prop} \).
elt x y, \( x \ni y \), is the same as \( y \in x \).
empty_function, empty_functionC is the identity on \( \emptyset \).
emptyset, \( \emptyset \), is a set without elements.
eq_rel_associated f is the graph of the equivalence relation \( f(x) = f(y) \).
equipotent x y means that there is a bijection from \( x \) into \( y \).
equipotent_to_subset x y means that \( x \) is equipotent to \( s \) subset of \( x \), \([69]\).
equivalence_associated f is the equivalence relation \( f(x) = f(y) \).
equivalence_associated_o r is the equivalence relation \( x \leq r y \) and \( y \leq r x \), \([19]\).
equivalence_r r, equivalence_r r x, says that the relation \( r \) is an equivalence relation (in \( x \)).
equivalence_corr r says that the correspondence \( r \) is associated to an equivalence.
exists_unique \( p.(\exists!x)p \), (this notation is not in Bourbaki) means that there exists a unique \( x \) such that \( p(x) \).

expansion_value \( f b \) assume that \( f \) is a functional graph, defined for \( i < k \) and such that \( f_i < b \); the value is \( \sum f_i b_i \), \([123]\).
extends gf, extendsC g f says \( g(x) = f(x) \) whenever \( f(x) \) is defined.
extends_in EF is the relation \( \text{extends} \) in \( \Phi(E,F) \), \([16]\).
extension_order EF is the order associated to \( \text{extends}_\text{in} EF \), \([16]\).
ext_map_prod I X Y g is the function \((x_i)_{i \in I} \mapsto (g_i(x_i))_{i \in I} \) from \( \prod I X_i \) into \( \prod I Y_i \).
ext_to_produ v is the function \((x,y) \mapsto (u(x),v(y)) \), sometimes denoted \( u \times v \).
extension_to_parts f denotes the function \( x \mapsto f(x) \), from \( \Psi(A) \) into \( \Psi(B) \).

factorial \( n \), \( n! \), is the factorial function, \([125]\).

fct_to_list A f n is the list of type \( A \) containing \( f(i) \) for \( i < n \), \([109]\).
fct_sum f n, fct_prod f n, is the sum or product of the values \( f(k) \) for \( k < n \), computed via fct_to_list. \( ^{115} \)

finer_equivalence s r, comparison of equivalences, \( x \preceq y \) implies \( x \triangleq y \).

finite_int_fam f says that \( f \) is a functional graph, with a finite domain and whose range is a subset of the set of integers. \( ^{98} \)

first_proj g is the function \( x \mapsto \text{pr}_1 x \ (x \in g) \).

first_proj_equiv x y, first_proj_equivalence x y, is the equivalence associated to first_proj on the set \( x \times y \).

fcompose f g, \( f \circ g \), composition of two graphs, without assumption.

fcomposable f g says that graphs \( g \) and \( f \circ g \) have the same domain.

fgraph f says that \( f \) is a functional graph.

functional_graph f says that \( f \) is a functional graph.

function_order E F G, function_order_r E F G, is the order defined on \( \mathcal{F}(E; F) \) by \( \forall x, f(x) \prec_G g(x) \). \( ^{24} \)

function_prop f s t, function_prop_sub f s t. This is the property that \( f \) is a function from \( s \) into \( t \), or into a subset of \( t \).

fun_image x f, \( f \langle x \rangle \), is the value of \( f \) on the set \( x \).

fun_on_quotient r f, function_on_quotient r f b, function_on_quotients, fun_on_quotients \( r' f \), the function obtained from \( f \) on passing to the quotient of \( r \) (or \( r \) and \( r' \)).

fun_set_to_prod E X is the canonical bijection between \( \prod_X \iota^E \) and \( \prod_X E \iota^E \).

gcompose f g, \( f \circ g \), composition of two graphs, assumes that range \( g \) is a subset of domain \( f \).

gge r x y, \( x \geq y \), says that \( y \leq x \). \( ^{14} \)

ggt r x y, \( x > y \), says that \( x \geq y \) and \( x \neq y \). \( ^{14} \)

gle r x y, \( x \leq y \), says that \( x \) and \( y \) are related by \( r \). \( ^{14} \)

glt r x y, \( x < y \), says \( x \leq y \) and \( x \neq y \). \( ^{14} \)

graph f is a part of a correspondence.

graph_of_function X Y is the function \( f \mapsto G_f \) defined on \( \Phi(E,F) \), where \( G_f \) is the graph of \( f \). \( ^{22} \)

graph_of_partition, is the function \( \circ \mapsto \circ \), see partition_relation_set. \( ^{23} \)

graph_on r X is the graph of the relation \( r \) restricted to \( X \).

graph_order E F G, graph_order_r E F G is the order defined on \( E^G \) by \( \forall x, f(x) \prec_G g(x) \), \( ^{24} \).

greatest_element r a is the property that \( a \) is the greatest (unique maximal) element of the substrate of the order \( r \). \( ^{30} \)

greatest_lower_bound r X a is the property that \( a \) is the greatest element of the set of lower bounds of \( X \). \( ^{34} \)

has_infimum r X says that \( X \) has an infimum. \( ^{34} \)

has_inf_graph r f says that the image of the graph \( f \) has an infimum. \( ^{37} \)

has_supremum r X says that \( X \) has a supremum. \( ^{34} \)

has_sup_graph r f says that the image of the graph \( f \) has a supremum. \( ^{37} \)

identity A, \( 1_A \), is is the graph of the identity function on the set \( A \).

identity_fun A, \( 1_A \), is the identity function on the set \( A \).

IM stands for the image of a function. Its axioms implement the Schema of Selection and Union.
image_by_fun \( f A \), \( f (A) \), is \( \{ t, \exists x \in A, t = f (x) \} \).

image_by_graph \( f x \), \( f (A) \), is \( \{ t, \exists x \in A, (x, t) \in f \} \).

image_of_fun \( f \) is the image of \( f \).

\( \text{inc} x y \) or \( x \in y \) means that \( x \) is an element of \( y \).

inclusionC \( x y \), \( I_{xy} \), it is the inclusion map on \( x \subset y \) as a Coq function.

inclusion_order \( A \), is the order induced by \( \subset \) on \( \mathcal{P}(A) \) [15].

inclusion_suborder \( A \), is the order induced by \( \subset \) on \( A \) [15].

increasing_map \( f s r r' \), increasing_fun \( f r r' \) is a function such that \( x \leq r y \) implies \( f(x) \leq r' f(y) \), [26].

increasing_pre \( f r r' \) says that \( f \) is an increasing function for preorders \( r \) and \( r' \), [163].

increasing_sequence \( f r \) says that \( f \) is an increasing function with source \( N \) and target \( r \), [148].

induced_relation \( R A \), \( R_A \), is the equivalence induced by \( R \) on \( A \).

induced_order \( R A \), \( R_A \), is the order induced by \( R \) on \( A \) [15].

induction_defined \( s a \) is the function \( f \) defined by \( f(0) = a \) and \( f(n + 1) = s(f(n)) \), [142].

induction_defined\( 1 E h a \) is the function \( f \) defined by \( f(0) = a \) and \( f(n + 1) = h(n, f(n)) \), [142].

induction_defined\( 2 E h a p \) is the function \( f \) defined for \( n < p \) by \( f(0) = a \) and \( f(n + 1) = h(n, f(n)) \), [142].

inductive_set \( r \) means that \( r \) is an order whose substrate is inductive, [57].

inf \( r x y \), \( \text{inf}(x, y) \), is the greatest lower bound of pair \( \{ x, y \} \) (if it exists), [34].

infinum \( r X \), \( \text{inf}_E X \), is the greatest lower bound of \( X \) (if it exists), [34].

infinite_set \( x \) means that \( x \) is a not a finite set, [85].

inf_graph \( r f \), \( \text{inf}(f(x)) \), is the greatest lower bound of the image of the graph \( f \) (if it exists), [37].

injective \( f \), injectiveC \( f \), means that \( f \) is an injection.

in_same_coset \( f \) is the relation “there exists \( i \) such that \( x \in f(i) \) and \( y \in f(i) \)” between \( x \) and \( y \).

intersection \( X \cap X \), is the intersection of a set of sets.

intersection\( 1 f \), intersection\( f x f \), intersection\( \bigcap \{ X_i \}_{i \in I} \) is the set of elements \( a \) such that \( \forall i \in I \) we have \( a \in X_i \).

intersection\( 2 X Y, X \cap Y \), is the intersection of two sets.

intersection_covering, intersection of coverings,.

interval_oo \( r a b \), interval_oc \( r a b \), interval_ou \( r a b \), interval_co \( r a b \), interval_cc \( r a b \),

interval_cu \( r a b \), interval_uo \( r b n \), interval_uc \( r b interval_uu \), [44].

interval_Bnat \( a b \), interval_co_0a \( c \) is the interval \([a, b]\) or \([0, c]\) as a subset of \( N \), [105]

interval_Bnato \( a b \), interval_Bnatco \( a \) is the interval \([a, b]\) or \([0, c]\) as an ordered set, [106]

inverse_direct_value \( f X, X_f \), is \( f^{-1}(f(X)) \).

inverse_graph \( G, G^{-1} \), inverse graph of the graph \( G \).

inverse_fun \( f \) or inverseC \( a b f H, f^{-1} \), inverse of the function \( f \).

inverse_image \( x f, f^{-1}(x) \), is the inverse value of \( f \) on the set \( x \).

inv_image_relation \( f r \), is the inverse image of the relation \( r \) under the function \( f \).
\begin{align*}
\text{inv_image_by_graph} \ f \ x, \ \text{inv_image_by_fun} \ r \ x, \ f^{-1}(x), \text{direct image of a set by the inverse function} \\
\text{inv_corr_value} \ t \text{ associates to a } t = (G, A, B) \text{ its correspondence } f. \\
\text{inv_graph_canon} \ G \text{ is the bijection } (x, y) \mapsto (y, x) \text{ from } G \text{ to } G^{-1}. \\
\text{is_antisymmetric} \ r \text{ says that the graph } r \text{ is antisymmetric.} \quad [13] \\
\text{is_bounded_interval} \ r \ x, \text{see interval.} \\
\text{is_cardinal} \ x \text{ says that } x \text{ is of the form Card}(x), \quad [69]. \\
\text{is_class} \ r \ x \text{ says that } x \text{ is an equivalence class for } r. \\
\text{is_closed_interval} \ r \ x, \text{see interval.} \\
\text{is_countable_set} \ x \text{ says that } x \text{ is equipotent to } \mathbb{N}, \quad [147]. \\
\text{is_correspondence} \ f \text{ says that } f \text{ is associated to a triple } (G, A, B). \\
\text{is_equivalence} \ r \text{ says that the graph } r \text{ is an equivalence.} \\
\text{is_expansion} \ f \ b \ k \text{ say that } f \text{ is a functional graph, defined for } i < k \text{ and such that } f_i < b, \quad [123]. \\
\text{is_finite_c} \ x, \text{is_finite_set} \ y: \text{a cardinal } x \text{ is finite if } x \neq x + 1, \text{a set is finite if its cardinal is finite}, \quad [82]. \\
\text{is_function} \ f \text{ says that } f \text{ is a function in the sense of Bourbaki.} \\
\text{is_graph} \ f \text{ says that } f \text{ is a set of pairs.} \\
\text{is_graph_of} \ g \ r \text{ is true if } g \text{ is the graph of the relation } r. \\
\text{is_infinite_c} \ x \text{ means that } x \text{ is a cardinal that is not finite}, \quad [85]. \\
\text{is_inf_fun} \ r \ f \ x, \text{is_inf_graph} \ r \ f \ x, \text{ says that } x \text{ is the supremum of the image of the function of graph } f \text{ for the order } r, \quad [37]. \\
\text{is_interval} \ r \ x, \text{see interval.} \\
\text{is_left_inverse} \ r \ f \text{ means that } r \text{ is a retraction or left-inverse of } f, \text{ and } r \circ f \text{ is the identity.} \\
\text{is_left_unbounded_interval} \ r \ x, \text{see interval.} \\
\text{is_open_interval} \ r \ x, \text{see interval.} \\
\text{is_reflexive} \ r \text{ says that the graph } r \text{ is reflexive.} \\
\text{is_restriction} \ f \ g \text{ says that } f \text{ is the restriction of } g \text{ to some set.} \\
\text{is_right_inverse} \ s \ f \text{ means that } s \text{ is a section or right-inverse of } f, \text{ and } f \circ s \text{ is the identity.} \\
\text{is_right_unbounded_interval} \ r \ x, \text{see interval.} \\
\text{is_segment} \ r \ s, \text{says that } s \text{ is the interval } [x, y] \text{ or the whole substrate of a well ordered relation } r, \quad [48]. \\
\text{is_semi_open_interval} \ r \ x, \text{see interval.} \\
\text{is_singleton} \ x \text{ means that } x \text{ is a singleton.} \\
\text{is_sup_fun} \ r \ f \ x, \text{is_sup_graph} \ r \ f \ x, \text{ says that } x \text{ is the supremum of the image of the function or graph } f \text{ for the order } r, \quad [37]. \\
\text{is_symmetric} \ r \text{ says that the graph } r \text{ is symmetric.} \\
\text{is_unbounded_interval} \ r \ x, \text{see interval.} \\
\text{is_transitive} \ r \text{ says that the graph } r \text{ is transitive.} \\
\text{J} \ x \ y, \text{or } (x, y), \text{is an ordered pair, formed of two items } x \text{ and } y. \\
\text{nil} \text{ is the empty list.} \\
L X f, \text{fcreate } X f, \mathcal{L}_X f \text{ is the graph formed of all } (x, f(x)) \text{ with } x \in X. \\
\end{align*}
largest\_partition \(x\) is the set of all singletons of \(x\).

lattice \(r\), is a relation for which \(\sup(x, y)\) and \(\inf(x, y)\) exist, \(42\).

least\_element \(r\) \(a\) ids the property that \(a\) is the least (unique minimal) element of the substrate of the order \(r\), \(30\).

least\_upper\_bound \(r\) \(X\) \(a\) is the property that \(a\) is the least element of the set of upper bounds of \(X\), \(34\).

left\_directed \(r\) means that each doubleton is bounded below, \(41\).

left\_inverse\(C\), left inverse of a Coq function.

lexicographic\_order \(r\) \(f\) \(g\), lexicographic\_order\_r \(r\) \(f\) \(g\), lexicographic\_order\_axioms \(r\) \(f\) \(g\):
assume that \(f\) is a family of sets with index \(I\), \(g\) is a family of orders with index \(I\) such that the substrate of \(g_i\) is \(f_i\), and \(r\) is a well-ordering on \(I\); these conditions are the axioms; they allow to define an ordering and an order relation on the product of the family \(f\), \(59\).

LHS is the left hand side of an equality.

list\_range \(L\) is the smallest set containing all elements of the list, \(112\)

list\_subset \(L\) \(E\) says that all elements of the list \(L\) belong to the set \(E\), \(112\)

list\_sum \(L\), list\_prod \(L\), is the sum or product of the element of the list \(L\), \(115\).

list\_to\_fct \(L\), list\_to\_f \(L\), list\_to\_fctB \(L\), list\_to\_fB \(L\) \(E\), converts the list \(L\) into a mapping \(\mathbb{N} \rightarrow \mathbb{N}\), or a function with source \([0, n]\) and target \(\mathbb{N}\) or \(E\), \(109\), \(110\).

lower\_bound \(r\) \(X\) \(x\) says that for all \(y \in X\), we have \(x \leq r y\), \(33\).

L\variant \(a\) \(b\) \(x\) \(y\), variant \(a\) \(x\) \(y\), L\variantc \(x\) \(y\), these are functions whose range is the doubleton \([x, y]\).

maximal\_element \(r\) \(a\) says that \(x \leq r a\) implies \(x = a\), \(28\).

merge\_int \(n\) \(m\) is a bijection \(\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}\), \(145\).

minimal\_element \(r\) \(a\) says that \(x \geq r a\) implies \(x = a\), \(28\).

monotone\_fun \(f\) \(r\) \(r'\) is a, increasing or decreasing function, \(26\).

mutually\_disjoint \(f\) says that for all distinct \(i\) and \(j\), \(f(i)\) and \(f(j)\) are disjoint.

nat, \(\mathbb{N}\) is the type of natural integers in Coq.

nat\_to\_B, \(\mathcal{N}\) is the canonical bijection from \(\text{nat}\) to the set of finite cardinals, \(95\).

nat\_R \(n\) is maps a natural number onto a pseudo-ordinal, \(92\).

neq \(x\) \(y\), \(x \neq y\), is inequality.

\(\text{Nquo}\) \(a\) \(b\) and \(\text{Nrem}\) \(a\) \(b\) are the quotient and remainder in the division of \(a\) by \(b\), \(120\).

\(\text{number\_of\_injections}\) \(b\) \(a\) is \(a!/(a-b)!\), \(126\).

\(\text{of\_finite\_character}\) \(x\) says that \(x\) is of finite character, \(89\).

\(\text{one\_point}\) is the basic singleton.

\(\text{opposite\_relation}\) \(r\) is the relation \(r(y, x)\) between \(x\) and \(y\), \(13\).

\(\text{opposite\_order}\) \(r\) is inverse graph of \(r\), \(13\).

\(\text{order}\) \(r\) says that the graph \(r\) is an order, \(14\).

\(\text{order\_associated}\) \(r\) is the order associated to a preorder by passing on the quotient of “\(x < y\) and \(y < x\)”, \(19\).

\(\text{order\_axioms}\) \(r\) \(s\) is the condition on which \(r\) is an order on \(s\), \(21\).

\(\text{order\_c}\) \(f\) \(r\) says that the graph of the function \(r\) is an order, \(14\).

\(\text{order\_isomorphism}\) \(f\) \(r\) \(r'\) says that \(f\) is an injective increasing function from the support of the order \(r\) into the support of the order \(r'\), \(21\).
order_morphism \( f \) \( r \) \( r' \) says that \( f \) is an injective increasing function from the support of the order \( r \) into the support of the order \( r' \). \[21\.

order_\_r \( r \) says that the relation \( r \) is an order, \[13\.

order_\_re \( r \) \( x \) says that the relation \( r \) is an order on \( x \), \[14\.

order_\_with_\_greatest \( r \) \( a \) is the order obtained from \( r \) by adjoining a greatest element \( a \). \[32\]

\( \text{ordinal}\_\_sum \text{ r f g} \), \( \sum_{i \in I} X_i \), is the ordinal sum of the family of sets \( f(i) \), where each set is ordered by \( g(i) \) and the index set by \( r \). \[61\].

\( \text{ordinal}\_\_sum2 \text{ r r'} \), \( E_1 + E_2 \), is ordinal sum of two sets. \[61\].

\( P \) \( z \), \( \text{pr}_1 \) \( z \) denotes \( x \) if \( z \) is the pair \( (x, y) \).

partial_\_fun1 \( f \) \( y \), partial functions.

partition \( y \) \( x \), partition_\_s \( y \) \( x \), partition_\_fam \( f \) \( x \), thee variants that say that \( y \) or \( f \) is a partition of \( x \).

partition_\_fun_\_of_\_set \( Y \) \( X \) is the canonical injection from \( Y \) \( \text{int} \) \( \mathcal{P}(X) \), (if \( Y \) is a partition of \( X \) then \( Y \in \mathcal{P}(\mathcal{P}(X)) \)) \[16\].

partition_\_relation \( f \) \( x \) is the equivalence relation associated to the partition \( f \) of \( x \).

partition_\_relation_\_set \( y \) \( x \), \( \tilde{\omega} \), is the graph of the equivalence associated to the partition \( y = \tilde{\omega} \) of \( x \), \[17\].

partition_\_with_\_complement \( X \) \( A \), is the partition of \( X \) formed of \( A \) and its complementary set.

partition_\_with_\_pi_\_elements \( p \) \( E \) \( f \) says that the sets \( f(i) \) are of cardinal \( p_i \), mutually disjoint and form a covering of \( E \). \[127\].

pow \( x \) \( y \), \( x^y \), is the power function on the type \( \text{nat} \). \[95\].

powerset \( x \) , \( \mathcal{P}(x) \), is the set of subsets of \( x \).

\( \text{pr}_1 \) \( z \), \( \text{pr}_2 \) \( z \) stand for \( \text{pr}_1 \) \( z \) and \( \text{pr}_2 \) \( z \). These are also denoted by \( P \) and \( Q \). If \( z \) is the pair \( (x, y) \), these functions return \( x \) and \( y \) respectively.

\( \text{pr}_i \) \( f \) \( i \), \( \text{pr}_\text{it} \) \( f \) \( i \), \( \text{pr}_i \) \( f \) , denotes a component of an element of a product.

\( \text{pr}_j \) \( f \) \( J \), \( \text{pr}_\text{J} \) \( f \) , is the function \( (x_\iota)_{\iota \in I} \mapsto (x_\jmath)_{\jmath \in J} \).

prec \( x \) is the finite cardinal \( y \) whose successor is \( y \). It exists if \( x \) is a non-zero finite cardinal, \[83\].

preorder \( r \) is a reflexive and transitive graph, \[19\].

preorder_\_r \( r \) is a reflexive and transitive relation, \[19\].

prod_\_assoc_\_map is the function whose bijectivity is the “theorem of associativity of products”.

prod_\_of_\_function \( u \) \( v \), is the function \( x \mapsto (u(x), v(x)) \).

prod_\_of_\_products_\_canon \( F \) \( F' \), is the bijection between \( \prod F_i \times \prod F'_i \) and \( \prod(F_i \times F'_i) \).

prod_\_of_\_relation \( R \) \( R' \), \( R \times R' \), is the product of two equivalences.

product \( A \) \( B \), \( A \times B \), is the set of all pairs \( (a, b) \) with \( a \in A \) and \( b \in B \)

product_\_I \( X \) \( product \_b \) \( g \) or \( product_\_f \) \( f \) \( \prod_{i \in I} X_i \) is the product of a family of sets.

product_\_1 \( x \) \( a \) is the product of the family defined on the singleton \{\( a \)\} via value \( x \).

product_\_1_\_canon \( x \) \( a \) is the canonical application from \( x \) into \( \text{product}_\_1 \) \( x \) \( a \).

product_\_2 \( x \) \( y \) is the product of the family defined on the doubleton \{\( a, b \)\} via value \( x \) and \( y \).

product_\_2_\_canon \( x \) \( y \) is the canonical application from \( x \times y \) into \( \text{product}_\_2 \) \( x \) \( y \).

product_\_compose, auxiliary function used for change of variables in a product.
product_order \ f \ g, \ product_order_r \ f \ g, \ is \ the \ order \ on \ the \ product \ \prod X_i \ induced \ by \ \Gamma_i \n
(\text{where } f \ \text{defines the family } X_i \ \text{and } g \ \text{defines the family } \Gamma_i) , [24].

pseudo_ordinal \ x \ says \ that \ x \ is \ a \ pseudo-ordinal, \ [90].

Q \ z, \ pr_2\!\!z \ denotes \ y \ if \ z \ is \ the \ pair \ (x, y).

quotient \ R, \ E/R, \ is \ the \ set \ of \ equivalence \ classes \ of \ R

quotient_of_relations \ r \ s, \ R/S, \ is \ the \ quotient \ of \ two \ equivalences

quotient_order_r \ r \ s \ is \ the \ preorder \ relation \ induced \ in \ the \ quotient \ E/S \ by \ the \ pre-

order \ \triangleright, \ \text{where } E \ \text{is the common substrate of } R \ \text{and } S, [163].

range \ f \ is \ the \ set \ of \ y \ for \ which \ there \ is \ an \ x \ with \ (x, y) \in \ f, \ \text{it} \ \text{is} \ \text{pr}_2\langle f \rangle.

reflexive_r \ r \ x \ says \ that \ the \ relation \ r \ is \ reflexive \ in \ x.

related \ r \ x \ y \ \text{is a short-hand for} \ (x, y \in \ r) \ \text{or} \ \text{pr}_2\langle r \rangle.

relation_on_quotient \ p \ r \ is \ the \ relation \ induced \ by \ p(x) \ on \ passing \ to \ the \ quotient \ (with \ respect \ to \ x) \ with \ respect \ to \ R.

rep \ x \ is \ an \ element \ y \ such \ that \ y \in x, \ whenever \ x \ is \ not \ empty.

representative_system \ f \ x \ means \ that, \ for \ all \ i, \ s \cap X_i \ is \ a \ singleton, \ where \ X_i \ is \ a \ partition \ of \ x \ associated \ to \ the function \ f.

representative_system_function \ g f x \ means \ that \ g \ is \ an \ injection \ whose \ image \ is \ a \ system \ of \ representatives \ (see \ definition \ above).

restr \ x \ G \ is \ the \ restriction \ to \ x \ of \ the \ graph \ G.

rest_plus_interval \ a b, \ rest_minus_interval \ a b \ are \ the \ function \ x \mapsto x+b \ and \ x \mapsto x−b \ as \ bijections \ between \ \{0, a\} \ \text{and} \ \{b, a + b\}, [107].

restriction_function \ f x \ is \ like \ restr, \ \text{but} \ \text{f} \ \text{and} \ \text{the} \ \text{restrictions} \ \text{are} \ \text{functions}.

restriction2_axioms \ f x y \ \text{is} \ \text{the} \ \text{condition:} \ \text{f} \ \text{is} \ \text{a} \ \text{function} \ \text{whose} \ \text{source} \ \text{contains} \ \text{x}, \ \text{whose} \ \text{target} \ \text{contains} \ \text{y}, \ \text{moreover} \ \text{a} \ \in \ \text{x} \ \text{implies} \ \text{f(a)} \ \in \ \text{y}.

restriction2 f x y, \ restriction2C \ f x y, \ restriction \ of \ f \ as \ a \ function \ x \mapsto y.

restrictionC \ f H \ is \ the \ restriction \ to \ x \ of \ the \ function \ f : a \to b, \ \text{where } H \ \text{proves} \ \text{x} \ \subset \ \text{a} \ \text{implicitly}.

restriction_product \ f j \ is \ the \ product \ of \ the \ restrictions \ of \ \prod f \ \text{to} \ \text{J}.

restriction_to_image \ f \ is \ the \ restriction \ of \ the \ function \ f \ \text{to} \ \text{its} \ \text{range}.

restriction_to_segment \ r \ x \ g, \ g^{(x)} \ \text{is} \ \text{the} \ \text{restriction} \ \text{of} \ \text{g} \ \text{to} \ \text{the} \ \text{segment} \ S_x \ \text{defined} \ \text{by} \ \text{the} \ \text{order} \ \text{r}, [53].

restriction_to_segment_axiom \ r \ x \ g \ \text{is} \ \text{the} \ \text{property} \ \text{for} \ \text{restriction_to_segment} \ \text{to} \ \text{be} \ \text{well-behaved}, [53].

retraction: \ \text{see} \ \text{is_left_inverse}.

RHS \ is \ the \ right \ hand \ side \ of \ an \ equality.

right_directed \ r \ means \ that \ each \ doubleton \ is \ bounded \ above, [41].

right_inverseC, \ right inverse \ of \ a \ Coq \ function.

Ro \ x \ or R x \ converts \ its \ argument \ x \ of \ type \ u \ to \ a \ set, \ which \ is \ an \ element \ of \ u.

saturated \ r \ x \ means: \ \text{for every} \ y \in x, \ \text{the} \ \text{class} \ \text{of} \ \text{x} \ \text{for} \ \text{the} \ \text{relation} \ \text{r} \ \text{is} \ \text{a} \ \text{subset} \ \text{of} \ \text{x}.

satisfaction_of \ r \ x \ is \ the \ satisfaction \ of \ x \ \text{for} \ \text{r}.

second_proj \ g \ is \ the \ function \ x \mapsto pr_2 x \ \text{(} x \in g \).}

section: \ \text{see} \ \text{is_right_inverse}.

section_canon_proj \ R \ is \ the \ function \ from \ E/R \ into \ E \ induced \ by \ rep.
segment $r x$, $S_x$, is the interval $] -\infty, x [$, $[48]$.  
Set or $\mathcal{E}$ is the type of sets.

$\text{set_for_equi} \text{potent} \_\text{inf} E \psi$ is a set used when proving that $E$ is equi- 
potent to $E \times E$ when $E$ is infinite, $[146]$.  
$\text{set_of_correspondences} A B$ means the set of triples 
$\text{set_of_cardinals} \_\text{le} x$ is the set of all cardinals $\leq x$, $[72]$.  
$\text{set_of_endomorphisms} E$, is the set of triples $(G, E, E)$ associated to functions from $E$ into $E$.  
$\text{set_of_finite_subsets} x$ is the set of finite subset sof $x$, $[88]$.  
$\text{set_of_functions} E F$, denoted $\mathcal{F}(E; F)$, is the set of triples $(G, E, F)$ associated to func- 
tions from $E$ into $F$.  
$\text{set_of_functions} \_\text{sum} \_\text{le} E n$, $\text{set_of_functions} \_\text{sum} \_\text{eq} E n$ is the set of functions $f : E \rightarrow [0, n]$ such that the sum $\sum f(i)$ is $\leq n$ or $\neq n$, $[136]$.  
$\text{set_of_gfunctions} E F$, denoted $\Phi E$, is the set of graphs of functions from $E$ to $F$.  
$\text{set_of_injections} E F$ is the set of injective functions from $E$ into $F$, $[126]$.  
$\text{set_of_partition} p E$ is the set of all partitions $X_i$ of $E$, where each $X_i$ has $p_i$ elements, $[127]$.  
$\text{set_of_partition} \_\text{set} X$ is the set of all partitions of $X$, $[16]$.  
$\text{set_of_permutations} E F$, is the set of injective functions from $E$ onto itself, $[126]$.  
$\text{set_of_segments} r$, $\text{set_of_segments} \_\text{strict} r$, is the set of all segments of an ordered set 
(with possible exclusion of the whole set), $[50]$.  
$\text{set_of_sub_functions} E F$, denoted $\Phi(E; F)$ is the set of triples $(G, A, F)$ associated to 
functions from $A \subset E$ into $F$.  
$\text{set_of_graphs} E F$, is the set of functional graphs from $E$ to $F$, $[22]$.  
$\text{set_of_preorders} E$, is the set of preorders on $E$, $[23]$.  
$\text{singleton} x$, $\{x\}$, is a set with one element.  
$\text{single_list_prop} A L Q$ says that all elements of the list $L$ of type $A$ satisfy the predicate $Q$, $[111]$.  
$\text{sof_value} x y z$ converts three elements into a correspondence,.  
$\text{small_set} x$ means that $x$ hast at most one element.  
$\text{smallest_partition} x$ is the singleton $\{x\}$.  
$\text{source} f$ contains (resp. is equal to) the domain of the graph of a correspondence $f$ 
(resp. function $f$).  
$\text{stationary_sequence} f$ says that the restriction of $f$ to some interval $[n, \rightarrow [ \$ is constant, $[149]$.  
$\text{strict_decreasing_map} f s r^r$, $\text{strict_decreasing_fun} f r r'$ is a function such that $x <_r y$ 
implies $f(x) >_{r'} f(y)$, $[26]$.  
$\text{strict_increasing_map} f s r^r$, $\text{strict_increasing_fun} f r r'$ is a function such that $x <_r y$ 
implies $f(x) <_{r'} f(y)$, $[26]$.  
$\text{strict_monotone_fun} f r r'$ is a strictly increasing or strictly decreasing function, $[26]$.  
$\text{strict_sub} x y$, $x \subset y$, means $x \subset y$ and $x \neq y$.  
$\text{sub} x y$, $x \subset y$, means that $x$ is a subset of $y$.  
$\text{substrate} r$ is the union of the domain and range.  
$\text{subsets_with_p_elements} p E$, is the set of subsets of $E$ having $p$ elements, $[130]$.  

RR n° 7150
succ $x$ is $x + 1$, \[\text{(82)}\].

sup $r x y$, sup$(x, y)$, is the least upper bound of the pair \{x, y\} (if it exists), \[\text{(54)}\].

supremum $r X$, sup$_E X$, is the least upper bound of $X$ (if it exists), \[\text{(54)}\].

sup$_{graph}$ $r f$, sup $f(x)$, is the least upper bound of the image of the graph $f$ (if it exists), \[\text{(37)}\].

surjective $f$, surjective$_C f$, means that $f$ is a surjection.

symmetric$_r r$ says that the relation $r$ is symmetric.

target $f$ contains the range of the graph of the correspondence $f$.

trans$_f$$_A B$ \[\text{(L35)}\] says that $f$ is a function.

trans$_f$$_A B$ \[\text{(L35)}\] says that $f$ is defined by transfinite induction on the set $E$, well-ordered by $r$, via the property $p$, \[\text{(53)}\].

trans$_f$$_A B$ \[\text{(L35)}\] says that the relation $r$ is transitive.

transitive set $x$ says that if $a \in b$ and $b \in x$ then $a \in x$, \[\text{(90)}\].

total order $r$ means that $r$ is a total order, \[\text{(43)}\].
two_points is the basic doubleton.

union $X$, \[\bigcup X\], is the union of a set of sets.

union$_I f$, union$_f x f$, union$_g \bigcup_i X_i$ is the set elements $a$ with $a \in X_i$ for some $i \in I$.

union2 $a b$, $a \cup b$, is the union of two sets.

upper bound $r X x$ says that for all $y \in X$, we have $y \leq_r x$, \[\text{(53)}\].

V$_x f$, V$_x (x, f)$ or V$_f x$, is the value at the point $x$ of the graph $f$.

variant, see Lvariant.

W$_x f$, W$_f x$, is the value at the point $x$ of the function $f$.

well-ordered set, well-ordering relation, well-ordering: see worder.

 worder $r$ says that $r$ is a well-ordering, \[\text{(47)}\].

worder$_r r$ says that $r$ is a relation, that induces a well-ordering on each set where it is reflexive, \[\text{(69)}\].

X$_a f y$, $\mathcal{X}(f, y)$, this is $f(x)$ if $y = x$.

Y$_o P x y$, $\mathcal{Y}(P, x, y)$, is a function that associates to $z$ the value $x$ is $P$ is true, and $y$ if $P$ is false.

Z$_o R$, $\mathcal{Z}(x, R)$, $\mathcal{E}_x(R)$ or \{x, R\}: it is the set of all $x$ that satisfy $R$. 

INRIA
Index

addition, 72
antisymmetric, 13
associated, 19
bijective, 21
binomial coefficient, 129
cardinal, 65, 68
cofinal, 32
coinitial, 32
comparable, 43
compatible, 19
contraction, 112
decreasing, 26
difference, 102
disjoint, 67
doubleton, 66
equipotent, 66
equivalence, 19
extension, 16, 22
factorial, 125
finer, 16
finite, 82
greatest, 29
greatest lower bound, 34
increasing, 26
induced, 21
induction, 52, 86, 140
inf, 34
infimum, 34
infinite, 85, 139
injective, 21
integer, 82
intersection, 36
interval, 44, 86, 105
isomorphism, 21
lattice, 42
least, 29
least upper bound, 34
lexicographic product, 59
lower bound, 33
max, 30
maximal, 28
min, 30
minimal, 28
monotone, 26
morphism, 21
multiplication, 72
natural integer, 85
opposite, 13
order, 13
ordinal sum, 61
partition, 16
predecessor, 83
product, 24, 66, 72
pseudo-ordinal, 90
quotient, 118
range, 112
reflexive, 13
remainder, 118
segment, 48
singleton, 29, 66
subtraction, 102
successor, 82
sum, 72
sup, 54
supremum, 54, 72
symmetric, 13
total, 29, 43
transitive, 13
union, 36, 67
upper bound, 33
well-ordering, 47
Bibliography


# Contents

## 1 Introduction

1.1 Objectives ........................................... 3  
1.2 Content of this document ............................... 3  
1.3 Terminology ........................................... 4  
1.4 Tactics ................................................ 5  
1.5 Removed theorems ...................................... 6  
1.5.1 Definition of a function by induction ............. 7  
1.5.2 Intervals ........................................... 8

## 2 Order relations. Ordered sets .......................... 13

2.1 Definition of an order relation ......................... 13  
2.2 Preorder relations ..................................... 18  
2.3 Notation and terminology ............................... 20  
2.4 Ordered subsets. Product of ordered sets ............. 21  
2.5 Increasing mappings .................................... 26  
2.6 Maximal and minimal elements ......................... 28  
2.7 Greatest element and least element .................... 29  
2.8 Upper and lower bounds ................................ 33  
2.9 Least upper bound and greatest lower bound ........... 34  
2.10 Directed sets ......................................... 41  
2.11 Lattices ............................................... 42  
2.12 Totally ordered sets .................................. 43  
2.13 Intervals ............................................... 44

## 3 Well-ordered sets .................................... 47  

3.1 Segments of a well-ordered set ......................... 47  
3.2 The principle of transfinite induction .................. 52  
3.3 Zermelo's theorem ..................................... 55  
3.4 Inductive sets .......................................... 56
3.5 Isomorphisms of well-ordered sets ................................. 58
3.6 Lexicographic products .............................................. 59
3.7 Ordinals ............................................................... 60

4 Equipotent Sets. Cardinals ........................................... 65
4.1 The cardinal of a set .................................................. 66
4.2 Order relation between cardinals .................................. 69
4.3 Operations on cardinals .............................................. 72
4.4 Properties of the cardinals 0 and 1 ............................... 75
4.5 Exponentiation of cardinals ........................................ 77
4.6 Order relation and operations on cardinals ..................... 79

5 Natural integers. Finite sets ........................................... 81
5.1 Definition of integers ................................................ 82
5.2 Inequalities between integers ..................................... 83
5.3 The set of natural integers ......................................... 85
5.4 The principle of induction ......................................... 86
5.5 Finite subsets of ordered sets ..................................... 88
5.6 Properties of finite character ..................................... 89
5.7 Finite cardinals and the type nat ................................ 89
5.7.1 Pseudo-ordinals .................................................. 89
5.7.2 Pseudo-ordinals and the type nat ............................ 91
5.7.3 Bijection between nat and the integers ..................... 94

6 Properties of integers .................................................. 97
6.1 Operations on integers and finite sets ......................... 97
6.2 Strict inequalities between integers ............................. 99
6.3 Intervals in sets of integers ...................................... 105
6.4 Finite sequences ..................................................... 108
6.4.1 Lists as functions ............................................. 109
6.4.2 Contracting lists ............................................... 114
6.5 Characteristic functions on sets ................................. 117
6.6 Euclidean Division .................................................. 118
6.7 Expansion to base b ................................................ 121
6.8 Combinatorial analysis ............................................. 124
6.8.1 Iterated functions ............................................. 124
6.8.2 Factorial ......................................................... 125
6.8.3 Number of injections ......................................... 125
6.8.4 Number of coverings ........................................... 127
6.8.5 The binomial coefficient ...................................... 129
6.8.6 Number of increasing functions .......................... 132
6.8.7 Number of monomials ......................................... 135

7 Infinite sets .............................................................. 139
7.1 The set of natural integers ...................................... 139
7.2 Definition of mappings by induction ...................... 140
7.3 Properties of infinite cardinals ............................... 145
7.4 Countable sets ...................................................... 147
7.5 Stationary sequences ............................................ 148

8 The size of one ........................................................ 151

9 Exercises ............................................................... 157
9.1 Section 1 .............................................................. 162
9.2 Section 2 .............................................................. 248
9.3 Section 3 .............................................................. 254
9.4 Section 4 .............................................................. 255
9.5 Section 5 .............................................................. 258
9.6 Section 6 .............................................................. 262

10 Theorems, Notations, Definitions